DrayTek

Vigor2927 Series

Dual-WAN Security Router

USER'S GUIDE

V1.6

Serie Vigor2927

Enrutador de seguridad de doble WAN

Guía de usuario

Versión: 1.6

Versión de firmware: V4.4.2.2

(Para actualizaciones futuras, visite el sitio web de DrayTek)

Fecha: 5 de enero de 2023

derechos de autor

© Todos los derechos reservados. Esta publicación contiene información que está protegida por derechos de autor. Ninguna parte puede ser reproducida, transmitida, transcrita, almacenada en un sistema de recuperación o traducida a ningún idioma sin el permiso por escrito de los titulares de los derechos de autor.

Marcas registradas

En este documento se utilizan las siguientes marcas comerciales:

- Microsoft es una marca registrada de Microsoft Corp.
- Windows, Windows 7, 8, 10, 11 y Explorer son marcas comerciales de Microsoft Corp.
- Apple y Mac OS son marcas registradas de Apple Inc.
- Otros productos pueden ser marcas comerciales o marcas comerciales registradas de sus respectivos fabricantes.

Instrucciones de seguridad

- Lea detenidamente la guía de instalación antes de configurar el enrutador.
- El enrutador es una unidad electrónica complicada que solo puede ser reparada por personal autorizado y calificado. No intente abrir o reparar el enrutador usted mismo.
- No coloque el enrutador en un lugar húmedo o húmedo, por ejemplo, un baño.
- El enrutador debe usarse en un área protegida, dentro de un rango de temperatura de +5 a +40 Celsius.
- No exponga el enrutador a la luz solar directa u otras fuentes de calor. La carcasa y los componentes electrónicos pueden dañarse con la luz solar directa o fuentes de calor.
- No despliegue el cable para la conexión LAN al aire libre para evitar riesgos de descargas eléctricas.
- Mantenga el paquete fuera del alcance de los niños.
- Cuando desee desechar el enrutador, siga las normas locales sobre conservación del medio ambiente.

Garantía

-Garantizamos al usuario final original (comprador) que el enrutador estará libre de defectos de fabricación o materiales durante un período de dos (2) años a partir de la fecha de compra al distribuidor. Guarde su recibo de compra en un lugar seguro, ya que sirve como prueba de la fecha de compra. Durante el período de garantía, y previa prueba de compra, si el producto tiene indicios de falla debido a mano de obra o materiales defectuosos, repararemos o reemplazaremos, a nuestra discreción, los productos o componentes defectuosos, sin cargo por piezas o mano de obra. , en la medida en que lo consideremos necesario, almacene el producto en condiciones de funcionamiento adecuadas.
Cualquier reemplazo consistirá en un producto funcionalmente equivalente nuevo o refabricado de igual valor, y se ofrecerá únicamente a nuestra discreción. Esta garantía no se aplicará si el producto se modifica, se usa indebidamente, se altera, se daña por fuerza mayor o se somete a condiciones de trabajo anormales. La garantía no cubre el software incluido o con licencia de otros proveedores. Los defectos que no afecten significativamente la usabilidad del producto no estarán cubiertos por la garantía. Nos reservamos el derecho de revisar el manual y la documentación en línea y de realizar cambios de vez en cuando en el contenido del mismo sin obligación de notificar a ninguna persona sobre dicha revisión o cambios.

Ser un propietario registrado

-Se prefiere el registro web. Puede registrar su enrutador Vigor a través de https://myvigor.draytek.com.

Actualizaciones de firmware y herramientas

-Debido a la evolución continua de la tecnología DrayTek, todos los enrutadores se actualizarán periódicamente. Consulte el sitio web de DrayTek para obtener más información sobre el firmware, las herramientas y los documentos más recientes.

https://www.draytek.com

Parte I Instalación i

I-1 Introducción 1

I-1-1 Indicadores y conectores 2

I-1-1-1 Vigor2927 2
I-1-1-2 Vigor2927L 4
I-1-1-3 Vigor2927ac / Vigor2927ax / Vigor2927Lac 6
I-1-1-4 Vigor2927Vac 10

I-1-2 Notas para la instalación de la antena (para el modelo "L") 12

I-2 Instalación de hardware 14

I-2-1 Instalación del enrutador Vigor 14

I-2-2 Instalación montada en la pared 15

I-2-3 Instalación de la impresora USB en el enrutador Vigor .... dieciséis

I-3 Acceso a la página web 23

I-4 Cambio de contraseña 25

Tablero I-5 26

I-5-1 Panel virtual 27

I-5-2 Nombre con un enlace 28

I-5-3 Estado de LTE..... 28

I-5-4 Acceso rápido para el menú de uso común 29

I-5-5 Mapa de interfaz gráfica de usuario 30

I-5-6 Consola web 31

I-5-7 Copia de seguridad de configuración 32

I-5-8 Descarga del manual 32

I-5-9 Cerrar sesión 32

I-5-10 Estado en línea 33

I-5-10-1 Conexión física..... 33
I-5-10-2 WAN virtual 35

I-6 Asistente de inicio rápido 36

I-6-1 Para WAN1/WAN2 (Ethernet) 37

I-6-2 Para WAN3/WAN4 (Inalámbrico 2.4G/Inalámbrico 5G) 46

I-6-3 Para WAN5/WAN6 (USB) 52

I-7 Asistente de activación del servicio 54

I-8 Registro del enrutador Vigor..... 56

Parte II Conectividad 59

II-1 WAN 60

Interfaz de usuario web 62

II-1-1 Configuración general 62

II-1-1-1 WAN1/WAN2 (Ethernet) ....sesenta y cinco
II-1-1-2 WAN3/WAN4 (Inalámbrica 2.4G o 5G)..... 67
II-1-1-3 WAN5 / WAN6 (USB) o LTE 68

II-1-2 Acceso a Internet..... 70

II-1-2-1 Página de detalles para PPPoE en WAN1/WAN2 (Modo físico: Ethernet) 73
II-1-2-2 Página de detalles para IP estática o dinámica en WAN1/WAN2 (modo físico: Ethernet) 76
II-1-2-3 Página de detalles para PPTP/L2TP en WAN1/WAN2 (Modo físico: Ethernet) 80
II-1-2-4 Página de detalles para WAN3/WAN4 (Modo físico: Wireless 2.4G/ Wireless 5G) ..83 II-1-2-5 Página de detalles para módem USB 3G/4G (modo PPP) en WAN5 / WAN6 85
II-1-2-6 Página de detalles para módem USB 3G/4G (modo DHCP) en WAN5 / WAN6 87
II-1-2-7 Página de detalles para módem USB 3G/4G (modo DHCP) en LTE WAN 90
II-1-2-8 Página de detalles para IPv6: fuera de línea en WAN1/WAN2/WAN5/WAN6 93
II-1-2-9 Página de detalles para IPv6 – PPP en WAN1/WAN2 94
II-1-2-10 Página de detalles para IPv6 – TSPC en WAN1/WAN2/WAN5/WAN6 95
II-1-2-11 Página de detalles para IPv6 – AICCU en WAN1/WAN2/WAN5/WAN6.....97
II-1-2-12 Página de detalles para IPv6: cliente DHCPv6 en WAN1/WAN2.....98
II-1-2-13 Página de detalles para IPv6: IPv6 estático en WAN1/WAN2 100
II-1-2-14 Página de detalles para IPv6 – Túnel estático 6 en 4 en WAN1/WAN2 101
II-1-2-15 Página de detalles para IPv6 – 6.º en WAN1/WAN2 103

II-1-3 Múltiples VLAN 105

II-1-4 Presupuesto de la WAN 110
II-1-4-1 Configuración general 110
II-1-4-2 Estado 113

Notas de aplicación 114
A-1 ¿Cómo configurar Multi-PVC para el despliegue de triple play?..... 114

II-2 LAN 119

Interfaz de usuario web 121

II-2-1 Configuración general 121
II-2-1-1 Página de detalles para LAN1: Configuración de Ethernet TCP/IP y DHCP 123
II-2-1-2 Página de detalles para LAN2 ~ LAN8 y DMZ 127
II-2-1-3 Página de detalles para la subred enrutada IP 129
II-2-1-4 Página de detalles para la configuración de LAN IPv6 131
II-2-1-5 Opciones del servidor DHCP 134

II-2-2 VLAN 136

II-2-3 Vincular IP a MAC 140

II-2-4 Duplicación de puerto LAN 143

II-2-5 Cableado 802.1x 144

II-2-6 Agregación de enlaces 145

II-3 Aceleración de hardware 146

II-4 NAT 148

Interfaz de usuario web 149

II-4-1 Redirección de puertos 149

II-4-2 Anfitrión DMZ 153

II-4-3 Puertos abiertos 156

II-4-4 Activación de puertos 158

II-4-5 ALG 160

II-5 Aplicaciones 161

Interfaz de usuario web 163

II-5-1 DNS dinámico 163

II-5-2 LAN DNS / Reenvío de DNS 169

II-5-3 Seguridad DNS 172

II-5-3-1 Configuración general 172
II-5-3-2 Diagnóstico de dominio 173
II-5-4 Horario 174
II-5-5 RADIO/TACACS+ 177
II-5-5-1 RADIO externo..... 177
II-5-5-2 RADIO Interno 179
II-5-5-3 TACACS+ externo..... 182
II-5-6 Directorio activo/LDAP 183
II-5-6-1 Configuración general 183
II-5-6-2 Directorio activo/Perfiles LDAP 184
II-5-7 UPnP 186
II-5-8 IGMP..... 187
II-5-8-1 Ajustes generales 187
II-5-8-2 Estado de trabajo 188
II-5-9 Despertar en LAN/WAN 189
II-5-10 Servicio de Alerta por SMS / Correo..... 191
II-5-10-1 Alerta SMS 191
II-5-10-2 Alerta por correo 192
II-5-11 Bonjour 193
II-5-12 Alta disponibilidad 196
II-5-12-1 Configuración general..... 197
II-5-12-2 Sincronización de configuración 199
II-5-13 Configuración general local 802.1X 201
Notas de aplicación 203
A-1 ¿Cómo usar DrayDDNS? 203
A-2 ¿Cómo configurar un DDNS personalizado?..... 208
II-6 Enrutamiento 212
Interfaz de usuario web 213
II-6-1 Ruta Estática 213
II-6-2 Balance de Carga/Política de Ruta 218
Diagnóstico para política de ruta 224
II-6-3 BGP 228
II-6-3-1 Ajustes básicos 228
II-6-3-2 Red estática 229
Notas de aplicación 230
A-1 ¿Cómo configurar el mapeo de direcciones con la política de ruta? 230
A-2 ¿Cómo usar el nombre de dominio de destino en una política de ruta?..... 232
A-3 Introducción a la política de ruta/equilibrio de carga 234
II-7 LTE..... 236
Interfaz de usuario web 237
II-7-1 Ajustes generales..... 237
II-7-1-1 Cuota de SMS 237
II-7-1-2 Bandeja de entrada/salida de SMS 238
II-7-2 Bandeja de entrada de SMS 239
II-7-3 Enviar SMS 242
II-7-4 Pasarela SMS..... 243

II-7-5 Comandos del enrutador 247
II-7-6 Estado 249

Parte III LAN inalámbrica 251

III-1 LAN inalámbrica (2,4 GHz/5 GHz) 252
Interfaz de usuario web 255
III-1-1 Asistente inalámbrico 255
III-1-2 Configuración general 259
III-1-3 Seguridad 261
III-1-4 Control de acceso 263
III-1-5 MPS 265
III-1-6 WDS (para 5 GHz) 268
III-1-7 Configuración avanzada 270
III-1-8 Control de la estación 274
III-1-9 Gestión de ancho de banda 275
III-1-10 Descubrimiento AP 276
III-1-11 Imparcialidad en el tiempo aire 277
III-1-12 Dirección de banda (2,4 GHz) 279
III-1-13 Itinerancia 283
III-1-14 Lista de emisoras 284
III-2 Red en malla 286
III-2-1 Asistente de malla 287
III-2-2 Configuración de la malla 291
III-2-3 Estado de la malla 293
III-2-4 Descubrimiento de mallas 294
III-2-5 Sincronización de configuración básica/avanzada 295
III-2-6 Lista de soporte 297

Parte IV VoIP..... 299

IV-1 VoIP 300
Interfaz de usuario web 302
IV-1-1 Asistente de VoIP 302
IV-1-2 Ajustes generales 304
IV-1-3 Cuentas SIP 307
IV-1-3-1 Lista de alias 310
IV-1-4 Plan de marcación 313
IV-1-4-1 Directorio telefónico 313
IV-1-4-Mapa de 2 dígitos 314
IV-1-4-3 Restricción de llamadas 317
IV-1-4-4 Regionales 319
IV-1-5 Configuración del teléfono 321
IV-1-6 Estado 325
IV-1-7 Diagnóstico 327

IV-1-7-1 Identificador de llamadas 327
IV-1-7-2 Tono 327

Parte V VPN 329

V-1 VPN y Acceso Remoto 330

Interfaz de usuario web 331

Asistente de cliente VPN V-1-1 331

Asistente del servidor VPN V-1-2 338

V-1-3 Control de acceso remoto 348

V-1-4 Configuración general de PPP 349

V-1-5 Configuración general de SSL 351

V-1-6 Configuración general de IPsec 353

V-1-7 Identidad de pares IPsec 356

Configuración del comparador de VPN V-1-8 358

V-1-9 VPN abierta 360

V-1-9-1 Configuración del servidor OpenVPN 360
V-1-9-2 Configuración del cliente 362
V-1-9-3 Certificado de Importación 363

V-1-10 Usuario de marcación remota 365

V-1-11 LAN a LAN 370

V-1-12 Gestión de troncales VPN 380

V-1-13 Gestión de conexiones 385

Gestión de certificados V-2 387

Interfaz de usuario web 388

Certificado local V-2-1 388

Certificado de CA de confianza V-2-2 393

Copia de seguridad del certificado V-2-3 397

V-2-4 Certificado autofirmado 398

V-2-5 Lista de Servicios Locales 399

Parte VI Seguridad 401

VI-1 Cortafuegos 402

Interfaz de usuario web 404

VI-1-1 Configuración general 404

VI-1-2 Configuración del filtro 409

VI-1-3 Configuración de defensa 419

VI-1-3-1 Defensa DoS 419
VI-1-3-2 Defensa contra la suplantación de identidad 422

VI-1-4 Diagnosticar 423

VI-2 Gestión de seguridad central (CSM) 426

Interfaz de usuario web 427

VI-2-1 Perfil de aplicación de la aplicación 427

VI-2-2 Actualización de la firma APPE 429

VI-2-3 Perfil de filtro de contenido de URL 431
VI-2-4 Perfil de filtro de contenido web..... 435
VI-2-5 Perfil de filtro DNS 439
Notas de aplicación 441
A-1 Cómo crear una cuenta para MyVigor 441
A-2 Cómo bloquear el servicio de Facebook al que acceden los usuarios a través del filtro de contenido web/filtro de contenido de URL 446

Parte VII Gestión 451

VII-1 Mantenimiento del sistema 452
Interfaz de usuario web 453
VII-1-1 Estado del sistema 453
VII-1-2 TR-069 455
VII-1-2-1 Ajustes de ACS y CPE 455
VII-1-2-2 Configuración de informes 457
VII-1-2-3 Parámetros de exportación 458
VII-1-3 Flujo de red 458
VII-1-4 Contraseña del administrador 459
VII-1-5 Contraseña de usuario 463
VII-1-6 Saludo en la página de inicio de sesión 466
VII-1-7 Copia de seguridad de la configuración 468
VII-1-8 Webhook 471
VII-1-9 Syslog/Alerta de correo 472
VII-1-10 Hora y fecha 475
VII-1-11 SNMP..... 476
VII-1-11 Gestión 478
VII-1-12 Panel de control 482
VII-1-13 Certificado autofirmado 488
VII-1-14 Sistema de reinicio 490
VII-1-15 Actualización de firmware 491
VII-1-16 Copia de seguridad del firmware 492
VII-1-17 Lista de Usuarios del Servicio Interno 493
VII-1-18 Tablero de control 494
VII-2 Gestión del ancho de banda 495
Interfaz de usuario web 496
VII-2-1 Límite de sesiones 496
VII-2-2 Límite de ancho de banda 498
VII-2-3 Calidad de Servicio 500
VII-2-4 QoS de la aplicación 506
VII-3 Gestión de usuarios 507
Interfaz de usuario web 508
VII-3-1 Configuración general 508
VII-3-2 Perfil de usuario 509

VII-3-3 Grupo de usuarios 513
VII-3-4 Estado en línea del usuario 514
Notas de aplicación 516
A-1 Cómo autenticar clientes a través de la Administración de usuarios 516
A-2 Cómo utilizar la función de página de destino 525
VII-4 Portal web de puntos de acceso 529
Interfaz de usuario web 529
Configuración del perfil VII-4-1 529
VII-4-1-1 Método de inicio de sesión 530
VII-4-1-2 Pasos para configurar un perfil de portal web 531
VII-4-2 Información del usuario 550
VII-4-2-1 Información del usuario 550
VII-4-2-2 Configuración de la base de datos 551
VII-4-3 Gestión de cuotas 553
VII-4-4 Generador de PIN 556
VII-4-4-1 Estado del PIN 556
VII-4-4-2 Generador de PIN 557
VII-4-4-3 Generador de PIN JSON 558
VII-4-4-4 Vale PIN 559
Notas de aplicación 561
A-1 ¿Cómo crear una aplicación de Facebook para la autenticación del portal web? 561
A-2 ¿Cómo crear la aplicación de Google para la autenticación del portal web? 567
VII-5 Gestión central (VPN) 569
Interfaz de usuario web 570
VII-5-1 Configuración general 570
VII-5-1-1 Ajustes generales 570
VII-5-1-2 Configuración de IPsec VPN 571
VII-5-2 Gestión de CPE 572
VII-5-2-1 Lista de dispositivos administrados 572
VII-5-2-2 Mantenimiento de CPE 575
VII-5-2-3 Mapa de Google 577
VII-5-3 Gestión de VPN 579
VII-5-4 Registro y alerta 580
Notas de aplicación 581
A-1 Aplicación CVM - ¿Cómo administrar el CPE (router) a través de la serie Vigor2927? . 581 A-2 Aplicación CVM - ¿Cómo actualizar el firmware del CPE a través de la serie Vigor2927? 585
VII-6 Gestión Central (AP) 588
Interfaz de usuario web 589
VII-6-1 Tablero 589
VII-6-2 Estado 590
VII-6-3 Perfil WLAN 591
Mantenimiento de AP VII-6-4 597
VII-6-5 Gráfico de tráfico 598
VII-6-6 Registro de eventos 599
VII-6-7 Tráfico Total 600
VII-6-8 Número de estación 600

VII-6-9 Equilibrio de carga 601
VII-7 Gestión central (interruptor) 603
Interfaz de usuario web 604
VII-7-1 Estado 604
VII-7-1-1 Estado del interruptor 604
VII-7-1-2 Jerarquía de interruptores 606
VII-7-1-3 Información detallada 607
VII-7-1-4 Ajuste TR069 608
VII-7-2 Perfil 610
Grupo VII-7-3 613
VII-7-4 Mantenimiento 615
VII-7-5 Alerta y registro 616
VII-7-5-1 Configuración de alertas 616
VII-7-5-2 Configuración de conmutadores y puertos 617
VII-7-5-3 Registros de alertas..... 618
VII-7-6 Configuración de la base de datos 619
VII-7-7 Lista de soporte 620
VII-8 Administración central (dispositivos externos) 621

Título VIII Otros 623

VIII-1 Ajustes de objetos 624
Interfaz de usuario web 625
VIII-1-1 Objeto IP 625
VIII-1-2 Grupo IP 628
VIII-1-3 Objeto IPv6..... 630
VIII-1-4 Grupo IPv6 632
VIII-1-5 Objeto de tipo de servicio..... 634
VIII-1-6 Grupo de tipo de servicio 636
VIII-1-7 Objeto de palabra clave 638
VIII-1-8 Grupo de palabras clave 640
VIII-1-9 Objeto de extensión de archivo 641
VIII-1-10 Objeto de servicio de SMS/correo 643
VIII-1-11 Objeto de notificación 648
VIII-1-12 Objeto de cadena 650
VIII-1-13 Objeto País 651
VIII-1-14 Copia de seguridad/restauración de objetos 653
Notas de aplicación 654
A-1 Cómo enviar una notificación a un número de teléfono específico a través del servicio de SMS en desconexión de WAN 654
VIII-2 Aplicación USB 658
Interfaz de usuario web 659
VIII-2-1 Configuración general de USB..... 659
VIII-2-2 Gestión de usuarios USB 660
VIII-2-3 Explorador de archivos 662

VIII-2-4 Estado del dispositivo USB 663
VIII-2-5 Sensor de temperatura 664
VIII-2-6 Lista de soporte de módem 667
VIII-2-7 Lista de soporte de clientes SMB 668
Notas de aplicación 669
A-1 ¿Cómo puedo obtener los archivos del dispositivo de almacenamiento USB que se conecta al enrutador Vigor? ... 669

Parte IX Solución de problemas 673
Diagnóstico IX-1 674
Interfaz de usuario web 675
IX-1-1 Activación de marcación de salida 675
IX-1-2 Tabla de enrutamiento 676
IX-1-3 Tabla de caché ARP 677
IX-1-4 Tabla de vecinos IPv6 678
IX-1-5 Tabla DHCP 679
IX-1-6 Tabla de sesiones NAT 680
IX-1-7 Tabla de caché de DNS 681
IX-1-8 Diagnóstico de ping 682
IX-1-9 Monitor de flujo de datos 683
IX-1-10 Gráfico de tráfico 686
IX-1-11 Gráfica VPN 687
IX-1-12 Trazar ruta 688
IX-1-13 Explorador de Syslog 689
IX-1-14 Estado de TSPC de IPv6 690
IX-1-15 Estado de alta disponibilidad 690
IX-1-16 Información de autenticación 692
IX-1-17 Tabla de inundación DoS 694
IX-1-18 Diagnóstico de Política de Ruta 695
IX-2 Comprobación de si el estado del hardware es correcto o no 697
IX-3 Comprobación de si la configuración de la conexión de red en su computadora es correcta o no 698
IX-4 Hacer ping al enrutador desde su computadora 701
IX-5 Comprobación de si la configuración del ISP está bien o no 703
IX-6 Problemas para la conexión de red 3G/4G 704
IX-7 Restablecimiento de la configuración predeterminada de fábrica si es necesario 705
IX-8 Cómo ponerse en contacto con DrayTek 706

Parte X Comandos Telnet 707
Accediendo a Telnet de Vigor2927 708

Parte I Instalación

Esta parte presentará el enrutador Vigor y la guía para instalar el dispositivo en hardware y software.

I-1 Introducción

Esta es una versión internacional genérica de la guía del usuario. Las especificaciones, la compatibilidad y las características varían según la región. Para obtener guías de usuario específicas adecuadas para su región o producto, comuníquese con el distribuidor local.

La serie Vigor2927 integra QoS de capa IP, gestión de sesión/ancho de banda NAT para ayudar a los usuarios a controlar que funcione bien con un gran ancho de banda.

Al adoptar la plataforma VPN basada en hardware y el cifrado de hardware de AES/DES/3DES, el enrutador aumenta enormemente el rendimiento de VPN y ofrece varios protocolos (como IPsec/ PPTP/L2TP) con túneles VPN.

El diseño basado en objetos que se utiliza en el cortafuegos SPI (Stateful Packet Inspection) permite a los usuarios establecer políticas de cortafuegos con facilidad. CSM (Content Security Management) brinda a los usuarios control y administración en IM (Instant Messenger) y P2P (Peer to Peer) más eficiente que antes. Por cierto, la prevención DoS/DDoS y el filtro de contenido web/URL fortalecen la seguridad exterior y el control interior. El cortafuegos basado en objetos es flexible y permite que su red esté segura.

La administración de usuarios implementada en el firmware de su enrutador puede permitirle evitar que cualquier computadora acceda a su conexión a Internet sin un nombre de usuario o contraseña. También puede asignar presupuestos de tiempo a sus empleados dentro de la red de oficinas.

Con el conmutador Gigabit de 4 puertos en el lado LAN, proporciona una conectividad de velocidad extremadamente alta para la transferencia de datos local de mayor velocidad de cualquier servidor o PC local. Las VLAN etiquetadas (IEEE802.1Q) pueden marcar datos con un identificador de VLAN. Este identificador se puede llevar a través de un conmutador Ethernet hacia puertos específicos. Los clientes de VLAN específicos también pueden recoger este identificador cuando se acaba de pasar a la LAN. Puede establecer las prioridades para QoS del lado LAN. Puede asignar cada una de las VLAN a cada una de las diferentes subredes de IP que el enrutador también puede estar operando, para proporcionar aún más aislamiento. Dicha funcionalidad está basada en etiquetas Multi-subnet (Multiple-Private LAN Subnets).

En los modelos equipados con tecnología inalámbrica (p. ej., Vigor2927lac), cada uno de los SSID inalámbricos también se puede agrupar dentro de una de las VLAN.

Además, la serie Vigor2927 es compatible con la interfaz USB para conectar una impresora USB para compartir la función de impresión o un módem USB 3G para la conexión de red.

La serie Vigor2927 proporciona administración de dos niveles para simplificar la configuración de la conexión de red. El modo de usuario permite al usuario acceder a la interfaz WEB a través de una configuración simple. Sin embargo, si los usuarios desean tener configuraciones avanzadas, pueden acceder a la interfaz WEB a través del modo de administración.

Indicadores y conectores I-1-1

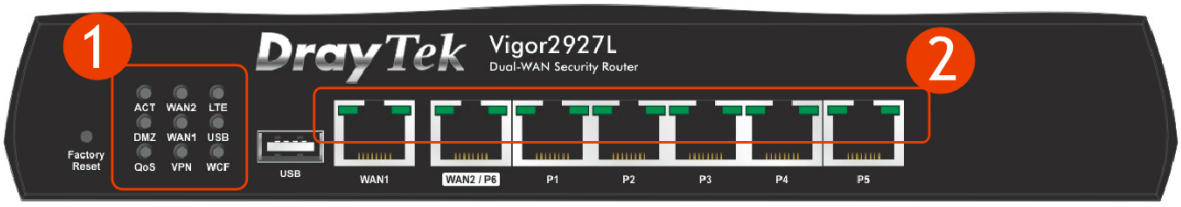
Antes de usar el enrutador Vigor, primero familiarícese con los indicadores LED y los conectores.

I-1-1-1 Vigor2927

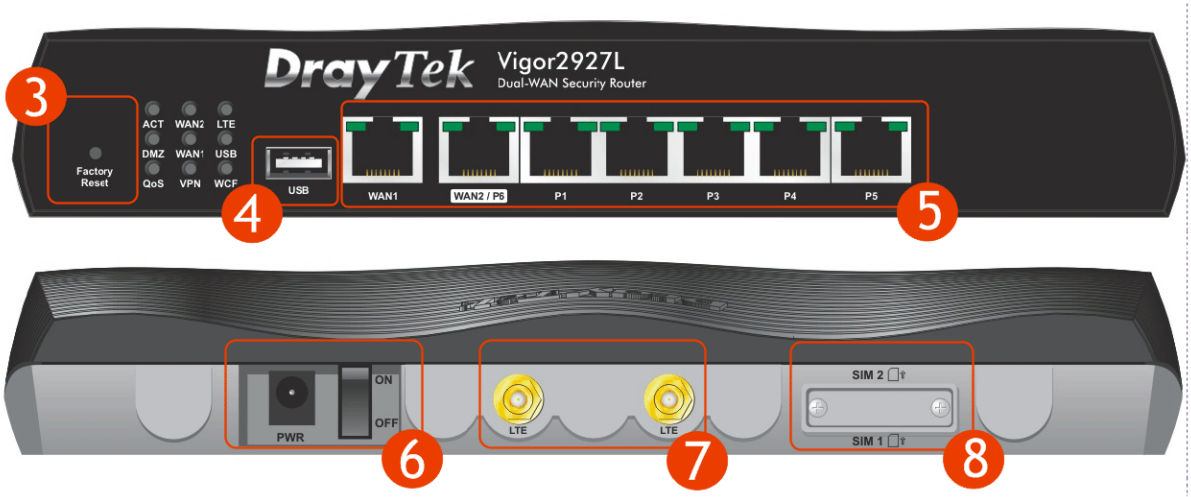
No.	CONDUJO	Estado	Explicación
(1)	ACTO	Apagado	El enrutador está apagado.
		Parpadeo	El enrutador está encendido y funcionando normalmente.
	WAN2/WAN1	En	La conexión a Internet está lista.
		Apagado	La conexión a Internet no está lista.
		Parpadeo	Los datos se están transmitiendo.
	USB1/USB2	En	El dispositivo USB está conectado y listo para usar.
		Apagado	No hay ningún dispositivo USB conectado.
		Parpadeo	Los datos se están transmitiendo.
	DMZ	En	La función DMZ está habilitada.
		Apagado	La función DMZ está deshabilitada.
		Parpadeo	Los datos se están transmitiendo.
	QoS	En	La función QoS está activa.
		Apagado	La función QoS está inactiva.
	vpn	En	El túnel VPN está activo.
		Apagado	Los servicios VPN están deshabilitados
		Parpadeo	El tráfico está pasando a través del túnel VPN.
	WCF	En	El filtro de contenido web está activo. (Se habilita desde **Cortafuegos >> Configuración general**).
		Apagado	WCF está deshabilitado.
(2)	WAN1, WAN2 / P6		
	LED izquierdo	En	El puerto está conectado.
		Apagado	El puerto está desconectado.
		Parpadeo	Los datos se están transmitiendo.
	LED derecho	En	El puerto está conectado con 1000Mbps.
		Apagado	El puerto está conectado con 10/100Mbps.
	LAN P1-P5		
	LED izquierdo	En	El puerto está conectado.
		Apagado	El puerto está desconectado.
		Parpadeo	Los datos se están transmitiendo.
	LED derecho	En	El puerto está conectado con 1000Mbps.
		Apagado	El puerto está conectado con 10/100Mbps

No.	Interfaz	Descripción
(3)	Restablecimiento de fábrica	Restaurar la configuración predeterminada. Uso: Encienda el enrutador (el LED ACT parpadea). Presionar el agujero y mantener durante más de 5 segundos. Cuando vea que el LED ACT comienza a parpadear más rápido de lo habitual, suelte el botón. Luego, el enrutador se reiniciará con la configuración predeterminada de fábrica.
(4)	USB	Conector para un dispositivo USB (para Módem USB 3G/4G o impresora o termómetro).
(5)	WAN1	Conector para un módem para acceder a Internet.
	WAN2 / P6	Conector para dispositivos de red local o módem para acceder a Internet. Es un puerto conmutable. Se puede utilizar para conexión LAN o conexión WAN según la configuración configurada en WUI.
	LAN P1-P5	Conectores para dispositivos de red local.
(6)	poder	Conector para un adaptador de corriente.
	ENCENDIDO APAGADO	Interruptor de alimentación.

I-1-1-2 Vigor2927L

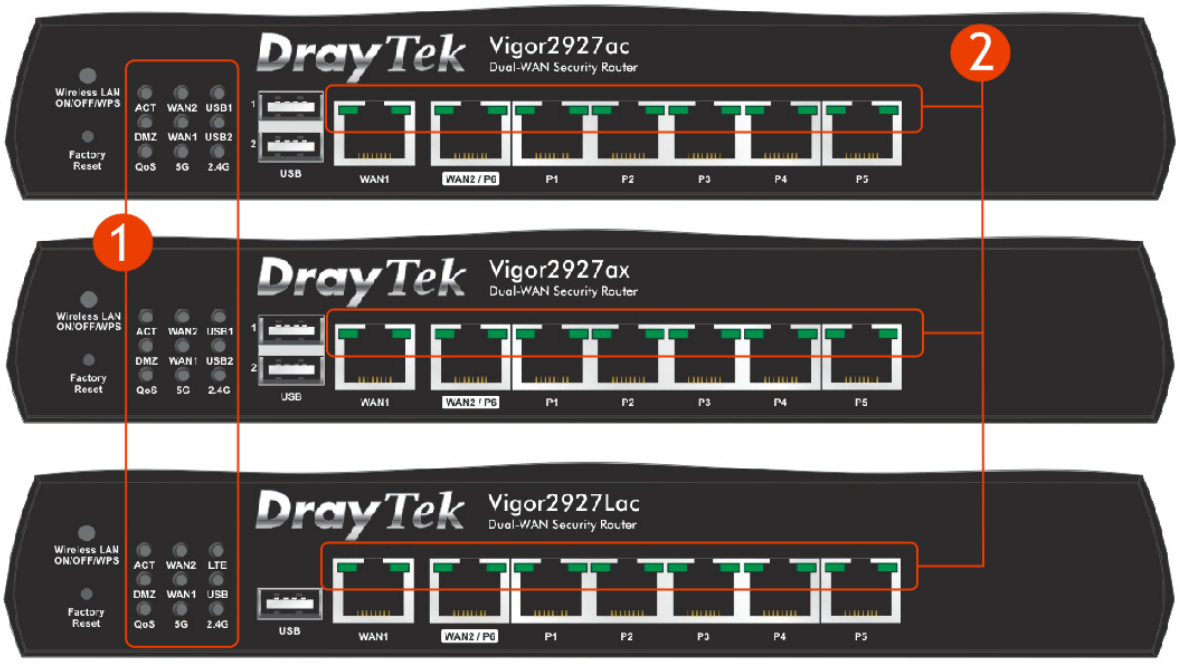


No.	CONDUJO	Estado	Explicación
(1)	ACTO	Apagado	El enrutador está apagado.
		Parpadeo	El enrutador está encendido y funcionando normalmente.
	WAN2/WAN1	En	La conexión a Internet está lista.
		Apagado	La conexión a Internet no está lista.
		Parpadeo	Los datos se están transmitiendo.
	LTE	En	El dispositivo LTE está conectado y listo para usar.
		Apagado	El dispositivo LTE no se detecta o tiene un problema grave (p. ej., sin tarjeta SIM, error de pin de SIM, SIM desactivada, etc.).
		Parpadeo	Lentamente: el dispositivo LTE está marcando. Rápidamente: Los datos se están transmitiendo.
	DMZ	En	La función DMZ está habilitada.
		Apagado	La función DMZ está deshabilitada.
		Parpadeo	Los datos se están transmitiendo.
	USB	En	El dispositivo USB está conectado y listo para usar.
		Apagado	No hay ningún dispositivo USB conectado.
		Parpadeo	Los datos se están transmitiendo.
	QoS	En	La función QoS está activa.
		Apagado	La función QoS está inactiva.
	vpn	En	El túnel VPN está activo.
		Apagado	Los servicios VPN están deshabilitados
		Parpadeo	El tráfico está pasando a través del túnel VPN.
	WCF	En	El filtro de contenido web está activo. (Se habilita desde **Cortafuegos >> Configuración general**).
		Apagado	WCF está deshabilitado.
(2)	WAN1, WAN2 / P6		
	LED izquierdo	En	El puerto está conectado.
		Apagado	El puerto está desconectado.
		Parpadeo	Los datos se están transmitiendo.
	LED derecho	En	El puerto está conectado con 1000Mbps.
		Apagado	El puerto está conectado con 10/100Mbps.
	LAN P1-P5		
	LED izquierdo	En	El puerto está conectado.
		Apagado	El puerto está desconectado.
		Parpadeo	Los datos se están transmitiendo.
	LED derecho	En	El puerto está conectado con 1000Mbps.
		Apagado	El puerto está conectado con 10/100Mbps



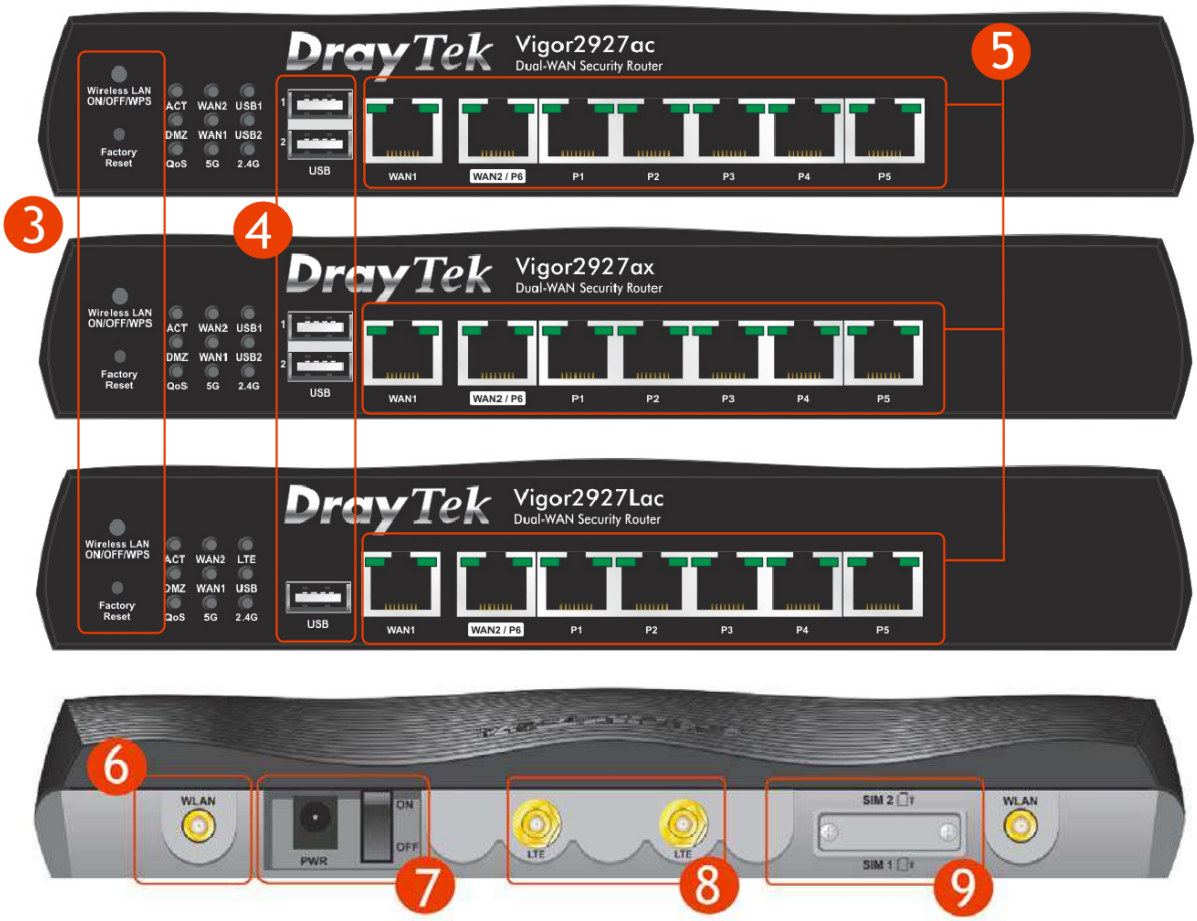
No.	Interfaz	Descripción
(3)	Restablecimiento de fábrica	Restaurar la configuración predeterminada. Uso: Encienda el enrutador (el LED ACT parpadea). Presionar el agujero y mantener durante más de 5 segundos. Cuando vea que el LED ACT comienza a parpadear más rápido de lo habitual, suelte el botón. Luego, el enrutador se reiniciará con la configuración predeterminada de fábrica.
(4)	USB	Conector para un dispositivo USB (para Módem USB 3G/4G o impresora o termómetro).
(5)	WAN1	Conector para un módem para acceder a Internet.
	WAN2 / P6	Conector para dispositivos de red local o módem para acceder a Internet. Es un puerto conmutable. Se puede utilizar para conexión LAN o conexión WAN según la configuración configurada en WUI.
	LAN P1-P5	Conectores para dispositivos de red local.
(6)	poder	Conector para un adaptador de corriente.
	ENCENDIDO APAGADO	Interruptor de alimentación.
(7)		Conector para instalar antenas LTE.
(8)	tarjeta SIM 2/1	Ranuras para instalar tarjeta SIM.

I-1-1-3 Vigor2927ac / Vigor2927ax / Vigor2927Lac



No.	CONDUJO	Estado	Explicación
(1)	ACTO	Apagado	El enrutador está apagado.
		Parpadeo	El enrutador está encendido y funcionando normalmente.
	WAN2/WAN1	En	La conexión a Internet está lista.
		Apagado	La conexión a Internet no está lista.
		Parpadeo	Los datos se están transmitiendo.
	USB1/USB2	En	El dispositivo USB está conectado y listo para usar.
		Apagado	No hay ningún dispositivo USB conectado.
		Parpadeo	Los datos se están transmitiendo.
	LTE	En	El dispositivo LTE está conectado y listo para usar.
		Apagado	El dispositivo LTE no se detecta o tiene un problema grave (p. ej., sin tarjeta SIM, error de pin de SIM, SIM desactivada, etc.).
		Parpadeo	Lentamente: el dispositivo LTE está marcando. Rápidamente: Los datos se están transmitiendo.
	DMZ	En	La función DMZ está habilitada.
		Apagado	La función DMZ está deshabilitada.
		Parpadeo	Los datos se están transmitiendo.

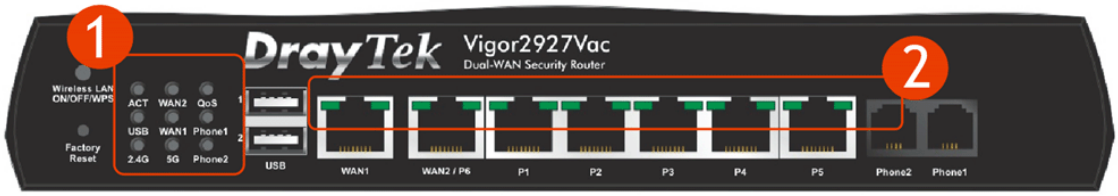
(1)	QoS	En	La función QoS está activa.
		Apagado	La función QoS está inactiva.
	5G/2,4G	En	5G/2,4G: el punto de acceso inalámbrico con ancho de banda de 5 GHz/2,4 GHz está listo. WLAN: el punto de acceso inalámbrico está listo.
		Apagado	La función inalámbrica está deshabilitada.
		Parpadeo	Parpadeará lentamente mientras pasa el tráfico inalámbrico. Los LED ACT y WLAN parpadean rápida y simultáneamente cuando WPS está funcionando y volverán a su estado normal después de dos minutos. (Debe configurar WPS en 2 minutos).
(2)	WAN1, WAN2 / P6		
	LED izquierdo	En	El puerto está conectado.
		Apagado	El puerto está desconectado.
		Parpadeo	Los datos se están transmitiendo.
	LED derecho	En	El puerto está conectado con 1000Mbps.
		Apagado	El puerto está conectado con 10/100Mbps.
	LAN P1-P5		
	LED izquierdo	En	El puerto está conectado.
		Apagado	El puerto está desconectado.
		Parpadeo	Los datos se están transmitiendo.
	LED derecho	En	El puerto está conectado con 1000Mbps.
		Apagado	El puerto está conectado con 10/100Mbps



No.	Interfaz	Descripción
(3)	LAN inalámbrico ENCENDIDO/APAGADO/WPS	La banda inalámbrica se cambiará/cambiará de acuerdo con el botón presionado y liberado. Por ejemplo, -2.4G (Encendido) y 5G (Encendido) – por defecto. -2.4G (Apagado) y 5G (Encendido): presionó y soltó el botón una vez. -2.4G (Encendido) y 5G (Apagado): presionó y soltó el botón dos veces. -2.4G (Apagado) y 5G (Apagado): presionó y soltó el botón tres veces. Cuando la interfaz de usuario web habilita la función WPS, presione este botón durante más de 2 segundos para esperar a que el dispositivo del cliente se conecte a la red a través de WPS.
	Restablecimiento de fábrica	Restaurar la configuración predeterminada. Uso: Encienda el enrutador (el LED ACT parpadea). Presionar el agujero y mantener durante más de 5 segundos. Cuando vea que el LED ACT comienza a parpadear más rápido de lo habitual, suelte el botón. Luego, el enrutador se reiniciará con la configuración predeterminada de fábrica.
(4)	USB1~2 / USB	Conector para un dispositivo USB (para Módem USB 3G/4G o impresora o termómetro).
(5)	WAN1	Conector para un módem para acceder a Internet.
	WAN2 / P6	Conector para dispositivos de red local o módem para acceder a Internet. Es un puerto conmutable. Se puede utilizar para conexión LAN o conexión WAN según la configuración configurada en WUI.
	LAN P1-P5	Conectores para dispositivos de red local.
(6)		Conector para instalar antenas WLAN. (Para el modelo de CA)
(7)	poder	Conector para un adaptador de corriente.

	ENCENDIDO APAGADO	Interruptor de alimentación.
(8)		Conector para instalar antenas LTE. (Para modelo L).
(9)	tarjeta SIM 2/1	Ranuras para instalar tarjeta SIM. (Para modelo L).

I-1-1-4 Vigor2927Vac

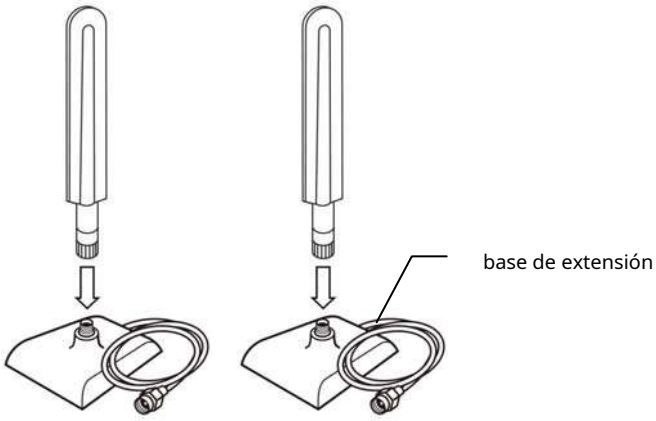


No.	CONDUJO	Estado	Explicación
(1)	ACTO	Apagado	El enrutador está apagado.
		Parpadeo	El enrutador está encendido y funcionando normalmente.
	WAN2/WAN1	En	La conexión a Internet está lista.
		Apagado	La conexión a Internet no está lista.
		Parpadeo	Los datos se están transmitiendo.
	QoS	En	La función QoS está activa.
		Apagado	La función QoS está inactiva.
	USB	En	El dispositivo USB está conectado y listo para usar.
		Apagado	No hay ningún dispositivo USB conectado.
		Parpadeo	Los datos se están transmitiendo.
	Teléfono1/Teléfono 2	En	El teléfono conectado a este puerto está descolgado.
		Apagado	El teléfono conectado a este puerto está colgado.
		Parpadeo	Llega una llamada telefónica.
	2.4G/5G	En	5G/2,4G: el punto de acceso inalámbrico con ancho de banda de 5 GHz/2,4 GHz está listo. WLAN: el punto de acceso inalámbrico está listo.
		Apagado	La función inalámbrica está deshabilitada.
		Parpadeo	Parpadeará lentamente mientras pasa el tráfico inalámbrico. Los LED ACT y WLAN parpadean rápida y simultáneamente cuando WPS está funcionando y volverán a su estado normal después de dos minutos. (Debe configurar WPS en 2 minutos).
(2)	WAN1, WAN2 / P6		
	LED izquierdo	En	El puerto está conectado.
		Apagado	El puerto está desconectado.
		Parpadeo	Los datos se están transmitiendo.
	LED derecho	En	El puerto está conectado con 1000Mbps.
		Apagado	El puerto está conectado con 10/100Mbps.
	LAN P1-P5		
	LED izquierdo	En	El puerto está conectado.
		Apagado	El puerto está desconectado.
		Parpadeo	Los datos se están transmitiendo.
	LED derecho	En	El puerto está conectado con 1000Mbps.
		Apagado	El puerto está conectado con 10/100Mbps

No.	Interfaz	Descripción
(3)	LAN inalámbrico ENCENDIDO/APAGADO/WPS	La banda inalámbrica se cambiará/cambiará de acuerdo con el botón presionado y liberado. Por ejemplo, -2.4G (Encendido) y 5G (Encendido) – por defecto. -2.4G (Apagado) y 5G (Encendido): presionó y soltó el botón una vez. -2.4G (Encendido) y 5G (Apagado): presionó y soltó el botón dos veces. -2.4G (Apagado) y 5G (Apagado): presionó y soltó el botón tres veces. Cuando la interfaz de usuario web habilita la función WPS, presione este botón durante más de 2 segundos para esperar a que el dispositivo del cliente se conecte a la red a través de WPS.
	Restablecimiento de fábrica	Restaurar la configuración predeterminada. Uso: Encienda el enrutador (el LED ACT parpadea). Presionar el agujero y mantener durante más de 5 segundos. Cuando vea que el LED ACT comienza a parpadear más rápido de lo habitual, suelte el botón. Luego, el enrutador se reiniciará con la configuración predeterminada de fábrica.
(4)	USB1~2 / USB	Conector para un dispositivo USB (para Módem USB 3G/4G o impresora o termómetro).
(5)	WAN1	Conector para un módem para acceder a Internet.
	WAN2 / P6	Conector para dispositivos de red local o módem para acceder a Internet. Es un puerto conmutable. Se puede utilizar para conexión LAN o conexión WAN según la configuración configurada en WUI.
	LAN P1-P5	Conectores para dispositivos de red local.
(6)		Conector para instalar antenas WLAN. (Para el modelo de CA)
(7)	poder	Conector para un adaptador de corriente.
	ENCENDIDO APAGADO	Interruptor de alimentación.

I-1-2 Notas para la instalación de la antena (para"L"modelo)

La antena magnética debe instalarse en la base de extensión antes de conectarse al enrutador Vigor.



Hay dos orificios de montaje para instalar antenas con base de extensión en el enrutador Vigor. Instálelos como se muestra a continuación.

Tenga en cuenta que si solo va a instalar una antena, utilice el orificio de montaje (orificio de transmisión de la señal principal) cerca del interruptor de alimentación.

Mientras instala la tarjeta SIM en la ranura de la tarjeta, tenga en cuenta que la placa posterior de la ranura de la tarjeta SIM debe quitarse primero y la dirección de la muesca de la tarjeta debe estar en el lado izquierdo.

Se proporcionan dos tipos de antenas para Vigor2927Lac, que deben instalarse en diferentes ubicaciones con cuidado y correctamente. Una instalación incorrecta puede causar una mala señal de conexión inalámbrica. Por lo tanto, preste atención a la instalación de antenas consultando la siguiente ilustración.

Instalación de hardware I-2

I-2-1 Instalación del enrutador Vigor

Antes de comenzar a configurar el enrutador, debe conectar sus dispositivos correctamente. (Para la conexión de hardware, tomamos *"C.A"* modelo como ejemplo).

1. Conecte la interfaz DSL a la toma de línea terrestre con un cable de línea DSL.

   Conecte el módem por cable/módem DSL/convertidor de medios al puerto WAN del enrutador con un cable Ethernet (RJ-45).

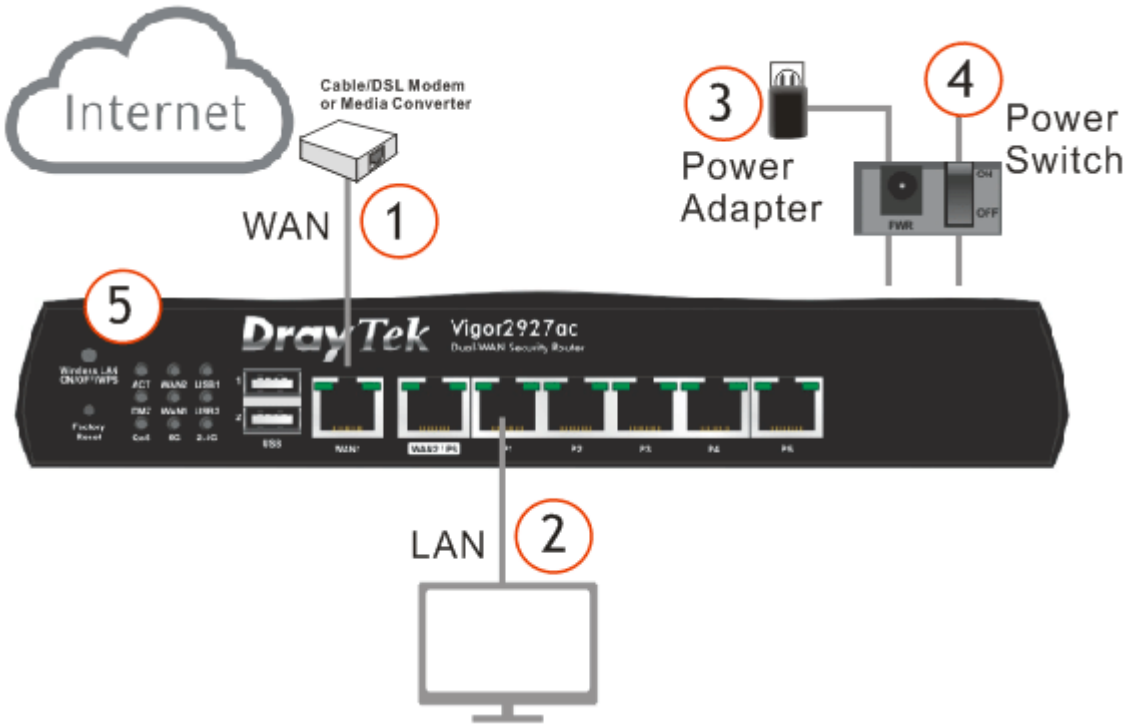
2. Conecte un extremo de un cable Ethernet (RJ-45) a uno de los**LAN**puertos del enrutador y el otro extremo del cable (RJ-45) en el puerto Ethernet de su computadora.

3. Conecte un extremo del adaptador de corriente al puerto de alimentación del enrutador en el panel posterior y el otro extremo a un tomacorriente de pared.

4. Encienda el dispositivo presionando el interruptor de encendido en el panel trasero.

5. El sistema comienza a iniciarse. Después de completar la prueba del sistema, el**ACTO**El LED se encenderá y comenzará a parpadear.

(Para la conexión de hardware, tomamos *"C.A"* modelo como ejemplo).

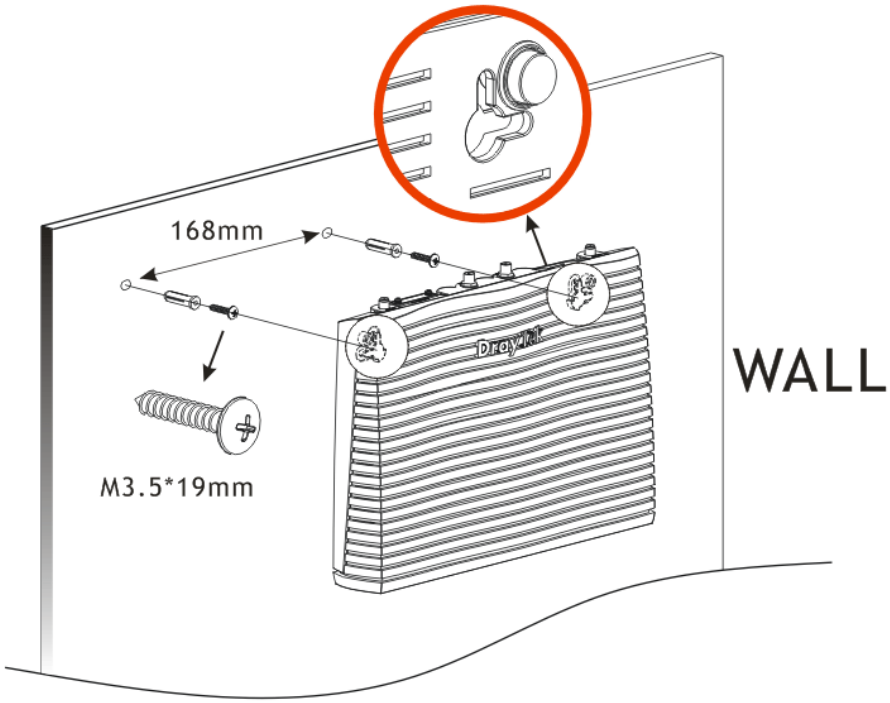


I-2-2 Instalación montada en la pared

El enrutador Vigor tiene ranuras de montaje tipo ojo de cerradura en la parte inferior.

1. Haz dos agujeros en la pared. La distancia entre los agujeros será de 168 mm.

2. Coloque los tornillos en la pared utilizando el tipo adecuado de taco de pared.

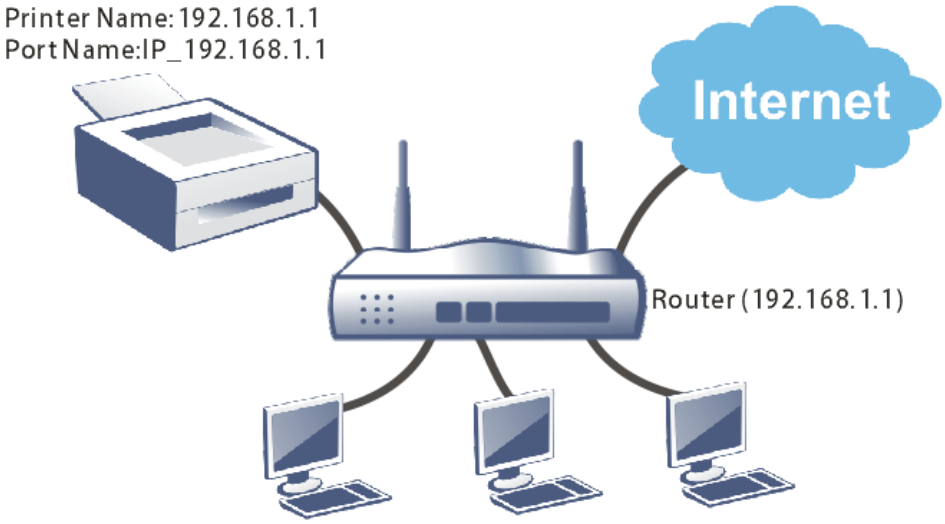


Información	El diámetro de perforación recomendado será de 6,5 mm (1/4”).

3. Cuando haya terminado con el procedimiento, el enrutador se ha montado firmemente en la pared.

I-2-3 Instalación de la impresora USB en el enrutador Vigor

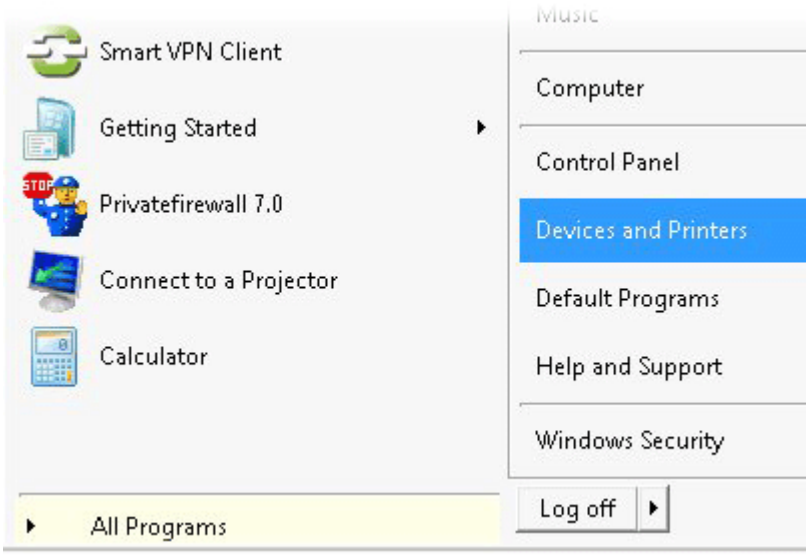
Puede instalar una impresora en el enrutador para compartir la impresión. Todas las PC conectadas a este enrutador pueden imprimir documentos a través del enrutador. El ejemplo proporcionado aquí se basa en Windows 7. Para otro sistema de Windows, visite**www.DrayTek.com**.



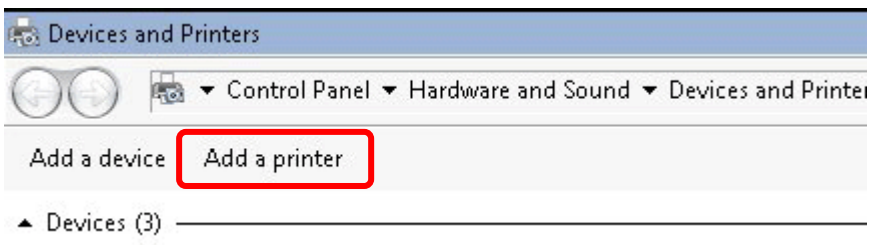
Antes de usarlo, siga los pasos a continuación para configurar los ajustes de las computadoras conectadas (o clientes inalámbricos).

1. Conecte la impresora con el enrutador a través del puerto USB/paralelo.

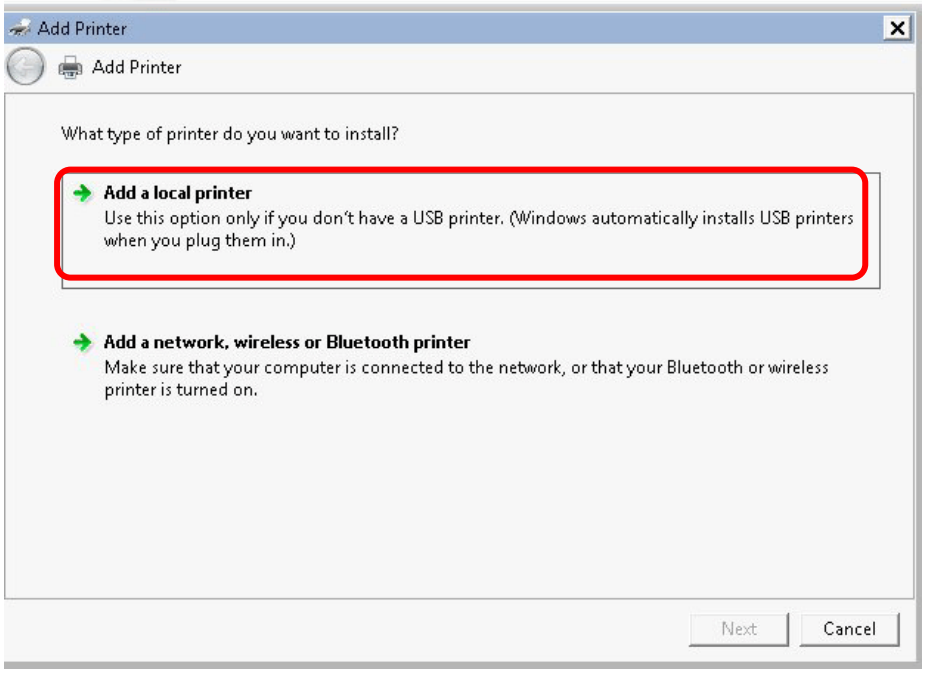
2. Abierto**Todos los programas>>Primeros pasos>>Dispositivos e impresoras**.



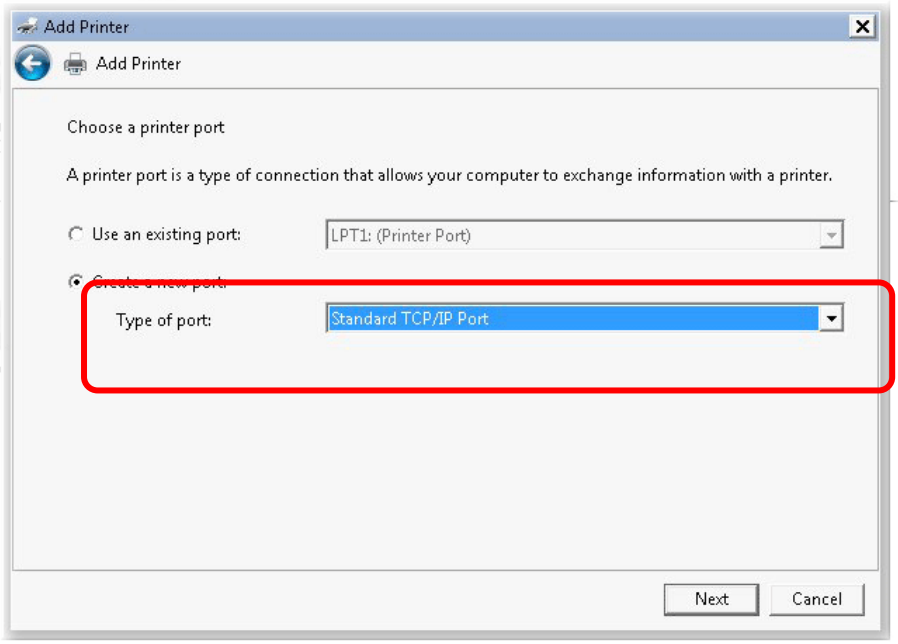
3. Haga clic en**Añadir una impresora**.



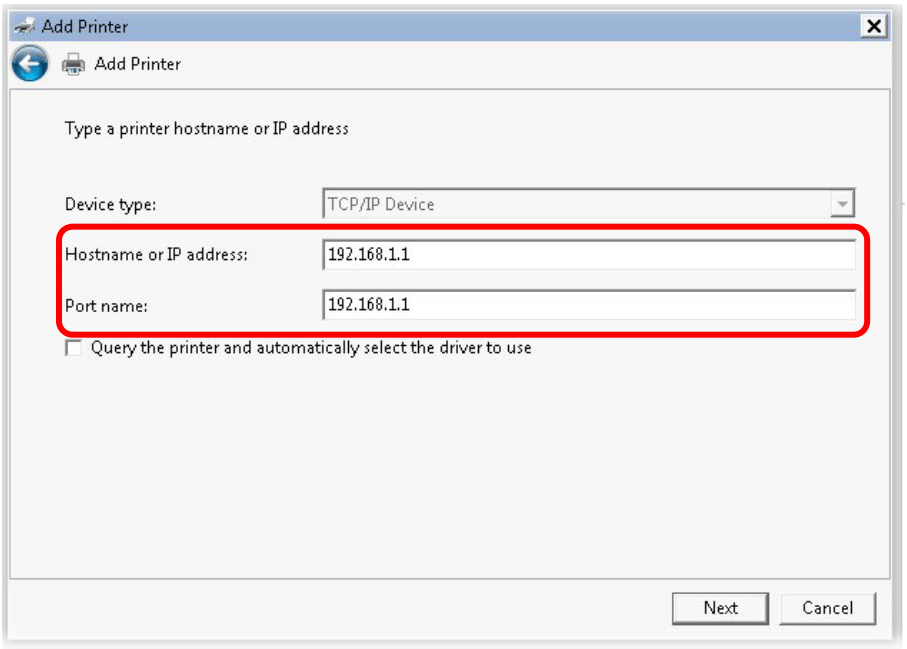
4. Aparecerá un cuadro de diálogo. Hacer clic**Agregar una impresora local**y haga clic**Próximo**.



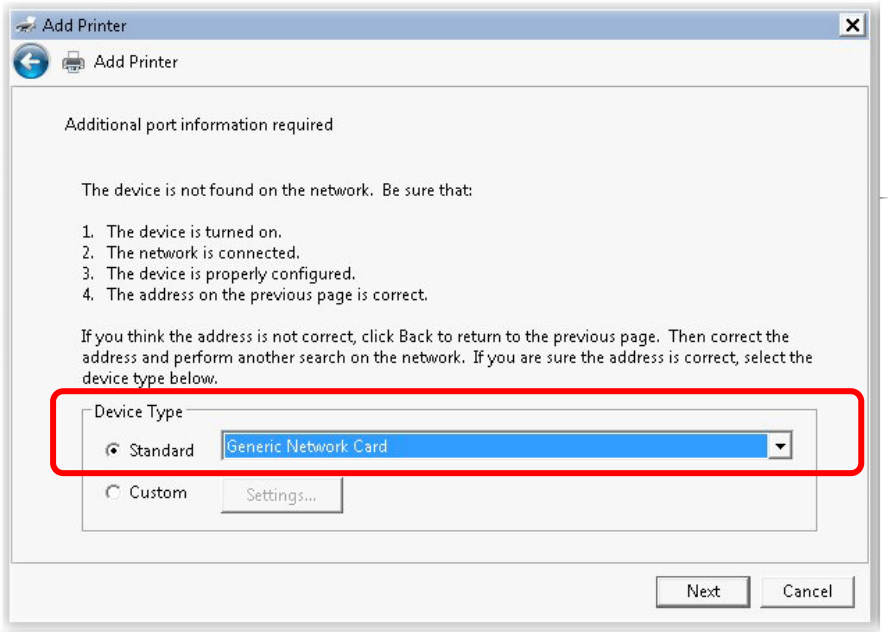
5. En este cuadro de diálogo, elija**Crear un nuevo puerto.**En el campo de**tipo de puerto,**utilice la lista desplegable para seleccionar**Puerto TCP/IP estándar**. Luego, haga clic en**Próximo**.



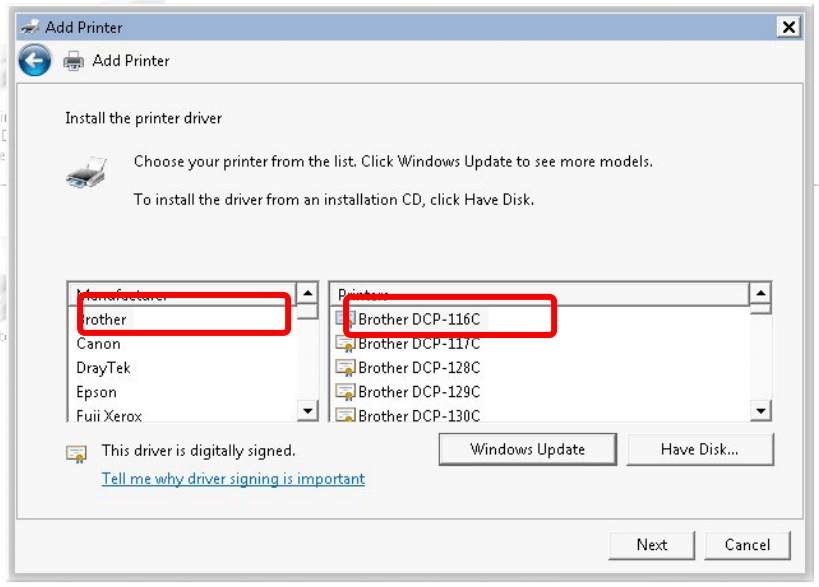
6. En el siguiente cuadro de diálogo, escriba**192.168.1.1**(IP LAN del enrutador) en el campo de**Nombre de host o la dirección IP**y tipo**192.168.1.1**como el**Nombre del puerto**. Luego, haga clic en**Próximo**.



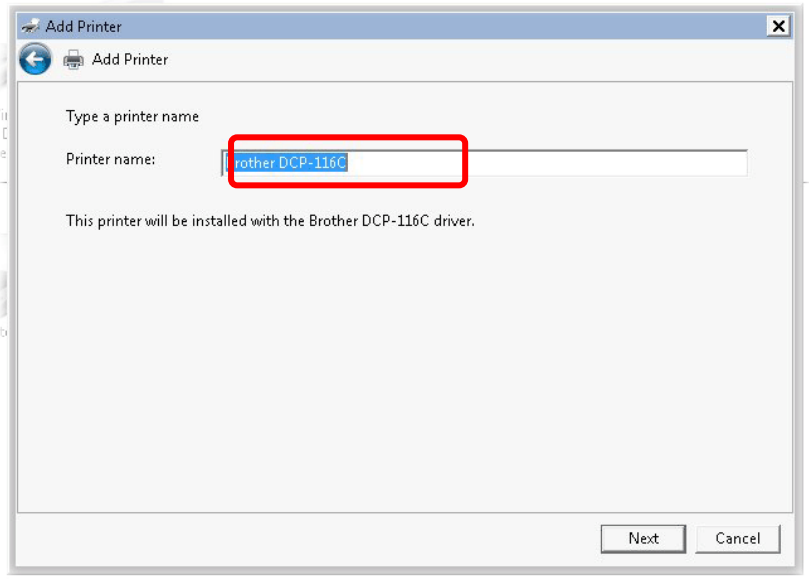
7. Haga clic en**Estándar**y elige**Tarjeta de red genérica**.



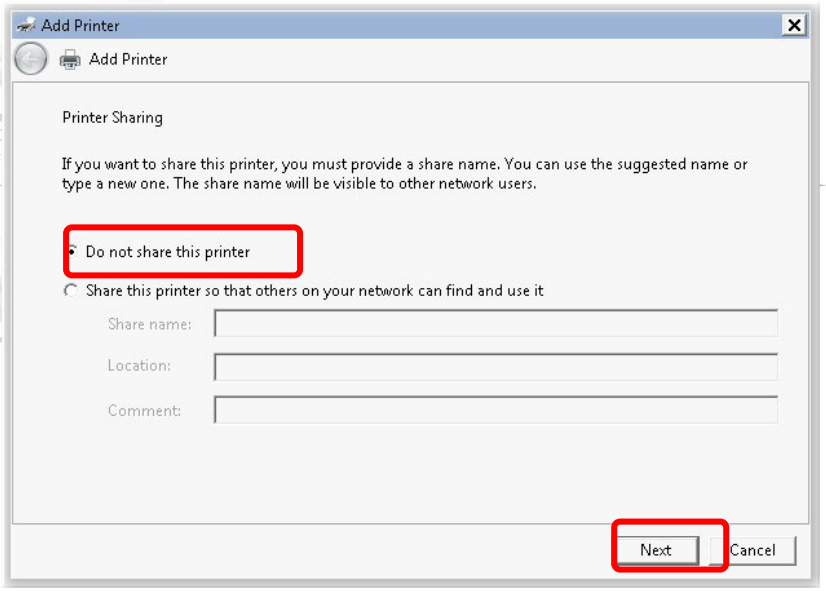
8. Ahora, su sistema le pedirá que elija el nombre correcto de la impresora que instaló en el enrutador. Tal paso puede hacer que el controlador correcto se cargue en su PC. Cuando termine la selección, haga clic en **Próximo**.



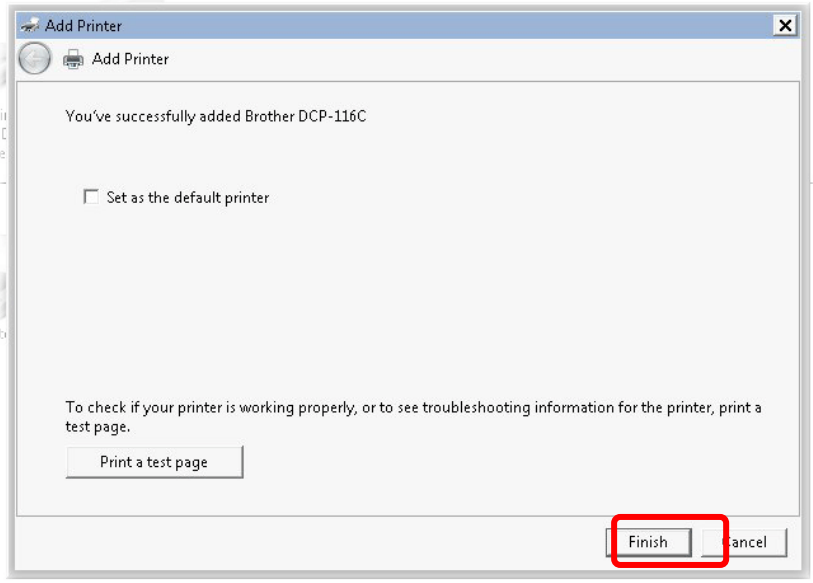
9. Escriba un nombre para la impresora elegida. Hacer clic**Próximo.**



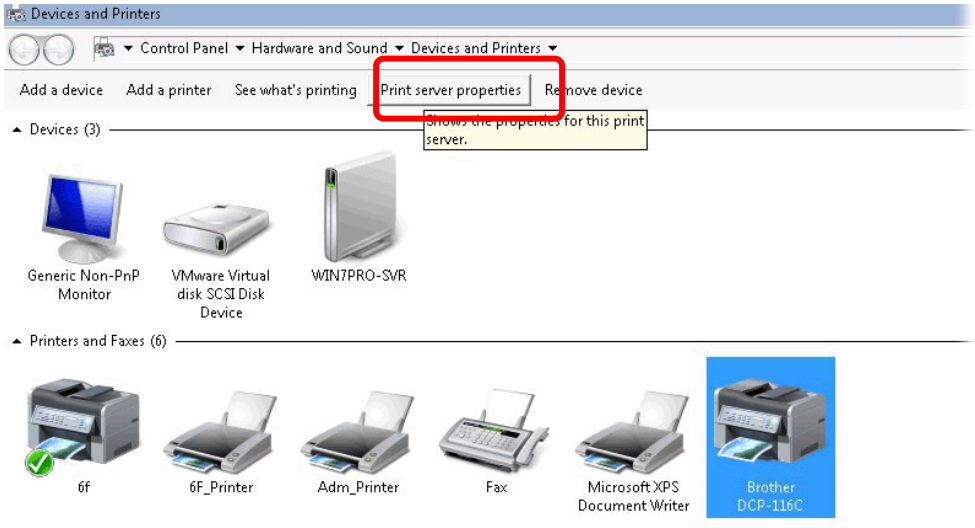
10. Elige**No compartas esta impresión.**r y haga clic**Próximo**.



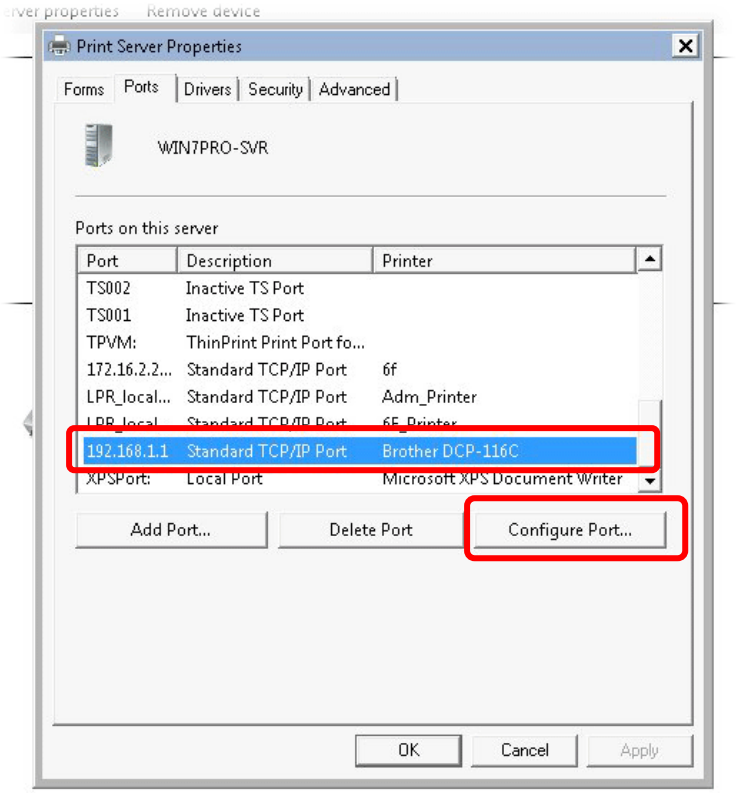
11. Luego, en el siguiente cuadro de diálogo, haga clic en**Finalizar**.



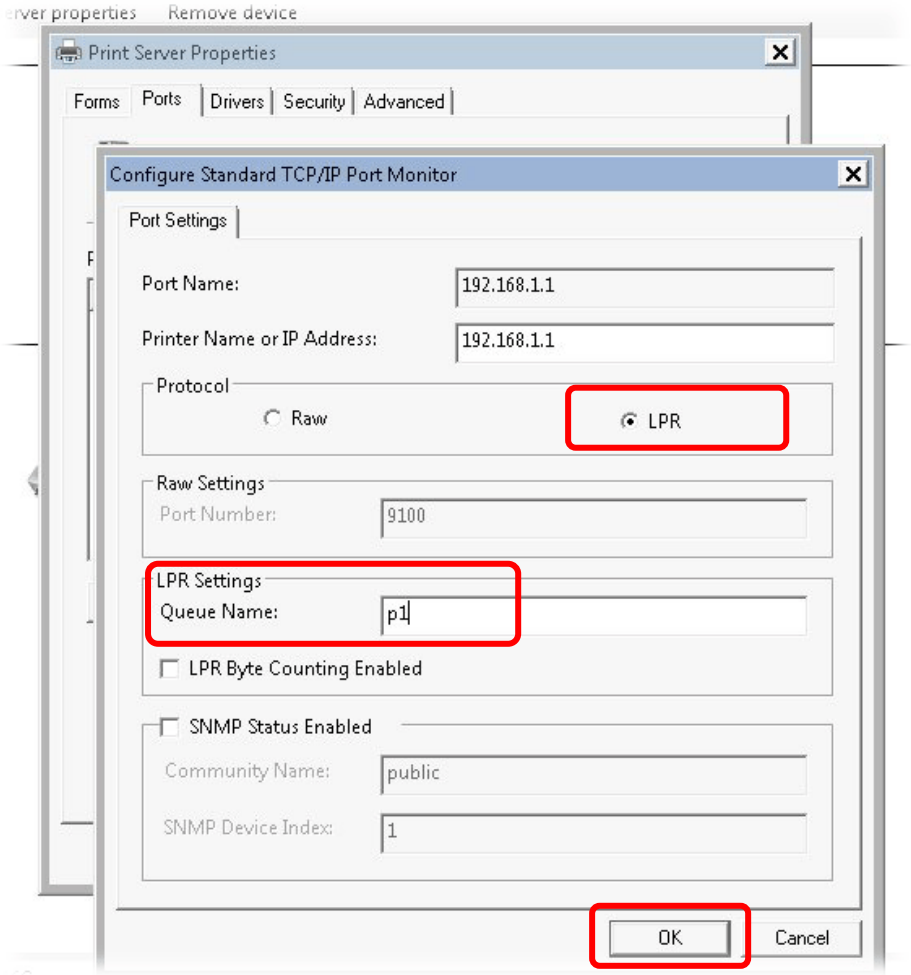
12. La nueva impresora se ha agregado y se muestra en**Impresoras y Faxes**. Haga clic en el icono de la nueva impresora y haga clic en**Propiedades del servidor de impresoras**.



13. Edite la propiedad de la nueva impresora que ha agregado haciendo clic en**Configurar puerto**.



14. Seleccione "**LPR**" en Protocolo, escriba**p1**(número 1) como**Nombre de cola**. Luego haga clic**DE ACUERDO**. A continuación, consulte el rectángulo rojo para elegir el protocolo correcto y el nombre LPR.



La impresora se puede utilizar para imprimir ahora. La mayoría de las impresoras de diferentes fabricantes son compatibles con vigor router.

Información

Algunas impresoras con fax/escáner u otras funciones adicionales no son compatibles.

El enrutador Vigor admite la solicitud de impresión de las computadoras a través de los puertos LAN pero no del puerto WAN.

I-3 Acceso a la página web

1. Asegúrese de que su PC se conecte correctamente al enrutador.

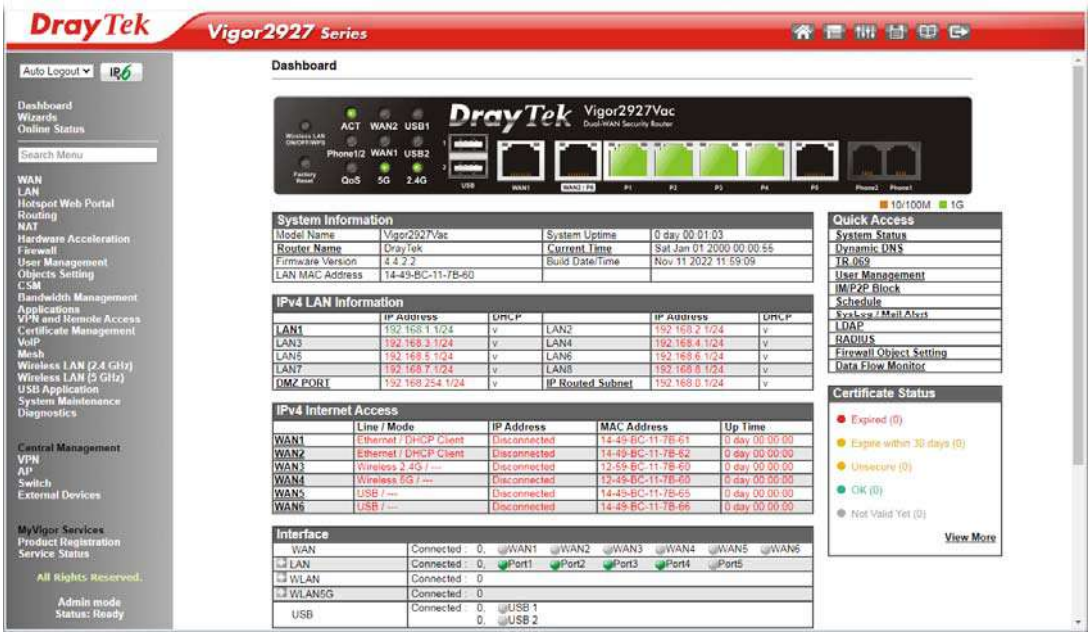
   Puede simplemente configurar su computadora para obtener IP dinámicamente desde el enrutador o configurar la dirección IP de la computadora para que sea la misma subred que**la dirección IP predeterminada del enrutador Vigor 192.168.1.1**. Para obtener información detallada, consulte la sección posterior - Resolución de problemas de la guía.

2. Abra un navegador web en su PC y escriba**http://192.168.1.1.**Se abrirá la siguiente ventana para solicitar usuario y contraseña.

3. Escriba "admin/admin" como nombre de usuario/contraseña y haga clic en**Acceso**.

Información	Si no puede acceder a la configuración web, vaya a "Solución de problemas" para detectar y solucionar su problema.

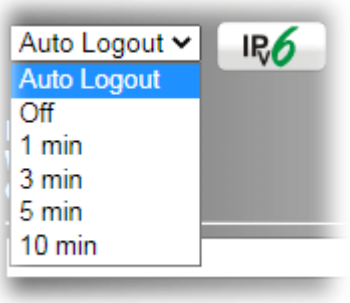
4. Ahora, el**Pantalla principal**aparecerá. Tome Vigor2927ac como ejemplo.



Información

La página de inicio será ligeramente diferente de acuerdo con el tipo de enrutador que tenga.

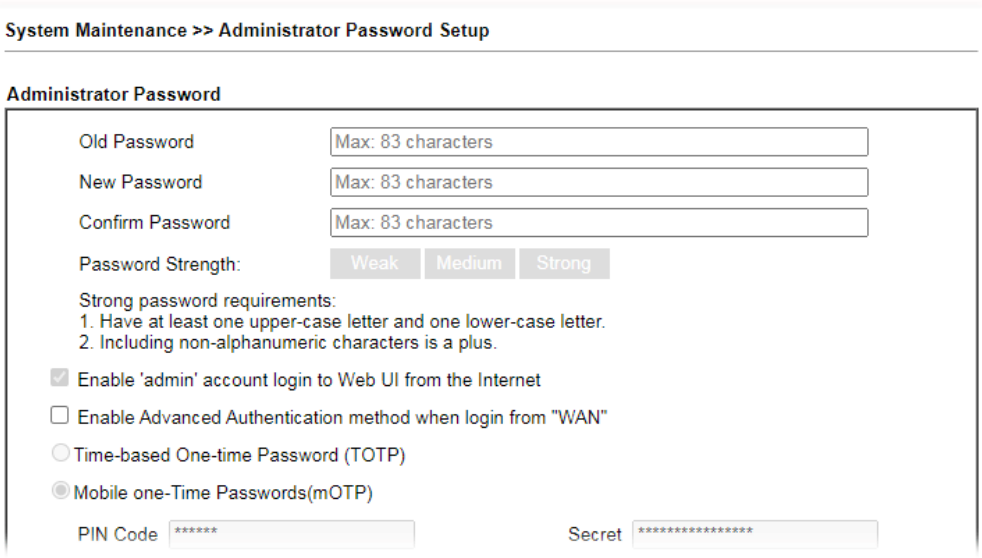
5. La página web se puede cerrar de acuerdo con la condición elegida. La configuración predeterminada es**Cierre de sesión automático**, lo que significa que el sistema de configuración web se cerrará después de 5 minutos sin ninguna operación. Cambie la configuración según sus necesidades.



I-4 Cambio de contraseña

Cambie la contraseña para la seguridad original del enrutador.

1. Abra un navegador web en su PC y escriba**http://192.168.1.1.**Se abrirá una ventana emergente para solicitar el nombre de usuario y la contraseña.
2. Escriba "admin/admin" como nombre de usuario/contraseña para acceder a la interfaz de usuario web con el modo de administrador.
3. Ir a**Mantenimiento del sistema**pagina y elige**Contraseña de administrador**.



4. Introduzca la contraseña de inicio de sesión (la predeterminada es "admin") en el campo de**Contraseña anterior**. Tipo **Nueva contraseña**y**confirmar Contraseña**. Luego haga clic**DE ACUERDO**continuar.

Información

La longitud máxima de la contraseña que puede establecer es de 23 caracteres.

5. Ahora, la contraseña ha sido cambiada. La próxima vez, utilice la nueva contraseña para acceder a la interfaz de usuario web de este enrutador.

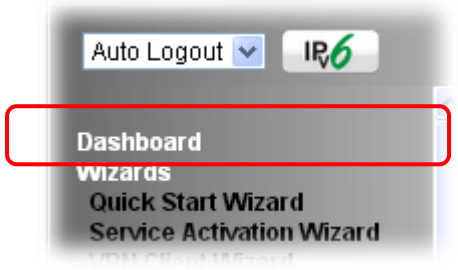
Información

Incluso si se cambia la contraseña, el nombre de usuario para iniciar sesión en la interfaz de usuario web sigue siendo "admin".

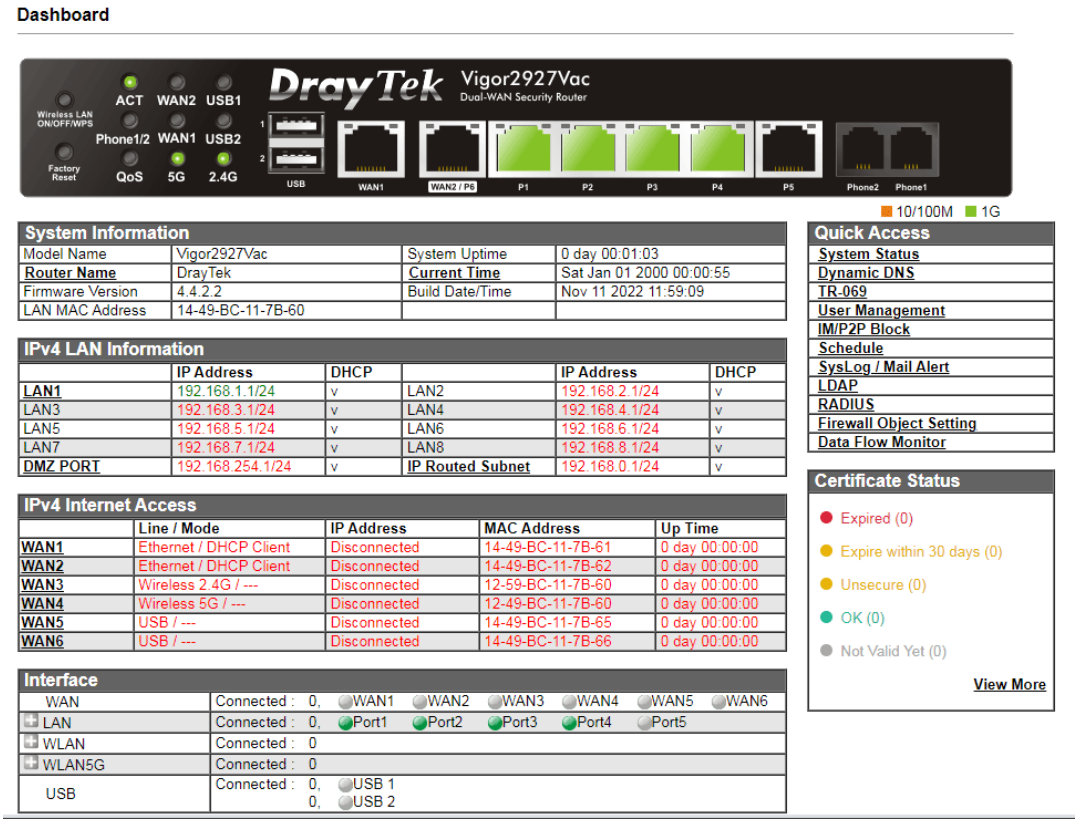
Tablero I-5

El panel muestra el estado de la conexión, incluida la información del sistema, el acceso a Internet IPv4, el acceso a Internet IPv6, la interfaz (conexión física), la seguridad y el acceso rápido.

Hacer clic**Panel**desde el menú principal en el lado izquierdo de la página principal.



Se mostrará una página web con las selecciones predeterminadas en la pantalla. Consulte la siguiente figura:



Panel virtual I-5-1

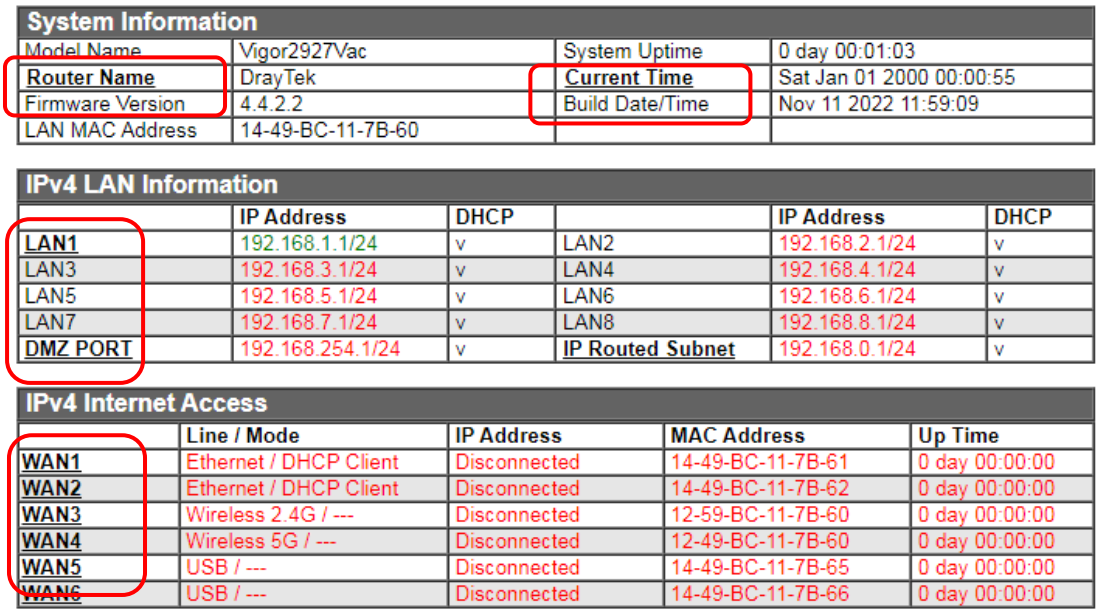
En la parte superior del Tablero, un panel virtual (que simula el panel físico del enrutador) muestra la conexión de la interfaz física. Se actualizará cada cinco segundos. Cuando mueve y hace clic con el cursor del mouse en los LED (excepto ACT), los puertos USB, WAN2/P6 o LAN1 – LAN5 (P1~P5), se abrirá la página de configuración web relacionada para que la configure si es necesario.

Puerto	Color	Descripción
WAN2/P6	Negro	El puerto WAN2 está desconectado.
	Verde	El puerto WAN2 está conectado a 1 Gbps.
	Naranja	El puerto WAN2 está conectado a 10/100 Mbps.
P1 ~ P5	Negro	El puerto LAN está desconectado.
	Verde	El puerto LAN está conectado a 1 Gbps.
	Naranja	El puerto LAN está conectado a 10/100 Mbps.

Para obtener información detallada sobre la pantalla LED, consulte**Conectores e indicadores LED I-1-1**.

I-5-2 Nombre con enlace

Un nombre con un enlace (p. ej.,Nombre del enrutador ,Tiempo actual ,WAN1~6 y etc.) a continuación significa que puede hacer clic en él para abrir la página de configuración para su modificación.



System Information

Model Name	Vigor2927Vac	System Uptime	0 day 00:01:03
Router Name	DrayTek	Current Time	Sat Jan 01 2000 00:00:55
Firmware Version	4.4.2.2	Build Date/Time	Nov 11 2022 11:59:09
LAN MAC Address	14-49-BC-11-7B-60		

IPv4 LAN Information

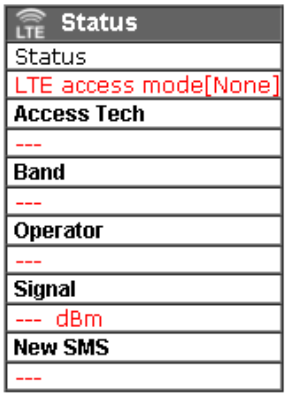
	IP Address	DHCP		IP Address	DHCP
LAN1	192.168.1.1/24	v	LAN2	192.168.2.1/24	v
LAN3	192.168.3.1/24	v	LAN4	192.168.4.1/24	v
LAN5	192.168.5.1/24	v	LAN6	192.168.6.1/24	v
LAN7	192.168.7.1/24	v	LAN8	192.168.8.1/24	v
DMZ PORT	192.168.254.1/24	v	IP Routed Subnet	192.168.0.1/24	v

IPv4 Internet Access

	Line / Mode	IP Address	MAC Address	Up Time
WAN1	Ethernet / DHCP Client	Disconnected	14-49-BC-11-7B-61	0 day 00:00:00
WAN2	Ethernet / DHCP Client	Disconnected	14-49-BC-11-7B-62	0 day 00:00:00
WAN3	Wireless 2.4G / ---	Disconnected	12-59-BC-11-7B-60	0 day 00:00:00
WAN4	Wireless 5G / ---	Disconnected	12-49-BC-11-7B-60	0 day 00:00:00
WAN5	USB / ---	Disconnected	14-49-BC-11-7B-65	0 day 00:00:00
WAN6	USB / ---	Disconnected	14-49-BC-11-7B-66	0 day 00:00:00

Estado I-5-3 para LTE

Es una tabla breve que muestra el estado actual de Vigor2927L/Vigor2927Lac, incluido el modo de acceso utilizado, la tecnología de acceso adoptada, el uso de banda, el operador, la intensidad de la señal y la notificación de nuevos SMS recibidos.



LTE Status

Status
LTE access mode[None]
Access Tech

Band

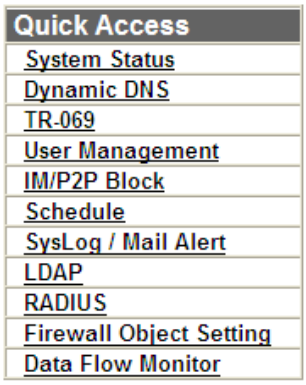
Operator

Signal
--- dBm
New SMS

I-5-4 Acceso rápido al menú de uso común

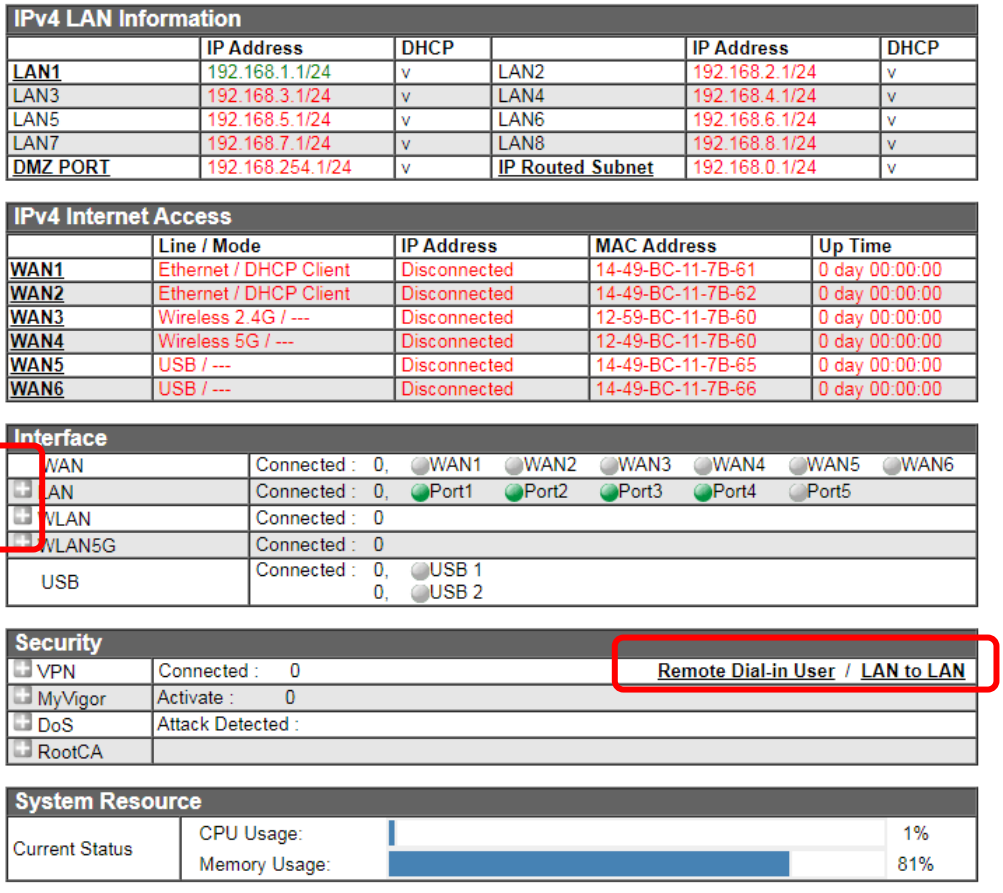
Se puede acceder a todos los elementos del menú y organizarlos ordenadamente en el lado izquierdo de la página principal para su solicitud. Sin embargo, algunos**importante**y**común**Elementos de menú usados a los que se puede acceder de forma rápida solo por comodidad.

Mire el lado derecho del Tablero. Encontrará un grupo de funciones de uso común agrupadas en**Acceso rapido**.



Aquí se muestran los enlaces de funciones de Estado del sistema, DDNS dinámico, TR-069, Gestión de usuarios, Bloqueo IM/P2P, Programación, Syslog/Alerta de correo, LDAP, RADIUS, Configuración de objetos de cortafuegos y Monitor de flujo de datos. Mueva el cursor del mouse sobre cualquiera de los enlaces y haga clic en él. La página de configuración correspondiente se abrirá inmediatamente.

Además, el acceso rápido a la configuración de seguridad de VPN, como**Usuario de marcación remota**y**LAN a LAN**se encuentran en la parte inferior de esta página. Desplácese hacia abajo en la página para encontrarlos y utilícelos si es necesario.



Tenga en cuenta que hay un plus) ubicado en el lado izquierdo de VPN/LAN. Haga clic para revisar el (conexiones VPN utilizadas actualmente.

Interface		
WAN	Connected : 0,	WAN1 WAN2 WAN3 WAN4 WAN5 WAN6
LAN	Connected : 0,	Port1 Port2 Port3 Port4 Port5
WLAN	Connected : 0	
WLAN5G	Connected : 0	
USB	Connected : 0,	USB 1
	0,	USB 2

El host conectado físicamente al enrutador a través de los puertos LAN se mostrará con círculos verdes en el campo Conectado.

Todos los hosts (incluidos los clientes inalámbricos) que se muestran con ID de host, dirección IP y dirección MAC indican que el tráfico se transmitirá a través de los puertos LAN y luego del puerto WAN. El propósito es realizar el monitor de tráfico de los hosts.

I-5-5 Mapa de interfaz gráfica de usuario

Todas las funciones que admite el enrutador se enumeran claramente en una tabla en esta página. Los usuarios pueden hacer clic en el enlace de la función para acceder a la página de configuración de la función para una configuración detallada. Haga clic en el icono en la parte superior de la pantalla principal para mostrar todas las funciones.

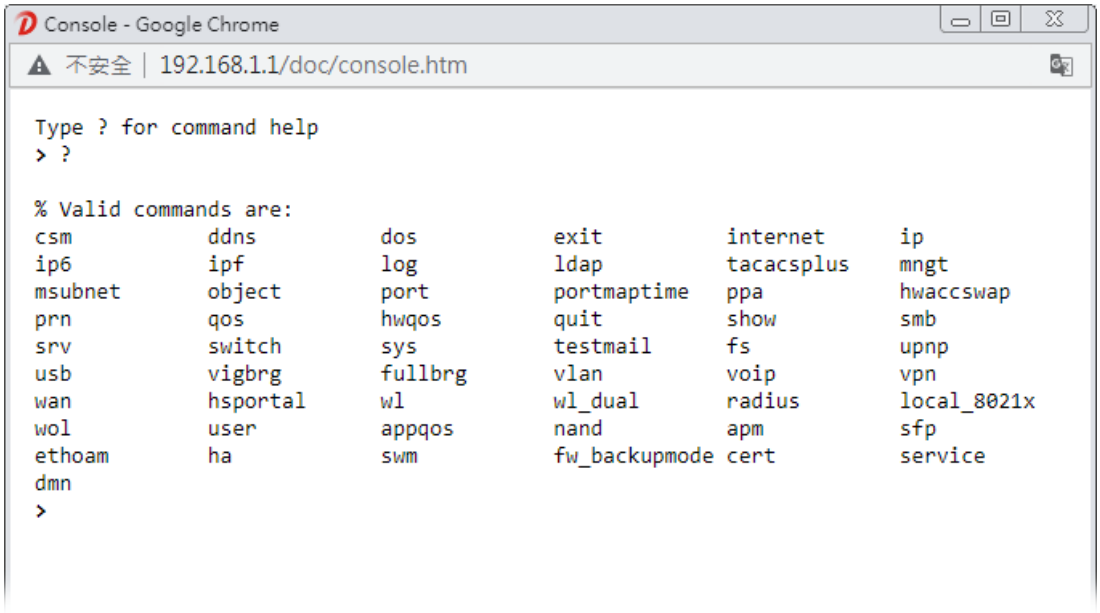
System Maintenance >> Administrator Password

Dashboard		**VoIP**	
Wizards			General Settings
	Quick Start Wizard	**Mesh**	
	Service Activation Wizard		Mesh Setup
	VPN Client Wizard		Mesh Status
	VPN Server Wizard		Mesh Discovery
	Wireless Wizard		Basic Config Sync
	Mesh Wizard		Advanced Config Sync
	VoIP Wizard		Support List
Online Status		**Wireless LAN (2.4 GHz)**	
	Physical Connection		General Setup
	Virtual WAN		Security
WAN			Access Control
	General Setup		WPS
	Internet Access		Advanced Setting
	Multi-VLAN		Station Control
	WAN Budget		Bandwidth Management
LAN			AP Discovery
	General Setup		Airtime Fairness
	VLAN		Band Steering
	Bind IP to MAC		Roaming
	LAN Port Mirror		Station List
	Wired 802.1X	**Wireless LAN (5 GHz)**	
	Link Aggregation		General Setup
Hotspot Web Portal			Security
	Profile Setup		Access Control
	Users Information		WPS
	Quota Management		WDS
	PIN Generator		Advanced Setting
Routing			Station Control

Consola web I-5-6

No es necesario utilizar el comando telnet a través del indicador de DOS. Los cambios realizados mediante la consola web tienen los mismos efectos que los modificados a través de la interfaz de usuario web. Las funciones/ configuraciones modificadas en Web Console también se pueden revisar en la interfaz de usuario web.

Haga clic en el**Consola web**en la parte superior de la pantalla principal para abrir la siguiente pantalla.

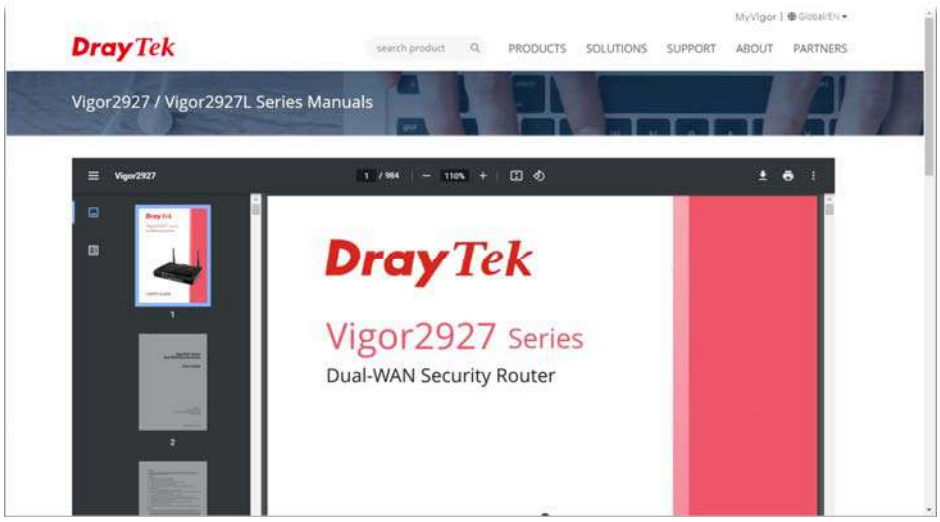


I-5-7 Copia de seguridad de configuración

Hay una forma de almacenar rápidamente la configuración utilizada actual haciendo clic en el botón**Copia de seguridad de configuración**icono. Le permite hacer una copia de seguridad de la configuración actual como un archivo. Tal archivo de configuración se puede restaurar usando **Mantenimiento del sistema>>Copia de seguridad de la configuración**.

Descarga del Manual I-5-8

Haga clic en este icono para abrir la guía del usuario en línea del enrutador Vigor. Este documento ofrece información detallada sobre la configuración de la interfaz de usuario web.



I-5-9 Cerrar sesión

Haga clic en este icono para salir de la interfaz de usuario web.

I-5-10 Estado en línea

I-5-10-1 Conexión física

Dicha página muestra el estado de la conexión física, como el estado de la conexión LAN, el estado de la conexión WAN, etc.

Conexión física para el protocolo IPv4

Online Status

Physical Connection — **System Uptime: 4days 23:49:54**

IPv4 | IPv6

LAN Status

IP Address	TX Packets	RX Packets	Router Primary DNS:	Router Secondary DNS:
192.168.1.1	289,820	206,065	8.8.8.8	8.8.4.4

WAN 1 Status >> Renew

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	00:00:00	
IP	**GW IP**	**TX Bytes**	**TX Rate(bps)**	**RX Bytes**	**RX Rate(bps)**
---	---	0 (B)	0	0 (B)	0

WAN 2 Status >> Renew

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	00:00:00	
IP	**GW IP**	**TX Bytes**	**TX Rate(bps)**	**RX Bytes**	**RX Rate(bps)**
---	---	0 (B)	0	0 (B)	0

WAN 3 Status

Enable	Line	Name	Mode	Up Time	
No	Wireless 2.4G		---	00:00:00	
IP	**GW IP**	**TX Bytes**	**TX Rate(bps)**	**RX Bytes**	**RX Rate(bps)**
---	---	0 (B)	0	0 (B)	0

SSID	Channel	Security	PHY Mode	Rate	Signal Strength
	6	Disable	---	---	0%

WAN 4 Status

Enable	Line	Name	Mode	Up Time	
No	Wireless 5G		---	00:00:00	
IP	**GW IP**	**TX Bytes**	**TX Rate(bps)**	**RX Bytes**	**RX Rate(bps)**
---	---	0	0	0	0

SSID	Channel	Security	PHY Mode	Rate	Signal Strength
	36	Disable	---	---	0%

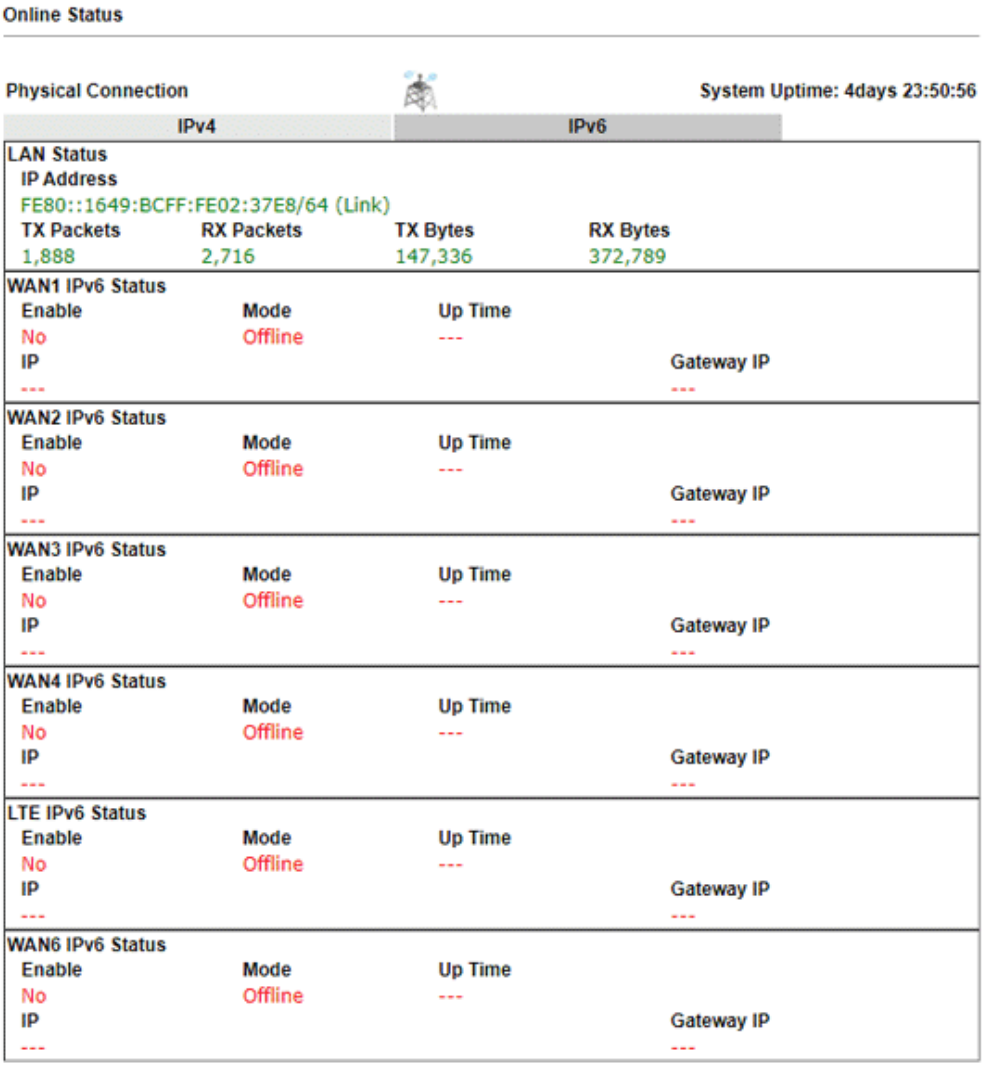
LTE Status

Enable	Line	Name	Mode	Up Time	Signal
Yes	USB		---	00:00:00	
IP	**GW IP**	**TX Bytes**	**TX Rate(bps)**	**RX Bytes**	**RX Rate(bps)**
---	---	0	0	0	0

WAN 6 Status

Enable	Line	Name	Mode	Up Time	Signal
Yes	USB		---	00:00:00	
IP	**GW IP**	**TX Bytes**	**TX Rate(bps)**	**RX Bytes**	**RX Rate(bps)**
---	---	0	0	0	0

Conexión física para el protocolo IPv6



A continuación se muestra una explicación detallada (para IPv4):

Artículo	Descripción
Estado de la LAN	**DNS primario-**Muestra la dirección del servidor DNS principal para la interfaz WAN. **DNS secundario -**Muestra la dirección del servidor DNS secundario para la interfaz WAN. **Dirección IP**-Muestra la dirección IP de la interfaz LAN. **Paquetes de transmisión**-Muestra el total de paquetes transmitidos en la interfaz LAN. **Paquetes RX**-Muestra el total de paquetes recibidos en la interfaz LAN.
WAN1/WAN2/WAN3 /WAN4/WAN5/WAN6 Estado	**Habilitar – Sí**en rojo significa que dicha interfaz está disponible pero no habilitada.**Sí**en verde significa que dicha interfaz está habilitada. **Modo**-Muestra el tipo de conexión WAN (p. ej., PPPoE). **tiempo activo**-Muestra el tiempo de actividad total de la interfaz. **IP**-Muestra la dirección IP de la interfaz WAN. **PI de GW**-Muestra la dirección IP de la puerta de enlace predeterminada. **Paquetes de transmisión**-Muestra el total de paquetes transmitidos en el

Artículo	Descripción
	interfaz WAN. **Tasa de TX**-Muestra la velocidad de los octetos transmitidos en la interfaz WAN. **Paquetes RX**-Muestra el número total de paquetes recibidos en la interfaz WAN. **Tasa de RX**-Muestra la velocidad de los octetos recibidos en la interfaz WAN.

A continuación se muestra una explicación detallada (para IPv6):

Artículo	Descripción
Estado de la LAN	**Dirección IP**- Muestra la dirección IPv6 de la interfaz LAN.. **Paquetes de transmisión**-Muestra el total de paquetes transmitidos en la interfaz LAN. **Paquetes RX**-Muestra el total de paquetes recibidos en la interfaz LAN. **Bytes de transmisión**-Muestra la velocidad de los octetos transmitidos en la interfaz LAN. **Bytes RX**-Muestra la velocidad de los octetos recibidos en la interfaz LAN.
Estado de WAN IPv6	**Habilitar – No**en rojo significa que dicha interfaz está disponible pero no habilitada.**Sí**en verde significa que dicha interfaz está habilitada. No en rojo significa que dicha interfaz no está disponible. **Modo**-Muestra el tipo de conexión WAN (p. ej., TSPC). **tiempo activo** -Muestra el tiempo de actividad total de la interfaz. **IP**-Muestra la dirección IP de la interfaz WAN. **IP de acceso**-Muestra la dirección IP de la puerta de enlace predeterminada.

Información	Las palabras en verde significan que la conexión WAN de esa interfaz está lista para acceder a Internet; las palabras en rojo significan que la conexión WAN de esa interfaz no está lista para acceder a Internet.

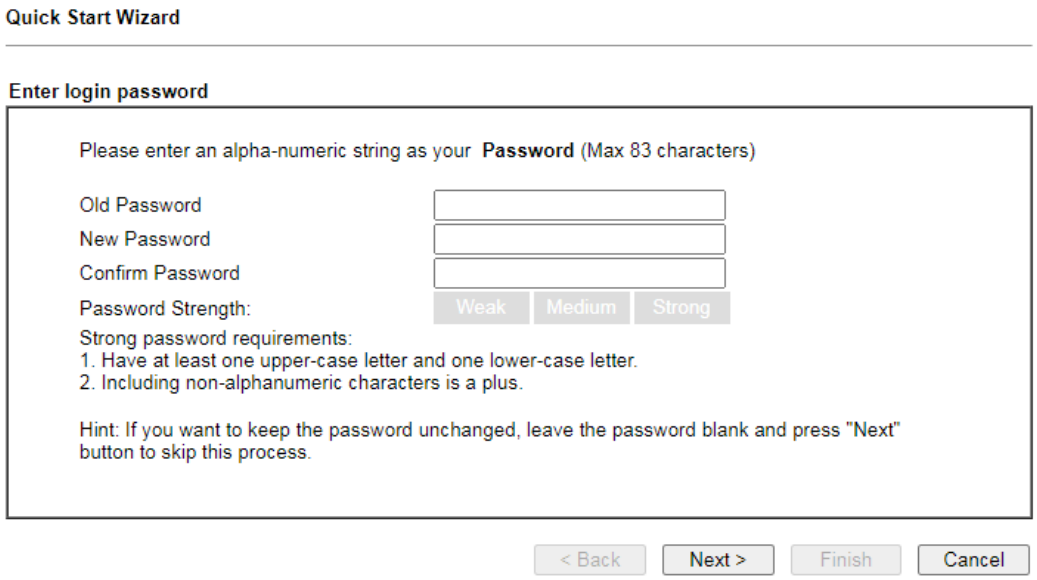
I-5-10-2 WAN virtual

Dicha página muestra la información de conexión de WAN virtual. Las WAN virtuales son utilizadas por la administración TR-069, el servicio VoIP, etc. El campo de Aplicación enumerará el propósito de dicha conexión WAN.

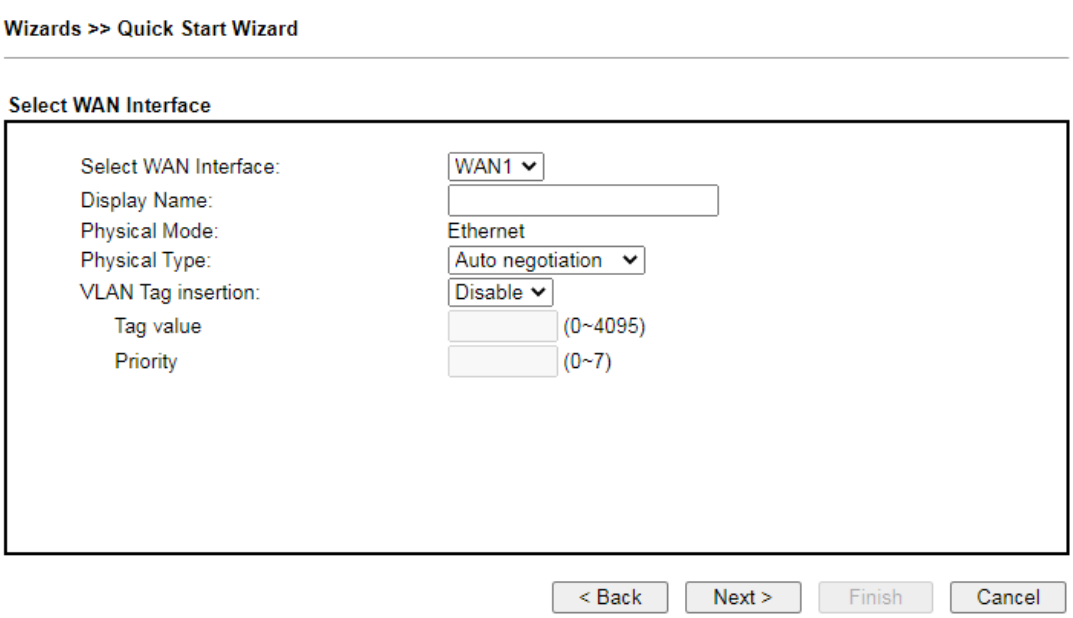
Asistente de inicio rápido I-6

El asistente de inicio rápido puede ayudarlo a implementar y usar el enrutador de manera fácil y rápida.

Ir a**Asistentes>>Asistente de inicio rápido**. La primera pantalla de**Asistente de inicio rápido**está ingresando la contraseña de inicio de sesión. Después de escribir la contraseña, haga clic en**Próximo**.



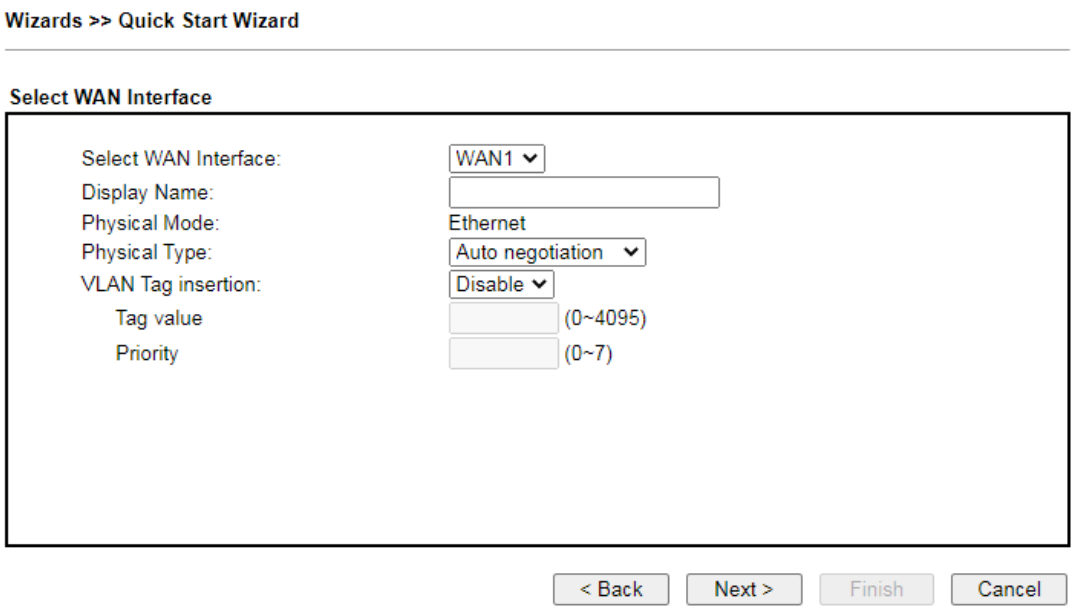
En la página siguiente, como se muestra a continuación, seleccione la interfaz WAN que utiliza. Si se utiliza la interfaz Ethernet, elija WAN1/WAN2; si se utiliza un módem USB 3G, elija WAN3 o WAN4. Luego haga clic**Próximo**para el siguiente paso.



WAN1, WAN2, WAN3, WAN4, WAN5 y WAN6 mostrarán una página de configuración diferente. Consulte lo siguiente para obtener información detallada.

I-6-1 Para WAN1/WAN2 (Ethernet)

WAN1/WAN2 se puede configurar para el modo físico de Ethernet.



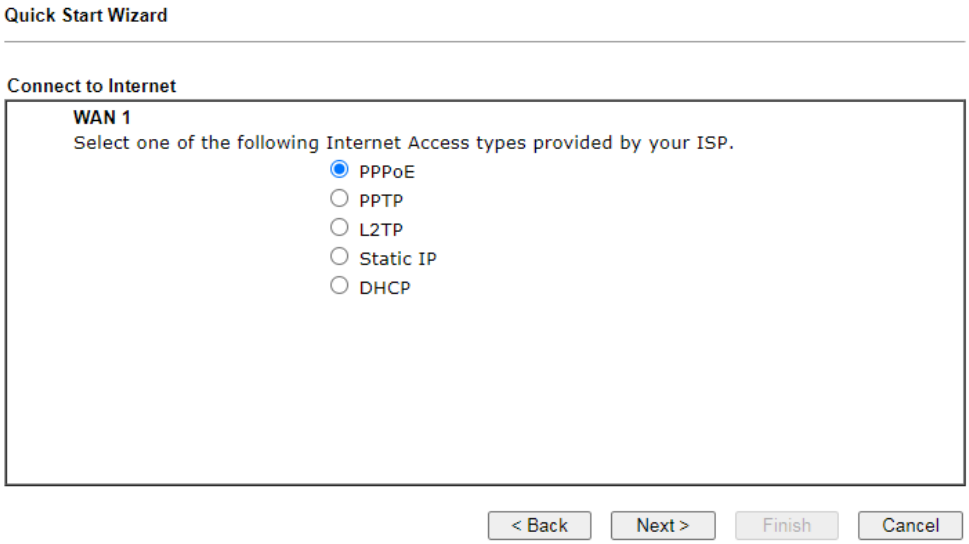
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre para mostrar	Introduzca un nombre para el enrutador.
Tipo físico	Esta configuración está disponible cuando**ethernet**se selecciona como **Modo físico**. En general,**Autonegociación**es sugerido.
Inserción de etiquetas VLAN	Los ajustes configurados en este campo están disponibles cuando **ethernet**se selecciona como**Modo físico**. **Desactivar**–Deshabilite la función de VLAN con etiqueta. **Permitir**–Habilite la función de VLAN con etiqueta. El enrutador agregará un número de VLAN específico a todos los paquetes en la WAN mientras los envía. Ingrese el valor de la etiqueta y especifique la prioridad para el envío de paquetes por WAN. - **Valor de la etiqueta**–Ingrese el valor como el número de ID de VLAN. El rango es de 0 a 4095. - **Prioridad**–Ingrese el número de prioridad del paquete para dicha VLAN. El rango es de 0 a 7.

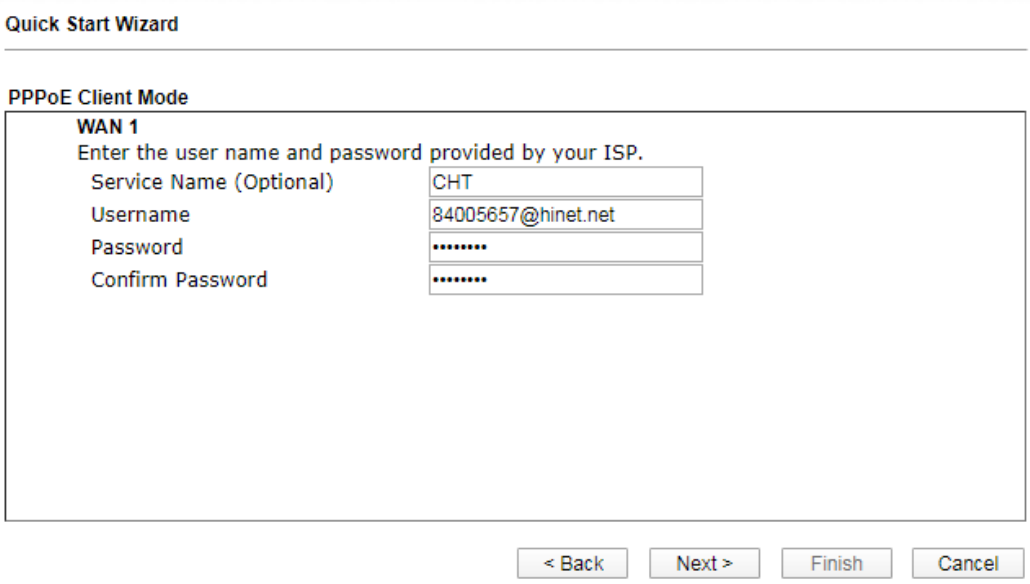
En la página siguiente, como se muestra a continuación, seleccione el tipo de acceso a Internet apropiado de acuerdo con la información de su ISP. Por ejemplo, debe seleccionar el modo PPPoE si el ISP le proporciona una interfaz PPPoE. Luego haga clic**Próximo**para el siguiente paso.

Ethernet WAN1/2 - PPPoE

1. Elige**WAN1**como interfaz WAN y seleccione**ethernet**como el**Modo físico**. Haga clic en el **Próximo**botón. Se abrirá la siguiente página para que especifique el tipo de acceso a Internet.



2. Haga clic en**PPPoE**como el Tipo de acceso a Internet. Luego haga clic**Próximo**continuar.



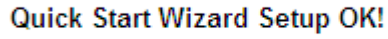
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre del Servicio (Opcional)	Introduzca la descripción del servicio de red específico.
Nombre de usuario	Asigne un nombre de usuario válido específico proporcionado por el ISP. **Nota:**La longitud máxima del nombre de usuario que puede establecer es de 63 caracteres.
Contraseña	Asigne una contraseña válida proporcionada por el ISP. **Nota:**La longitud máxima de la contraseña que puede establecer es de 62 caracteres.

Artículo	Descripción
confirmar Contraseña	Vuelva a ingresar la contraseña.
Atrás	Haga clic en él para volver a la página de configuración anterior.
Próximo	Haga clic en él para acceder a la siguiente página de configuración.
Cancelar	Haga clic en él para abandonar el asistente de inicio rápido.

3. Ingrese manualmente el nombre de usuario/contraseña proporcionado por su ISP. Hacer clic**Próximo** para ver el resumen de dicha conexión.

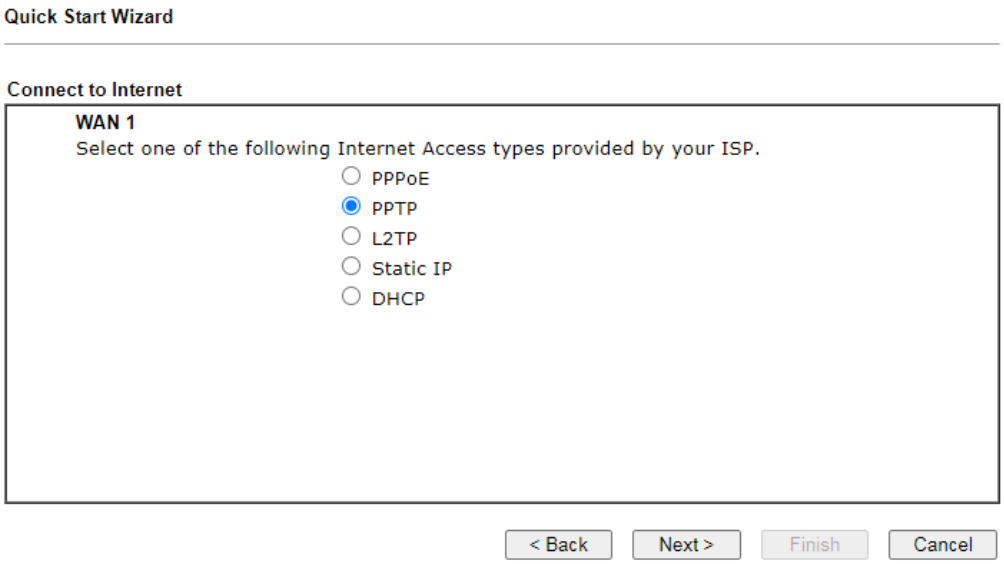
4. Haga clic en**Finalizar.**una pagina de**¡Configuración del asistente de inicio rápido OK!**aparecerá. Luego, se mostrará el estado del sistema de este protocolo.



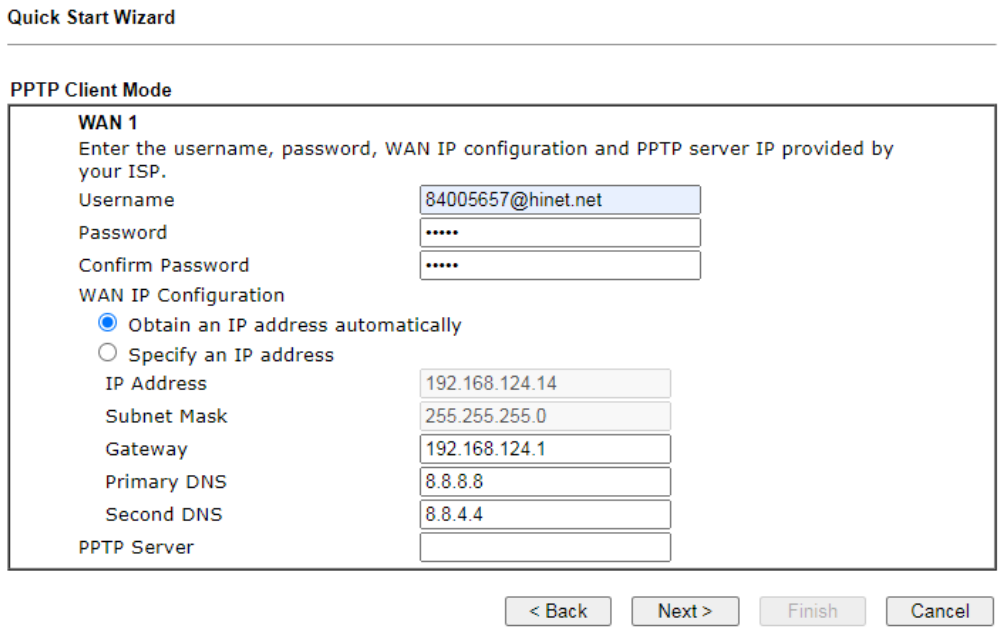
5. Ahora puedes disfrutar navegando en Internet.

Ethernet WAN1/2 - PPTP/L2TP

1. Elige**WAN1**como interfaz WAN y seleccione**ethernet**como el**Modo físico**. Haga clic en el **Próximo**botón. Se abrirá la siguiente página para que especifique el tipo de acceso a Internet.



2. Haga clic en**PPTP/L2TP**como el Tipo de acceso a Internet. Luego haga clic**Próximo**continuar.



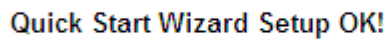
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre de usuario	Asigne un nombre de usuario válido específico proporcionado por el ISP. **Nota:**La longitud máxima del nombre de usuario que puede establecer es de 63 caracteres.
Contraseña	Asigne una contraseña válida proporcionada por el ISP. **Nota:**La longitud máxima de la contraseña que puede establecer es de 62 caracteres.

confirmar Contraseña	Vuelva a ingresar la contraseña.
Configuración IP WAN	**Obten una direccion IP automaticamente**–El enrutador obtendrá una dirección IP automáticamente del servidor DHCP. **Especifique una dirección IP**–Tienes que escribir la configuración relacional manualmente. **Dirección IP**-Introduzca la dirección IP. **Máscara de subred**–Introduzca la máscara de subred. Puerta de enlace: ingrese la dirección IP de la puerta de enlace. **DNS primario**–Introduzca la dirección IP principal del enrutador. **Segundo DNS**–Ingrese la dirección IP secundaria por necesidad en el futuro.
Servidor PPTP / Servidor L2TP	Introduzca la dirección IP del servidor.
Atrás	Haga clic en él para volver a la página de configuración anterior.
Próximo	Haga clic en él para acceder a la siguiente página de configuración.
Cancelar	Haga clic en él para abandonar el asistente de inicio rápido.

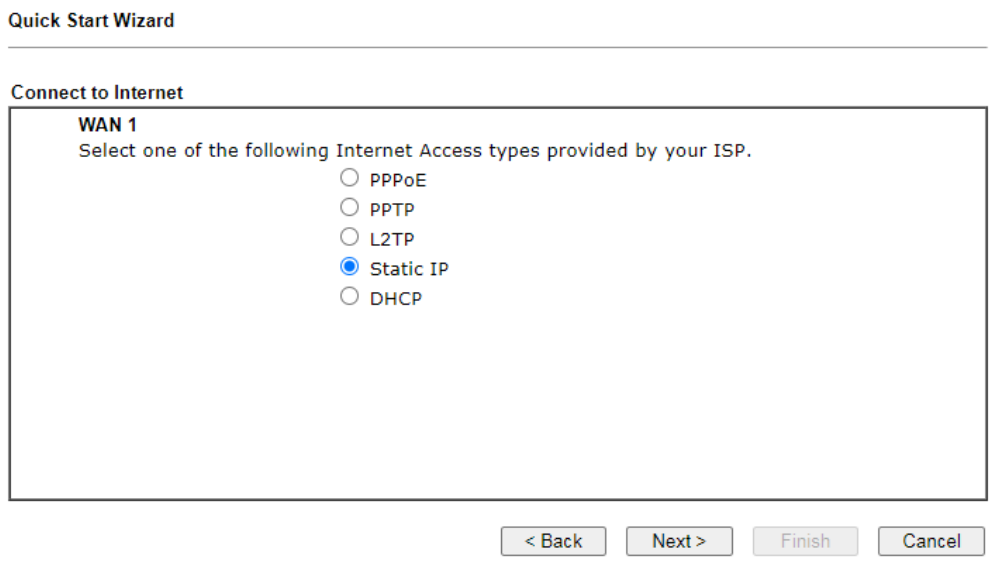
3. Ingrese la información de la dirección IP/máscara/puerta de enlace proporcionada originalmente por su ISP. Luego haga clic**Próximo**para ver el resumen de dicha conexión.

4. Haga clic en**Finalizar.**una pagina de**¡Configuración del asistente de inicio rápido OK!**aparecerá. Luego, se mostrará el estado del sistema de este protocolo.

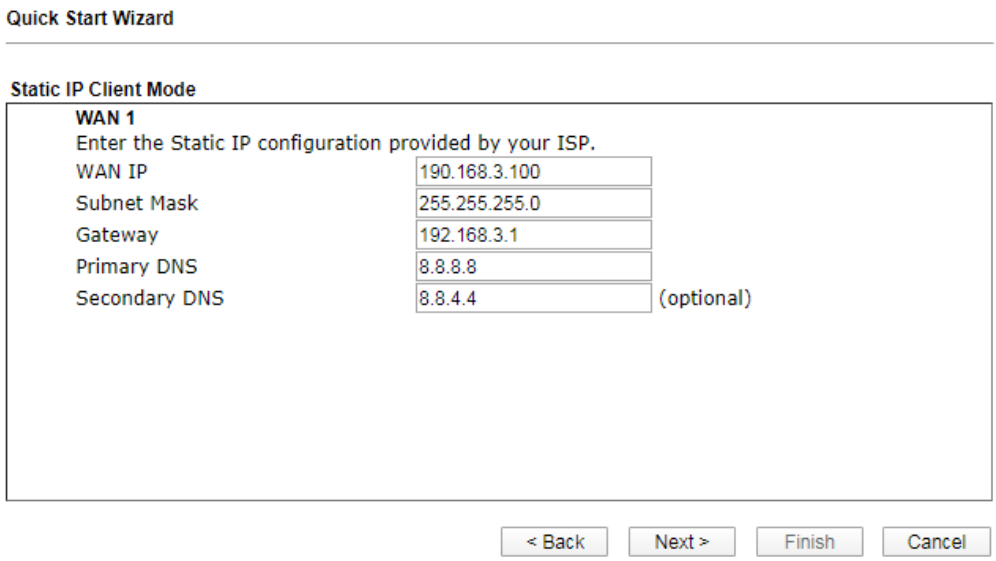


5. Ahora puedes disfrutar navegando en Internet.

1. Elige**WAN1**como interfaz WAN y seleccione**ethernet**como el**Modo físico**. Haga clic en el **Próximo**botón. Se abrirá la siguiente página para que especifique el tipo de acceso a Internet.



2. Haga clic en**IP estática**como el tipo de Acceso a Internet. Simplemente haga clic**Próximo**continuar.

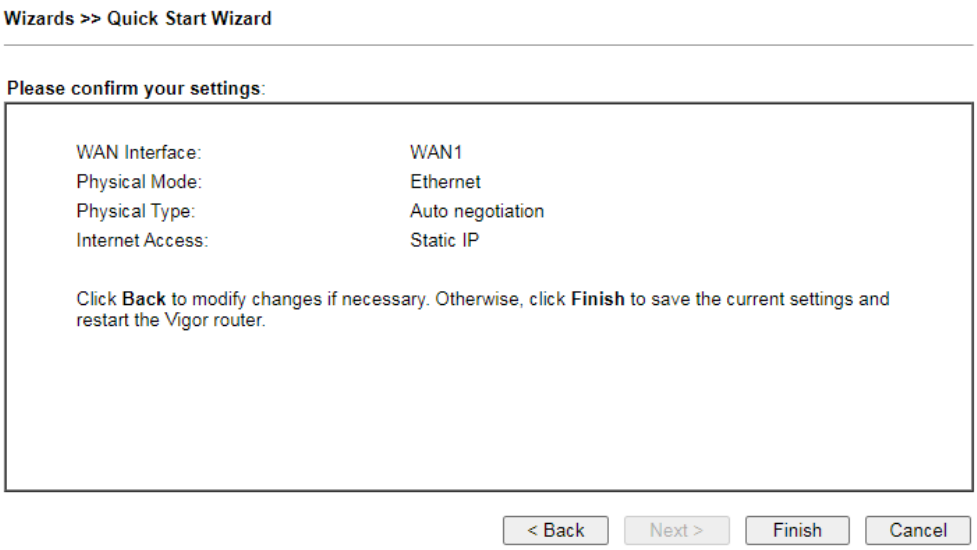


Los ajustes disponibles se explican a continuación:

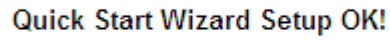
Artículo	Descripción
IP WAN	Introduzca la dirección IP.
Máscara de subred	Introduzca la máscara de subred.
Puerta	Introduzca la dirección IP de la puerta de enlace.
DNS primario	Introduzca la dirección IP principal del enrutador.
DNS secundario	Ingrese la dirección IP secundaria por necesidad en el futuro.
Atrás	Haga clic en él para volver a la página de configuración anterior.

Próximo	Haga clic en él para acceder a la siguiente página de configuración.
Cancelar	Haga clic en él para abandonar el asistente de inicio rápido.

3. Ingrese la información de la dirección IP proporcionada originalmente por su ISP. Luego haga clic**Próximo** para el siguiente paso.



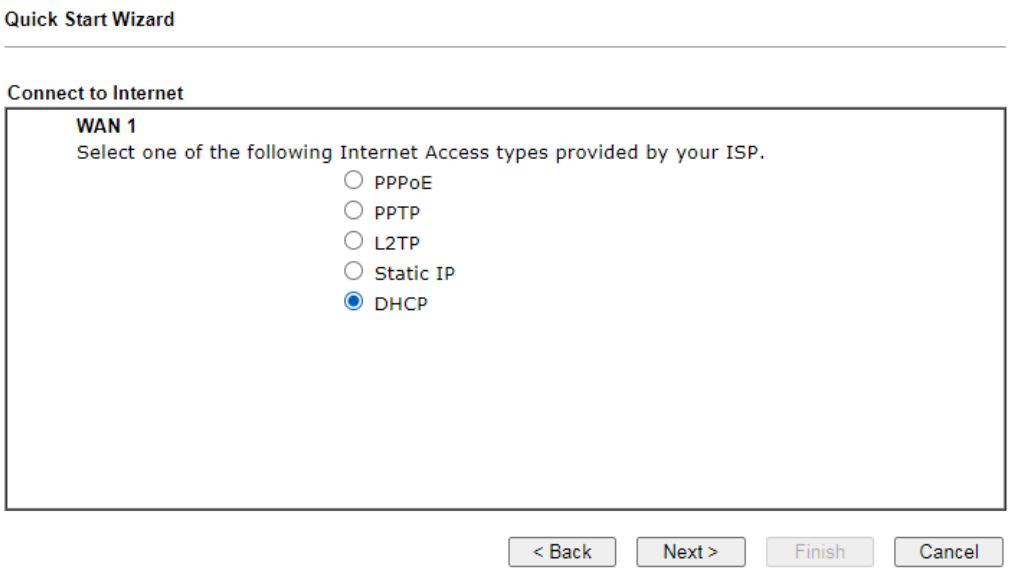
4. Haga clic en**Finalizar.**una pagina de**¡Configuración del asistente de inicio rápido OK!**aparecerá. Luego, se mostrará el estado del sistema de este protocolo.



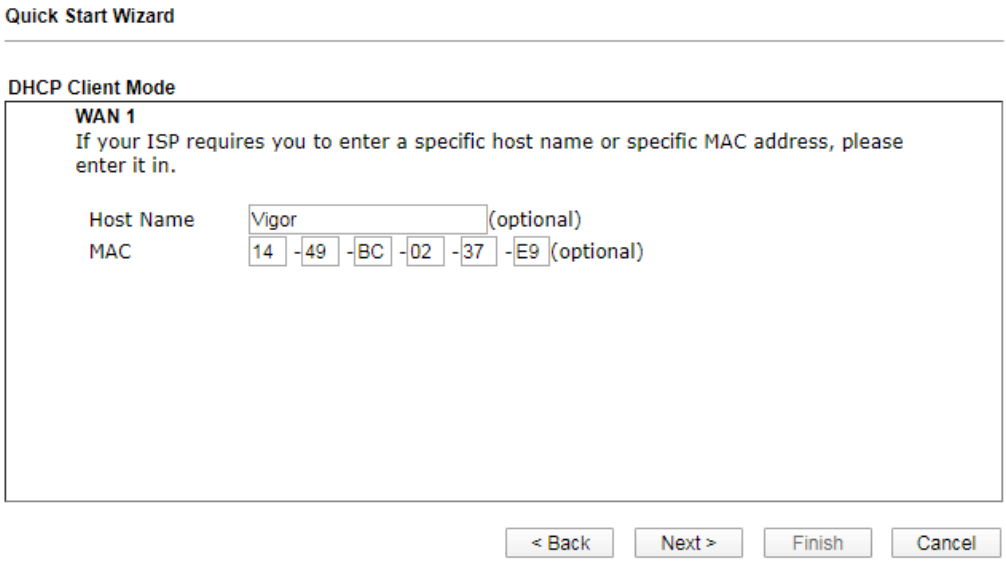
5. Ahora puedes disfrutar navegando en Internet.

Ethernet WAN1/2 - DHCP

1. Elige**WAN1**como interfaz WAN y seleccione**ethernet**como el**Modo físico**. Haga clic en el **Próximo**botón. Se abrirá la siguiente página para que especifique el tipo de acceso a Internet.



2. Haga clic en**DHCP**como el tipo de Acceso a Internet. Simplemente haga clic**Próximo**continuar.

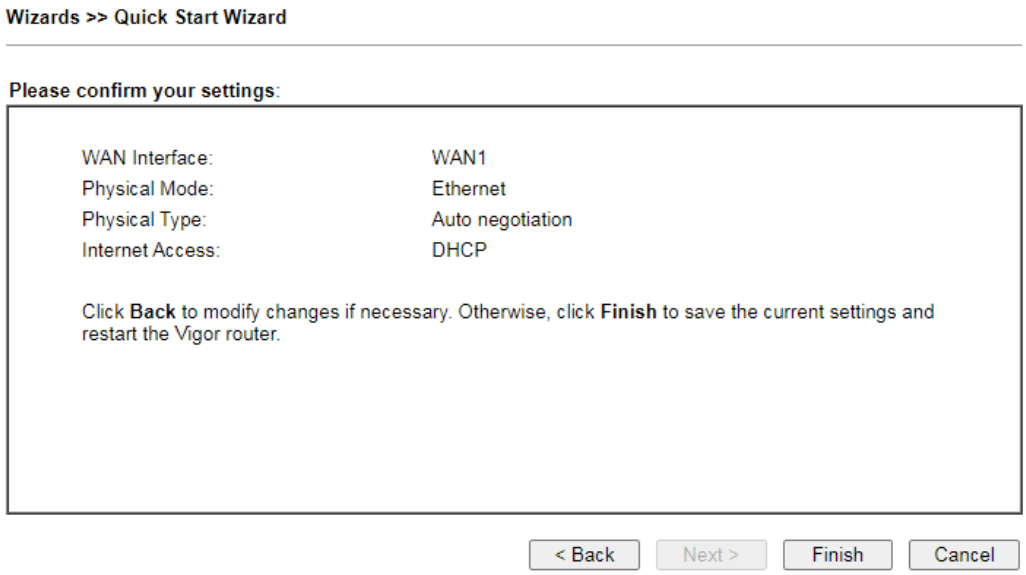


Los ajustes disponibles se explican a continuación:

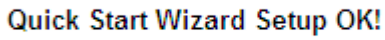
Artículo	Descripción
Nombre de anfitrión	Introduzca el nombre del anfitrión. **Nota:**La longitud máxima del nombre de host que puede configurar es de 39 caracteres.
MAC	Algunos proveedores de servicios de cable especifican una dirección MAC específica para la autenticación de acceso. En tales casos, debe ingresar la dirección MAC.
Atrás	Haga clic en él para volver a la página de configuración anterior.

Próximo	Haga clic en él para acceder a la siguiente página de configuración.
Cancelar	Haga clic en él para abandonar el asistente de inicio rápido.

3. Después de terminar la configuración anterior, haga clic en**Próximo**para ver el resumen de dicha conexión.



4. Haga clic en**Finalizar.**una pagina de**¡Configuración del asistente de inicio rápido OK!**aparecerá. Luego, se mostrará el estado del sistema de este protocolo.



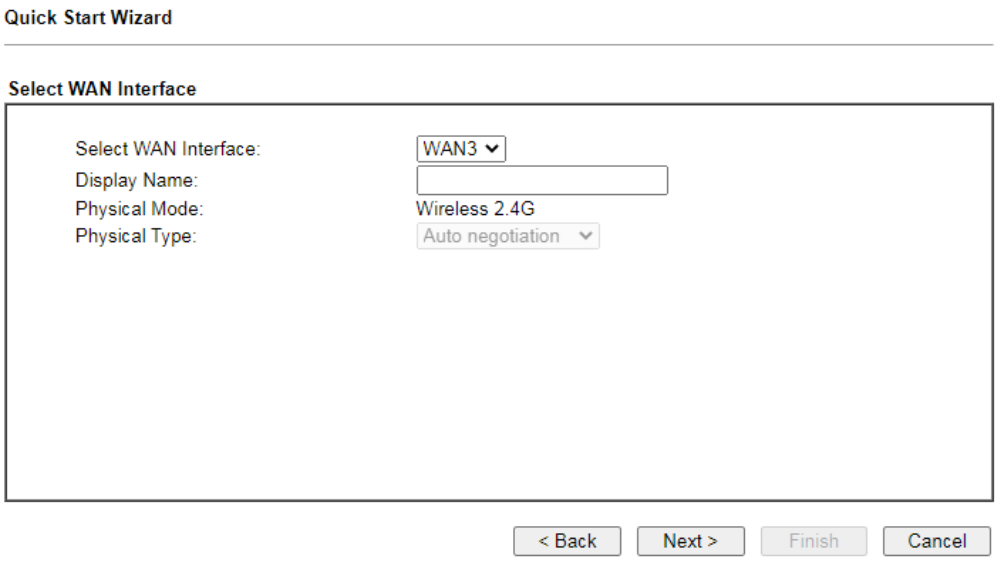
5. Ahora puedes disfrutar navegando en Internet.

I-6-2 Para WAN3/WAN4 (Inalámbrico 2.4G/Inalámbrico 5G)

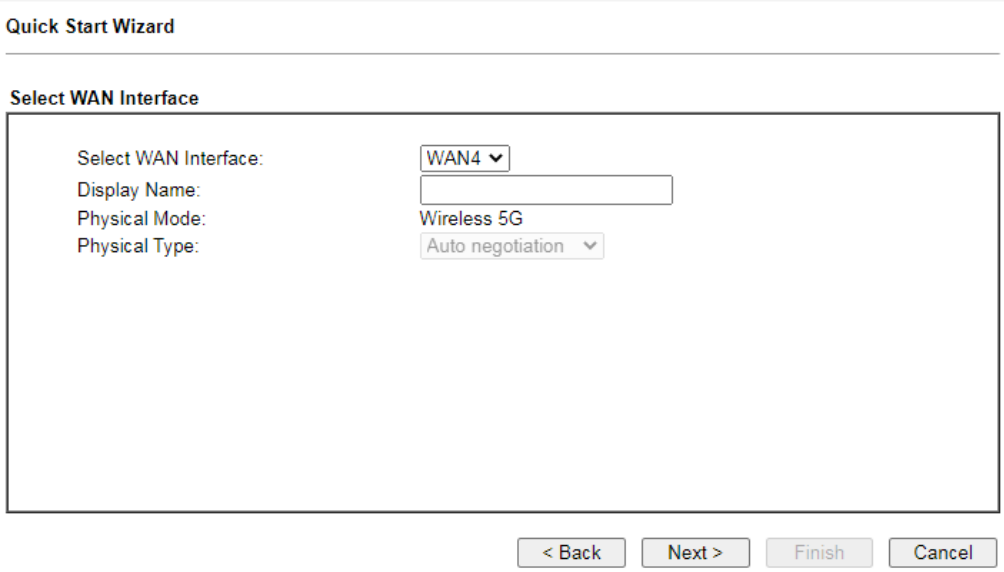
WAN3/WAN4 se utilizará para la conexión inalámbrica (2.4G o 5G).

WAN3/WAN4 inalámbrica - IP estática

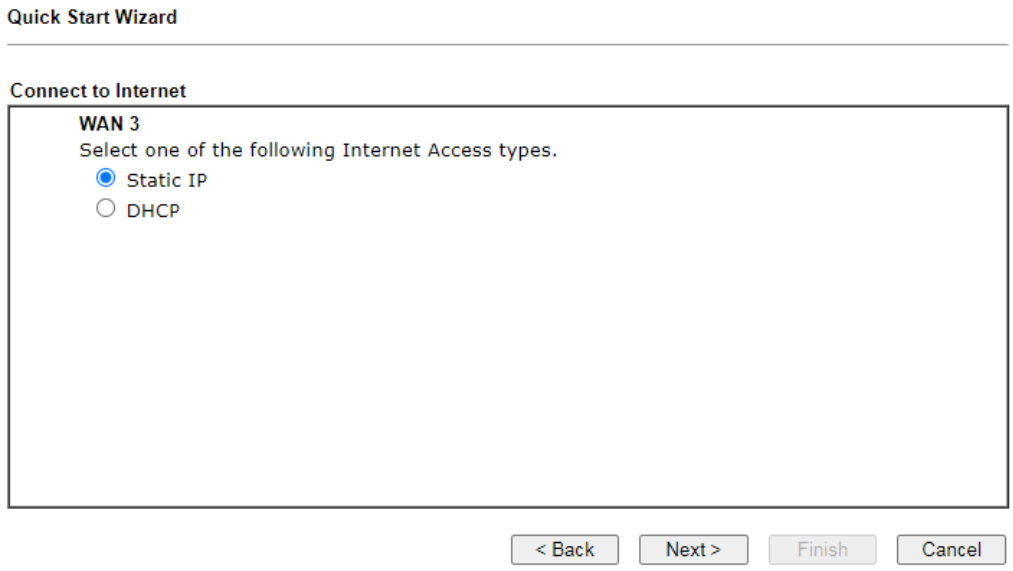
1. Elige**WAN3/WAN4**como interfaz WAN y elija**Inalámbrico 2.4G**o**5G inalámbrico**como el modo físico.



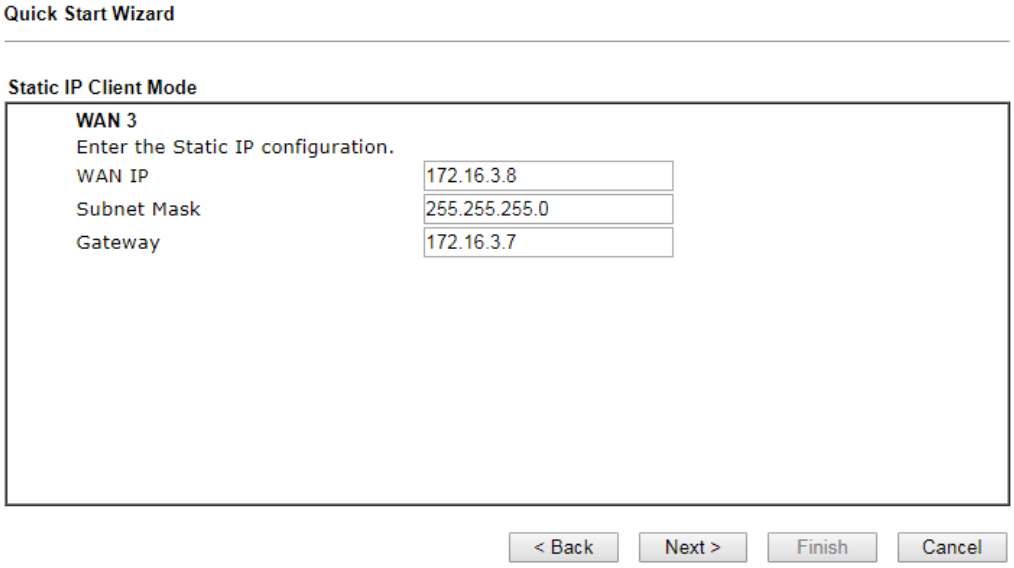
o



2. Luego, haga clic en**Próximo**por obtener la siguiente página.



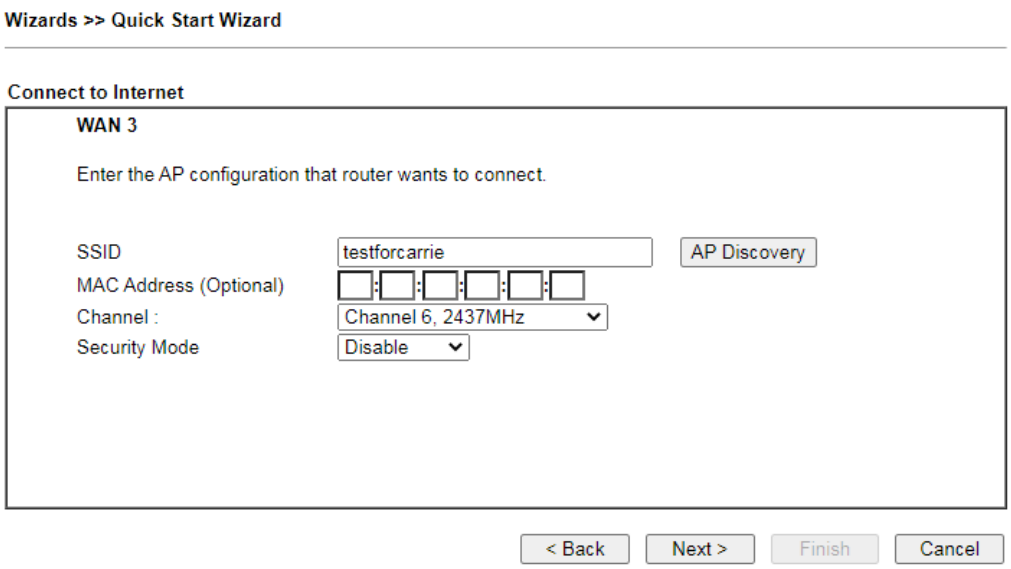
3. Después de hacer clic**IP estática**como tipo de Acceso a Internet, obtendrá la siguiente página. Ingrese la información requerida y haga clic**Próximo**continuar.



Los ajustes disponibles se explican a continuación:

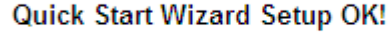
Artículo	Descripción
IP WAN	Introduzca la dirección IP.
Máscara de subred	Introduzca la máscara de subred.
Puerta	Introduzca la dirección IP de la puerta de enlace.
Atrás	Haga clic en él para volver a la página de configuración anterior.
Próximo	Haga clic en él para acceder a la siguiente página de configuración.
Cancelar	Haga clic en él para abandonar el asistente de inicio rápido.

4. En la siguiente página, ingrese el SSID de un AP existente como servidor de conexión inalámbrica para esta WAN. O haga clic**Descubrimiento de puntos de acceso**para encontrar un punto de acceso como servidor para esta interfaz WAN. Hacer clic**Próximo**continuar.



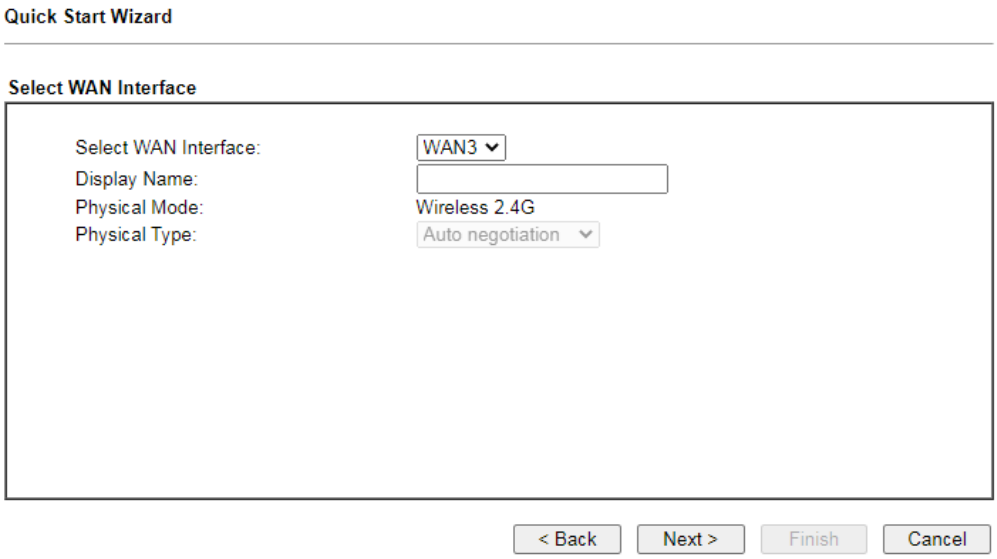
5. A continuación, se mostrará en pantalla un resumen de la conexión.

6. Haga clic en**Finalizar.**una pagina de**¡Configuración del asistente de inicio rápido OK!**aparecerá. Luego, se mostrará el estado del sistema de este protocolo.

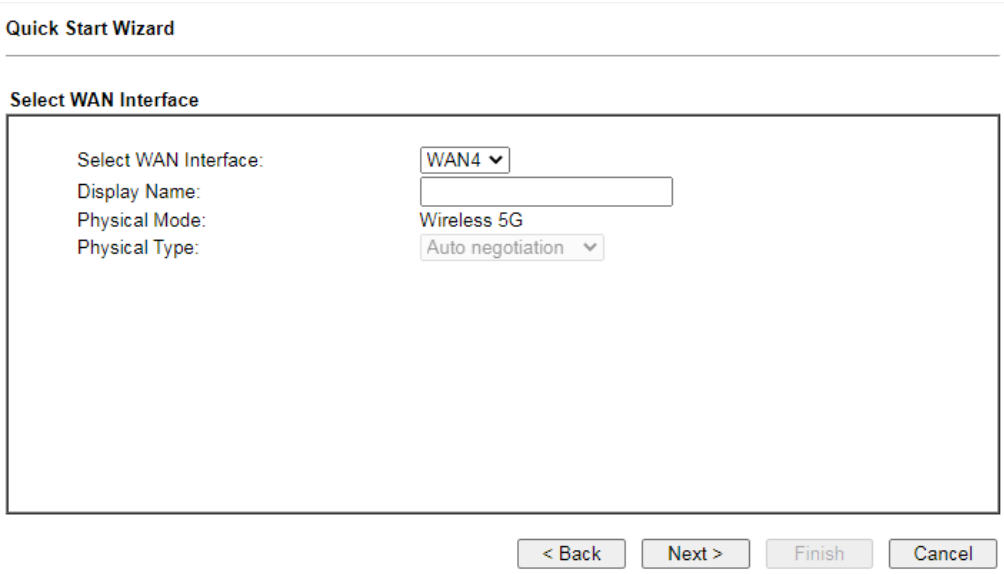


7. Ahora puedes disfrutar navegando en Internet.

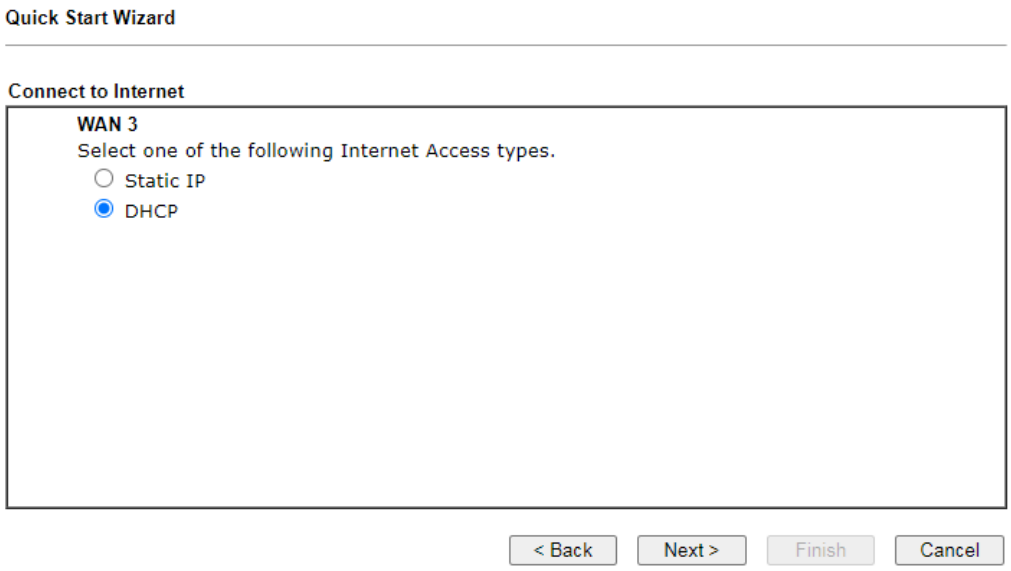
1. Elige**WAN3/WAN4**como interfaz WAN y elija**Inalámbrico 2.4G**o**5G inalámbrico**como el modo físico.



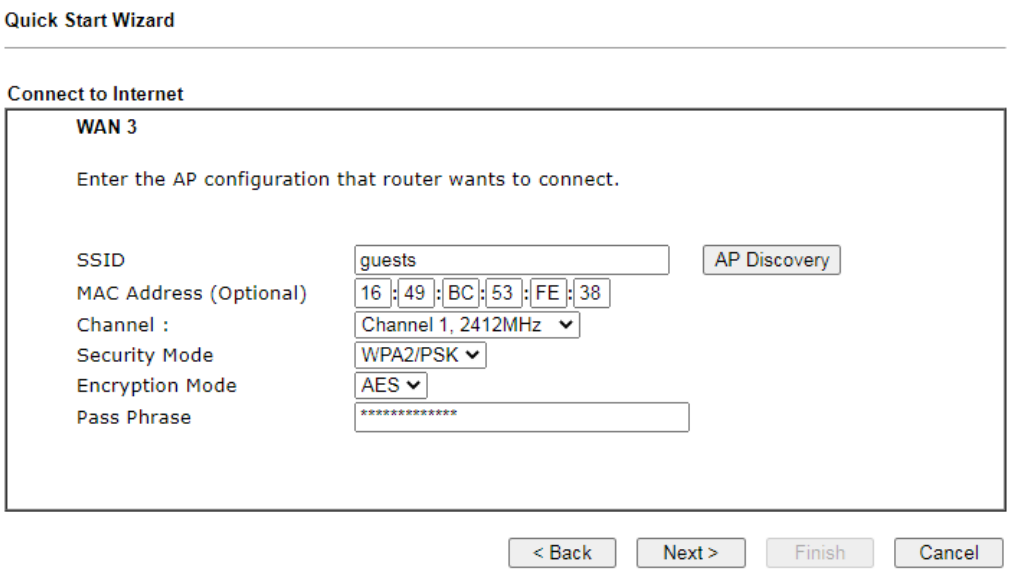
o



2. Luego, haga clic en**Próximo**por obtener la siguiente página.



3. Después de hacer clic**DHCP**como tipo de Acceso a Internet, obtendrá la siguiente página. Eingrese el SSID de un AP existente como servidor de conexión inalámbrica para esta WAN. O haga clic**Descubrimiento de puntos de acceso**para encontrar un punto de acceso como servidor para esta interfaz WAN. Hacer clic**Próximo**continuar.



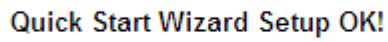
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
SSID	Ingrese el SSID de un AP existente. O haga clic**Descubrimiento de puntos de acceso**para encontrar un punto de acceso como servidor para esta interfaz WAN.
Dirección MAC	Ingrese la dirección MAC de un AP existente.
Canal	Elija un canal de frecuencia del AP inalámbrico.
Modo de seguridad	El enrutador se conecta al punto de acceso inalámbrico como cliente WEP, WPA o WPA2. Seleccione un modo para conectarse al punto de acceso inalámbrico.
Modo de encriptación	WPA/PSK utiliza TKIP como modo de cifrado. WPA2/PSK utiliza AES como modo de cifrado.

Frase de paso	Está disponible cuando WPA/PSK o WPA2/PSK están habilitados.
Claves WEP	Está disponible cuando WEP está habilitado.
Atrás	Haga clic en él para volver a la página de configuración anterior.
Próximo	Haga clic en él para acceder a la siguiente página de configuración.
Cancelar	Haga clic en él para abandonar el asistente de inicio rápido.

4. A continuación, se mostrará en pantalla un resumen de la conexión.

5. Haga clic en**Finalizar.**una pagina de**¡Configuración del asistente de inicio rápido OK!**aparecerá. Luego, se mostrará el estado del sistema de este protocolo.

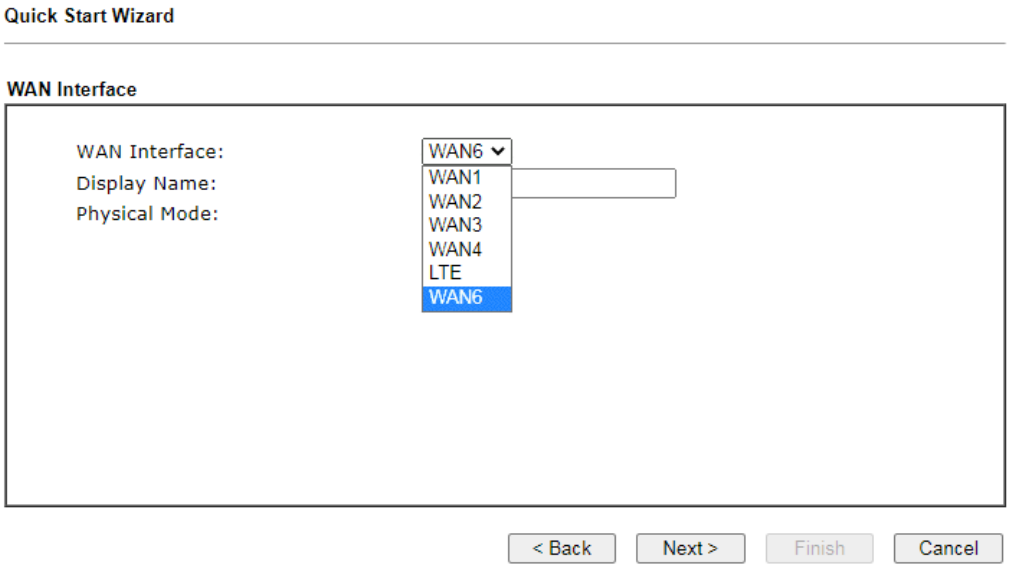


6. Ahora puedes disfrutar navegando en Internet.

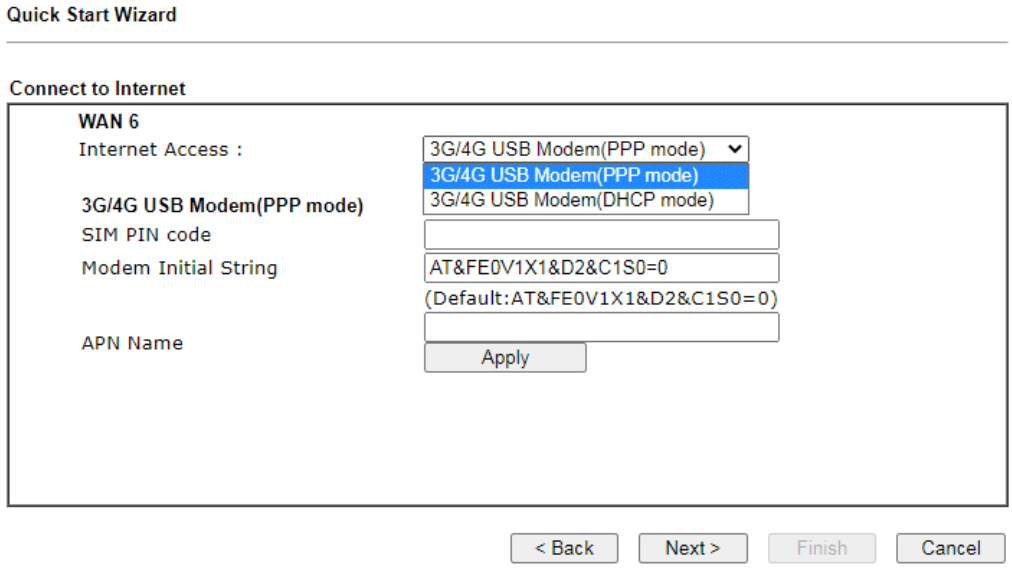
I-6-3 Para WAN5/WAN6 (USB)

WAN3/WAN4 está dedicado al modo físico en USB.

1. Elige**WAN5/WAN6**como interfaz WAN. Para el modelo "L", la WAN5 se cambiará como LTE.



2. Luego, haga clic en**Próximo**por obtener la siguiente página.

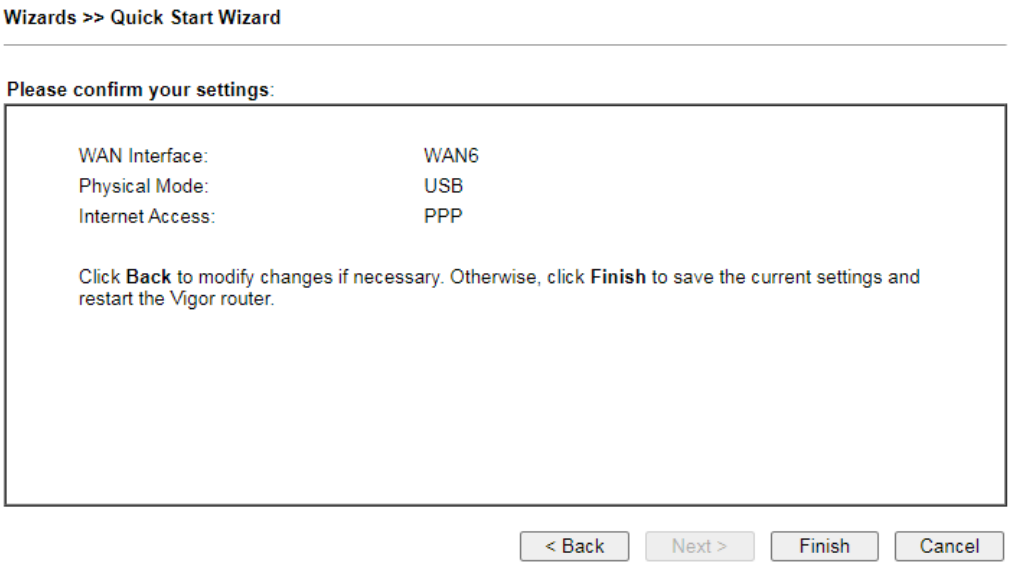


Los ajustes disponibles se explican a continuación:

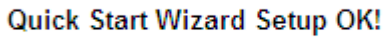
Artículo	Descripción
Acceso a Internet	Elija una de las selecciones como protocolo de acceso a Internet.
Módem USB 3G/4G (modo PPP)	**Código PIN de la tarjeta SIM**–Escriba el código PIN de la tarjeta SIM que se utilizará para acceder a Internet. La longitud máxima del código PIN que puede configurar es de 15 caracteres. **Cadena inicial del módem**–Dicho valor se utiliza para inicializar el módem USB. Utilice el valor predeterminado. Si tiene alguna pregunta, póngase en contacto con su ISP. La longitud máxima de la cadena que puede establecer es de 47 caracteres.

	Nombre de APN–APN significa Nombre de punto de acceso proporcionado y requerido por algunos ISP. Introduzca el nombre y haga clic**Aplicar**.
Módem USB 3G/4G (modo DHCP)	**Código PIN de la tarjeta SIM**–Escriba el código PIN de la tarjeta SIM que se utilizará para acceder a Internet. **Modo de red**–Obligue al enrutador Vigor a conectarse a Internet con el modo especificado aquí. Si elige 4G/3G/2G como modo de red, el enrutador elegirá automáticamente uno adecuado de acuerdo con la señal inalámbrica real. **Nombre de APN**–APN significa Nombre de punto de acceso proporcionado y requerido por algunos ISP.
Atrás	Haga clic en él para volver a la página de configuración anterior.
Próximo	Haga clic en él para acceder a la siguiente página de configuración.
Cancelar	Haga clic en él para abandonar el asistente de inicio rápido.

3. Luego, haga clic en**Próximo**para ver el resumen de dicha conexión.



4. Haga clic en**Finalizar.**una pagina de**¡Configuración del asistente de inicio rápido OK!**aparecerá. Luego, se mostrará el estado del sistema de este protocolo.



5. Ahora puedes disfrutar navegando en Internet.

Asistente de activación del servicio I-7

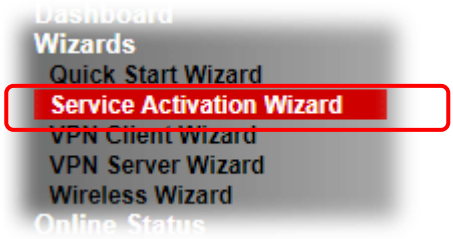
El asistente de activación del servicio puede guiarlo para activar el servicio WCF (filtro de contenido web) de una manera rápida y fácil.**El asistente de activación del servicio solo está disponible para la operación de administrador, por lo tanto, escriba "admin/admin" en el nombre de usuario/contraseña mientras inicia sesión en la interfaz de usuario web.**

Service Activation Wizard es una herramienta que le permite usar la versión de prueba de WCF directamente sin acceder al servidor (***MiVigor***) ubicado en http://myvigor.draytek.com. Para usar el perfil de filtro de contenido web, consulte la sección posterior**Perfil de filtro de contenido web**para obtener información detallada.

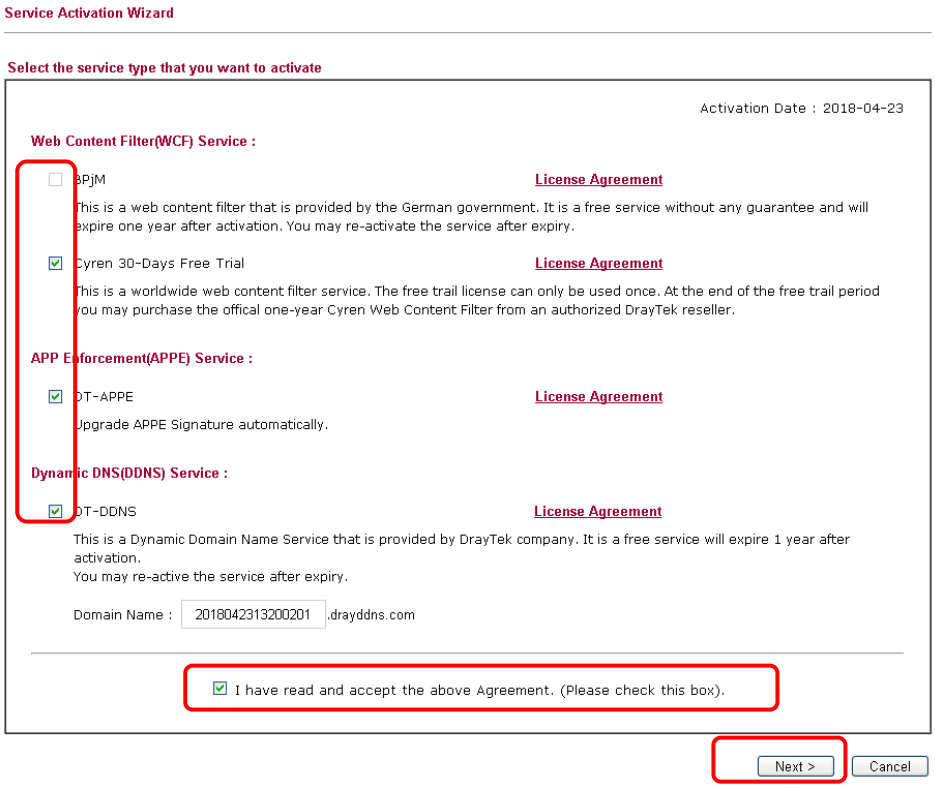
Ahora, siga los pasos que se enumeran a continuación para activar la función WCF para su enrutador.

Información	Esta función solo está disponible para el modo de administración.

1. Abierto**Asistentes>>Asistente de activación del servicio**.



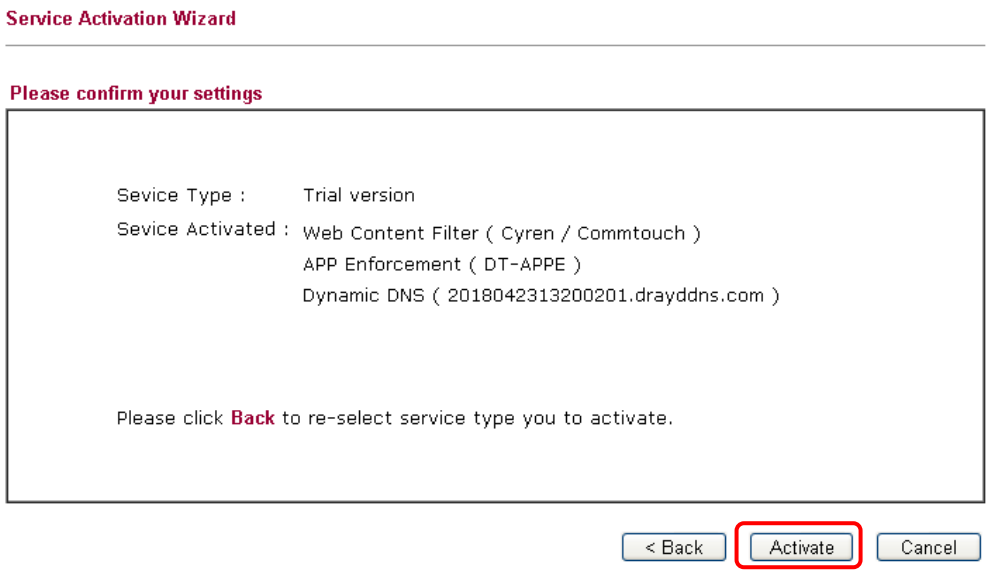
2. La pantalla de**Asistente de activación de servicios**se mostrará de la siguiente manera. Puede activar los servicios de filtro de contenido web y/o el servicio de aplicación de APPE y/o el servicio DDNS al mismo tiempo o individualmente. Cuando termine la selección, haga clic en**Próximo**.



Información

- BPjM es un filtro de contenido web (WCF) para usuarios de habla alemana. Es ideal para que su familia brinde más seguridad en Internet a los jóvenes.
- La prueba de 30 días de Cryan es WCF, que ofrece un período de prueba de 30 días.
- DT-APPE, desarrollado por DrayTek, ofrece un mecanismo para actualizar la firma APPE automáticamente.
- DT-DDNS, desarrollado por DrayTek, ofrece un año de servicio gratuito de DNS dinámico para uso interno.

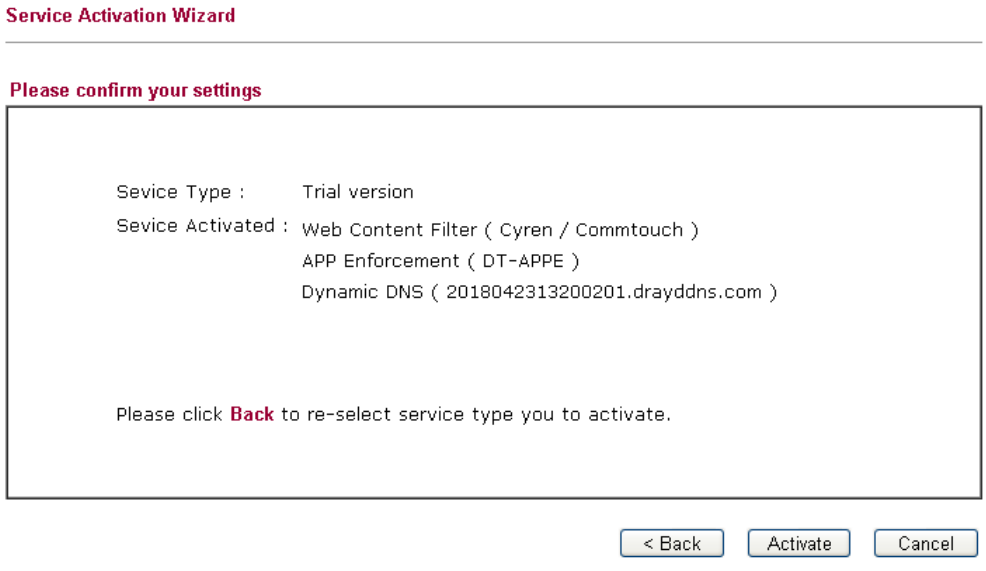
3. La página de confirmación de configuración se mostrará de la siguiente manera, haga clic en**Activar**.



Información

El servicio se activará y aplicará como la regla predeterminada configurada en Firewall>>Configuración general.

4. Ahora, la página web mostrará el servicio que ha activado de acuerdo con su(s) selección(es).

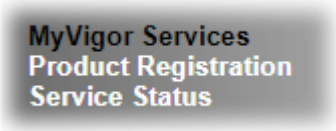


I-8 Registro del enrutador Vigor

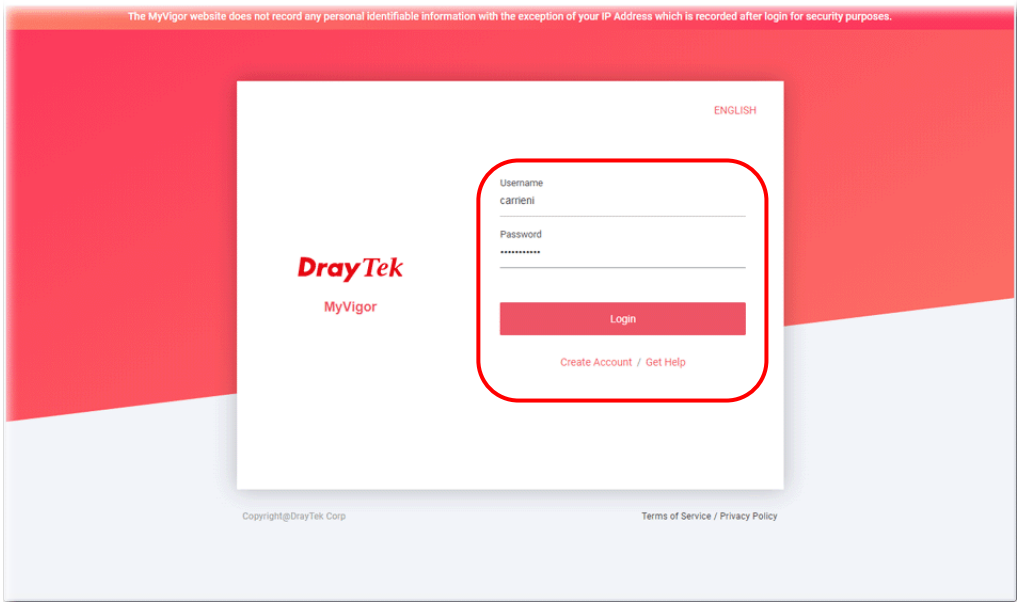
Ha finalizado la configuración del Asistente de inicio rápido y puede navegar por Internet en cualquier momento. Ahora es el momento de registrar su enrutador Vigor en el sitio web MyVigor para obtener más servicio. Siga los pasos a continuación para finalizar el registro del enrutador.

1 Inicie sesión en la interfaz de configuración web del enrutador Vigor escribiendo "**administrador/administrador**" como nombre de usuario/contraseña.

2 Hacer clic**Servicios MyVigor>>Registro de producción**desde la página de inicio.



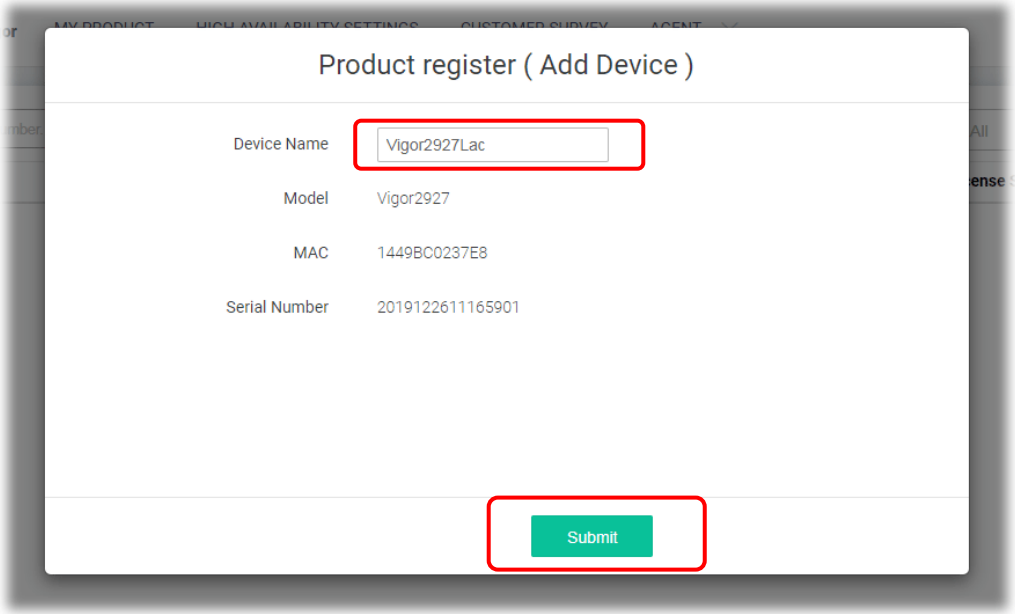
3 A**Acceso**La página se mostrará en la pantalla. Ingrese la cuenta y la contraseña que creó anteriormente. y haga clic**Acceso**.



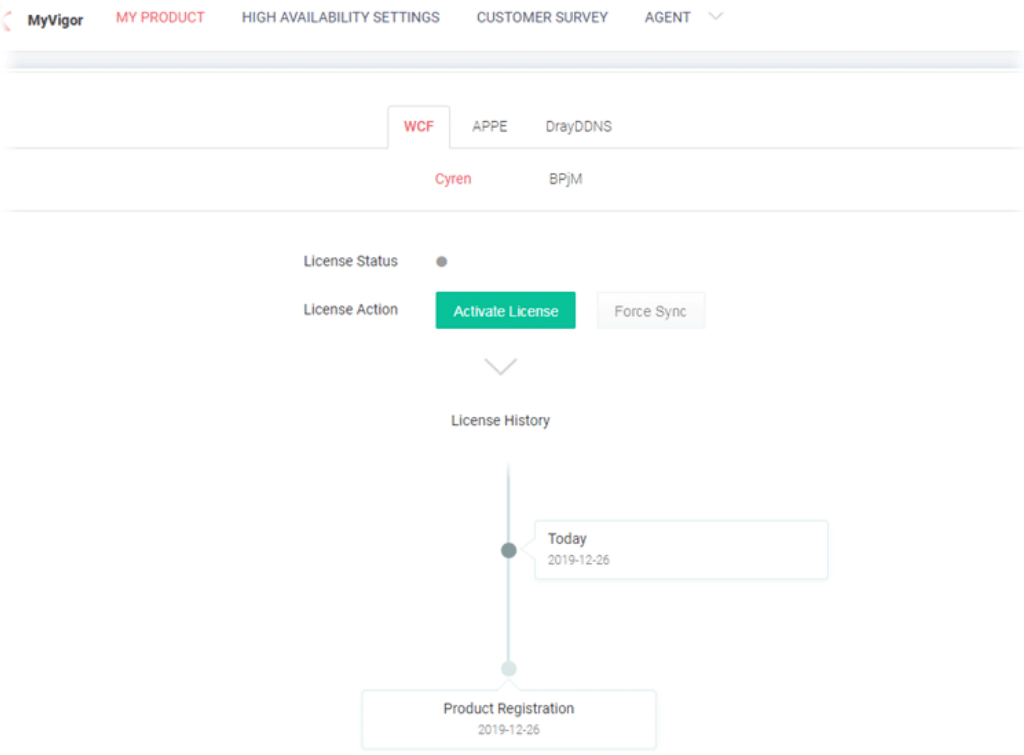
Información

Si no tiene una cuenta de acceso, consulte la sección Creación de una cuenta para MyVigor para crear una propia. Lea atentamente los artículos del Acuerdo sobre los derechos de los usuarios al crear una cuenta de usuario.

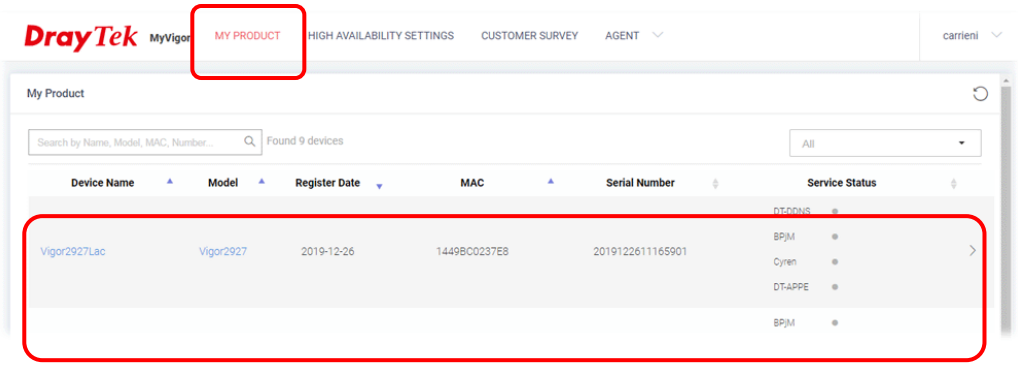
4 La siguiente página se mostrará después de iniciar sesión en MyVigor. Escriba un apodo para el enrutador, luego haga clic en**Entregar**.



5 Cuando aparece la siguiente página, la información de su enrutador se ha agregado a la base de datos. Su enrutador ha sido registrado en*mivigor*sitio web con éxito.



6 haciendo clic**MI PRODUCTO**para ver la información general del enrutador registrado en el sitio web MyVigor.



Parte II Conectividad

WAN

Significa red de área amplia. La IP pública se utilizará en WAN.

LAN

Significa red de área local. La IP privada se utilizará en LAN. La red de área local (LAN) es un grupo de subredes reguladas y gobernadas por un enrutador. El diseño de la estructura de la red está relacionado con el tipo de direcciones IP públicas que provienen de su ISP.

NAT

Cuando el flujo de datos pasa, la función de traducción de direcciones de red (NAT) del enrutador se dedicará a traducir las direcciones públicas/privadas, y los paquetes se entregarán a la PC host correcta en la red de área local.

Applications

DNS, LAN DNS, LDAP, UPnP, IGMP, Wake on LAN/ WAN, RADIUS/TACACS+, SMS/Alerta por correo, Bonjour, Alta disponibilidad, Local 802.1x

Routing

Ruta estática, equilibrio de carga/política de ruta, BGP

II-1 PÁLIDA

Permite a los usuarios acceder a Internet.

Conceptos básicos de la red de protocolo de Internet (IP)

IP significa Protocolo de Internet. Cada dispositivo en una red basada en IP, incluidos los enrutadores, el servidor de impresión y las PC anfitrionas, necesita una dirección IP para identificar su ubicación en la red. Para evitar conflictos de direcciones, las direcciones IP se registran públicamente en el Network Information Center (NIC). Tener una dirección IP única es obligatorio para aquellos dispositivos que participan en la red pública pero no en las redes de área local (LAN) TCP/IP privadas, como las PC anfitrionas bajo la administración de un enrutador, ya que no es necesario que el usuario acceda a ellas. público. Por lo tanto, la NIC ha reservado ciertas direcciones que nunca se registrarán públicamente. Estos son conocidos como ***privado***direcciones IP, y se enumeran en los siguientes rangos:

Del 10.0.0.0 al 10.255.255.255 Del 172.16.0.0 al 172.31.255.255 Del 192.168.0.0 al 192.168.255.255

¿Qué son la dirección IP pública y la dirección IP privada?

Como el enrutador desempeña un papel para administrar y proteger aún más su LAN, interconecta grupos de PC host. Cada uno de ellos tiene una dirección IP privada asignada por el servidor DHCP integrado del enrutador Vigor. El enrutador mismo también usará el valor predeterminado**ip privada**dirección: 192.168.1.1 para comunicarse con los hosts locales. Mientras tanto, el enrutador Vigor se comunicará con otros dispositivos de red a través de un**IP pública**DIRECCIÓN. Cuando el flujo de datos pasa, la función de traducción de direcciones de red (NAT) del enrutador se dedicará a traducir las direcciones públicas/privadas, y los paquetes se entregarán a la PC host correcta en la red de área local. Por lo tanto, todas las PC anfitrionas pueden compartir una conexión a Internet común.

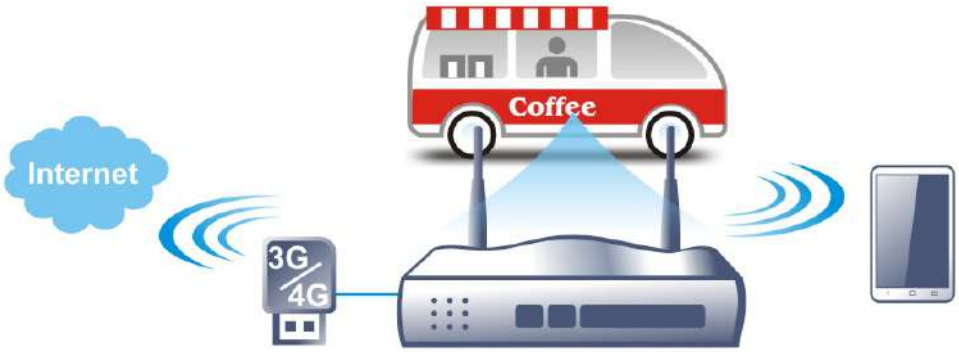
Obtenga su dirección IP pública del ISP

En la implementación de ADSL, se requiere autenticación y autorización de estilo PPP (punto a punto) para puentear el equipo de las instalaciones del cliente (CPE). El protocolo punto a punto sobre Ethernet (PPPoE) conecta una red de hosts a través de un dispositivo de acceso a un concentrador de acceso remoto o concentrador de agregación. Esta implementación proporciona a los usuarios una gran facilidad de uso. Mientras tanto, proporciona control de acceso, facturación y tipo de servicio según el requisito del usuario.

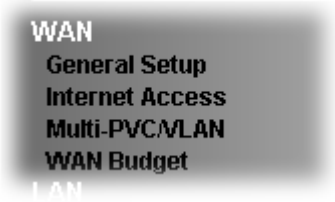
Cuando un enrutador comienza a conectarse a su ISP, se producirá una serie de procesos de descubrimiento para solicitar una conexión. Luego se creará una sesión. Su ID de usuario y contraseña se autentican a través de **PAPILLA**o**CAP**con**RADIO**sistema de autenticación Y su dirección IP, servidor DNS y otra información relacionada generalmente serán asignadas por su ISP.

Conexión de red por módem USB 3G/4G

Dado que la comunicación móvil 3G/4G a través de Access Point es cada vez más popular, Vigor2927 agrega la función de conexión de red 3G/4G para tal fin. Al conectar un módem USB 3G/4G al puerto USB de Vigor2927, puede admitir LTE/HSDPA/UMTS/EDGE/GPRS/GSM y el futuro estándar 3G/4G (HSUPA, etc.). Vigor2927n con módem USB 3G/4G le permite recibir señales 3G/4G en cualquier lugar, como su automóvil o cierta ubicación con actividad al aire libre y compartir el ancho de banda para que lo usen más personas. Los usuarios pueden usar puertos LAN en el enrutador para acceder a Internet. Además, pueden acceder a Internet a través del estándar inalámbrico 802.11(a/b/g/n/ac) y disfrutar del potente firewall, la gestión del ancho de banda y las funciones de VPN de la serie Vigor2927n.



Después de conectarse al enrutador, el módem USB 3G/4G se considerará como el puerto WAN3/WAN4. Sin embargo, todavía se pueden usar las WAN1 y WAN2 originales y se puede realizar el equilibrio de carga en el enrutador. Además, el módem USB 3G/4G en WAN3/WAN4 también se puede utilizar como dispositivo de respaldo. Por lo tanto, cuando WAN1 y WAN2 no estén disponibles, el enrutador usará 3.5G para admitir automáticamente. El módem USB 3G/4G compatible aparecerá en el sitio web de DrayTek. Visite www.draytek.com para obtener información más detallada.

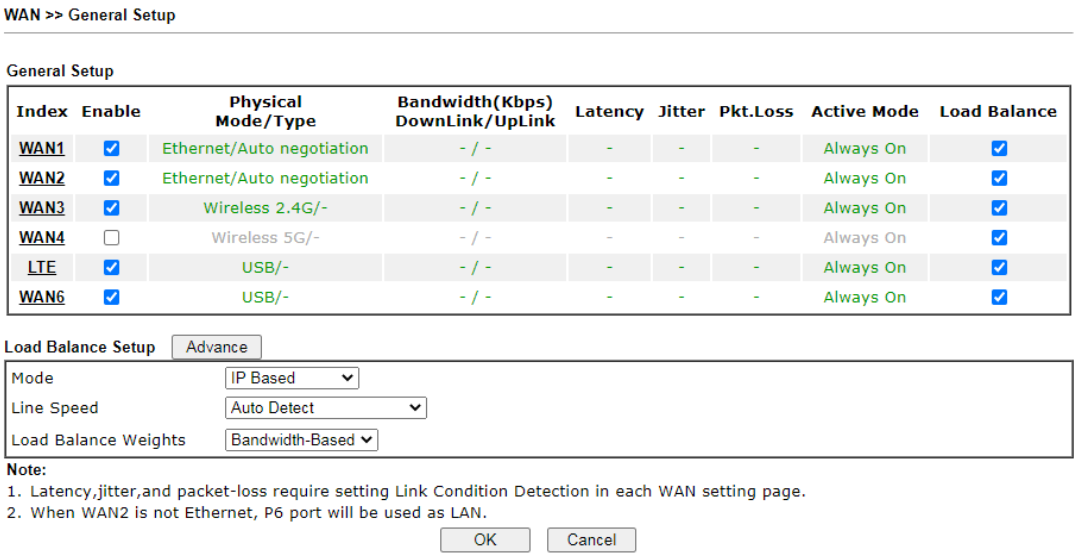


II-1-1 Configuración general

Esta sección presentará algunas configuraciones generales de Internet y explicará en detalle los modos de conexión para WAN1, WAN2, WAN3, WAN4, WAN5/LTE y WAN6.

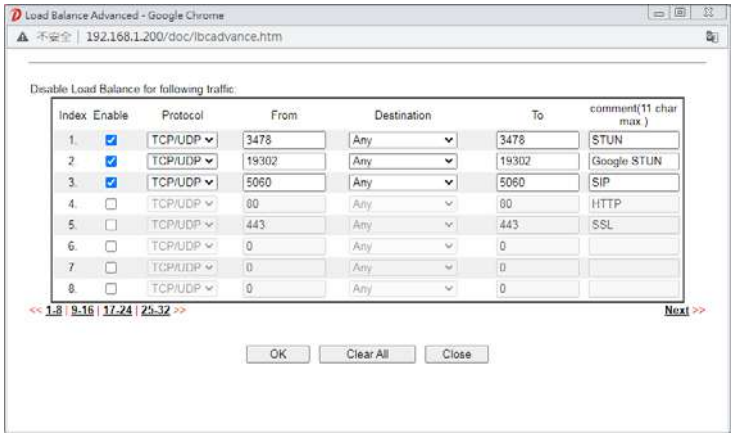
Este enrutador admite la función de WAN múltiple. Permite a los usuarios acceder a Internet y combinar el ancho de banda de las múltiples WAN para acelerar la transmisión a través de la red. Cada puerto WAN se puede conectar a diferentes ISP, incluso si los ISP utilizan una tecnología diferente para brindar servicios de telecomunicaciones (como DSL, módem por cable, etc.). Si ocurriera algún problema de conexión en una de las conexiones del ISP, todo el tráfico será guiado y cambiado al puerto de comunicación normal para una operación adecuada. Configure los ajustes de WAN1, WAN2, WAN3, WAN4, WAN5/LTE y WAN6.

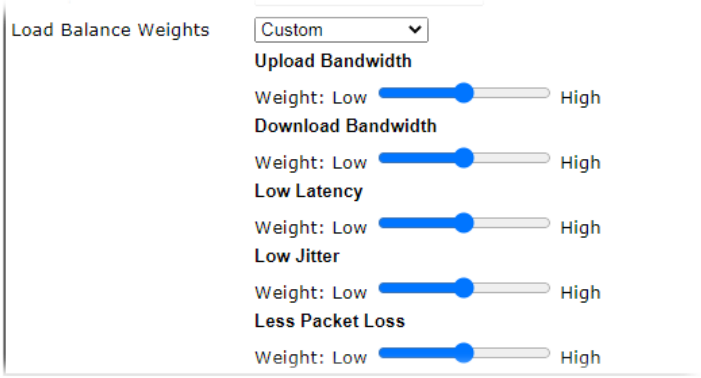
Esta página web le permite establecer la configuración general para WAN1, WAN2, WAN3, WAN4, WAN5/LTE y WAN6 respectivamente.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Índice	Haga clic en el enlace de la interfaz WAN en Índice para acceder a la página de configuración de WAN.
Permitir	**V**significa que dicha interfaz WAN está habilitada y lista para usarse.
Modo/tipo físico	Muestra el modo físico y el tipo físico de dicha interfaz WAN.
Ancho de banda (Kbps) Enlace descendente/Enlace ascendente	Muestre la velocidad de subida y bajada de dicha interfaz WAN.

Modo activo	Muestra si dicha interfaz WAN es un dispositivo activo o un dispositivo de respaldo. **Copia de seguridad (WAN#) -**Muestra la interfaz WAN de respaldo para dicha WAN cuando está deshabilitada.
Equilibrio de carga	Seleccione para habilitar la función de equilibrio de carga.
Configuración del equilibrio de carga	**Avance**-El equilibrio de carga para el tráfico de STUN, google STUN y SIP está deshabilitado de forma predeterminada para evitar conflictos. El siguiente cuadro de diálogo le permite definir el protocolo, el puerto y el nombre para que el tráfico no se aplique con equilibrio de carga. Es decir, cuando un elemento está habilitado (marcado), es posible que no se vea afectado por el equilibrio de carga. 
Modo	**Basado en IP**-El mismo par de IP de origen/destino seleccionará la misma interfaz WAN como política. Es la configuración predeterminada. **Basado en sesiones**- Todas las interfaces WAN se utilizarán (como WAN saliente) para pasar por nuevas sesiones para obtener una mejor velocidad de transmisión. Aunque se puede alcanzar un buen resultado de prueba de velocidad para el rendimiento; sin embargo, es posible que algunos sitios web no se abran sin problemas, especialmente si el sitio necesita autenticación, por ejemplo, FTP. Si no tiene una gran demanda sobre el resultado de la prueba de velocidad, mantenga la configuración predeterminada basada en IP.
Linea de velocidad	Esta opción está disponible para múltiples WAN para obtener suficiente ancho de banda para cada puerto WAN. Si conoce el ancho de banda práctico para su interfaz WAN, elija la configuración de**Según la velocidad de la línea**. De lo contrario, elija**Detección automática**para permitir que el enrutador alcance el mejor equilibrio de carga.
Pesos de equilibrio de carga	Hay cuatro tipos de peso para elegir para satisfacer su solicitud. **Costumbre**-Puede distribuir la proporción de uso para cada interfaz WAN configurando pesos para el ancho de banda, la latencia, la inestabilidad y la pérdida de paquetes, respectivamente.



- **Cargar/Descargar Ancho de Banda**-Cuanto mayor sea el peso, la interfaz WAN con mayor ancho de banda obtendrá un mayor uso.
- **Baja latencia**-Define el tiempo que tarda el enrutador Vigor en enviar los paquetes a la IP configurada en Detección de condición de enlace. Cuanto mayor sea el peso, la interfaz WAN con menor latencia obtendrá un mayor uso.
- **Jitter bajo**-Define la tasa de cambio de latencia. Para una sesión estable, un valor de fluctuación pequeño será mejor. Cuanto mayor sea el peso, la interfaz WAN con menor fluctuación obtendrá un mayor uso.
- **Menos pérdida de paquetes**-Define la proporción en que los paquetes serán descartados antes de llegar a la IP configurada en Link Condition Detection. Cuanto mayor sea el peso, la interfaz WAN con menor pérdida de paquetes obtendrá un mayor uso.

Basado en ancho de banda-El peso del equilibrio de carga para cada WAN se ejecutará de acuerdo con la configuración de velocidad de línea (velocidad de enlace descendente/enlace ascendente). Esta es la configuración predeterminada.

basado en la calidad-El peso del equilibrio de carga para cada WAN se ejecutará de acuerdo con la tasa de transmisión, el tiempo de latencia y el tiempo de fluctuación.

Basado en Confiabilidad-El peso del equilibrio de carga para cada WAN se ejecutará de acuerdo con la velocidad de línea y el valor de pérdida de paquetes. Por lo general, la interfaz WAN con baja pérdida de paquetes tendrá la relación más alta que se utilizará.

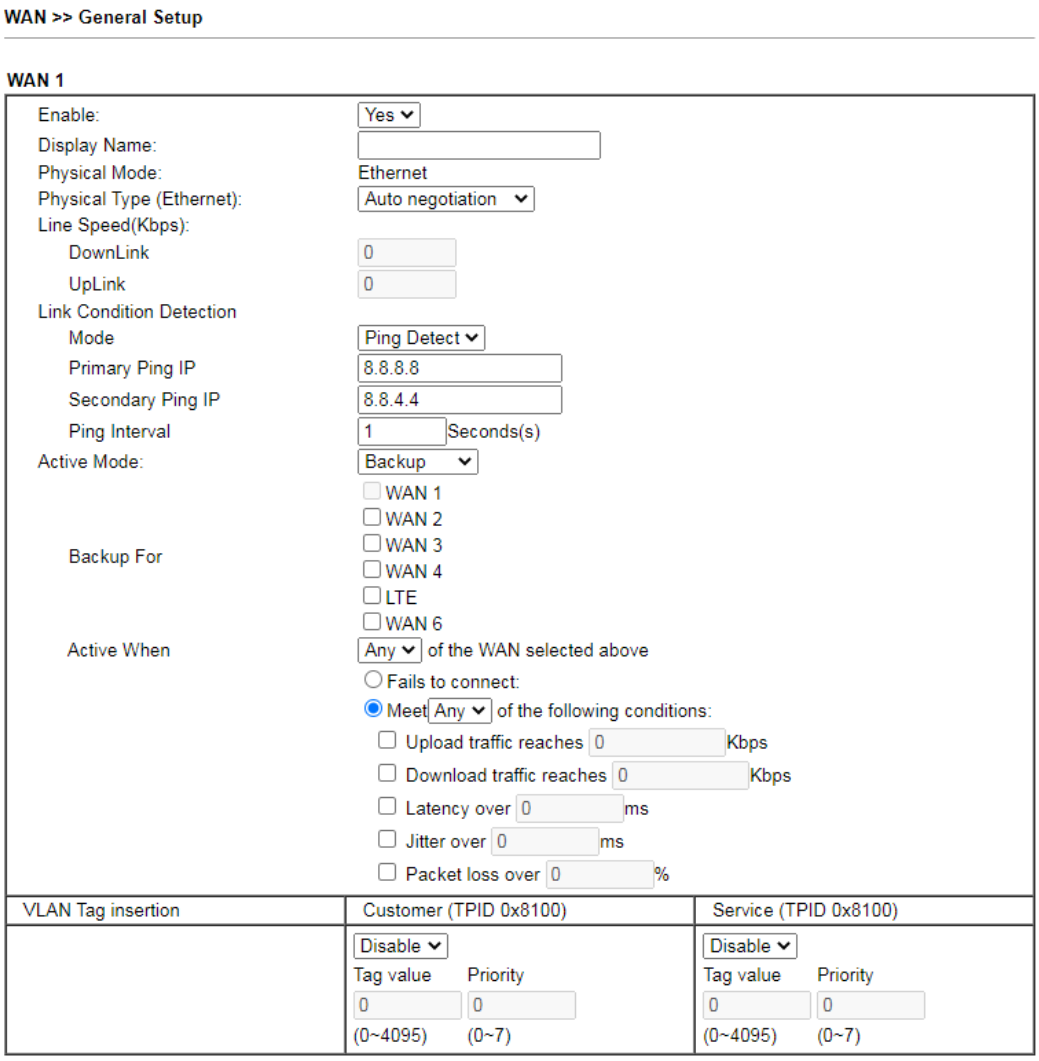
Información

El enrutador con cable (p. ej., Vigor2927) no es compatible con WAN3 y WAN4.

Después de terminar la configuración anterior, haga clic en**DE ACUERDO**para guardar la configuración.

II-1-1-1 WAN1/WAN2 (Ethernet)

WAN1/WAN2 se puede configurar para el modo físico de Ethernet.



Los ajustes disponibles se explican a continuación:

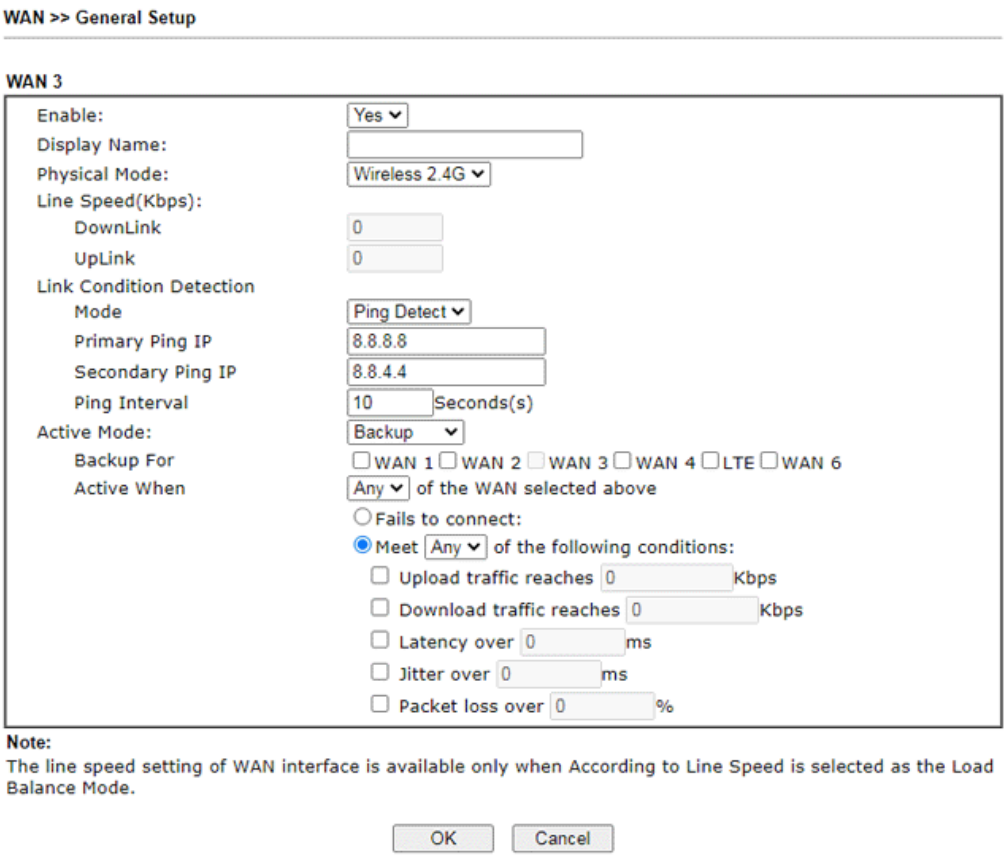
Artículo	Descripción
Permitir	Elegir**Sí**para invocar la configuración de esta interfaz WAN. Elegir **No**para deshabilitar la configuración de esta interfaz WAN.
Nombre para mostrar	Introduzca la descripción de dicha interfaz WAN.
Modo físico	Muestra el modo físico (Ethernet) de la interfaz.
Tipo físico	Puede cambiar el tipo físico para WAN1/2 o elegir **Autonegociación**determinado por el sistema.
Velocidad de línea (Kbps)	Si tu eliges**Según la velocidad de la línea**como el**Linea de velocidad** en**WAN>>Configuración general**, ingrese la velocidad de línea para descargar y cargar para dicha interfaz WAN. La unidad es kbps.
Detección de condición de enlace	Para que el sistema detecte el estado de latencia, fluctuación y pérdida de paquetes para cada interfaz WAN, debe especificar la IP que transmite los datos a través de la interfaz. **Modo**-Elija Ping Detect, Http Detect o Disable como modo de detección. Si se selecciona Ping Detect o Http Detect,

	tienes que configurar la siguiente opción. - **IP de ping principal**-Introduzca una dirección IP. **IP de** - **ping secundario**-Introduzca una dirección IP. - **Intervalo de ping**-Establezca un intervalo de tiempo (unidad:segundo) para que el sistema haga ping a la dirección IP especificada anteriormente.
Modo activo	**siempre encendido**-La WAN siempre está habilitada. **Respaldo**–La WAN está habilitada solo cuando otros puertos WAN especificados en Copia de seguridad para (ver a continuación) han perdido la conexión. - **Copia de seguridad para**-Seleccione las WAN para las que esta WAN está destinada a servir como respaldo. - **Activo cuando**-Establezca la condición para la conexión de respaldo. - **Cualquier**–Las WAN seleccionadas se activarán cuando se desconecte cualquier interfaz WAN maestra. - **Todo**–Todas las WAN de respaldo se activarán solo cuando todas las interfaces WAN maestras se desconecten. - **no se puede conectar**–Cuando falla la WAN activa, la WAN seleccionada anteriormente se activará como la conexión de red principal. - **Cumplir con todas/cualquiera de las siguientes condiciones**–Cuando el tráfico de carga, el tráfico de descarga, la latencia, la inestabilidad o la pérdida de paquetes de la WAN activa alcancen el umbral de tráfico (especificado aquí), la WAN de respaldo se habilitará automáticamente para compartir el tráfico de datos sobrecargado.
Inserción de etiquetas VLAN	Esta función se ofrece al usuario con un entorno compatible con IEEE_802.1ad. En el cual, el servicio se usa para la etiqueta externa; El cliente se utiliza para la etiqueta interna. Está disponible sólo cuando**ethernet**se selecciona como**Modo físico**. **Desactivar**–Deshabilite la función de VLAN con etiqueta. **Permitir**–Habilite la función de VLAN con etiqueta. El enrutador agregará un número de VLAN específico a todos los paquetes en la WAN mientras los envía. Ingrese el valor de la etiqueta y especifique la prioridad para el envío de paquetes por WAN1. - **Valor de la etiqueta**–Ingrese el valor como el número de ID de VLAN. El rango es de 0 a 4095. - **Prioridad**–Ingrese el número de prioridad del paquete para dicha VLAN. El rango es de 0 a 7.

Después de terminar la configuración anterior, haga clic en**DE ACUERDO**para guardar la configuración.

II-1-1-2 WAN3/WAN4 (Inalámbrico 2.4G o 5G)

WAN3/WAN4 se puede configurar para el modo físico de Wireless 2.4G o Wireless 5G.



Los ajustes disponibles se explican a continuación:

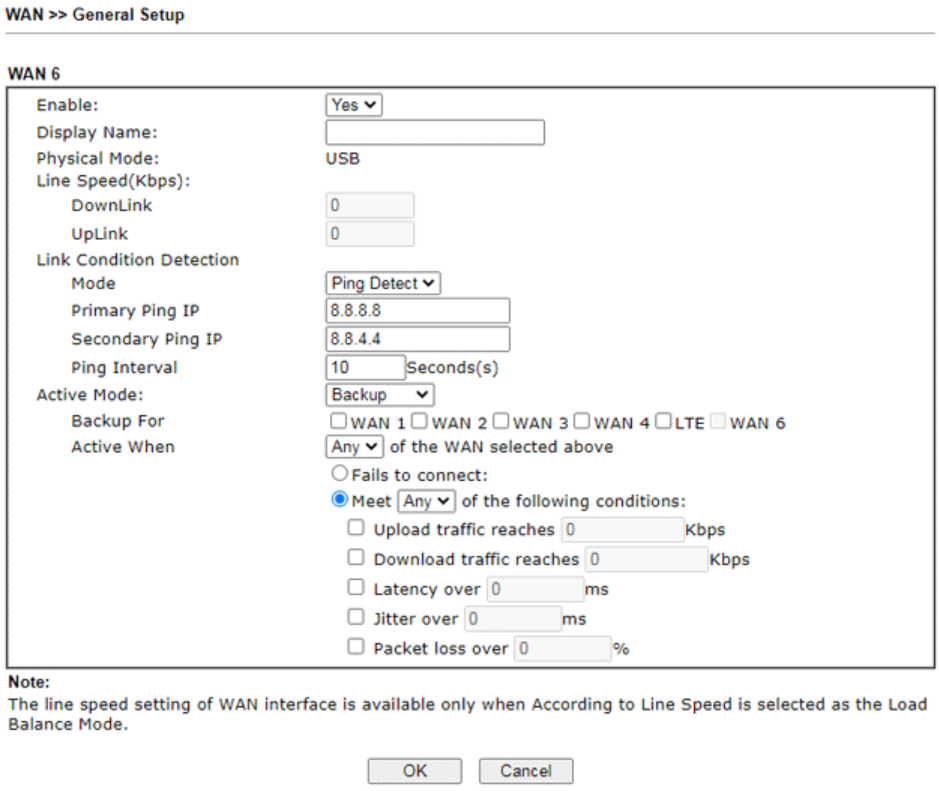
Artículo	Descripción
Permitir	Elegir**Sí**para invocar la configuración de esta interfaz WAN. Elegir **No**para deshabilitar la configuración de esta interfaz WAN.
Nombre para mostrar	Introduzca la descripción de dicha interfaz WAN.
Modo físico	Elija el modo físico (Wireless 2.4G / Wireless 5G) de la interfaz.
Velocidad de línea (Kbps)	Si tu eliges**Según la velocidad de la línea**como el**Linea de velocidad** en**WAN>>Configuración general**, ingrese la velocidad de línea para descargar y cargar para dicha interfaz WAN. La unidad es kbps.
Detección de condición de enlace	Para que el sistema detecte el estado de latencia, fluctuación y pérdida de paquetes para cada interfaz WAN, debe especificar la IP que transmite los datos a través de la interfaz. **Modo**-Elija Ping Detect, Http Detect o Disable como modo de detección. Si se selecciona Ping Detect o Http Detect, debe configurar la siguiente opción. - **IP de ping principal**-Introduzca una dirección IP. **IP de** - **ping secundario**-Introduzca una dirección IP. - **Intervalo de ping**-Establezca un intervalo de tiempo (unidad:segundo) para que el sistema haga ping a la dirección IP especificada anteriormente.
Modo activo	**siempre encendido**-La WAN siempre está habilitada. **Respaldo**–WAN está habilitado solo cuando otros puertos WAN

	especificado en Copia de seguridad para (ver más abajo), ha perdido la conexión.
	- **Copia de seguridad para**-Seleccione las WAN para las que esta WAN está destinada a servir como respaldo.
	- **Activo cuando**-Establezca la condición para la conexión de respaldo.
	  - **Cualquier**–Las WAN seleccionadas se activarán cuando se desconecte cualquier interfaz WAN maestra.
	  - **Todo**–Todas las WAN de respaldo se activarán solo cuando todas las interfaces WAN maestras se desconecten.
	  - **no se puede conectar**–Cuando falla la WAN activa, la WAN seleccionada anteriormente se activará como la conexión de red principal.
	  - **Cumplir con todas/cualquiera de las siguientes condiciones**–Cuando el tráfico de carga, el tráfico de descarga, la latencia, la inestabilidad o la pérdida de paquetes de la WAN activa alcancen el umbral de tráfico (especificado aquí), la WAN de respaldo se habilitará automáticamente para compartir el tráfico de datos sobrecargado.

Después de terminar la configuración anterior, haga clic en**DE ACUERDO**para guardar la configuración.

II-1-1-3 WAN5 / WAN6 (USB) o LTE

Para usar una conexión de red 3G/4G a través de un módem USB 3G/4G, configure**WAN5 o LTE/ WAN6**interfaz.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Elegir**Sí**para invocar la configuración de esta interfaz WAN. Elegir **No**para deshabilitar la configuración de esta interfaz WAN.
Nombre para mostrar	Introduzca la descripción de dicha interfaz WAN.

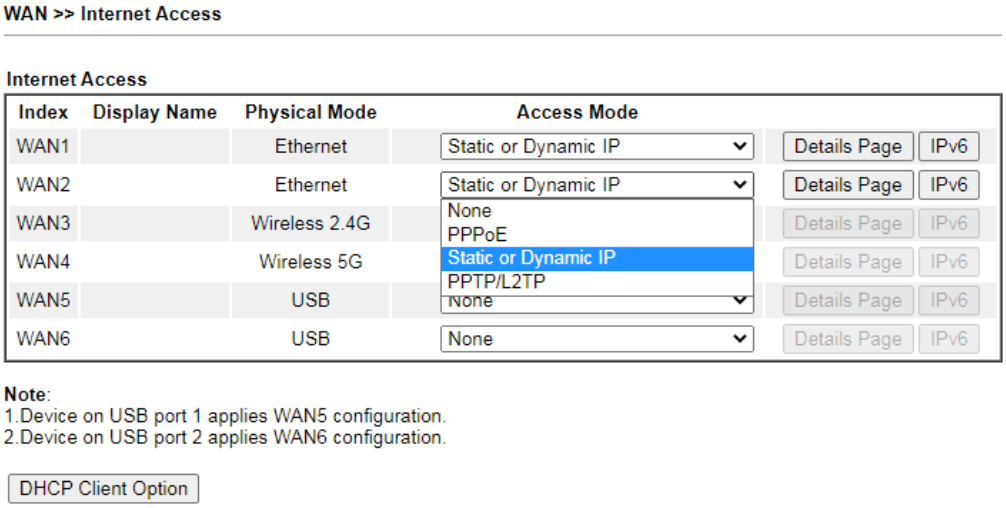
Modo físico	Muestra el modo físico de dicha interfaz WAN.
Velocidad de línea (Kbps)	Si tu eliges**Según la velocidad de la línea**como el**Linea de velocidad**en **WAN>>Configuración general**, ingrese la velocidad de línea para descargar y cargar para dicha interfaz WAN. La unidad es kbps.
Detección de condición de enlace	Para que el sistema detecte el estado de latencia, fluctuación y pérdida de paquetes para cada interfaz WAN, debe especificar la IP que transmite los datos a través de la interfaz. **Modo**-Elija Ping Detect, Http Detect o Disable como modo de detección. Si se selecciona Ping Detect o Http Detect, debe configurar la siguiente opción. - **IP de ping principal**-Introduzca una dirección IP. **IP de** - **ping secundario**-Introduzca una dirección IP. - **Intervalo de ping**-Establezca un intervalo de tiempo (unidad:segundo) para que el sistema haga ping a la dirección IP especificada anteriormente.
Modo activo	**siempre encendido**-La WAN siempre está habilitada. **Respaldo**–La WAN está habilitada solo cuando otros puertos WAN especificados en Copia de seguridad para (ver a continuación) han perdido la conexión. - **Copia de seguridad para**-Seleccione las WAN para las que esta WAN está destinada a servir como respaldo. - **Activo cuando**-Establezca la condición para la conexión de respaldo. - **Cualquier**–Las WAN seleccionadas se activarán cuando se desconecte cualquier interfaz WAN maestra. - **Todo**–Todas las WAN de respaldo se activarán solo cuando todas las interfaces WAN maestras se desconecten. - **no se puede conectar**–Cuando falla la WAN activa, la WAN seleccionada anteriormente se activará como la conexión de red principal. - **Cumplir con todas/cualquiera de las siguientes condiciones**–Cuando el tráfico de carga, el tráfico de descarga, la latencia, la inestabilidad o la pérdida de paquetes de la WAN activa alcancen el umbral de tráfico (especificado aquí), la WAN de respaldo se habilitará automáticamente para compartir el tráfico de datos sobrecargado.

Después de terminar la configuración anterior, haga clic en**DE ACUERDO**para guardar la configuración.

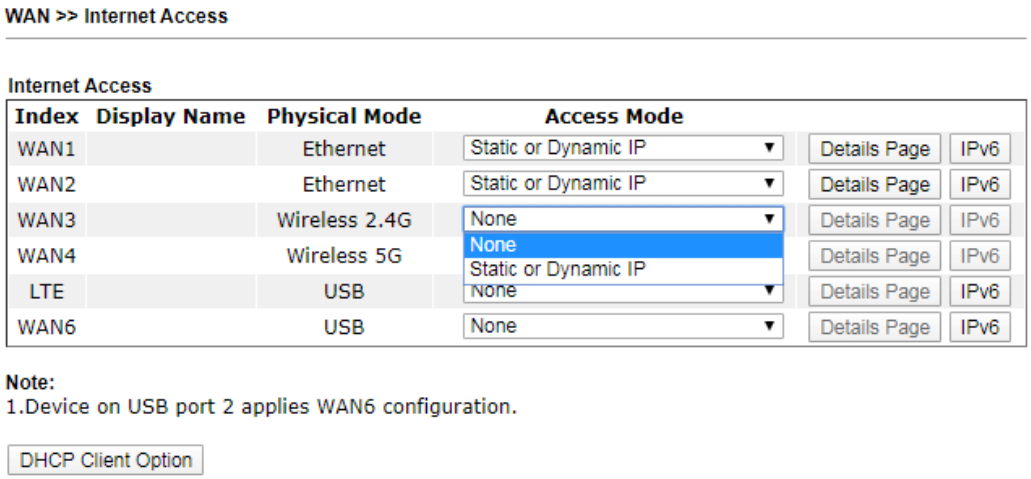
II-1-2 Acceso a Internet

Para que el enrutador admita la función de WAN múltiple, los usuarios pueden establecer diferentes configuraciones de WAN (para WAN1, WAN2, WAN3 o LTE, WAN4) para el acceso a Internet. Debido al modo físico diferente para la interfaz WAN, el modo de acceso para estas conexiones también varía. Consulte las siguientes figuras para ver ejemplos.

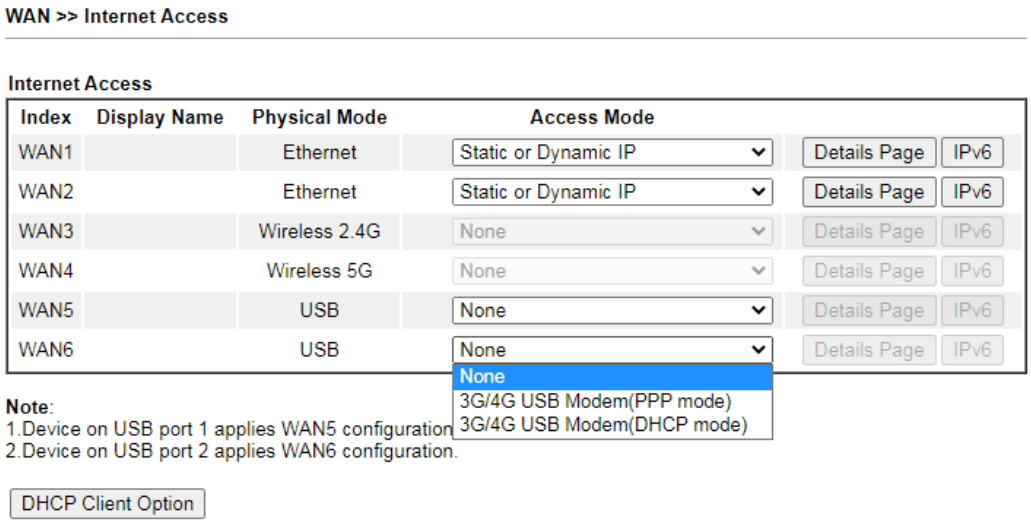
Modo de acceso para Ethernet,



Modo de acceso para Wireless 2.4G/5G,

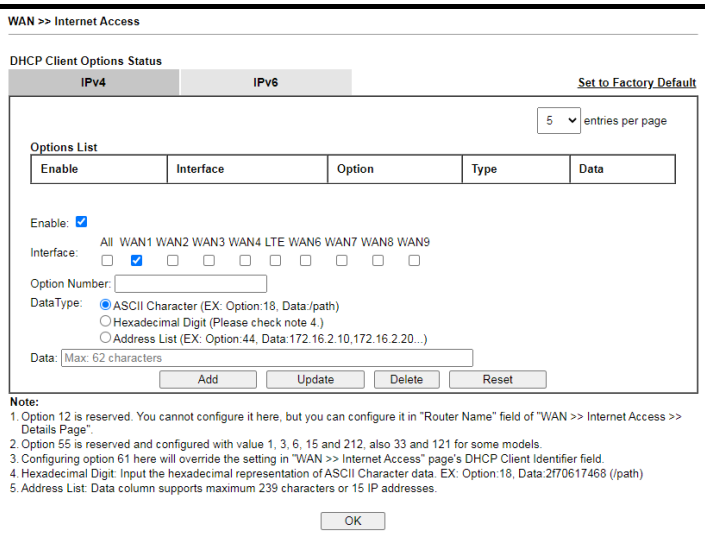


Modo de acceso para USB,



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Índice	Muestra la interfaz WAN.
Nombre para mostrar	Muestra el nombre de la WAN1/WAN2/WAN3/WAN4/WAN5 o LTE/ WAN6 que ingresó en configuración general.
Modo físico	Muestra la conexión física para las interfaces WAN de acuerdo con la conexión de red real.
Modo de acceso	Utilice la lista desplegable para elegir un modo de acceso adecuado. Aparecerá la página de detalles de ese modo. De lo contrario, haga clic en Página de detalles para acceder a la página y configurar los ajustes.
Página de detalles	Este botón abrirá una página web diferente (basada en IPv4) según el modo de acceso que elija en la interfaz WAN. Tenga en cuenta que**Página de detalles**e cambiará ligeramente según el modo físico especificado en**WAN>>Configuración general**.
IPv6	Este botón abrirá una página web diferente (basada en el modo físico) para configurar el modo de acceso a Internet IPv6 para la interfaz WAN.
Opción de cliente DHCP	Este botón le permite configurar las opciones del cliente DHCP. Los paquetes DHCP se pueden procesar agregando el número de opción y la información de datos cuando dicha función está habilitada y configurada.



Habilitar deshabilitar–Habilita/deshabilita la función de la opción DHCP. Cada opción DHCP está compuesta por un número de opción con datos. Por ejemplo,

Número de opción: 100

Datos: abcd

Cuando dicha función está habilitada, los valores especificados para la opción DHCP se verán en los paquetes de respuesta de DHCP.

Interfaz–Especifique las interfaces WAN que se sobrescribirán con dicha función. WAN7 ~ WAN9 se puede ubicar debajo **WAN>>Multi-PVC/VLAN**.

Número de opción–Escriba un número para dicha función.

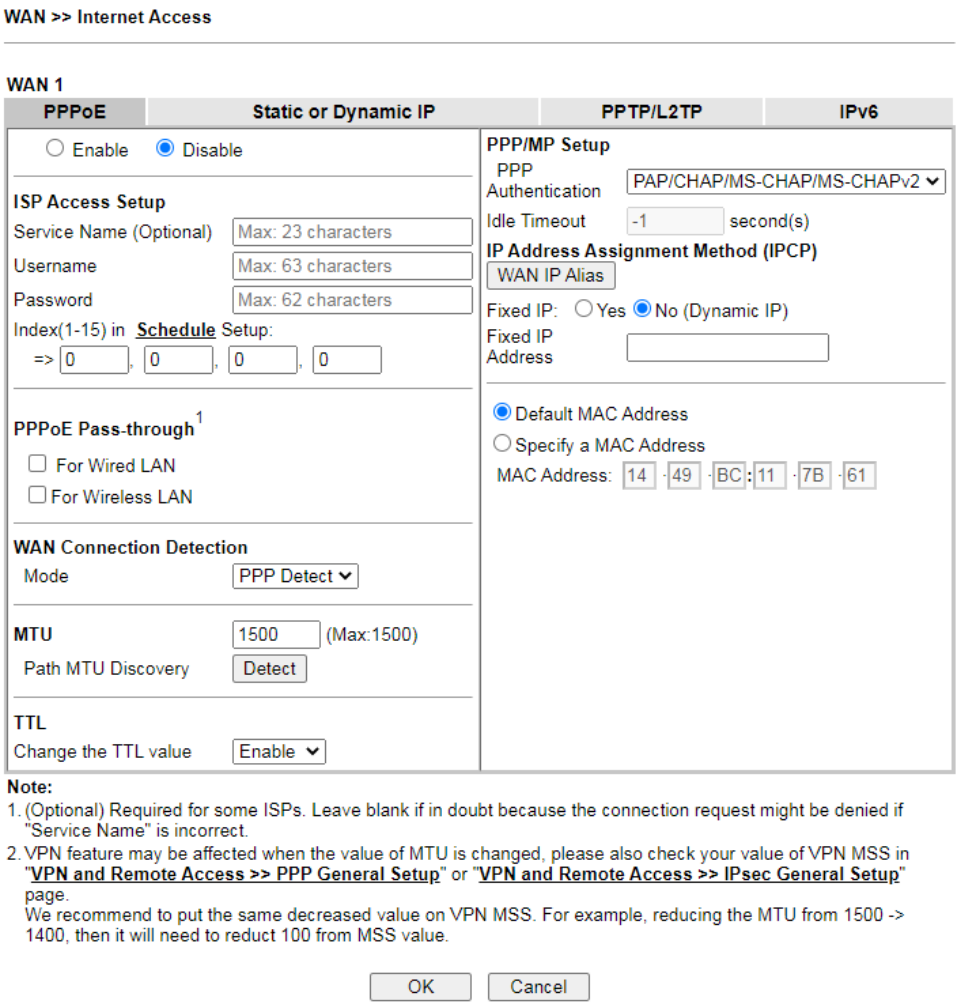
Tipo de datos–Elija el tipo (ASCII o hexadecimal) de los datos que se almacenarán.

Datos–Ingrese el contenido de los datos a ser procesados por la función de la opción DHCP.

Información

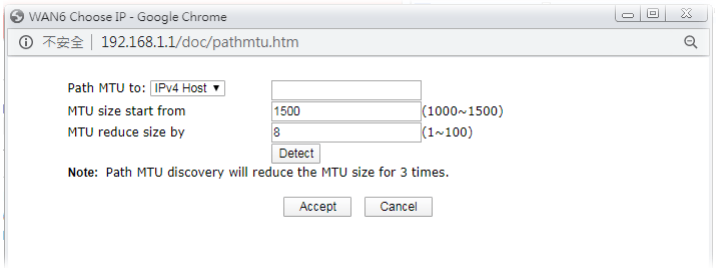
Si elige configurar la opción 61 aquí, se sobrescribirán las configuraciones detalladas en WAN>>Acceso a la interfaz.

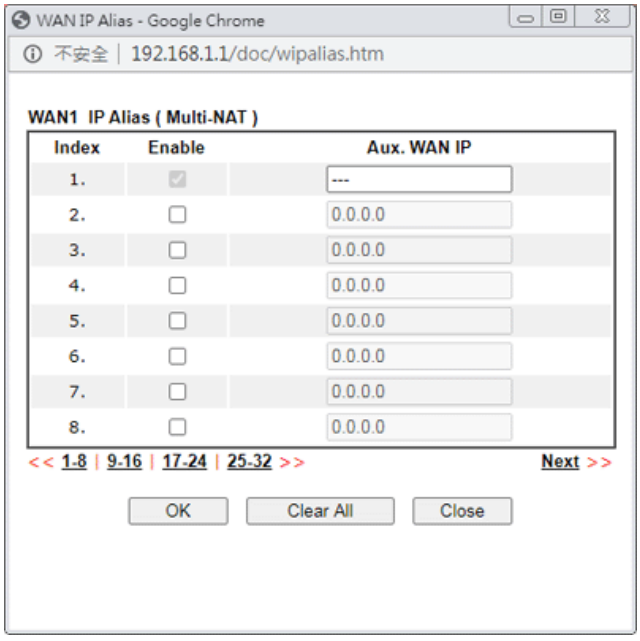
Para elegir PPPoE como protocolo de acceso a Internet, seleccione**PPPoE**desde el **WAN>>** **Acceso a Internet >>WAN1/2**página. Se mostrará la siguiente página web.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar deshabilitar	Hacer clic**Permitir**para activar esta función. si haces clic**Desactivar**, esta función se cerrará y todas las configuraciones que ajustó en esta página no serán válidas.
Configuración de acceso ISP	Ingrese su nombre de usuario, contraseña y parámetros de autenticación asignados de acuerdo con la información proporcionada por su ISP. **Nombre del servicio (opcional)**-Introduzca la descripción del servicio de red específico. **Nombre de usuario**–Introduzca el nombre de usuario proporcionado por el ISP en este campo. La longitud máxima del nombre de usuario que puede establecer es de 63 caracteres. **Contraseña**–Introduzca la contraseña proporcionada por el ISP en este campo. La longitud máxima de la contraseña que puede establecer es de 62 caracteres. **Índice (1-15) en Configuración de programación -**Puede ingresar cuatro conjuntos de horarios para su solicitud. Todos los horarios se pueden configurar previamente en**Aplicaciones >> Horario**pagina web y tu

	puede utilizar el número que ha establecido en esa página web.
Transferencia PPPoE	El enrutador ofrece conexión de acceso telefónico PPPoE. Además, también puede establecer la conexión PPPoE directamente desde los clientes locales a su ISP a través del enrutador Vigor. Cuando se selecciona el protocolo PPPoA, el paquete PPPoE transmitido por la PC se transformará en un paquete PPPoA y se enviará al servidor WAN. Por lo tanto, la PC puede acceder a Internet a través de dicha dirección. **Para LAN cableada**–Si marca esta casilla, las PC en la misma red pueden usar otro conjunto de sesiones PPPoE (diferente con la PC host) para acceder a Internet. **Para LAN inalámbrica**–esta disponible para*norte*modelo. Si marca esta casilla, las PC en la misma red inalámbrica pueden usar otro conjunto de sesiones PPPoE (diferente con la PC host) para acceder a Internet. **Nota:**Para tener transferencia PPPoA, elija el protocolo PPPoA y marque las casillas aquí. El enrutador se comportará como un módem que solo atiende al cliente PPPoE en la LAN. Es decir, el enrutador ofrecerá conexión de acceso telefónico PPPoA.
Conexión WAN **Detección**	Esta función le permite verificar si la conexión de red está activa o no a través de PPP Detect o Ping Detect. **Modo**–Elegir**Detección de PPP**o**Detección de ping**para que el sistema se ejecute para la detección de WAN. Si elige Ping Detect como el modo de detección, debe escribir la configuración requerida para los siguientes elementos. - **IP de ping primaria/secundaria**–Si tu eliges**Detección de ping** como modo de detección, debe escribir la dirección IP principal o secundaria en este campo para hacer ping. **Hacer ping a la IP de la puerta de enlace**–Si - tu eliges**Detección de ping**como modo de detección, también puede habilitar esta configuración para usar la dirección IP de la puerta de enlace WAN actual para hacer ping. - Con el ping de la(s) dirección(es) IP, el enrutador Vigor puede verificar si la conexión WAN está activada o desactivada. - **TTL (tiempo de vida)**–Establezca el valor TTL de la operación - PING. **Intervalo de ping –**Ingrese el intervalo para que el sistema ejecute la operación PING. - **Reintentar ping –**Ingrese el número de veces que el sistema puede ejecutar la operación PING antes de que se juzgue la desconexión de WAN.
MTU	Significa Unidad de transmisión máxima por paquete. **Detección de MTU de ruta**–Se utiliza para detectar el tamaño máximo de MTU de un paquete que no se segmentará en una ruta de transmisión específica. Hacer clic**Detectar**para abrir el siguiente diálogo.  - **Ruta MTU a**–Ingrese la dirección IP como la ruta de transmisión específica. - **El tamaño de MTU comienza desde**–Determine el valor del punto de partida del paquete. La configuración predeterminada es 1500. - **MTU reduce el tamaño en**–Determina el tamaño decreciente

	del valor de MTU. Por ejemplo, el número especificado en este campo es "8". El tamaño máximo de MTU es "1500". Después de hacer clic en el botón "detectar", el sistema calculará y obtendrá automáticamente el valor de MTU adecuado, como 1500, 1492, 1484, etc. - **Detectar**–Haga clic para detectar un valor de MTU adecuado - **Aceptar**–Después de hacer clic en él, el valor detectado se mostrará en el campo de MTU.
TTL	**Cambiar el valor TTL –**Habilite o deshabilite el TTL (Tiempo de vida) para un paquete transmitido a través del enrutador Vigor. - **Permitir**-El valor TTL se reducirá (-1) cuando pase a través del enrutador Vigor. Hará que el cliente, accediendo a Internet a través del enrutador Vigor, sea bloqueado por cierto ISP cuando el valor TTL sea "0". - **Desactivar**–El valor TTL no se reducirá. Entonces, cuando un paquete pasa a través del enrutador Vigor, no se cancelará. Es decir, el ISP no bloqueará al cliente que envía el paquete.
Configuración PPP/MP	**Autenticación PPP**–Seleccionar**Papanicolaou solo**o**PAP/CHAP/ MS-CHAP/MS-CHAPv2**para PPP. **Tiempo de inactividad**–Establezca el tiempo de espera para romper Internet después de pasar el tiempo sin ninguna acción. **Método de asignación de dirección IP (IPCP)-**Por lo general, el ISP le asigna dinámicamente una dirección IP cada vez que se conecta y solicita. En algunos casos, su ISP brinda servicio para asignarle siempre la misma dirección IP cuando lo solicite. En este caso, puede completar esta dirección IP en el campo IP fija. Póngase en contacto con su ISP antes de querer utilizar esta función. **Alias de IP de WAN**-Si tiene varias direcciones IP públicas y desea utilizarlas en la interfaz WAN, utilice el alias de IP de WAN. Puede configurar hasta 32 direcciones IP públicas distintas de la actual que está utilizando. Ingrese la dirección IP WAN adicional y marque la casilla Habilitar. Luego haga clic**DE ACUERDO**para salir del diálogo.  **Dirección IP fija**–Introduzca una dirección IP fija. **Dirección MAC predeterminada**–Ingrese la dirección MAC para el enrutador. Tú

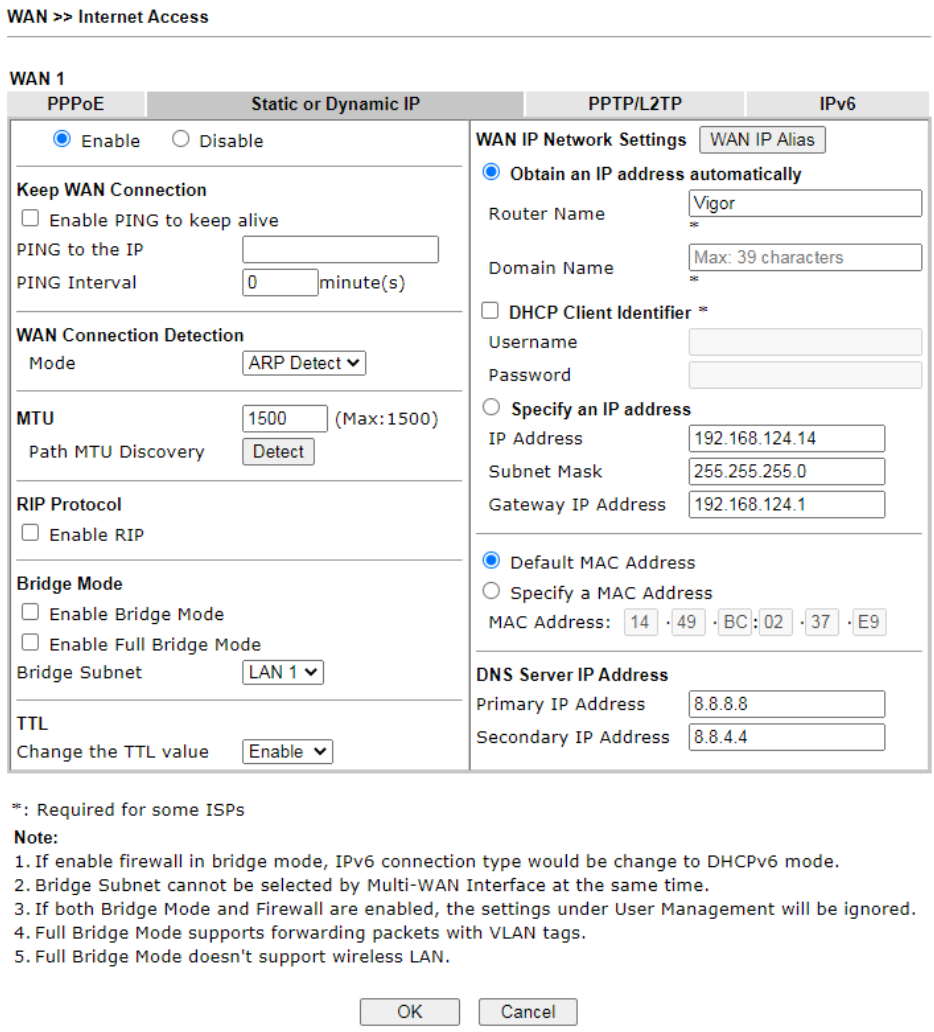
	puedo usar**Dirección MAC predeterminada**o especifique otra dirección MAC para su necesidad. **Especifique una dirección MAC**–Ingrese la dirección MAC para el enrutador manualmente.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para activarlos.

II-1-2-2 Página de detalles para IP estática o dinámica en WAN1/WAN2 (modo físico: Ethernet)

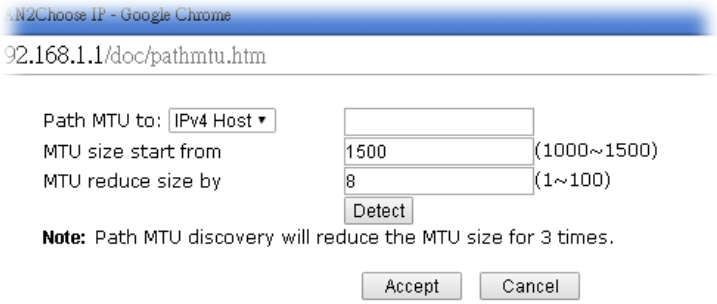
Para el modo de IP estática, generalmente recibe una dirección IP pública fija o una subred pública, es decir, varias direcciones IP públicas de sus proveedores de servicios de DSL o ISP por cable. En la mayoría de los casos, un proveedor de servicios de cable ofrecerá una IP pública fija, mientras que un proveedor de servicios de DSL ofrecerá una subred pública. Si tiene una subred pública, puede asignar una dirección IP o varias direcciones IP a la interfaz WAN.

Usar**IP estática o dinámica**como protocolo de acceso a Internet, haga clic en el**IP estática o dinámica**pestaña. Se mostrará la siguiente página web.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar deshabilitar	Hacer clic**Permitir**para activar esta función. si haces clic**Desactivar**, esta función se cerrará y todas las configuraciones que ajustó en esta página no serán válidas.

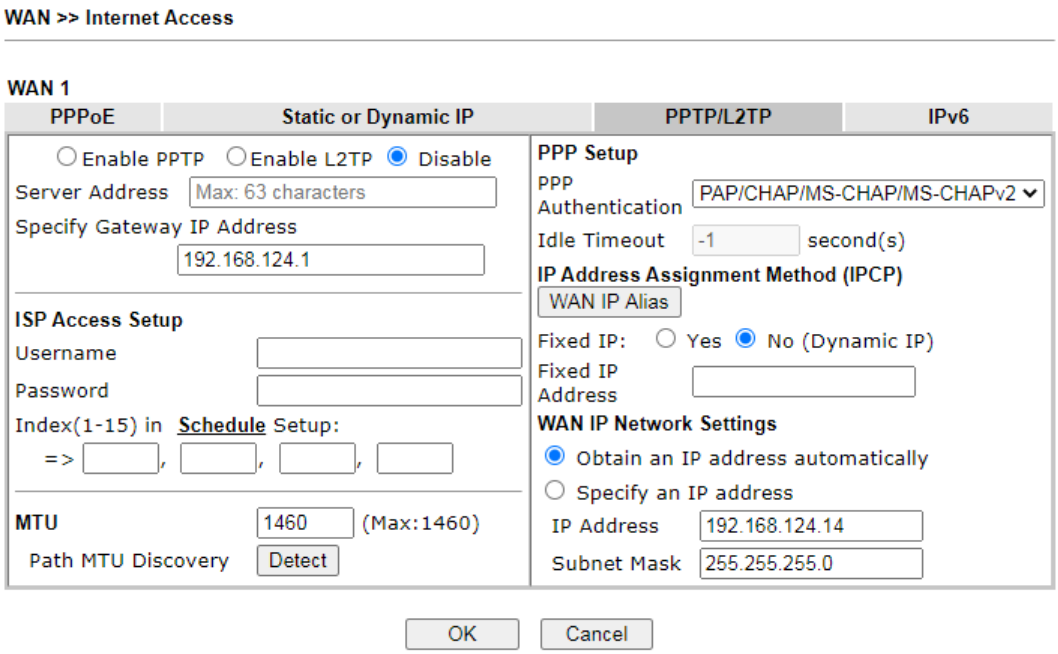
Mantener conexión WAN	Normalmente, esta función está diseñada para entornos de IP dinámica porque algunos ISP dejarán de conectarse si no hay tráfico dentro de ciertos períodos de tiempo. Controlar **Habilitar PING para mantener vivo**casilla para activar esta función. **PING a la IP**-Si habilita la función PING, especifique la dirección IP para que el sistema haga PING para mantenerlo vivo. **Intervalo de PING**-Ingrese el intervalo para que el sistema ejecute la operación PING.
Conexión WAN **Detección**	Esta función le permite verificar si la conexión de red está activa o no a través de ARP Detect o Ping Detect. **Modo**–Elegir**Detección ARP, detección de ping**o**siempre encendido**para que el sistema se ejecute para la detección de WAN. Si elige Ping Detect como el modo de detección, debe escribir la configuración requerida para los siguientes elementos. - **IP de ping primaria/secundaria**–Si tu eliges**Detección de ping** como modo de detección, debe escribir la dirección IP principal o secundaria en este campo para hacer ping. **Hacer ping a la IP de la puerta de enlace**–Si - tu eliges**Detección de ping**como modo de detección, también puede habilitar esta configuración para usar la dirección IP de la puerta de enlace WAN actual para hacer ping. Con el ping de la(s) dirección(es) IP, el enrutador Vigor puede verificar si la conexión WAN está activada o desactivada. - **TTL (tiempo de vida)**–Establezca el valor TTL de la operación - PING. **Intervalo de ping –**Ingrese el intervalo para que el sistema ejecute la operación PING. - **Reintentar ping –**Ingrese el número de veces que el sistema puede ejecutar la operación PING antes de que se juzgue la desconexión de WAN.
MTU	Significa Unidad de transmisión máxima por paquete. **Detección de MTU de ruta**–Se utiliza para detectar el tamaño máximo de MTU de un paquete que no se segmentará en una ruta de transmisión específica. Hacer clic**Detectar**para abrir el siguiente diálogo.  - **Ruta MTU a**–Ingrese la dirección IP como la ruta de transmisión específica. - **El tamaño de MTU comienza desde**–Determine el valor del punto de partida del paquete. La configuración predeterminada es 1500. - **MTU reduce el tamaño en**–Determina el tamaño decreciente del valor de MTU. Por ejemplo, el número especificado en este campo es "8". El tamaño máximo de MTU es "1500". Después de hacer clic en el botón "detectar", el sistema calculará y obtendrá automáticamente el valor de MTU adecuado, como 1500, 1492, 1484, etc.

	- **Detectar**–Haga clic para detectar un valor de MTU adecuado - **Aceptar**–Después de hacer clic en él, el valor detectado se mostrará en el campo de MTU.
Protocolo RIP	El protocolo de información de enrutamiento se abrevia como RIP(RFC1058) especificando cómo los enrutadores intercambian información de tablas de enrutamiento. Hacer clic**Habilitar RIP**para activar esta función.
Modo Puente	**Habilitar el modo de puente completo**–Si la función está habilitada, el enrutador funcionará como un módem puente que puede reenviar paquetes entrantes con etiquetas VLAN. **Habilitar modo puente**-Si la función está habilitada, el enrutador funcionará como un módem puente. Sin embargo, los paquetes entrantes con etiquetas VLAN se descartarán. **habilitar firewall**–Está disponible cuando el modo Bridge está habilitado. Cuando las casillas de verificación Modo puente y Cortafuegos están activadas, se ignorarán los ajustes configurados (perfiles de usuario) en Administración de usuarios. Y se activarán todas las reglas de filtro definidas y habilitadas en el menú Firewall. **Subred de puente**–Haga un puente entre la subred LAN seleccionada y dicha interfaz WAN.
TTL	**Cambiar el valor TTL –**Habilite o deshabilite el TTL (Tiempo de vida) para un paquete transmitido a través del enrutador Vigor. - **Si está habilitado**-El valor TTL se reducirá (-1) cuando pase a través del enrutador Vigor. Hará que el cliente, accediendo a Internet a través del enrutador Vigor, sea bloqueado por cierto ISP cuando el valor TTL sea "0". - **Si está deshabilitado**–El valor TTL no se reducirá. Entonces, cuando un paquete pasa a través del enrutador Vigor, no se cancelará. Es decir, el ISP no bloqueará al cliente que envía el paquete.
Configuración de red IP WAN	Este grupo le permite obtener una dirección IP automáticamente y le permite ingresar la dirección IP manualmente. **Alias de IP de WAN**-Si tiene varias direcciones IP públicas y desea utilizarlas en la interfaz WAN, utilice el alias de IP de WAN. Puede configurar hasta 32 direcciones IP públicas distintas de la actual que está utilizando. **Obten una direccion IP automaticamente**–Haga clic en este botón para obtener la dirección IP automáticamente si desea utilizar **IP dinámica**modo. - **Nombre del enrutador**: Ingrese el nombre del enrutador proporcionado por el ISP. - **Nombre de dominio**: Introduzca el nombre de dominio que ha asignado. **Identificador de cliente DHCP:**Marque la casilla para especificar el nombre de usuario y la contraseña como identificador de cliente DHCP para algún ISP. - **Nombre de usuario:**Escriba un nombre como nombre de usuario. La longitud máxima del nombre de usuario que puede configurar es de 63 caracteres. - **Contraseña:**Teclea una contraseña. La longitud máxima de la contraseña que puede establecer es de 62 caracteres. **Especifique una dirección IP**–Haga clic en este botón de radio para especificar algunos datos si desea utilizar**IP estática**modo. - **Dirección IP**: Introduzca la dirección IP. **Máscara de subred**: Introduzca la - máscara de subred. **Dirección IP de la puerta de enlace**: Introduzca la dirección - IP de la puerta de enlace. **Dirección MAC predeterminada**: Haga clic en este botón de opción para usar el valor predeterminado.

	Dirección MAC del enrutador. **Especifique una dirección MAC**: algunos proveedores de servicios de cable especifican una dirección MAC específica para la autenticación de acceso. En tales casos, debe hacer clic en el**Especifique una dirección MAC**e ingrese la dirección MAC en el campo Dirección MAC.
Dirección IP del servidor DNS	Ingrese la dirección IP principal para el enrutador si desea usar **IP estática**modo. Si es necesario, ingrese la dirección IP secundaria por si fuera necesario en el futuro.

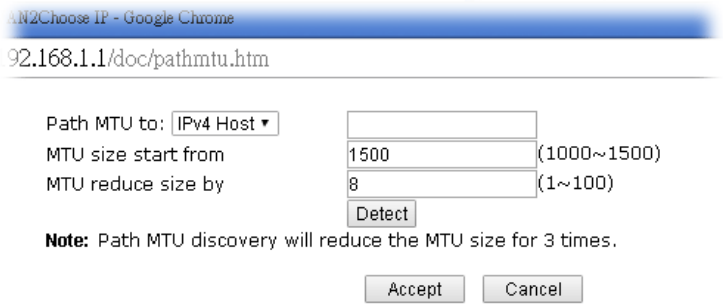
Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para activarlos.

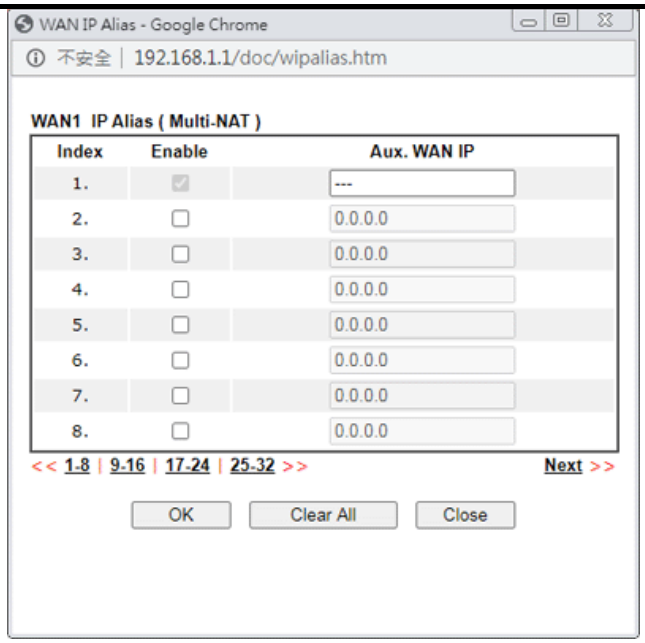
Usar**PPTP/L2TP**como protocolo de acceso a Internet, haga clic en el**PPTP/L2TP**pestaña. Se mostrará la siguiente página web.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
PPTP/L2TP	**Habilitar PPTP**-Haga clic en este botón de radio para permitir que un cliente PPTP establezca un túnel a un módem DSL en la interfaz WAN. **Habilitar L2TP**-Haga clic en este botón de radio para permitir que un cliente L2TP establezca un túnel a un módem DSL en la interfaz WAN. **Desactivar**–Haga clic en este botón de radio para cerrar la conexión a través de PPTP o L2TP. **Dirección del servidor**-Especifique la dirección IP del servidor PPTP/ L2TP si habilita el modo de cliente PPTP/L2TP. **Especifique la dirección IP de la puerta de enlace**–Especifique la dirección IP de la puerta de enlace para el servidor DHCP.
Configuración de acceso ISP	**Nombre de usuario**-Introduzca el nombre de usuario proporcionado por el ISP en este campo. La longitud máxima del nombre de usuario que puede establecer es de 63 caracteres. **Contraseña**-Introduzca la contraseña proporcionada por el ISP en este campo. La longitud máxima de la contraseña que puede establecer es de 62 caracteres. **Índice (1-15) en Configuración de programación -**Puede ingresar cuatro conjuntos de horarios para su solicitud. Todos los horarios se pueden configurar previamente en**Aplicaciones >> Horario**página web y puede utilizar el número que ha establecido en esa página web.
MTU	Significa Unidad de transmisión máxima por paquete. **Detección de MTU de ruta**–Se utiliza para detectar el tamaño máximo de MTU de un paquete que no se segmentará en una ruta de transmisión específica. Hacer clic**Detectar**para abrir el siguiente diálogo.

	 - **Ruta MTU a**–Ingrese la dirección IP como la ruta de transmisión específica. - **El tamaño de MTU comienza desde**–Determine el valor del punto de partida del paquete. La configuración predeterminada es 1500. - **MTU reduce el tamaño en**– Determina el tamaño decreciente del valor de MTU. Por ejemplo, el número especificado en este campo es "8". El tamaño máximo de MTU es "1500". Después de hacer clic en el botón "detectar", el sistema calculará y obtendrá automáticamente el valor de MTU adecuado, como 1500, 1492, 1484, etc. - **Detectar**–Haga clic para detectar un valor de MTU adecuado - **Aceptar**–Después de hacer clic en él, el valor detectado se mostrará en el campo de MTU.
Configuración PPP/MP	**Autenticación PPP**–Seleccionar**Papanicolaou solo**o**PAP/CHAP/ MS-CHAP/MS-CHAPv2**para PPP. **Tiempo de inactividad**–Establezca el tiempo de espera para romper Internet después de pasar el tiempo sin ninguna acción. **Método de asignación de dirección IP (IPCP)-**Por lo general, el ISP le asigna dinámicamente una dirección IP cada vez que se conecta y solicita. En algunos casos, su ISP brinda servicio para asignarle siempre la misma dirección IP cuando lo solicite. En este caso, puede completar esta dirección IP en el campo IP fija. Póngase en contacto con su ISP antes de querer utilizar esta función. **Alias de IP de WAN**-Si tiene varias direcciones IP públicas y desea utilizarlas en la interfaz WAN, utilice el alias de IP de WAN. Puede configurar hasta 32 direcciones IP públicas distintas de la actual que está utilizando. Ingrese la dirección IP WAN adicional y marque la casilla Habilitar. Luego haga clic**DE ACUERDO**para salir del diálogo.

	 **Dirección IP fija**–Introduzca una dirección IP fija.
Configuración de red IP WAN	**Obten una direccion IP automaticamente**–Haga clic en este botón para obtener la dirección IP automáticamente. **Especifique una dirección IP**–Haga clic en este botón de opción para especificar algunos datos. - **Dirección IP**–Introduzca la dirección IP. **Máscara de** - **subred**–Introduzca la máscara de subred.

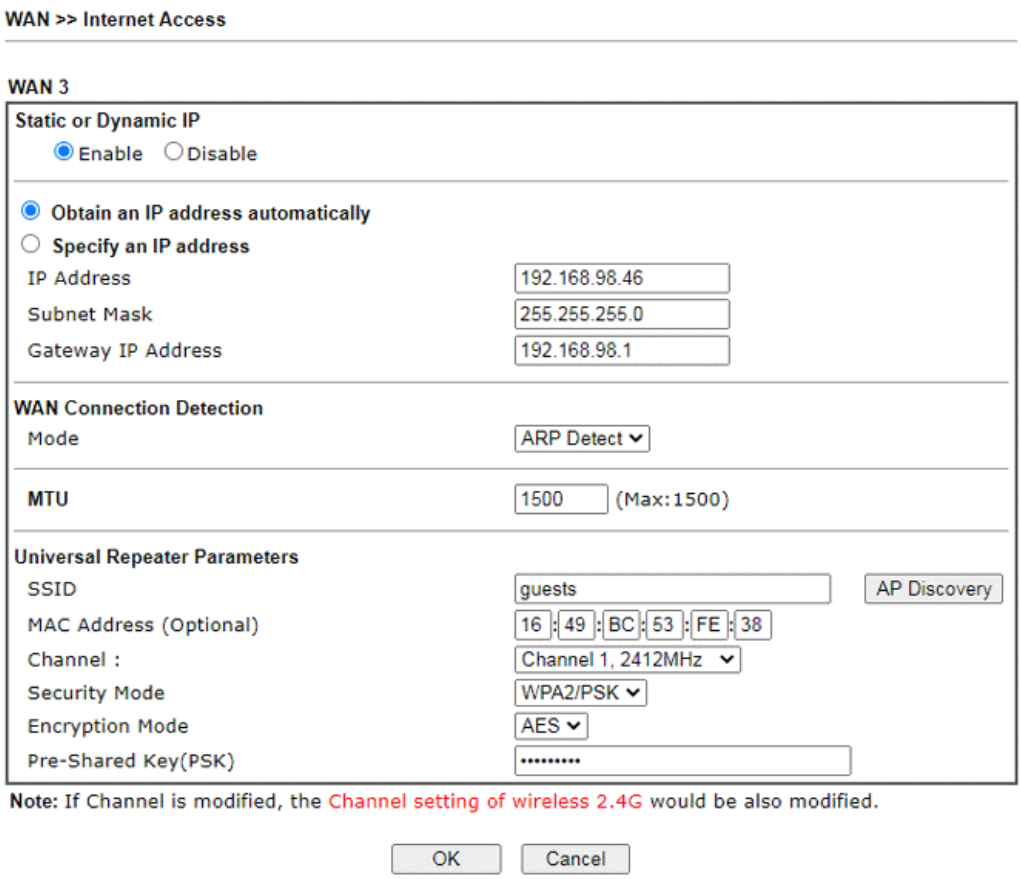
Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para activarlos.

II-1-2-4 Página de detalles para WAN3/WAN4 (Modo físico: Inalámbrico 2.4G/ Inalámbrico 5G)

Cuando se selecciona Inalámbrico 2.4G como Modo físico, la WAN utiliza el modo de estación inalámbrica para acceder a Internet. El enrutador actúa como una estación inalámbrica de 2,4 GHz y se conecta al punto de acceso inalámbrico específico.

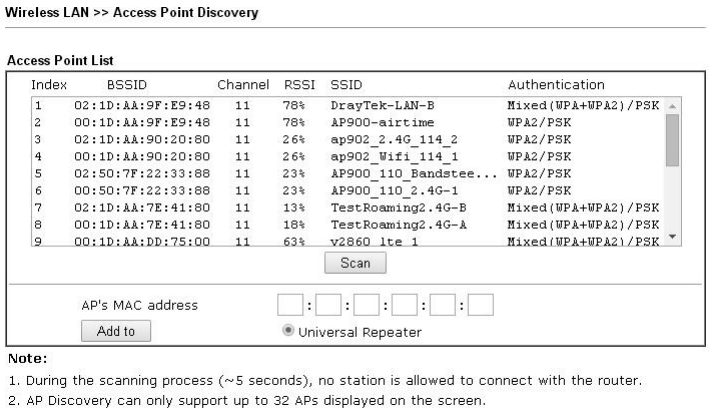
Información	WAN3/WAN4 (WAN inalámbrica) no está disponible para el modelo "ax".

Abierto**WAN>>Acceso a Internet>>WAN3/4**página. Se mostrará la siguiente página web.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar deshabilitar	Hacer clic**Permitir**para activar esta función. si haces clic**Desactivar**, esta función se cerrará y todas las configuraciones que ajustó en esta página no serán válidas.
Obten una direccion IP automaticamente	Haga clic en este botón de radio para obtener la dirección IP automáticamente si desea utilizar**IP dinámica**modo.
Especifique una dirección IP	Haga clic en este botón de opción para especificar los datos del domo si desea utilizar**IP estática**modo. **dirección IP**-Introduzca la dirección IP. **Máscara de subred**-Introduzca la máscara de subred. **Dirección IP de la puerta de enlace**-Introduzca la dirección IP de la puerta de enlace.
Conexión WAN Detección	Esta función le permite verificar si la conexión de red está activa o no a través de ARP Detect o Ping Detect.

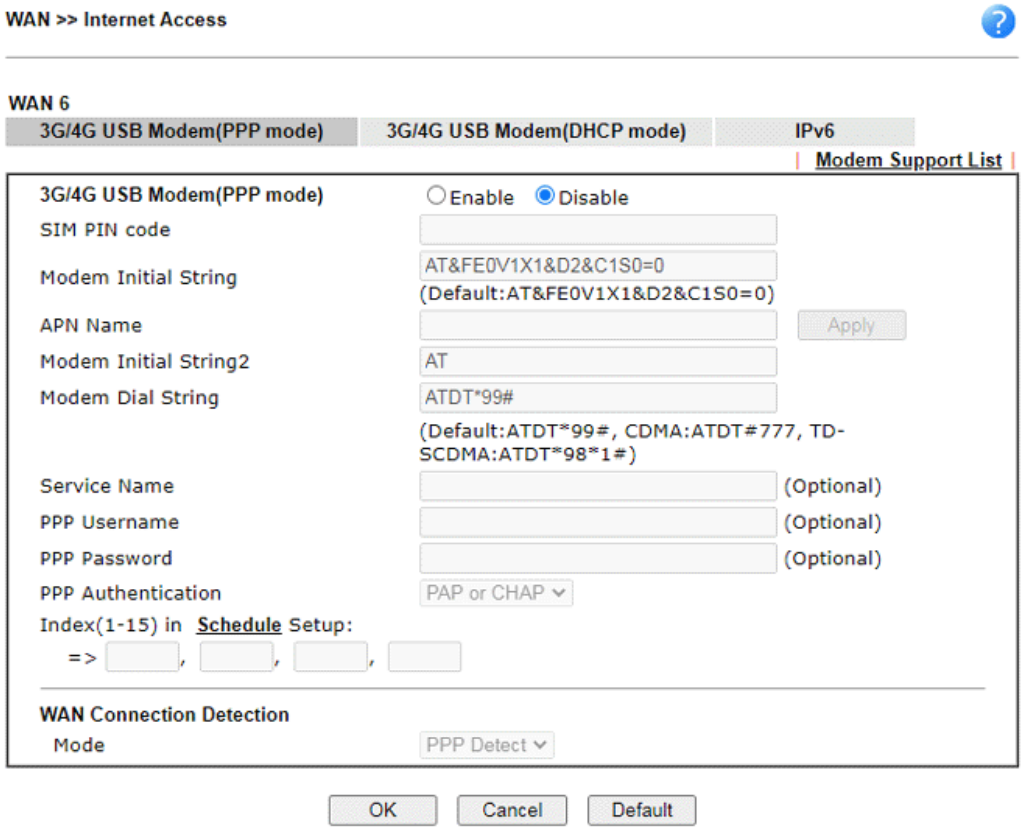
	Modo–Elegir**Detección ARP, detección de ping**o**siempre encendido**para que el sistema se ejecute para la detección de WAN. Si elige Ping Detect como el modo de detección, debe escribir la configuración requerida para los siguientes elementos. -**IP de ping**–Si tu eliges**Detección de ping**como modo de detección, también puede habilitar esta configuración para usar la dirección IP de la puerta de enlace WAN actual para hacer ping. Con el ping de la(s) dirección(es) IP, el enrutador Vigor puede verificar si la conexión WAN está activada o desactivada. -**TTL (tiempo de vida)**–Establezca el valor TTL de la operación PING.
MTU	Significa Unidad de transmisión máxima por paquete.
Repetidor universal Parámetros	**Descubrimiento de puntos de acceso**-Haga clic en este botón para abrir la ventana de detección de puntos de acceso. Deje que la tecnología inalámbrica de 2,4 GHz descubra AP y elija el AP inalámbrico al que desea conectarse.  Wireless LAN >> Access Point Discovery Access Point List Index BSSID Channel RSSI SSID Authentication 1 02:1D:AA:9F:E9:48 11 78% DrayTek-LAN-B Mixed(WPA+WPA2)/PSK 2 00:1D:AA:9F:E9:48 11 78% AP900-airtime WPA2/PSK 3 02:1D:AA:90:20:80 11 26% ap902_2.4G_114_2 WPA2/PSK 4 00:1D:AA:90:20:80 11 26% ap902_Wifi_114_1 WPA2/PSK 5 02:50:7F:22:33:88 11 23% AP900_110_Bandstee... WPA2/PSK 6 00:50:7F:22:33:88 11 23% AP900_110_2.4G-1 WPA2/PSK 7 02:1D:AA:7E:41:80 11 13% TestRoaming2.4G-B Mixed(WPA+WPA2)/PSK 8 00:1D:AA:7E:41:80 11 18% TestRoaming2.4G-A Mixed(WPA+WPA2)/PSK 9 00:1D:AA:DD:75:00 11 63% v2860_lte_1 Mixed(WPA+WPA2)/PSK Scan AP's MAC address Add to Universal Repeater Note: 1. During the scanning process (~5 seconds), no station is allowed to connect with the router. 2. AP Discovery can only support up to 32 APs displayed on the screen. **SSID**-La identificación del AP inalámbrico. **Dirección MAC (Opcional)-**La dirección MAC del punto de acceso inalámbrico. **Canal**-El canal de frecuencia del Wireless AP. **modo de seguridad**-El modo para conectarse al punto de acceso inalámbrico. - **Desactivar**–El enrutador se conecta al punto de acceso inalámbrico sin ningún mecanismo de encriptación. - **WEP**–El enrutador se conecta al punto de acceso inalámbrico como un cliente WEP y la clave de cifrado debe ingresarse en Clave WEP. - **64 bits**-Para la clave WEP de 64 bits, 5 caracteres ASCII, como 12345 (o 10 dígitos hexadecimales que empiezan por 0x, como 0x4142434445). - **128 bits**-Para la clave WEP de 128 bits, 13 caracteres ASCII, como ABCDEFGHIJKLM (o 26 dígitos hexadecimales que comienzan con 0x, como 0x41424344454647484 94A4B4C4D). - **Claves WEP**–Aquí se pueden ingresar cuatro claves, pero solo se puede seleccionar una clave a la vez. Las claves se pueden ingresar en ASCII o Hexadecimal. Marque la clave que desea utilizar. - **PSK WPA**–El enrutador se conecta al punto de acceso inalámbrico como un cliente WPA y la clave de cifrado debe ingresarse en PSK. - **WPA2/PSK**–El enrutador se conecta al punto de acceso inalámbrico como un cliente WPA2 y la clave de cifrado debe ingresarse en PSK. - **Modo de encriptación**-WPA/PSK utiliza TKIP como

	Modo de encriptación. WPA2/PSK utiliza AES como modo de cifrado. - **Clave precompartida (PSK)**–El PSK. De 8 a 63 caracteres ASCII, como 012345678... (o 64 dígitos hexadecimales que empiezan por 0x, como "0x321253abcde...").

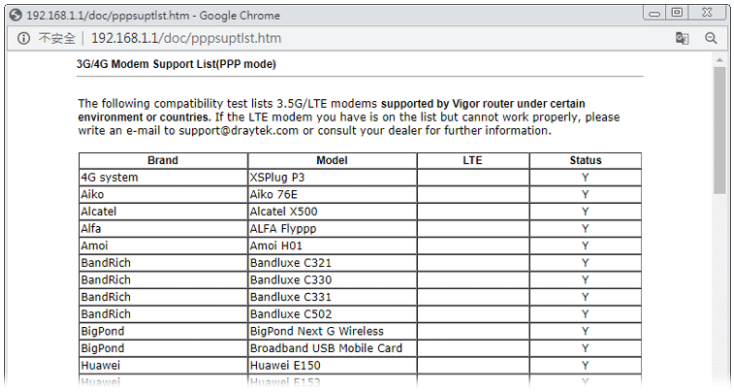
Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para activarlos.

II-1-2-5 Página de detalles para módem USB 3G/4G (modo PPP) en WAN5 / WAN6

Usar**Módem USB 3G/4G (modo PPP)**como protocolo de acceso a Internet, elija**Acceso a Internet**de**PÁLIDO**menú. Luego, seleccione**Módem USB 3G/4G (modo PPP)**para WAN5/WAN6. Se mostrará la siguiente página web.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Lista de soporte de módem	Enumera todos los módems compatibles con dicho enrutador. 
Módem USB 3G/4G (PPP	Hacer clic**Permitir**para activar esta función. si haces clic**Desactivar**,

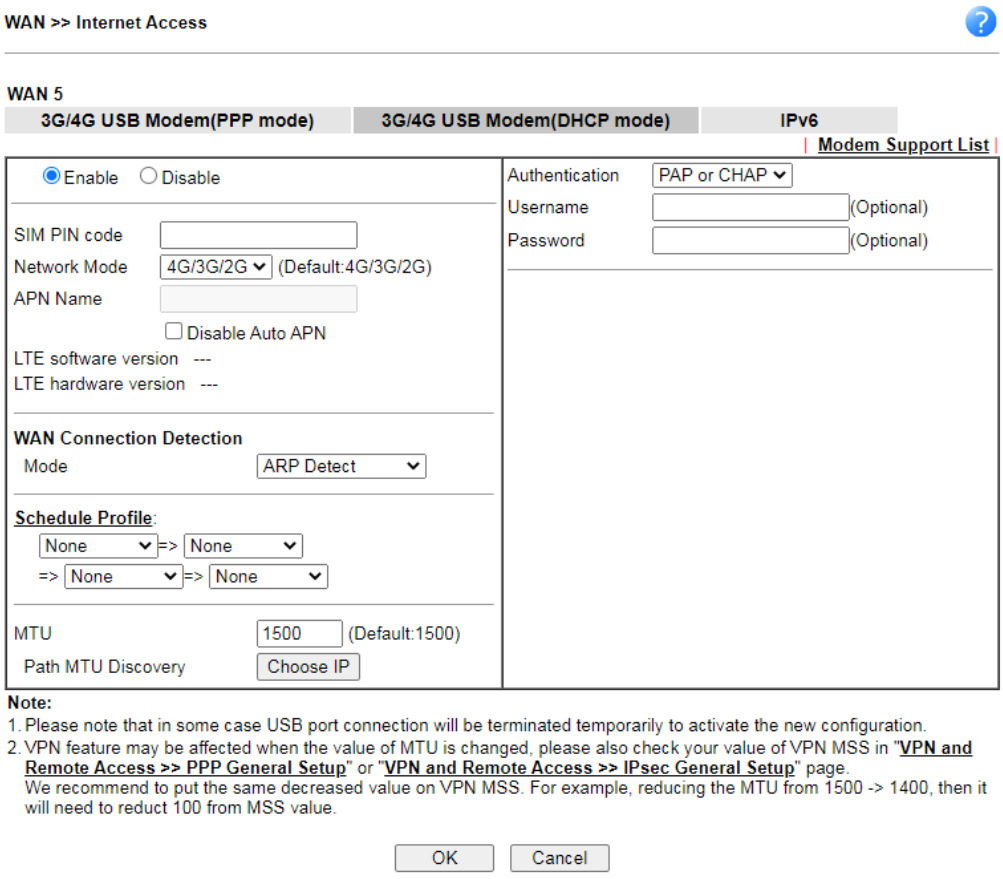
modo)	esta función se cerrará y todas las configuraciones que ajustó en esta página no serán válidas.
Código PIN de la tarjeta SIM	Escriba el código PIN de la tarjeta SIM que se utilizará para acceder a Internet. La longitud máxima del código PIN que puede establecer es de 15 caracteres.
Cadena inicial del módem	Dicho valor se utiliza para inicializar el módem USB. Utilice el valor predeterminado. Si tiene alguna pregunta, póngase en contacto con su ISP. La longitud máxima de la cadena que puede establecer es de 47 caracteres.
Nombre de APN	APN significa Nombre de punto de acceso proporcionado y requerido por algunos ISP. Introduzca el nombre y haga clic**Aplicar**. La longitud máxima del nombre que puede establecer es de 43 caracteres.
Cadena inicial del módem2	La cadena inicial 1 se comparte con APN. En algunos casos, el usuario puede necesitar otro comando AT inicial para restringir la banda 3G o realizar alguna configuración especial. La longitud máxima de la cadena que puede establecer es de 47 caracteres.
Cadena de marcación del módem	Dicho valor se utiliza para marcar a través del modo USB. Utilice el valor predeterminado. Si tiene alguna pregunta, póngase en contacto con su ISP. La longitud máxima de la cadena que puede establecer es de 31 caracteres.
Nombre del Servicio	Introduzca la descripción del servicio de red específico.
Nombre de usuario PPP	Ingrese el nombre de usuario de PPP (opcional). La longitud máxima del nombre que puede establecer es de 63 caracteres.
Contraseña PPP	Introduzca la contraseña de PPP (opcional). La longitud máxima de la contraseña que puede establecer es de 62 caracteres.
Autenticación PPP	Seleccionar**Papanicolaou solo**o**PAP o CHAP**para PPP.
Índice (1-15) en Configuración de programación	Configure la LAN inalámbrica para que funcione solo en determinados intervalos de tiempo. Puede elegir hasta 4 horarios de los 15 horarios predefinidos en**Aplicaciones >> Horario**configuración. La configuración predeterminada de este campo está en blanco y la función siempre funcionará.
Conexión WAN **Detección**	Esta función le permite verificar si la conexión de red está activa o no a través de PPP Detect o Ping Detect. **Modo**–Elegir**Detección de PPP**o**Detección de ping**para que el sistema se ejecute para la detección de WAN. Si elige Ping Detect como el modo de detección, debe escribir la configuración requerida para los siguientes elementos. -**IP de ping primaria/secundaria**–Si tu eliges**Detección de ping**como modo de detección, debe escribir la dirección IP principal o secundaria en este campo para hacer ping. -**Hacer ping a la IP de la puerta de enlace**–Si tu eliges**Detección de ping**como modo de detección, también puede habilitar esta configuración para usar la dirección IP de la puerta de enlace WAN actual para hacer ping. Con el ping de la(s) dirección(es) IP, el enrutador Vigor puede verificar si la conexión WAN está activada o desactivada. -**TTL (tiempo de vida)**–Establezca el valor TTL de la operación PING.

	-**Intervalo de ping –**Ingrese el intervalo para que el sistema ejecute la operación PING. -**Reintentar ping –**Ingrese el número de veces que el sistema puede ejecutar la operación PING antes de que se juzgue la desconexión de WAN.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para activarlos.

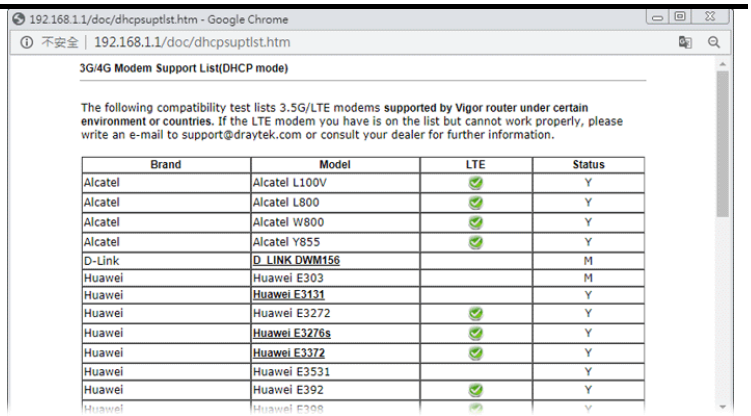
II-1-2-6 Página de detalles para módem USB 3G/4G (modo DHCP) en WAN5 / WAN6

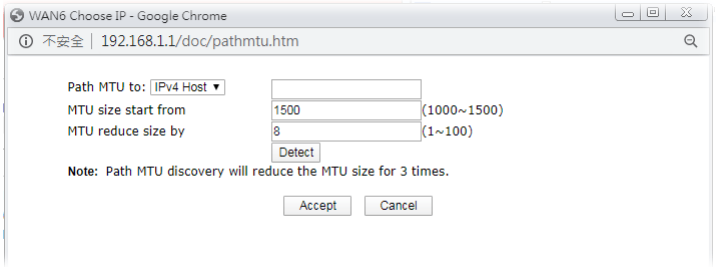
Usar**Módem USB 3G/4G (modo DHCP)**como protocolo de acceso a Internet, elija**Acceso a Internet**de**PÁLIDO**menú. Luego, seleccione**Módem USB 3G/4G (modo DHCP)**para WAN5/WAN6. Se mostrará la siguiente página web.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Lista de soporte de módem	Enumera todos los módems compatibles con dicho enrutador.

	
Habilitar deshabilitar	Hacer clic**Permitir**para activar esta función. si haces clic**Desactivar**, esta función se cerrará y todas las configuraciones que ajustó en esta página no serán válidas.
Código PIN de la tarjeta SIM	Escriba el código PIN de la tarjeta SIM que se utilizará para acceder a Internet. La longitud máxima del código PIN que puede configurar es de 19 caracteres.
Modo de red	Obligue al enrutador Vigor a conectarse a Internet con el modo especificado aquí. Si elige 4G/3G/2G como modo de red, el enrutador elegirá automáticamente uno adecuado de acuerdo con la señal inalámbrica real.
Nombre de APN	APN significa Nombre de punto de acceso proporcionado y requerido por algunos ISP. Introduzca el nombre y haga clic**Aplicar.** La longitud máxima del nombre que puede establecer es de 47 caracteres. **Desactivar APN automático**-De forma predeterminada, el sistema de enrutador Vigor proporcionará automáticamente el nombre de APN (a través de la lista de perfiles de APN preconfigurada). Para especificar un nombre de APN, marque esta casilla e ingrese el nombre de APN manualmente en el campo Nombre de APN.
Conexión WAN **Detección**	Esta función le permite verificar si la conexión de red está activa o no a través de ARP Detect, Strict ARP Detect o Ping Detect. **Modo**–Elegir**Detección ARP, Detección ARP estricta**o**Detección de ping** para que el sistema se ejecute para la detección de WAN. Si elige Ping Detect como el modo de detección, debe escribir la configuración requerida para los siguientes elementos. -**IP de ping primaria/secundaria**–Si tu eliges**Detección de ping**como modo de detección, debe escribir la dirección IP principal o secundaria en este campo para hacer ping. -**Hacer ping a la IP de la puerta de enlace**–Si tu eliges**Detección de ping**como modo de detección, también puede habilitar esta configuración para usar la dirección IP de la puerta de enlace WAN actual para hacer ping. Con el ping de la(s) dirección(es) IP, el enrutador Vigor puede verificar si la conexión WAN está activada o desactivada. -**TTL (tiempo de vida)**–Establezca el valor TTL de la operación PING. -**Intervalo de ping –**Ingrese el intervalo para que el sistema ejecute la operación PING. -**Reintentar ping –**Ingrese el número de veces que el sistema puede ejecutar la operación PING antes de que se juzgue la desconexión de WAN.

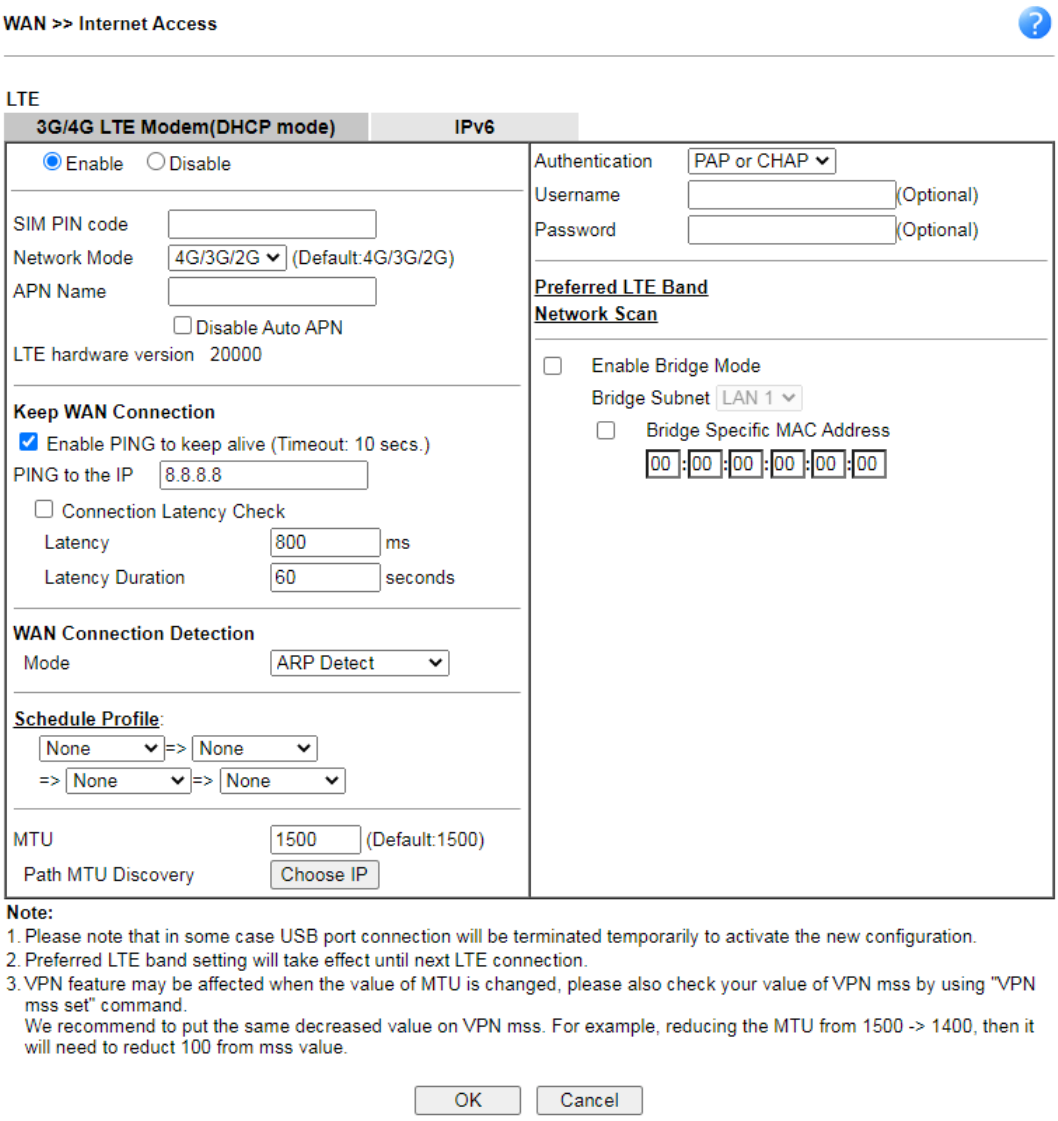
Programar perfiles	Configure la LAN inalámbrica para que funcione solo en determinados intervalos de tiempo. Puede elegir hasta 4 horarios de los 15 horarios predefinidos en**Aplicaciones >> Horario**configuración. La configuración predeterminada de este campo está en blanco y la función siempre funcionará.
MTU	Significa Unidad de transmisión máxima por paquete. **Detección de MTU de ruta**–Se utiliza para detectar el tamaño máximo de MTU de un paquete que no se segmentará en una ruta de transmisión específica. Hacer clic**Elija IP**para abrir el siguiente diálogo.  - **Ruta MTU a**–Ingrese la dirección IP como la ruta de transmisión específica. - **El tamaño de MTU comienza desde**–Determine el valor del punto de partida del paquete. La configuración predeterminada es 1500. - **MTU reduce el tamaño en**– Determina el tamaño decreciente del valor de MTU. Por ejemplo, el número especificado en este campo es "8". El tamaño máximo de MTU es "1500". Después de hacer clic en el botón "detectar", el sistema calculará y obtendrá automáticamente el valor de MTU adecuado, como 1500, 1492, 1484, etc. - **Detectar**–Haga clic para detectar un valor de MTU adecuado - **Aceptar**–Después de hacer clic en él, el valor detectado se mostrará en el campo de MTU.
Autenticación	Seleccionar**Papanicolaou solo**o**PAP o CHAP**para la autenticación PPP. **Nombre de usuario**–Introduzca el nombre de usuario para la autenticación (opcional). **Contraseña**–Introduzca la contraseña para la autenticación (opcional).

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para activarlos.

II-1-2-7 Página de detalles para módem USB 3G/4G (modo DHCP) en LTE WAN

Está disponible solo para el modelo “L”. LTE WAN utiliza el módulo LTE integrado para acceder a Internet.

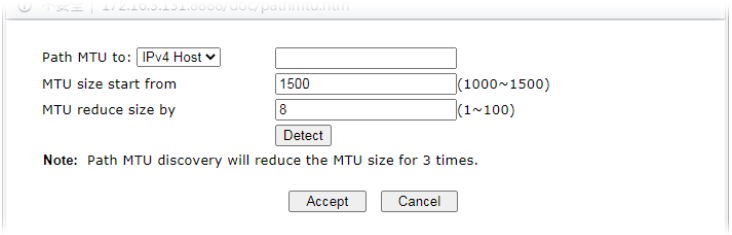
Usar**Módem USB 3G/4G (modo DHCP)**como protocolo de acceso a Internet, elija**Acceso a Internet**de**PÁLIDO**menú. Luego, seleccione**Módem USB 3G/4G (modo DHCP)**para LTE. Se mostrará la siguiente página web.

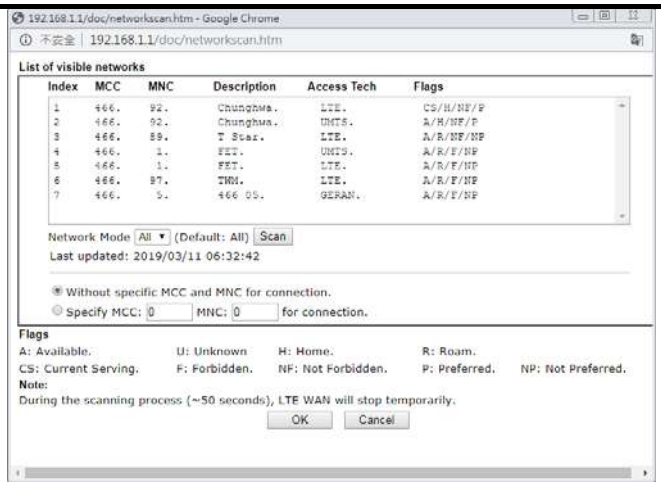


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Hacer clic**Permitir**para activar esta función. si haces clic**Desactivar**, esta función se cerrará y todas las configuraciones que ajustó en esta página no serán válidas.
Código PIN de la tarjeta SIM	Introduzca el código PIN de la tarjeta SIM que se utilizará para acceder a Internet. La longitud máxima del código PIN que puede establecer es de 15 caracteres.
Modo de red	Obligue al enrutador Vigor a conectarse a Internet con el modo especificado aquí. Si elige 4G/3G/2G como modo de red, el enrutador elegirá automáticamente uno adecuado de acuerdo con la señal inalámbrica real.

Nombre de APN	APN significa Nombre de punto de acceso proporcionado y requerido por algunos ISP. Introduzca el nombre y haga clic**Aplicar.** La longitud máxima del nombre que puede establecer es de 47 caracteres. **Desactivar APN automático**-De forma predeterminada, el sistema de enrutador Vigor proporcionará automáticamente el nombre de APN (a través de la lista de perfiles de APN preconfigurada). Para especificar un nombre de APN, marque esta casilla e ingrese el nombre de APN manualmente en el campo Nombre de APN.
Versión de hardware LTE	La versión de hardware del módulo LTE integrado.
Mantener conexión WAN	Normalmente, esta función está diseñada para entornos de IP dinámica porque algunos ISP dejarán de conectarse si no hay tráfico dentro de ciertos períodos de tiempo. Controlar **Habilitar PING para mantener vivo**casilla para activar esta función. **Habilitar PING para mantener vivo**–Si habilita la función PING, especifique una dirección IP para que el sistema haga PING para mantenerlo activo. El sistema Vigor enviará un paquete por segundo a la dirección IP especificada. Si el sistema no recibe ninguna respuesta de esa IP dentro de los 10 segundos, el sistema Vigor reiniciará el módulo LTE hasta que establezca correctamente la conexión LTE. - **PING a la IP**–Introduzca una dirección IP. **Comprobación de latencia de conexión**-Habilite la configuración del tiempo de latencia para la respuesta del paquete. Si está habilitado (marcado), el sistema Vigor esperará la respuesta del paquete desde la dirección IP especificada. Cuando el tiempo de espera de la respuesta del paquete alcanza el umbral de tiempo (definido en Latencia) y continúa durante un período de tiempo (definido en Duración de la latencia), el sistema Vigor reiniciará el módulo LTE hasta que se establezca correctamente la conexión LTE. - **Latencia**–Establezca un umbral de tiempo para la respuesta del paquete. El valor predeterminado es 800 (unidad: microsegundo). - **Duración de latencia**–Establezca un período de tiempo. El valor predeterminado es 60 (unidad: segundo).
Conexión WAN **Detección**	Esta función le permite verificar si la conexión de red está activa o no a través de ARP Detect o Ping Detect. **Modo**–Elegir**Detección ARP**o**Detección de ping**para que el sistema se ejecute para la detección de WAN. Si elige Ping Detect como el modo de detección, debe escribir la configuración requerida para los siguientes elementos. - **IP de ping primaria/secundaria**–Si tu eliges**Detección de ping** como modo de detección, debe escribir la dirección IP principal o secundaria en este campo para hacer ping. - **Hacer ping a la IP de la puerta de enlace**–Si tu eliges**Detección de ping**como modo de detección, también puede habilitar esta configuración para usar la dirección IP de la puerta de enlace WAN actual para hacer ping. - Con el ping de la(s) dirección(es) IP, el enrutador Vigor puede verificar si la conexión WAN está activada o desactivada. - **TTL (tiempo de vida)**–Establezca el valor TTL de la operación PING. - **Intervalo de ping –**Ingrese el intervalo para que el sistema ejecute la operación PING. - **Reintentar ping –**Ingrese el número de veces que el sistema puede ejecutar la operación PING antes de que se juzgue la desconexión de WAN.
Programar perfil	Configure la WAN LTE para que funcione solo en cierto intervalo de tiempo. Especifique hasta 4 entradas de horario para habilitar o deshabilitar la WAN. Todos los horarios se pueden configurar previamente en**Aplicaciones** **> > Horario**página web y puede utilizar el número que

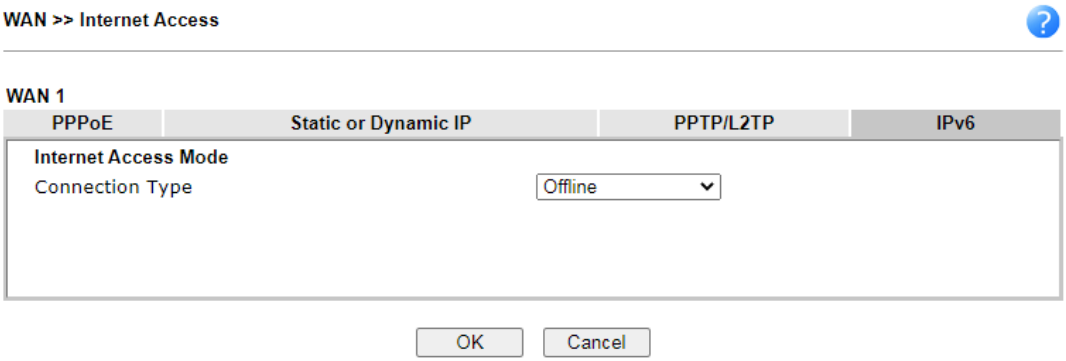
	han establecido en esa página web.
MTU	Unidad máxima de transmisión, el tamaño del paquete más grande, en bytes, que se puede transmitir a la WAN. El valor máximo es 1500. **Detección de MTU de ruta**–Utilice esta función para determinar el tamaño de MTU óptimo para la WAN. Hacer clic**Elija IP**para abrir el siguiente diálogo.  - **Ruta MTU a**–Seleccione Host/IP, para una dirección IPv4 o Host/IPv6, para una dirección IPv6 y luego ingrese la dirección IP en el cuadro de texto. - **El tamaño de MTU comienza desde**–Determine el valor del punto de partida del paquete. - **MTU reduce el tamaño en**–Número de octetos por los que disminuir la MTU de 1500 bytes. Comience con un valor 0 para reducir el tamaño y haga clic en el botón Detectar. Si se devuelve el mensaje Fail, aumente el tamaño de reducción de MTU y vuelva a intentarlo. Repita hasta que vea el mensaje Success, que indica que se ha alcanzado el tamaño de MTU óptimo. - **Detectar**–Haga clic para detectar un valor de MTU adecuado - **Aceptar**–Después de hacer clic en él, el valor detectado se mostrará en el campo de MTU.
Autenticación	El protocolo utilizado para la autenticación PPP. - **Papanicolaou solo**-Solo se utiliza PAP (Protocolo de autenticación de contraseña). - **PAP o CHAP**-Tanto PAP como CHAP (Challenge-Handshake Authentication Protocol) se pueden usar para PPP autenticación. El enrutador negocia con el servidor PPTP o L2TP para determinar qué protocolo usar. **Nombre de usuario**–Nombre de usuario proporcionado por el ISP para la autenticación (opcional). **Contraseña**–Contraseña proporcionada por el ISP para la autenticación (opcional).
Banda LTE preferida	Haga clic en el enlace para especificar la banda LTE preferida. Se abrirá un cuadro de diálogo y se enumerarán las bandas LTE disponibles compatibles con el módulo LTE para que el usuario elija para establecer la conexión de red.
Escaneo de red	Haga clic en él para buscar el ISP cercano para la conexión LTE. El siguiente cuadro de diálogo enumera los servicios ISP disponibles detectados por el enrutador Vigor.

	
Habilitar modo puente	Si la función está habilitada, el enrutador funcionará como un módem puente LTE. **Dirección MAC específica del puente**-Ingrese la dirección MAC del dispositivo (por ejemplo, una computadora, un enrutador o un enrutador WiFi) que necesita conectarse a Internet a través del módem LTE.

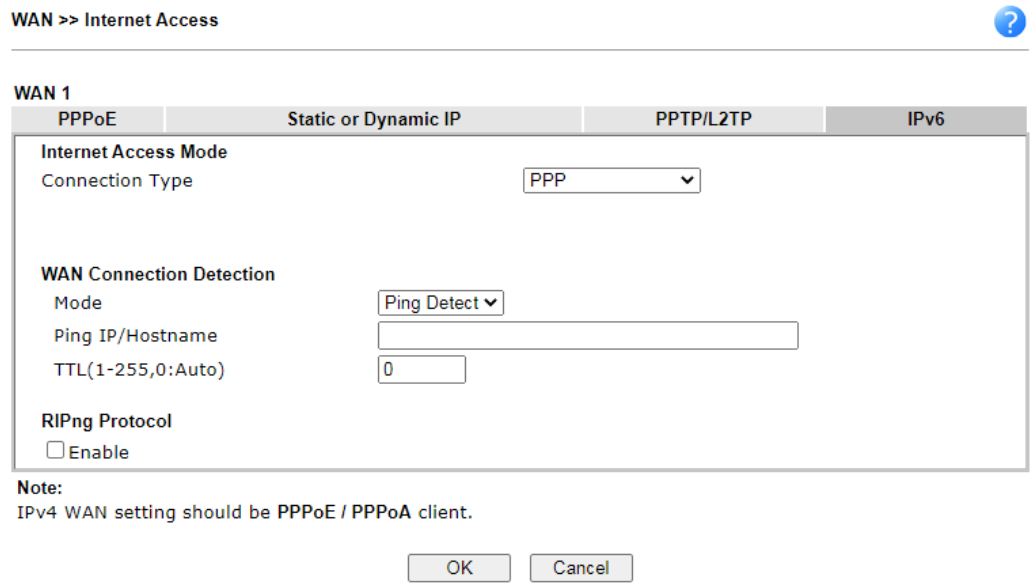
Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para activarlos.

II-1-2-8 Página de detalles para IPv6–Fuera de línea en WAN1/WAN2/WAN5/WAN6

Cuando se selecciona Fuera de línea, la conexión IPv6 se desactivará.



II-1-2-9 Página de detalles para IPv6–PPP en WAN1/WAN2



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Conexión WAN Detección	Esta función le permite verificar si la conexión de red está activa o no a través de Ping Detect. **Modo**–Elegir**siempre encendido**o**Detección de ping**para que el sistema se ejecute para la detección de WAN.**siempre encendido**significa que no se ejecutará ninguna detección. La conexión de red estará siempre activada. -**Ping IP/nombre de host**–Si tu eliges**Detección de ping**como modo de detección, debe escribir la dirección IP en este campo para hacer ping. -**TTL (tiempo de vida)**–Si tu eliges**Detección de ping**como modo de detección, debe escribir el valor TTL.
Protocolo RIPng	RIPng (RIP next generation) ofrece las mismas funciones y beneficios que IPv4 RIP v2.

A continuación se muestra un ejemplo de una conexión IPv6 exitosa basada en el modo PPP.

Información

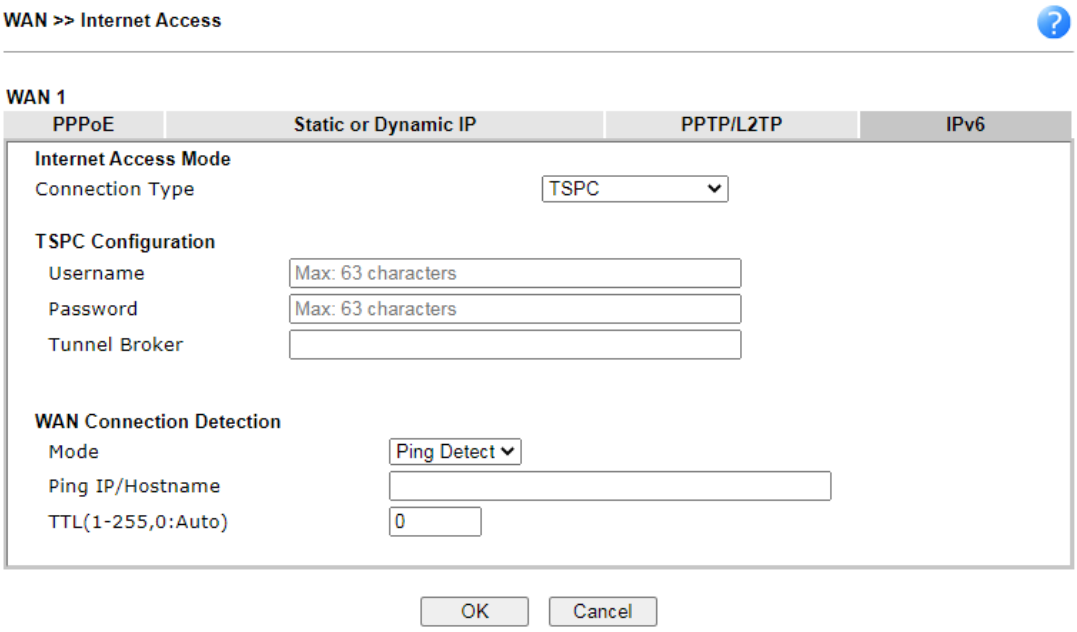
En la actualidad, el prefijo IPv6 se puede adquirir a través de la conexión en modo PPPoE que está disponible para áreas como Taiwán (hinet), los Países Bajos, Australia y el Reino Unido.

II-1-2-10 Página de detalles para IPv6–TSPC en WAN1/WAN2/WAN5/WAN6

El cliente de protocolo de configuración de túnel (TSPC) es una aplicación que podría ayudarlo a conectarse fácilmente a la red IPv6.

Asegúrese de que su conexión WAN IPv4 esté bien y aplique una cuenta gratuita de hexago (http://gogonet.gogo6.com/page/freenet6-account) antes de intentar usar TSPC para la conexión de red. TSPC se conectaría al corredor de túneles y solicitaría un túnel de acuerdo con las especificaciones dentro del archivo de configuración. Obtiene una dirección IP IPv6 pública y un prefijo IPv6 del intermediario del túnel y luego monitorea el estado del túnel en segundo plano.

Después de obtener el prefijo IPv6 e iniciar el demonio de anuncio de enrutador (RADVD), la PC detrás de este enrutador puede conectarse directamente a Internet IPv6.

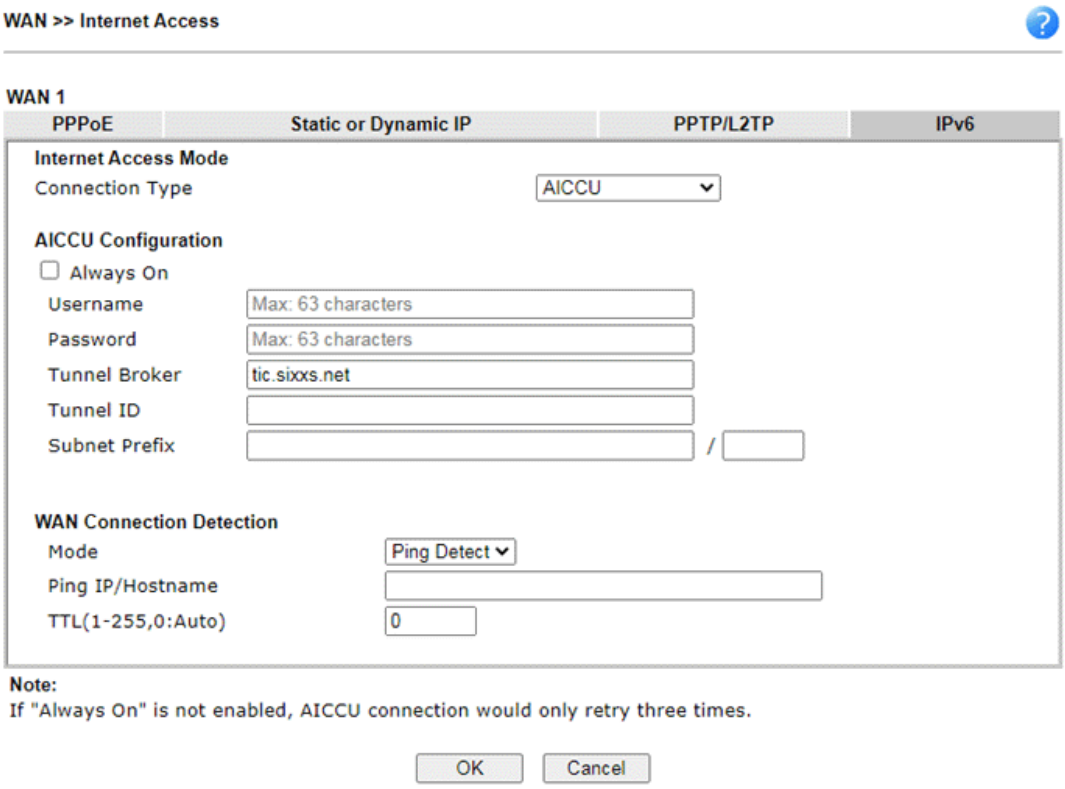


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre de usuario	Se sugiere que aplique otro nombre de usuario y contraseña para http://gogonet.gogo6.com/page/freenet6-account. La longitud máxima del nombre que puede establecer es de 63 caracteres.
Contraseña	Introduzca la contraseña asignada con el nombre de usuario. La longitud máxima del nombre que puede establecer es de 19 caracteres.
Corredor de túneles	Ingrese la dirección para la IP del agente de túnel, FQDN o un número de puerto opcional.
Conexión WAN Detección	Esta función le permite verificar si la conexión de red está activa o no a través de Ping Detect. **Modo**–Elegir**siempre encendido**o**Detección de ping**para que el sistema se ejecute para la detección de WAN.**siempre encendido**significa que no se ejecutará ninguna detección. La conexión de red estará siempre activada. -**Ping IP/nombre de host**–Si tu eliges**Detección de ping**como modo de detección, debe escribir la dirección IP en este campo para hacer ping. -**TTL (tiempo de vida)**–Si tu eliges**Detección de ping**como modo de detección, debe escribir el valor TTL.

Después de terminar la configuración anterior, haga clic en**DE ACUERDO**para guardar la configuración.

II-1-2-11 Página de detalles para IPv6–AICCU en WAN1/WAN2/WAN5/WAN6



Los ajustes disponibles se explican a continuación:

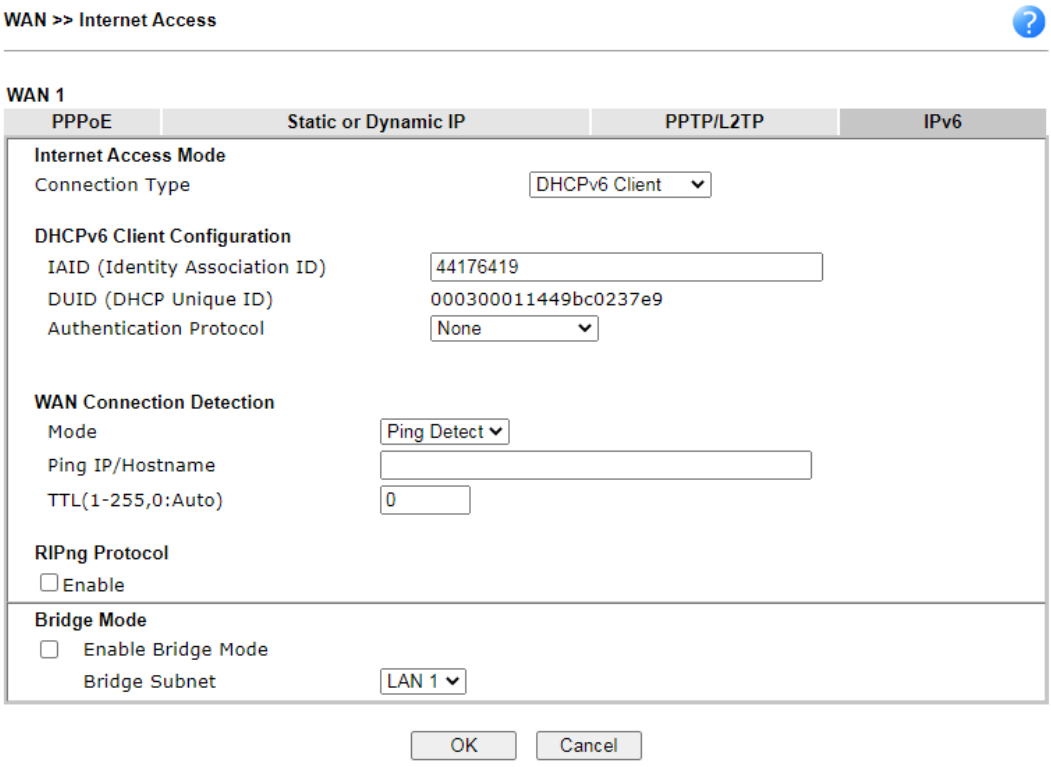
Artículo	Descripción
siempre encendido	Marque esta casilla para mantener la conexión de red siempre.
Nombre de usuario	Introduzca el nombre obtenido del corredor. Solicite una nueva cuenta en http://www.sixxs.net/. Se sugiere que aplique otro nombre de usuario y contraseña. La longitud máxima del nombre que puede establecer es de 19 caracteres.
Contraseña	Introduzca la contraseña asignada con el nombre de usuario. La longitud máxima de la contraseña que puede establecer es de 19 caracteres.
Corredor de túneles	Significa un servidor de AICCU. El servidor puede proporcionar túneles IPv6 a sitios o usuarios finales a través de IPv4. Ingrese la dirección para la IP del agente de túnel, FQDN o un número de puerto opcional.
Identificación del túnel	Una cuenta de usuario puede tener varios túneles. Y, cada túnel tendrá una ID de túnel específica (por ejemplo, T115394). Ingrese el ID ofrecido por Tunnel Broker.
Prefijo de subred	Introduzca la dirección de prefijo de subred obtenida del proveedor de servicios. La longitud máxima del prefijo que puede establecer es de 128 caracteres.
Conexión WAN Detección	Esta función le permite verificar si la conexión de red está activa o no a través de Ping Detect. **Modo**–Elegir**siempre encendido**o**Detección de ping**para que el sistema

	ejecutar para la detección de WAN. -**Ping IP/nombre de host**–Si tu eliges**Detección de ping**como modo de detección, debe escribir la dirección IP en este campo para hacer ping. -**TTL (tiempo de vida)**–Si tu eliges**Detección de ping**como modo de detección, debe escribir el valor TTL.

Después de terminar la configuración anterior, haga clic en**DE ACUERDO**para guardar la configuración.

II-1-2-12 Página de detalles para IPv6–Cliente DHCPv6 en WAN1/WAN2

El modo de cliente DHCPv6 usaría el protocolo DHCPv6 para obtener la dirección IPv6 del servidor.



Los ajustes disponibles se explican a continuación:

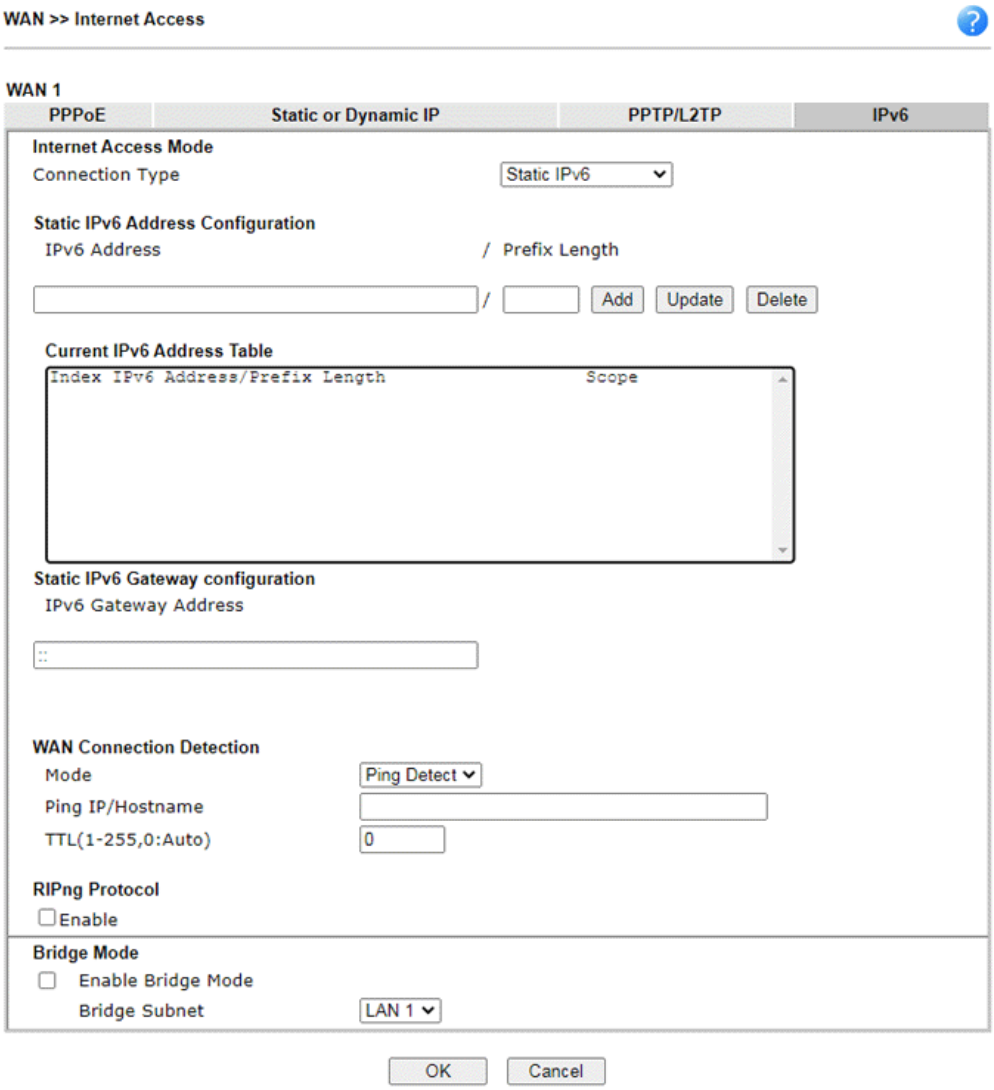
Artículo	Descripción
Cliente DHCPv6 Configuración	**AIID**-Escriba un número como IAID. **DUID**–Muestra la ID única de DHCP utilizada por dicha interfaz WAN. **Protocolo de autenticación**–Dicho protocolo se utilizará para que el cliente sea autenticado por el servidor DHCPv6 antes de acceder a Internet. Se pueden especificar tres tipos,**Reconfigurar clave**, **Demorado**y**Ninguno**. En general, la configuración predeterminada es Ninguno. -**Reconfigurar clave**–Durante el proceso de conexión, el servidor DHCPv6 autenticará al cliente automáticamente. -**Demorado**-Durante el proceso de conexión, el servidor DHCPv6 autenticará e identificará al cliente según el ID de clave, el dominio y la información secreta especificada en estos campos. **ID de clave**–Escriba un valor (rango de 1 a 65535) que

	utilizarse para generar el valor HMAC-MD5. **Reino**–El nombre (de 1 a 31 caracteres) escrito aquí identificará la clave que genera el valor HMAC-MD5. **Secreto**–Escriba un texto (de 1 a 31 caracteres) como identificador único para cada cliente en cada servidor DHCP.
Conexión WAN **Detección**	Esta función le permite verificar si la conexión de red está activa o no a través de NS Detect o Ping Detect. **Modo**–Elegir**siempre encendido**,**Detección de ping**o**Detección de NS**para que el sistema se ejecute para la detección de WAN. Con**Detección de NS** modo, el sistema verificará si la conexión de red está establecida o no, como IPv4 ARP Detect.**siempre encendido**significa que no se ejecutará ninguna detección. La conexión de red estará siempre activada. -**Ping IP/nombre de host**–Si tu eliges**Detección de ping**como modo de detección, debe escribir la dirección IP en este campo para hacer ping. -**TTL (tiempo de vida)**–Si tu eliges**Detección de ping**como modo de detección, debe escribir el valor TTL.
Protocolo RIPng	RIPng (RIP next generation) ofrece las mismas funciones y beneficios que IPv4 RIP v2.
Modo Puente	**Habilitar modo puente**-Si la función está habilitada, el enrutador funcionará como un módem puente. **habilitar firewall**–Está disponible cuando el modo Bridge está habilitado. Cuando las casillas de verificación Modo puente y Cortafuegos están activadas, se ignorarán los ajustes configurados (perfiles de usuario) en Administración de usuarios. Y se activarán todas las reglas de filtro definidas y habilitadas en el menú Firewall. **Subred de puente**–Haga un puente entre la subred LAN seleccionada y dicha interfaz WAN.

Después de terminar la configuración anterior, haga clic en**DE ACUERDO**para guardar la configuración.

II-1-2-13 Página de detalles para IPv6–IPv6 estático en WAN1/WAN2

Este tipo le permite configurar una dirección IPv6 estática para la interfaz WAN.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Dirección IPv6 estática Configuración	**Dirección IPv6 –**Ingrese la dirección IP estática IPv6. **Prefijo Longitud –** Ingrese el valor fijo para la longitud del prefijo. **Agregar -**Haga clic en él para agregar una nueva entrada. **Actualizar**-Haga clic en él para modificar una entrada existente. **Borrar -**Haga clic en él para eliminar una entrada existente.
Dirección IPv6 actual Mesa	Muestra la dirección IPv6 de la interfaz actual.
Puerta de enlace IPv6 estática Configuración	**Dirección de puerta de enlace IPv6 -**Escriba su dirección de puerta de enlace IPv6 aquí.
Conexión WAN Detección	Esta función le permite verificar si la conexión de red está activa o no a través de Ping Detect. **Modo**–Elegir**siempre encendido**o**Detección de ping**para que el sistema se ejecute para la detección de WAN.**siempre encendido**significa que no se ejecutará ninguna detección. La conexión de red estará siempre activada.

	-**Ping IP/nombre de host**–Si tu eliges**Detección de ping**como modo de detección, debe escribir la dirección IP en este campo para hacer ping. -**TTL (tiempo de vida)**–Si tu eliges**Detección de ping**como modo de detección, debe escribir el valor TTL.
Protocolo RIPng	RIPng (RIP next generation) ofrece las mismas funciones y beneficios que IPv4 RIP v2.
Modo Puente	**Habilitar modo puente**-Si la función está habilitada, el enrutador funcionará como un módem puente. **habilitar firewall**–Está disponible cuando el modo Bridge está habilitado. Cuando las casillas de verificación Modo puente y Cortafuegos están activadas, se ignorarán los ajustes configurados (perfiles de usuario) en Administración de usuarios. Y se activarán todas las reglas de filtro definidas y habilitadas en el menú Firewall. **Subred de puente**–Haga un puente entre la subred LAN seleccionada y dicha interfaz WAN.

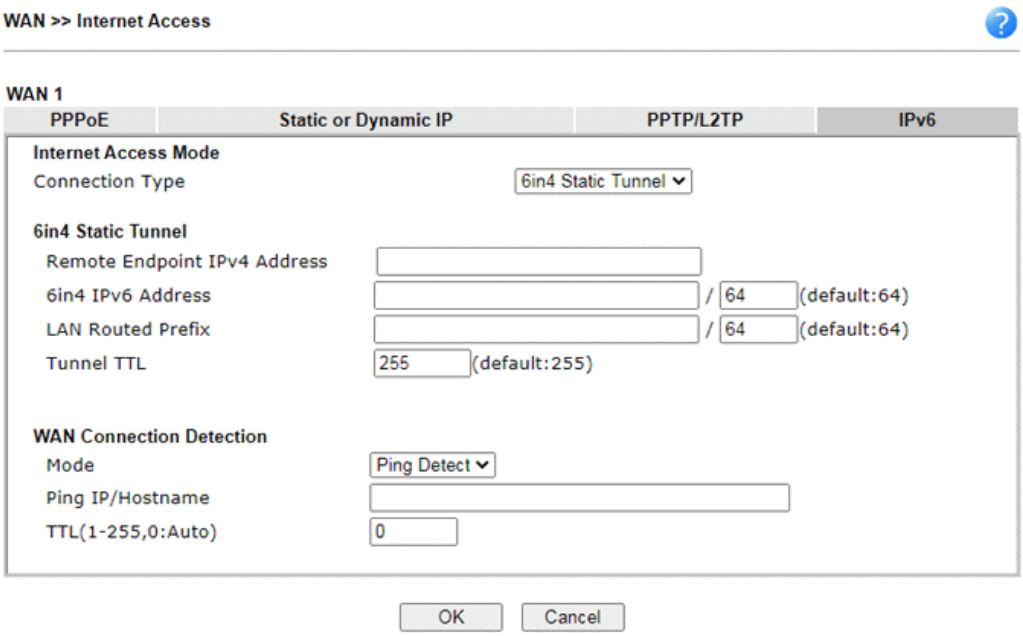
Después de terminar la configuración anterior, haga clic en**DE ACUERDO**para guardar la configuración.

II-1-2-14 Página de detalles para IPv6–Túnel estático 6in4 en WAN1/WAN2

Este tipo le permite configurar un túnel estático 6 en 4 para la interfaz WAN. Dicho modo

permite que el enrutador acceda a la red IPv6 a través de la red IPv4.

Sin embargo, 6in4 ofrece un prefijo fuera de 2002::0/16. Por lo tanto, puede usar un punto final fijo en lugar de un punto final anycast. El modo tiene más fiabilidad.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Túnel estático 6in4	**Dirección IPv4 de extremo remoto -**Ingrese la dirección IPv4 estática para el servidor remoto. **Dirección IPv6 6 en 4**-Ingrese la dirección IPv6 estática para el túnel IPv4 con el valor para la longitud del prefijo. **Prefijo enrutado LAN**-Ingrese la dirección IPv6 estática para el enrutamiento LAN con el valor para la longitud del prefijo.

	Túnel TTL-Ingrese el número para la vida útil de los datos en el túnel.
Conexión WAN **Detección**	Esta función le permite verificar si la conexión de red está activa o no a través de Ping Detect. **Modo**–Elegir**siempre encendido**o**Detección de ping**para que el sistema se ejecute para la detección de WAN.**siempre encendido**significa que no se ejecutará ninguna detección. La conexión de red estará siempre activada. -**Ping IP/nombre de host**–Si tu eliges**Detección de ping**como modo de detección, debe escribir la dirección IP en este campo para hacer ping. -**TTL (tiempo de vida)**–Si tu eliges**Detección de ping**como modo de detección, debe escribir el valor TTL.

Después de terminar la configuración anterior, haga clic en**DE ACUERDO**para guardar la configuración.

A continuación se muestra un ejemplo de una conexión IPv6 exitosa basada en el modo de túnel estático 6in4.

Online Status

Physical Connection **System Uptime: 0day 0:4:16**

IPv4	IPv6

LAN Status

IP Address

2001:4DD0:FF00:83E4:21D:AAFF:FE83:11B4/64 (Global)
FE80::21D:AAFF:FE83:11B4/64 (Link)

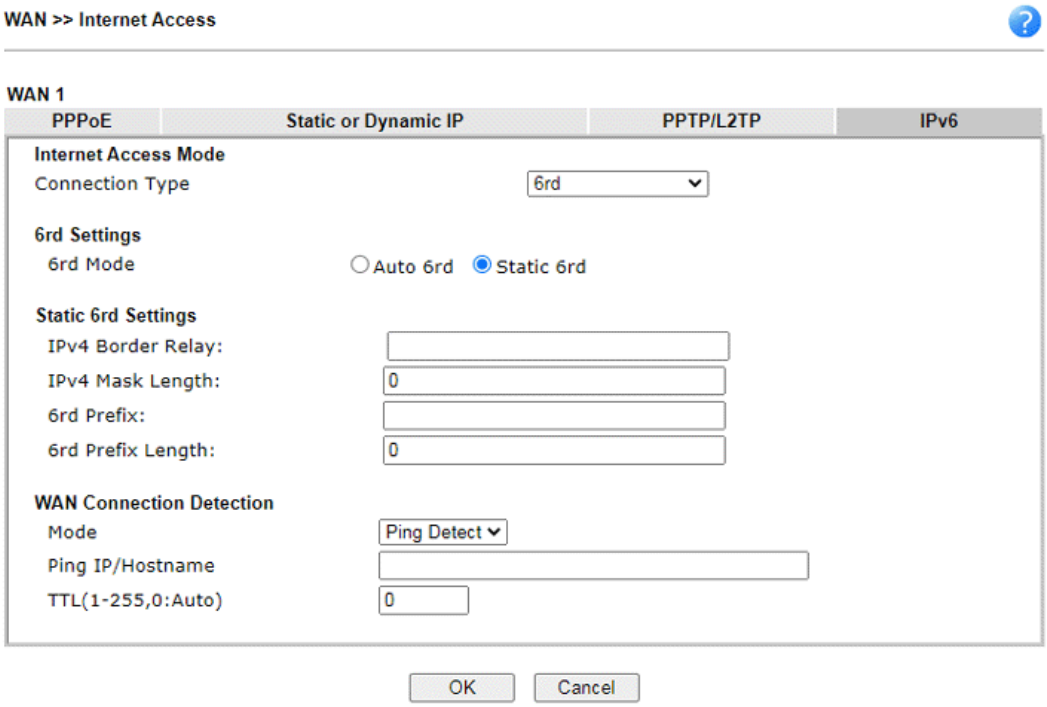
TX Packets	RX Packets	TX Bytes	RX Bytes
14	80	1244	6815

WAN1 IPv6 Status

Enable	Mode	Up Time	
Yes	6in4 Static Tunnel	0:04:07	
IP			**Gateway IP**
2001:4DD0:FF10:83E4::2131/64 (Global) FE80::C0A8:651D/128 (Link)			---
TX Packets	**RX Packets**	**TX Bytes**	**RX Bytes**
3	26	211	2302

II-1-2-15 Página de detalles para IPv6–6º en WAN1/WAN2

Este tipo le permite configurar el sexto para la interfaz WAN.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
6.º modo	**6º automático –**Recupere el sexto prefijo automáticamente del sexto proveedor de servicios. La WAN IPv4 debe configurarse como "DHCP". **6º estático -**Configure la sexta opción manualmente.
Retransmisión de borde IPv4	Ingrese las direcciones IPv4 del 6.er retransmisor de frontera para un 6.er dominio determinado.
Longitud de la máscara IPv4	Escriba una cantidad de bits de orden superior que sean idénticos en todas las direcciones IPv4 de CE dentro de un sexto dominio determinado. Puede ser cualquier valor entre 0 y 32.
6.º prefijo	Introduzca la sexta dirección IPv6.
Longitud del sexto prefijo	Ingrese la longitud del prefijo IPv6 para el sexto prefijo IPv6 en número de bits.
Conexión WAN Detección	Esta función le permite verificar si la conexión de red está activa o no a través de Ping Detect. **Modo**–Elegir**siempre encendido**o**Detección de ping**para que el sistema se ejecute para la detección de WAN.**siempre encendido**significa que no se ejecutará ninguna detección. La conexión de red estará siempre activada. -**Ping IP/nombre de host**–Si tu eliges**Detección de ping**como modo de detección, debe escribir la dirección IP en este campo para hacer ping. -**TTL (tiempo de vida)**–Si tu eliges**Detección de ping**como modo de detección, debe escribir el valor TTL.

Después de terminar la configuración anterior, haga clic en**DE ACUERDO**para guardar la configuración.

A continuación se muestra un ejemplo de una conexión IPv6 exitosa basada en el sexto modo.

Online Status

Physical Connection **System Uptime: 0day 0:9:15**

IPv4	IPv6

LAN Status

IP Address

2001:E41:A865:1D00:21D:AAFF:FE83:11B4/64 (Global)
FE80::21D:AAFF:FE83:11B4/64 (Link)

TX Packets	RX Packets	TX Bytes	RX Bytes
15	113	1354	18040

WAN1 IPv6 Status

Enable	Mode	Up Time	
Yes	6rd	0:09:06	
IP			**Gateway IP**
2001:E41:A865:1D01:21D:AAFF:FE83:11B5/128 (Global) FE80::C0A8:651D/128 (Link)			---
TX Packets	**RX Packets**	**TX Bytes**	**RX Bytes**
13	29	967	2620

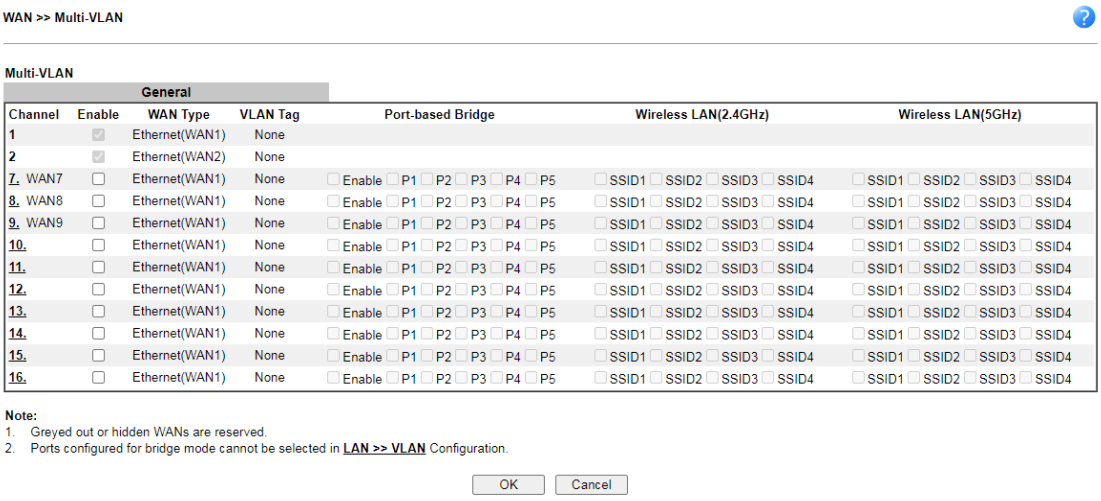
II-1-3 VLAN múltiple

Multi-VLAN permite a los usuarios crear perfiles para interfaces WAN específicas y conexiones de puente para aplicaciones de usuario que requieren un rendimiento de red muy alto. Simplemente ve a**PÁLIDO**y seleccione **VLAN múltiple**.

- Canal 1/2: Ethernet en WAN1/WAN2.
- Canal 3: Inalámbrico de 2,4 GHz en WAN3.
- Canal 4: 5 GHz inalámbrico en WAN4.
- Canal 5/6: USB1/USB2 (WAN5/WAN6).

Canales 7 a 16se puede conectar a uno o más de los 4 puertos LAN P2 a P5. Además, **Canales 7 a 9**se pueden configurar como WAN virtuales (WAN7 a WAN9).

General

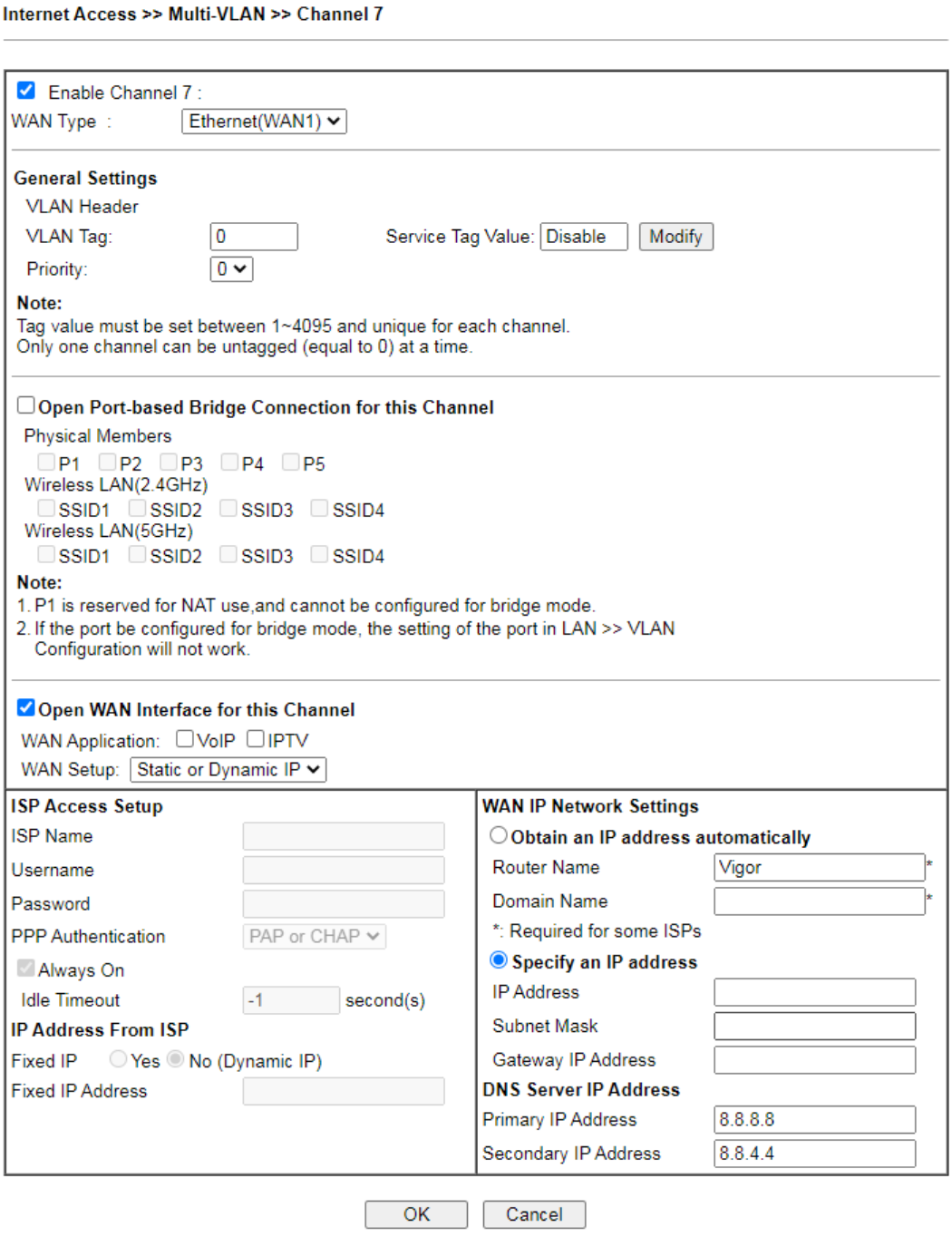


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Canal	Muestra el número de cada canal. Los canales 7 ~ 16 son configurables.
Permitir	Muestra si la configuración en este canal está habilitada (Sí) o no (No).
Tipo de WAN	Muestra el medio físico que utilizará el canal.
Etiqueta VLAN	Muestra el valor de la etiqueta VLAN que se usará para los paquetes que viajan en este canal.
Puente basado en puerto	El tráfico de red que fluye en cada canal será identificado por el sistema a través de sus etiquetas VLAN. Es posible que los canales que usan el mismo tipo de WAN no configuren el mismo valor de etiqueta de VLAN. **Permitir**-Marque esta casilla para habilitar la función de puente basada en puerto en este canal. **P1 ~ P5**–Marque la(s) casilla(s) para crear una conexión de puente en la LAN.

Para configurar un canal de PVC, haga clic en su número de canal.

Los enlaces WAN para los canales 7, 8 y 9 se proporcionan para aplicaciones basadas en enrutadores, como **TR-069**. La configuración debe aplicarse y obtenerse de su ISP. Para su solicitud especial, comuníquese con su ISP y luego haga clic en el enlace WAN de los canales 7, 8 y 9 para configurar su enrutador.



Los ajustes disponibles se explican a continuación:

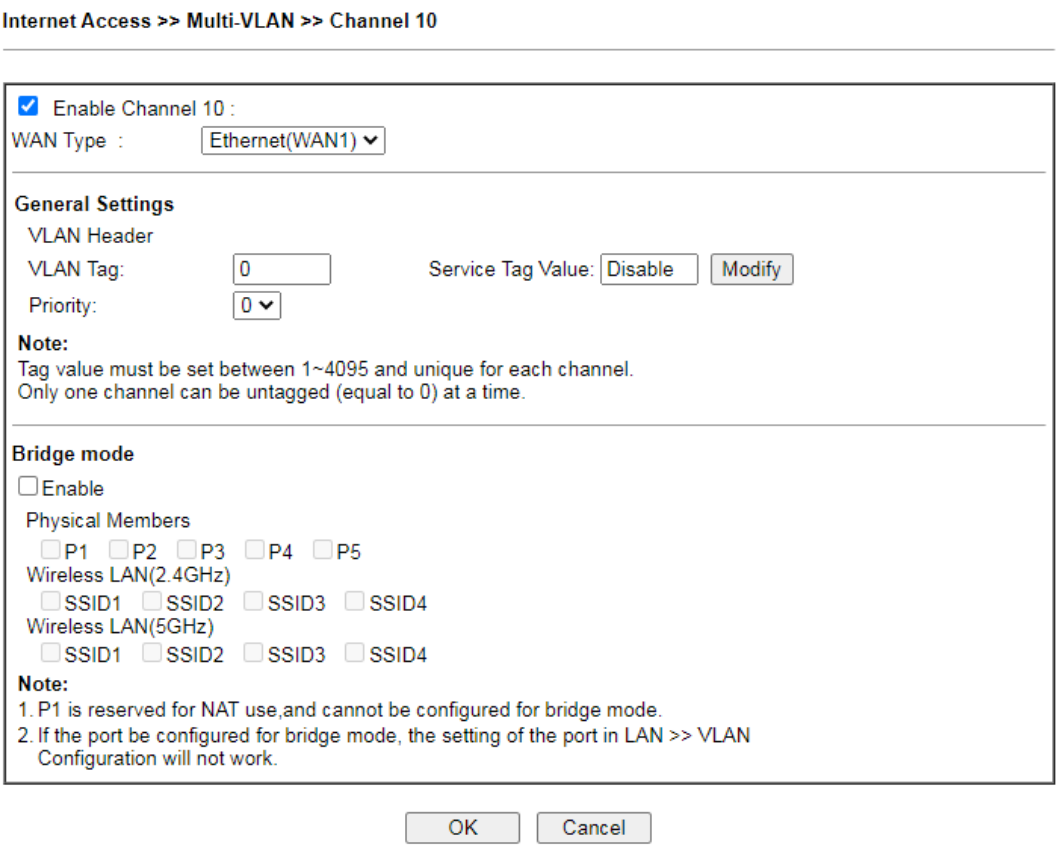
Artículo	Descripción
Habilitar canal 7/8/9	Márquelo para habilitar este canal.
Tipo de WAN	Especifique un tipo de WAN de la VLAN. **Ethernet (WAN1/2)**-Se creará una VLAN en WAN1/2.
Configuración general	**Etiqueta VLAN –**Ingrese el valor como el número de ID de VLAN. Las configuraciones válidas están en el rango de 1 a 4095. El sistema identificará el tráfico de red que fluye en cada canal a través de sus etiquetas VLAN. Es posible que los canales que usan el mismo tipo de WAN no

	configure el mismo valor de etiqueta VLAN. **Prioridad -**Elija el número para determinar la prioridad del paquete para dicha VLAN. El rango es de 0 a 7. **Valor de etiqueta de servicio**–Dicho valor varía dependiendo de la configuración configurada en**WAN>>Configuración general**. Si es necesario, haga clic en**Modificar**abrir**WAN>>Configuración general.**Luego, habilite **Inserción de etiquetas VLAN**para el servicio (etiqueta externa) y especifique el valor como el número de ID de VLAN. O bien, desactívelo.
Puente basado en puerto abierto **Conexión para esto Canal**	La configuración aquí creará un puente entre los puertos LAN seleccionados y la WAN. La interfaz WAN de la conexión del puente se basará en el tipo de WAN seleccionado mediante la etiqueta VLAN configurada. **Miembros físicos –**Agrupe los puertos físicos marcando las casillas de verificación correspondientes para aplicar la conexión de puente basada en puertos. **LAN inalámbrica (2 GHz/5 GHz)**-Agrupe los SSID marcando las casillas de verificación correspondientes para aplicar la conexión de puente basada en puerto. **Nota:**El puerto LAN P1 está reservado para uso NAT y no se puede seleccionar para puente.
Interfaz WAN abierta para este canal	Marque la casilla para habilitar la función relacionada. **Aplicación WAN -**El uso previsto de este canal. - **IPTV**-Los paquetes IGMP se pueden enviar a servidores de IPTV en este canal. **Configuración de WAN**– (Disponible cuando el tipo de WAN es VDSL o Ethernet (WAN2)) El método de acceso a la WAN de este canal. Las opciones disponibles son PPPoE/PPPoA e IP estática o dinámica. - **PPPoE/PPPoA**-Cuando se selecciona PPPoE/PPPoA, la configuración de acceso al ISP y la configuración de la dirección IP del ISP están disponibles para la configuración y se utilizarán para establecer la conexión WAN. - **IP estática o dinámica**-Cuando se selecciona IP estática o dinámica, la configuración de la red IP de WAN y la configuración de la dirección IP del servidor DNS están disponibles para la configuración y se utilizarán para establecer la conexión WAN..
Configuración de acceso ISP	Ingrese su nombre de usuario, contraseña y parámetros de autenticación asignados de acuerdo con la información proporcionada por su ISP. **Nombre del ISP**–Nombre del servicio PPP. Ingrese si su ISP requiere esta configuración; de lo contrario, déjelo en blanco. **Nombre de usuario**–Nombre proporcionado por el ISP para la autenticación PPPoE/PPPoA. La longitud máxima es de 62 caracteres. **Contraseña**–Contraseña proporcionada por el ISP para la autenticación PPPoE/PPPoA. La longitud máxima es de 62 caracteres. **Autenticación PPP**–El protocolo utilizado para la autenticación PPP. - **Papanicolaou solo**- Solo se utiliza PAP (Protocolo de autenticación de contraseña). - **PAP o CHAP**- Tanto PAP como CHAP (Challenge-Handshake Authentication Protocol) se pueden usar para la autenticación PPP. El enrutador negocia con el servidor PPTP o L2TP para determinar qué protocolo usar. **siempre encendido**–Si se selecciona, el enrutador mantendrá la

	Conexión PPPoE/PPPoA. **Tiempo de inactividad**–Período máximo de tiempo, en segundos, de inactividad permitido (sin tráfico) antes de que se corte la conexión. **Dirección IP del ISP**-Especifica cómo se configuró la dirección IP WAN del canal. - **ip fija** **Sí**-La dirección IP ingresada en el campo Dirección IP fija se usará como la dirección IP de la WAN virtual. **No**-La dirección IP de WAN virtual será asignada por el servidor PPPoE/PPPoA del ISP.
Configuración de red IP WAN	**Obten una direccion IP automaticamente**–Seleccione esta opción si el enrutador va a recibir información de configuración IP de un servidor DHCP. - **Nombre del enrutador**–Establece el valor de la opción 12 de DHCP, que utilizan algunos ISP. - **Nombre de dominio**–Establece el valor de la opción 15 de DHCP, que utilizan algunos ISP. **Especifique una dirección IP**–Seleccione esta opción para ingresar manualmente la dirección IP. - **Dirección IP**–Escriba la dirección IP. **Máscara de subred**–Escriba la - máscara de subred. **Dirección IP de la puerta de enlace**–Escriba la - dirección IP de la puerta de enlace. **Dirección IP del servidor DNS -**Escriba la dirección IP principal del enrutador si desea utilizar**IP estática**modo. Si es necesario, escriba la dirección IP secundaria por si fuera necesario en el futuro.

Después de terminar la configuración anterior, haga clic en**DE ACUERDO**para guardar la configuración y volver a la página anterior.

Haga clic en cualquier índice (10~16) para obtener la siguiente página web:



Los ajustes disponibles se explican a continuación:

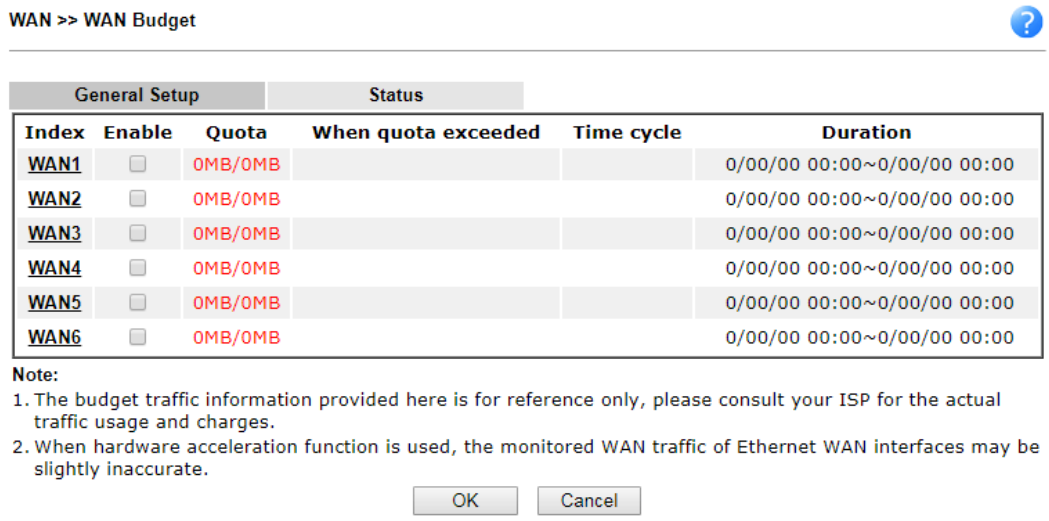
Artículo	Descripción
Habilitar canal 10~16	Haga clic en él para habilitar la configuración de este canal.
Tipo de WAN	Las conexiones e interfaces creadas en cada canal pueden seleccionar un tipo de WAN específico para construir. En la aplicación Multi-VLAN, solo está disponible el tipo de WAN Ethernet. El usuario podrá seleccionar aquí la interfaz WAN física que utilizará el canal.
Configuración general	**Etiqueta VLAN –**Ingrese el valor como el número de ID de VLAN. Las configuraciones válidas están en el rango de 1 a 4095. El sistema identificará el tráfico de red que fluye en cada canal a través de sus etiquetas VLAN. Es posible que los canales que usan el mismo tipo de WAN no configuren el mismo valor de etiqueta de VLAN. **Prioridad -**Elija el número para determinar la prioridad del paquete para dicha VLAN. El rango es de 0 a 7.
Modo Puente	**Permitir -**Haga clic en él para habilitar el modo Puente para dicho canal. **Miembros físicos –**Agrupe los puertos físicos marcando las casillas de verificación correspondientes para aplicar la conexión de puente. **LAN inalámbrica (2 GHz/5 GHz)**-Agrupe los SSID marcando las casillas de verificación correspondientes para aplicar la conexión de puente. **Nota:**El puerto LAN P1 está reservado para uso NAT y no se puede seleccionar para puente.

Después de terminar la configuración anterior, haga clic en**DE ACUERDO**para guardar la configuración.

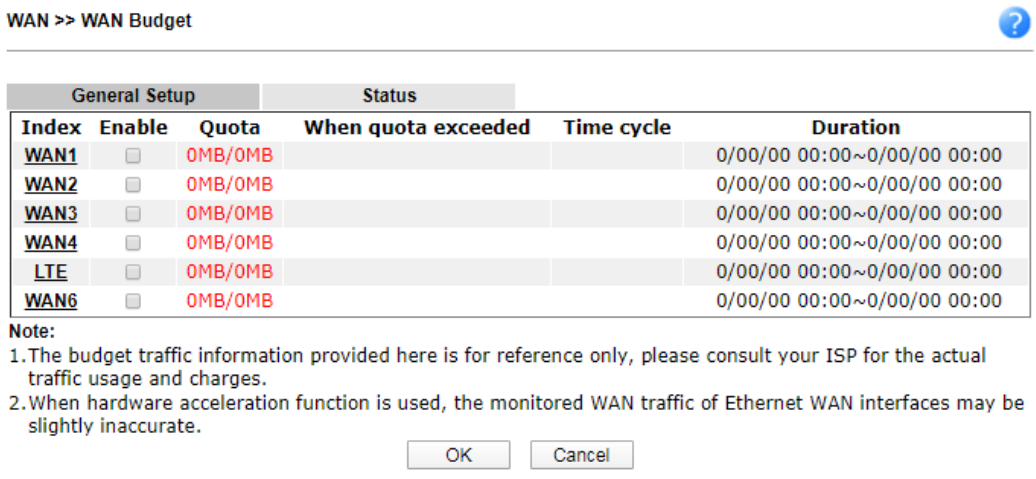
II-1-4 Presupuesto de la WAN

Esta función se utiliza para determinar los datos*volumen de tráfico*para cada interfaz WAN respectivamente para evitar sobrecargas por la transmisión de datos por parte del ISP. Tenga en cuenta que los ajustes de Límite de cuota y Día del mes del ciclo de facturación deberán configurarse correctamente primero para que algunos cálculos de períodos se realicen correctamente.

II-1-4-1 Configuración general



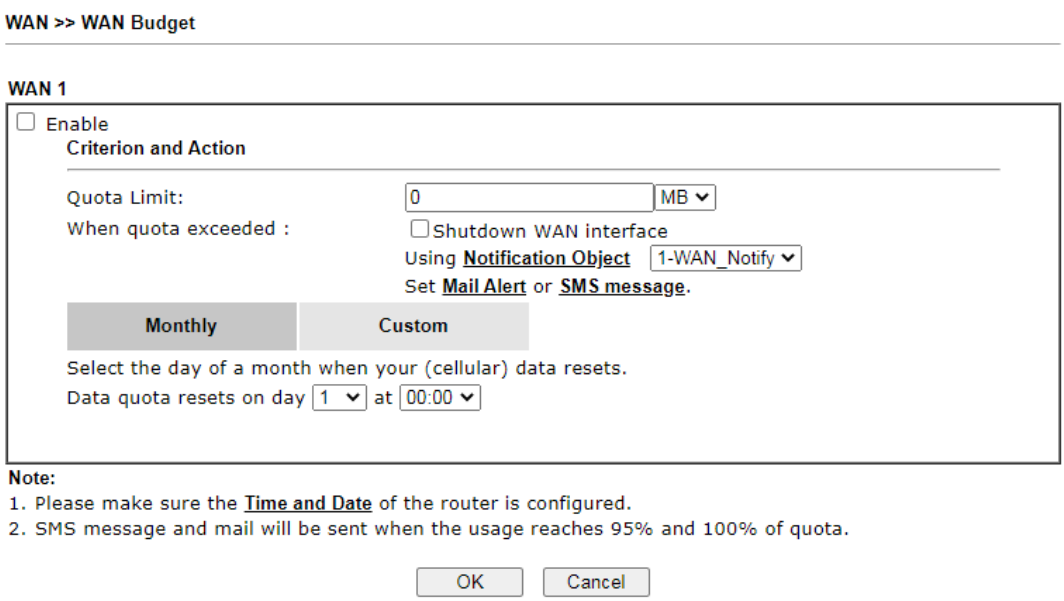
O



Artículo	Descripción
Índice	El puerto WAN. Haga clic para configurar el presupuesto de WAN para una WAN en particular.
Permitir	**v**-El presupuesto de WAN está habilitado en esta WAN. **X** -El presupuesto de WAN está deshabilitado en esta WAN.
Cuota	El uso de Internet del ciclo actual se expresa como*x/y*dónde *X*es el uso acumulado y*y*es el límite superior. Por ejemplo, 100 MB/200 MB significa que el uso hasta ahora en este ciclo es de 100 MB y el límite superior es de 200 MB.

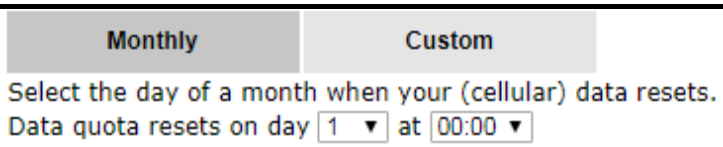
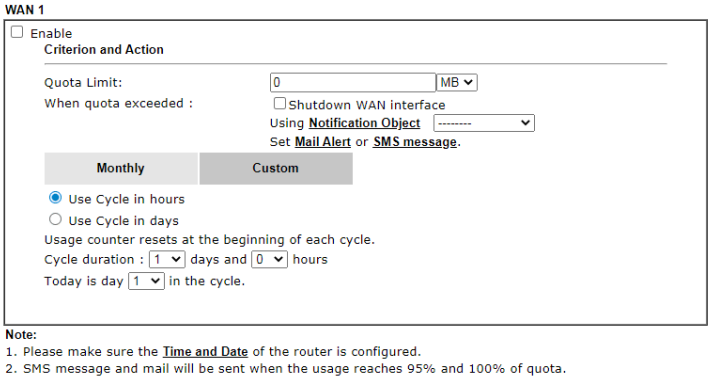
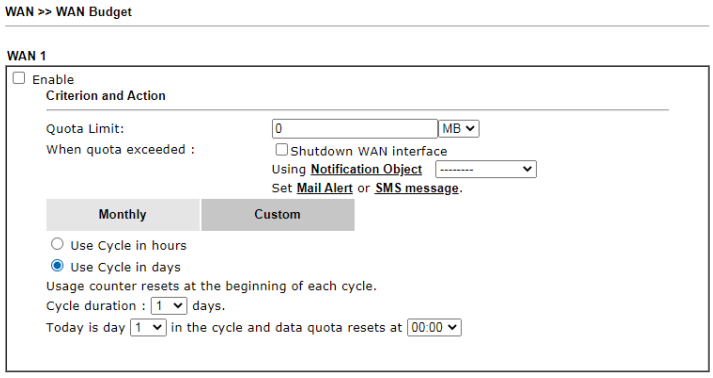
Cuando se supera la cuota	Acciones a realizar una vez alcanzada la cuota. **Cerrar**–La WAN se desactivará. **Alerta de correo**–Se enviará un correo electrónico al administrador.
Ciclo de tiempo	Restablecer la frecuencia de los datos de uso. **Mensual**–La opción Mensual en el**Criterio y Acción** La pestaña se usó para configurar la cuota de uso. **Definido por el usuario**d: La opción Definido por el usuario en el**Criterio y Acción**La pestaña se usó para configurar la cuota de uso.
Duración	Marcas de tiempo de inicio y finalización del ciclo actual.

Haga clic en el enlace WAN1 (a WAN6) o LTE para abrir la siguiente página web.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Marque la casilla para habilitar dicha función.
Límite de cuota	Ingrese la cuota de tráfico de datos permitida para dicha interfaz WAN. Se ofrecen dos unidades (MB y GB) para que las especifique.
Cuando se supera la cuota	Marque la(s) casilla(s) como la(s) condición(es) para que el sistema funcione cuando el tráfico haya excedido el límite del presupuesto. **Apague la interfaz WAN**–Se terminará todo el tráfico saliente a través de dicha interfaz WAN. - **Uso del objeto de notificación**–El sistema enviará una notificación basada en el contenido del objeto de notificación. - **Establecer alerta de correo**–El sistema enviará un mensaje de advertencia al administrador cuando se esté agotando la cuota. Sin embargo, los cargos de conexión se calcularán continuamente. - **Establecer mensaje SMS**-El sistema enviará un mensaje SMS al administrador cuando se agote la cuota.
Mensual	Algunos ISP pueden solicitar la limitación de la red según el límite de tráfico por mes. Esta configuración es para ofrecer un mecanismo de reinicio del registro de tráfico cada mes.

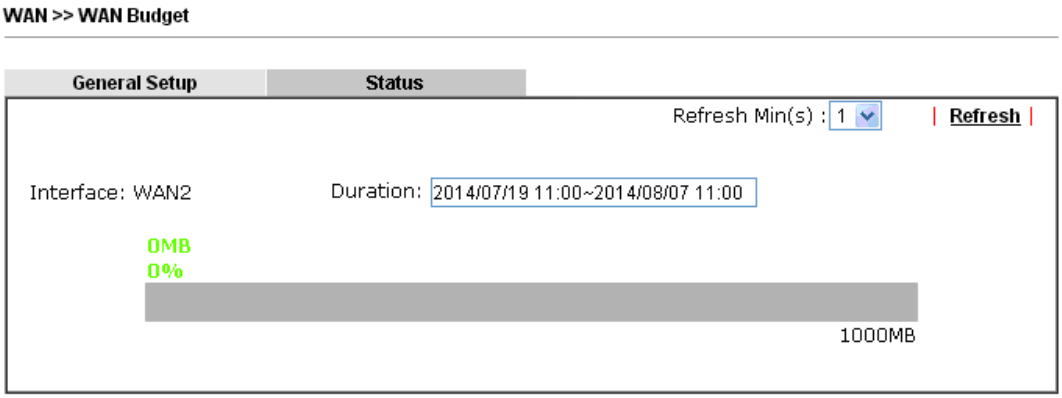
	 **La cuota de datos se restablece el día...**–Puede determinar el día de inicio en un mes.
Costumbre	Esta configuración permite al usuario definir el ciclo de facturación de acuerdo a su solicitud. El presupuesto de WAN se restablecerá con un intervalo de ciclo de facturación. Mensual es la configuración predeterminada. Si se requiere un período largo o corto, utilice**Costumbre**. El período de duración del ciclo es de 1 día a 60 días. Puede determinar la duración del ciclo especificando los días y las horas. Además, puede especificar qué día de hoy está en un ciclo. **Ciclo de uso en horas**–  - **Duración del ciclo**: Especifique los días y horas para restablecer el registro de tráfico. Por ejemplo, 7 significa que todo el ciclo es de 7 días; 20 significa que todo el ciclo es de 20 días. Cuando se acabe el tiempo, el enrutador restablecerá el registro de tráfico automáticamente. - **Hoy es el dia**–Especifique el día del ciclo como punto de partida en el que el enrutador Vigor restablecerá el registro de tráfico. Por ejemplo, "3" significa el tercer día de la duración del ciclo. **Ciclo de uso en días**-  - **Duración del ciclo**: Especifique los días para restablecer el registro de tráfico. Por ejemplo, 7 significa que todo el ciclo es de 7 días; 20 significa que todo el ciclo es de 20 días. Cuando se acabe el tiempo, el enrutador restablecerá el registro de tráfico automáticamente. - **Hoy es el dia**–Especifique el día y la hora para el descanso de la cuota de datos en el ciclo como el punto de partida que el enrutador Vigor

	restablecerá el registro de tráfico. Por ejemplo, “3” significa el tercer día de la duración del ciclo.

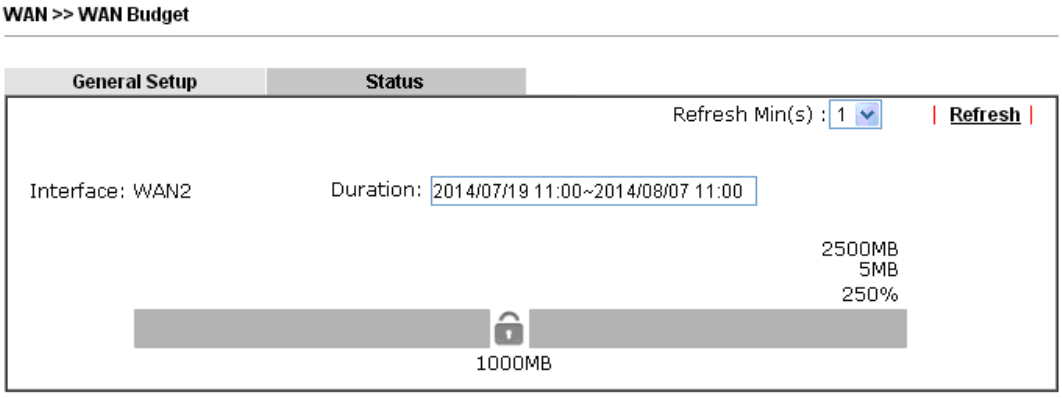
Después de terminar la configuración anterior, haga clic en**DE ACUERDO**para guardar la configuración.

II-1-4-2 Estado

La página de estado muestra el presupuesto de WAN de estado, incluida la duración y el uso.



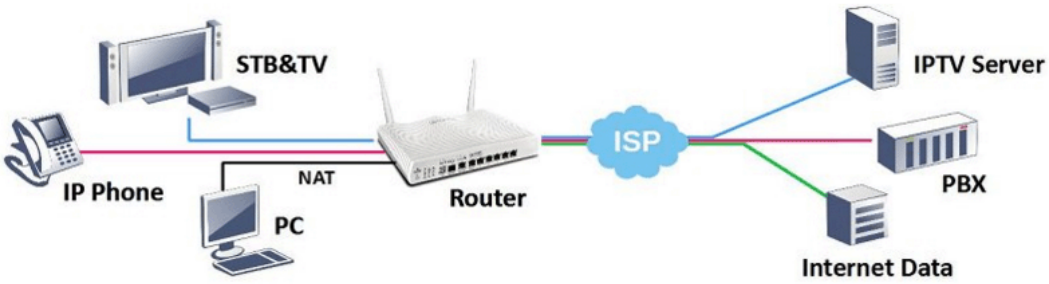
Si se agota el presupuesto de WAN, se mostrará un candado en la página si**Apague la interfaz WAN**es seleccionado. Lo que significa que no se llevará a cabo ninguna transmisión de datos. Además, el sistema enviará un mensaje de advertencia al administrador si**Alerta de correo**es seleccionado**.**O bien, el sistema enviará un mensaje SMS al administrador si**mensaje de texto**es seleccionado.



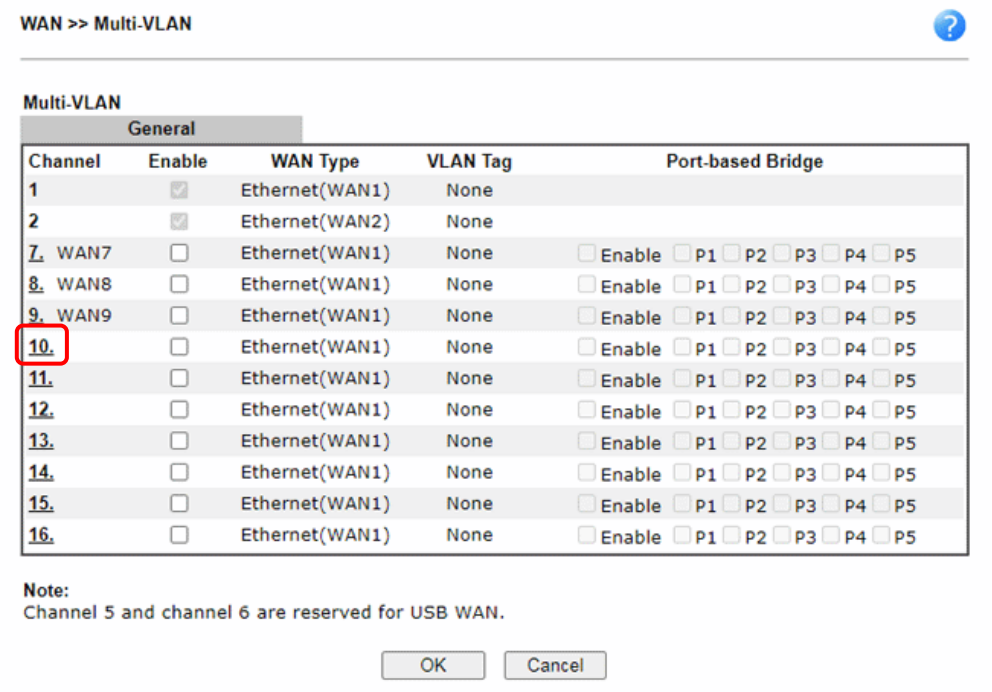
A-1 ¿Cómo configurar Multi-PVC para la implementación de triple play?

Al agregar etiquetas VLAN para diferenciar el tráfico, el proveedor de servicios puede entregar video, voz y datos a los suscriptores a través de una sola conexión, lo que también se conoce como servicio triple play. Este documento demostrará cómo configurar la función Multi-PVC para la implementación de triple play. Hay dos tipos de configuración, uno es un puente basado en puerto que conectará los medios, como el decodificador (STB), directamente al proveedor de servicios a través de un puerto LAN específico; el otro es abrir una interfaz WAN virtual y hacer NAT para la aplicación.

Conecte la WAN virtual a un puerto LAN



1. Ir a**WAN >> VLAN múltiple**, haga clic en un canal para configurar.



WAN >> Multi-VLAN

Multi-VLAN

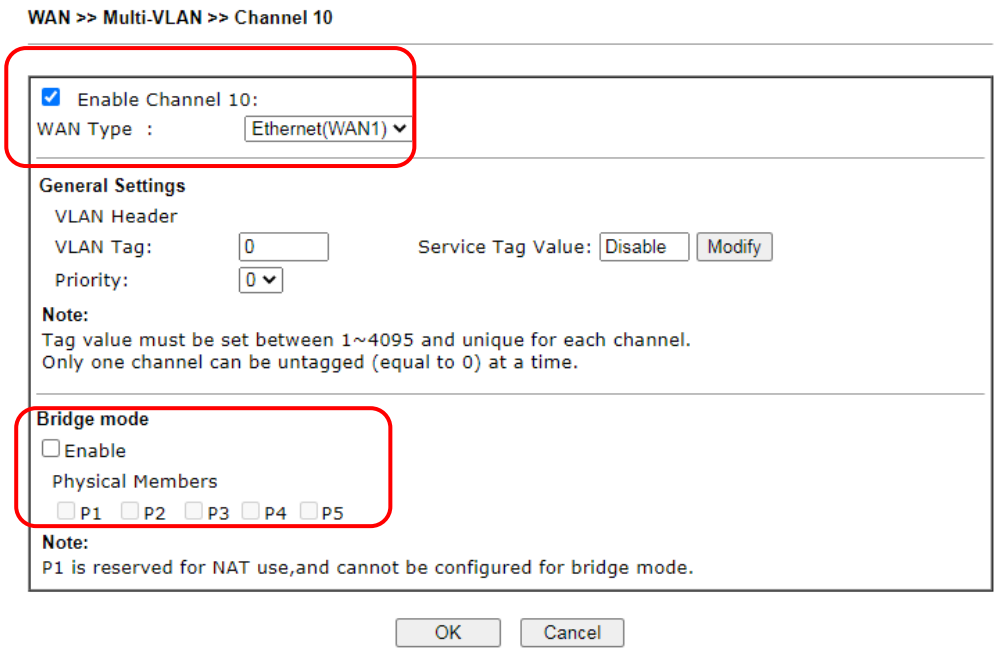
General

Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge
1	☑	Ethernet(WAN1)	None	
2	☑	Ethernet(WAN2)	None	
7. WAN7	☐	Ethernet(WAN1)	None	Enable P1 P2 P3 P4 P5
8. WAN8	☐	Ethernet(WAN1)	None	Enable P1 P2 P3 P4 P5
9. WAN9	☐	Ethernet(WAN1)	None	Enable P1 P2 P3 P4 P5
10.	☐	Ethernet(WAN1)	None	Enable P1 P2 P3 P4 P5
11.	☐	Ethernet(WAN1)	None	Enable P1 P2 P3 P4 P5
12.	☐	Ethernet(WAN1)	None	Enable P1 P2 P3 P4 P5
13.	☐	Ethernet(WAN1)	None	Enable P1 P2 P3 P4 P5
14.	☐	Ethernet(WAN1)	None	Enable P1 P2 P3 P4 P5
15.	☐	Ethernet(WAN1)	None	Enable P1 P2 P3 P4 P5
16.	☐	Ethernet(WAN1)	None	Enable P1 P2 P3 P4 P5

Note:
Channel 5 and channel 6 are reserved for USB WAN.

OK Cancel

2. Configure el canal de la siguiente manera,



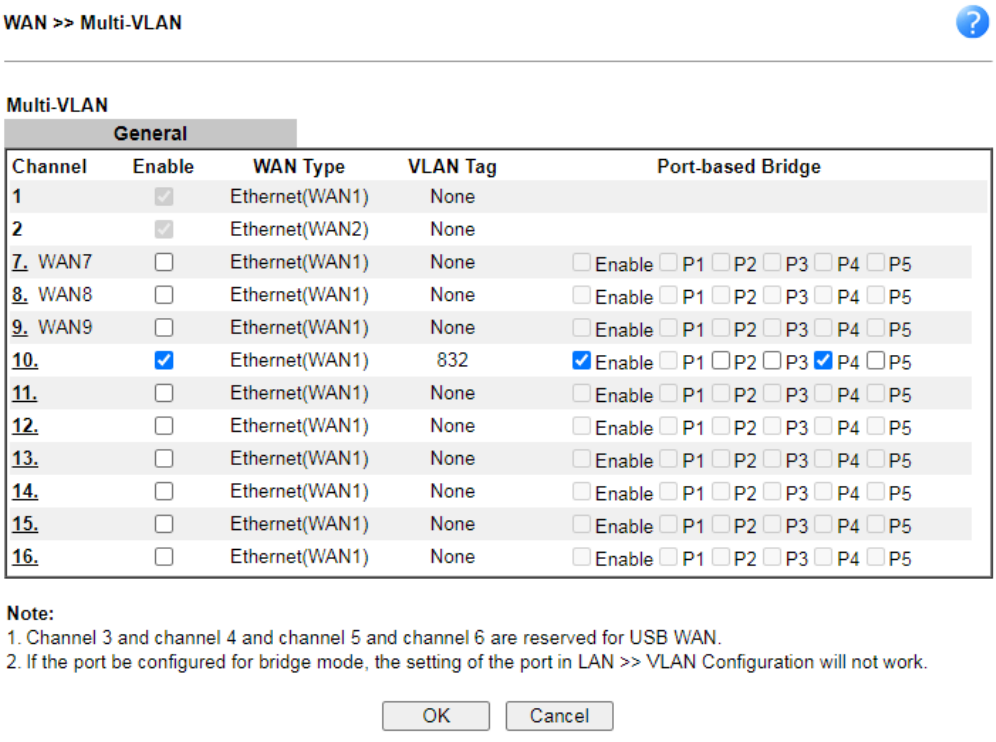
(a) habilitar este canal.

(b) establezca el tipo de WAN en la interfaz WAN en la que se encuentra el proveedor de servicios.

(c) habilite Agregar encabezado de VLAN e ingrese la etiqueta y la prioridad de VLAN según lo requiera el proveedor de servicios.

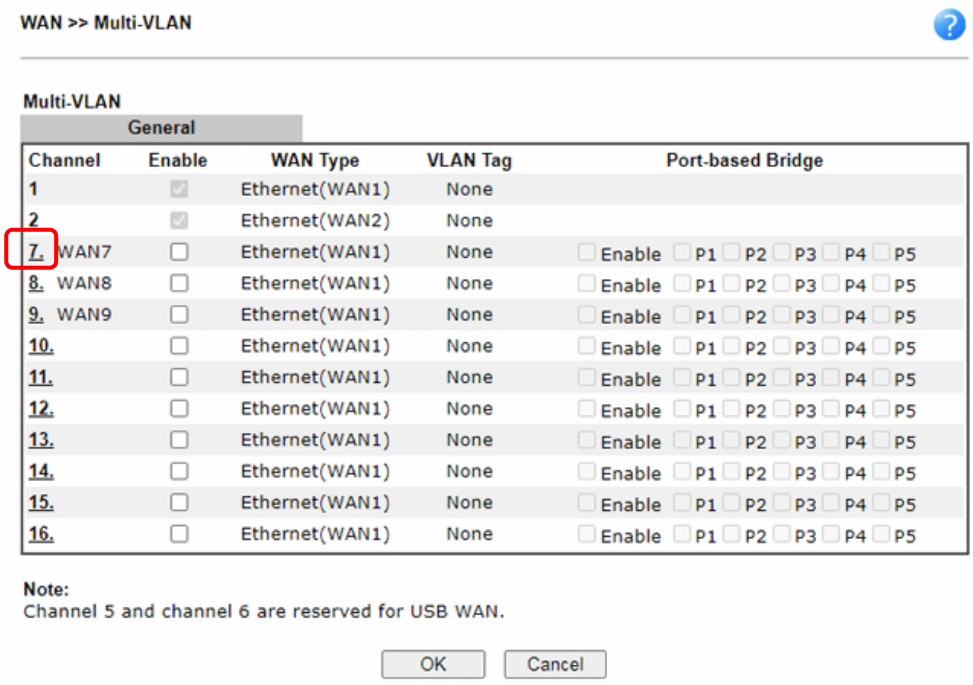
(d) marque Habilitar para Modo puente y seleccione el miembro del puerto físico al que va a conectar el STB.

3. Haga clic en**DE ACUERDO**para guardar la configuración, la configuración se mostrará en la página principal. Y ahora puede conectar el STB al puerto Bridged para usar el servicio de IPTV.



Abra una interfaz WAN virtual

1. Ir a**WAN >> Múltiples PVC/VLAN**, haga clic en el canal 7, 8 o 9 para configurar.



WAN >> Multi-VLAN

Multi-VLAN

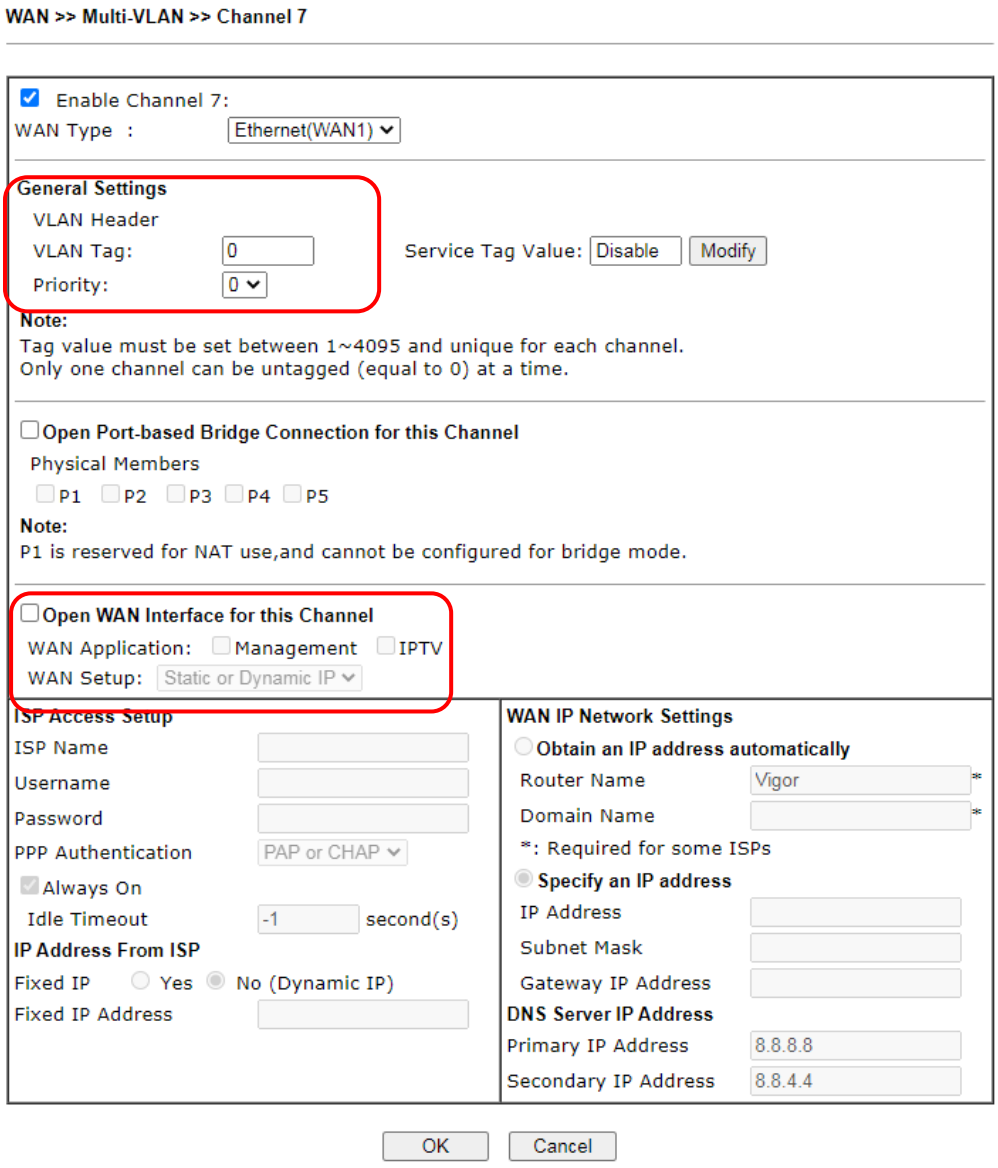
General

Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge
1	☑	Ethernet(WAN1)	None	
2	☑	Ethernet(WAN2)	None	
7. WAN7	☐	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5
8. WAN8	☐	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5
9. WAN9	☐	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5
10.	☐	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5
11.	☐	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5
12.	☐	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5
13.	☐	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5
14.	☐	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5
15.	☐	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5
16.	☐	Ethernet(WAN1)	None	☐ Enable ☐ P1 ☐ P2 ☐ P3 ☐ P4 ☐ P5

Note:
Channel 5 and channel 6 are reserved for USB WAN.

OK Cancel

2. Configure el canal de la siguiente manera,



(a) habilitar este canal.

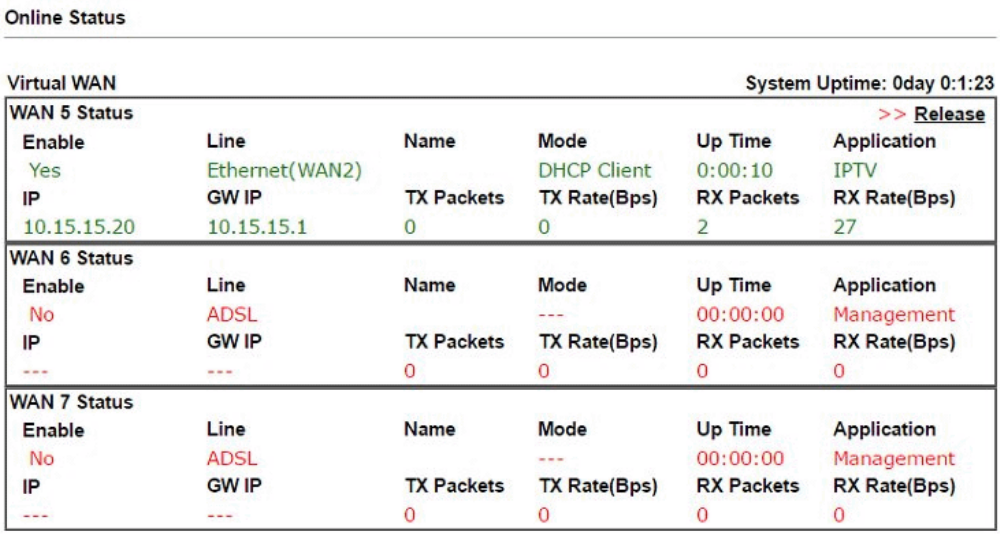
(b) establezca el tipo de WAN en la interfaz WAN en la que se encuentra el proveedor de servicios.

(c) ingrese la etiqueta VLAN y la prioridad según lo requiera el proveedor de servicios.

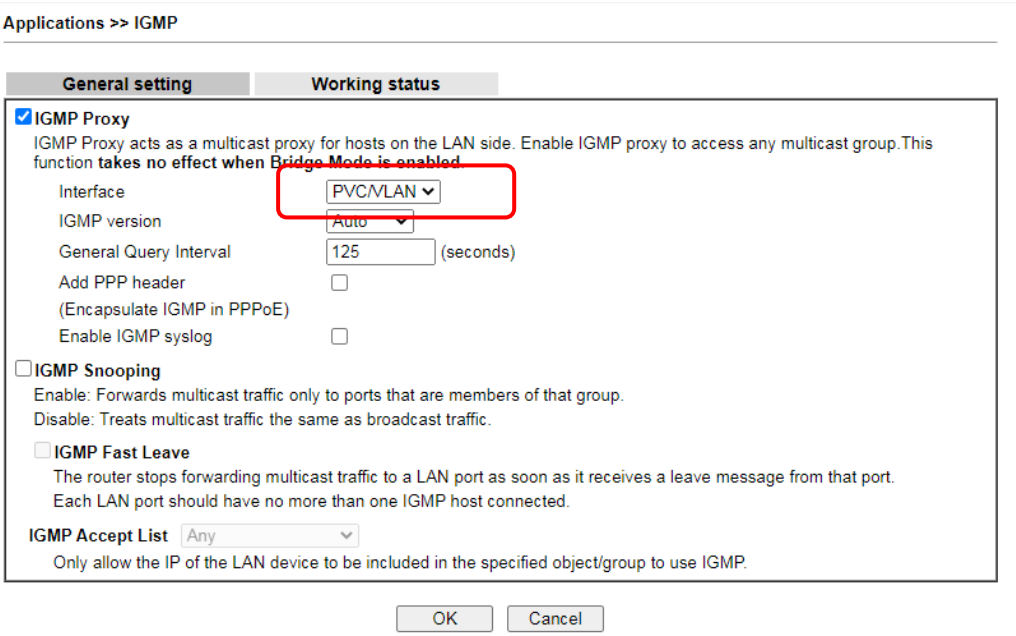
(d) habilite "Abrir interfaz WAN para este canal" y seleccione el tipo de aplicación que se usará en este canal. (Nota: esta opción solo está disponible en el canal 7-9)

(e) configurar el tipo de Acceso a Internet según lo requiera el ISP.

3. Haga clic en**DE ACUERDO**para guardar el perfil y reiniciar el enrutador para aplicar la configuración. Después de reiniciar el enrutador, vaya a**Estado en línea >> WAN virtual**para asegurarse de que la interfaz WAN esté activa y haya obtenido una dirección IP.



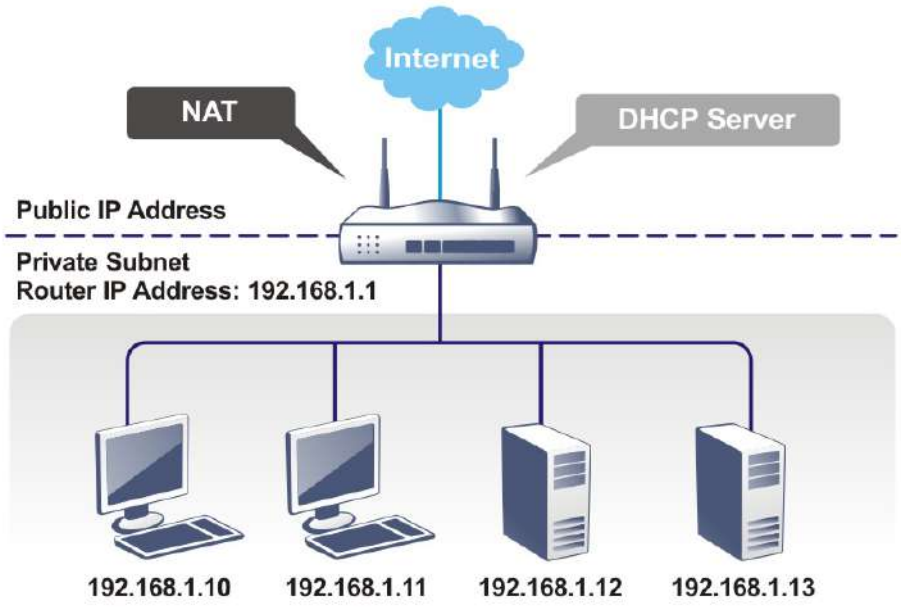
4. Ahora, puede usar la interfaz WAN virtual para aplicaciones como IGMP Proxy, esto se puede hacer seleccionando la interfaz WAN como "PVC/VLAN".



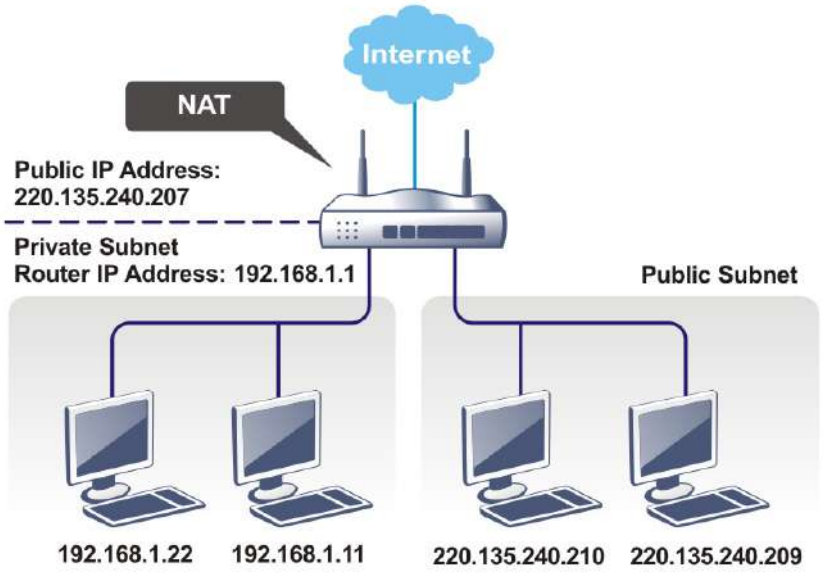
II-2 LAN

La red de área local (LAN) es un grupo de subredes reguladas y gobernadas por un enrutador. El diseño de la estructura de la red está relacionado con el tipo de direcciones IP públicas que provienen de su ISP.

La función más genérica del enrutador Vigor es NAT. Crea una subred privada propia. Como se mencionó anteriormente, el enrutador se comunicará con otros hosts públicos en Internet mediante el uso de una dirección IP pública y se comunicará con los hosts locales mediante su dirección IP privada. Lo que hace NAT es traducir los paquetes de la dirección IP pública a la dirección IP privada para reenviar los paquetes correctos al host correcto y viceversa. Además, el enrutador Vigor tiene un servidor DHCP incorporado que asigna una dirección IP privada a cada host local. Vea el siguiente diagrama para una breve comprensión.



En algún caso especial, puede tener una subred de IP pública de su ISP, como 220.135.240.0/24. Esto significa que puede configurar una subred pública o llamar a una segunda subred para que cada host esté equipado con una dirección IP pública. Como parte de la subred pública, el enrutador Vigor servirá para el enrutamiento de IP para ayudar a los hosts en la subred pública a comunicarse con otros hosts públicos o servidores externos. Por lo tanto, el enrutador debe configurarse como puerta de enlace para hosts públicos.



¿Qué es el protocolo de información de enrutamiento (RIP)?

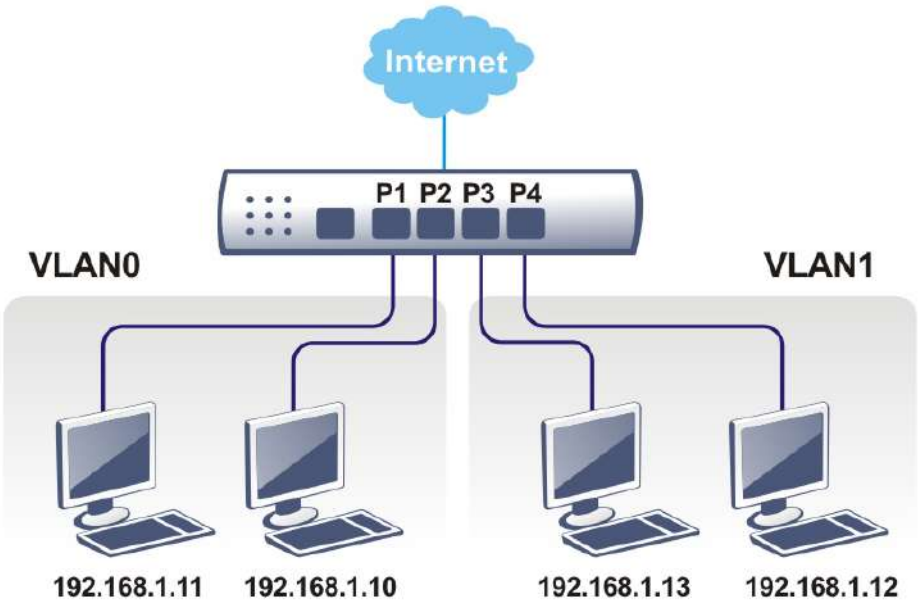
El enrutador Vigor intercambiará información de enrutamiento con enrutadores vecinos utilizando el RIP para lograr el enrutamiento IP. Esto permite a los usuarios cambiar la información del enrutador, como la dirección IP, y los enrutadores se informarán automáticamente entre sí.

¿Qué es la ruta estática?

Cuando tiene varias subredes en su LAN, a veces una forma más efectiva y rápida de conexión es la **Rutas estáticas**función en lugar de otro método. Simplemente puede establecer reglas para reenviar datos de una subred específica a otra subred específica sin la presencia de RIP.

¿Qué son las LAN virtuales y el control de velocidad?

Puede agrupar hosts locales por puertos físicos y crear hasta 8 LAN virtuales. Para administrar la comunicación entre diferentes grupos, configure reglas en la función LAN virtual (VLAN) y la velocidad de cada uno.



Una LAN comprende una colección de clientes de LAN, que son dispositivos en red en sus instalaciones. Un cliente LAN puede ser una computadora, una impresora, un teléfono de voz sobre IP (VoIP), un teléfono móvil, una consola de juegos, una televisión de protocolo de Internet (IPTV), etc., y puede tener una conexión por cable (usando cableado Ethernet).) o conexión de red inalámbrica (usando Wi-Fi).

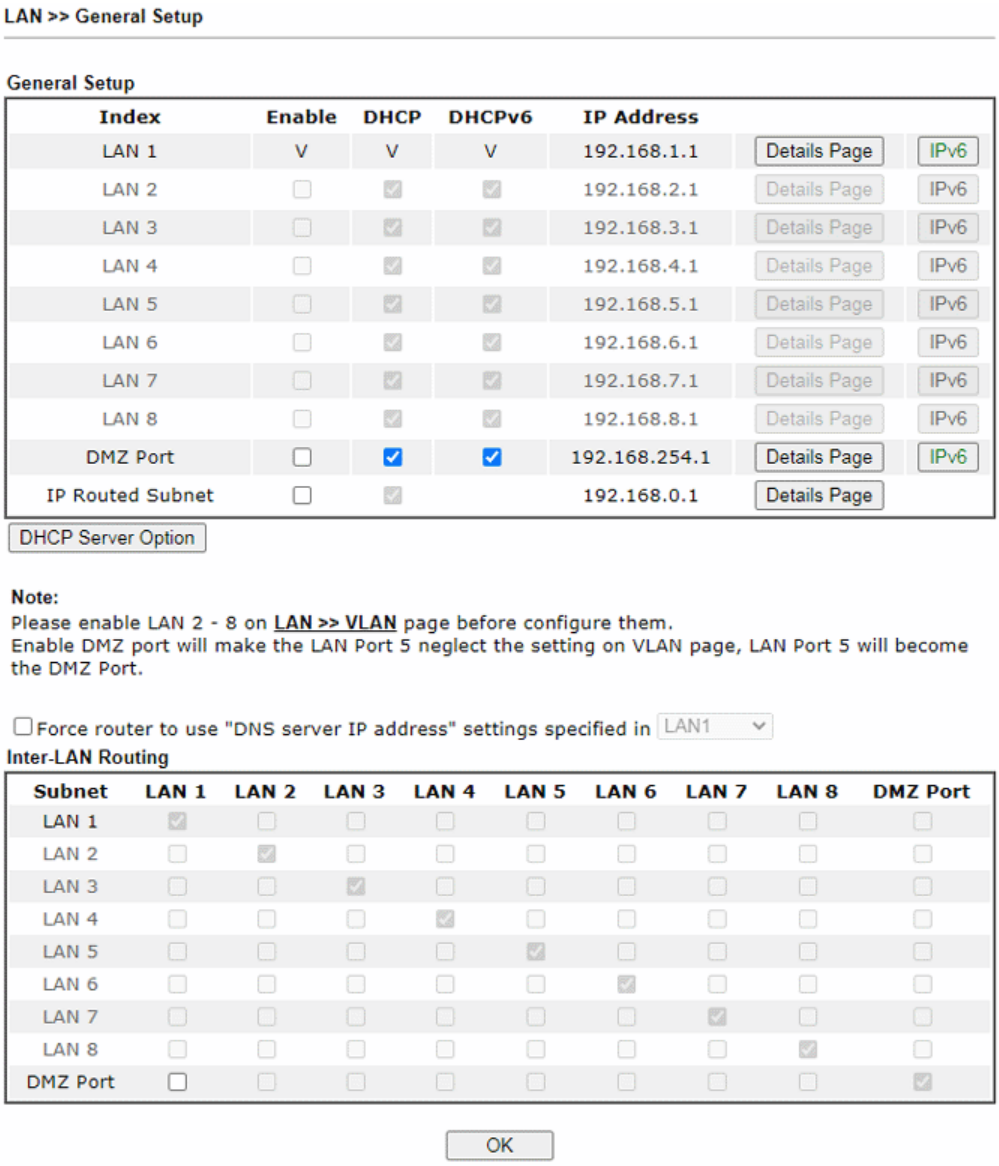
Los clientes de LAN dentro de la misma LAN normalmente pueden comunicarse entre sí directamente, ya que son pares entre sí, a menos que se hayan implementado medidas, como firewalls o VLAN, para restringir dicho acceso. Hoy en día, los cortafuegos LAN más comunes se implementan en el propio cliente LAN. Por ejemplo, Microsoft Windows desde Windows XP y Apple OS X tienen firewalls integrados que se pueden configurar para restringir el tráfico que entra y sale de la computadora. Las VLAN, por otro lado, generalmente se configuran mediante conmutadores o enrutadores de red, como el Vigor2927.

Para comunicarse con los hosts fuera de la LAN, los clientes de la LAN deben pasar por una puerta de enlace de red, que en la mayoría de los casos es un enrutador (como el Vigor 2862) que se encuentra entre la LAN y la red del ISP, que es la WAN. El enrutador actúa como director para garantizar que el tráfico entre la LAN y la WAN llegue a sus destinos previstos.

II-2-1 Configuración general

Esta página le proporciona la configuración general para LAN. Hacer clic**LAN**para abrir la página de configuración de LAN y elegir**Configuración general**.

El enrutador proporciona ocho subredes que permiten a los usuarios dividir grupos en diferentes subredes (LAN1 - LAN8). Además, diferentes subredes pueden vincularse entre sí configurando **Enrutamiento entre LAN**. Actualmente, la configuración de LAN1 está fijada solo con el modo NAT. LAN2 – LAN8 se puede operar bajo**NAT**o**Ruta**modo. La subred enrutada IP se puede operar en el modo de ruta.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Configuración general	Permita configurar los ajustes para cada subred respectivamente. **Índice -**Muestra todos los elementos de LAN. **Permitir-**Básicamente, el estado LAN1 está habilitado de forma predeterminada. LAN2 –LAN8 y la subred enrutada IP se pueden observar marcando la casilla de**Permitir**. **DHCP/DHCPv6-**LAN1 está configurado con DHCP/DHCPv6 de forma predeterminada. Si es necesario, marque la casilla DHCP para cada LAN. **Dirección IP -**Muestra la dirección IP para cada elemento de LAN. Dicha información está configurada de forma predeterminada y no puede modificarla. **Página de detalles -**Haga clic en él para acceder a la página de configuración. Cada LAN tendrá una página de configuración de LAN diferente.**Cada LAN debe configurarse en una subred diferente.** **IPv6 –**Haga clic en él para acceder a la página de configuración de IPv6.
Opción de servidor DHCP	Los paquetes DHCP se pueden procesar agregando el número de opción y la información de datos cuando dicha función está habilitada. Para obtener información detallada, consulte la sección posterior.

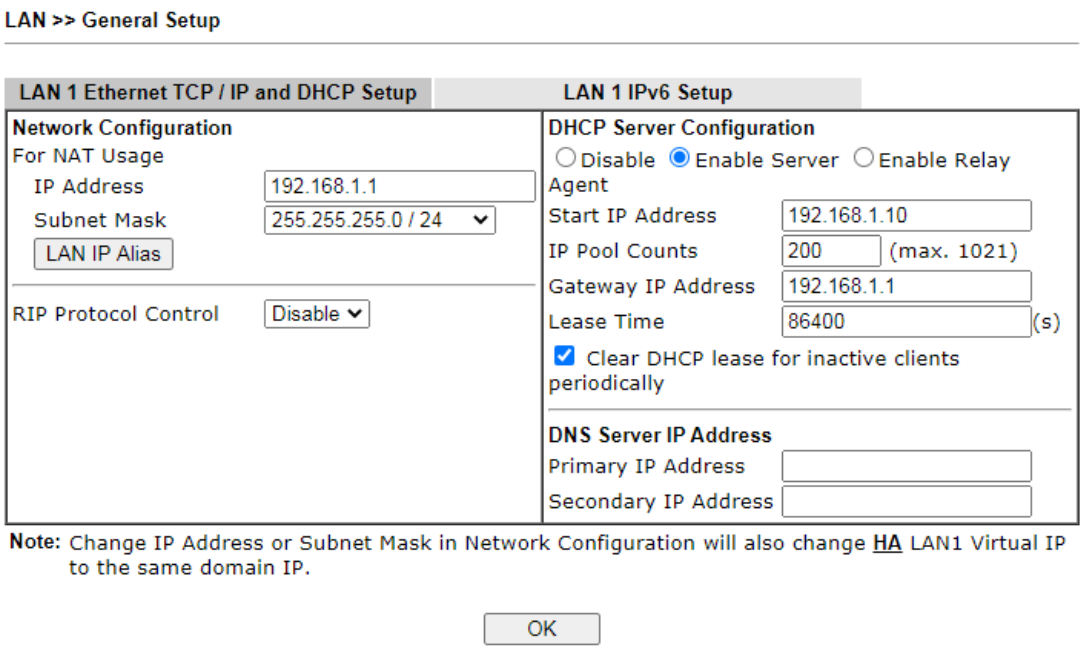
Forzar al enrutador a usar "Dirección IP del servidor DNS..."	Obligue al enrutador Vigor a usar servidores DNS configurados en el puerto LAN1/LAN2/LAN3/LAN4/LAN5/LAN6/LAN7/LAN8/DMZ en lugar de servidores DNS proporcionados por el servidor de acceso a Internet (PPPoE, PPTP, L2TP o servidor DHCP).
Enrutamiento entre LAN	Marque la casilla para vincular dos o más subredes diferentes (LAN y LAN). El enrutamiento entre LAN permite interconectar o aislar diferentes subredes de LAN. Solo está disponible cuando la funcionalidad VLAN está habilitada. Consulte la sección II-2-2 VLAN sobre cómo configurar las VLAN. En la matriz de enrutamiento entre LAN, una casilla de verificación seleccionada significa que las 2 LAN que se cruzan pueden comunicarse entre sí.

Cuando termine la configuración, haga clic en**DE ACUERDO**para guardar y salir de esta página.

Información	Para configurar una subred, seleccione su botón Página de detalles para que aparezca la página de detalles de LAN.

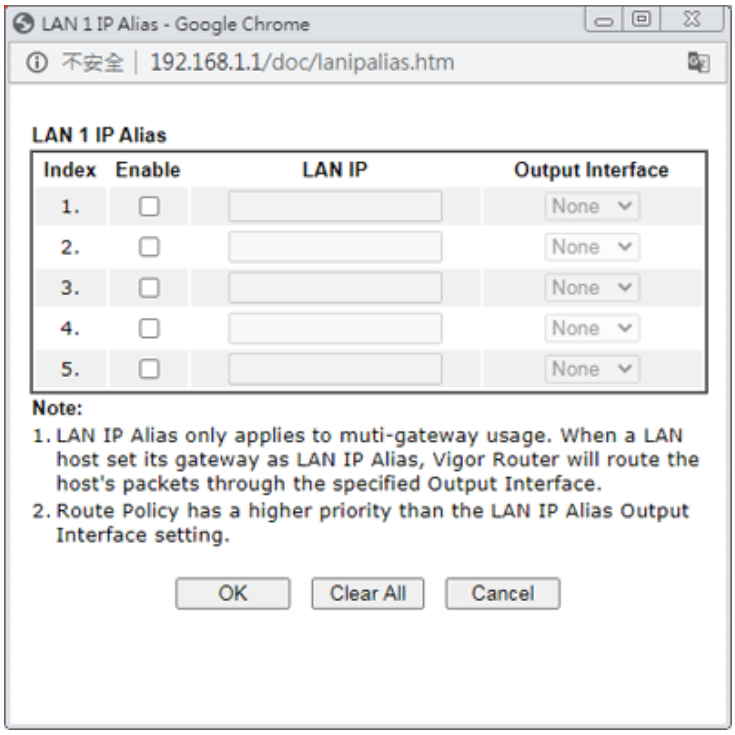
II-2-1-1 Página de detalles para LAN1–Configuración de Ethernet TCP/IP y DHCP

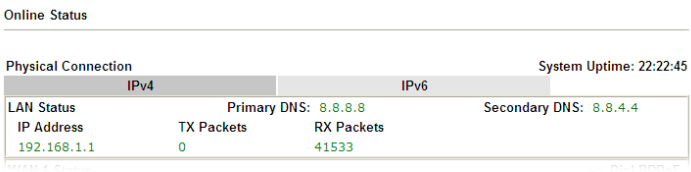
Hay dos páginas de configuración para LAN1, Configuración de Ethernet TCP/IP y DHCP (basado en IPv4) y Configuración de IPv6. Haga clic en la pestaña de cada tipo y consulte las siguientes explicaciones para obtener información detallada.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
configuración de la red	**Para el uso de NAT,** **Dirección IP**-Esta es la dirección IP del enrutador. (Predeterminado: 192.168.1.1). **Máscara de subred -**La máscara de subred, junto con la dirección IP

	campo, indica el número máximo de clientes permitidos en la subred. (Predeterminado: 255.255.255.0/ 24). **Alias de IP de LAN**–Esta función permite especificar varias puertas de enlace (bajo un conmutador) con diferentes interfaces WAN para acceder a Internet a través del enrutador Vigor.  **Control de protocolo RIP,** **Permitir -**Cuando está habilitado, el enrutador intentará intercambiar información de enrutamiento con enrutadores vecinos utilizando el Protocolo de información de enrutamiento.
servidor DHCP Configuración	DHCP significa Protocolo de configuración dinámica de host. El enrutador, de forma predeterminada de fábrica, actúa como un servidor DHCP para su red, por lo que envía automáticamente la configuración de IP relacionada a cualquier usuario local configurado como cliente DHCP. Se recomienda enfáticamente que deje el enrutador habilitado como servidor DHCP si no tiene un servidor DHCP para su red. Si desea utilizar otro servidor DHCP en la red que no sea el Vigor Router, puede dejar que Relay Agent lo ayude a redirigir la solicitud DHCP a la ubicación especificada. **Desactivar -**Le permite asignar manualmente la dirección IP a cada host en la LAN. **Habilitar servidor -**Deje que el enrutador asigne una dirección IP a cada host en la LAN. - **Dirección IP de inicio -**La dirección IP de LAN inicial que se proporciona a los clientes DHCP de LAN. - **Recuentos de grupos de IP:**El número máximo de direcciones IP que DHCP entregará. El valor predeterminado es 200. El rango válido es entre 1 y 1021. El número real de direcciones IP disponibles para la asignación es el número de grupos de IP, o 1021 menos el último octeto de la dirección IP de inicio, el que sea menor. - **Dirección IP de la puerta de enlace -**La dirección IP de la puerta de enlace, que es el host en la LAN que retransmite todo el tráfico que entra y sale de la LAN. La puerta de enlace es normalmente el enrutador y, por lo tanto, la IP de la puerta de enlace.

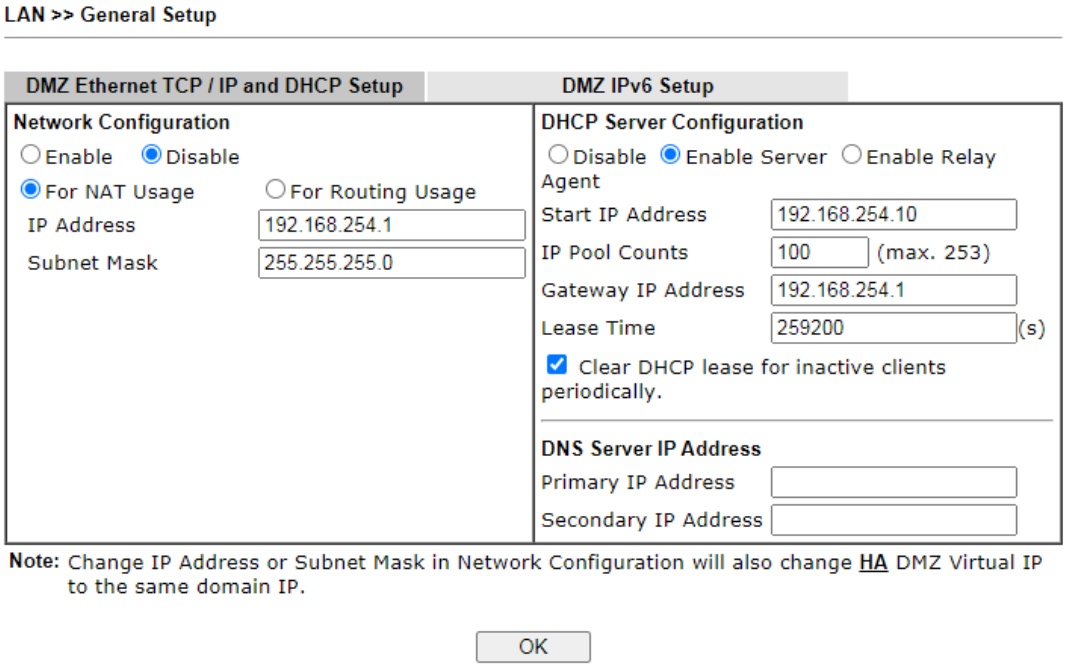
	La dirección debe ser idéntica a la dirección IP en el **configuración de la red**sección anterior. - **Tiempo de arrendamiento**-La duración máxima de las direcciones IP emitidas por DHCP se puede utilizar antes de tener que renovarlas. - **Borrar concesión de DHCP para clientes inactivos periódicamente -**Si se selecciona, el enrutador envía solicitudes ARP y recicla las direcciones IP previamente asignadas a clientes DHCP inactivos para evitar el agotamiento del grupo de direcciones IP. **Nota**: Cuando se habilita Borrar concesión de DHCP para clientes inactivos periódicamente, el enrutador hará lo siguiente: - Compruebe las actividades de los clientes DHCP mediante solicitudes ARP cada minuto cuando las direcciones IP DHCP disponibles sean inferiores a 30 - Borre la concesión de DHCP cuando el cliente no responde respuestas ARP. **Habilitar agente de retransmisión:**Cuando se selecciona, todas las solicitudes DHCP se reenvían a un servidor DHCP fuera de la subred LAN, y cuya dirección se especifica en el campo Dirección IP del servidor DHCP. - **Dirección IP del servidor DHCP –**Está disponible cuando**Habilitar agente de retransmisión**está chequeado. Establezca la dirección IP del servidor DHCP que va a utilizar para que el Agente de retransmisión pueda ayudar a reenviar la solicitud DHCP al servidor DHCP.
Dirección IP del servidor DNS	DNS significa Sistema de nombres de dominio. Cada host de Internet debe tener una dirección IP única, también pueden tener un nombre amigable para los humanos y fácil de recordar, como www.yahoo.com. El servidor DNS convierte el nombre fácil de usar en su dirección IP equivalente. **Dirección IP principal -**Debe especificar una dirección IP del servidor DNS aquí porque su ISP debería proporcionarle normalmente más de un servidor DNS. **Dirección IP secundaria -**Puede especificar la dirección IP del servidor DNS secundario aquí porque su ISP a menudo le proporciona más de un servidor DNS. La dirección IP predeterminada del servidor DNS se puede encontrar a través de Estado en línea:  Si se dejan vacíos los campos IP principal y Dirección IP secundaria, el enrutador asignará los servidores DNS obtenidos de la interfaz WAN a los usuarios locales como un servidor proxy DNS y mantendrá una caché de DNS. Si no hay servidores DNS disponibles, el enrutador usará su propia dirección IP en su lugar. Si la dirección IP de un nombre de dominio ya está en la caché de DNS, el enrutador resolverá el nombre de dominio inmediatamente. De lo contrario, el enrutador reenvía el paquete de consulta DNS al servidor DNS externo estableciendo una conexión WAN (por ejemplo, DSL/Cable).

Cuando termine la configuración, haga clic en**DE ACUERDO**para guardar y salir de esta página.

Las direcciones IP privadas se pueden asignar automáticamente a los clientes LAN mediante el Protocolo de configuración dinámica de host (DHCP) o se pueden asignar manualmente. El servidor DHCP puede ser el

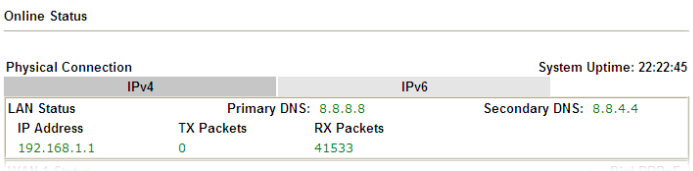
enrutador (el caso más común), o un servidor separado, que distribuye las direcciones IP a los clientes DHCP.

Alternativamente, las direcciones IP estáticas se pueden configurar manualmente en los clientes LAN como parte de su configuración de red. No importa cómo se configuren las direcciones IP, es importante que no haya dos dispositivos que obtengan la misma dirección IP. Si en una red se utilizan DHCP y asignaciones estáticas, es importante excluir las direcciones IP estáticas del conjunto de direcciones IP de DHCP. Por ejemplo, si su LAN usa la subred 192.168.1.x y tiene 20 clientes DHCP y 20 clientes de IP estática, podría configurar 192.168.1.10 como la dirección IP de inicio, 50 como el número de grupos de IP (suficiente para el número actual). de clientes DHCP, más espacio para futuras expansiones) y utilice direcciones superiores a 192.168.1.100 para la asignación estática.

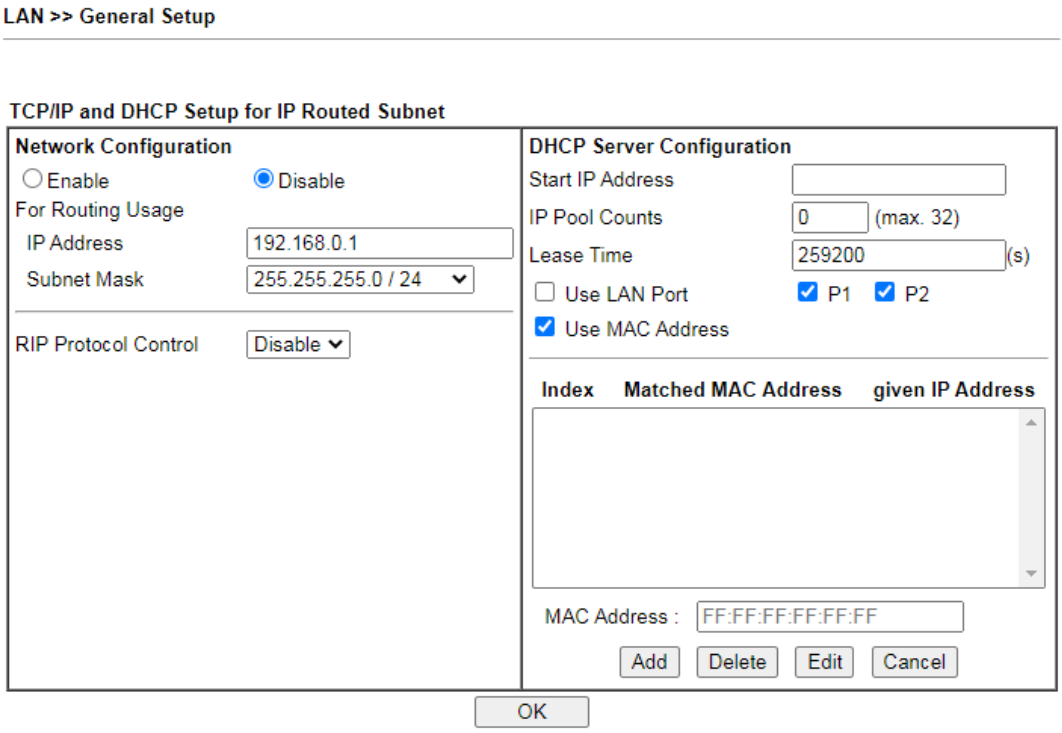


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
configuración de la red	**Habilitar deshabilitar -**Hacer clic**Permitir**para habilitar dicha configuración; hacer clic**Desactivar**para deshabilitar dicha configuración. **Para uso NAT -**Haga clic en este botón de radio para invocar la función NAT. **Para el uso de enrutamiento:**Haga clic en este botón de radio para invocar esta función. **Dirección IP**-Esta es la dirección IP del enrutador. (Predeterminado: 192.168.1.1). **Máscara de subred -**La máscara de subred, junto con el campo Dirección IP, indica el número máximo de clientes permitidos en la subred. (Predeterminado: 255.255.255.0/ 24).
servidor DHCP Configuración	**Desactivar -**Le permite asignar manualmente la dirección IP a cada host en la LAN. **Habilitar servidor -**Deje que el enrutador asigne una dirección IP a cada host en la LAN. - **Dirección IP de inicio -**La dirección IP de LAN inicial que se proporciona a los clientes DHCP de LAN. - **Recuentos de grupos de IP:**El número máximo de direcciones IP que DHCP entregará. El valor predeterminado es 100. El rango válido es entre 1 y 1021. El número real de direcciones IP disponibles para la asignación es el número de grupos de IP, o 1021 menos el último octeto de la dirección IP de inicio, el que sea menor. - **Dirección IP de la puerta de enlace -**La dirección IP de la puerta de enlace, que es el host en la LAN que retransmite todo el tráfico que entra y sale de la LAN. La puerta de enlace es normalmente el enrutador y, por lo tanto, la dirección IP de la puerta de enlace debe ser idéntica a la dirección IP en el **configuración de la red**sección anterior.

	- **Tiempo de arrendamiento**-La duración máxima de las direcciones IP emitidas por DHCP se puede utilizar antes de tener que renovarlas. - **Borrar concesión de DHCP para clientes inactivos periódicamente -**Si se selecciona, el enrutador envía solicitudes ARP y recicla las direcciones IP previamente asignadas a clientes DHCP inactivos para evitar el agotamiento del grupo de direcciones IP. **Nota**: Cuando se habilita Borrar concesión de DHCP para clientes inactivos periódicamente, el enrutador hará lo siguiente: - Compruebe las actividades de los clientes DHCP mediante solicitudes ARP cada minuto cuando las direcciones IP DHCP disponibles sean inferiores a 30 - Borre la concesión de DHCP cuando el cliente no responde respuestas ARP. **Habilitar agente de retransmisión:**Cuando se selecciona, todas las solicitudes DHCP se reenvían a un servidor DHCP fuera de la subred LAN, y cuya dirección se especifica en el campo Dirección IP del servidor DHCP. - **Dirección IP del servidor DHCP –**Está disponible cuando**Habilitar agente de retransmisión**está chequeado. Establezca la dirección IP del servidor DHCP que va a utilizar para que el Agente de retransmisión pueda ayudar a reenviar la solicitud DHCP al servidor DHCP.
Dirección IP del servidor DNS	DNS significa Sistema de nombres de dominio. Cada host de Internet debe tener una dirección IP única, también pueden tener un nombre amigable para los humanos y fácil de recordar, como www.yahoo.com. El servidor DNS convierte el nombre fácil de usar en su dirección IP equivalente. **Dirección IP principal -**Debe especificar una dirección IP del servidor DNS aquí porque su ISP debería proporcionarle normalmente más de un servidor DNS. **Dirección IP secundaria -**Puede especificar la dirección IP del servidor DNS secundario aquí porque su ISP a menudo le proporciona más de un servidor DNS. La dirección IP predeterminada del servidor DNS se puede encontrar a través de Estado en línea:  Si los campos IP principal y Dirección IP secundaria se dejan vacíos, el enrutador asignará su propia dirección IP a los usuarios locales como un servidor proxy DNS y mantendrá una caché DNS. Si la dirección IP de un nombre de dominio ya está en la caché de DNS, el enrutador resolverá el nombre de dominio inmediatamente. De lo contrario, el enrutador reenvía el paquete de consulta DNS al servidor DNS externo estableciendo una conexión WAN (por ejemplo, DSL/Cable).

Cuando termine la configuración, haga clic en**DE ACUERDO**para guardar y salir de esta página.



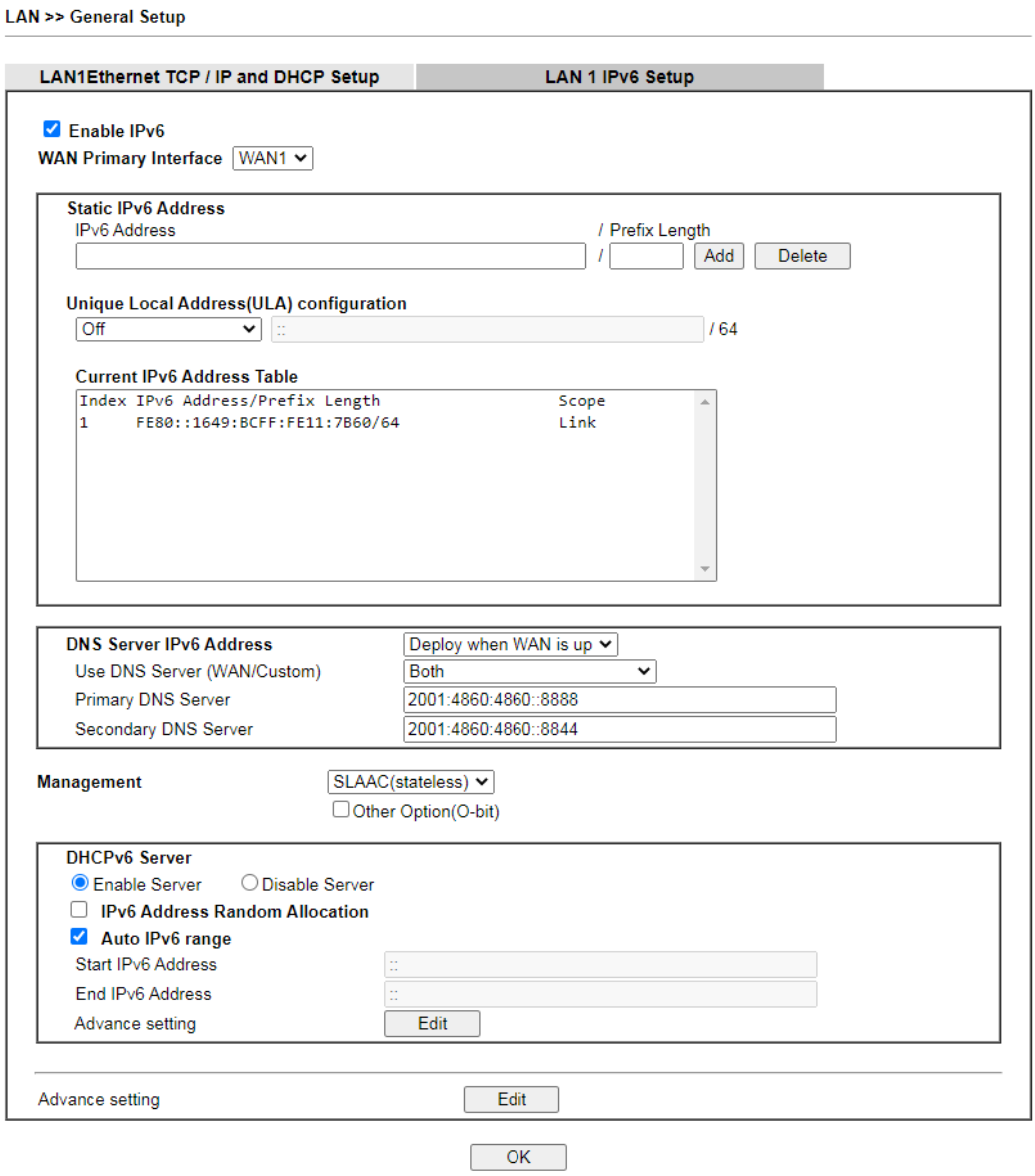
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
configuración de la red	**Habilitar deshabilitar -**Hacer clic**Permitir**para habilitar dicha configuración; hacer clic**Desactivar**para deshabilitar dicha configuración. **Para el uso de enrutamiento,** **Dirección IP**-Esta es la dirección IP del enrutador. (Predeterminado: 192.168.1.1). **Máscara de subred -**La máscara de subred, junto con el campo Dirección IP, indica el número máximo de clientes permitidos en la subred. (Predeterminado: 255.255.255.0/ 24). **Control de protocolo RIP,** **Permitir -**Cuando está habilitado, el enrutador intentará intercambiar información de enrutamiento con enrutadores vecinos utilizando el Protocolo de información de enrutamiento**.**
servidor DHCP Configuración	DHCP significa Protocolo de configuración dinámica de host. El enrutador por defecto de fábrica actúa como un servidor DHCP para su red, por lo que envía automáticamente la configuración de IP relacionada a cualquier usuario local configurado como cliente DHCP. Se recomienda enfáticamente que deje el enrutador habilitado como servidor DHCP si no tiene un servidor DHCP para su red. **Dirección IP de inicio -**Ingrese un valor del grupo de direcciones IP para que el servidor DHCP comience cuando emita direcciones IP. Si la primera dirección IP de su enrutador es 192.168.1.1, la dirección IP inicial debe ser 192.168.1.2 o mayor, pero menor que 192.168.1.254. **Recuentos de grupos de IP:**Ingrese la cantidad máxima de PC a las que desea que el servidor DHCP asigne direcciones IP. El valor predeterminado es 50 y el máximo es 253. **Tiempo de arrendamiento**-Ingrese el tiempo para determinar cuánto tiempo la IP

	Se puede utilizar la dirección asignada por el servidor DHCP. **Usar puerto LAN –**Especifique una IP para la subred de ruta IP. Si está habilitado, el servidor DHCP asignará la dirección IP automáticamente para los clientes que provienen de P1 y/o P2. Por favor marque la casilla de P1 y P2. **Usar dirección MAC -**Marque dicha casilla para especificar la dirección MAC. - **Dirección MAC -**Ingrese la dirección MAC del host uno por uno y haga clic en**Agregar**para crear una lista de hosts que se pueden asignar, eliminar o editar desde el grupo anterior. Establecer una lista de direcciones MAC para 2Dakota del NorteEl servidor DHCP ayudará al enrutador a asignar la dirección IP correcta de la subred correcta al host correcto. Entonces esos anfitriones en 2Dakota del Nortela subred no obtendrá una dirección IP que pertenezca a 1calle subred. **Agregar -**Ingrese la dirección MAC en los cuadros y haga clic en este botón para agregar. **Borrar**–Haga clic en él para eliminar la dirección MAC seleccionada. **Editar**–Haga clic en él para editar la dirección MAC seleccionada. **Cancelar**–Haga clic en él para cancelar el trabajo de agregar, eliminar y editar.

Cuando termine la configuración, haga clic en**DE ACUERDO**para guardar y salir de esta página.

Hay dos páginas de configuración para LAN1/LAN2/LAN3/LAN4/LAN5/LAN6/LAN7/LAN8/DMZ Port, Ethernet TCP/IP y DHCP Setup (basado en IPv4) y IPv6 Setup. Haga clic en la pestaña de cada tipo y consulte las siguientes explicaciones para obtener información detallada. A continuación se muestra la página de configuración de IPv6.

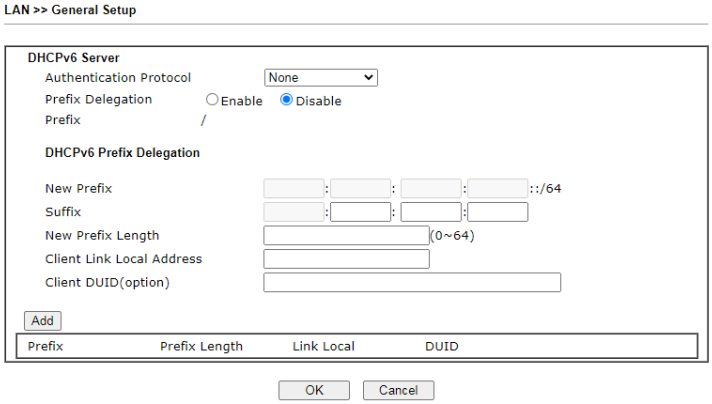
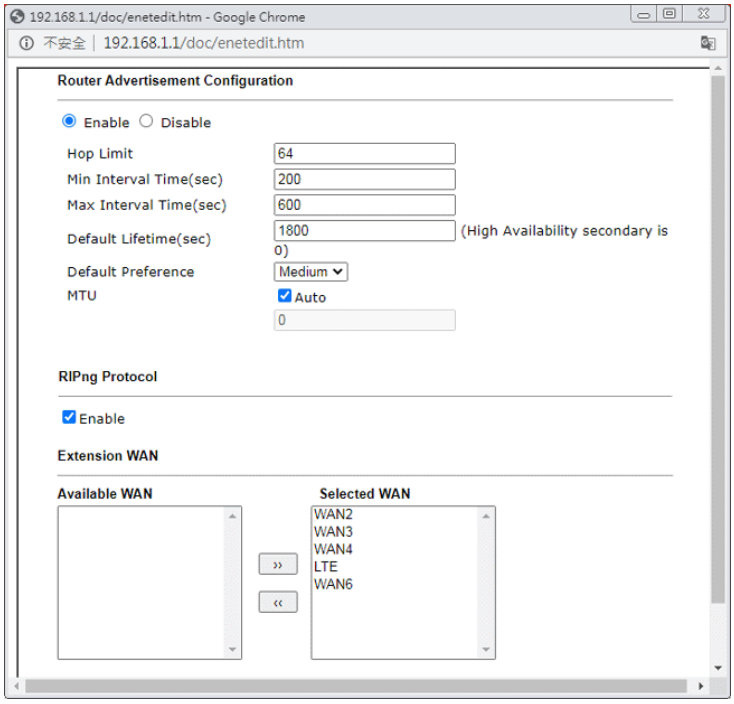


Proporciona 2 demonios para la configuración de direcciones IPv6 del lado LAN. Uno es**SLAAC**(apátrida) y el otro es**DHCPv6**(servidor con estado).

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Marque la casilla para habilitar la configuración de LAN 1 IPv6 Setup.
Interfaz primaria WAN	Utilice la lista desplegable para especificar una interfaz WAN para IPv6.
Dirección IPv6 estática configuración	**Dirección IPv6**–Escriba la dirección IPv6 estática para LAN. **Prefijo Longitud –**Ingrese el valor fijo para la longitud del prefijo. **Agregar -**Haga clic en él para agregar una nueva entrada.

	Borrar -Haga clic en él para eliminar una entrada existente.
Dirección local única (ULA) configuración	Las direcciones locales únicas (ULA) son direcciones IPv6 privadas asignadas a clientes LAN. **Apagado -**ULA está deshabilitado. **Prefijo ULA manual -**A los clientes de LAN se les asignarán ULA generados en función del prefijo ingresado manualmente. **Prefijo ULA automático -**A los clientes de LAN se les asignarán ULA utilizando un prefijo determinado automáticamente.
Dirección IPv6 actual Mesa	Muestra las direcciones IPv6 utilizadas actualmente.
Dirección IPv6 del servidor DNS	**Implementar cuando la WAN esté activa:**Los paquetes RA (anuncio de enrutador) se enviarán a la PC LAN con información del servidor DNS solo cuando la conexión de red mediante cualquiera de las interfaces WAN esté activa. **Permitir**–Los paquetes RA (anuncio de enrutador) se enviarán a la PC LAN con información del servidor DNS sin importar si la conexión WAN está activa o no. **Usar servidor DNS (WAN/Personalizado)**-Determina el servidor DNS para enviar los paquetes a través del servidor DNS WAN, el servidor DNS personalizado o ambos servidores. La configuración predeterminada es Ambos. Si se selecciona Servidor DNS WAN, el cliente LAN puede visitar Internet a través del servidor DNS dinámico ofrecido por el ISP para la transmisión de datos. Sin embargo, si se selecciona Servidor DNS personalizado, el cliente LAN puede visitar Internet a través del servidor DNS primario/secundario. Especifique la configuración para el servidor DNS primario/secundario o utilice los valores predeterminados. Cuando se elige Ambos, el cliente LAN puede visitar Internet a través del servidor DNS dinámico o de los servidores DNS personalizados. - **Servidor DNS primario**–Ingrese la dirección IPv6 para el servidor DNS primario. - **Servidor DNS secundario**–Ingrese otra dirección IPv6 para el servidor DNS si es necesario. **Desactivar**–No se utilizará el servidor DNS.
Gestión	Configura el indicador de configuración de dirección administrada (M-bit) en los anuncios de ruta. - **Apagado**-No se envía información de configuración mediante anuncios de ruta. - **SLAAC (sin estado) -**El bit M está desactivado. - **DHCPv6 (con estado**) - El bit M está configurado, lo que indica a los clientes de LAN que deben adquirir toda la información de configuración de IPv6 de un servidor DHCPv6. El servidor DHCPv6 puede ser el integrado en el Vigor2927 o un servidor DHCPv6 separado. **Otra opción (O-bit)**-Marque esta casilla para habilitar el bit O para obtener información adicional (p. ej., DNS) de DHCPv6.
Servidor DHCPv6	**Habilitar servidor**–Haga clic en él para habilitar el servidor DHCPv6. El servidor DHCPv6 podría asignar la dirección IPv6 a la PC de acuerdo con la configuración de la dirección IPv6 de inicio/fin. **Deshabilitar servidor**–Haga clic en él para deshabilitar el servidor DHCPv6. **Rango IPv6 automático:**Después de marcar la casilla, el enrutador Vigor asignará el rango IPv6 automáticamente. **Iniciar dirección IPv6/Dirección IPv6 final**–Introduzca el inicio y

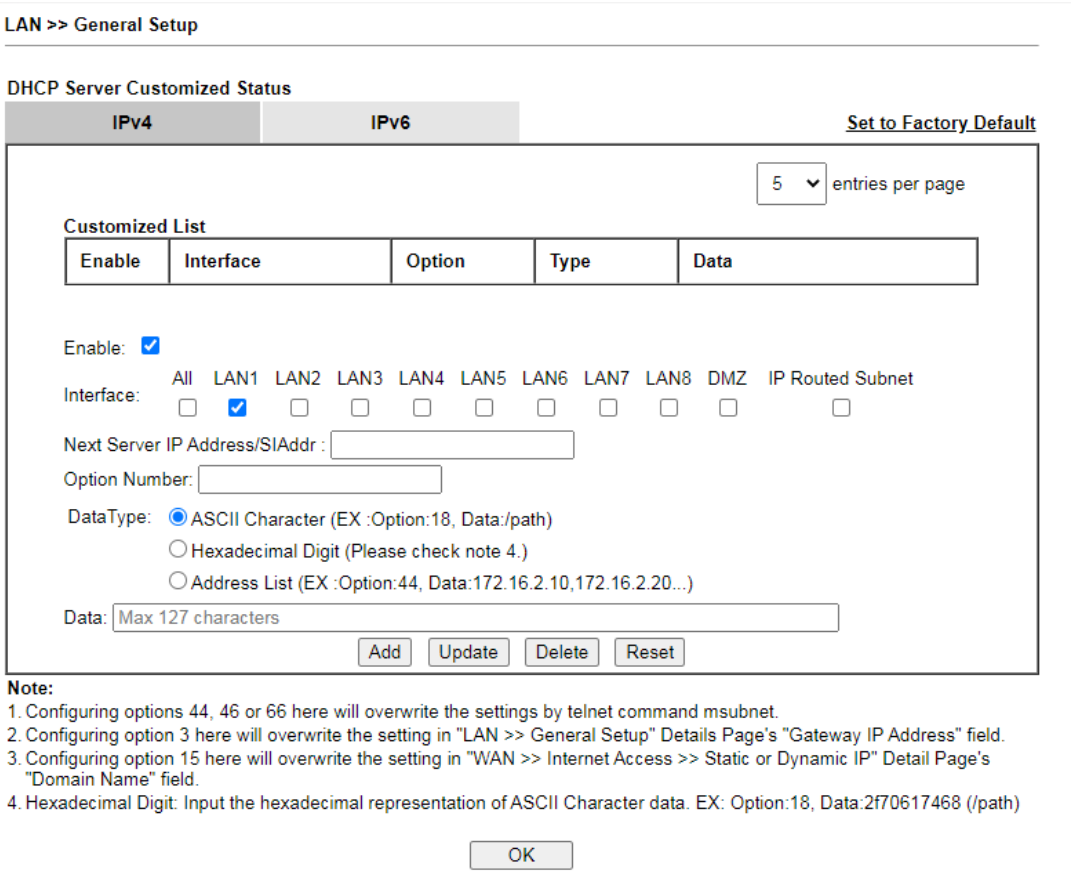
	dirección final para el servidor IPv6. **Configuración avanzada**–Haga clic en el botón Editar para configurar los ajustes avanzados de IPv6 para el servidor DHCPv6. 
Configuración avanzada	La página Configuración avanzada tiene configuraciones adicionales para el anuncio del enrutador y habilita varias WAN para el tráfico IPv6.  **Configuración de anuncios de enrutador**–Hacer clic**Permitir**para habilitar el servidor de publicidad del enrutador. El daemon de anuncio de enrutador envía mensajes de anuncio de enrutador, especificados por RFC 2461, a una LAN Ethernet local periódicamente y cuando lo solicita un nodo que envía un mensaje de solicitud de enrutador. Estos mensajes son necesarios para la configuración automática sin estado de IPv6. **Desactivar**–Haga clic en él para deshabilitar el servidor de publicidad del enrutador. **Límite de lúpulo –**El valor es necesario para el dispositivo detrás del enrutador cuando se utiliza IPv6. **Tiempo de intervalo mín./máx. (seg.) –**Define el intervalo (entre el tiempo mínimo y el tiempo máximo) para el envío de paquetes RA (anuncio de enrutador). **Vida útil predeterminada (seg) –**Dentro de dicho período de tiempo, el enrutador Vigor puede tratarse como la puerta de enlace predeterminada. **Preferencia predeterminada:**Determina la prioridad del host.

	detrás del enrutador cuando se transmiten paquetes RA (anuncio de enrutador). **MTU –**Significa Unidad de transmisión máxima por paquete. Si**Auto**está seleccionado, el enrutador determinará el valor de MTU para LAN. **Protocolo RIPng –**RIPng (RIP next generation) ofrece las mismas funciones y beneficios que IPv4 RIP v2. **Extensión WAN –**Además de la WAN predeterminada utilizada para el tráfico IPv6 especificada en la Interfaz principal de WAN en la página Configuración de LAN IPv6, se pueden seleccionar WAN adicionales para transportar tráfico IPv6 habilitándolas en la sección WAN de extensión. **WAN disponible**–WAN adicionales disponibles pero no seleccionadas actualmente para transportar tráfico IPv6. **WAN seleccionada**–WAN adicionales seleccionadas para transportar tráfico IPv6.

Después de realizar cambios en la página de configuración avanzada, haga clic en el botón**DE ACUERDO**para conservar los cambios y volver a la página de configuración de LAN IPv6. Asegúrese de hacer clic en Aceptar en la página Configuración LAN IPv6 o, de lo contrario, no se guardarán los cambios realizados en la página Configuración avanzada.

II-2-1-5 Opciones del servidor DHCP

Las opciones de DHCP se pueden configurar haciendo clic en el**Opción de servidor DHCP**botón en el**LAN**>> **Configuración general**pantalla.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Lista personalizada	Muestra todas las opciones de DHCP que se han configurado en el sistema.

Permitir	Si se selecciona, se habilita la entrada de la opción DHCP. Si no se selecciona, la entrada de la opción DHCP está deshabilitada.
Interfaz	Interfaz(s) LAN a las que se aplica esta entrada.
Próxima IP del servidor Dirección/dirección SI	Anula la dirección IP del próximo servidor DHCP (opción 66 de DHCP) proporcionada por el servidor DHCP.
Número de opción	Número de opción de DHCP (p. ej., 100).
Tipo de datos	Tipo de datos en el campo Datos: **Carácter ASCII**-Una cadena de texto. Ejemplo: /ruta. **Dígito hexadecimal -**Una cadena hexadecimal. Los caracteres válidos son del 0 al 9 y de la a a la f. Ejemplo: 2f70617468. **Lista de direcciones -**Una o más direcciones IPv4, delimitadas por comas.
Datos	Datos de esta opción DHCP.

Para agregar una entrada de opción DHCP desde cero, borre los campos de entrada de datos (**Habilitar, interfaz, número de opción, tipo de datos**y**Datos**) haciendo clic en Restablecer. Después de completar los valores, haga clic en**Agregar** para crear la nueva entrada.

Para agregar una entrada de opción DHCP modelada a partir de una entrada existente, haga clic en la entrada del modelo en **Lista personalizada**. Los campos de entrada de datos se completarán con valores de la entrada del modelo. Después de realizar todos los cambios necesarios para la nueva entrada, haga clic en**Agregar**para crearlo

Para modificar una entrada de opción DHCP existente, haga clic en ella en**Lista personalizada**. Los campos de entrada de datos se completarán con los valores actuales de la entrada. Después de realizar todos los cambios necesarios, haga clic en **Actualizar**para guardar los cambios.

Para eliminar una entrada de opción DHCP, haga clic en ella en**Lista personalizada**y luego haga clic en**Borrar**.

II-2-2 VLAN

Las redes de área local virtuales (VLAN) le permiten subdividir su LAN para facilitar la administración o mejorar la seguridad de la red.

Seleccionar**LAN>>VLAN**desde la barra de menú de la interfaz de usuario web para abrir la página de configuración de VLAN.

VLAN etiquetada

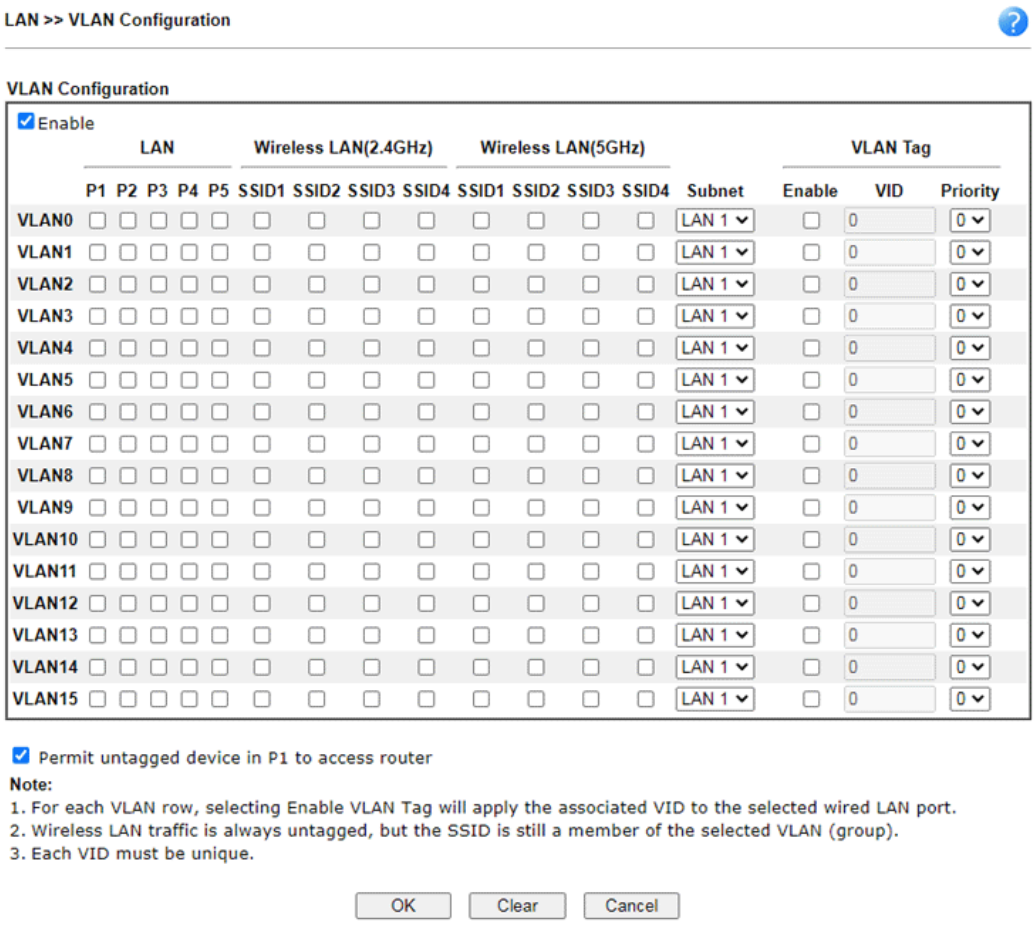
Las VLAN etiquetadas (802.1q) pueden marcar datos con un identificador de VLAN. Este identificador se puede llevar a través de un conmutador Ethernet hacia puertos específicos. Los clientes de VLAN específicos también pueden recoger este identificador cuando se acaba de pasar a la LAN. Puede establecer las prioridades para QoS del lado LAN. Puede asignar cada una de las VLAN a cada una de las diferentes subredes de IP que el enrutador también puede estar operando, para proporcionar aún más aislamiento. Dicha funcionalidad es**subred múltiple basada en etiquetas**.

VLAN basada en puerto

En relación con la VLAN basada en etiquetas que agrupa a los clientes con un identificador, la VLAN basada en puertos utiliza puertos físicos (P1 ~ P4) para separar a los clientes en diferentes grupos de VLAN.

La función de LAN virtual le brinda una forma muy conveniente de administrar hosts agrupándolos según el puerto físico. La subred múltiple puede permitir que las pequeñas empresas tengan un aislamiento mucho mejor para aplicaciones de ocupación múltiple. Ir a**LAN**página y seleccione**VLAN**. Aparecerá la siguiente página. Hacer clic**Permitir**para invocar la función VLAN.

A continuación se muestra una página de ejemplo en Vigor2927ac:



Información	Las configuraciones en esta página solo se aplican al puerto LAN pero no al puerto WAN.

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Haga clic en él para habilitar la configuración de VLAN.
LAN	**P1-P5**–Verifique los puertos LAN para agruparlos bajo la VLAN seleccionada.
LAN inalámbrica (2,4 GHz)	**SSID1 – SSID4 –**Marque las casillas SSID para agruparlos bajo la VLAN seleccionada.
LAN inalámbrica (5 GHz)	**SSID1 – SSID4 –**Marque las casillas SSID para agruparlos bajo la VLAN seleccionada.
subred	Elija uno de ellos para realizar la asignación de VLAN seleccionada solo a la subred especificada. Por ejemplo, LAN1 se especifica para VLAN0. Significa que las PC agrupadas en VLAN0 pueden obtener las direcciones IP especificadas por la subred.
Etiqueta VLAN	**Permitir**–Marque la casilla para habilitar la función de VLAN con etiqueta. El enrutador agregará un número de VLAN específico a todos los paquetes en la LAN mientras los envía. Ingrese el valor de la etiqueta y especifique la prioridad para los paquetes enviados por LAN. **VÍDEO**–Ingrese el valor como el número de ID de VLAN. El rango es de 0 a 4095. Los VID deben ser únicos. **Prioridad**–Los valores válidos son de 0 a 7, donde 1 tiene la prioridad más baja, seguido de 0 y finalmente de 2 a 7 en orden creciente de prioridad.
Permitir que el dispositivo sin etiquetar en P1 acceda al enrutador	Seleccione para permitir que los hosts sin etiquetar conectados al puerto LAN P1 accedan al enrutador. En caso de que haya configurado incorrectamente la funcionalidad de VLAN, aún podrá acceder al enrutador a través de la interfaz de usuario web y los shells de telnet y SSH para ajustar la configuración.

Información	Deje una VLAN sin etiquetar al menos para evitar que no se conecte al enrutador Vigor debido a un error inesperado.

Enrutamiento entre LAN

El enrutador Vigor admite hasta 15 VLAN. Cada VLAN se puede configurar para usar uno o más puertos Ethernet e identificadores de conjunto de servicios (SSID) de LAN inalámbrica. Dentro de la cuadrícula de VLAN (filas horizontales) e interfaces LAN (columnas verticales),

- todos los hosts dentro de la misma VLAN (fila horizontal) son visibles entre sí
- todos los hosts conectados a la misma interfaz LAN o WLAN (columna vertical) son visibles entre sí si
  - pertenecen a la misma VLAN, o
  - pertenecen a diferentes VLAN y el enrutamiento entre LAN (LAN>>Configuración general) entre ellas está habilitado (ver más abajo).

Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5	LAN 6	LAN 7	LAN 8	DMZ Port
LAN 1	☑	☐	☐	☐	☐	☐	☐	☐	☐
LAN 2	☑	☑	☐	☐	☐	☐	☐	☐	☐
LAN 3	☑	☐	☑	☐	☐	☐	☐	☐	☐
LAN 4	☑	☐	☐	☑	☐	☐	☐	☐	☐
LAN 5	☐	☐	☐	☐	☑	☐	☐	☐	☐
LAN 6	☐	☐	☐	☐	☐	☑	☐	☐	☐
LAN 7	☐	☐	☐	☐	☐	☐	☑	☐	☐
LAN 8	☐	☐	☐	☐	☐	☐	☐	☑	☐
DMZ Port	☐	☐	☐	☐	☐	☐	☐	☐	☑

El enrutamiento entre LAN permite interconectar o aislar diferentes subredes de LAN. Solo está disponible cuando la funcionalidad VLAN está habilitada. En la matriz de enrutamiento entre LAN, una casilla de verificación seleccionada significa que las 2 LAN que se cruzan pueden comunicarse entre sí.

La serie Vigor2927 presenta un sistema VLAN enormemente flexible. En su forma más simple, cada uno de los puertos LAN Gigabit se puede aislar entre sí, por ejemplo, para alimentar a diferentes empresas o departamentos, pero manteniendo su tráfico local completamente separado.

Configuración de VLAN basada en puerto para clientes inalámbricos y no inalámbricos

1. Todos los clientes de la red cableada se clasifican en el grupo VLAN0 en la subred 192.168.1.0/24 (LAN1).
2. Todos los clientes de la red inalámbrica se clasifican en el grupo VLAN1 en la subred 192.168.2.0/24 (LAN2).
3. Abierto**LAN>>Configuración de VLAN**. Marque las casillas de acuerdo con la declaración en el paso 1 y el Paso 2.

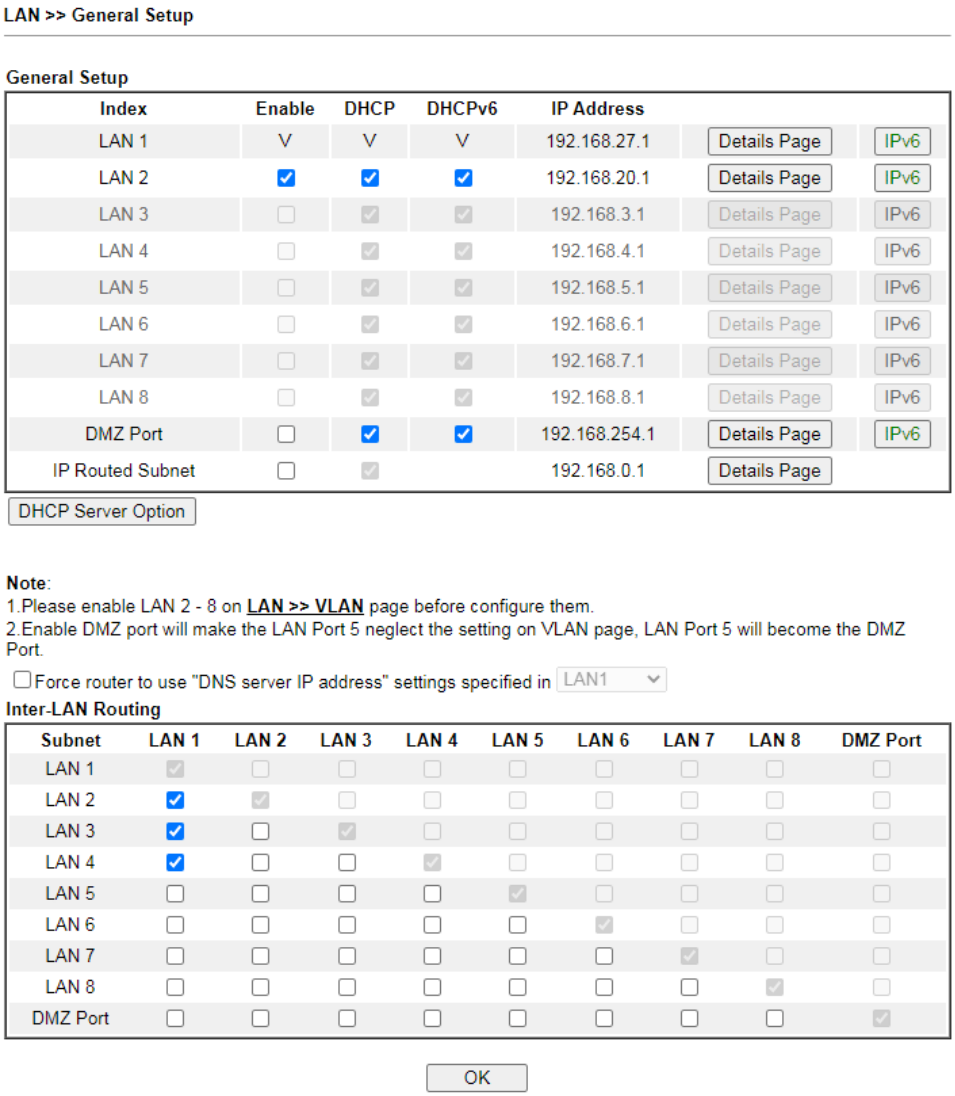
LAN >> VLAN Configuration

VLAN Configuration

☑ Enable

	LAN					Wireless LAN(2.4GHz)				Wireless LAN(5GHz)					VLAN Tag		
	P1	P2	P3	P4	P5	SSID1	SSID2	SSID3	SSID4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	LAN1	☐	0	0
VLAN1	☐	☐	☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	LAN2	☑	20	0
VLAN2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	LAN3	☐	0	0
VLAN3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	LAN4	☐	0	0
VLAN4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	LAN1	☐	0	0

4. Haga clic en**DE ACUERDO**.
5. Abierto**LAN>>Configuración general**. Si desea permitir que los clientes de ambos grupos se comuniquen entre sí, simplemente active**Enrutamiento entre LAN**marcando la casilla entre**LAN1** y**LAN2.**



LAN >> General Setup

General Setup

Index	Enable	DHCP	DHCPv6	IP Address		
LAN 1	V	V	V	192.168.27.1	Details Page	IPv6
LAN 2	☑	☑	☑	192.168.20.1	Details Page	IPv6
LAN 3	☐	☑	☑	192.168.3.1	Details Page	IPv6
LAN 4	☐	☑	☑	192.168.4.1	Details Page	IPv6
LAN 5	☐	☑	☑	192.168.5.1	Details Page	IPv6
LAN 6	☐	☑	☑	192.168.6.1	Details Page	IPv6
LAN 7	☐	☑	☑	192.168.7.1	Details Page	IPv6
LAN 8	☐	☑	☑	192.168.8.1	Details Page	IPv6
DMZ Port	☐	☑	☑	192.168.254.1	Details Page	IPv6
IP Routed Subnet	☐	☑		192.168.0.1	Details Page	

DHCP Server Option

Note:
1.Please enable LAN 2 - 8 on LAN >> VLAN page before configure them.
2.Enable DMZ port will make the LAN Port 5 neglect the setting on VLAN page, LAN Port 5 will become the DMZ Port.

☐ Force router to use "DNS server IP address" settings specified in LAN1

Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5	LAN 6	LAN 7	LAN 8	DMZ Port
LAN 1	☑	☐	☐	☐	☐	☐	☐	☐	☐
LAN 2	☑	☑	☐	☐	☐	☐	☐	☐	☐
LAN 3	☑	☐	☑	☐	☐	☐	☐	☐	☐
LAN 4	☑	☐	☐	☑	☐	☐	☐	☐	☐
LAN 5	☐	☐	☐	☐	☑	☐	☐	☐	☐
LAN 6	☐	☐	☐	☐	☐	☑	☐	☐	☐
LAN 7	☐	☐	☐	☐	☐	☐	☑	☐	☐
LAN 8	☐	☐	☐	☐	☐	☐	☐	☑	☐
DMZ Port	☐	☐	☐	☐	☐	☐	☐	☐	☑

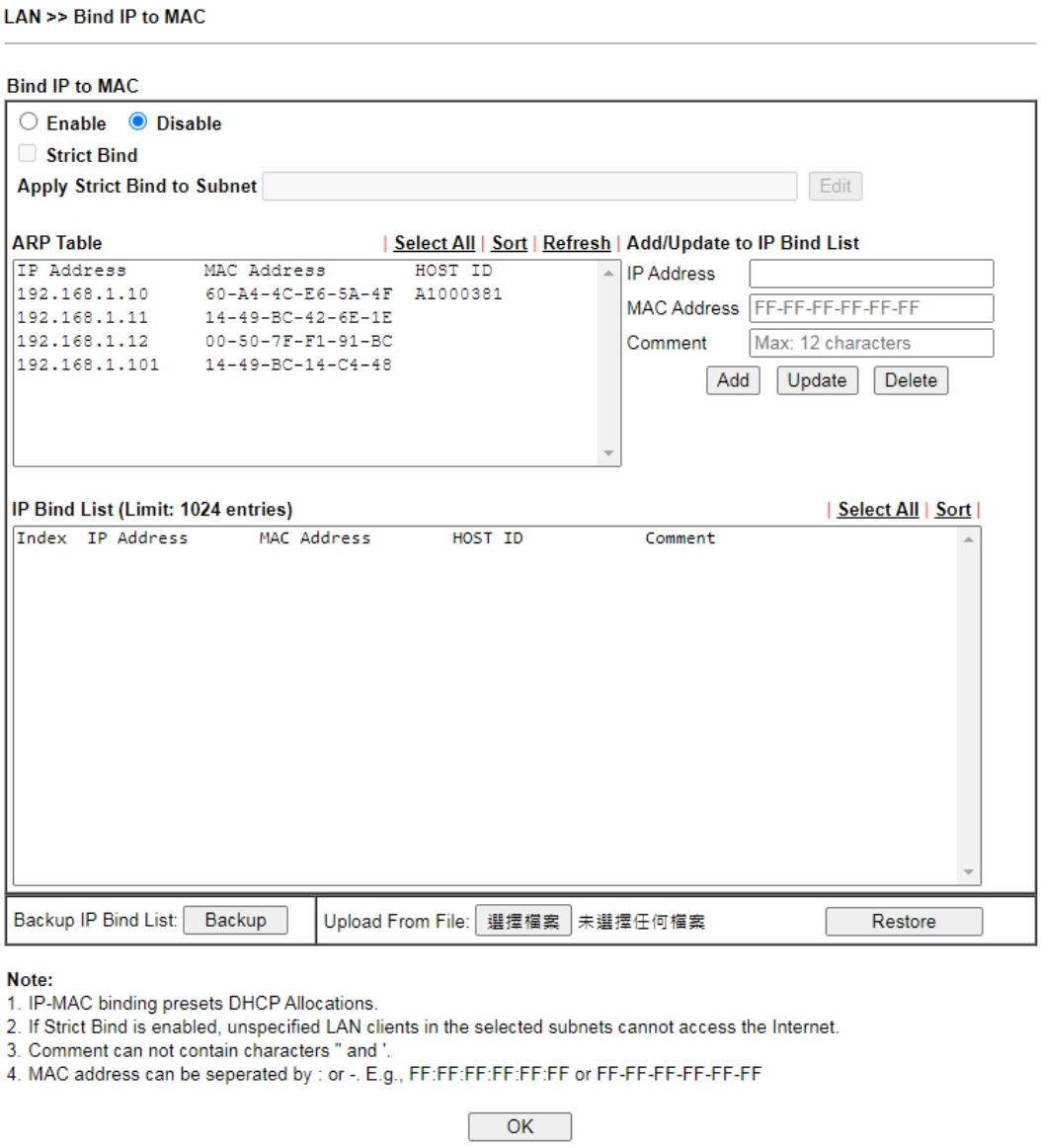
OK

El enrutador Vigor admite hasta seis subredes IP privadas en LAN. Cada uno puede ser independiente (aislado) o común (capaz de comunicarse entre sí). Esto es ideal para aplicaciones departamentales o de ocupación múltiple.

II-2-3 Vincular IP a MAC

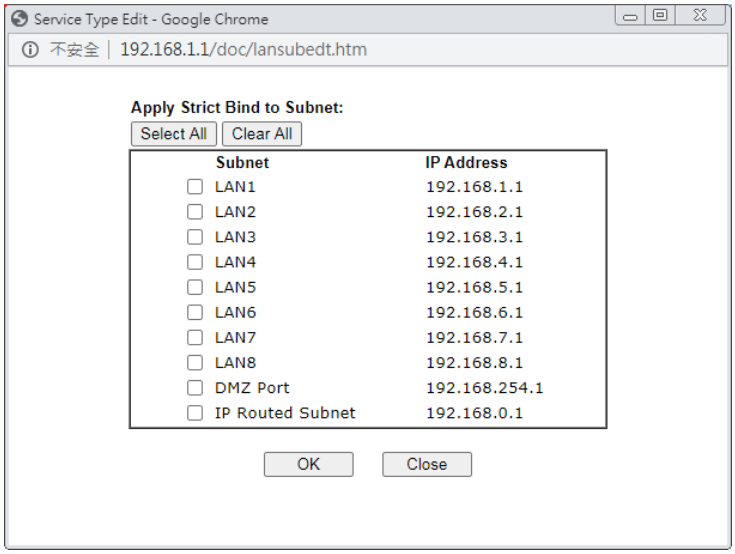
Esta función se utiliza para vincular la dirección IP y MAC en LAN para tener un control de fortalecimiento en la red. Con la función Vincular IP a MAC, puede reservar direcciones IP de LAN para clientes de LAN. Cada dirección IP reservada está asociada con una dirección de control de acceso a medios (MAC).

Hacer clic**LAN**y haga clic**Vincular IP a MAC**para abrir la página de configuración.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Haga clic en este botón de radio para invocar esta función. Sin embargo, IP/MAC que no se encuentra en la lista de vinculación de IP también puede conectarse a Internet.
Desactivar	Haga clic en este botón de opción para desactivar esta función. Todas las configuraciones en esta página no serán válidas.
Lazo estricto	Marque la casilla para bloquear la conexión de la IP/MAC que no aparece en la Lista de vinculación de IP. A los clientes LAN se les asignarán direcciones IP de acuerdo con la

	Asociaciones de direcciones MAC a IP en esta página. Al cliente LAN cuya dirección MAC no se haya vinculado a una dirección IP se le negará el acceso a la red. **Nota**: Antes de seleccionar**Lazo estricto**, asegúrese de que al menos una dirección MAC válida se haya vinculado a una dirección IP. De lo contrario, ningún cliente LAN tendrá acceso a la red y no será posible conectarse al enrutador para realizar cambios en su configuración. **Aplicar enlace estricto a la subred**–Elija la(s) subred(es) para aplicar las reglas de Bind IP to MAC. 
Tabla ARP	Esta tabla es la tabla LAN ARP de este enrutador. La información de IP y MAC se mostrará en este campo. Cada par de direcciones IP y MAC enumeradas en la tabla ARP se puede seleccionar y agregar a la lista de enlaces de IP haciendo clic en**Agregar**abajo.
Seleccionar todo	Seleccione todas las entradas en la tabla ARP para su manipulación.
Clasificar	Reordene la entrada según la dirección IP.
Actualizar	Actualice la tabla ARP que se muestra a continuación para obtener la información más reciente de la tabla ARP.
Agregar o actualizar a la lista de vinculación de IP	**Dirección IP**–Introduzca la dirección IP que se asociará con una dirección MAC. **Dirección MAC**–Ingrese la dirección MAC de la interfaz de red del cliente LAN. **Comentario**–Escriba una breve descripción de la entrada.
Agregar	Le permite agregar el que elija de la tabla ARP o la dirección IP/ MAC ingresada**Agregar y editar**a la mesa de**Lista de enlaces de IP**.
Actualizar	Te permite editar y modificar la dirección IP seleccionada y la dirección MAC que creaste antes.
Borrar	Puede eliminar cualquier elemento enumerado en**Lista de enlaces de IP**. Simplemente haga clic y seleccione uno, y haga clic en**Borrar**. El elemento seleccionado será eliminado de la**Lista de enlaces de IP**.
Lista de enlaces de IP	Muestra una lista para el enlace de IP a la información de MAC.
Lista de vinculación de IP de copia de seguridad	Hacer clic**Respaldo**e ingrese un nombre de archivo para hacer una copia de seguridad de IP Bind List en un archivo.
Cargar desde archivo	Hacer clic**Navegar...**para seleccionar un archivo de copia de seguridad de la lista IP Bind. Hacer clic

	Restaurarpara restaurar la copia de seguridad y sobrescribir la lista existente.

Información

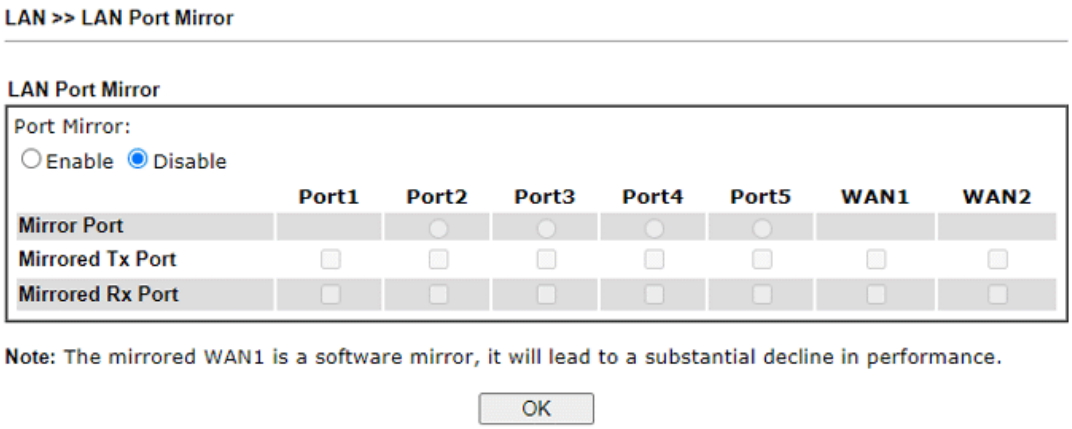
Antes de seleccionar Strict Bind, debe vincular un conjunto de direcciones IP/MAC para una PC. Si no, ninguna de las PC puede acceder a Internet. Y es posible que no se acceda a la interfaz de usuario web del enrutador.

Cuando termine la configuración, haga clic en**DE ACUERDO**para guardar la configuración.

II-2-4 Espejo de puerto LAN

El**Espejo de puerto LAN**La función permite que el tráfico de red de puertos LAN seleccionados se reenvíe a otro puerto LAN para su análisis. Esto es útil para aplicar políticas, detectar accesos no autorizados, monitorear el rendimiento de la red, etc.

Seleccionar**LAN>>Espejo de puerto LAN**desde la barra de menú de la Web UI para que aparezca la**Espejo de puerto LAN** página de configuración



Los ajustes disponibles se explican a continuación:

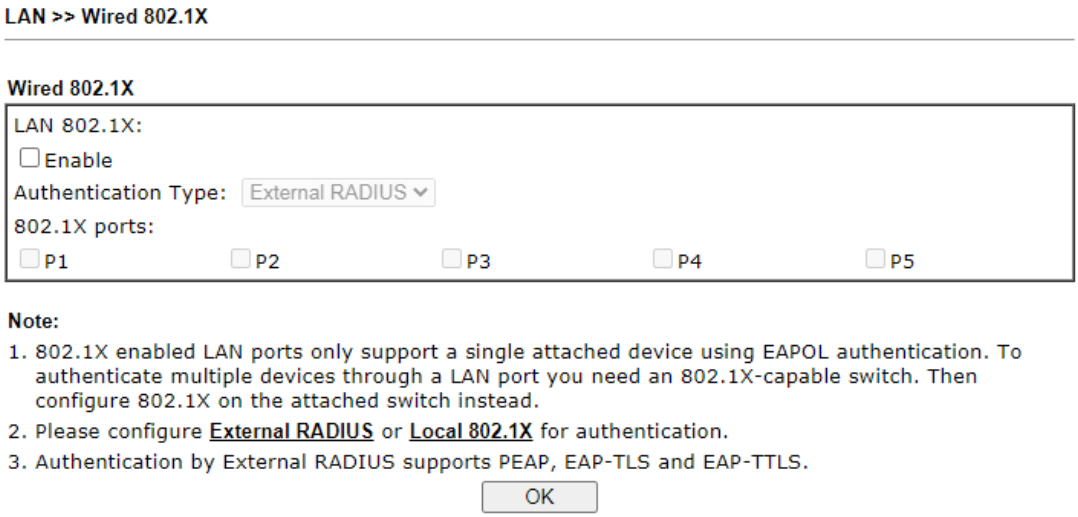
Artículo	Descripción
Espejo de puerto	Habilita o deshabilita la duplicación de puertos LAN.
Puerto espejo	Se selecciona uno y solo un puerto como puerto espejo, al que se reenviará el tráfico.
Puerto Tx duplicado	Puerto(s) cuyo tráfico saliente se reenviará al puerto espejo.
Puerto Rx duplicado	Puerto(s) cuyo tráfico entrante se reenviará al puerto espejo.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

II-2-5 Cableado 802.1x

802.1X con cableproporciona autenticación para los clientes que deseen conectarse a la LAN por Ethernet. Solo se puede autenticar un cliente en cada puerto LAN.

Seleccionar**LAN>>Alámbrico 802.1X**desde la barra de menú de la Web UI para que aparezca la**802.1X con cable** página de configuración



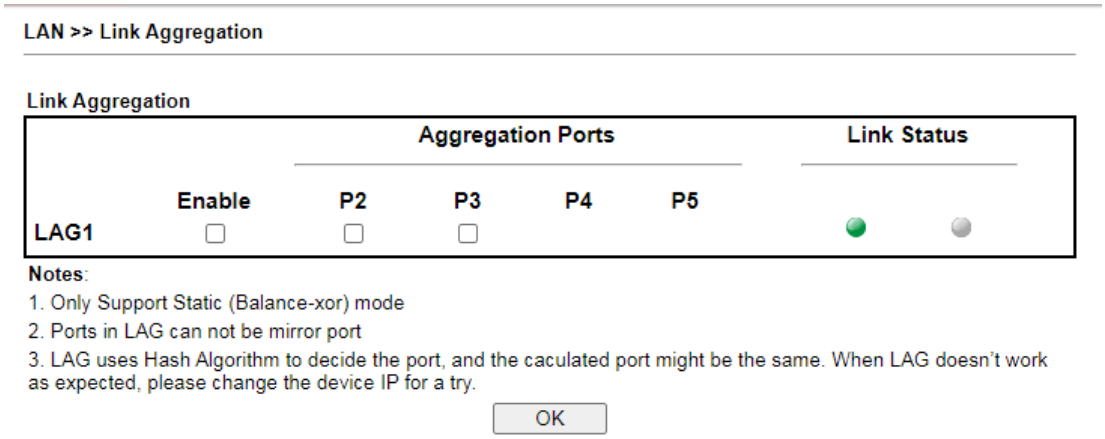
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Marque la casilla para habilitar la función LAN 802.1x.
tipo de autenticación	**RADIO externo -**Se utilizará un servidor RADIUS externo para la autenticación 802.1X. Ir a**Aplicaciones >> RADIUS / TACACS+>>RADIUS externo**para especificar el servidor RADIUS. **802.1X locales**-Use la base de datos de usuarios en el enrutador para autenticar a los clientes. Ir a**Gestión de usuarios >> Perfil de usuario** para configurar usuarios ingresando nombres de usuario, contraseñas y asegúrese de que el servicio Local 802.1X esté habilitado para los perfiles.
Puertos 802.1X	La autenticación 802.1X estará disponible para los puertos LAN seleccionados.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

II-2-6 Agregación de enlaces

LAG significa Grupo de agregación de enlaces que agrupa algunos puertos físicos para crear una única ruta de datos de gran ancho de banda. Por lo tanto, puede implementar el intercambio de carga de tráfico entre los puertos miembros de un grupo para mejorar la confiabilidad de la conexión.



Los ajustes disponibles se explican a continuación:

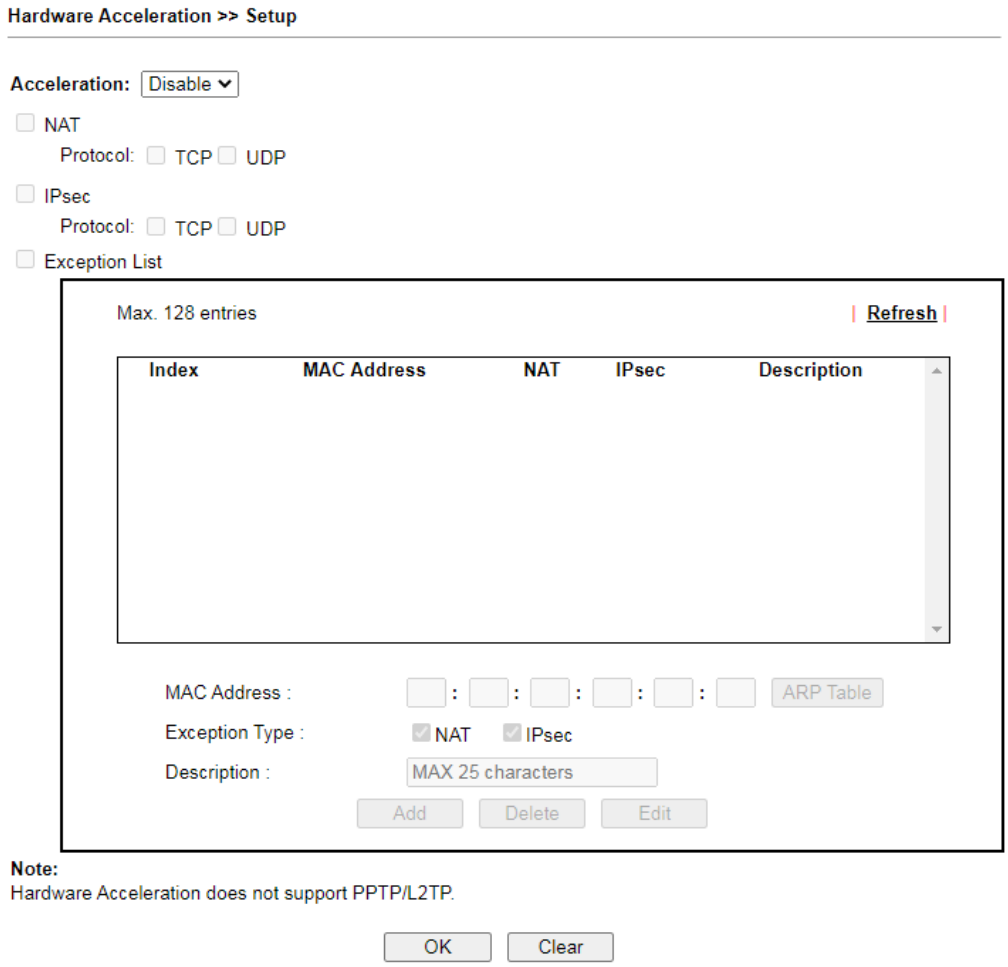
Artículo	Descripción
Permitir	Marque la casilla para habilitar la función LAN 802.1x.
Puertos de agregación	Seleccione el número de puerto (al menos dos puertos) para crear una ruta de datos de gran ancho de banda. Actualmente, los puertos disponibles para seleccionar incluyen P2 y P3.
Estado del enlace	La luz verde significa que el puerto LAG está conectado mediante cable(s) Ethernet.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

Aceleración de hardware II-3

La aceleración de hardware también se llama**APP**en DrayTek porque se basa en**Motor de procesamiento de protocolos (PPE)**de Infineon. Solo puede admitir 4096 sesiones para el tráfico de red (ENTRADA y SALIDA).

Cuando el tráfico de datos es intenso y la transmisión de datos es cada vez más lenta, puede configurar esta página para acelerar la transmisión de datos por el propio hardware. Abierto **Aceleracion de hardware**para acceder a la siguiente página:



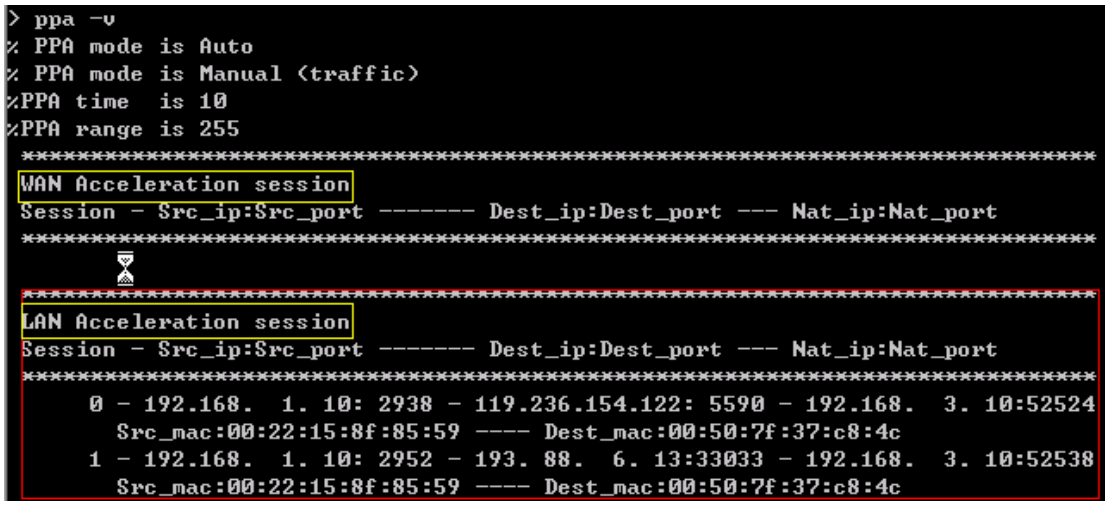
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Aceleración	**Desactivar -**La configuración predeterminada. **Permitir -**Elija habilitar la función de aceleración de hardware.
NAT	Seleccione TCP y/o UDP.
IPsec	Seleccione TCP y/o UDP.
Lista de excepciones	Si desea restringir que algunos usuarios/clientes transmitan datos a través del enrutador utilizando la función de aceleración de hardware, marque esta casilla para crear una lista de exclusión. **Dirección MAC -**Introduzca la dirección MAC del cliente. **Tabla ARP -**Haga clic para seleccionar el cliente que aparece en la tabla ARP.

	Luego, la dirección MAC del cliente seleccionado se mostrará en el campo Dirección MAC. **Tipo de excepción -**Seleccione NAT y/o IPsec. **Descripción -**Introduzca una breve explicación para el cliente seleccionado.

Comprobación del estado de PPA

Para comprobar si la regla de PPA funciona o no, un usuario puede iniciar sesión en la serie Vigor2927 mediante telnet. El usuario puede ver cuántas sesiones se están transfiriendo en cada dirección de la tabla PPA después de ingresar "**ppa-v**".



II-4 NAT

Por lo general, el enrutador sirve como un enrutador NAT (traducción de direcciones de red). NAT es un mecanismo en el que una o más direcciones IP privadas se pueden asignar a una sola pública. La dirección IP pública generalmente la asigna su ISP, por lo que es posible que le cobren. Las direcciones IP privadas se reconocen solo entre hosts internos.

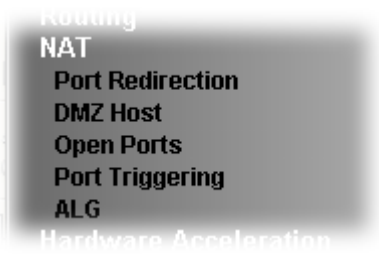
Cuando los paquetes salientes destinados a algún servidor público en Internet lleguen al enrutador NAT, el enrutador cambiará su dirección de origen a la dirección IP pública del enrutador, seleccionará el puerto público disponible y luego lo reenviará. Al mismo tiempo, el enrutador listará una entrada en una tabla para memorizar esta relación dirección/mapeo de puertos. Cuando la respuesta del servidor público, el tráfico entrante, por supuesto, está destinado a la dirección IP pública del enrutador y el enrutador hará la inversión según su tabla. Por lo tanto, el host interno puede comunicarse con el host externo sin problemas.

El beneficio de la NAT incluye:

- **Ahorre costos al aplicar una dirección IP pública y aplique un uso eficiente de la dirección IP.**NAT permite que las direcciones IP internas de los hosts locales se traduzcan en una dirección IP pública, por lo que solo puede tener una dirección IP en nombre de todos los hosts internos.
- **Mejore la seguridad de la red interna ocultando la dirección IP.**Hay muchos ataques dirigidos a las víctimas en función de la dirección IP. Dado que el atacante no puede conocer ninguna dirección IP privada, la función NAT puede proteger la red interna.

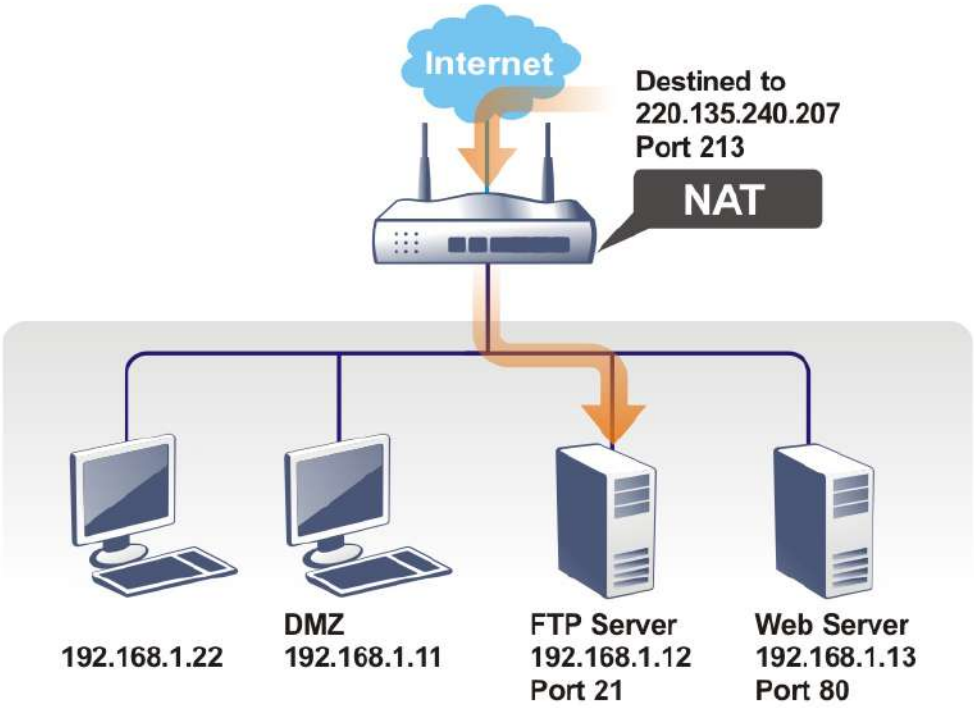
Información

En la página NAT, verá la dirección IP privada definida en RFC-1918. Usualmente usamos la subred 192.168.1.0/24 para el enrutador. Como se indicó anteriormente, la instalación NAT puede asignar una o más direcciones IP y/o puertos de servicio a diferentes servicios especificados. En otras palabras, la función NAT se puede lograr mediante el uso de métodos de mapeo de puertos.



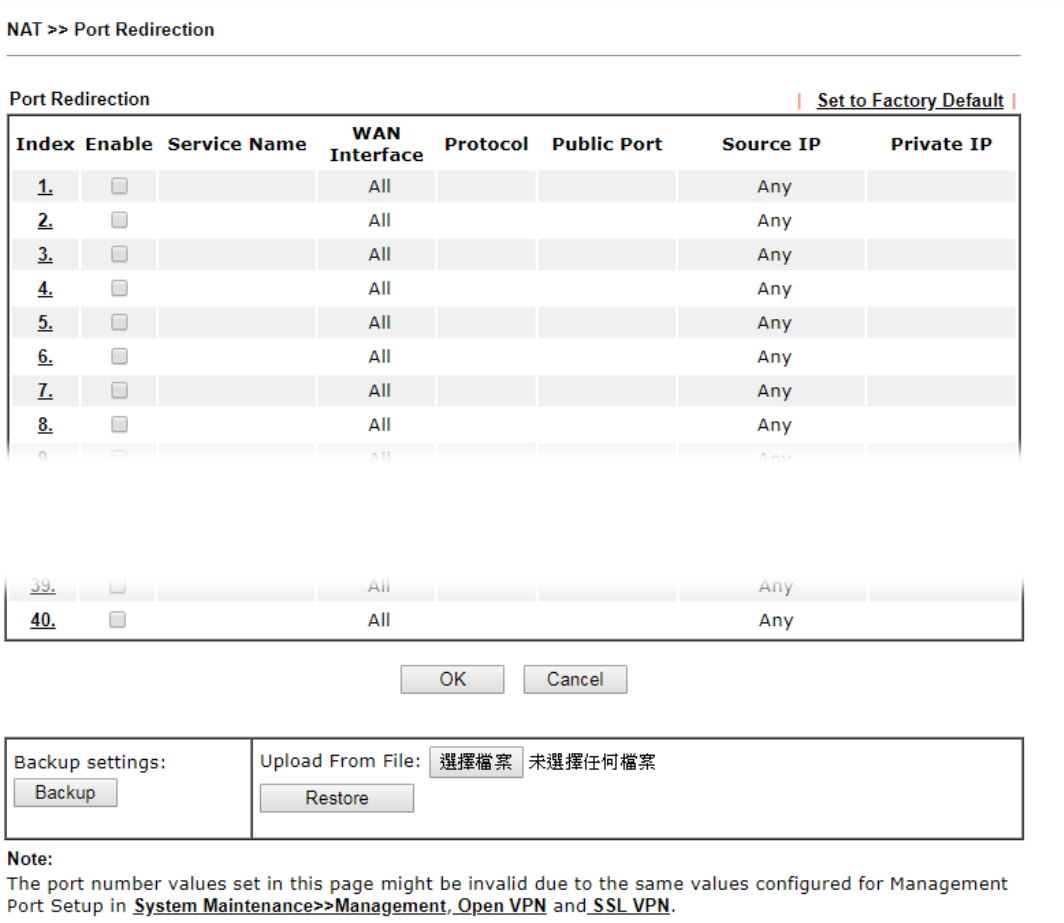
II-4-1 Redirección de puertos

La redirección de puertos generalmente se configura para el servicio relacionado con el servidor dentro de la red local (LAN), como servidores web, servidores FTP, servidores de correo electrónico, etc. En la mayoría de los casos, necesita una dirección IP pública para cada servidor y esta IP pública dirección/nombre de dominio son reconocidos por todos los usuarios. Dado que el servidor está realmente ubicado dentro de la LAN, la red está bien protegida por NAT del enrutador e identificada por su puerto/dirección IP privada, el objetivo de la función Redirección de puertos es reenviar todas las solicitudes de acceso con direcciones IP públicas de usuarios externos a la asignación de dirección IP privada/ puerto del servidor.



La redirección de puertos solo se puede aplicar al tráfico entrante.

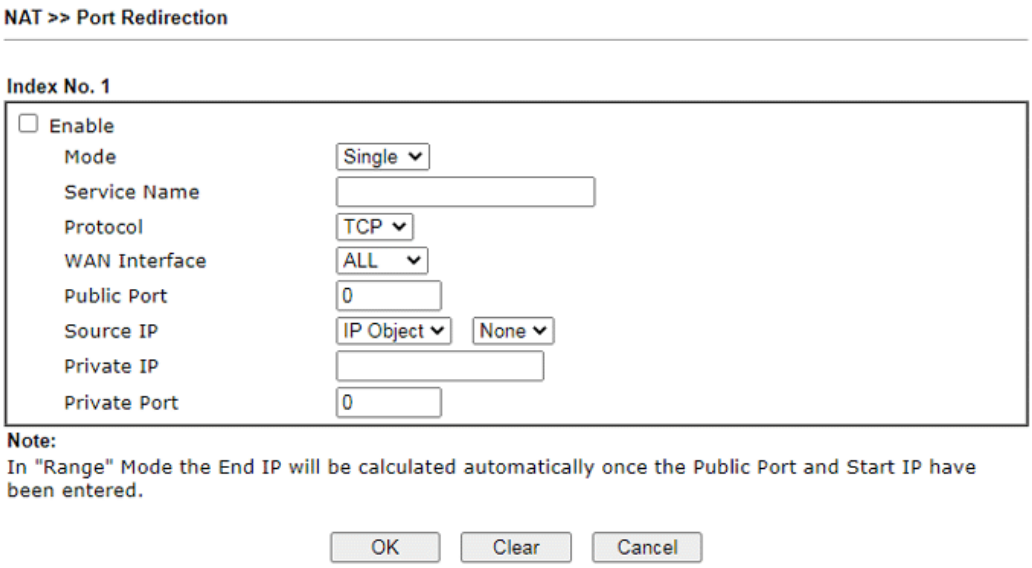
Para utilizar esta función, vaya a**NAT**pagina y elige**Redirección de puertos**Página web. El**Tabla de redirección de puertos**proporciona 40 entradas de mapeo de puertos para los hosts internos.



Cada elemento se explica de la siguiente manera:

Artículo	Descripción
Índice	Muestra el número del perfil.
Permitir	Marque la casilla para habilitar el perfil de redirección de puertos.
Nombre del Servicio	Muestra la descripción del servicio de red específico.
Interfaz WAN	Muestra la dirección IP de WAN utilizada por el perfil.
Protocolo	Muestra el protocolo de la capa de transporte (TCP o UDP).
Puerto Público	Muestra el número de puerto que será redirigido al especificado**IP privada y puerto**del anfitrión interno.
IP de origen	Muestra el objeto IP de la IP de origen.
ip privada	Muestra la dirección IP del host interno que proporciona el servicio.
Respaldo	Haga clic en él para hacer una copia de seguridad de la configuración de la redirección de puertos.
Restaurar	Haga clic en él para restaurar la configuración de la redirección de puertos. Antes de hacer clic, asegúrese de cargar el archivo de configuración en el enrutador Vigor.

Presione cualquier número debajo de Índice para acceder a la página siguiente para configurar la redirección de puertos.



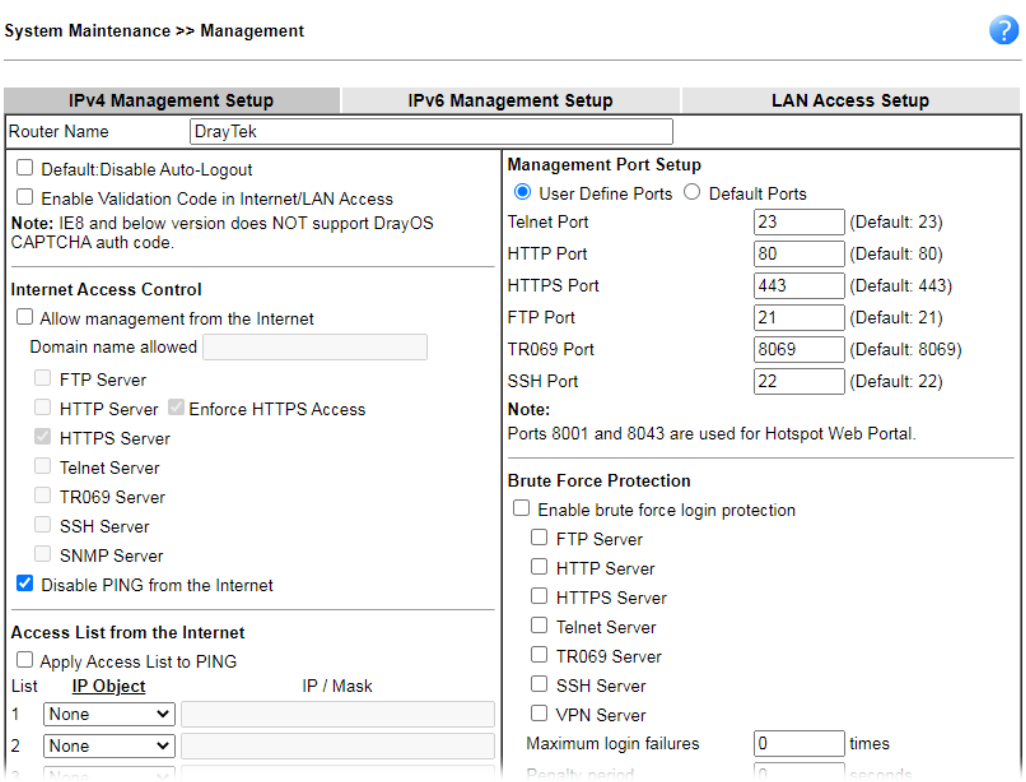
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Marque esta casilla para habilitar dicha configuración de redirección de puertos.
Modo	Aquí se proporcionan dos opciones (Single y Range) para que usted elija. Para establecer un rango para el servicio específico, seleccione **Rango**. En el modo Rango, si se ingresó el puerto público (puerto inicial y puerto final) y la IP inicial de la IP privada, el sistema calculará y mostrará la IP final de la IP privada automáticamente.
Nombre del Servicio	Introduzca la descripción del servicio de red específico.
Protocolo	Seleccione el protocolo de la capa de transporte (TCP o UDP).
Interfaz WAN	Seleccione la interfaz WAN utilizada para la redirección de puertos. Hay ocho alias de IP de WAN que se pueden seleccionar y usar para la redirección de puertos. La configuración predeterminada es**Todo**lo que significa que todos los datos entrantes de cualquier puerto se redirigirán al rango especificado de dirección IP y puerto.
Puerto Público	Especifique qué puerto se puede redirigir al especificado**IP privada y puerto**del anfitrión interno. Si tu eliges**Rango**como modo de redirección de puertos, verá dos cuadros en este campo. Ingrese el número requerido en el primer cuadro (como puerto de inicio) y el segundo cuadro (como puerto final).
IP de origen	**Objeto IP**-Utilice la lista desplegable para especificar un perfil de objeto IP. **Grupo de IP**-Utilice la lista desplegable para especificar un perfil de grupo de IP.
ip privada	Especifique la dirección IP privada del host interno que proporciona el servicio. Si tu eliges**Rango**como modo de redirección de puertos, verá dos cuadros en este campo. Escriba una dirección IP completa en el primer cuadro (como punto de partida). El segundo se asignará automáticamente más tarde.
Puerto privado	Especifique el número de puerto privado del servicio ofrecido por el host interno.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

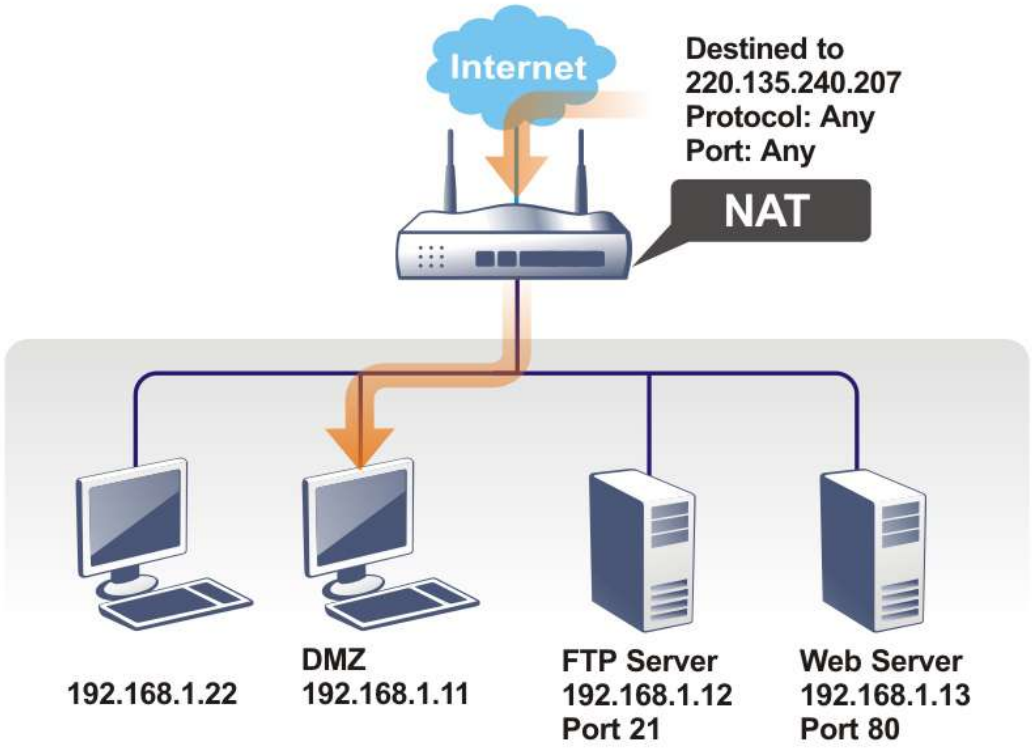
Tenga en cuenta que el enrutador tiene sus propios servicios integrados (servidores) como Telnet, HTTP y FTP, etc. Dado que los números de puerto comunes de estos servicios (servidores) son todos iguales, es posible que deba reiniciar el enrutador para evitar conflicto

Por ejemplo, la interfaz de usuario web integrada en el enrutador tiene el puerto predeterminado 80, que puede entrar en conflicto con el servidor web en la red local, http://192.168.1.13:80. Por lo tanto, necesita**cambie el puerto http del enrutador a cualquier otro que no sea el puerto predeterminado 80**para evitar conflictos, como 8080. Esto se puede establecer en el**Mantenimiento del sistema >>Configuración de gestión**. Luego accederá a la pantalla de administración agregando el sufijo 8080 a la dirección IP, por ejemplo, http://192.168.1.1:8080 en lugar del puerto 80.



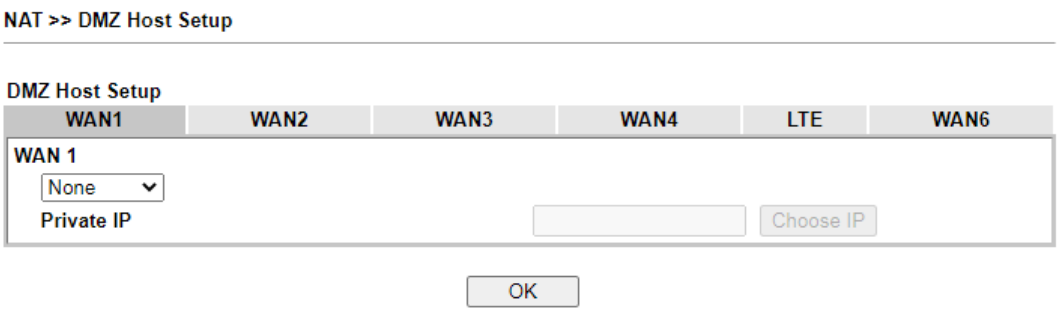
II-4-2 Anfitrión de DMZ

Como se ha mencionado más arriba,**Redirección de puertos**puede redirigir TCP/UDP entrante u otro tráfico en puertos particulares a la dirección IP privada/puerto específico del host en la LAN. Sin embargo, otros protocolos IP, por ejemplo, los protocolos 50 (ESP) y 51 (AH), no viajan en un puerto fijo. El enrutador Vigor proporciona una instalación**Anfitrión de DMZ**que asigna TODOS los datos no solicitados en cualquier protocolo a un solo host en la LAN. La navegación web regular y otras actividades similares de Internet de otros clientes continuarán funcionando sin interrupciones inapropiadas.**Anfitrión de DMZ**permite que un usuario interno definido esté totalmente expuesto a Internet, lo que generalmente ayuda a algunas aplicaciones especiales como Netmeeting o Internet Games, etc.

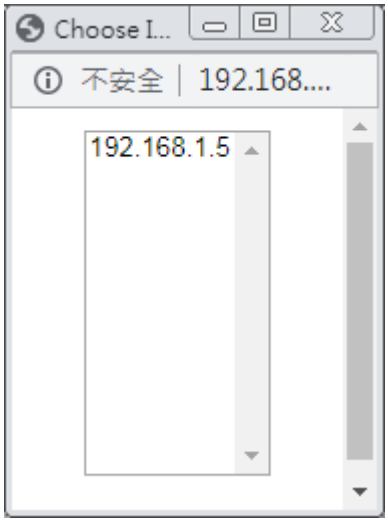
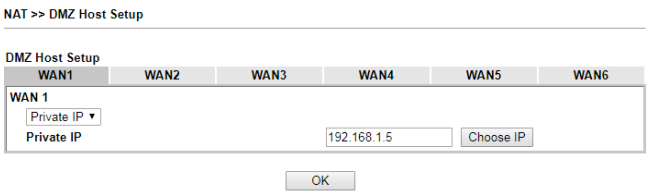


Las propiedades de seguridad de NAT se pasan por alto un poco si configura un host DMZ. Le sugerimos que agregue reglas de filtro adicionales o un firewall secundario.

Hacer clic**Anfitrión de DMZ**para abrir la página siguiente. Puede configurar un host DMZ diferente para cada interfaz WAN. Haga clic en la pestaña WAN para cambiar a la página de configuración de esa WAN.

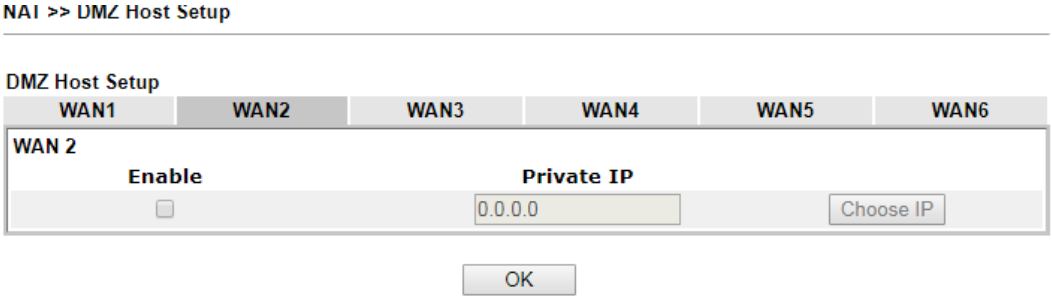


Los ajustes disponibles se explican a continuación:

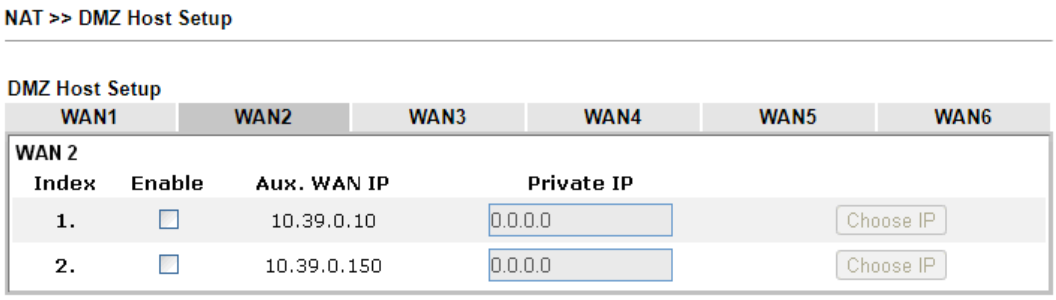
Artículo	Descripción
WAN 1	Elegir**ip privada**o**Ninguno**primero.
ip privada	Ingrese la dirección IP privada del host DMZ o haga clic en Elegir PC para seleccionar uno.
Elija IP	Haga clic en este botón y aparecerá automáticamente una ventana, como se muestra a continuación. La ventana consta de una lista de direcciones IP privadas de todos los hosts en su red LAN. Seleccione una dirección IP privada en la lista para que sea el host DMZ.  Cuando haya seleccionado una IP privada del cuadro de diálogo anterior, la dirección IP se mostrará en la siguiente pantalla. Hacer clic**DE ACUERDO** para guardar la configuración. 

El host DMZ para WAN2, WAN3, LTE o WAN4 es ligeramente diferente con WAN1.**IP verdadera activa** La selección está disponible solo para WAN1.

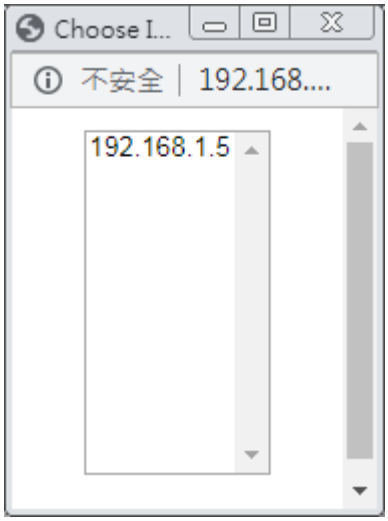
Consulte la figura siguiente.



Si previamente ha configurado**Alias de WAN**para**PPPoE**o**IP estática o dinámica**modo en la interfaz WAN2**,**los encontrarás en**auxiliar IP WAN**para su selección.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Marque para habilitar la función de host DMZ.
ip privada	Ingrese la dirección IP privada del host DMZ o haga clic en Elegir PC para seleccionar uno.
Elija IP	Haga clic en este botón y aparecerá automáticamente una ventana, como se muestra a continuación. La ventana consta de una lista de direcciones IP privadas de todos los hosts en su red LAN. Seleccione una dirección IP privada en la lista para que sea el host DMZ.  Cuando haya seleccionado una IP privada del cuadro de diálogo anterior, la dirección IP se mostrará en la pantalla. Hacer clic**DE ACUERDO** para guardar la configuración.

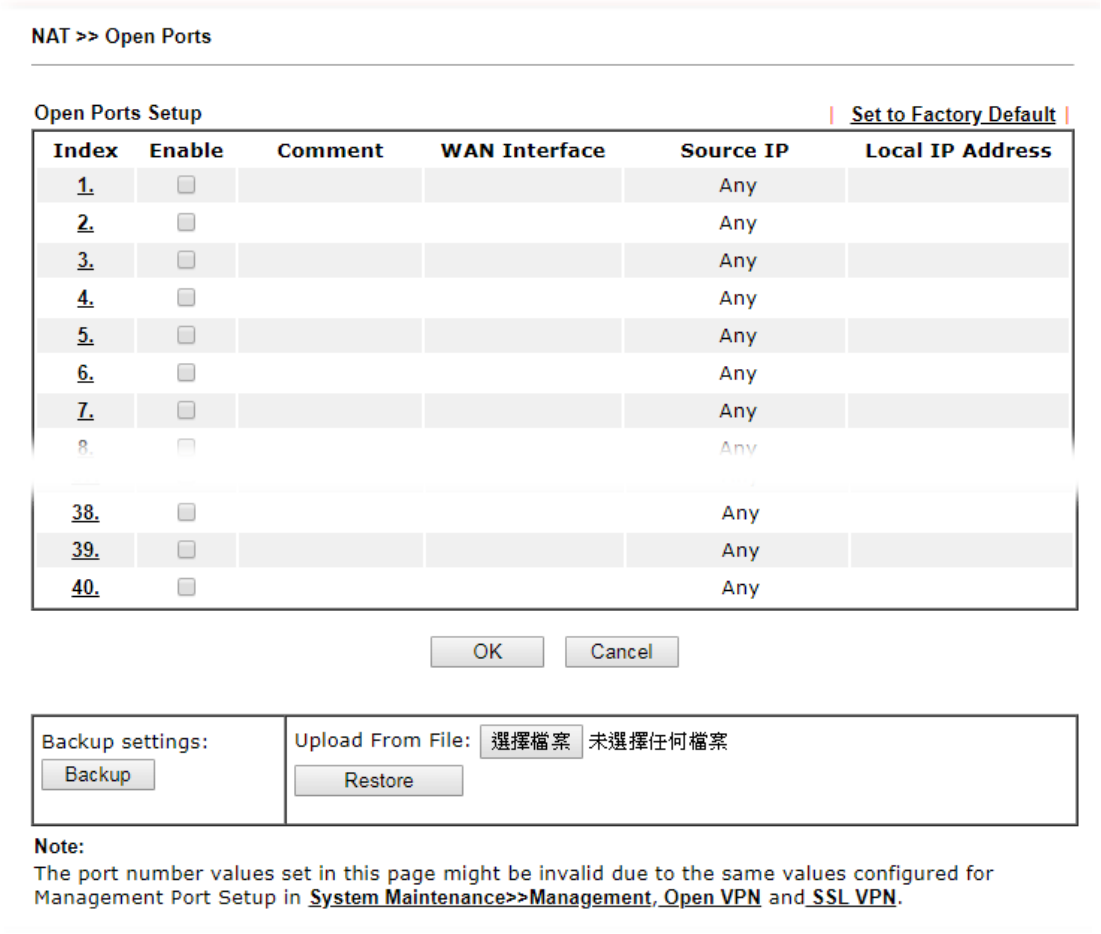
Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

II-4-3 Puertos Abiertos

Puertos abiertosle permite abrir una gama de puertos para el tráfico de aplicaciones especiales.

La aplicación común de Open Ports incluye la aplicación P2P (p. ej., BT, KaZaA, Gnutella, WinMX, eMule y otras), cámara de Internet, etc. Asegúrese de mantener actualizada la aplicación involucrada para evitar ser víctima de vulnerabilidades de seguridad.

Hacer clic**Puertos abiertos**para abrir la siguiente página:

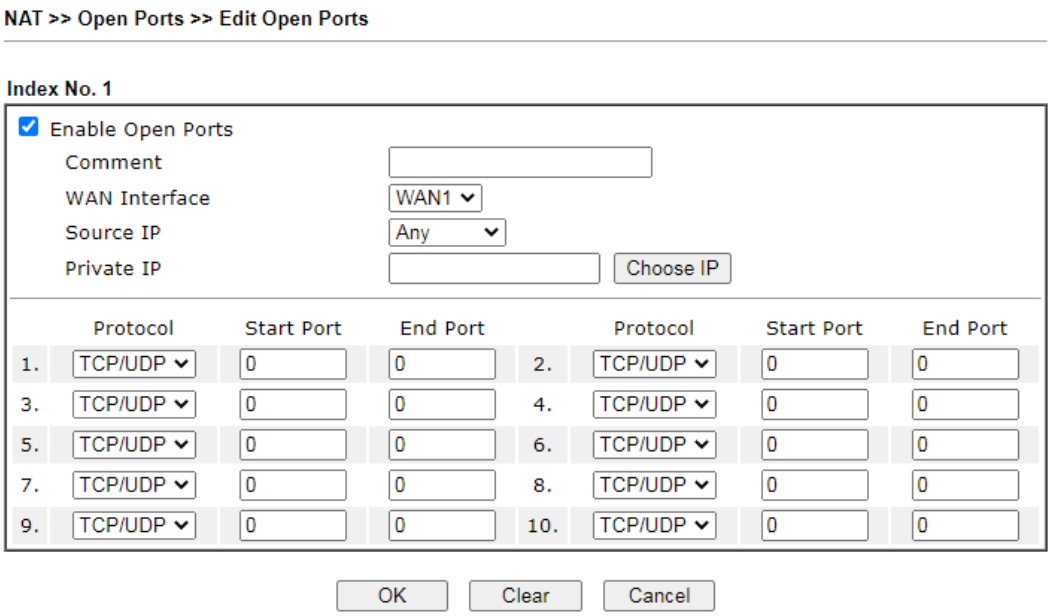


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Índice	Indique el número relativo para la entrada en particular que desea ofrecer servicio en un host local. Debe hacer clic en el número de índice apropiado para editar o borrar la entrada correspondiente.
Permitir	Marque la casilla para habilitar el perfil de puerto abierto.
Comentario	Especifique el nombre del servicio de red definido.
Interfaz WAN	Muestra la interfaz WAN utilizada por dicho índice.
auxiliar IP WAN	Muestra la configuración de alias de IP utilizada por dicho índice. Si no existe una configuración de alias de IP, dicho campo no aparecerá.
IP de origen	Muestra el nombre del objeto IP.
Dirección IP local	Muestra la dirección IP privada del host local que ofrece el servicio.

Respaldo	Haga clic en él para hacer una copia de seguridad de la configuración de los ajustes de los puertos abiertos.
Restaurar	Haga clic en él para restaurar la configuración de los ajustes de puertos abiertos. Antes de hacer clic, asegúrese de cargar el archivo de configuración en el enrutador Vigor.

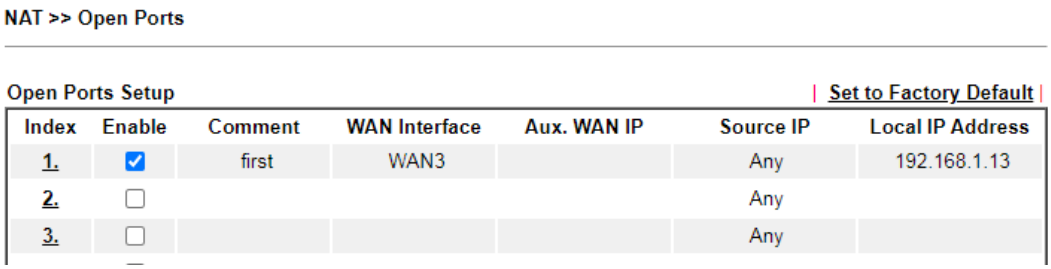
Para agregar o editar la configuración del puerto, haga clic en un número de índice en la página. Aparecerá la página de configuración de entrada de índice. En cada entrada del índice, puede especificar**10**gamas de puertos para diversos servicios.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar puertos abiertos	Marque para habilitar esta entrada.
Comentario	Asigne un nombre a la aplicación/servicio de red definido.
Interfaz WAN	Especifique la interfaz WAN que se utilizará para esta entrada.
IP de origen	**Cualquier -**Cualquier IP se puede utilizar como IP de origen. **Objeto IP**-Utilice la lista desplegable para especificar un perfil de objeto IP. **Grupo de IP**-Utilice la lista desplegable para especificar un perfil de grupo de IP.
IP WAN	Especifique la dirección IP de WAN que se usará para esta entrada. Esta configuración está disponible cuando se configura el alias de IP de WAN.
ip privada	Introduzca la dirección IP privada del host local o haga clic en**Elija PC** para seleccionar uno. **Elija IP -**Haga clic en este botón y, posteriormente, aparecerá automáticamente una ventana con una lista de direcciones IP privadas de hosts locales. Seleccione la dirección IP adecuada del host local en la lista.
Protocolo	Especifique el protocolo de la capa de transporte. Podría ser**TCP**,**UDP**, o**----** (ninguno) para la selección.
Puerto de inicio	Especifique el número de puerto inicial del servicio ofrecido por el host local.
Puerto final	Especifique el número de puerto final del servicio ofrecido por el host local.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.



II-4-4 Activación de puertos

Port Triggering es una variación de la función de puertos abiertos.

La diferencia clave entre "puerto abierto" y "activación de puerto" es:

- Una vez que se hace clic en el botón Aceptar y la configuración ha tenido efecto, "abrir puerto" mantiene los puertos abiertos para siempre.
- Una vez que se hace clic en el botón Aceptar y la configuración ha tenido efecto, la "activación de puertos" solo intentará abrir los puertos una vez que se cumplan las condiciones de activación.
- La duración de la apertura de estos puertos depende del tipo de protocolo utilizado. Las duraciones "predeterminadas" se muestran a continuación y estos valores de duración se pueden modificar a través de comandos telnet.

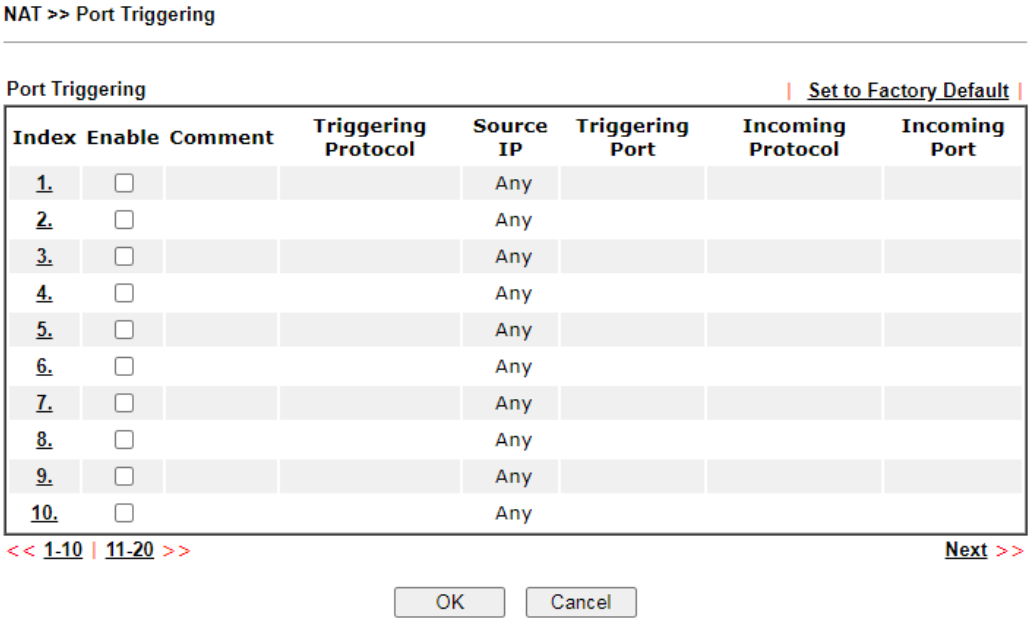
  TCP: 86400 seg.

  UDP: 180 seg.

  IGMP: 10 seg.

  TCP WWW: 60 seg.

  TCP SYN: 60 seg.

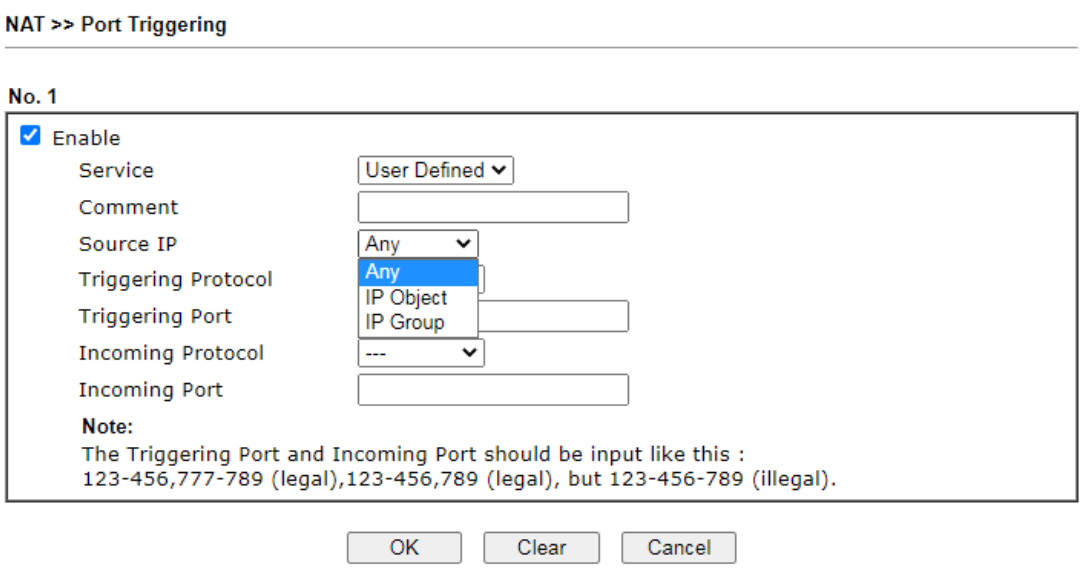


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Índice	Indique el número relativo para el perfil de activación del puerto. Debe hacer clic en el número de índice apropiado para editar o

	borrar la entrada correspondiente.
Permitir	Marque la casilla para habilitar el perfil Activación de puertos.
Comentario	Muestra el texto que memoriza la aplicación de esta regla.
Protocolo de activación	Muestra el protocolo de los paquetes desencadenantes.
IP de origen	Muestra el nombre del objeto IP.
Puerto de activación	Muestra el puerto de los paquetes desencadenantes.
Protocolo entrante	Muestra el protocolo para los datos entrantes de dicho perfil de activación.
Puerto entrante	Muestra el puerto para los datos entrantes de dicho perfil de activación.

Haga clic en el enlace del número de índice para abrir la página de configuración.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Marque para habilitar esta entrada.
Servicio	Elija el tipo de servicio a aplicar para dicho perfil de activación.
Comentario	Introduzca el texto para memorizar la aplicación de esta regla.
IP de origen	**Cualquier -**Cualquier IP se puede utilizar como IP de origen. **Objeto IP**-Utilice la lista desplegable para especificar un perfil de objeto IP. **Grupo de IP**-Utilice la lista desplegable para especificar un perfil de grupo de IP.
Protocolo de activación	Seleccione el protocolo (TCP, UDP o TCP/UDP) para dicho perfil de activación.
Puerto de activación	Ingrese el puerto o el rango de puertos para dicho perfil de activación.
Protocolo entrante	Cuando se reciben los paquetes de activación, se espera que los paquetes entrantes utilicen el protocolo seleccionado. Seleccione el protocolo (TCP, UDP o TCP/UDP) para los datos entrantes de dicho perfil de activación.
Puerto entrante	Ingrese el puerto o rango de puertos para los paquetes entrantes.

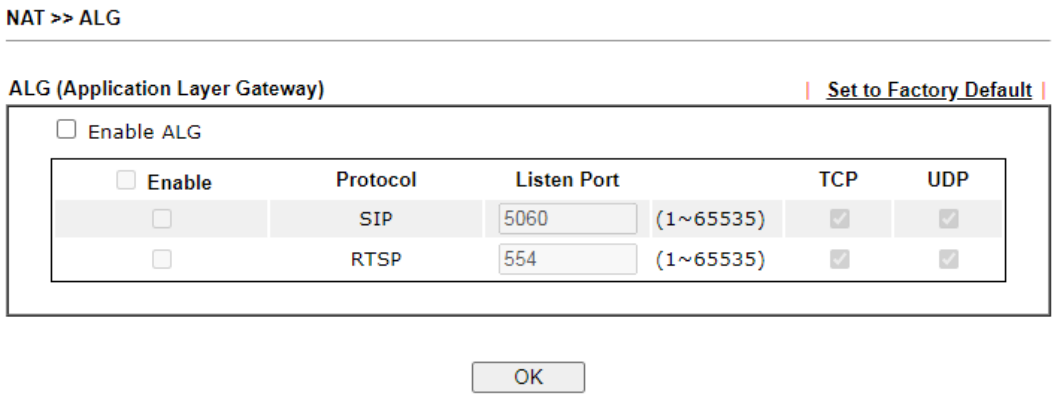
Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

II-4-5 ALG

ALG significa**Puerta de enlace de la capa de aplicación**. Hay dos métodos proporcionados por el enrutador Vigor, RTSP (Protocolo de transmisión en tiempo real) ALG y SIP (Protocolo de inicio de sesión) ALG, para procesar los paquetes de voz y video.

RTSP ALG hace que el mensaje RTSP, el mensaje RTCP y los paquetes RTP de voz y video se transmitan y reciban correctamente a través de NAT por el enrutador Vigor.

Sin embargo, SIP ALG hace que los mensajes SIP y los paquetes de voz RTP se transmitan y reciban correctamente a través de NAT por el enrutador Vigor.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar ALG	Marque para habilitar dicha función.
Puerto de escucha	Escriba un número de puerto para el protocolo SIP o RTSP.
TCP	Marque la casilla para hacer que el paquete de mensajes de protocolo correspondiente de TCP se transmita y reciba a través de NAT.
UDP	Marque la casilla para hacer que el paquete de mensajes de protocolo correspondiente de UDP se transmita y reciba a través de NAT.

II-5 Aplicaciones

DNS Dinámico

La mayoría de los ISP asignan direcciones IP WAN dinámicas a sus clientes. Las direcciones IP dinámicas presentan desafíos para los usuarios que deseen aceptar conexiones remotas a sus LAN desde Internet, ya que el servicio podría verse interrumpido debido al cambio de la dirección IP sin previo aviso. Al configurar el servicio con un proveedor de DNS dinámico (DDNS) y configurar las actualizaciones de DNS dinámico en el enrutador Vigor, puede tener acceso confiable a su red por medio de una dirección de dominio fácil de recordar que se resuelve en la IP WAN más actual DIRECCIÓN.

El enrutador Vigor es compatible con una amplia gama de proveedores de DDNS, como DynDNS, No-IP.com, DtDNS y ChangeIP. Comuníquese con el proveedor de DDNS de su elección para configurar el servicio antes de configurar DDNS en el enrutador.

LAN DNS / Reenvío de DNS

LAN DNS permite que el administrador de la red anule las resoluciones DNS estándar para seleccionar direcciones de dominio. El enrutador responderá a consultas sobre direcciones de dominio coincidentes con direcciones IP personalizadas.

El reenvío de DNS permite al administrador de la red reenviar consultas de DNS a diferentes servidores DNS en función del nombre de dominio.

El LAN DNS y el reenvío de DNS solo afectan las consultas de DNS que se envían a la WAN a través del enrutador. El enrutador no interceptará las consultas DNS que se dirijan a un servidor DNS en la LAN.

Cronograma

El enrutador Vigor tiene un reloj incorporado que puede actualizarse manualmente o automáticamente mediante Network Time Protocols (NTP). Como resultado, no solo puede programar el enrutador para conectarse a Internet a una hora específica, sino también restringir el acceso a Internet a ciertas horas para que los usuarios puedan conectarse a Internet solo durante ciertas horas, por ejemplo, horas laborales. El horario también es aplicable a otras funciones.

RADIO/TACACS+

El Servicio de Usuario de Acceso Telefónico de Autenticación Remota (RADIUS) es un protocolo cliente/servidor de autenticación de seguridad que admite autenticación, autorización y contabilidad, que es ampliamente utilizado por los proveedores de servicios de Internet. Es el método más común para autenticar y autorizar usuarios de redes de acceso telefónico y tunelizado.

La función de cliente RADIUS integrada permite que el enrutador ayude al usuario de marcación remota o a una estación inalámbrica y al servidor RADIUS a realizar la autenticación mutua. Permite la autenticación de acceso remoto centralizado para la gestión de la red.

Configuración de LDAP/Directorio Activo

El protocolo ligero de acceso a directorios (LDAP) es un protocolo de comunicación para usar en una red TCP/IP. Define los métodos para acceder al servidor de directorio de distribución por parte de los clientes, trabajar en el directorio y compartir la información en el directorio por parte de los clientes. El estándar LDAP es establecido por el equipo de trabajo de Internet Engineering Task Force (IETF).

Como se describe en el nombre, LDAP está diseñado como una forma efectiva de acceder al servicio de directorio sin la complejidad de otros protocolos de servicio de directorio. Para LDAP se define realizar, consultar y modificar la información dentro del directorio, y adquirir los datos en el directorio

de forma segura, por lo tanto, los usuarios pueden aplicar LDAP para buscar o enumerar el objeto del directorio, consultar o administrar el directorio activo.

UPnP

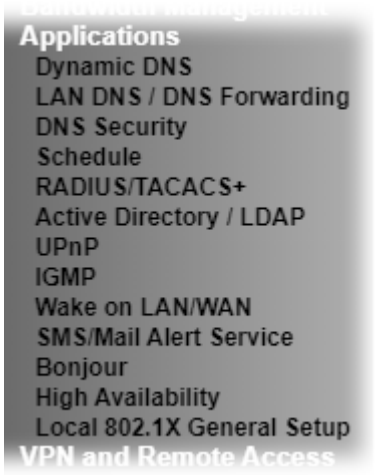
El Vigor es compatible con UPnP (Universal Plug and Play), que es un conjunto de protocolos de red que simplifica la configuración de la red. Las aplicaciones y los dispositivos de red en la LAN, que admiten UPnP, pueden solicitar al enrutador que modifique su configuración para permitir NAT Traversal, de modo que los hosts WAN puedan conectarse a ellos directamente.

Ejemplos de aplicaciones y dispositivos que admiten UPnP incluyen aplicaciones para compartir archivos como uTorrent, Vuze y eMule, consolas de juegos como Sony PlayStations 3 y 4 Xbox 360 y Xbox One, aplicaciones de transmisión de medios como Plex y XBMC, y mensajería y llamadas. aplicaciones como Skype. Para averiguar si una determinada aplicación o dispositivo de red admite o requiere UPnP, consulte su manual de usuario o consulte con su proveedor.

Activación de la LAN

Con la función Wake on LAN (WoL), los clientes de LAN que admiten WoL se pueden encender o reanudar desde el modo de suspensión a través de la red, sin necesidad de acceso físico al dispositivo.

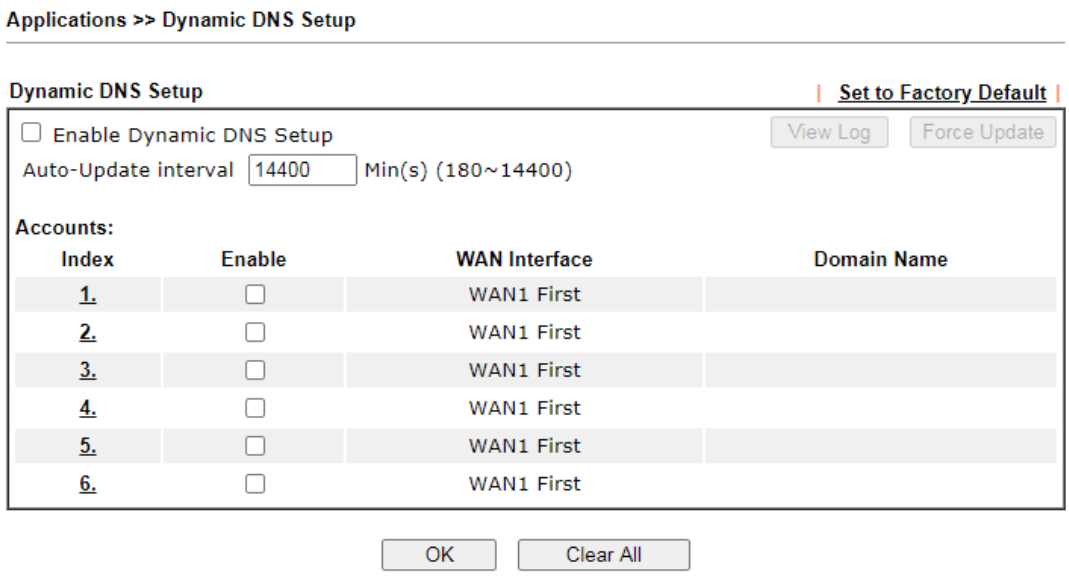
Para que los clientes de LAN puedan despertarse de los estados de suspensión o apagado, la tarjeta de interfaz de red debe estar configurada para monitorear los mensajes de Wake-on-LAN. Consulte la documentación del cliente LAN para obtener detalles sobre cómo configurar su interfaz de red para Wake on LAN.



II-5-1 DNS dinámico

Habilite la función y agregue una cuenta de DNS dinámico

Para comenzar a configurar el DNS dinámico, desde el menú principal, navegue hasta**Aplicaciones**y seleccione **DNS Dinámico**. Aparece la pantalla principal de configuración de DNS dinámico:

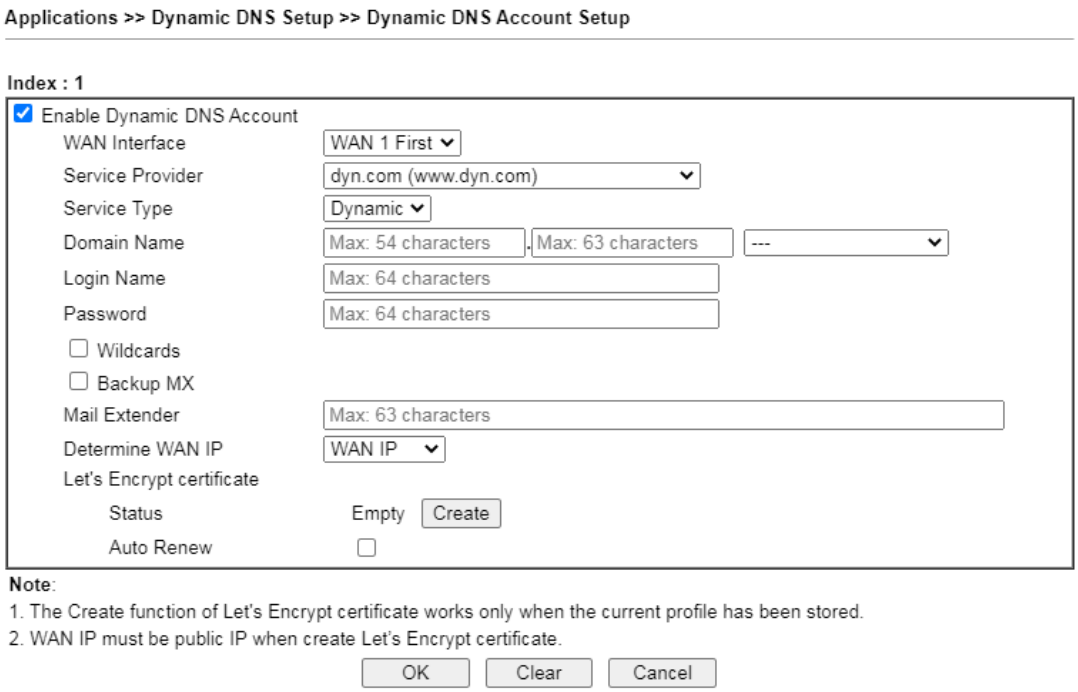


Los ajustes disponibles se explican a continuación:

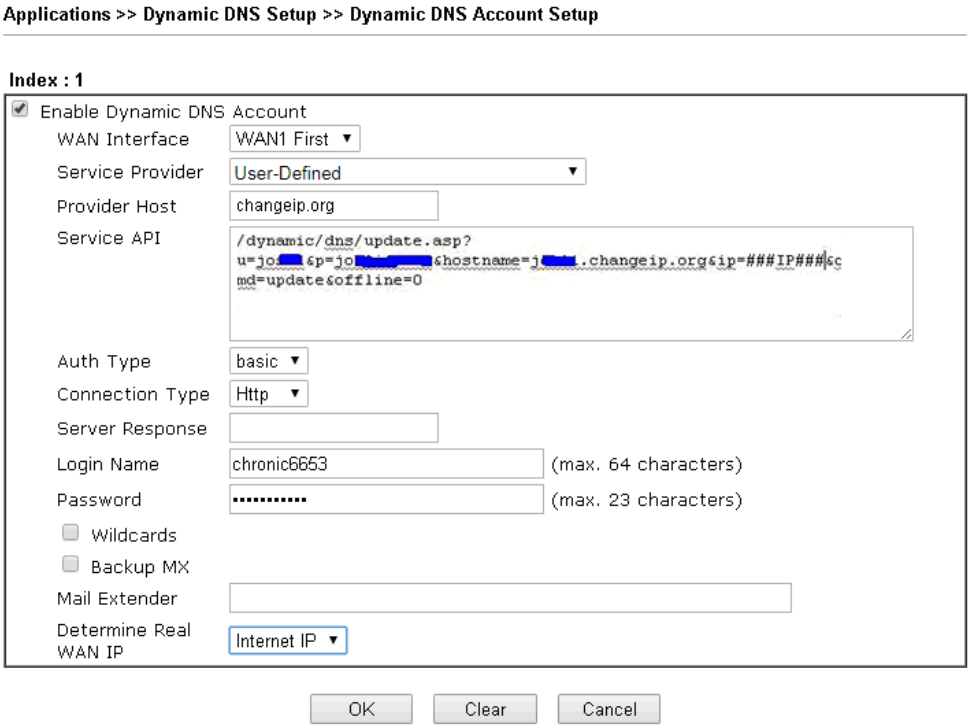
Artículo	Descripción
Habilitar la configuración de DNS dinámico	Seleccione para habilitar la función DDNS.
Establecer como predeterminado de fábrica	Haga clic para borrar todos los perfiles a la configuración de fábrica.
Ver registro	Seleccione para mostrar los mensajes de actualización de DDNS más recientes.
Forzar actualización	Haga clic para conectarse inmediatamente a los servidores DDNS para actualizar la información de la dirección IP.

Intervalo de actualización automática	La frecuencia, en minutos, con la que el enrutador se conecta a los servidores DDNS para actualizar la información de la dirección IP.
Índice	Haga clic para abrir la página de configuración del perfil DDNS.
Permitir	Marque la casilla para habilitar dicha cuenta.
Interfaz WAN	Muestra la interfaz WAN asociada con el perfil DDNS.
Nombre de dominio	Muestra el nombre de dominio con el que está asociado el perfil.

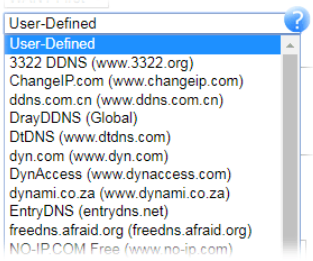
Después de hacer clic en el número de índice, aparece la pantalla de configuración detallada para el perfil DDNS:



Si**Usuario definido**se especifica como el proveedor de servicios, la página web cambiará ligeramente de la siguiente manera:



Los ajustes disponibles se explican a continuación:

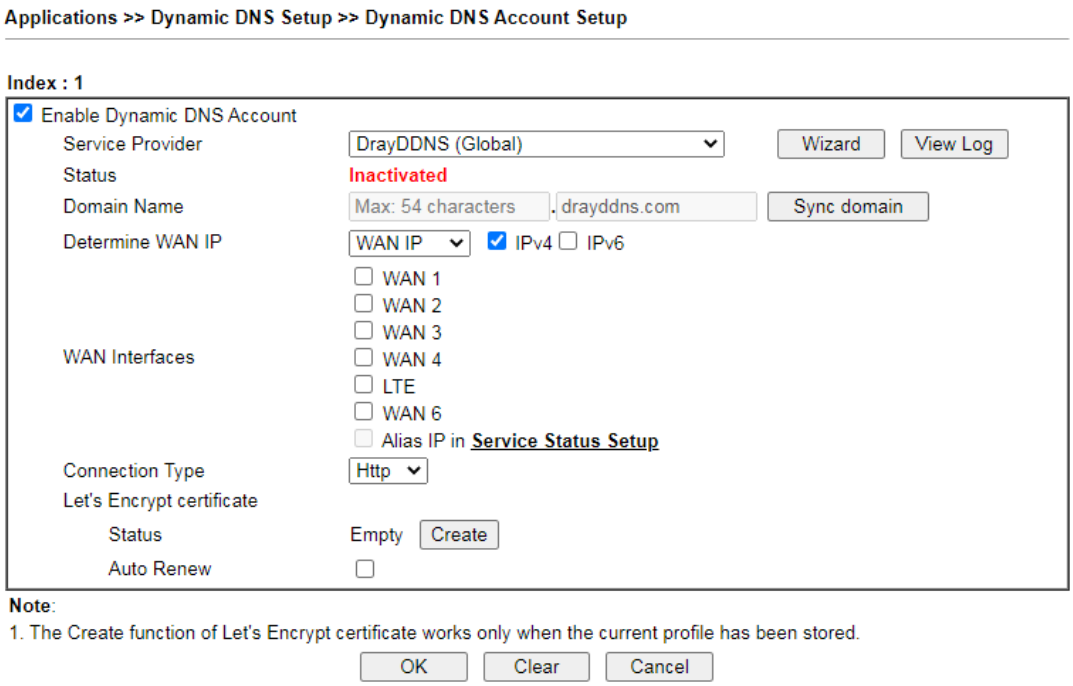
Artículo	Descripción
Habilitar DNS dinámico Cuenta	Seleccione para habilitar este perfil DDNS.
Interfaz WAN	Seleccione la interfaz WAN para monitorear los cambios de dirección IP. **WANx primero**–La interfaz WAN especificada se examinará primero. Si está en línea, su dirección IP se utilizará en la actualización de DDNS. **Solo WANx**–Solo se examinará la interfaz WAN especificada. Si la interfaz WAN está en línea, su dirección IP se utilizará en la actualización de DDNS. De lo contrario, no se realizará ninguna actualización para este perfil DDNS.
Proveedor de servicio	Seleccione el proveedor de DDNS. Si su proveedor de DDNS no está en la lista, seleccione**Usuario definido**y configurar manualmente el perfil.  - **Anfitrión del proveedor**-Ingrese la dirección IP o el nombre de dominio del host que brinda el servicio relacionado. Tenga en cuenta que dicha opción está disponible cuando se selecciona Personalizado como Proveedor de servicios. - **API de servicio**-Ingrese la información de la API obtenida del servidor DDNS. Tenga en cuenta que dicha opción está disponible cuando Personalizado está

	seleccionado como proveedor de servicios. (p.ej: /dynamic/dns/update.asp?u=jo***&p=jo********&hostname=j****.changeip.org&ip=###IP### &cmd=actualizar&fuera de línea=0) - **Tipo de autenticación**-Se pueden utilizar dos tipos para la autenticación. **Básico**–El nombre de usuario y la contraseña definidos más tarde se pueden mostrar a partir de los paquetes capturados. **URL**-El nombre de usuario y la contraseña definidos más adelante se pueden mostrar en la URL. (p. ej., http://ns1.vigorddns.com/ddns.php?username=xxxx&password=xxxx&domain=xxxx.vigorddns.com) Tenga en cuenta que dicha opción está disponible cuando se selecciona Personalizado como Proveedor de servicios. - **Tipo de conección**-Hay dos tipos de conexión (HTTP y HTTPs) para especificar. Tenga en cuenta que dicha opción está disponible cuando se selecciona Personalizado como Proveedor de servicios. - **Respuesta del servidor**-Escriba cualquier texto que desee recibir del servidor DDNS. Tenga en cuenta que dicha opción está disponible cuando se selecciona Personalizado como Proveedor de servicios. Si se selecciona otro proveedor de servicios, debe configurar el Tipo de servicio, el Nombre de dominio, el Nombre de inicio de sesión y la Contraseña. - **Tipo de servicio**-Seleccione el tipo de servicio que coincida con el de su cuenta DynDNS. Si no está seguro de qué tipo de servicio seleccionar, pruebe Dynamic primero. Esta opción es aplicable solo a DynDNS. - **Nombre de dominio**-El dominio y el subdominio que se actualizarán.
Nombre de inicio de sesión	El nombre de inicio de sesión de la cuenta DDNS.
Contraseña	La contraseña de la cuenta DDNS.
Comodín y copia de seguridad MX	Las funciones Wildcard y Backup MX (Mail Exchange) no son compatibles con todos los proveedores de DNS dinámico. Puede obtener información más detallada de sus sitios web.
Extensor de correo	Si el servidor de correo está definido con otro nombre, ingrese el nombre en esta área. Dicho servidor de correo se utilizará como intercambio de correo de respaldo.
Determinar la IP de la WAN	Si se instala un enrutador Vigor detrás de cualquier enrutador NAT, puede habilitar dicha función para ubicar la IP WAN real. Cuando la IP WAN utilizada por el enrutador Vigor es una IP privada, esta función puede detectar la IP pública utilizada por el enrutador NAT y usar la dirección IP detectada para la actualización de DDNS. Hay dos métodos ofrecidos para que usted elija: - **IP WAN**-Se utilizará la dirección IP de la interfaz WAN del enrutador. - **ip de internet**–Se utilizará la dirección IP pública real. Seleccione esta opción si la dirección IP asignada a la interfaz WAN del enrutador no es la dirección IP externa real.

Hacer clic**DE ACUERDO**para guardar los cambios,**Claro**para borrar todos los ajustes, o**Cancelar**para descartar los cambios y volver a la pantalla principal de DDNS.

DrayDDNS, un nuevo servicio DDNS desarrollado por DrayTek, puede registrar múltiples IP WAN (IPv4) en un solo nombre de dominio. Es conveniente para que los usuarios lo usen y fácil de configurar. Cada Vigor Router está disponible para registrar un nombre de dominio.

Elegir**DrayDDNS (Global)**como proveedor de servicios, la página web se mostrará de la siguiente manera:



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar DNS dinámico Cuenta	Marque esta casilla para habilitar la cuenta actual. Si marcó la casilla, verá que aparece una marca de verificación en la columna Activo de la página web anterior en el paso 2).
Proveedor de servicio	Elegir**DrayDDNS (Global)**como proveedor de servicios. **Mago**–Este botón está disponible cuando se selecciona DrayTek Global como proveedor de servicios. Para activar el servicio DDNS de DrayTek, haga clic en él para habilitar la licencia emitida por DrayTek a través de**Asistentes>>Asistente de activación del servicio**. Consulte la sección**A-1 ¿Cómo usar DrayDDNS?**para obtener información detallada.
Estado	Muestra si la licencia está activada o no.
Determinar la IP de la WAN	Si se instala un enrutador Vigor detrás de cualquier enrutador NAT, puede habilitar dicha función para ubicar la IP WAN real. Cuando la IP WAN utilizada por el enrutador Vigor es una IP privada, esta función puede detectar la IP pública utilizada por el enrutador NAT y usar la dirección IP detectada para la actualización de DDNS. Hay dos métodos ofrecidos para que usted elija: - **IP WAN**-Si se selecciona y la IP WAN del enrutador Vigor es privada, la actualización de DDNS se realizará de inmediato. - **ip de internet**–Si se selecciona y la IP WAN del enrutador Vigor es privada, se convertirá a IP pública antes de que se realice la actualización de DDNS.

Interfaces WAN	**WANx**-Mientras se conecta, el enrutador utilizará WANx como canal para dicha cuenta.
Vamos a cifrar certificado	**Crear -**Haga clic para generar un certificado emitido por Let's Encrypt para aplicar a dicha cuenta DDNS. **Actualización automática**–Marque la casilla para que el sistema actualice el certificado automáticamente.

Deshabilite la función y borre todas las cuentas de DNS dinámico

Desmarcar**Habilitar la configuración de DNS dinámico**y haga clic en**Limpiar todo**para deshabilitar la función y borrar todas las cuentas del enrutador.

Eliminar una cuenta de DNS dinámico

Haga clic en el**Índice**número que desea eliminar y luego haga clic en**Limpiar todo**botón para eliminar la cuenta.

Las actualizaciones de DDNS tienen lugar cuando:

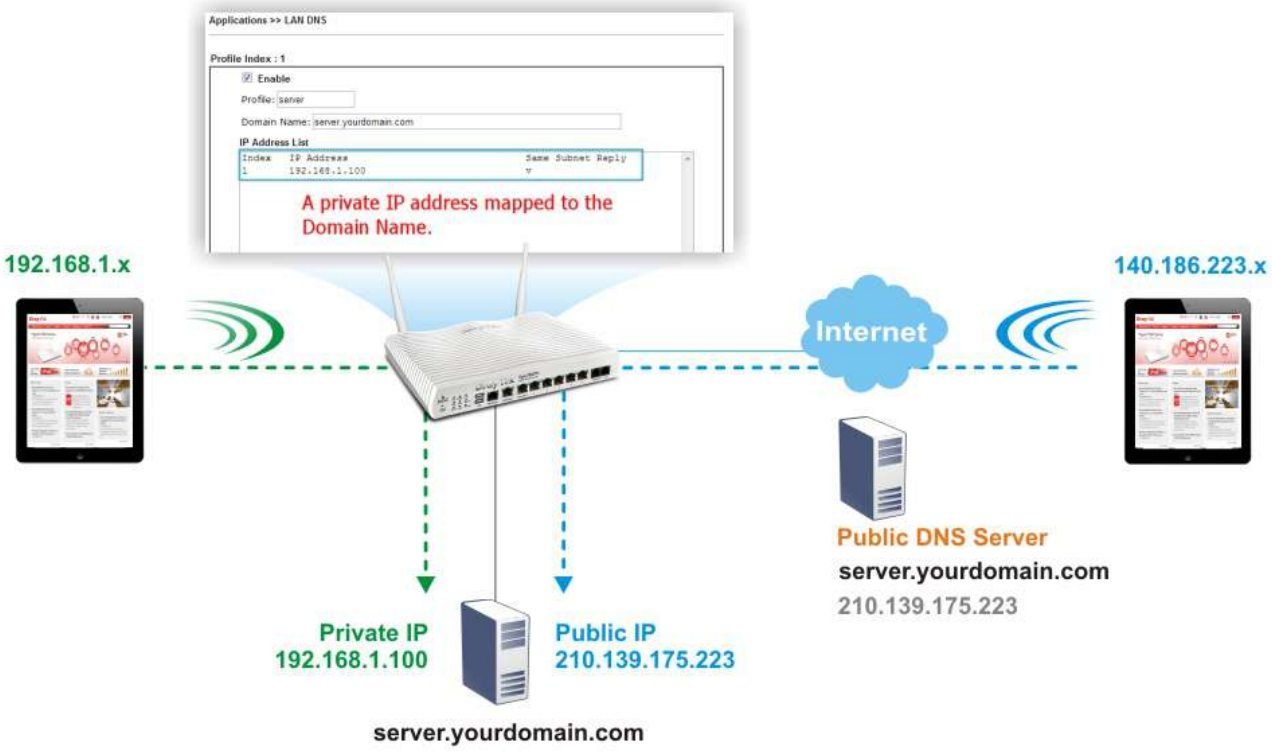
- El enrutador está encendido o reiniciado.
- La dirección IP pública de cualquier interfaz WAN cambia.
- El estado en línea de una interfaz WAN cambia (pasando de en línea a fuera de línea o viceversa).
- La función DDNS cambia de deshabilitada a habilitada.
- Se modifica y habilita una entrada de DDNS.
- Ha transcurrido el intervalo de actualización automática.

Procedimientos para configurar una entrada de DNS dinámico

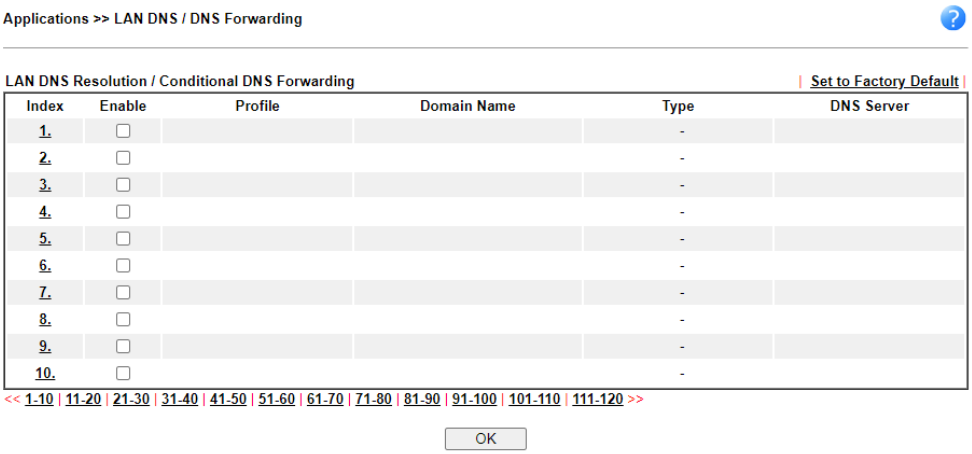
1. Comuníquese con el proveedor de DNS dinámico de su elección y configure el servicio. La mayoría de los proveedores de DDNS aceptan suscripciones en sus sitios web. El servicio se puede proporcionar de forma gratuita o mediante el pago de una tarifa.
2. Cree una entrada de DDNS en el enrutador seleccionando el proveedor de DDNS apropiado e ingrese la información de la cuenta.
3. Asegúrese de que tanto la entrada DDNS como la función DDNS estén habilitadas en el enrutador.
4. Haga clic en el botón Ver registro en la página principal de DDNS para abrir el registro de actualización.
5. Examine el registro de actualización para asegurarse de que la actualización se haya realizado correctamente.
6. Si la actualización no fue exitosa, verifique la entrada de DDNS para asegurarse de que la configuración se haya ingresado correctamente.

II-5-2 LAN DNS / Reenvío de DNS

LAN DNS permite a los administradores de red alojar servidores con privacidad y seguridad. Cuando los administradores de red de su oficina configuran un servidor FTP, de correo o web dentro de la LAN, puede especificar direcciones IP privadas específicas para los servidores correspondientes. Por lo tanto, incluso la PC remota está adoptando DNS público como servidor DNS, la resolución LAN DNS en la serie Vigor2927 responderá a la dirección IP privada especificada.



Para comenzar a configurar LAN DNS o DNS Forwarding, desde el menú principal, haga clic en**Aplicaciones**, seguido por**LAN DNS / Reenvío de DNS**.

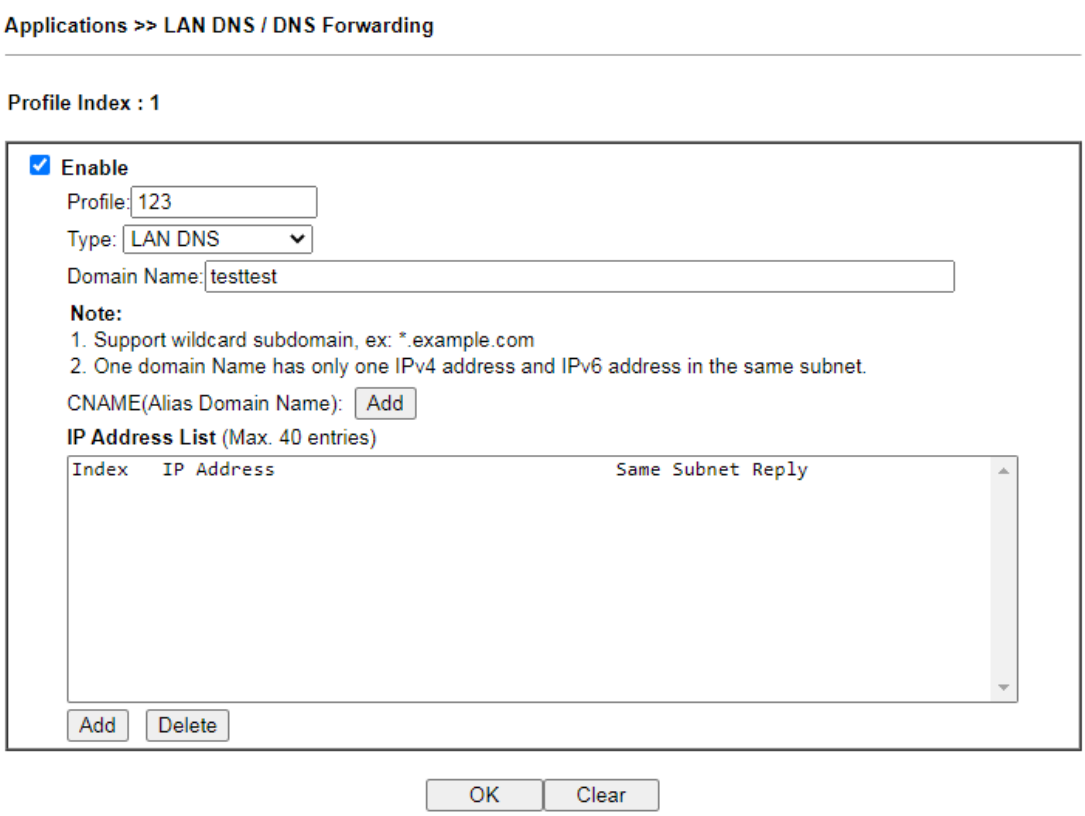


Cada elemento se explica de la siguiente manera:

Artículo	Descripción
Establecer como predeterminado de fábrica	Haga clic para borrar todos los perfiles a la configuración de fábrica.
Índice	Haga clic para abrir la página de configuración del perfil.

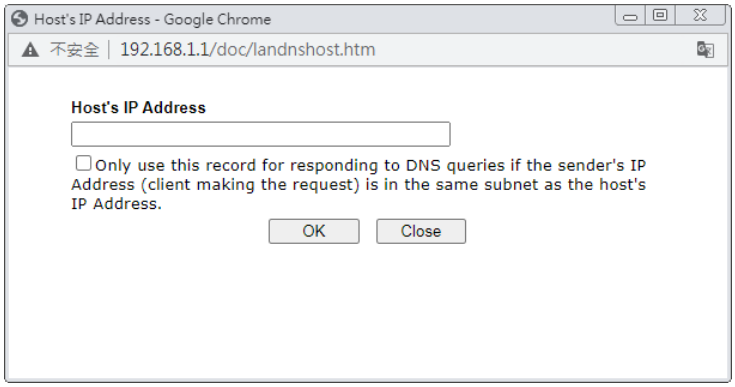
Permitir	Seleccione para habilitar este perfil.
Perfil	Muestra el nombre del perfil.
Nombre de dominio	Muestra el nombre de dominio configurado para el perfil.
Tipo	Muestra el tipo (DNS de LAN o Reenvío de DNS) del perfil.
Servidor DNS	Servidor DNS al que se reenviarán las consultas DNS para el nombre de dominio especificado.

Para configurar un perfil LAN DNS, haga clic en su índice para abrir la página de configuración.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Seleccione para habilitar este perfil.
Perfil	Introduzca un nombre para identificar este perfil. **Nota:**Si escribe aquí un nombre para LAN DNS y hace clic en**DE ACUERDO** para guardar la configuración, el nombre también se aplicará automáticamente al reenvío de DNS condicional.
Tipo	Elija DNS de LAN o Reenvío de LAN.
Si se selecciona LAN DNS	**Nombre de dominio -**Ingrese el nombre de dominio para que el enrutador busque en las consultas de DNS para interceptar y responder. Se pueden utilizar comodines en forma de asteriscos (*) para hacer coincidir un nivel de dominio. Por ejemplo, *.draytek.com coincidirá con nombres de dominio como www.draytek.com y ftp.draytek.com, mientras que www.draytek.* coincidirá con nombres de dominio como www.draytek.com y www.draytek.co. Reino Unido. **CNOMBRE-**Hacer clic**Agregar**para agregar un alias de nombre de dominio para el nombre de dominio. Haga clic en Eliminar junto a una entrada de alias para eliminarla.

	Lista de direcciones IP -La dirección IP que se indica aquí se utilizará para la asignación con el nombre de dominio especificado anteriormente. En general, un nombre de dominio se asigna a una dirección IP. Si es necesario, puede configurar la asignación de dos direcciones IP con el mismo nombre de dominio. **Agregar**–Hacer clic**Agregar**para abrir el cuadro de diálogo Agregar dirección IP:  - **Dirección IP del anfitrión –**Ingrese la dirección IP que se devolverá en respuesta a una consulta de DNS para los nombres de dominio y alias configurados. - **Solo responde al DNS....**–Seleccione usar esta dirección IP solo si la dirección IP del origen de la consulta de DNS pertenece a la misma subred que la dirección IP del host ingresada anteriormente. Una vez realizados los cambios, haga clic en**DE ACUERDO**para guardar y descartar el cuadro de diálogo, o**Cerca**para descartar los cambios y descartar el cuadro de diálogo. **Borrar**–Para eliminar una dirección IP, haga clic en ella y luego haga clic en Eliminar.
Si se selecciona el reenvío de DNS	**Nombre de dominio -**Ingrese el nombre de dominio para que el enrutador busque en las consultas de DNS para interceptar y responder. Se pueden utilizar comodines en forma de asteriscos (*) para hacer coincidir un nivel de dominio. Por ejemplo, *.draytek.com coincidirá con nombres de dominio como www.draytek.com y ftp.draytek.com, mientras que www.draytek.* coincidirá con nombres de dominio como www.draytek.com y www.draytek.co. Reino Unido. **Dirección IP del servidor DNS -**Ingrese la dirección IP del servidor DNS que desea usar para el reenvío de DNS.

Para guardar los cambios realizados en el perfil LAN DNS, haga clic en**DE ACUERDO**. Para borrar el perfil y restaurar los valores en blanco predeterminados de fábrica, haga clic en**Claro**.

II-5-3 Seguridad DNS

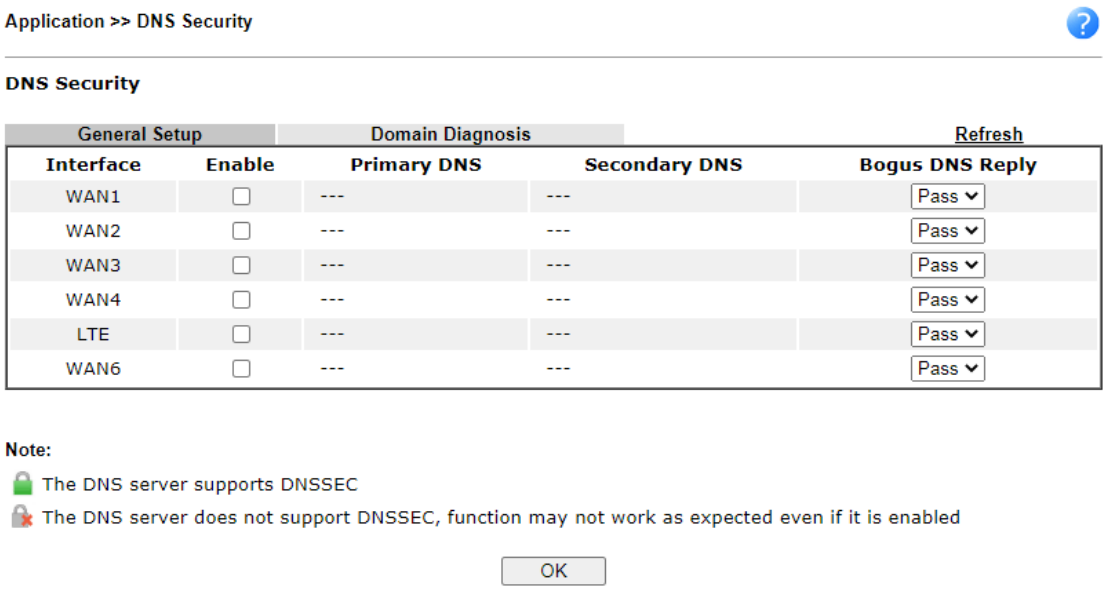
Las extensiones de seguridad del sistema de nombres de dominio (DNSSEC) protegen contra los ataques basados en DNS al autenticar las respuestas de DNS de los resolutores de DNS.

Los servidores DNS deben admitir la validación de seguridad DNS para que la función funcione correctamente.

Para configurar la seguridad DNS, desde el menú principal, haga clic en**Aplicaciones**, seguido por**Seguridad DNS**.

II-5-3-1 Configuración general

Todas las interfaces WAN del enrutador Vigor se pueden configurar con la seguridad DNS habilitada respectivamente.

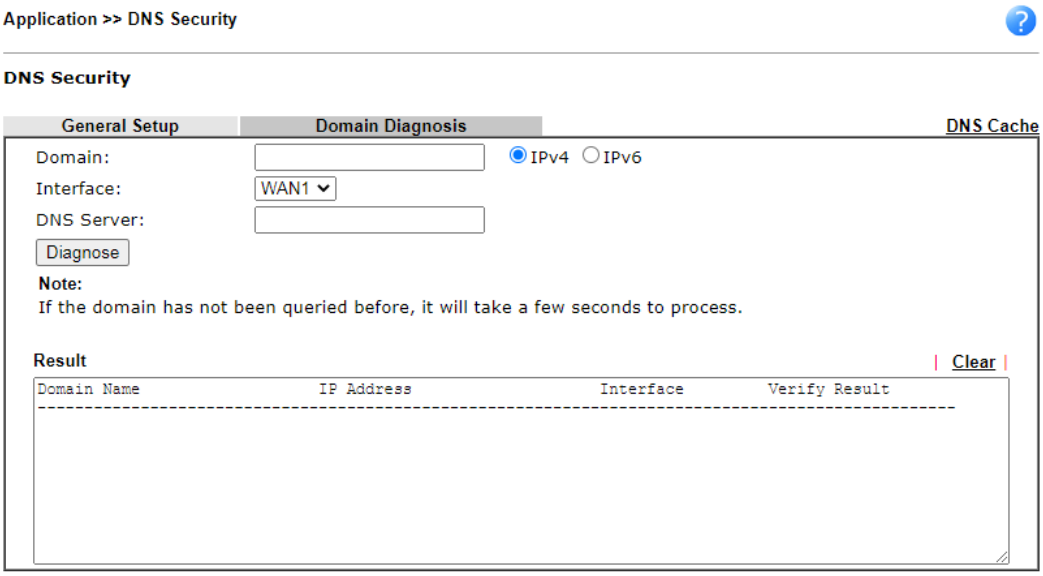


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Interfaz	El nombre de la interfaz WAN para la que se configurará la seguridad de DNS.
Permitir	Seleccione para habilitar la seguridad DNS para esta interfaz WAN.
DNS primario	Muestra la dirección IP del servidor DNS principal vigente para esta WAN.
DNS secundario	Muestra la dirección IP del servidor DNS secundario vigente para esta WAN.
Respuesta DNS falsa	Muestra la acción que se debe tomar para las respuestas de DNS que fallan en la autenticación. Elija Pasar o Bajar. **Aprobar**–Pase el resultado de DNS. **Gota**–No pase el resultado de DNS.

Prensa**DE ACUERDO**para guardar los cambios.

Mientras usa la función de diagnóstico de dominio, puede verificar si la función de seguridad DNS del enrutador funciona correctamente o si un dominio determinado está protegido por la seguridad DNS. Tenga en cuenta que la seguridad de DNS debe habilitarse primero o los resultados de la prueba no serían significativos.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Dominio	Ingrese la dirección del dominio para ser diagnosticado. Seleccione el tipo de dirección IP que se buscará. IPv4: busca registros A. IPv6: busca registros AAAA.
Interfaz	Seleccione el puerto WAN que se utilizará para la búsqueda.
Servidor DNS	Ingrese la dirección IPv4 del servidor DNS que se usará para la búsqueda.
Diagnosticar	Haga clic para comenzar la búsqueda de DNS.
Resultado	El historial de diagnóstico de dominio se muestra en el panel de resultados.

II-5-4 Horario

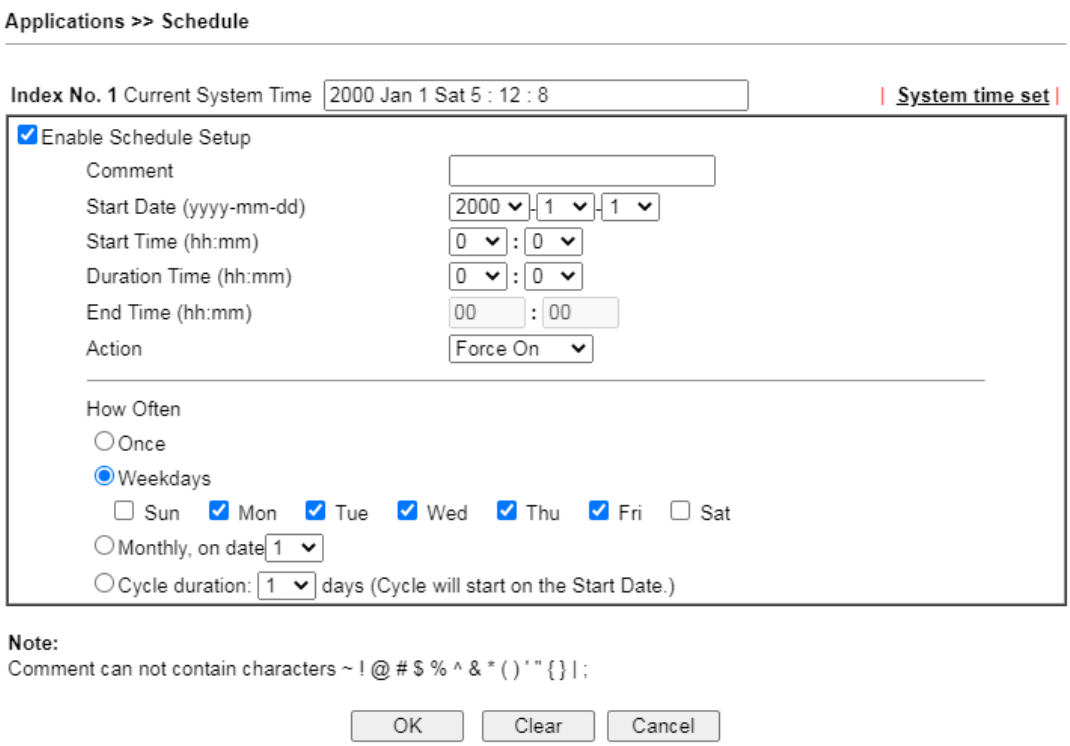
Los horarios se pueden crear y usar con las funciones del enrutador que los admitan, de modo que esas funciones se puedan activar y desactivar automáticamente en horarios preconfigurados.

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Hora actual del sistema	Muestra la hora actual del enrutador.
Configuración de la hora del sistema	Haga clic para navegar a**Mantenimiento del sistema >> Hora y fecha** para configurar la hora y la fecha del sistema.
Establecer como predeterminado de fábrica	Restablezca todos los horarios a los valores predeterminados de fábrica.
Índice	Muestra el número de índice de la entrada del programa.
Permitir	Seleccione para habilitar el horario; borre para deshabilitarlo.
Comentario	Muestra el nombre dado a la programación.
Tiempo	Muestra las horas de inicio y fin de la programación. El intervalo de tiempo del horario se indica en gris oscuro.

Frecuencia	Muestra los días de la semana configurados para el horario. Los días seleccionados se muestran en gris oscuro. - Si se enciende en verde, significa que dicho horario está activo.

Para configurar un horario, haga clic en su índice para que aparezca la página de configuración.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar configuración de programación	Seleccione para habilitar el horario; borre para deshabilitarlo.
Comentario	Nombre para identificar esta entrada del cronograma.
Fecha de inicio (aaaa-mm-dd)	La fecha en que la entrada surta efecto.
Hora de inicio (hh:mm)	La hora en que se activa la programación. Ver el**Con qué frecuencia** ajuste a continuación para más detalles.
Duración Tiempo (hh:mm)	Cuánto dura la acción cuando se activa el programa.
Hora de finalización (hh:mm)	Se calculará automáticamente cuando el tiempo de inicio y el tiempo de duración estén bien configurados.
Acción	Acción a realizar cuando se activa la programación. **Forzar**–Se activará la función con la que está asociado este horario. **Forzar abajo**–La función con la que está asociado este horario se desactivará.
Con qué frecuencia	Con qué frecuencia se activa la programación. - **Una vez**-El programa se activa una vez, en el**Fecha de inicio**en el**Hora de inicio**, Para el**Duración**. - **Días de semana**-El programa se activará repetidamente, comenzando en el**Fecha de inicio**en el**Hora de inicio**, en los días seleccionados de la semana, en el**Hora de inicio**, Para el **Duración**.

	- **Mensual, en la fecha –**El enrutador solo ejecutará la acción aplicada tal horario en la fecha (1 a 28) de un mes. - **Duración del ciclo –**Escriba un número como duración del ciclo. Luego, cualquier acción aplicada en dicho cronograma se ejecutará por varios días. Por ejemplo, se selecciona “3” como duración del ciclo. Es decir, la acción aplicada en dicho cronograma se ejecutará cada tres días a partir de la fecha definida en la Fecha de Inicio.

Para guardar los cambios realizados en el programa, haga clic en**DE ACUERDO**. Para borrar el programa y restaurar los valores en blanco predeterminados de fábrica, haga clic en**Claro**. Para cancelar los cambios y volver a la página principal de Programación, haga clic en**Cancelar**.

Ejemplo

Suponga que desea controlar la conexión de acceso a Internet PPPoE para que esté siempre activada (Force On) de 9:00 a 18:00 durante toda la semana. En otro momento, la conexión de acceso a Internet debe estar desconectada (Force Down).

Oficina
Hora:

(Forzar)

lun - dom **09 a.m** **a** **18:00**

1. Asegúrese de que la conexión PPPoE y**Configuración de tiempo**está funcionando correctamente.
2. Configure el PPPoE siempre encendido de 9:00 a 18:00 durante toda la semana.
3. Configure el**Forzar abajo**de 18:00 a 09:00 del día siguiente durante toda la semana.
4. Asigne estos dos perfiles al perfil de acceso a Internet PPPoE. Ahora, la conexión a Internet PPPoE seguirá el orden de programación para realizar**Forzar**o**Forzar abajo**acción de acuerdo con el plan de tiempo que se ha predefinido en los perfiles de horario.

II-5-5 RADIO/TACACS+

El Servicio de Usuario de Acceso Telefónico de Autenticación Remota (RADIUS) es un protocolo cliente/servidor de autenticación de seguridad que admite autenticación, autorización y contabilidad, que es ampliamente utilizado por los proveedores de servicios de Internet. Es el método más común para autenticar y autorizar usuarios de redes de acceso telefónico y tunelizado.

El enrutador admite servidores TACACS+ externos y RADIUS internos y externos para la autenticación de usuarios. Los servicios que requieren autenticación de usuario incluyen WLAN y VPN.

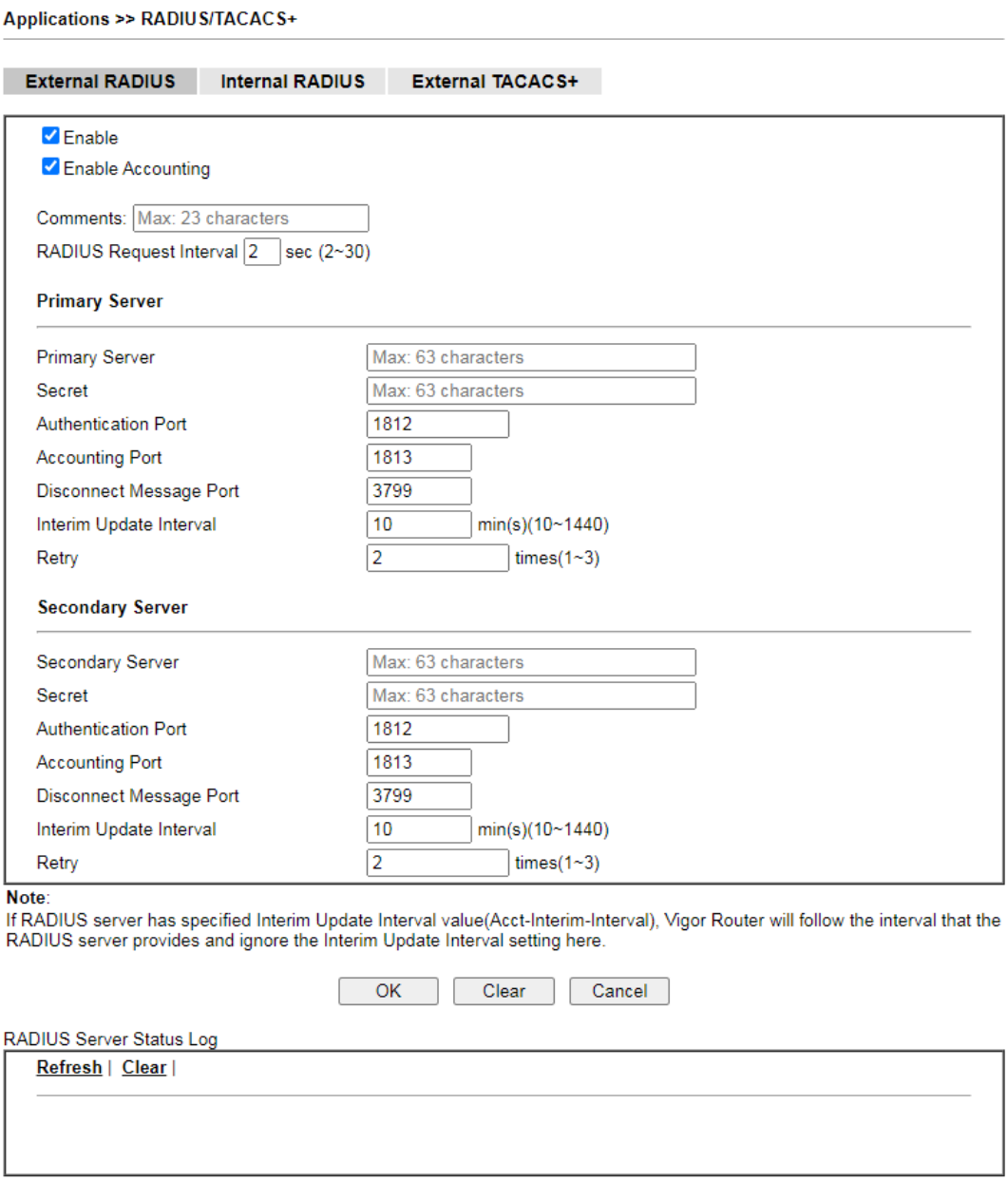
Para configurar los servidores RADIUS o TACACS+, desde el menú principal, seleccione**Aplicaciones >> RADIO/TACACS+**.

II-5-5-1 RADIO externo

La función de cliente RADIUS integrada permite que el enrutador ayude al usuario de marcación remota o a una estación inalámbrica y al servidor RADIUS a realizar la autenticación mutua. Permite la autenticación de acceso remoto centralizado para la gestión de la red.

El enrutador Vigor se puede operar como un cliente RADIUS. Esta página web se utiliza para configurar los ajustes del servidor RADIUS externo. Luego, los usuarios de LAN del enrutador Vigor serán autenticados y contabilizados por dicho servidor para la aplicación de red.

Seleccione RADIUS externo para configurar el enrutador para usar un servidor RADIUS externo para la autenticación de usuarios.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Marque para habilitar el perfil de cliente RADIUS. **Comentarios**- Introduzca una breve descripción para este perfil. **Intervalo de solicitud RADIUS**-Establezca un valor de tiempo de espera para el enrutador que espera una respuesta del servidor RADIUS. Si no hay respuesta, el enrutador Vigor enviará la solicitud de autenticación nuevamente. **Habilitar contabilidad** -RADIUS Accounting es un mecanismo de facturación de clientes de red para el servidor RADIUS. Si está habilitado, el enrutador Vigor enviará una solicitud de contabilidad (por ejemplo, dirección IP, tráfico del cliente) al servidor RADIUS especificado periódicamente. - **Puerto Contable** -Establezca el número de puerto UDP (1813 por defecto) como el puerto de contabilidad. - **Desconectar puerto de mensajes** -Establezca un número de puerto UDP (3799 por defecto) para recibir el

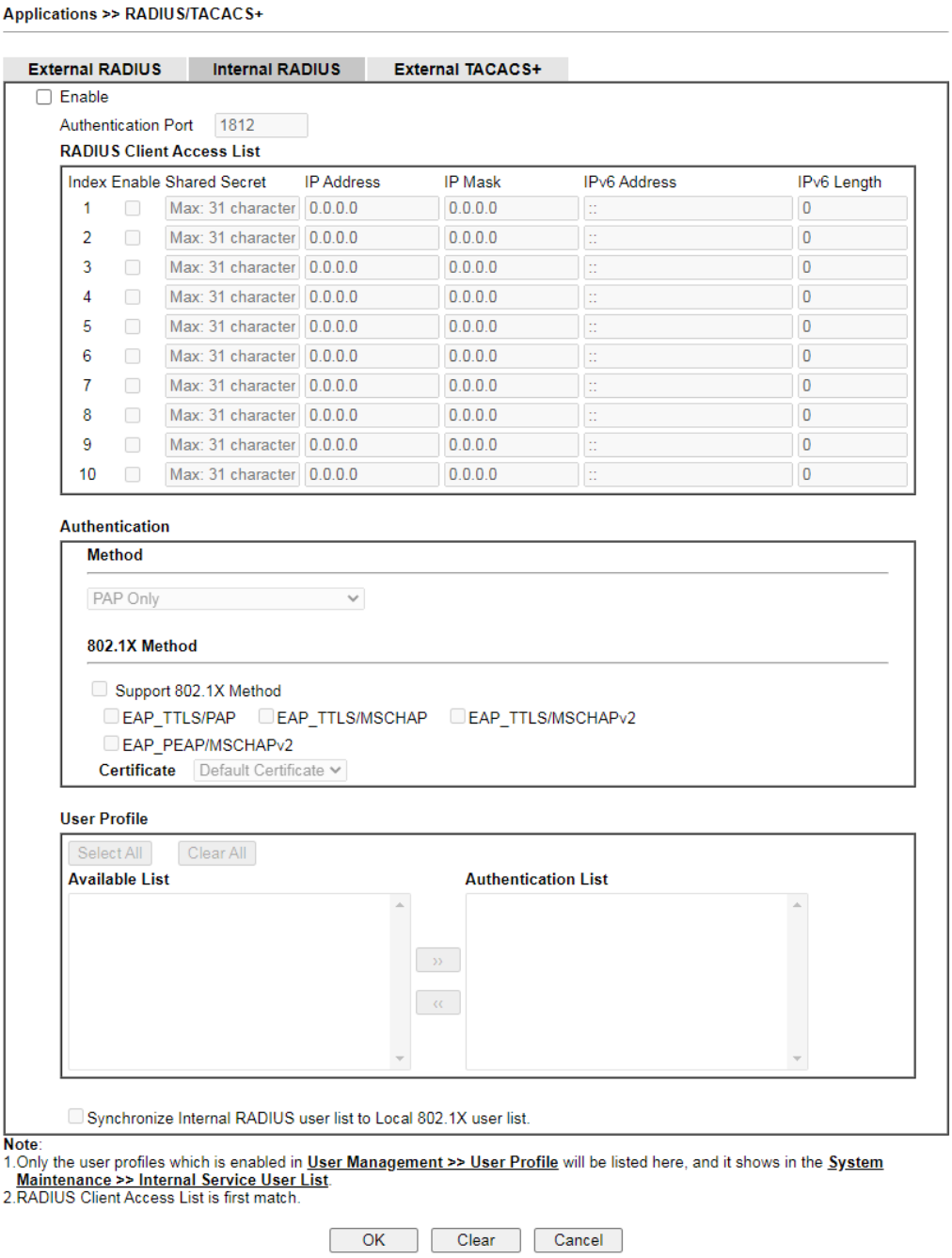
	paquetes de solicitud de desconexión del servidor AAA. Tenga en cuenta que estos paquetes han sido aceptados por el servidor RADIUS antes de ser desconectados por el servidor AAA. - **Intervalo de actualización provisional -**Establezca un valor (10 minutos por defecto). Indica el tiempo entre cada transmisión de una actualización provisional para una sesión específica.
Servidor primario	**Servidor primario**-Ingrese la dirección IP del servidor RADIUS. **Secreto**-El servidor y el cliente RADIUS comparten un secreto que se utiliza para autenticar los mensajes que se envían entre ellos. Ambos lados deben estar configurados para usar el mismo secreto compartido. La longitud máxima del secreto compartido que puede establecer es de 36 caracteres. **Puerto de autenticación**-El número de puerto UDP que utiliza el servidor RADIUS. El valor predeterminado es 1812, basado en RFC 2138. **Rever**-Establezca el número de intentos para realizar la reconexión con el servidor RADIUS. Si la conexión (con el servidor principal) sigue fallando, detenga el intento de conexión y comience a conectarse con el servidor secundario.
Servidor Secundario	**Servidor Secundario**-Ingrese la dirección IP del servidor RADIUS. **Secreto**-El servidor y el cliente RADIUS comparten un secreto que se utiliza para autenticar los mensajes que se envían entre ellos. Ambos lados deben estar configurados para usar el mismo secreto compartido. La longitud máxima del secreto compartido que puede establecer es de 36 caracteres. **Puerto de autenticación**-El número de puerto UDP que utiliza el servidor RADIUS. El valor predeterminado es 1812, basado en RFC 2138. **Rever**-Establezca el número de intentos para realizar la reconexión. Si la conexión (con el servidor secundario) aún falla, detenga el intento de conexión. La autenticación del cliente se determinaría como "fallida".
Registro de estado del servidor RADIUS	Muestra el registro del estado actual del servidor RADIUS.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para restablecer todas las configuraciones en blanco, haga clic en**Claro**.

II-5-5-2 RADIO Interno

Excepto por ser un cliente RADIUS incorporado, el enrutador Vigor también puede funcionar como un servidor RADIUS que realiza la autenticación de seguridad por sí mismo. Esta página se utiliza para configurar los ajustes del servidor RADIUS interno. Luego, el usuario de LAN del enrutador Vigor será autenticado directamente por el enrutador Vigor.

Seleccione RADIUS interno para configurar el servidor RADIUS integrado del enrutador.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Seleccione para habilitar el servidor RADIUS interno del enrutador.
Puerto de autenticación	El puerto UDP para mensajes de autenticación.
Lista de acceso de clientes RADIUS	Solo los clientes que cumplan con los criterios configurados en la lista de acceso pueden acceder al servidor RADIUS. **Permitir**-Seleccione para habilitar esta entrada de cliente. **Secreto compartido**-Una cadena de texto conocida tanto por el servidor RADIUS del enrutador como por el cliente RADIUS que se utiliza para autenticar los mensajes enviados entre ellos. La longitud máxima es de 36 caracteres. **Dirección IP**-Dirección base del bloque IP. **Máscara IP**-Introduzca la máscara de IP para configurar el tamaño de la IP

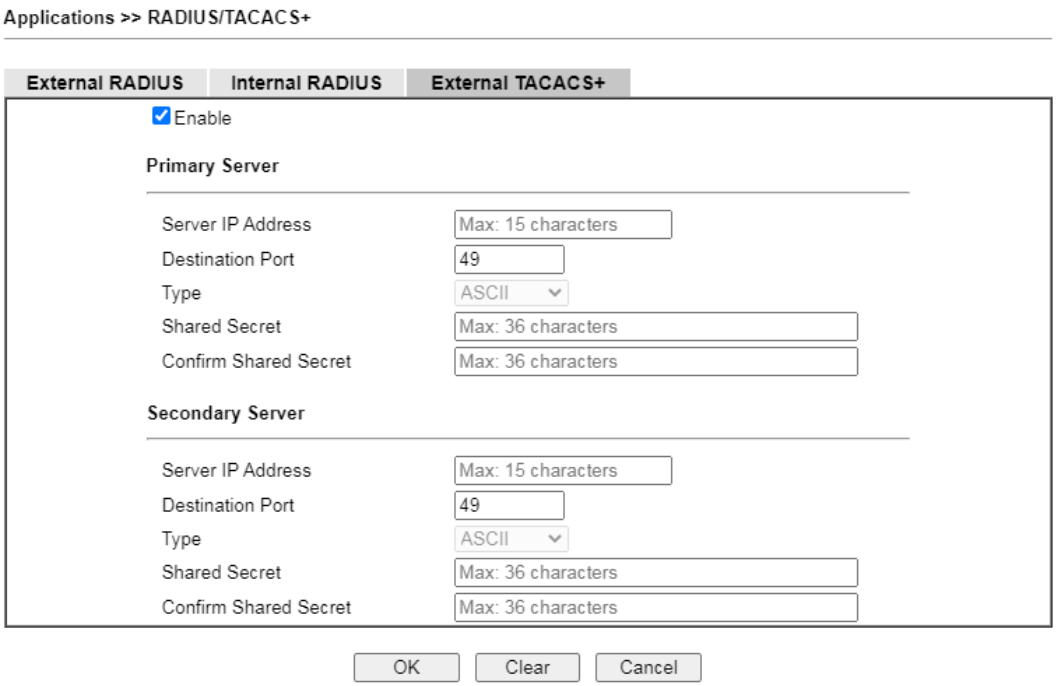
	bloquear. **Dirección IPv6**-Dirección base del bloque IPv6. **Longitud de IPv6**-La longitud del prefijo del bloque IPv6.
Autenticación	Configura los ajustes de autenticación. Especifique la forma de autenticar al cliente inalámbrico. **Papa Noel -**Solo se utilizará el Protocolo de autenticación de contraseña para validar a los usuarios. **PAP/CHAP/MS-CHAP/MS-CHAPv2 –**PAP, CHAP (Challenge-Handshake Authentication Protocol) y las versiones de Microsoft de CHAP se pueden usar para validar a los usuarios. **Compatible con el método 802.1X**–El servidor RADIUS integrado que ofrece el enrutador Vigor puede actuar como servidor AAA. Seleccione para habilitar la compatibilidad con 802.1X.
Perfil del usuario	Durante el proceso de autenticación de seguridad, se requerirá la cuenta de usuario y la contraseña de usuario para la identidad. autenticación. Antes de configurar dicha página, cree al menos un perfil de usuario en**Gestión de usuarios>>Perfil de usuario**primero. **Seleccionar todo**–Haga clic para mover todos los perfiles de usuario de la Lista disponible a la Lista de autenticación. **Limpiar todo**-Haga clic para eliminar todos los perfiles de usuario de la lista de autenticación. **Lista disponible**–Los perfiles de usuario**sin**Servidor RADIUS habilitado en**Gestión de usuarios >> Perfil de usuario**aparecerá en este campo. **Lista de autenticación**–Los perfiles de usuario con el servidor RADIUS habilitado en**Gestión de usuarios >> Perfil de usuario**aparecerá en este campo.
Sincronizar interna **Lista de usuarios RADIUS a lista de usuarios Local 802.1X**	Los usuarios pueden ser autenticados por el servidor RADIUS y 802.1X local para obtener cierto servicio de red. No es necesario crear nuevos perfiles de usuario (que contengan cuentas de usuario y contraseñas de usuario) para RADIUS y 802.1X local respectivamente. Simplemente seleccione actualizar la lista de autenticación 802.1X para que coincida con la lista de autenticación RADIUS.

Para agregar un perfil de usuario al servidor RADIUS, selecciónelo en**Lista disponible**, luego haga clic en el botón >>. Para eliminar un perfil de usuario del servidor RADIUS, selecciónelo en**Lista de autenticación seleccionada**, luego haga clic en el botón <<.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para restablecer todas las configuraciones en blanco, haga clic en**Claro**.

II-5-5-3 TACACS+ externo

Significa Terminal Access Controller Access-Control System Plus. Funciona como lo hace RADIUS. Haga clic en el**TACACS+ externo**para abrir la siguiente página:



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Seleccione para habilitar el uso de un servidor TACACS+ externo.
Servidor principal / Servidor Secundario	Se permite configurar dos servidores TACACS+ externos en esta página. El servidor TACACS+ secundario se usará como servidor de respaldo cuando el servidor TACACS+ principal esté inactivo.
Dirección IP del servidor	La dirección IP del servidor TACACS+.
Puerto de destino	El puerto utilizado por el servidor TACACS+. El puerto 49 es el más común.
Secreto compartido	Una cadena de texto conocida tanto por el servidor TACACS+ como por el cliente (el enrutador) que se utiliza para autenticar los mensajes que se envían entre ellos. La longitud máxima es de 36 caracteres.
Confirmar secreto compartido	Ingrese el secreto compartido nuevamente para verificarlo.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para restablecer todas las configuraciones en blanco, haga clic en**Claro**.

II-5-6 Directorio activo/LDAP

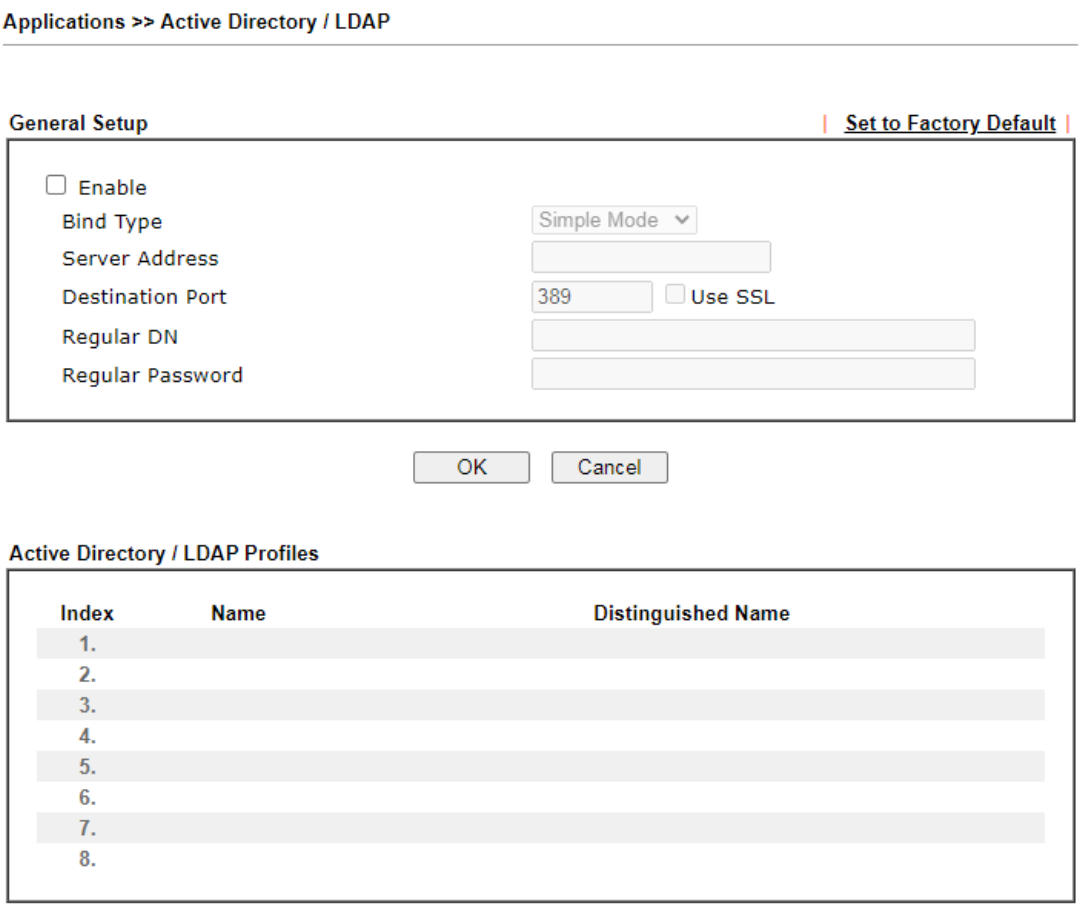
El protocolo ligero de acceso a directorios (LDAP) es un protocolo estándar de la industria para mantener y acceder a información de directorio en una red. Cuando se usa junto con un enrutador Vigor, LDAP se puede usar para autenticar los intentos de conexión VPN.

Active Directory (AD) es un servicio de directorio de Microsoft que admite consultas LDAP.

Para configurar los ajustes de Active Directory o LDAP, desde el menú principal, seleccione**Aplicaciones >> Directorio Activo/LDAP**.

II-5-6-1 Configuración general

Para configurar los ajustes del servidor LDAP, seleccione**Configuración general**.



Los ajustes disponibles se explican a continuación:

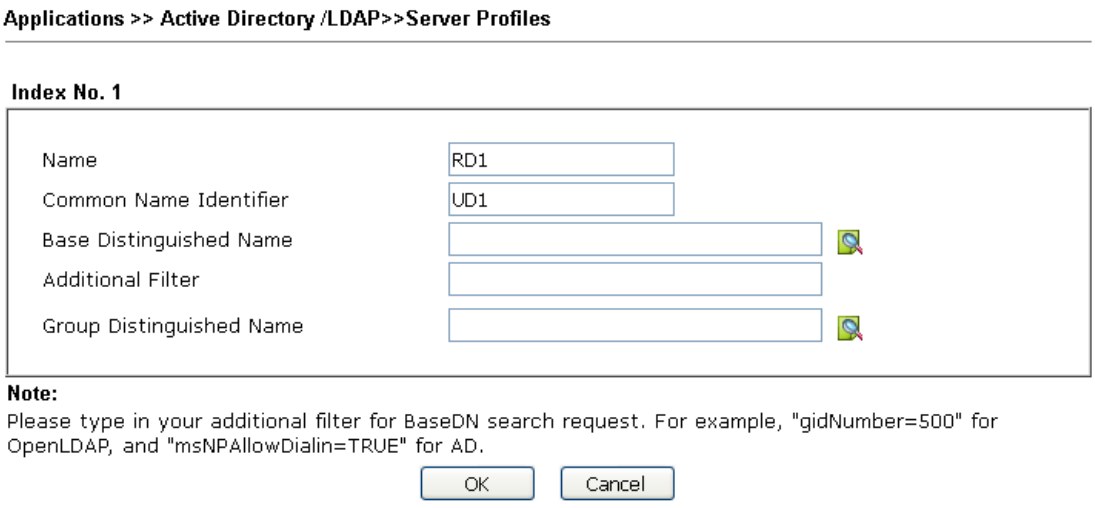
Artículo	Descripción
Permitir	Seleccione para habilitar el cliente LDAP. Si está habilitado, los perfiles LDAP estarán disponibles para la configuración.
Tipo de enlace	Seleccione uno de los 3 tipos de enlace: - **Modo simple**–Inicie la operación de vinculación (autenticación) sin realizar la búsqueda de usuarios. Este modo se puede utilizar cuando todos los usuarios pertenecen a la misma sucursal en la estructura LDAP. - **Anónimo**–Enlace de forma anónima, sin proporcionar el

	nombre distinguido (DN) y contraseña, y realice la búsqueda de usuarios. Este modo se puede utilizar cuando no todos los usuarios pertenecen a la misma sucursal y el servidor permite búsquedas anónimas. - **Modo normal**–Igual que el modo Anónimo, excepto que el DN y la contraseña se envían al servidor. Este modo se puede utilizar cuando no todos los usuarios pertenecen a la misma sucursal y el servidor no permite búsquedas anónimas. Para el modo regular, deberá ingresar el**DN normal**y **Contraseña normal**.
Dirección del servidor	La dirección de red del servidor LDAP.
Puerto de destino	El puerto de red en el que escucha el servidor LDAP. Los puertos predeterminados son 389 para conexiones no seguras y 636 para conexiones LDAPS (LDAP sobre SSL).
Usar SSL	Seleccione para usar la capa de sockets seguros (SSL) para el tráfico LDAP.
DN normal	Ingrese el nombre distinguido de LDAP para la autenticación si**Tipo de enlace** se establece en**Modo normal**.
Contraseña normal	Ingrese la contraseña LDAP para la autenticación si**Tipo de enlace**se establece en**Modo normal**.
Directorio activo/Perfiles LDAP	Se pueden crear hasta 8 perfiles LDAP. Estos perfiles se utilizarían con la Gestión de usuarios para diferentes propósitos en la gestión.

Para guardar los cambios en la página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**.

II-5-6-2 Directorio activo/Perfiles LDAP

Para configurar un perfil LDAP, haga clic en su índice para mostrar la siguiente página de configuración.



Los ajustes disponibles se explican a continuación:

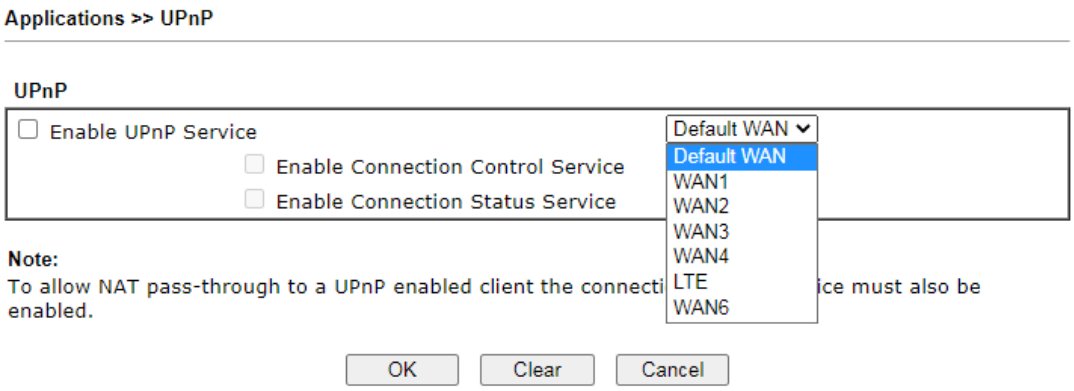
Artículo	Descripción
Nombre	Nombre que identifica a este perfil. La longitud máxima es de 19 caracteres.
Identificador de nombre común	El atributo de nombre común, que suele ser "cn" en la mayoría de las configuraciones de LDAP.
Nombre distinguido básico El punto de partida de la búsqueda de usuarios en el directorio LDAP, por	

	ejemplo, dc=draytek,dc=com. – haga clic en este icono para mostrar una lista de DN válidos en el LDAP directorio.
Filtro adicional	Filtro adicional que se aplicará a la solicitud de búsqueda para identificar a los usuarios elegibles. Por ejemplo, – “OpenLDAP: (gidNumber=500)” Aquí, el ID de grupo 500 es el grupo de usuarios de acceso telefónico. – “Directorio Activo: (msNPAllowDialin=TRUE)” El atributo msNPAllowDialin indica que el usuario tiene permiso para marcar de forma remota.
Grupo Distinguido Nombre	El DN base del árbol en el directorio LDAP que contiene grupos, por ejemplo, ou=groups,dc=draytek,dc=com. - haga clic en este icono para mostrar una lista de DN válidos en el LDAP directorio.

Para guardar los cambios en la página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**.

II-5-7 UPnP

Para configurar los ajustes de UPnP, desde el menú principal, seleccione**Aplicaciones >> UPnP**.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar el servicio UPNP	Seleccione para habilitar UPnP.
WAN predeterminada	Seleccione el puerto WAN en el que se abrirán los puertos en respuesta a los comandos UPnP.
Habilitar conexión Servicio de control	Seleccione para habilitar el servicio de control de conexión.
Habilitar servicio de estado de conexión	Seleccione para habilitar el servicio de estado de conexión.

Para guardar los cambios en la página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**; para revertir todas las configuraciones a los valores predeterminados de fábrica, seleccione**Claro**.

El recordatorio con respecto a la preocupación por Firewall y UPnP: **No**

puedo trabajar con el software de firewall

Habilitar las aplicaciones de firewall en su PC puede hacer que la función UPnP no funcione correctamente. Esto se debe a que estas aplicaciones bloquearán la capacidad de acceso de algunos puertos de red.

Consideraciones de Seguridad

La activación de UPnP permite que cualquier aplicación o dispositivo de red abra puertos en el lado WAN para permitir conexiones a la LAN, lo que podría comprometer la seguridad de la red. Además, si las aplicaciones UPnP o los dispositivos de red funcionan mal o terminan de manera anormal, los puertos abiertos pueden permanecer abiertos indefinidamente y, por lo tanto, aumentan las posibilidades de que sean explotados por personas malintencionadas.

Si no tiene aplicaciones o dispositivos de red que requieran UPnP, se recomienda desactivar UPnP.

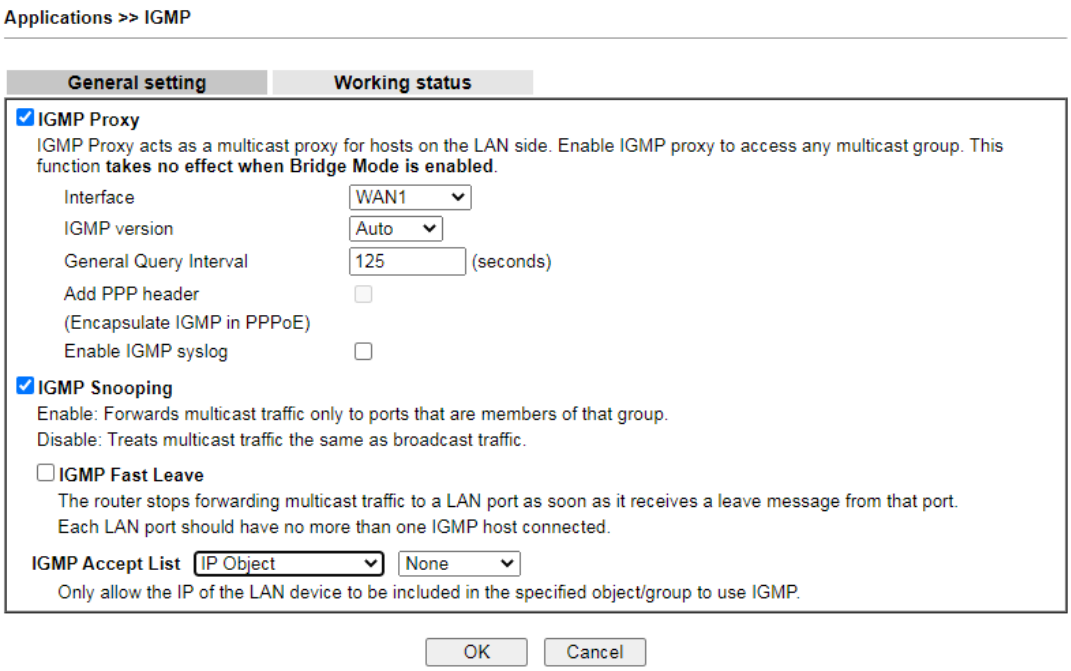
Información	Se requiere UPnP para algunas aplicaciones como PPS, Skype, eMule... y etc. Si no está familiarizado con UPnP, se sugiere desactivar esta función por seguridad.

II-5-8 IGMP

El Protocolo de administración de grupos de Internet (IGMP) es un protocolo de comunicación IPv4 para establecer membresías de grupos de multidifusión.

Para configurar los ajustes de IGMP, desde el menú principal, seleccione**Aplicaciones >> IGMP**.

II-5-8-1 Configuración general



Los ajustes disponibles se explican a continuación:

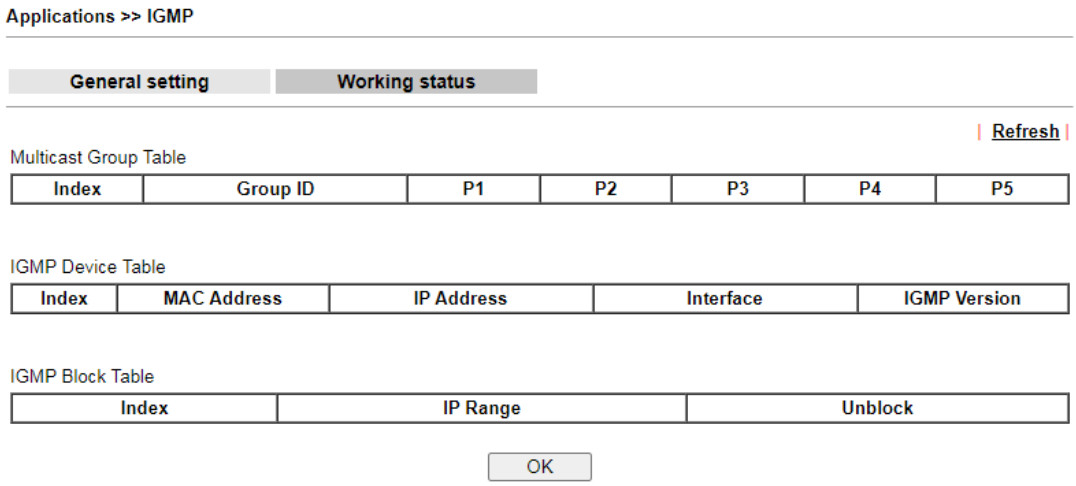
Artículo	Descripción
Proxy IGMP	Marque esta casilla para habilitar esta función. La aplicación de multidifusión se ejecutará a través del puerto WAN/PVC/VLAN. Además, dicha función está disponible en modo NAT. **Interfaz**–Especifique una interfaz para los paquetes que pasan. **versión IGMP**–En la actualidad, el enrutador Vigor admite dos versiones (v2 y v3). Elija la versión correcta según el servicio de IPTV al que se suscriba. **Intervalo de consulta general**–El enrutador Vigor verificará periódicamente qué IP obtiene el servicio de IPTV enviando una consulta. Podría causar inconvenientes para el cliente. Por lo tanto, establezca un tiempo adecuado (unidad: segundo) como intervalo de consulta para limitar la frecuencia de consulta enviada por el enrutador Vigor. **Agregar encabezado PPP**–Marque esta casilla si el tipo de interfaz para IGMP es PVC/VLAN. Depende de las especificaciones reguladas por cada ISP. Si no tiene idea de habilitar o deshabilitar, simplemente comuníquese con sus proveedores de ISP. **Habilitar registro del sistema IGMP**-Marque la casilla para almacenar el estado de IGMP en Syslog.

Indagación IGMP	Seleccione para habilitar IGMP Snooping para que el tráfico de multidifusión se reenvíe a los clientes IGMP que se han unido a un grupo de multidifusión.
Salida rápida de IGMP	Esta opción se muestra solo cuando IGMP Snooping está habilitado. Seleccione para habilitar IGMP Fast Leave. Normalmente, cuando el enrutador recibe un mensaje de "abandono" de un host IGMP, enviará un mensaje de consulta del último miembro para ver si todavía hay miembros dentro del grupo de multidifusión. Cuando Fast Leave está habilitado, la multidifusión para un grupo finaliza inmediatamente cuando el último host de ese grupo envía un mensaje de "abandono".
Lista de aceptación de IGMP	Seleccione Objeto de IP o Grupo de IP. Solo la IP del dispositivo LAN dentro del objeto IP/grupo IP podrá usar IGMP.

Para guardar los cambios en la página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**.

II-5-8-2 Estado de funcionamiento

Muestra una lista de grupos de multidifusión activos.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Actualizar	Haga clic para volver a cargar la tabla de grupos de multidifusión con la información más reciente.
Índice	Número de índice del grupo de multidifusión.
Identificación del grupo	Puerto de ID del grupo de multidifusión, que está dentro del rango de IP reservado para IGMP, 224.0.0.0 a 239.255.255.254.
P1 a P5	Puertos LAN que tienen hosts IGMP unidos a este grupo de multidifusión.

II-5-9 Despertar en LAN/WAN

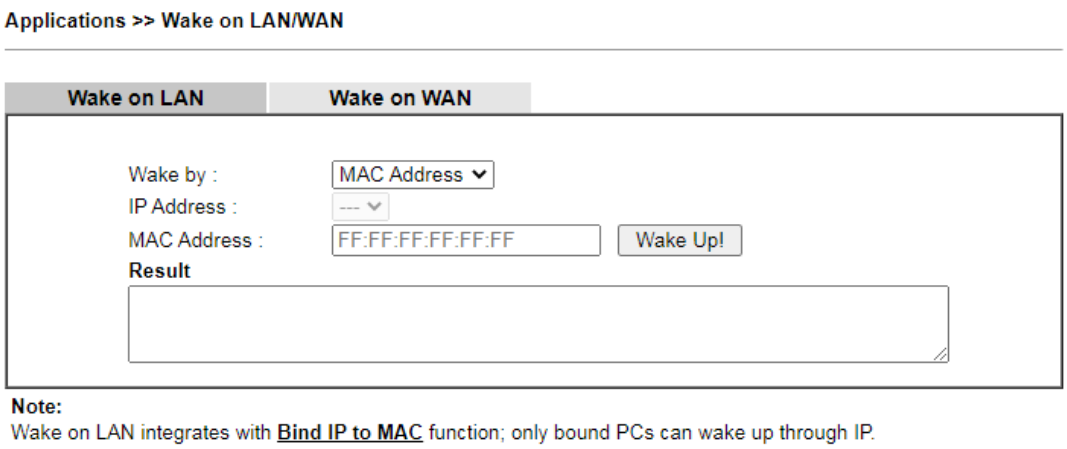
II-5-9-1 Despertar en LAN

Con la función Wake on LAN (WoL), los clientes de LAN que admiten WoL se pueden encender o reanudar desde el modo de suspensión a través de la red, sin necesidad de acceso físico al dispositivo.

Para que los clientes LAN puedan reactivarse desde los estados de suspensión o apagado, la tarjeta de interfaz de red debe estar configurada para monitorear los mensajes Wake-on-LAN. Consulte la documentación del cliente LAN para obtener detalles sobre cómo configurar su interfaz de red para Wake on LAN.

Si desea poder seleccionar la dirección IP del cliente Wake-on-LAN, primero debe vincular su dirección MAC a una dirección IP estática mediante la función Vincular IP a MAC.

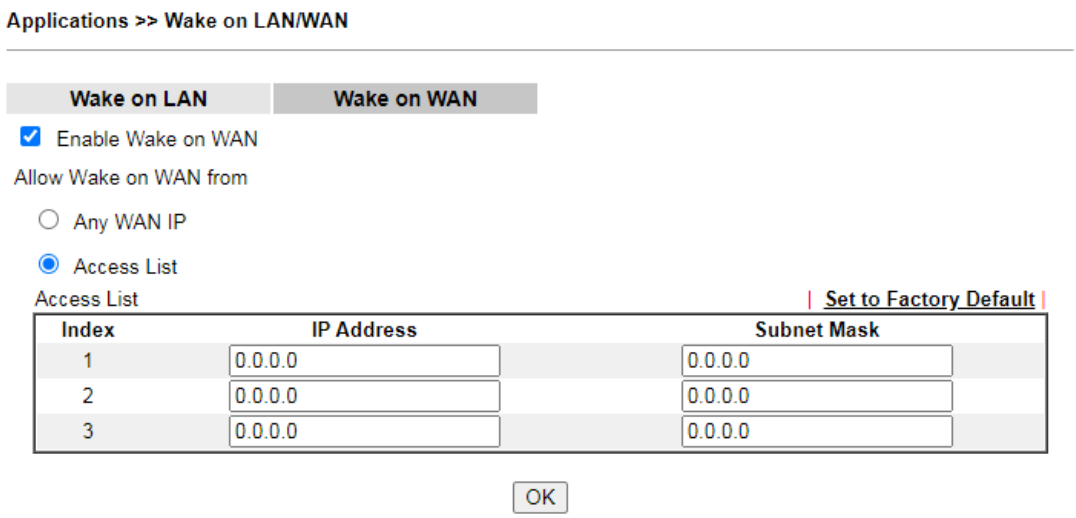
Para configurar los ajustes de Wake on LAN, en el menú principal, seleccione**Aplicaciones >> Wake on LAN**.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
despertar por	Hay dos tipos que le permiten activar la IP enlazada. - Si elige Wake by**Dirección MAC**, debe ingresar la dirección MAC correcta del host en los cuadros de dirección MAC. - Si tu eliges**Despertar por dirección IP**, debe elegir la dirección IP correcta.
Dirección IP	Las direcciones IP que se han configurado en **Cortafuegos >> Vincular IP a MAC**se mostrará en esta lista desplegable. Elija la dirección IP de la lista desplegable que desea activar.
Dirección MAC	Escriba cualquiera de las direcciones MAC de las PC vinculadas.
Despertar	Haga clic en este botón para activar la IP seleccionada. Consulte la figura siguiente. El resultado se mostrará en la caja.
Resultado	Resultado de la transmisión del mensaje Wake-on-LAN.

Para configurar los ajustes de Wake on WAN, en el menú principal, seleccione**Aplicaciones >> Wake on LAN** y seleccione la pestaña de**Despertar en WAN**.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar Wake on WAN	Seleccione para habilitar la función.
Permitir Wake on WAN desde	Establezca la ruta para que el paquete de inicio (enviado por un teléfono móvil) se entregue al dispositivo remoto. **Cualquier IP WAN**-Cualquier IP de WAN se puede utilizar como ruta para activar el dispositivo remoto. **Lista de acceso**-Ingrese la dirección IP WAN con la máscara de subred. Más tarde, use su teléfono móvil (instalando primero una aplicación para enviar los paquetes de arranque) para conectarse a la red del enrutador Vigor. Los paquetes de inicio se transferirán al dispositivo remoto a través de cualquier IP WAN o la IP que figura en la Lista de acceso.

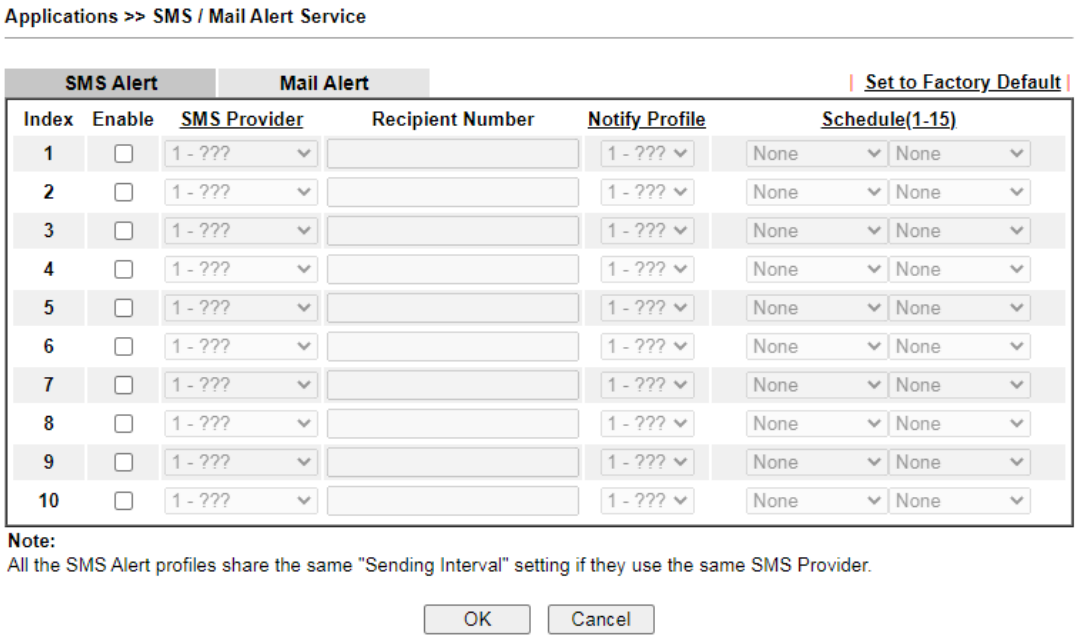
II-5-10 Servicio de Alerta por SMS/Correo

La función de SMS (Servicio de mensajes cortos)/Alerta de correo es que el enrutador Vigor envía un mensaje al móvil o al buzón de correo electrónico del usuario a través del proveedor de servicios especificado para ayudar al usuario a conocer las situaciones anormales en tiempo real.

El enrutador Vigor le permite configurar hasta**10**Perfiles de SMS que se enviarán de acuerdo con diferentes condiciones.

II-5-10-1 Alerta SMS

Esta página le permite especificar el proveedor de SMS, quién recibirá el SMS, cuál es el contenido y cuándo se enviará el SMS.

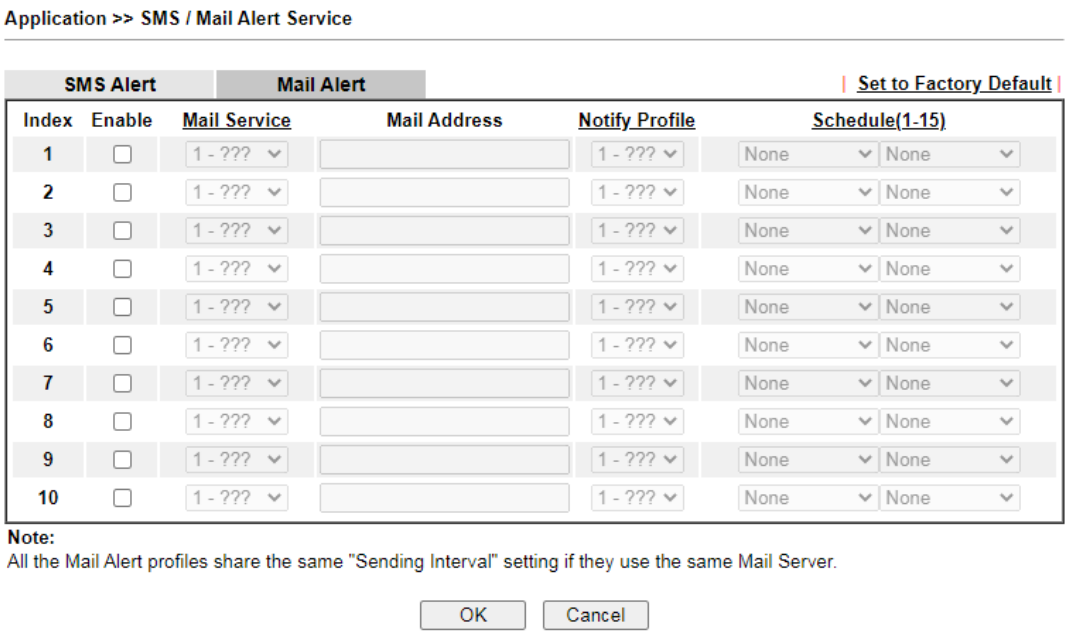


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Marque la casilla para habilitar o deshabilitar el perfil.
Proveedor de SMS	Utilice la lista desplegable para elegir el proveedor de servicios de SMS. Puedes hacer clic**Proveedor de SMS**enlace para definir el servidor SMS.
Número de destinatario	Introduce el número de teléfono de quien recibirá el SMS.
Notificar perfil	Utilice la lista desplegable para elegir un perfil de mensaje. El destinatario obtendrá el contenido indicado en el perfil del mensaje. Puede hacer clic en el**Notificar perfil**enlace para definir el contenido del SMS.
Horario (1-15)	Ingrese el número de horario en el que se enviará el SMS. Puede hacer clic en el**Horario (1-15)**enlace para definir el horario.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

Esta página le permite especificar el perfil del servidor de correo, quién recibirá el correo electrónico de notificación, cuál es el contenido y cuándo se enviará el mensaje.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Marque la casilla para habilitar/deshabilitar este perfil.
Servicio de correo	Utilice la lista desplegable para elegir el objeto del servicio de correo. Todos los objetos disponibles se crean en**Configuración de objetos>>Objeto de servicio de correo/SMS**. Si no hay ningún objeto en la lista, haga clic en**Servicio de correo**enlace para definir uno nuevo con el proveedor de servicios especificado.
Correo Electronico	Introduzca la dirección de correo electrónico de la persona que recibirá el mensaje de notificación.
Notificar perfil	Utilice la lista desplegable para elegir un perfil de mensaje. El destinatario obtendrá el contenido indicado en el perfil del mensaje. Puede hacer clic en el**Notificar perfil**enlace para definir el contenido del mensaje de correo.
Horario (1-15)	Ingrese el número de horario en el que se enviará la notificación. Puede hacer clic en el**Horario (1-15)**enlace para definir el horario.

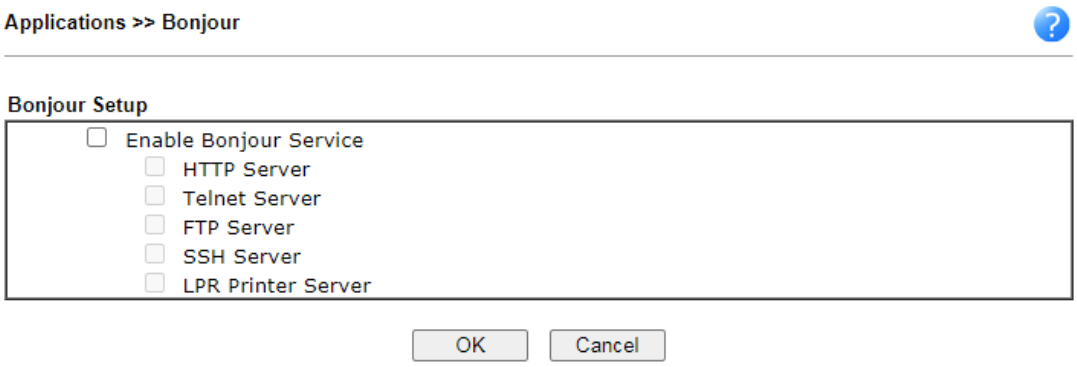
Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

II-5-11 Buen día

Bonjour es un protocolo de detección de servicios integrado en Mac OS X; para la plataforma Windows o Linux, existe un software correspondiente para habilitar esta función de forma gratuita.

Por lo general, los usuarios tienen que configurar el enrutador o las computadoras personales para usar los servicios anteriores. A veces, la configuración (p. ej., configuración de IP, número de puerto) es complicada y no es fácil de completar. El propósito de Bonjour es disminuir la configuración de los ajustes (por ejemplo, la configuración de IP). Si el host y la computadora del usuario tienen instalado el controlador bonjour del complemento, pueden utilizar el servicio ofrecido por el enrutador haciendo clic en el icono del nombre del enrutador. En resumen, lo que los Clientes/usuarios deben saber es solo el nombre del enrutador.

Para habilitar el servicio Bonjour, haga clic en**Aplicación>>Bonjour**para abrir la página siguiente. Marque la(s) casilla(s) de los servicios del servidor que desea compartir con los clientes LAN.

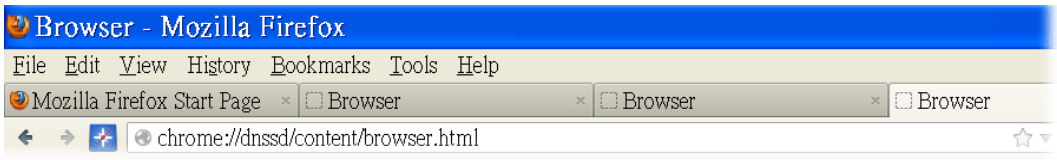


Los ajustes disponibles se explican a continuación:

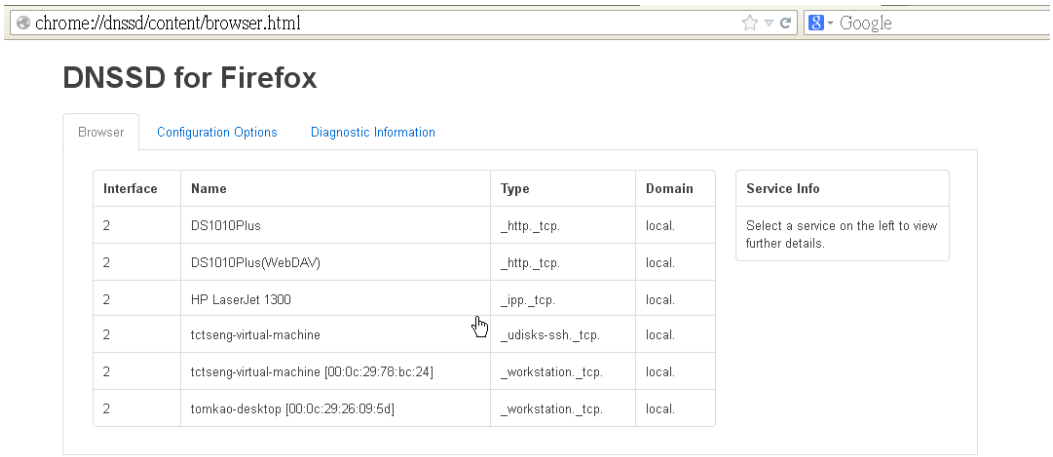
Artículo	Descripción
Habilitar el servicio Bonjour	Seleccione para habilitar el servicio Bonjour en el enrutador. El resto de las casillas de verificación estarán habilitadas para su selección cuando se haya seleccionado esta casilla de verificación.
Servidor HTTP	Seleccione para permitir que el servidor HTTP del enrutador se descubra a través de Bonjour.
Servidor Telnet	Seleccione para permitir que el servidor telnet del enrutador se detecte a través de Bonjour.
Servidor FTP	Seleccione para permitir que el servidor FTP del enrutador se descubra a través de Bonjour.
Servidor SSH	Seleccione para permitir que el servidor SSH del enrutador se descubra a través de Bonjour.
Servidor de impresión LPR	Seleccione para permitir que el servidor LPR del enrutador se descubra a través de Bonjour. Esto permite descubrir las impresoras conectadas a los puertos USB del enrutador.

A continuación se muestra un ejemplo para aplicar la función bonjour de que el enrutador Vigor se puede usar como servidor FTP.

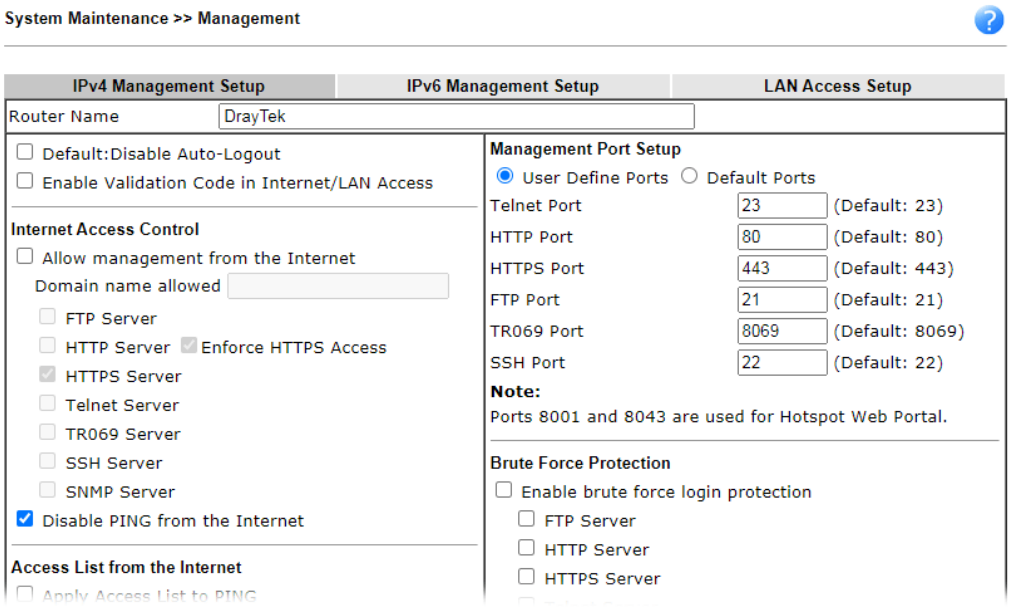
1. Aquí, usamos Firefox y DNSSD para descubrir el servicio en tal caso. Por lo tanto, solo asegúrese de que el programa cliente Bonjour y DNSSD para Firefox estén instalados en la computadora.



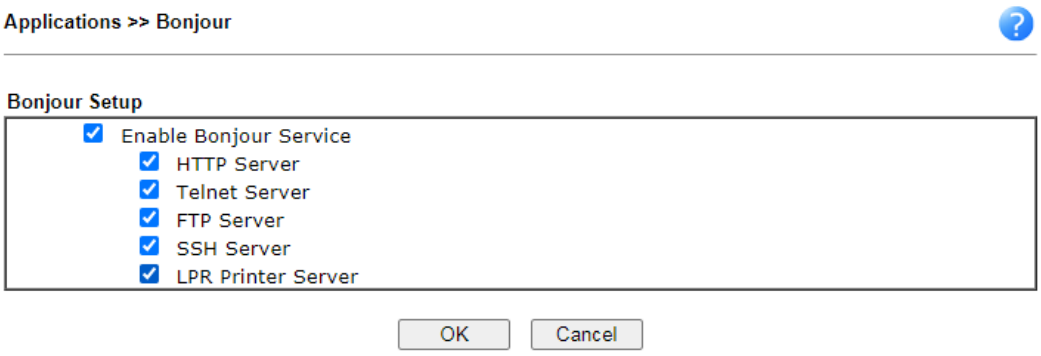
2. Abra el navegador web, Firefox. Si se han instalado Bonjour y DNSSD, puede abrir la página web (DNSSD) y ver los siguientes resultados.



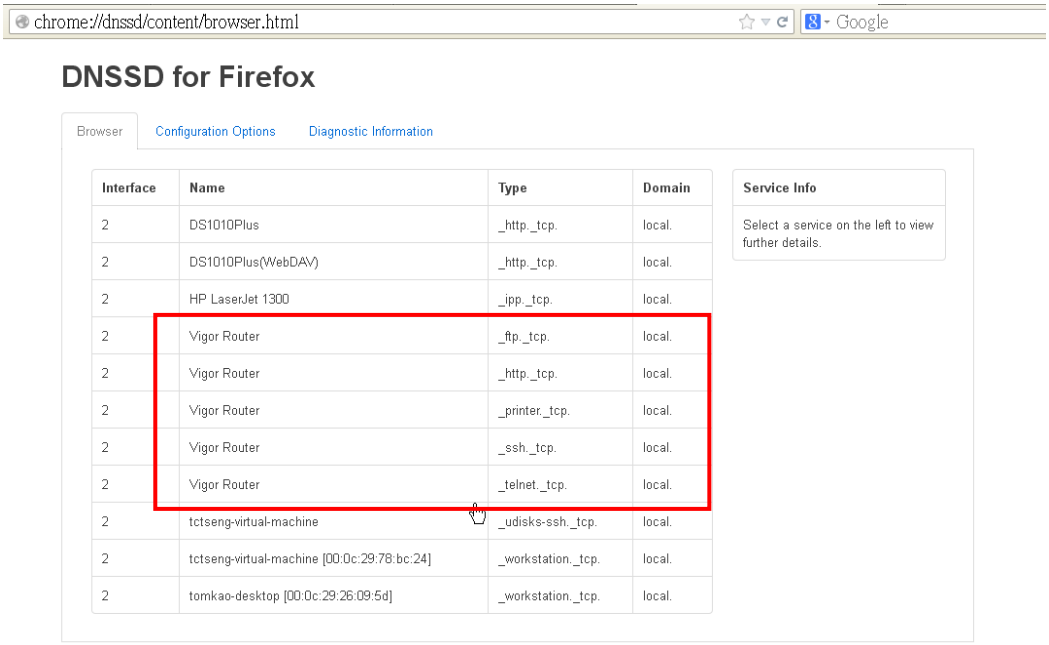
3. Abierto**Mantenimiento del Sistema>>Gestión**. Escriba un nombre como Nombre del enrutador y haga clic en **DE ACUERDO**.



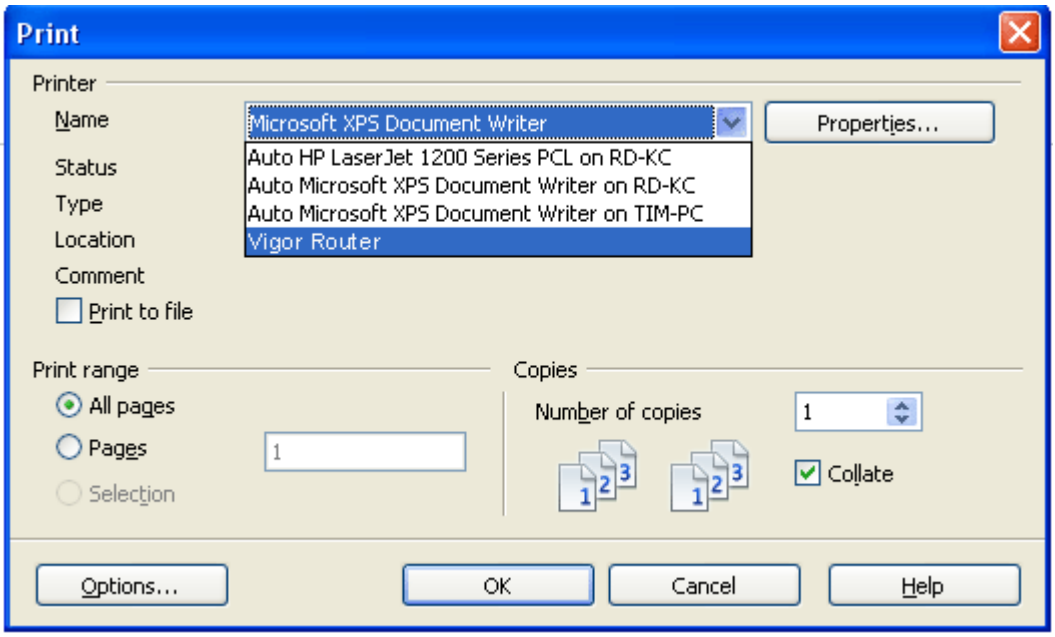
4. A continuación, abra**Aplicaciones>>Bonjour**. Marque el servicio que desea utilizar a través de Bonjour.



5. Abra la página DNSSD nuevamente. Los elementos disponibles se cambiarán de la siguiente manera. Significa que el enrutador Vigor (basado en el protocolo Bonjour) está listo para usarse como servidor de impresión, servidor FTP, servidor SSH, servidor Telnet y servidor HTTP.



6. Ahora, cualquier página o documento se puede imprimir a través del enrutador Vigor (instalado con una impresora).



II-5-12 Alta disponibilidad

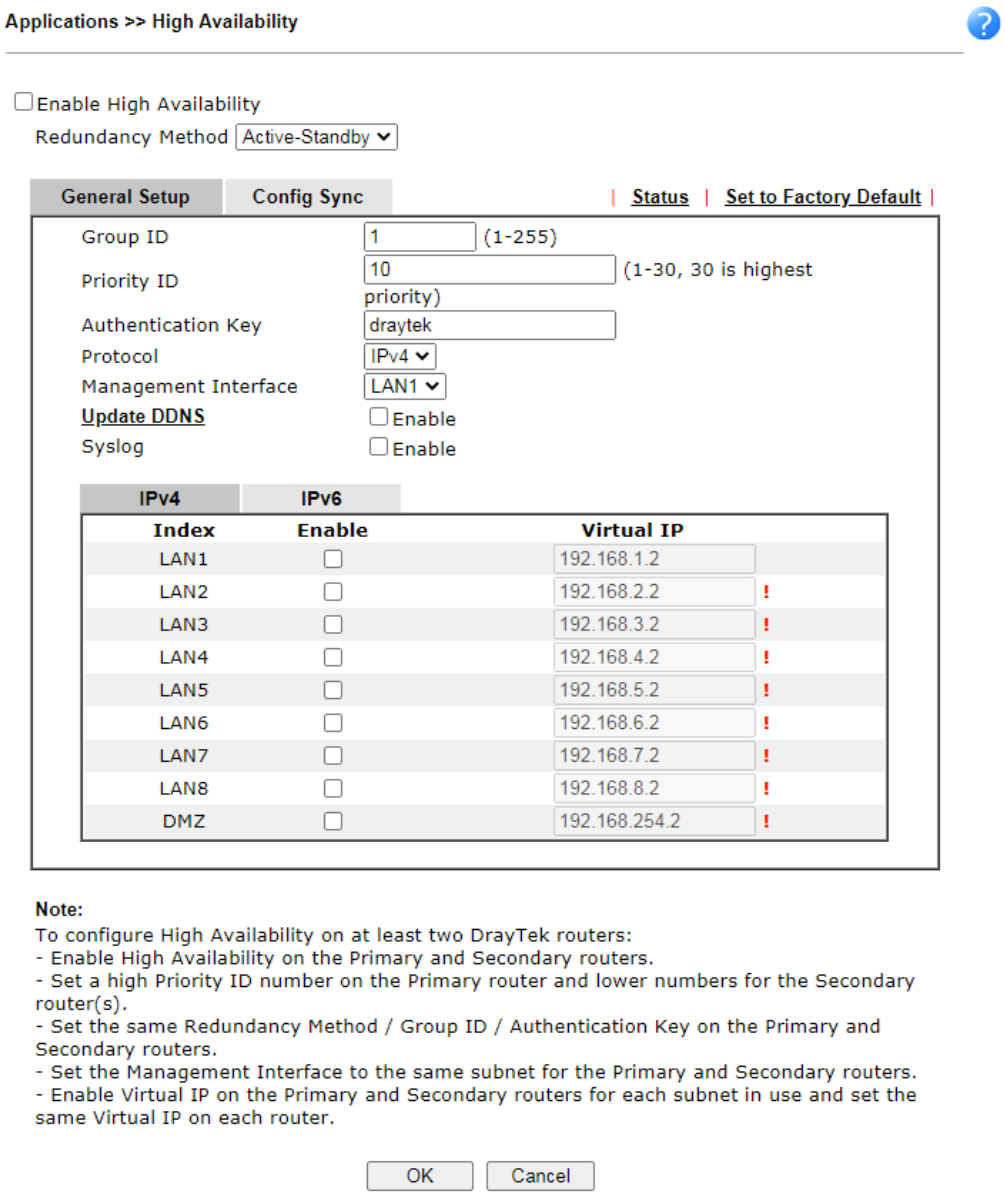
La función de alta disponibilidad (HA) del enrutador proporciona redundancia de recursos de red y reduce el tiempo de inactividad en caso de falla de un componente. El nivel de sofisticación de HA está determinado por los requisitos de disponibilidad y la tolerancia a las interrupciones del sistema. Los sistemas que brindan disponibilidad casi a tiempo completo suelen tener hardware y software redundantes.

El HA de la serie Vigor2927 está diseñado para evitar puntos únicos de falla. Cuando ocurren fallas, el proceso de conmutación por error transfiere la carga de la red manejada por el componente fallido (el enrutador principal) al componente de respaldo (el enrutador secundario), y se conserva la disponibilidad de los recursos de la red y se recuperan las transacciones parcialmente fallidas. En cuestión de segundos el sistema vuelve a su funcionamiento normal.

Para configurar la alta disponibilidad, se deben configurar al menos 2 enrutadores DrayTek de la siguiente manera:

- Habilite la alta disponibilidad en los enrutadores primario y secundario.
- Establezca una identificación de alta prioridad en el enrutador principal y una identificación de menor prioridad en el enrutador secundario.
- Configure métodos de redundancia, ID de grupo y claves de autenticación idénticos en ambos enrutadores.
- Configure la interfaz de administración de ambos enrutadores en la misma subred.
- Habilite la IP virtual en ambos enrutadores para cada subred en uso. Asegúrese de que las IP virtuales sean idénticas en ambos enrutadores.

Abierto**Aplicaciones>>Alta disponibilidad**para abrir la página de configuración para configurar la alta disponibilidad.



Los ajustes disponibles se explican a continuación:

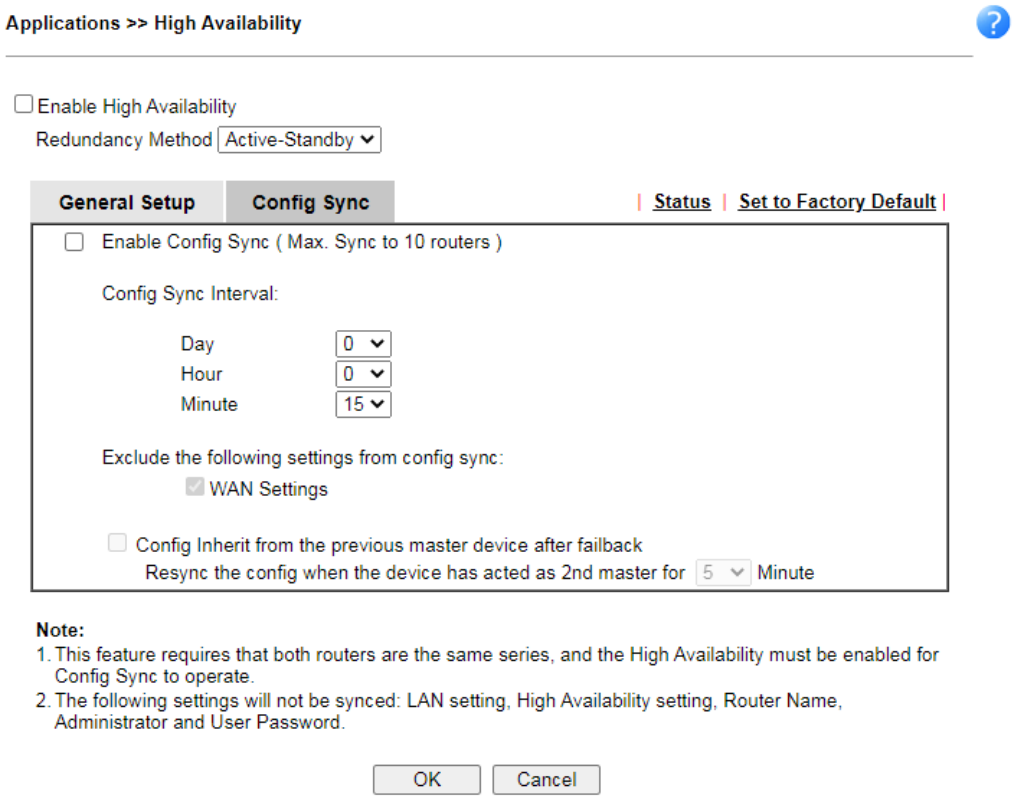
Artículo	Descripción
Habilitar alta disponibilidad	Marque esta casilla para habilitar la función HA.
Método de redundancia	Seleccione el método de redundancia para alta disponibilidad. **Hot-Standby -** Este método es adecuado cuando solo hay una cuenta de ISP. Cuando se selecciona este método, - Durante el funcionamiento normal, el enrutador secundario estará inactivo. Cuando el enrutador principal no funciona normalmente, los enrutadores secundarios tomarán el control. - La configuración de WAN de los enrutadores primario y secundario es idéntica.

	Nota: Cuando se utiliza Hot-Standby, la función LAN inalámbrica en el enrutador secundario se "deshabilitará" directamente. Los clientes ya no pueden conectarse al enrutador secundario. **Activo-Standby -** Este método es adecuado cuando hay múltiples conexiones ISP activas simultáneamente. Cuando se selecciona este método, - Todas las WAN en los enrutadores secundarios pueden estar activas al mismo tiempo. Las LAN que no están configuradas en alta disponibilidad se pueden enrutar a enrutadores secundarios. - Los ajustes de WAN de los enrutadores primario y secundario se configuran de forma independiente. - Se puede habilitar Config Sync para sincronizar la mayoría de los ajustes de configuración entre los enrutadores primario y secundario. - Todos los enrutadores deben configurarse con el mismo método de redundancia.
Identificación del grupo	Introduzca un valor (1~255). En un entorno LAN, varios enrutadores se pueden dividir en varios grupos. Cada enrutador debe especificarse con un ID de grupo. Los diferentes enrutadores con el mismo valor de ID se clasificarán en el mismo grupo. Solo uno de los enrutadores del mismo grupo se seleccionará como enrutador principal.
ID de prioridad	Introduzca un valor (1~30). Se deben configurar diferentes enrutadores con diferentes ID. A todos los enrutadores dentro de un grupo se les debe asignar una ID de prioridad. Dentro de un grupo, el enrutador con el ID de mayor prioridad (es decir, la prioridad más alta) será el enrutador principal. Cuando a varios enrutadores en un grupo se les asigna la misma ID de prioridad, los enrutadores con direcciones IP de LAN más bajas (configuradas en la LAN > > página Configuración general) tienen mayor prioridad.
Clave de autenticación	Introduzca una clave de autenticación de hasta 31 caracteres. Esto se utiliza para cifrar el tráfico DARP (DrayTek Address Redundancy Protocol) para protegerse contra ataques maliciosos.
Protocolo	Seleccione el protocolo IP que se usará para DARP.
Interfaz de gestión	Seleccione la interfaz que se utilizará para la negociación DARP entre enrutadores. Solo las interfaces que están habilitadas en **LAN>>Configuración general**están disponibles para la selección. Sin embargo, LAN1 siempre está habilitado.
Actualizar DNS	**Permitir -**Marque la casilla para actualizar el servidor DDNS para el dispositivo secundario cuando falla el enrutador principal. Si el dispositivo principal falla, el dispositivo secundario debe asumir el trabajo de transmisión y recepción de datos. Luego, el sistema actualizará el servidor DDNS para que el usuario se conecte al nombre de dominio especificado.
registro del sistema	**Permitir -**Marque la casilla para registrar la información requerida en Syslog.
LAN1 ~ LAN8, DMZ	**Permitir -**Marque la casilla para habilitar la interfaz. **IP virtuales -**Ingrese la dirección IP del enrutador que desempeña el papel de dispositivo principal.

Cuando termine la configuración, haga clic en**DE ACUERDO**para guardar y salir de esta página.

II-5-12-2 Sincronización de configuración

Esta página se utiliza para especificar el tiempo de sincronización para dicho enrutador Vigor.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar Config Sync (Max. Sync a 10 enrutadores)	Marque esta casilla para habilitar la sincronización de la configuración. Para sincronizar la configuración del enrutador principal al secundario, tanto el enrutador principal como el secundario deben habilitar la "sincronización de configuración". Tenga en cuenta que la sincronización de configuración se puede habilitar mediante**Hot-Standby** método de redundancia solamente.
Intervalo de sincronización de configuración	**Día / Hora / Minuto**-El enrutador principal sincronizará su configuración con los enrutadores secundarios en cada intervalo de tiempo especificado.
Excluir lo siguiente configuración de sincronización de configuración	Esta configuración está disponible cuando el método de redundancia se establece en**Espera activa**. Seleccione los ajustes de configuración que se excluirán de la sincronización.
Configuración Heredar del dispositivo maestro anterior después de la conmutación por recuperación	La configuración heredada se ejecutará solo cuando el dispositivo (enrutador) desempeñe el papel de dispositivo maestro. Una vez que otro dispositivo con una ID de prioridad superior a este dispositivo esté listo para hacerse cargo de la administración como dispositivo maestro, después de actuar como maestro principal durante un tiempo, este dispositivo sincronizará la configuración con todos los miembros del mismo grupo y volverá a la configuración. rol del dispositivo de respaldo (maestro secundario). **Heredar configuración**... por ( ) minuto: ingrese un valor.

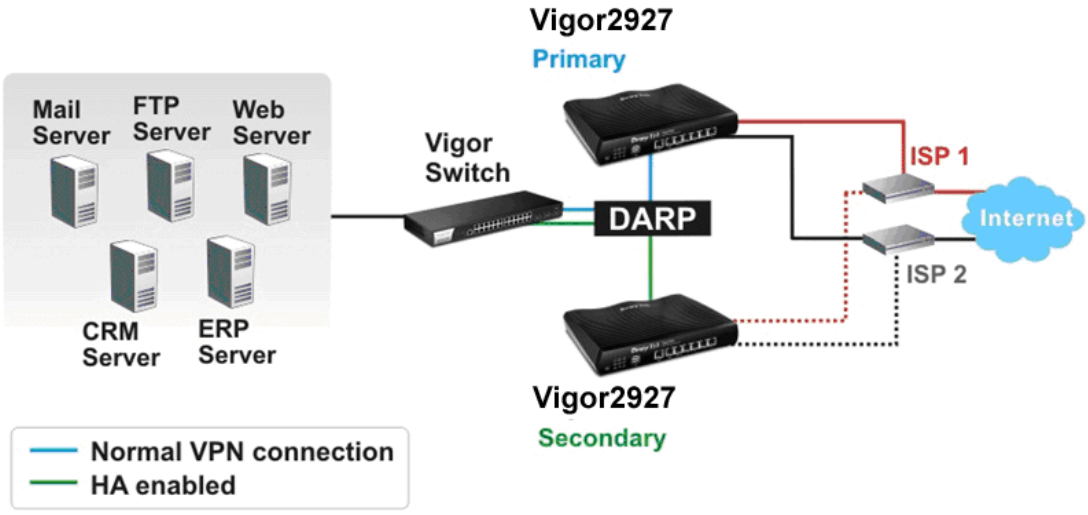
Cuando termine la configuración, haga clic en**DE ACUERDO**para guardar y salir de esta página.

Cuando el método de configuración se establece en “Hot Standby”, los siguientes ajustes no se sincronizarán:

- WAN (seleccionable por el usuario)
- LAN
- LANIPv6
- nombre del enrutador
- contraseñas de administrador y usuario

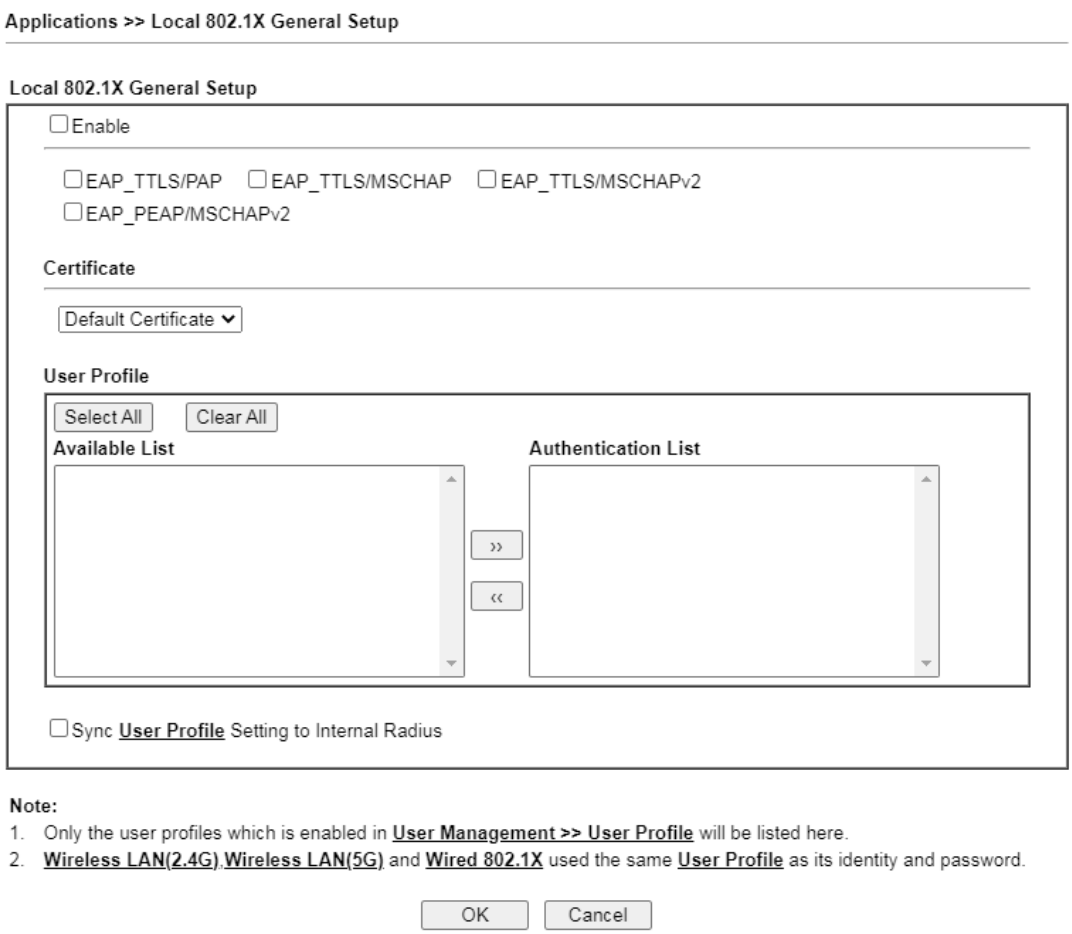
Ejemplo:

En el siguiente ejemplo, el primer Vigor2927 está configurado como dispositivo principal y el otro Vigor2927 es el dispositivo secundario. Cuando el Vigor2927 principal se avería, el dispositivo secundario asume el papel del dispositivo principal asumiendo todas las responsabilidades lo antes posible. Sin embargo, cuando el dispositivo principal se recupere, el dispositivo secundario volverá a ser el dispositivo de reserva.



II-5-13 Configuración general local 802.1X

Dicha página le permite configurar los ajustes generales para el servidor local 802.1X integrado en el enrutador Vigor. El servidor 802.X local se puede utilizar para autenticar clientes LAN inalámbricos y por cable.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Haga clic en él para habilitar el servidor 802.1X incorporado. En la actualidad, dicha función se puede utilizar para la autenticación 802.1x inalámbrica y por cable.
Certificado	Seleccione un certificado para los perfiles de usuario. Por lo general, el certificado autofirmado se utilizará como certificado predeterminado. Si hay muchos certificados locales/de confianza, seleccione uno de los certificados si es necesario.
Perfil del usuario	**Seleccionar todo**–Haga clic para agregar todos los perfiles de usuario al servidor 802.1X. Todos los perfiles aparecerán en la Lista de autenticación. **Limpiar todo**–Elimine todos los perfiles de usuario del servidor 802.1X. Todos los perfiles aparecerán en Lista disponible.
Sincronizar perfil de usuario....	Realice la configuración de habilitación/deshabilitación para RADIUS interno y sincronización local 802.1X para todos los perfiles de usuario (**Gestión de usuarios>>Perfil de usuario**). Por ejemplo, si Local 802.1x está configurado como Habilitado (marcado), el RADIUS interno se configurará como Habilitado

	también. Si Local 802.1X está configurado como Deshabilitado (sin marcar), el RADIUS interno también se cambiará como Deshabilitado, incluso si estaba habilitado previamente.
DE ACUERDO	Haga clic en él para guardar la configuración.
Cancelar	Haga clic en él para abandonar la configuración de todos los ajustes.

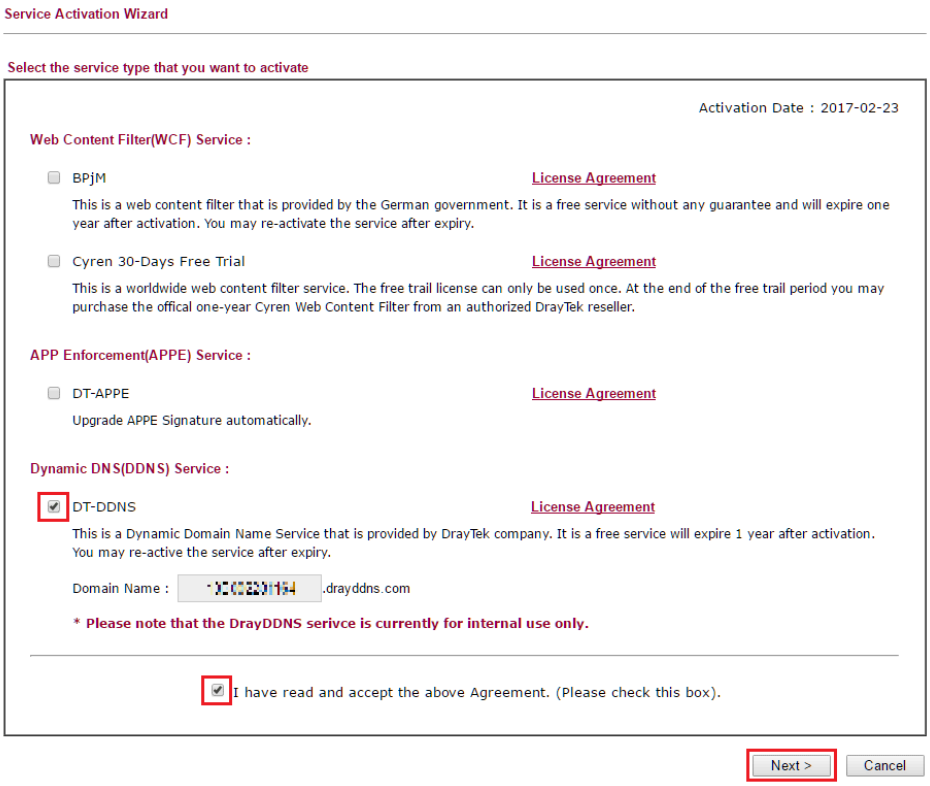
Cuando termine la configuración, haga clic en**DE ACUERDO**para guardar y salir de esta página.

A-1 ¿Cómo usar DrayDDNS?

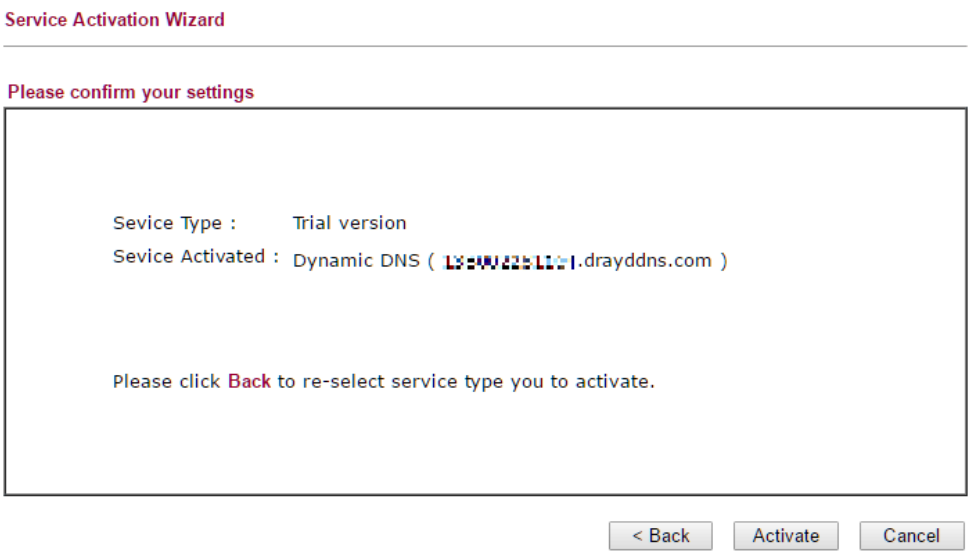
El enrutador Vigor es compatible con varios proveedores de servicios DDNS, el usuario puede configurar un perfil definido por el usuario para actualizar el DDNS incluso si el proveedor de servicios no está en la lista. Ahora, DrayTek comienza a admitir nuestro propio servicio DDNS: DrayDDNS. Proporcionaremos un nombre de dominio para cada enrutador Vigor, este único nombre de dominio puede registrar las direcciones IP de todas las WAN.

Activar licencia DrayDDNS

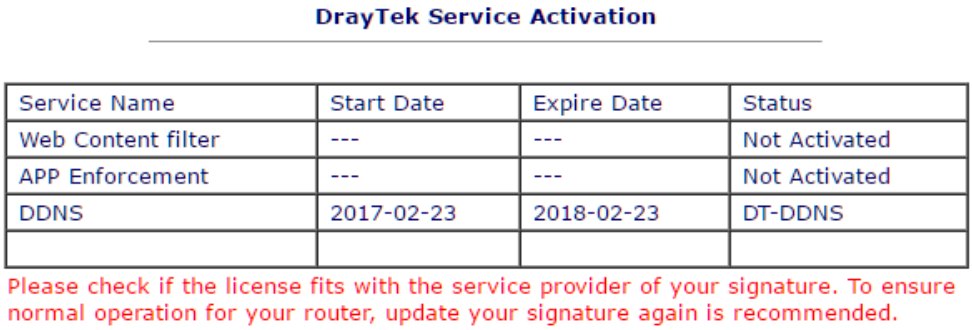
1. Ir a**Asistentes >> Asistente de activación de servicios**, espere a que el enrutador se conecte al servidor MyVigor, luego marque**DT-DDNS**y**He leído y acepto el Acuerdo anterior**, haga clic **Próximo**.



2. Confirme la información, luego haga clic en**Activar**.



3. El servidor MyVigor responderá con la información de activación del servicio.



Configurar perfil de DDNS

1. Ir a**Aplicaciones >> Configuración de DNS dinámico**,

a. Garrapata**Habilitar la configuración de DNS dinámico**

b. Haga clic en un índice de perfil disponible

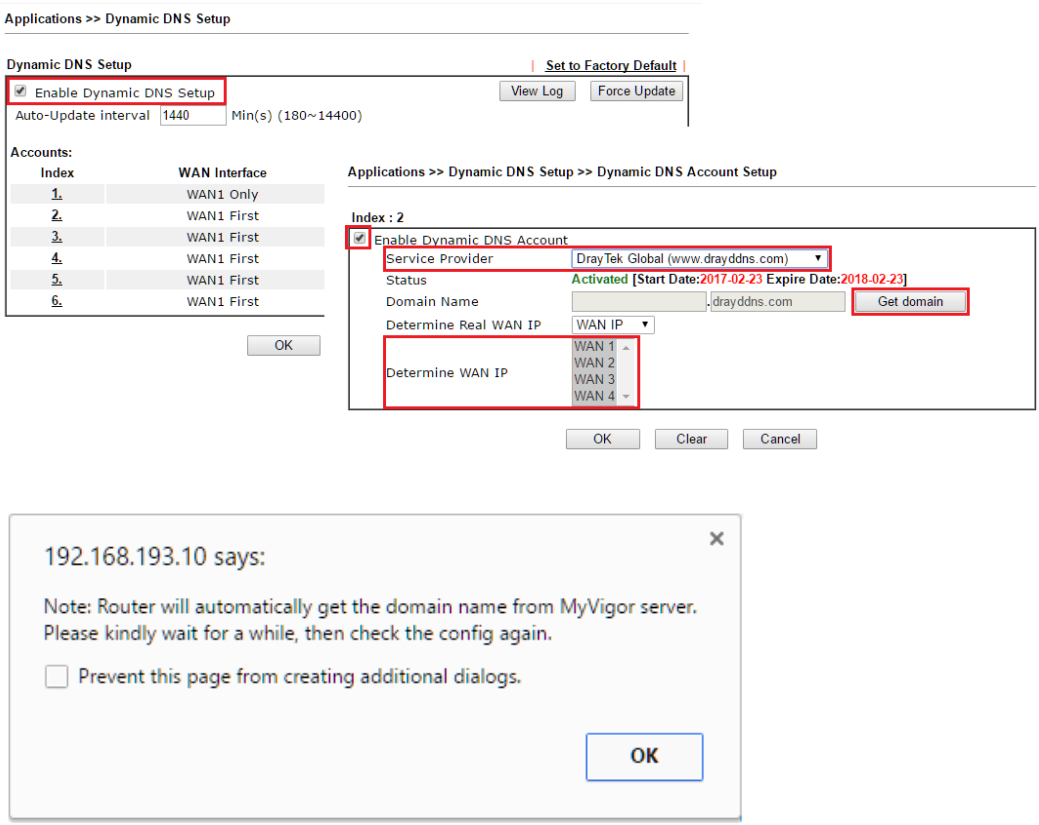
C. Garrapata**Habilitar cuenta de DNS dinámico**

d. Seleccionar**DrayDDNS Global (www.drayddns.com)**como**Proveedor de servicio**

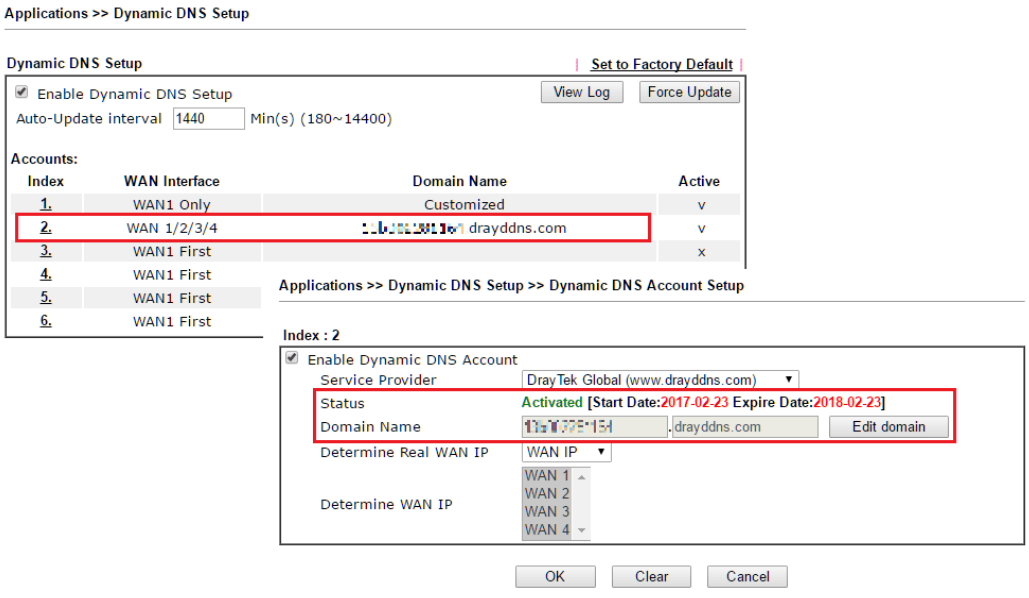
mi. Seleccione la WAN en la que le gustaría cargar la IP al servidor DDNS

F. Hacer clic**Obtener dominio**

gramo. Hacer clic**DE ACUERDO**en la ventana de notificación emergente



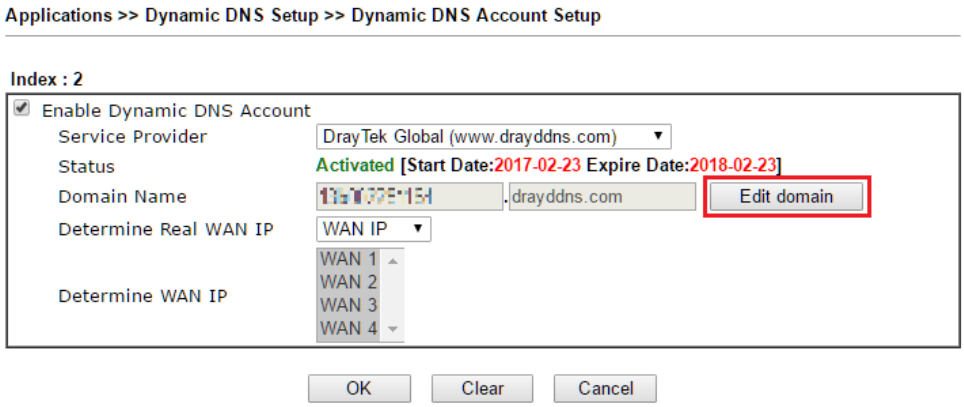
2. Espere unos segundos para que el enrutador obtenga el nombre de dominio, luego, podemos hacer clic en el perfil para verificar la información de la licencia y el nombre de dominio.



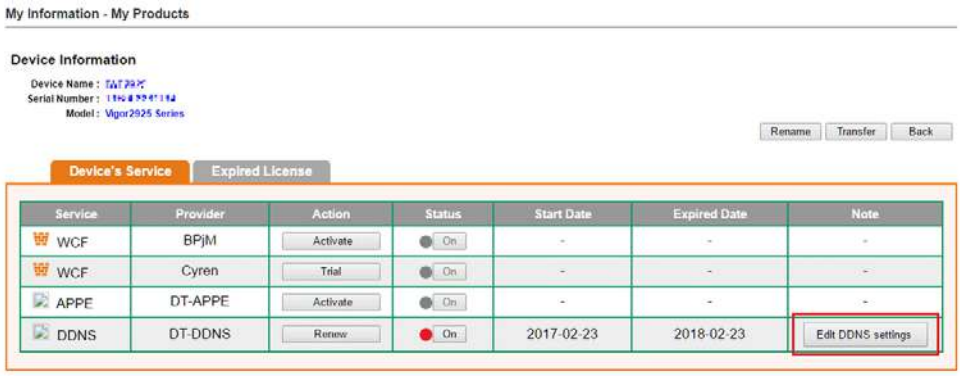
Modificar nombre de dominio

Actualmente, solo se permite modificar el nombre de dominio del sitio web MyVigor. Tendremos que registrar el enrutador en el servidor MyVigor e iniciar sesión en el sitio web de MyVigor para modificarlo.

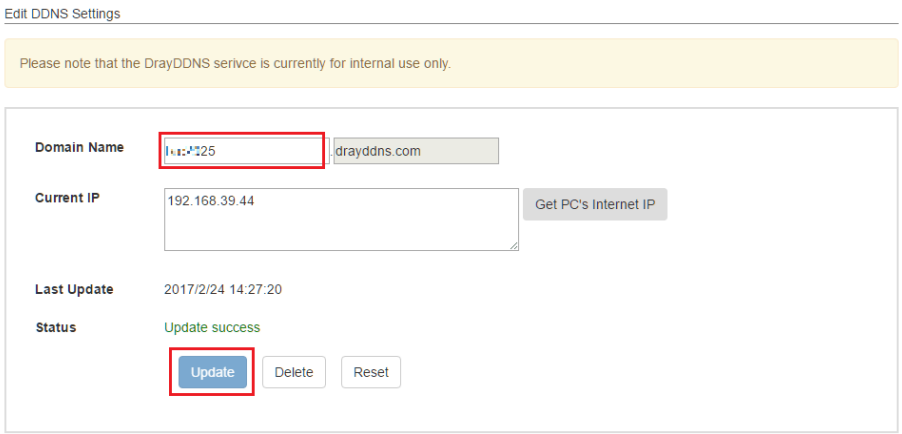
1. Visite https://myvigor.draytek.com/ o vaya a**Aplicaciones >> Configuración de DNS dinámico > > DrayDDNS**perfil y haga clic**Editar dominio**.



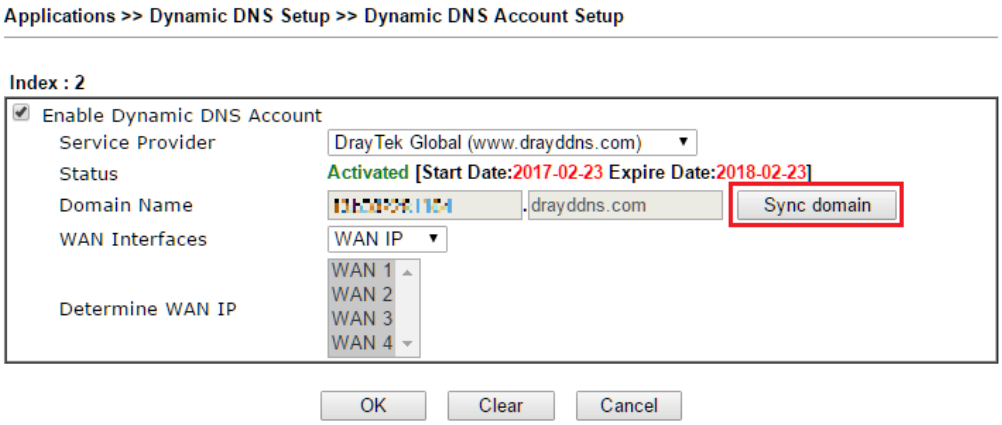
2. Inicie sesión en el sitio web de MyVigor, elija el perfil y haga clic en**Editar la configuración de DDNS**.



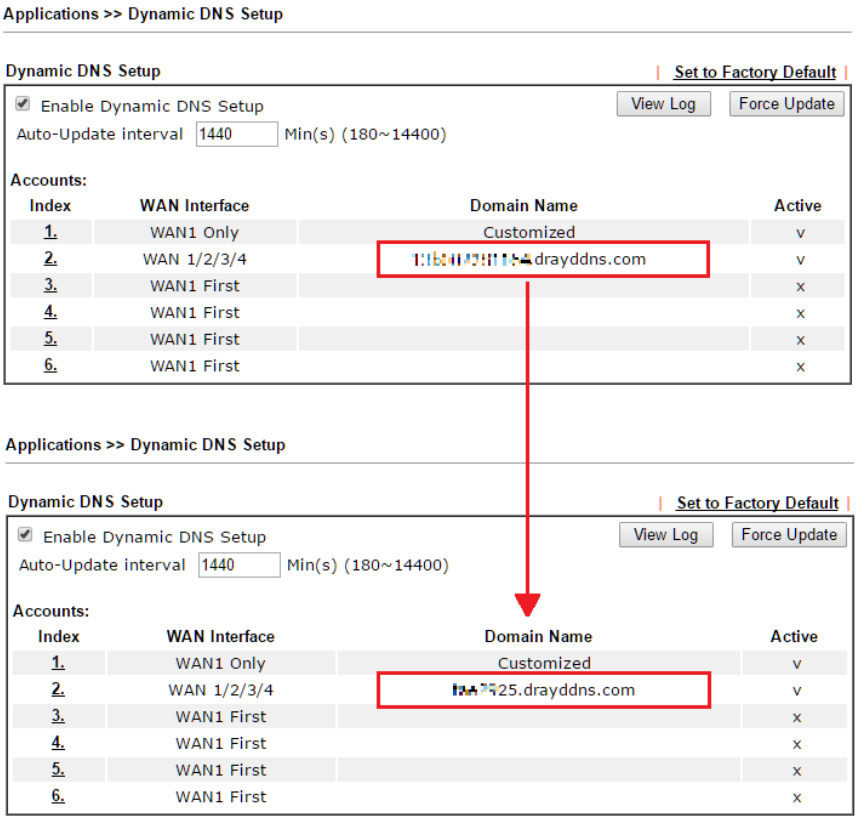
3. Ingrese el deseado**Nombre de dominio (p. ej., XXXX25)**y haga clic**Actualizar.**



4. El enrutador Vigor obtendrá el nombre de dominio modificado cuando realice la próxima actualización de DDNS. podemos hacer clic**Sincronizar dominio**para acelerar este proceso.



Después de unos segundos, el enrutador obtendrá el nuevo nombre de dominio y lo imprimirá en la lista de perfiles.



A-2 ¿Cómo configurar un DDNS personalizado?

Este artículo describe cómo configurar DDNS personalizado en enrutadores Vigor para actualizar su IP al servidor DDNS. Tomaremos "Changeip.org" y "3322.net" como ejemplo. Antes de configurar, asegúrese de que la conexión WAN esté activa.

Parte A: Changeip.org

Online Status

Physical Connection — **System Uptime: 0day 2:25:59**

IPv4	IPv6

LAN Status	Primary DNS: 168.95.192.1	Secondary DNS: 168.95.1.1
IP Address	TX Packets	RX Packets
10.1.7.1	2069	1036

WAN 1 Status >> Drop PPPoE

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	iwiz	PPPoE	2:25:53	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
1.169.185.242	168.95.98.254	14851	9506	11281	912

Tenga en cuenta que,

Nombre de usuario: jo***

Contraseña: jo********

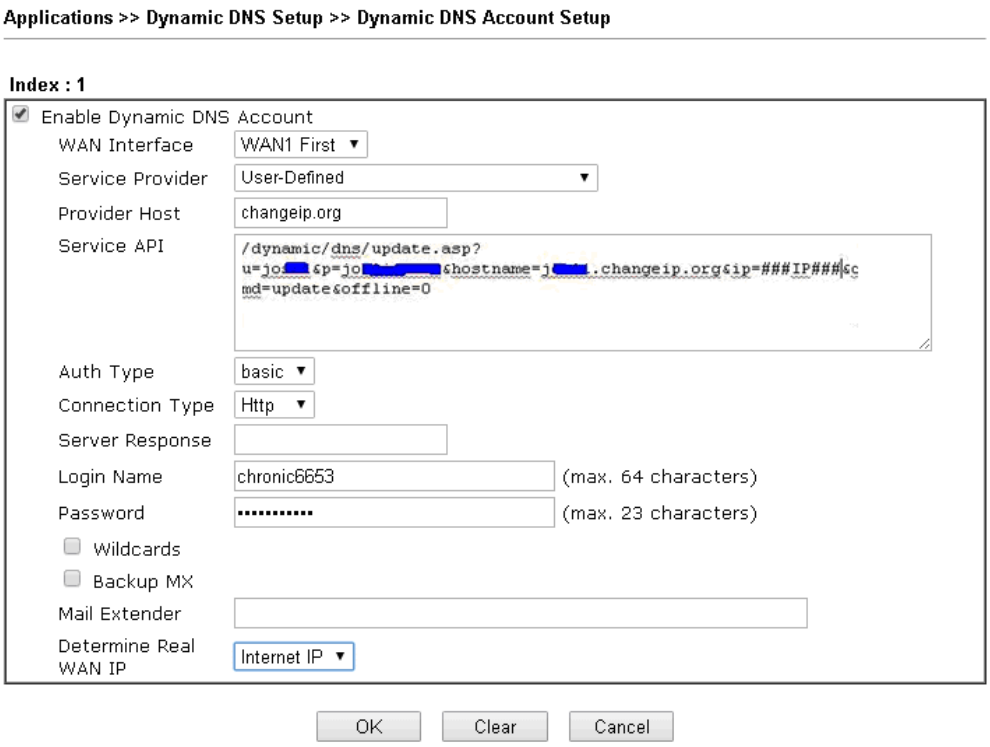
Nombre de host: j*****.changeip.org

Dirección IP de WAN: 1.169.185.242

A continuación se muestra la captura de pantalla de la edición del script HTML en el navegador para actualizar su IP al servidor DDNS.

Ahora tenemos que configurar el enrutador para que pueda hacer el mismo trabajo por nosotros automáticamente.

3. Vaya a**Aplicaciones >> DNS Dinámico**para crear un perfil para el cliente DDNS personalizado.



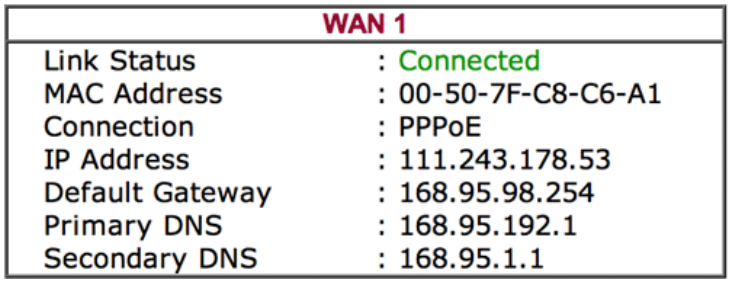
2. Configure el proveedor de servicios como**Usuario definido**.

3. Configure la API del servicio como: /dynamic/dns/update.asp?
u=jo***&p=jo********&hostname=j****.changeip.org&ip=###IP
# # # &cmd=actualizar&fuera de línea=0

En el cual, ###IP### es un valor que se reemplazará automáticamente con la dirección IP de la interfaz actual cuando se ejecute el servicio DDNS. En este caso la IP será 1.169.185.242.

4. Después de la configuración, el servicio DDNS personalizado estará activo y nuestra IP se actualizará al servidor DDNS.

Parte B : 3322.net



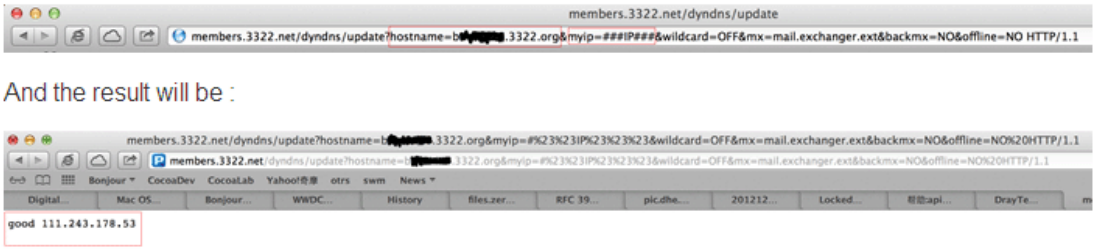
Nombre de usuario: bi*******

Contraseña: 88********

Nombre de host: bi*******.3322.org

Dirección IP WAN: 111.243.178.53

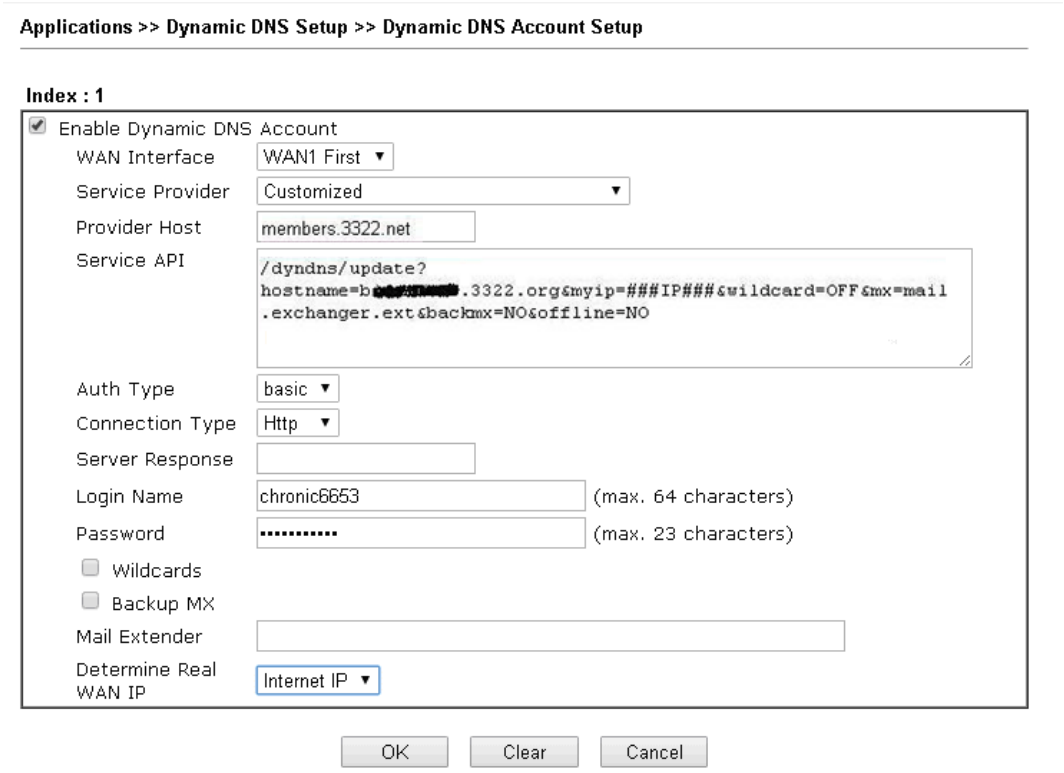
Para actualizar la IP al servidor DDNS mediante la edición del script HTML, podemos ingresar el siguiente script en el navegador:



"bueno 111.243.178.53" significa que nuestra IP se actualizó correctamente en el servidor.

Ahora tenemos que configurar el enrutador para que pueda hacer el mismo trabajo por nosotros automáticamente.

1. Vaya a**Aplicaciones >> DNS Dinámico**para crear un perfil para el cliente DDNS personalizado.



4. Establezca el proveedor de servicios como**Usuario definido**.

5. Establezca el host del proveedor como**miembro.3322.net**.

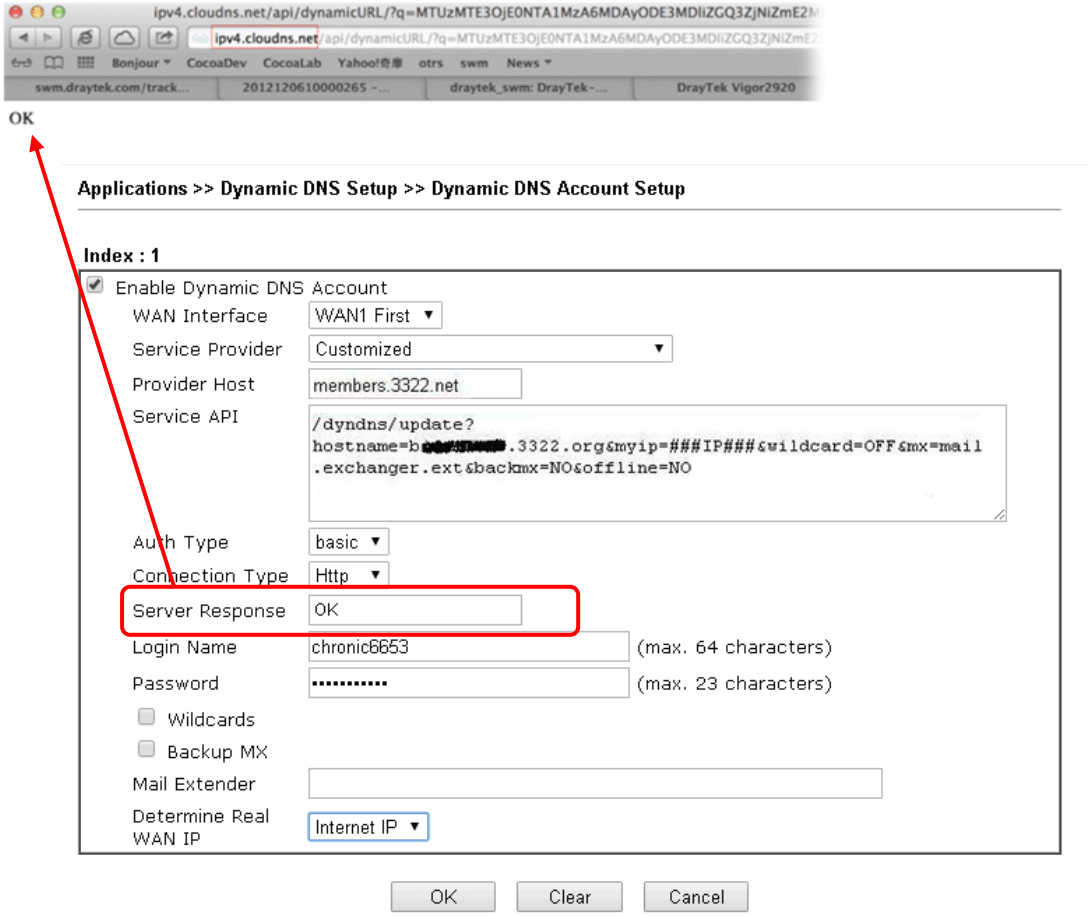
6. Configure la API del servicio como: /dyndns/update?
hostname=yourhost.3322.org&myip=###IP###&wildcard=OFF&mx=mail .
intercambiador.ext&backmx=NO&offline=NO

7. Ingrese su cuenta y contraseña.

8. Después de la configuración, el servicio DDNS personalizado estará activo y nuestra IP se actualizará al servidor DDNS automáticamente.

Parte C: Ampliar nota

El proveedor de servicios personalizado también es elegible con ClouDNS.net.



Política de ruta(también conocido como PBR, enrutamiento basado en políticas) es una función en la que es posible que necesite obtener una estrategia para el enrutamiento. Los paquetes se dirigirán a la interfaz especificada si coinciden con una de las políticas. Puede configurar políticas de ruta por varios motivos, como equilibrio de carga, seguridad, decisión de enrutamiento, etc.

A través del protocolo, la dirección IP, el número de puerto y la configuración de la interfaz, la Política de ruta se puede usar para configurar cualquier regla de enrutamiento para que se ajuste a la solicitud real. En general, la Política de ruta puede alcanzar fácilmente los siguientes propósitos:

Equilibrio de carga

Puede crear políticas manualmente para equilibrar el tráfico a través de la interfaz de red.

Especificar interfaz

A través de una interfaz dedicada (WAN/LAN/VPN), los datos se pueden enviar desde la IP de origen a la IP de destino.

Mapeo de direcciones

Le permite especificar las direcciones IP WAN salientes para una dirección IP privada interna o un rango de direcciones IP privadas internas.

Prioridad

El enrutador determinará qué política se adoptará para transmitir el paquete de acuerdo con la prioridad de la ruta estática y la política de ruta.

Conmutación por error a/Conmutación por recuperación

Los paquetes se enviarán a través de otra interfaz o seguirán otra política cuando la interfaz original se caiga (**Conmutación por error a**). Una vez que la interfaz original reanude el servicio (**Conmutación por recuperación**), los paquetes le serán devueltos inmediatamente.

Otras rutas

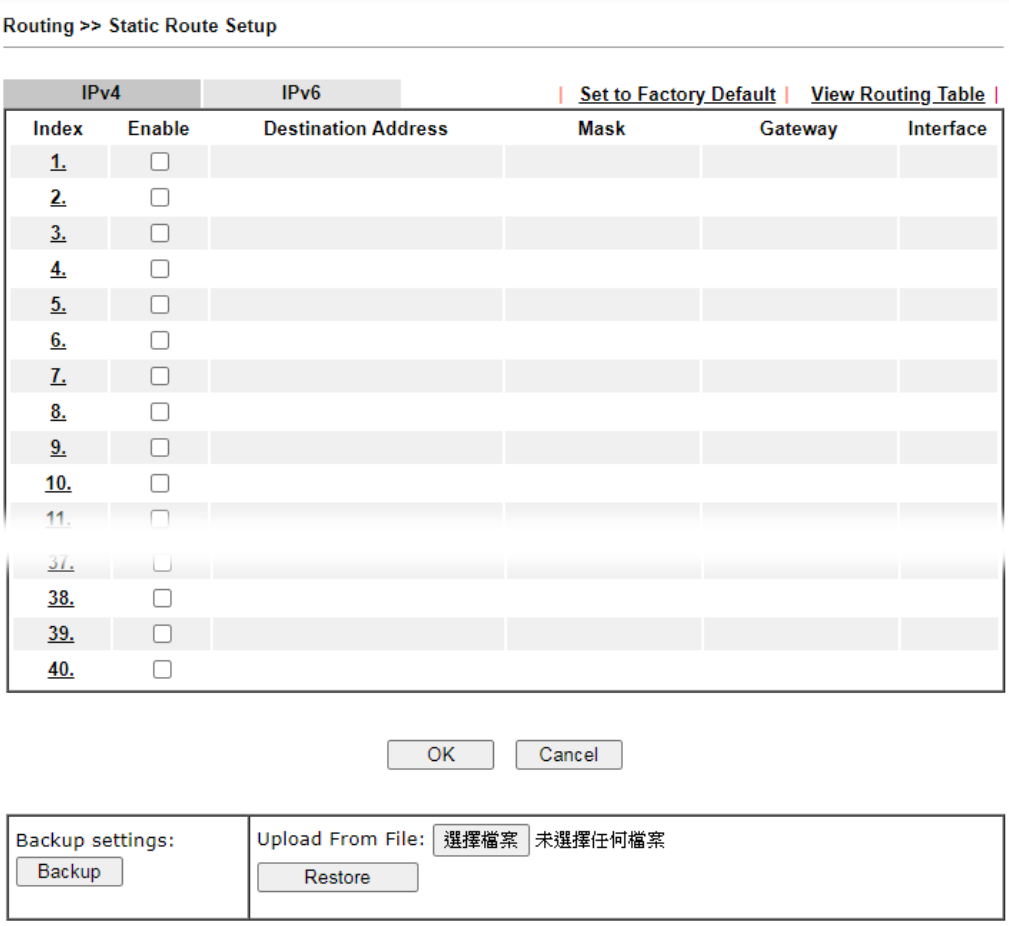
Especifique la política de enrutamiento para determinar la dirección de la transmisión de datos.

Información	Para obtener información más detallada sobre el uso de la ruta de política, consulte Soporte > > Preguntas frecuentes/nota de aplicación en www.draytek.com.

II-6-1 Ruta Estática

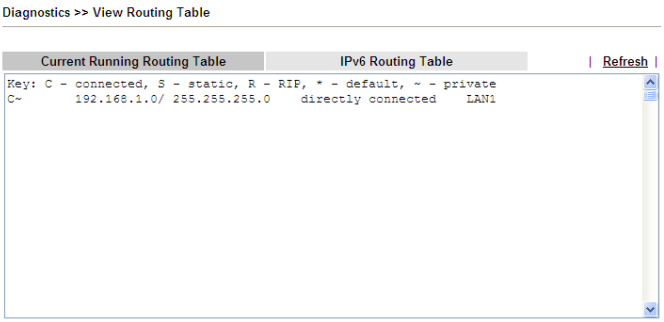
Ir a**Enrutamiento**>>**Ruta estática**. El enrutador ofrece IPv4 e IPv6 para que configure la ruta estática. Ambos protocolos traen páginas web diferentes.

Ruta estática para IPv4



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Índice	El número (1 a 40) debajo de Índice le permite abrir la página siguiente para configurar una ruta estática.
Permitir	Marque la casilla para habilitar el perfil de ruta estática.
Dirección de destino	Muestra la dirección de destino de la ruta estática.

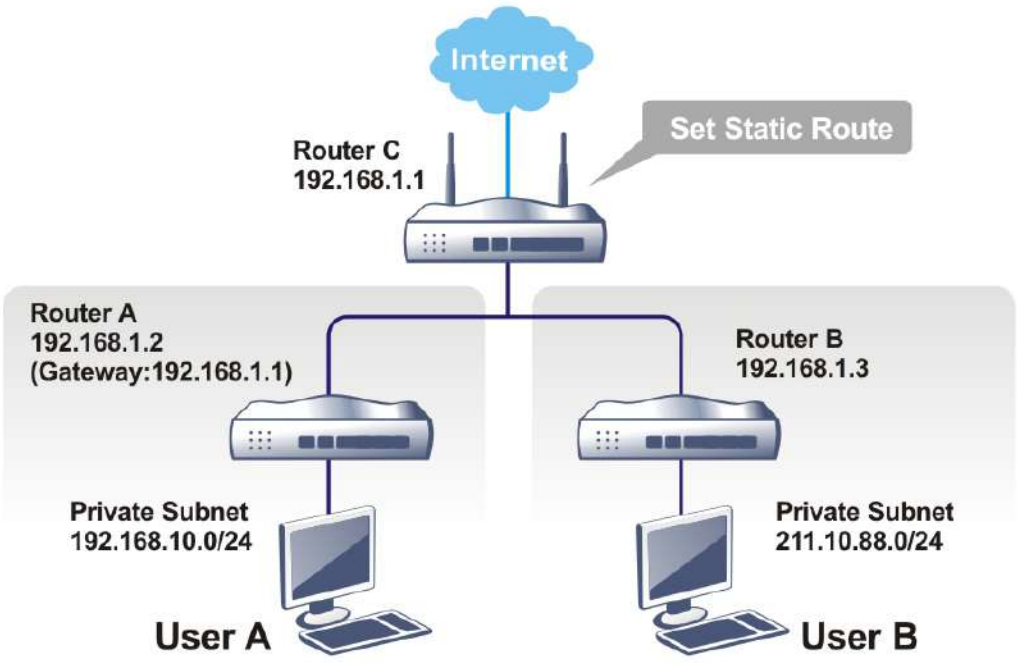
Establecer como predeterminado de fábrica	Borre todas las configuraciones y vuelva a la configuración predeterminada de fábrica.
Visualización de la tabla de enrutamiento	Muestra la tabla de enrutamiento para su referencia. 
Respaldo	Haga clic en él para hacer una copia de seguridad de la configuración de la ruta estática.
Restaurar	Haga clic en él para restaurar la configuración de la ruta estática. Antes de hacer clic, asegúrese de cargar el archivo de configuración en el enrutador Vigor.

Agregar rutas estáticas a redes públicas y privadas

Aquí hay un ejemplo (basado en IPv4) de configuración de ruta estática en el enrutador principal para que los usuarios A y B ubicados en diferentes subredes puedan comunicarse entre sí a través del enrutador. Suponiendo que se haya configurado el acceso a Internet y que el enrutador funcione correctamente:

- utilice el enrutador principal para navegar por Internet.
- cree una subred privada 192.168.10.0 usando un enrutador A interno (192.168.1.2) cree una
- subred pública 211.100.88.0 a través de un enrutador B interno (192.168.1.3).
- ha configurado el enrutador principal 192.168.1.1 como la puerta de enlace predeterminada para el enrutador A 192.168.1.2.

Antes de configurar la ruta estática, el usuario A no puede hablar con el usuario B porque el enrutador A solo puede reenviar paquetes reconocidos a su enrutador principal de puerta de enlace predeterminada.

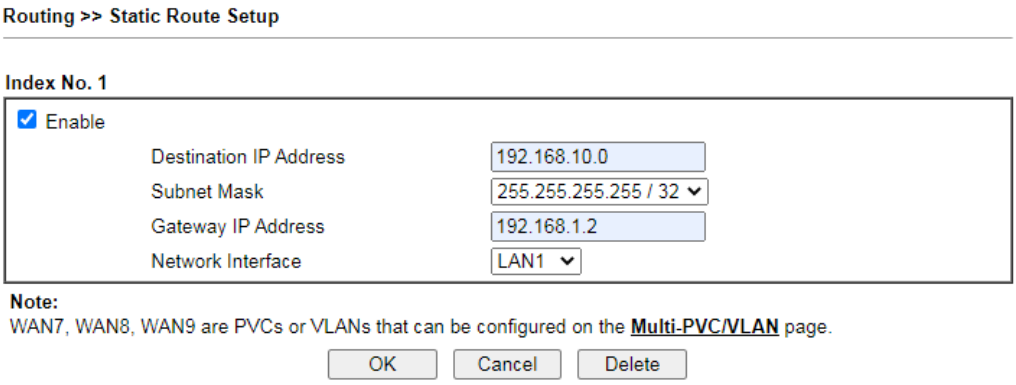


1. Ir a**LAN**página y haga clic**Configuración general**, seleccione 1.ª subred como**Control de protocolo RIP.** Luego haga clic en el**DE ACUERDO**botón.

Información

Hay dos razones por las que tenemos que aplicar el control del protocolo RIP en la primera subred. La primera es que la interfaz LAN puede intercambiar paquetes RIP con los enrutadores vecinos a través de la primera subred (192.168.1.0/24). La segunda es que esos hosts en las subredes privadas internas (por ejemplo, 192.168.10.0/24) pueden acceder a Internet a través del enrutador e intercambiar continuamente información de enrutamiento de IP con diferentes subredes.

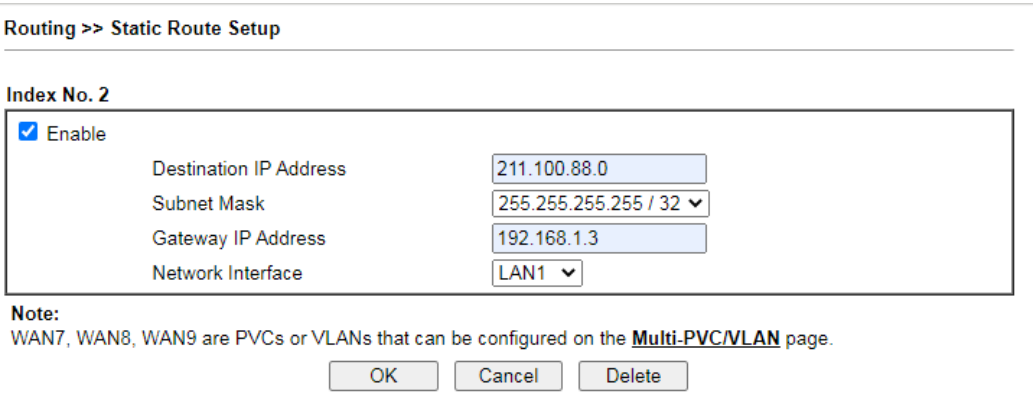
2. Haga clic en el**Enrutamiento >> Ruta estática**y haga clic en el**Número de índice 1.**Comprobar el**Permitir** caja. Agregue una ruta estática como se muestra a continuación, que regula que todos los paquetes destinados a 192.168.10.0 se reenviarán a 192.168.1.2. Hacer clic**DE ACUERDO**.



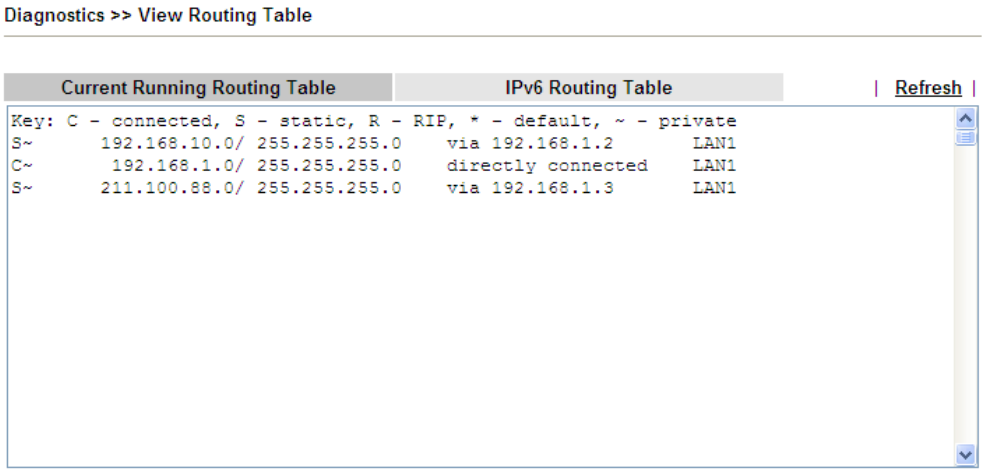
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Haga clic para habilitar este perfil.
IP de destino **DIRECCIÓN**	Introduzca una dirección IP como destino de dicha ruta estática.
Máscara de subred	Ingrese la máscara de subred para dicha ruta estática.
Dirección IP de la puerta de enlace	Introduzca la dirección IP de la puerta de enlace.
Interfaz de red	Utilice la lista desplegable para especificar una interfaz para dicha ruta estática.

3. Volver a**Configuración de ruta estática**página. Haga clic en otro**Número de índice**para agregar otra ruta estática como se muestra a continuación, que regula todos los paquetes destinados a 211.100.88.0 se reenviarán a 192.168.1.3. Hacer clic**DE ACUERDO**.

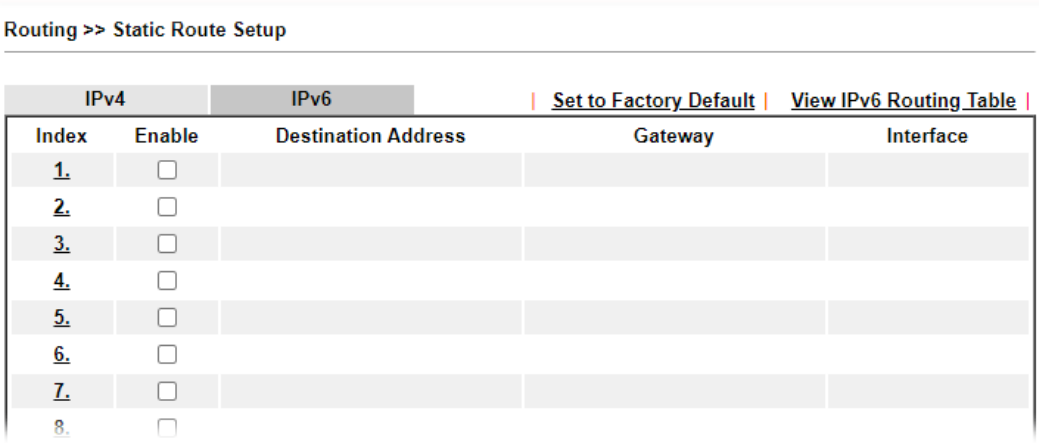


4. Ir a**Diagnóstico**y elige**Tabla de ruteo**para verificar la tabla de enrutamiento actual.



Ruta estática para IPv6

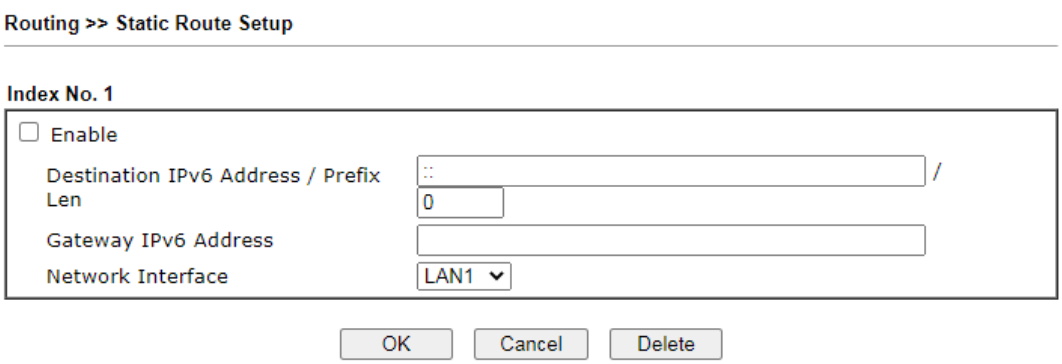
Puede configurar hasta 40 perfiles para la ruta estática IPv6. Haga clic en la pestaña IPv6 para abrir la siguiente página:



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Índice	El número (1 a 40) debajo de Índice le permite abrir la página siguiente para configurar una ruta estática.
Permitir	Marque la casilla para habilitar el perfil de ruta estática.
Dirección de destino	Muestra la dirección de destino de la ruta estática.
Puerta	Muestra la dirección IP de la puerta de enlace.
Interfaz	Muestra la interfaz utilizada para esta ruta estática.
Establecer como predeterminado de fábrica	Borre todas las configuraciones y vuelva a la configuración predeterminada de fábrica.
Visualización de enrutamiento IPv6 **Mesa**	Muestra la tabla de enrutamiento para su referencia.
Respaldo	Haga clic en él para hacer una copia de seguridad de la configuración de la ruta estática.
Restaurar	Haga clic en él para restaurar la configuración de la ruta estática. Antes de hacer clic, asegúrese de cargar el archivo de configuración en el enrutador Vigor.

Haga clic en cualquier subrayado del número de índice para obtener la siguiente página.



Los ajustes disponibles se explican a continuación:

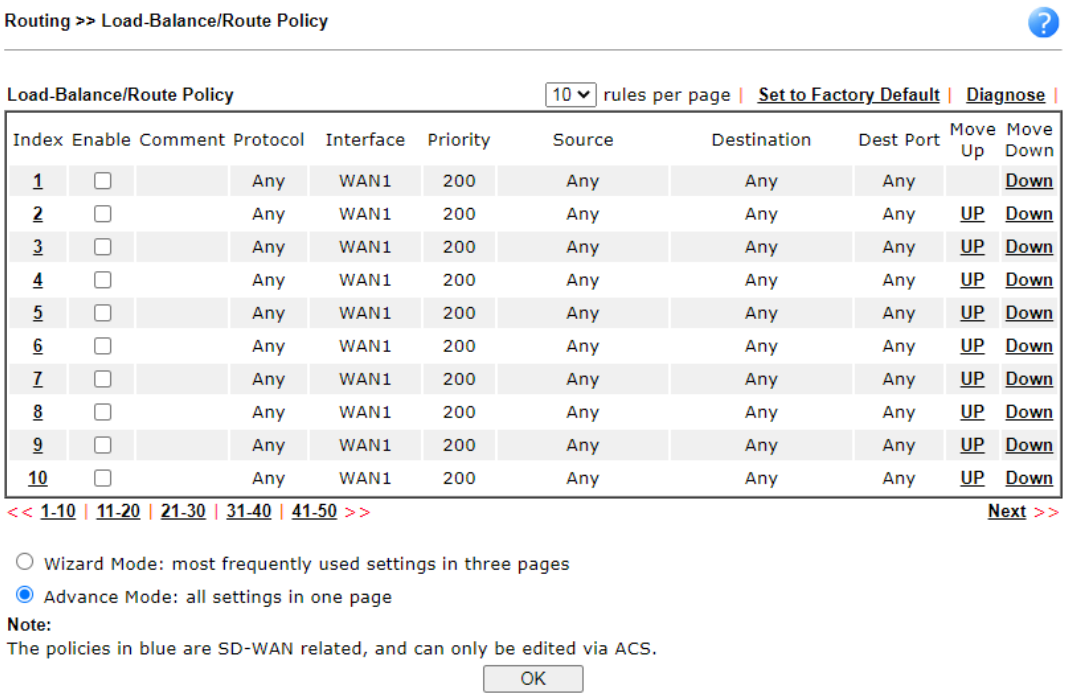
Artículo	Descripción
Permitir	Haga clic para habilitar este perfil.
Dirección IPv6 de destino / longitud del prefijo	Introduzca la dirección IP con la longitud del prefijo para esta entrada.
Dirección IPv6 de puerta de enlace	Introduzca la dirección de la puerta de enlace para esta entrada.
Interfaz de red	Utilice la lista desplegable para especificar una interfaz para esta ruta estática.

Cuando termine la configuración, haga clic en**DE ACUERDO**para guardar y salir de esta página.

II-6-2 Equilibrio de carga/Política de ruta

Permite al administrador de la red administrar el tráfico saliente de manera más específica. La política establecida en Load-Balance/Route Policy siempre tiene mayor prioridad que**Ruta por defecto**y**Equilibrio de carga automático** establecer en**WAN >> Acceso a Internet**, y siempre tiene menor prioridad que el**cortafuegos** Normas. El administrador también puede definir una prioridad para esta política.

Esta página enumera todas las políticas y muestra si la política está habilitada o deshabilitada, cuáles son los criterios que deben coincidir y a través de qué interfaz debe pasar el tráfico si se cumplen los criterios, y también su prioridad.



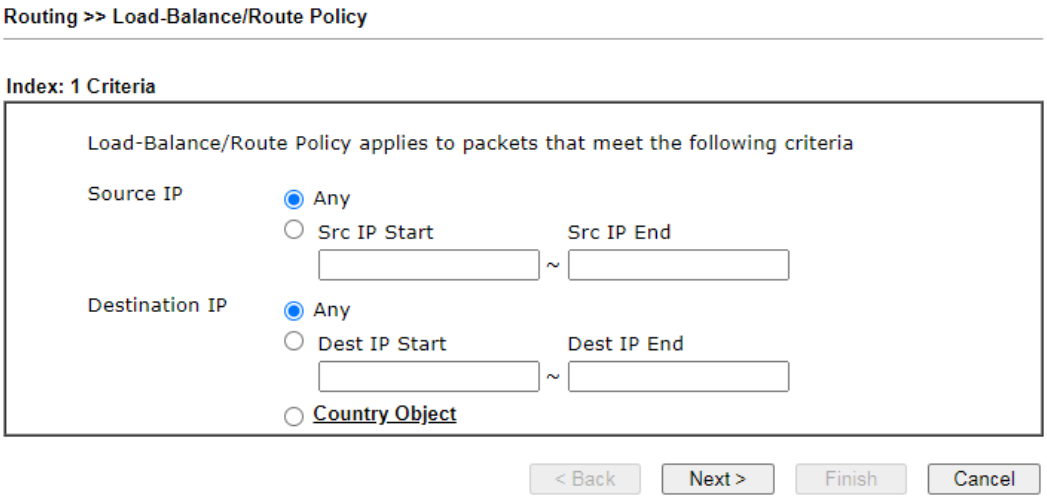
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Índice	Haga clic en el número de índice para acceder a la página web de configuración.
Permitir	Marque esta casilla para habilitar esta política.
Protocolo	Muestra el protocolo utilizado para esta política.
Interfaz	Muestre la interfaz a la que enviar paquetes una vez que coincida con la política.
Prioridad	Muestre el valor de prioridad para dicho perfil de política de ruta.
Fuente	Muestra el contenido de la fuente IP, subred, objeto o grupo.
Destino	Muestra el contenido de la IP, subred, objeto o grupo de destino.
Puerto de destino	Muestra el contenido del puerto de destino.
Mover ARRIBA/Mover Abajo	Usar**Arriba**o**Abajo**enlace para mover el orden de la política.
Modo mago	Permita configurar los ajustes de política de ruta (simples y básicos) de uso frecuente a través de tres páginas de configuración.
Modo avanzado	Permitir configurar ajustes detallados de la política de ruta.

Para usar el Modo Asistente, simplemente siga los siguientes pasos:

1. Haga clic en el**Modo mago**boton de radio.

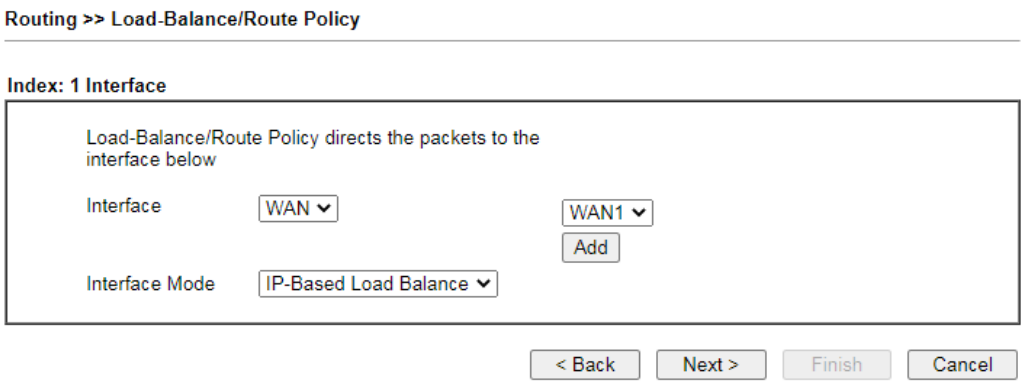
2. Haga clic en**Índice 1**. La página de configuración aparecerá de la siguiente manera:



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
IP de origen	**Cualquier**–Cualquier IP se puede tratar como la IP de origen. **Origen IP Inicio -**Ingrese el inicio de IP de origen para la interfaz WAN especificada. **Fin de IP de origen -**Ingrese el extremo IP de origen para la interfaz WAN especificada. Si este campo está en blanco, significa que todas las direcciones IP de origen dentro de la LAN pasarán a través de la interfaz WAN.
IP de destino	**Cualquier**–Cualquier IP puede ser tratada como la IP de destino. **Destino IP Inicio-**Ingrese el inicio de IP de destino para la interfaz WAN especificada. **Final de IP de destino:**Ingrese el extremo IP de destino para la interfaz WAN especificada. Si este campo está en blanco, significa que todas las direcciones IP de destino pasarán a través de la interfaz WAN. **Objeto País**–Especifique un objeto de país. Todas las direcciones IP provenientes del país (países) especificado en el objeto se pasarán a través de la interfaz WAN.

3. Haga clic en**Próximo**para obtener la siguiente página.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Interfaz	Puede seleccionar una interfaz de una de las siguientes: WAN, LAN, VPN, subred enrutada IP y subred DMZ. Los paquetes que coincidan con los criterios anteriores se transferirán a la interfaz elegida aquí. Seleccione una interfaz de la lista.
Modo de interfaz	Seleccione Equilibrio de carga basado en IP o Equilibrio de carga basado en sesión si se especifica WAN como interfaz.

4. Especifique una interfaz y haga clic en**Próximo.**La siguiente página aparecerá solo si elige WAN1 ~ WAN9 como interfaz.

Los ajustes disponibles se explican a continuación:

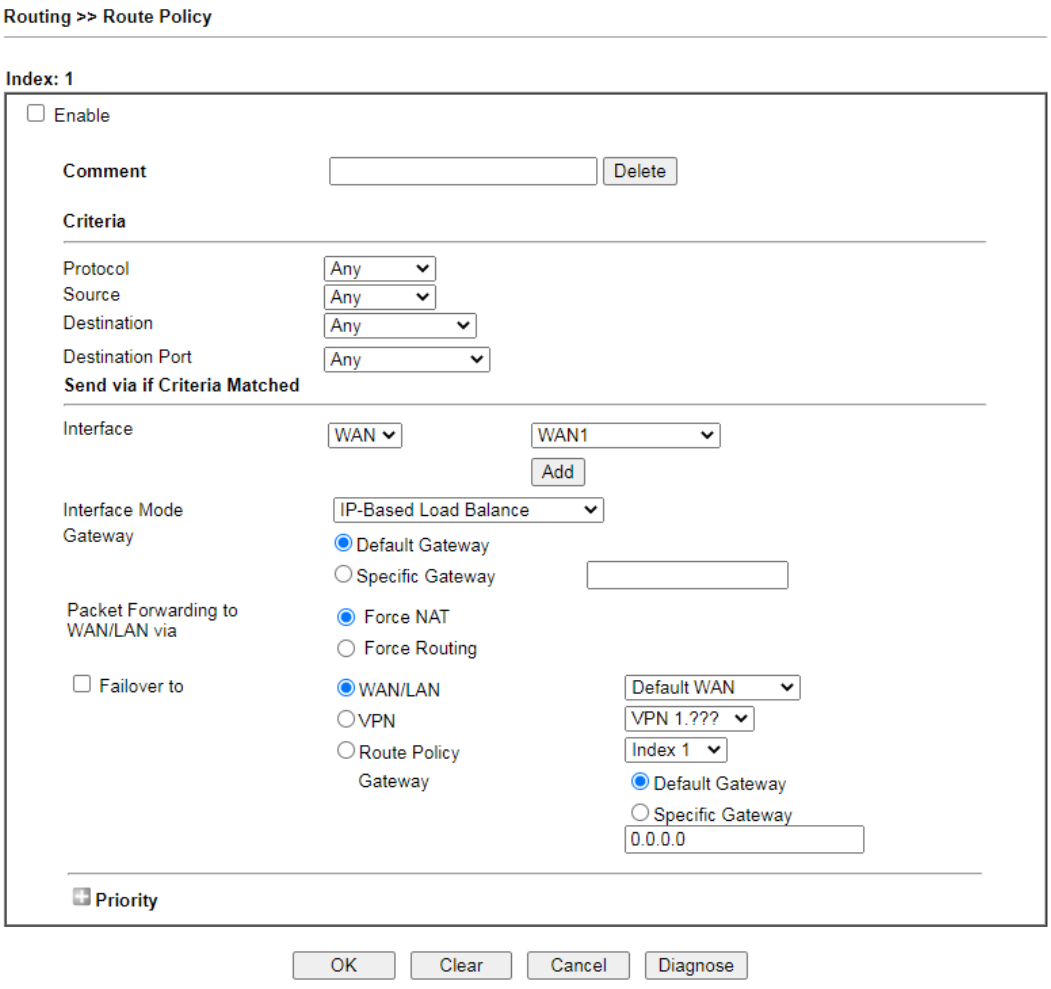
Artículo	Descripción
Fuerza NAT / Fuerza Enrutamiento	Determina qué mecanismo utilizará el enrutador para reenviar el paquete a la WAN.

5. Después de elegir el mecanismo, haga clic en**Próximo**para obtener la página de resumen como referencia.

6. Si no hay ningún error, haga clic en**Finalizar**para completar la configuración del asistente.

Usar**Avance**modo, siga los siguientes pasos:

1. Haga clic en el**Modo avanzado**boton de radio.
2. Haga clic en**Índice 1**para acceder a la página siguiente.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Marque esta casilla para habilitar esta política.
Comentario	Escriba una breve explicación para dicho perfil.
Criterios	El enrutador examina el tráfico LAN saliente para encontrar la primera regla cuyos criterios se cumplen. **Protocolo -**Utilice el menú desplegable para elegir un protocolo adecuado para la interfaz WAN. **Fuente -**Direcciones IP de origen a las que se aplicará esta regla. - **Cualquier**–Esta regla se aplica a todas las direcciones IP de origen. - **Rango de IP**–Esta regla se aplica al rango especificado de direcciones IP de origen. - **Comenzar**-Ingrese una dirección como la IP inicial para

	tal perfil. - **Fin**-Ingrese una dirección como IP final para dicho perfil. - **Subred IP**-Esta regla se aplica a las direcciones IP de origen definidas por la dirección IP de red y la máscara de subred especificadas. - **Red**–Introduzca una dirección IP aquí. - **Mascarilla**–Utilice la lista desplegable para elegir una máscara adecuada para la red. - **Objeto IP / Grupo IP**–Utilice la lista desplegable para elegir un objeto/grupo IP preconfigurado. **Destino -**Direcciones IP de destino a las que se aplicará esta regla. - **Cualquier**–Esta regla se aplica a todas las direcciones IP de origen. - **Rango de IP**–Esta regla se aplica al rango especificado de direcciones IP de destino. - **Comenzar -**Introduzca una dirección como IP inicial para dicho perfil. - **Fin -**Ingrese una dirección como IP final para dicho perfil. - **Subred IP**-Esta regla se aplica a las direcciones IP de destino definidas por la dirección IP de red y la máscara de subred especificadas. - **Red**–Introduzca una dirección IP aquí. - **Mascarilla**–Utilice la lista desplegable para elegir una máscara adecuada para la red. - **Nombre de dominio**–Especifique un nombre de dominio como destino. - **Seleccionar**–Haga clic en él para elegir un nombre de dominio existente definido en Configuración de objetos>>Objeto de cadena. - **Borrar**–Eliminar el nombre de dominio usado actual. - **Agregar**–Cree un nuevo nombre de dominio como destino. - **Objeto IP / Grupo IP**–Utilice la lista desplegable para elegir un objeto/grupo IP preconfigurado. - **Objeto País**–Utilice la lista desplegable para elegir un objeto preconfigurado. Luego, todas las IP dentro de ese país serán tratadas como la IP de destino. **Puerto de destino**-Números de puerto de destino a los que se aplicará esta regla. Como solo los protocolos TCP y UDP usan números de puerto, esta configuración no se aplica al protocolo ICMP. - **Cualquier**-Esta regla se aplica a todos los puertos de destino. - **Intervalo de puertos de destino**-Esta regla se aplica al rango especificado de puertos de destino. - **Comenzar -**Ingrese el inicio del puerto de destino para la IP de destino. - **Fin -**Ingrese el extremo del puerto de destino para la IP de destino. Si este campo está en blanco, significa que todos los puertos de destino pasarán a través de la interfaz WAN.
Enviar a si los criterios coinciden	Si los criterios coinciden, el tráfico se enviará a la interfaz y puerta de enlace designadas. **Interfaz**–Los paquetes que coincidan con los criterios anteriores serán

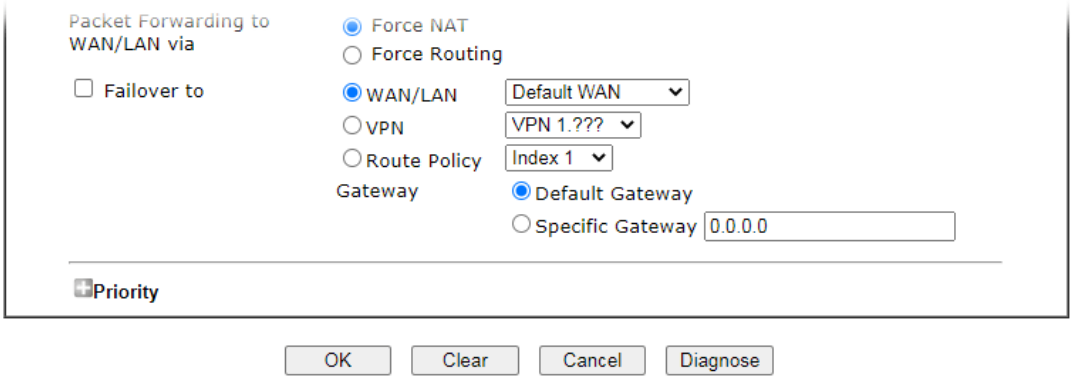
	transferido a la interfaz elegida aquí. Seleccione una interfaz de la lista (WAN/LAN: una interfaz WAN o LAN; VPN: una red privada virtual; PVC). **Modo de interfaz**-Está disponible si se selecciona WAN como interfaz. - **Equilibrio de carga basado en IP**-El mismo par de IP de origen/ destino seleccionará la misma interfaz WAN como política. Es la configuración predeterminada. - **Equilibrio de carga basado en sesiones**-Todas las interfaces WAN se utilizarán (como WAN saliente) para pasar a través de nuevas sesiones para obtener una mejor velocidad de transmisión. Aunque se puede alcanzar un buen resultado de prueba de velocidad para el rendimiento; sin embargo, es posible que algunos sitios web no se abran sin problemas, especialmente el sitio necesita autenticación, por ejemplo, FTP. Si no tiene una gran demanda sobre el resultado de la prueba de velocidad, mantenga la configuración predeterminada basada en IP. **Puerta**–Seleccione una puerta de enlace. - **Puerta de enlace predeterminada**-El tráfico se enviará a la dirección de puerta de enlace predeterminada de la interfaz especificada. - **Puerta de enlace específica**-El tráfico se enviará a la dirección de la puerta de enlace especificada en lugar de a la dirección de la puerta de enlace predeterminada. **Reenvío de paquetes a WAN/LAN a través de**–Cuando elige LAN/WAN (p. ej., WAN1) como interfaz para la transmisión de paquetes, debe especificar la forma en que se reenvía el paquete. - **Forzar NAT**-La dirección IP de origen no se utilizará para conectarse al destino remoto. Se utilizará la traducción de direcciones de red (NAT), donde se utilizará una dirección IP común. - **Forzar enrutamiento**-La dirección IP de origen se conservará cuando se conecte al destino remoto. **Conmutación por error a**–Si la interfaz especificada anteriormente pierde la conexión, el tráfico se puede reenviar a una interfaz alternativa o ser analizado por una política de ruta alternativa. - **WAN/LAN-**Utilice la lista desplegable para elegir una interfaz como interfaz de conmutación por error automática. - **vpn-**Utilice la lista desplegable para elegir un túnel VPN como túnel de conmutación por error. - **Política de ruta –**Utilice la lista desplegable para elegir un perfil de política de ruta existente. - **Puerta**–El tráfico conmutado por error se puede enviar a la puerta de enlace predeterminada de la política de ruta/interfaz alternativa o a una puerta de enlace específica en la dirección IP especificada. **Conmutación por recuperación**- Cuando**Conmutación por error a**está habilitada, el administrador también podría habilitar**Conmutación por recuperación**para borrar la sesión existente en la interfaz de conmutación por error y volver a la interfaz original inmediatamente una vez que la interfaz original reanude su servicio. Cuando la conmutación por recuperación no está habilitada, el enrutador solo dejará de enviar paquetes a través de la interfaz de conmutación por error cuando se borren las sesiones existentes, y esto puede llevar mucho tiempo porque algunas aplicaciones mantendrán

	enviando paquetes de vez en cuando. Por lo tanto, se recomienda la opción de conmutación por recuperación si el administrador desea que el tráfico pase a través de la interfaz principal lo antes posible.
Prioridad	Especifica la prioridad de la regla en relación con otras reglas. Reducir el valor de prioridad aumenta la prioridad de la regla y viceversa. Las rutas en la tabla de enrutamiento tienen un valor de prioridad de 150, mientras que las rutas predeterminadas tienen un valor de prioridad de 250. El valor de prioridad predeterminado de las reglas de política de enrutamiento/ equilibrio de carga es 200. Para cambiar la prioridad, mueva el control deslizante o ingrese un valor.

3. Cuando termine la configuración, haga clic en**DE ACUERDO**para guardar y salir de esta página.

Diagnosticar para política de ruta

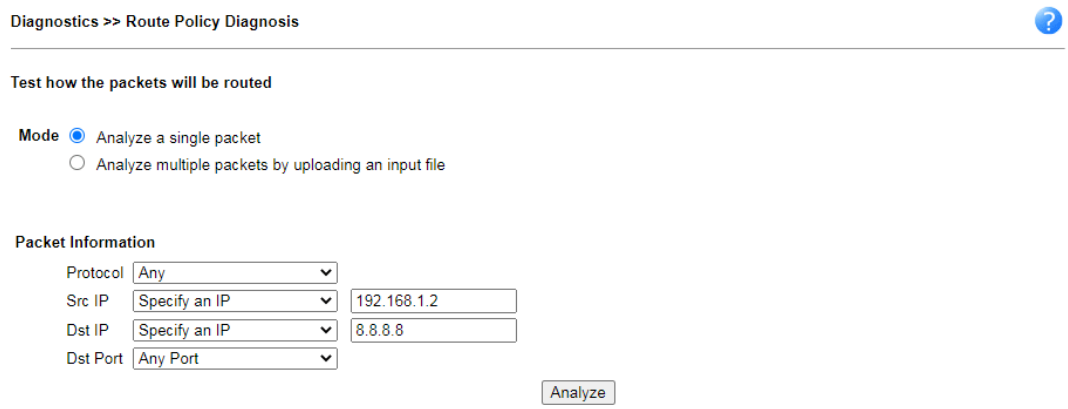
el boton de**Diagnosticar**ubicado debajo del perfil Load-Balance/Route Policy se usa para rastrear la posible ruta de los paquetes enviados fuera del enrutador.



Hacer clic**Diagnosticar**.

Analizar un solo paquete

Seleccione este modo para hacer que el enrutador Vigor analice cómo una política de ruta enviará un solo paquete.

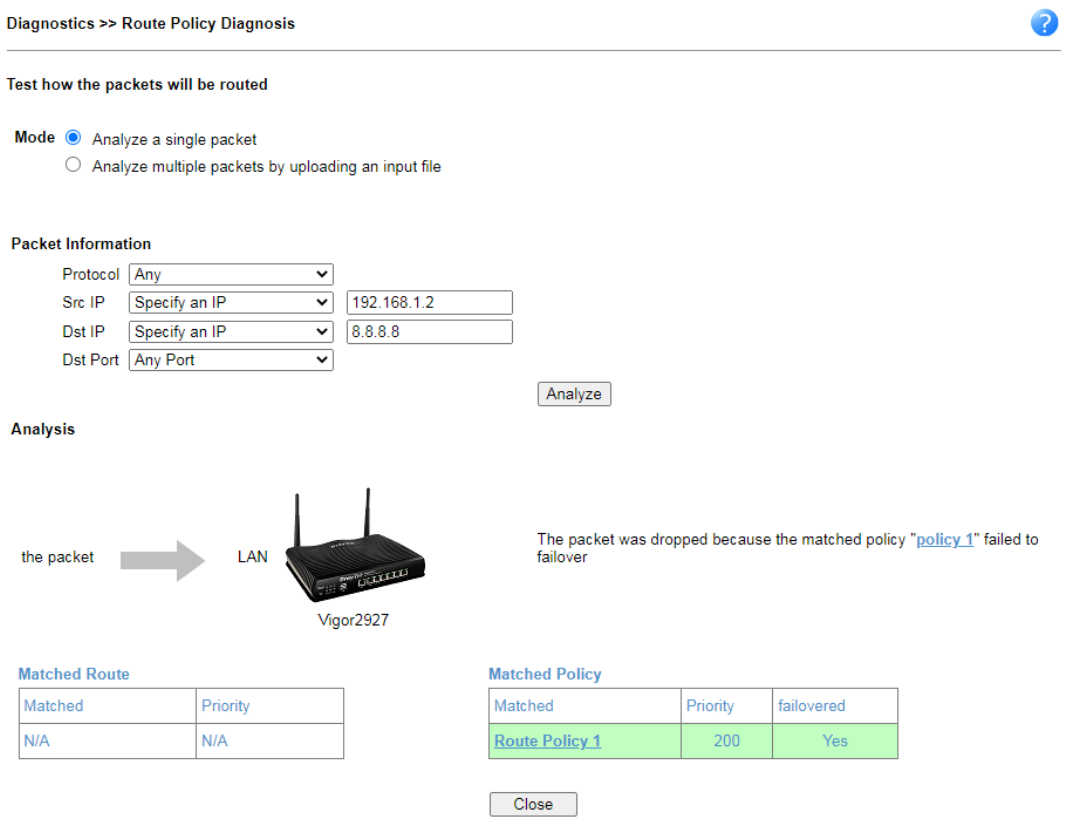


Los ajustes disponibles se explican a continuación:

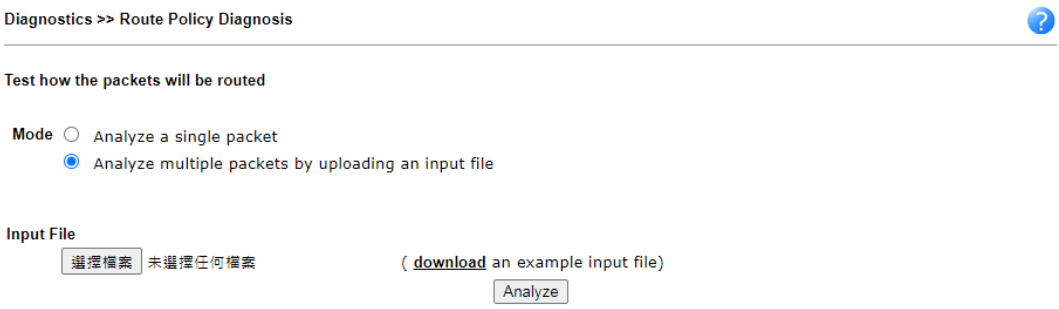
Artículo	Descripción
Información del paquete	Especifique la naturaleza de los paquetes que analizará el enrutador Vigor. **Protocolo -**Especificar un protocolo para el diagnóstico.

	IP de origen–Dirección IP del host donde se origina el tráfico. - **Especificar una IP**-Una dirección IP de origen. - **Cualquier IP**- No se especifica la dirección IP de origen. Cualquier IP de LAN 1/LAN 2/LAN 3/LAN 4/LAN 5/LAN 6/Subred enrutada LAN7/LAN8/ DMZ/IP. - **Subred/Subred enrutada por IP**-Cualquier dirección IP de origen en la subred especificada. **DST IP**–Dirección IP del host de destino. - **Especificar una IP**-Una dirección IP de destino. - **Cualquier IP**-No se especifica la dirección IP de destino. **puerto de horario de verano**–Número de puerto al que se envía el tráfico. Esta configuración solo se aplica a los protocolos UDP y TCP. Utilice la lista desplegable para especificar el puerto de destino. **Analizar**–Haga clic para analizar y mostrar rutas, políticas de ruta y reglas de equilibrio de carga con criterios coincidentes. Si es necesario, haga clic en **análisis de exportación**para exportar el resultado como un archivo.

A continuación se muestra un ejemplo de análisis. El paquete coincidía con los criterios de una política de ruta.



Analice varios paquetes cargando un archivo de entrada



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Fichero de entrada	**Navegar**–Haga clic para examinar la estructura de carpetas y seleccione un archivo de entrada. **Descarga y archivo de entrada de ejemplo**-Haga clic para descargar un archivo de entrada de muestra (archivo ".csv" en blanco). Luego, haga clic en el botón Examinar para seleccionar ese archivo ".csv" en blanco para guardar el resultado del análisis. **Analizar**–Después de seleccionar el archivo de entrada, haga clic para iniciar el proceso de análisis. Haga clic en el**exportar**botón para exportar el resultado como un archivo. Tenga en cuenta que el análisis se basó en la configuración actual de "política de ruta/equilibrio de carga", no garantizamos que sea 100 % igual al caso real.

A continuación se muestra el análisis del archivo de entrada de muestra. Las rutas y políticas coincidentes se resaltan en verde. La columna Resultado final muestra el resultado.

Load-Balance/Route Policy >> Diagnose

Mode

- analyze how a packet will be sent
- analyze how multiple packets as specified in the input file will be sent

Input File

選擇檔案 未選擇檔案 (**download** an example input file)

Analyze

Analysis export analysis

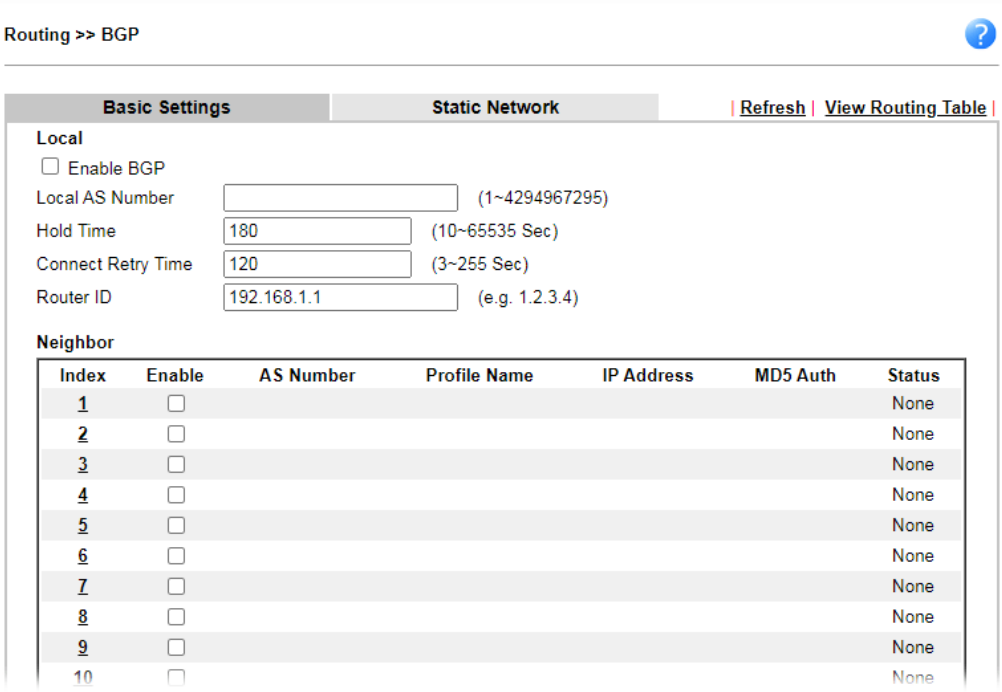
	Input Packet Information				Matched Route		Matched Policy			Final Result	
Profile	Proto	Src IP	Dst IP	Dst Port	Route	Priority	Policy	Priority	failovered	Interface	Reason
LA-branch	ICMP	192.168.1.10	10.10.10.10	N/A	No Match	N/A	No Match	N/A	N/A	N/A	The packet was dropped because neither "route" or "policy" was matched
NY-branch	TCP	192.168.1.20	20.20.20.20	5060	No Match	N/A	No Match	N/A	N/A	N/A	The packet was dropped because neither "route" or "policy" was matched
											The packet was dropped because

II-6-3 BGP

Border Gateway Protocol (BGP) es un protocolo estandarizado diseñado para intercambiar información de enrutamiento y accesibilidad entre sistemas autónomos (AS) en Internet.

II-6-3-1 Configuración básica

Establezca la configuración general para el enrutador local y los enrutadores vecinos.



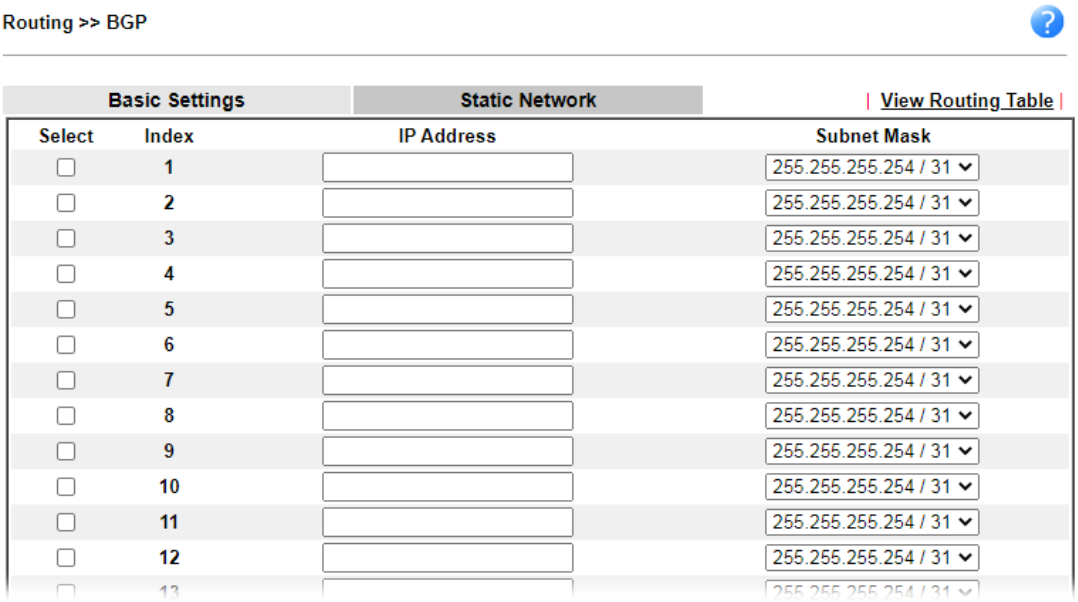
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Local	
Habilitar BGP	Marque la casilla para habilitar la función BGP básica para el enrutador local.
Número AS local	Configure el número AS para el enrutador local.
Hora de espera	Establezca el intervalo de tiempo (en segundos) para determinar que el par está inactivo cuando el enrutador no puede recibir ningún mensaje de actividad del par dentro del tiempo.
Tiempo de reintento de conexión	Si el enrutador no se conecta al enrutador vecino, se requiere un período de tiempo para volver a conectarse. Configure el intervalo de tiempo para realizar la reconexión.
Identificación del enrutador	Especifique la subred LAN para el enrutador.
Vecino	
Índice	Haga clic en el enlace del número de índice para configurar el perfil de vecino.
Permitir	Marque la casilla para habilitar la función BGP básica para el enrutador vecino.
como número	Muestra el número de AS para el enrutador vecino.
Nombre de perfil	Muestra el nombre del perfil vecino.

Dirección IP	Muestra la dirección IP especificada para el perfil vecino.
MD5 Autenticación	Muestra el estado (habilitado o deshabilitado) de la autenticación MD5.
Estado	Muestra el estado de la conexión para el enrutador local y el enrutador vecino.

II-6-3-2 Red Estática

Esta página le permite configurar hasta ocho enrutadores vecinos para intercambiar la información de enrutamiento con el enrutador local.



Los ajustes disponibles se explican a continuación:

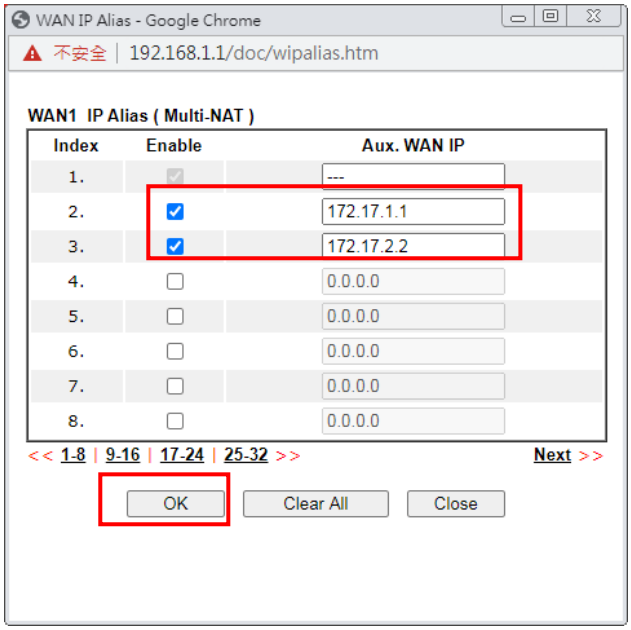
Artículo	**Descripción**
Seleccionar	Marque la casilla para habilitar la configuración de la entrada de índice seleccionada.
Dirección IP	Introduzca la dirección IP de un enrutador.
Máscara de subred	Utilice la lista desplegable para especificar una máscara de subred para la dirección IP.

A-1 ¿Cómo configurar el mapeo de direcciones con la política de ruta?

La asignación de direcciones se utiliza para asignar una IP privada específica o un rango de IP privadas de la subred NAT a una IP de WAN específica (o IP de alias de IP de WAN). Consulte la siguiente figura.

Este documento presenta cómo configurar el mapeo de direcciones con la política de ruta. Cuando una interfaz WAN tiene varias direcciones IP públicas, el administrador puede especificar la IP saliente para determinada dirección IP interna mediante una política de ruta.

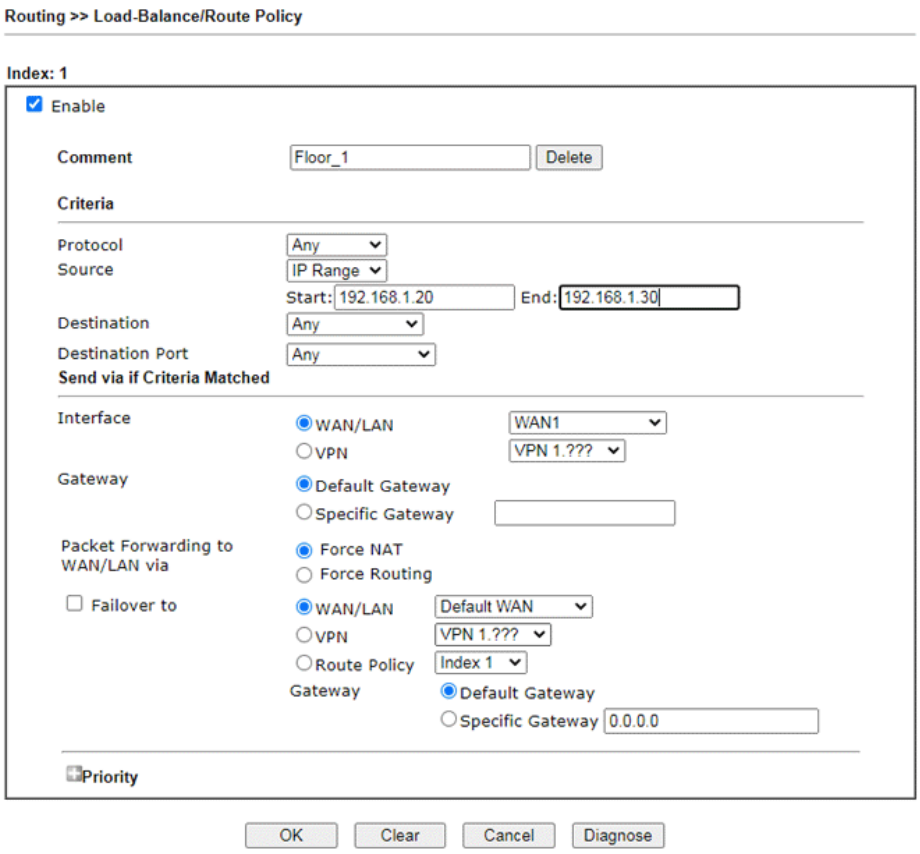
1. Configure el alias de IP de WAN. Ir a**WAN >> Acceso a Internet >> Detalles**página y haga clic en**Alias de IP de WAN**botón.



- Controlar**Permitir**.
- Introduzca la dirección IP de la WAN. Hacer
- clic**DE ACUERDO**ahorrar.

Después de configurar el alias de IP de WAN, las direcciones IP se mostrarán en la lista desplegable de Interfaz en la configuración de Política de ruta.

2. Ir a**Enrutamiento>> Equilibrio de carga/Política de ruta**. Cree una política de ruta para una dirección IP específica para enviar desde una dirección IP WAN específica.

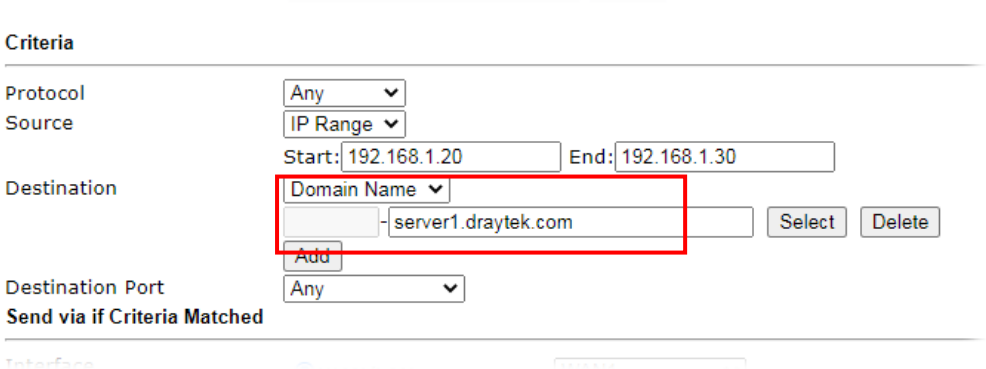


- Habilite esta política.
- Ingresar**IP de origen**como el rango de direcciones IP privadas.
- Deje la IP de destino y el puerto como**Cualquier**.
- Seleccionar**Interfaz**como WAN y luego seleccione Dirección de interfaz de la lista desplegable. (La lista se puede editar en**Alias de IP de WAN**configuración.)
- Permitir**Conmutación por error a**otra WAN para que el tráfico se envíe a través de otra interfaz cuando falle la ruta. Pero no habilite esta opción si desea que el tráfico solo use una dirección IP designada.
- Hacer clic**DE ACUERDO**ahorrar.

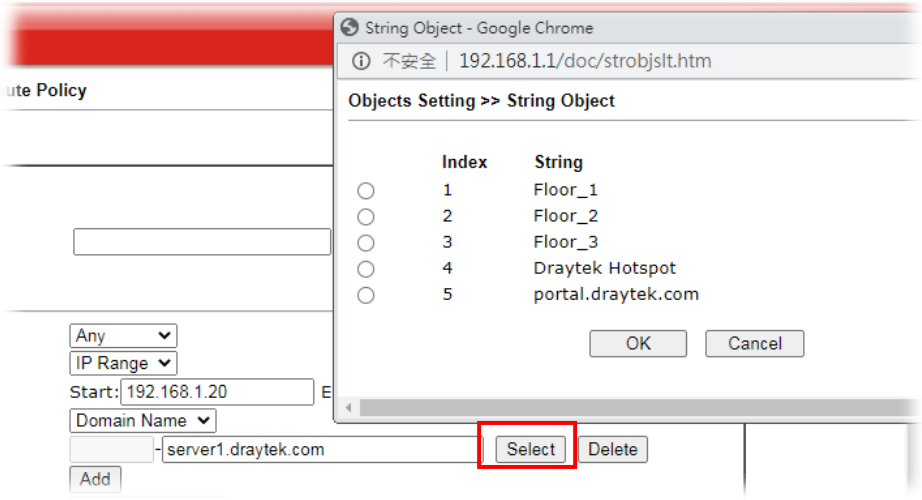
3. Después de la configuración anterior, la fuente del paquete del rango entre 192.168.1.20 y 192.168.1.30 enviado a Internet utilizará la IP pública 172.17.1.1.

La política de ruta admite el uso de un nombre de dominio como criterio de destino. Proporciona una forma más directa de configurar políticas de ruta si el administrador de la red intenta especificar la puerta de enlace para el tráfico destinado a un sitio web determinado.

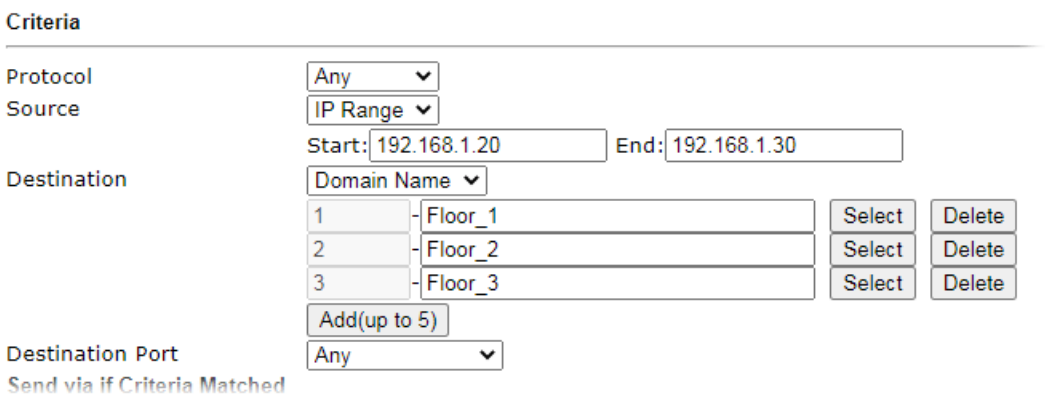
Para usar un nombre de dominio de destino como criterio, simplemente seleccione**Nombre de dominio**como **Destino**en Criterios e ingrese el nombre de dominio en el campo vacío.



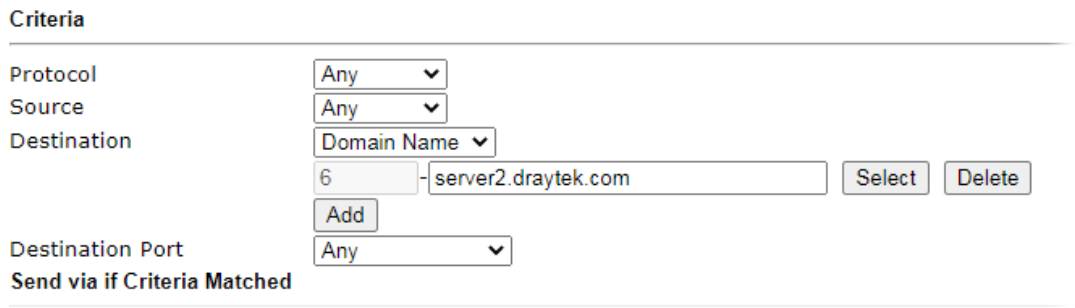
O puede hacer clic**Seleccionar**y utilice una cadena predefinida en Configuración de objetos >> Objeto de cadena como nombre de dominio.



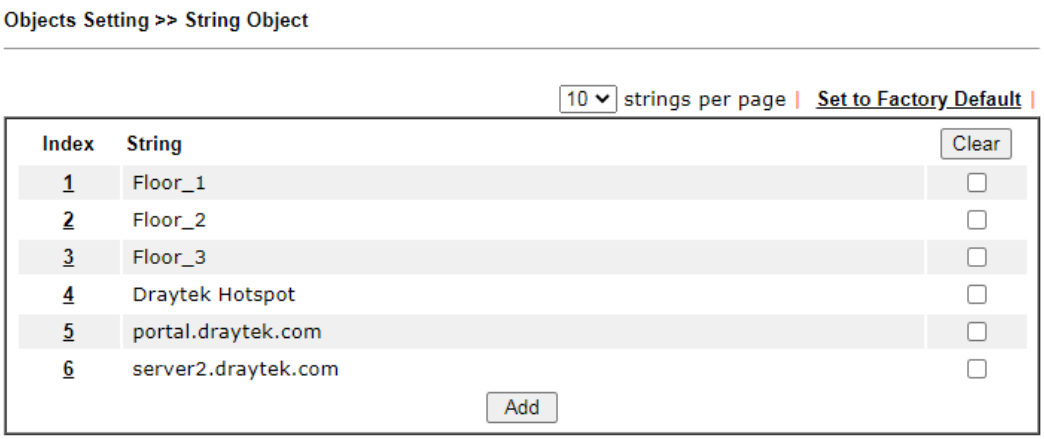
Hacer clic**Agregar**también agregar más nombres de dominio, podemos configurar hasta 5 nombres de dominio en una política de ruta.



Si ingresa manualmente el nombre de dominio en una política de ruta, después de hacer clic en**DE ACUERDO**para aplicar la política de ruta, esos nombres de dominio recibirán un número.



Eso significa que el enrutador ha creado automáticamente objetos de cadena para esos nombres de dominio, de modo que puedan usarse en otras políticas de ruta u otras funciones.

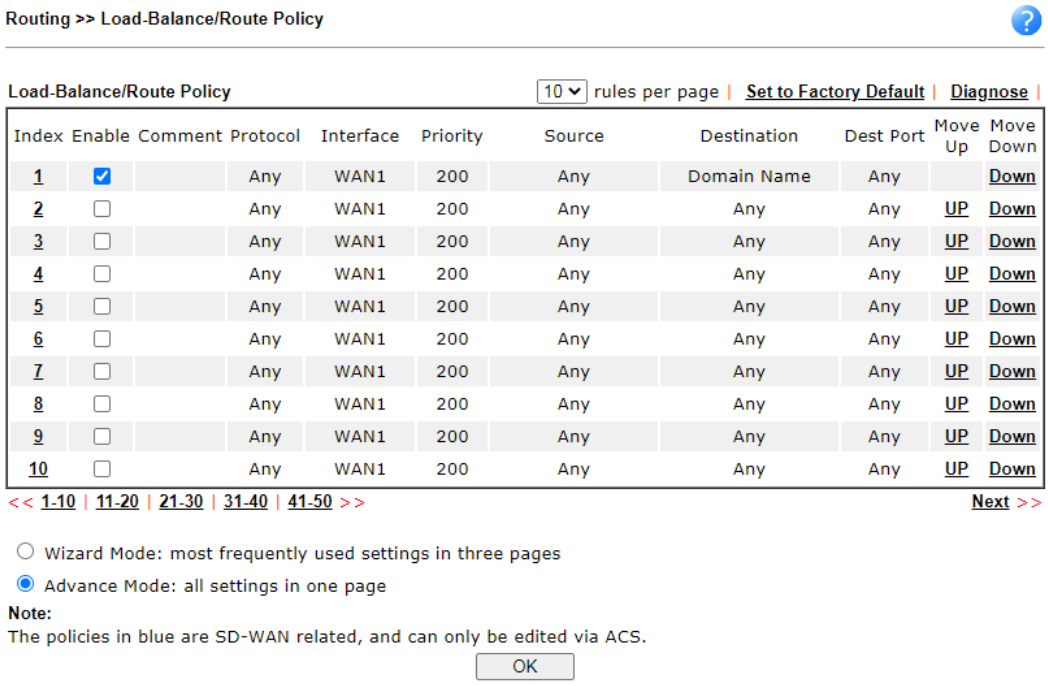


A-3 Introducción a la política de ruta/equilibrio de carga

Este documento presenta la política de ruta/equilibrio de carga. Esta característica permite que el administrador de la red administre el tráfico saliente de manera más específica.

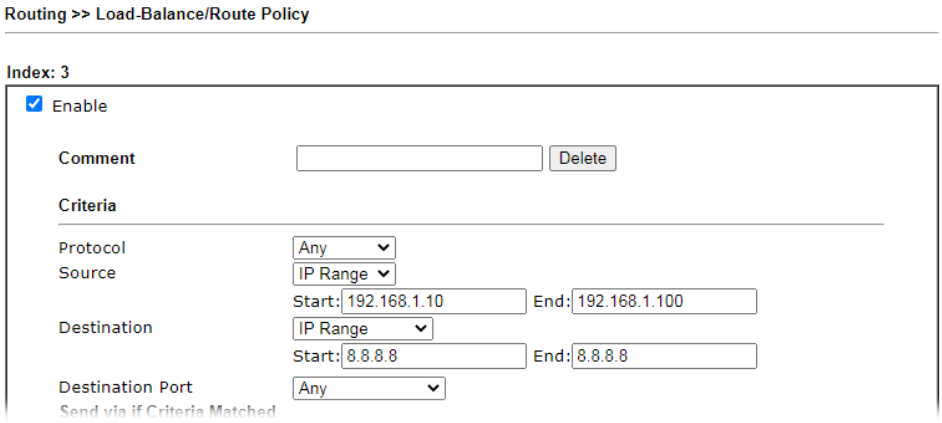
La política configurada en Load-Balance/Route Policy siempre tiene mayor prioridad que la ruta predeterminada y el Auto Load Balance configurados en**WAN >> Configuración general**, y siempre tiene menor prioridad que las Reglas de Firewall. El administrador también puede definir una prioridad para esta política.

Para configurar la política de ruta, vaya a**Enrutamiento>>Equilibrio de carga/Política de ruta**. La siguiente imagen es una captura de pantalla de la página de política Load-Balance/Route. Enumera todas las políticas y muestra si la política está habilitada, cuáles son los criterios que deben coincidir y a través de qué interfaz debe pasar el tráfico si se cumplen los criterios, y también su prioridad.



Para configurar una política de ruta, simplemente haga clic en un número de índice. En la parte inferior de la página, se pueden elegir dos modos de configuración: el Modo Asistente proporciona una configuración simple y básica; mientras que el Modo Avanzado permite más opciones.

1. Primero, establezca los criterios de los paquetes para aplicar esta política.



a. Seleccione un Protocolo.

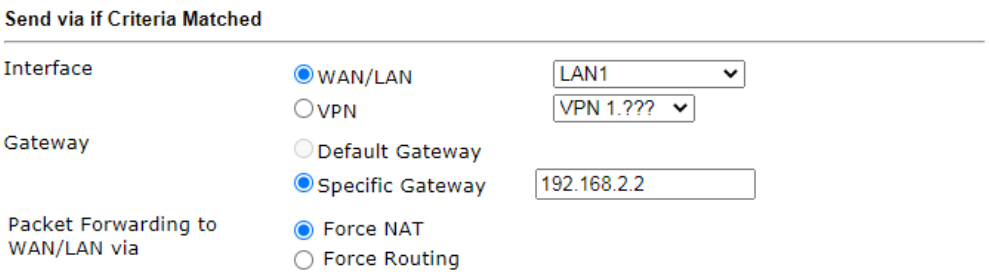
b. Ingrese el rango de dirección IP de origen, la IP de origen podría ser una sola dirección si el inicio y el final son iguales.

C. Ingrese el rango de direcciones IP de destino.

d. Seleccione el puerto de destino.

La configuración anterior es un ejemplo de que si un paquete se envía desde 192.168.1.10~192.168.1.100 a 8.8.8.8, sin importar cuál sea el protocolo o el puerto de destino, seguirá esta política de ruta.

2. A continuación, seleccionamos una interfaz y una puerta de enlace a través de la cual se debe enviar el paquete si cumple con los criterios.

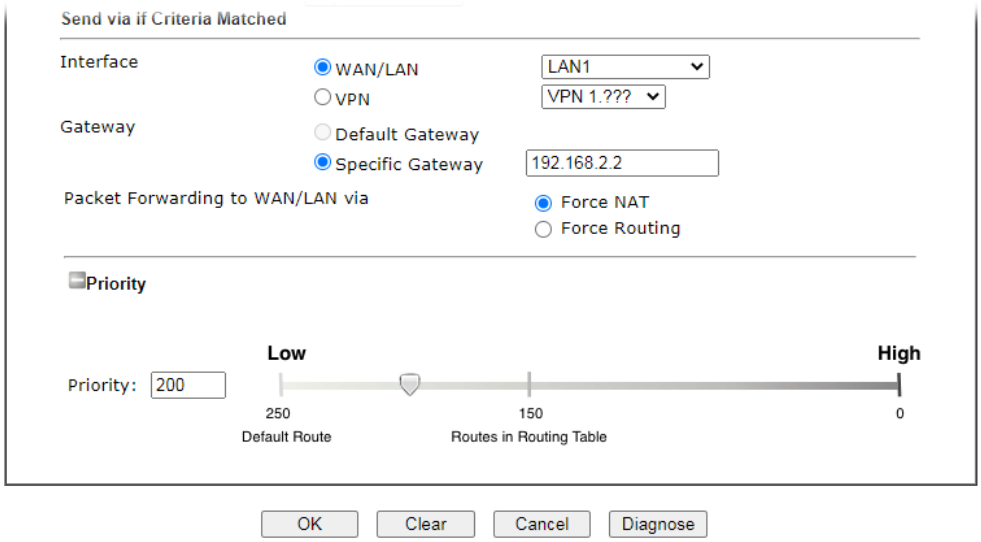


a. Seleccione una interfaz.

b. Seleccione una IP de puerta de enlace. Tenga en cuenta que si se elige la interfaz para que sea una LAN, es necesario designar una puerta de enlace específica.

La configuración anterior es un ejemplo de que si un paquete coincide con los criterios de esta Política de ruta, se enviará a la puerta de enlace predeterminada y luego al destino a través de VPN1.

3 en**Modo avanzado**, si la interfaz se selecciona como WAN o VPN, hay algunas opciones más:



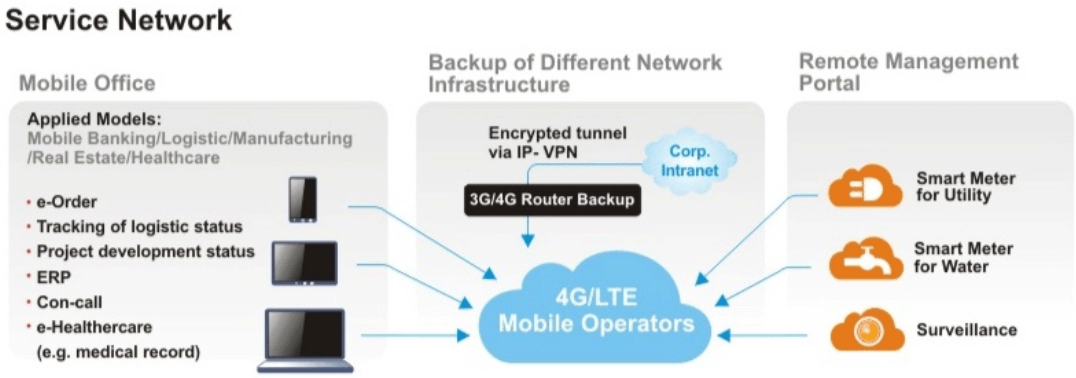
- **Prioridad**: el administrador puede establecer una prioridad entre 1 y 249 para esta política de ruta, donde un número más pequeño indica una prioridad más alta. Cuando dos políticas tienen la misma prioridad, se implementará la primera política coincidente (de acuerdo con el orden del índice de políticas).

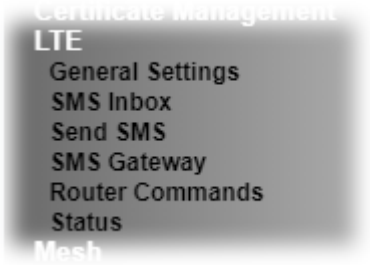
II-7 LTE

LTE WAN con tarjeta SIM puede proporcionar un acceso a Internet conveniente para el enrutador Vigor. Sin embargo, no podemos dejar de pensar en qué puede utilizar el enrutador Vigor con esta tarjeta SIM para proporcionar funciones más útiles para el usuario. Ahora, hemos desarrollado algunas funciones útiles para el usuario, como enviar SMS desde un enrutador para informar el estado del enrutador, reiniciar el enrutador de forma remota a través de SMS teniendo en cuenta la seguridad, etc.

Esta sección puede guiarlo para usar la tarjeta SIM en LTE WAN para realizar operaciones relacionadas con SMS.

Información	Esta función se utiliza solo para los modelos “L”.

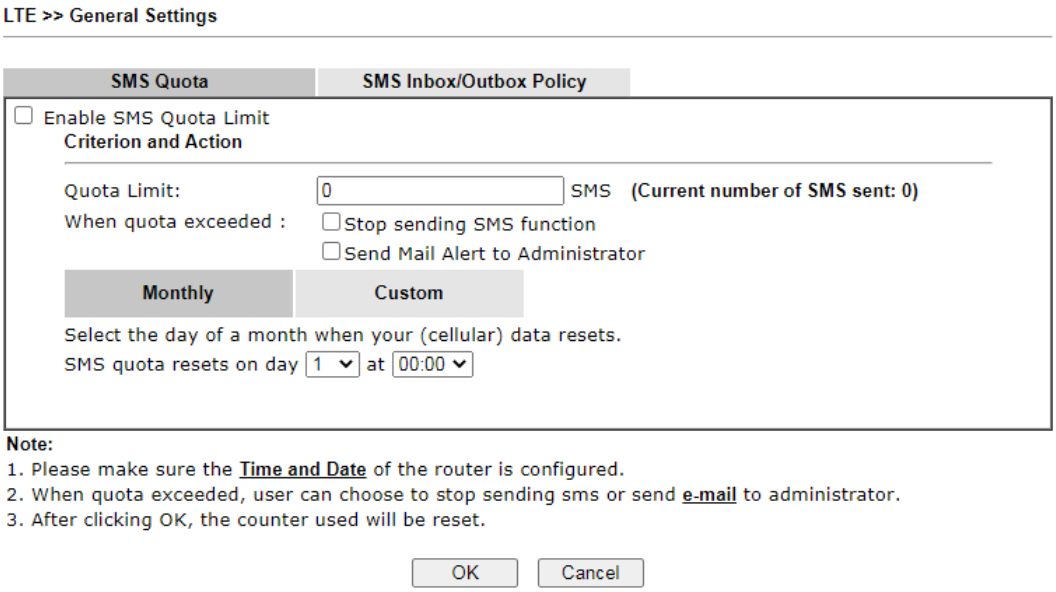




II-7-1 Configuración general

Esta página le permite configurar los ajustes generales para LTE. Cuando el límite de cuota de SMS está habilitado, puede especificar la cantidad de cuota de SMS, las acciones a realizar cuando se exceda la cuota y el período de restablecimiento de la cuota de SMS utilizada.

II-7-1-1 Cuota de SMS



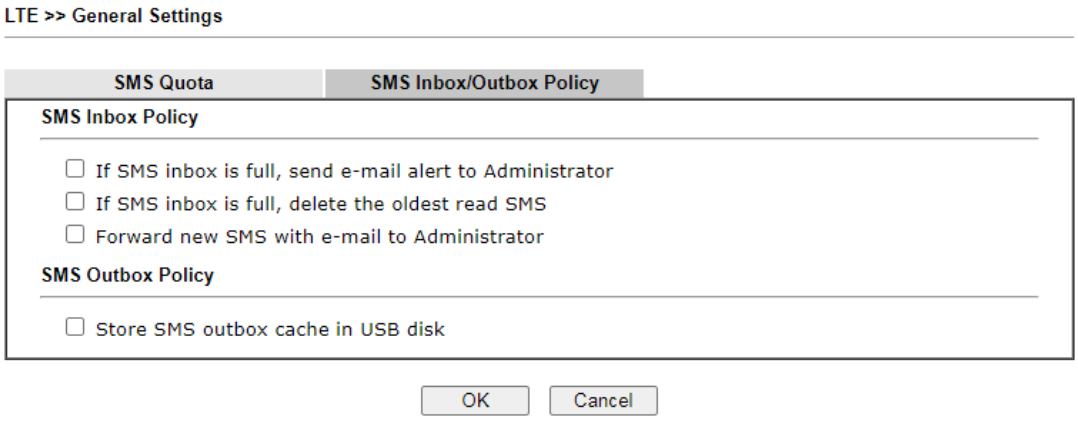
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar límite de cuota de SMS	Marque la casilla para habilitar dicha función.
Límite de cuota	Especifique el número máximo de envío de SMS para LTE.
Cuando se supera la cuota	Hay dos acciones que se deben realizar cuando el límite de la cuota caduca. **Dejar de enviar SMS**–Si está marcado, no se enviará ningún SMS para LTE después de que expire el límite de cuota. **Enviar alerta de correo al administrador**–Si está marcada, se enviará una alerta por correo al administrador cuando expire el límite de cuota.
Mensual	Esta configuración es para ofrecer un mecanismo de reinicio del número

	de registro de SMS enviados cada mes. **La cuota de SMS se restablece el día XX a las XX...**–Puede determinar el día de inicio en un mes. El número de SMS enviados se restablecerá.
Costumbre	Esta configuración permite al usuario definir el ciclo de facturación de acuerdo a su solicitud. El número de SMS enviados se restablecerá con un intervalo de duración del ciclo. **Costumbre**–Mensual es la configuración predeterminada. Si se requiere un período largo o corto, utilice**Costumbre**. El período de reinicio es entre 1 día y 60 días. Puede determinar la duración del ciclo especificando los días y las horas. - **Duración del ciclo**: Especifique los días para restablecer la cantidad de SMS enviados. Por ejemplo, 7 significa que todo el ciclo es de 7 días; 20 significa que todo el ciclo es de 20 días. Cuando se acabe el tiempo, el enrutador restablecerá la cantidad de SMS enviados automáticamente. - **Hoy es el día XX del ciclo**–Especifique el día en la duración del ciclo como punto de partida en el que el enrutador Vigor restablecerá la cantidad de SMS enviados. Por ejemplo, 3 significa el tercer día del ciclo de duración.

II-7-1-2 Bandeja de entrada/salida de SMS

Dicha página le permite determinar qué política se utilizará para la bandeja de entrada/salida de SMS.

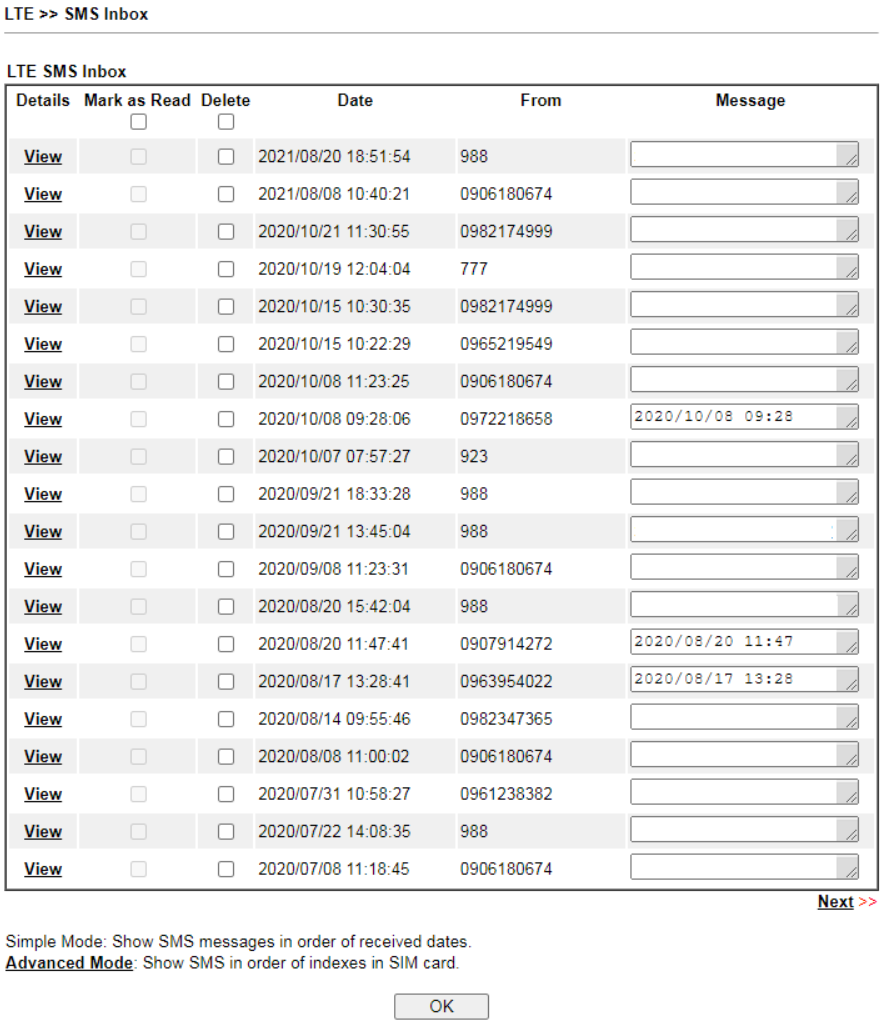


Esta página enumerará los mensajes SMS recibidos en la tarjeta SIM LTE. La tabla de la bandeja de entrada de SMS muestra la fecha de recepción, el número de teléfono o la identificación del remitente de donde proviene este mensaje y el comienzo del contenido del mensaje.

Dado que el tamaño de los datos de un SMS es limitado, varios SMS enviarán un mensaje largo. Para comodidad de los usuarios, ofrecemos dos modos.**Modo simple** enumera los mensajes SMS en orden de hora de recepción.**Modo avanzado** enumera los SMS para obtener un índice real en la tarjeta SIM. Diferentes tarjetas SIM tienen diferentes capacidades. En general, son alrededor de 30 a 40 SMS. Tenga en cuenta que la tarjeta SIM no puede recibir nuevos SMS cuando todos los índices de SMS están ocupados.

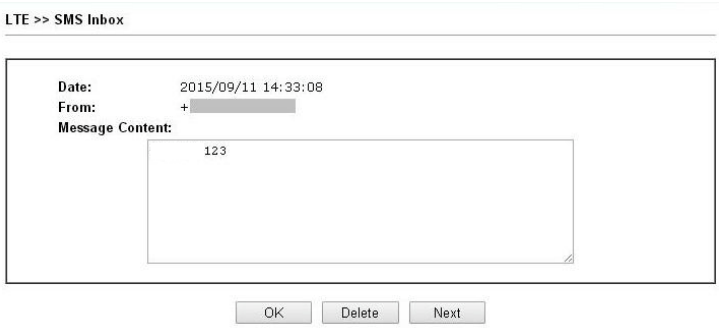
Haga clic en el enlace Modo simple o en el enlace Modo avanzado a continuación para cambiar entre estos dos modos.

II-7-2-1 Modo sencillo

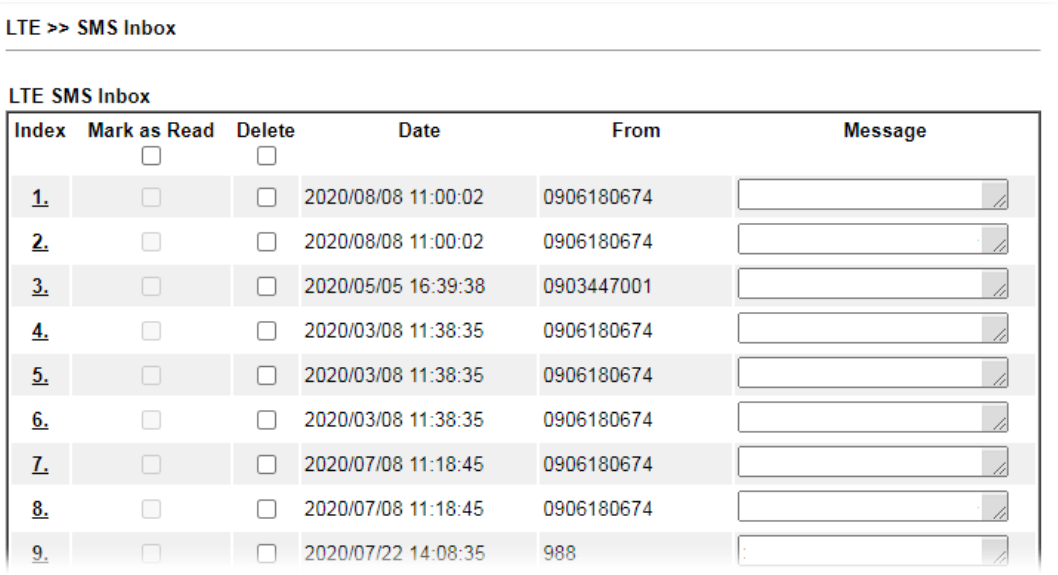


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Marcar como leído	Los mensajes en estado "no leído" se muestran en negrita. Si desea cambiar los mensajes al estado "leído", selecciónelos y haga clic en el botón Aceptar. Al marcar la casilla de verificación en el título, se seleccionarán todos los mensajes "no leídos" en esta página.

Borrar	Si desea eliminar mensajes, selecciónelos y haga clic en el botón Aceptar. Al marcar la casilla de verificación en el título, se seleccionarán todos los mensajes en esta página.
Detalles	Si desea leer el contenido completo del mensaje, haga clic en el Vista enlace de ese mensaje para abrir la página siguiente. Cambiará el mensaje al estado "leído".  - **Contenido del mensaje**-Mostrar el contenido completo del mensaje. - **DE ACUERDO**-Volver a la pagina anterior. - **Borrar**-Haga clic para eliminar este mensaje y volver a la página anterior. - **Próximo**-Haga clic para ver el contenido del siguiente mensaje.

II-7-2-1 Modo avanzado



Los ajustes disponibles se explican a continuación:

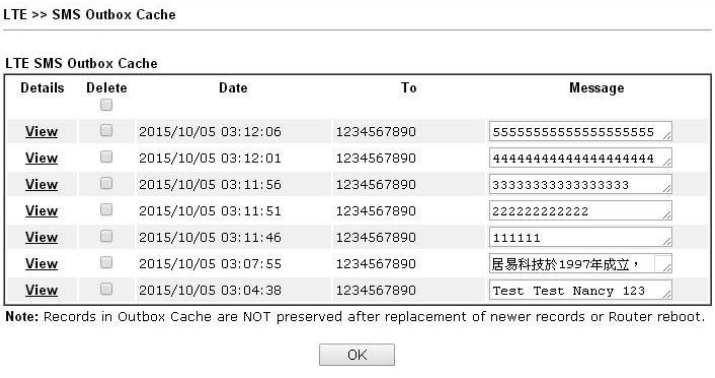
Artículo	Descripción
Marcar como leído	Los SMS en estado "no leído" se muestran en negrita. Si desea cambiar los SMS al estado de "lectura", selecciónelos y haga clic en el botón Aceptar. Al marcar la casilla de verificación en el título, se seleccionarán todos los SMS "no leídos" en esta página.
Borrar	Si desea eliminar SMS, selecciónelos y haga clic en el botón Aceptar. Al marcar la casilla de verificación en el título, se seleccionarán todos los SMS en esta página.
Índice	Si desea leer el contenido completo del mensaje de la

	SMS, haga clic en el enlace de índice de ese SMS para abrir la página siguiente. Cambiará todos los SMS del mensaje al estado "leído". **Contenido del mensaje**-Mostrar el contenido completo del mensaje. **DE ACUERDO**-Volver a la pagina anterior. **Borrar**-Haga clic para eliminar todos los SMS de este mensaje y volver a la página anterior. **Próximo -**Haga clic para ver el contenido del siguiente índice de SMS.

II-7-3 Enviar SMS

Esta página se utiliza para enviar mensajes SMS mediante la tarjeta SIM LTE. También muestra la cantidad de SMS necesarios para enviar el mensaje.

Los ajustes disponibles se explican a continuación:

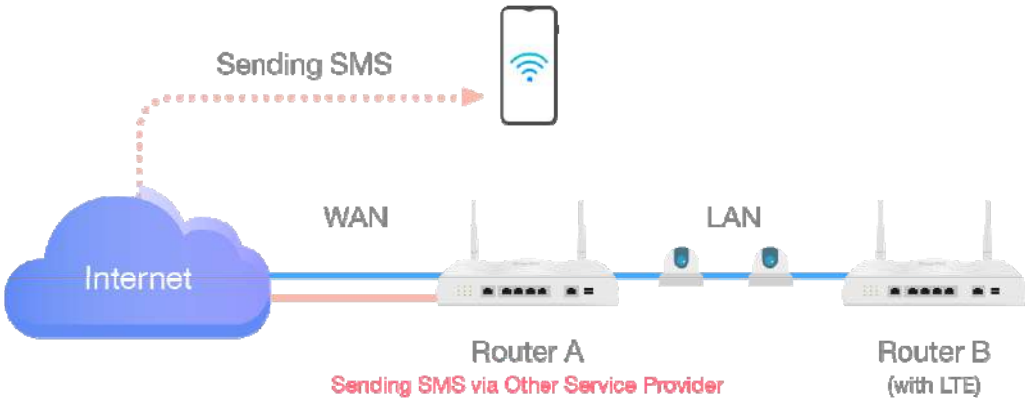
Artículo	Descripción
Número de destinatario	Introduzca el número de teléfono del destinatario. El formato puede ser un número de teléfono internacional (+8869123455678) o un número de teléfono general (0912345678).
Esquema de codificación de datos	El enrutador seleccionará automáticamente un esquema de codificación de datos adecuado de acuerdo con el contenido actual del mensaje. Se admiten GSM de 7 bits y UCS-2.
Mensaje	Introduzca el contenido del mensaje a enviar. El número total de caracteres que puede ingresar en este campo es 1024.
Enviar mensaje	Haga clic para enviar este mensaje SMS al destinatario inmediatamente.
VistaCaché de la bandeja de salida de SMS	Muestra el registro de mensajes SMS enviados desde el enrutador. 

II-7-4 Puerta de enlace SMS

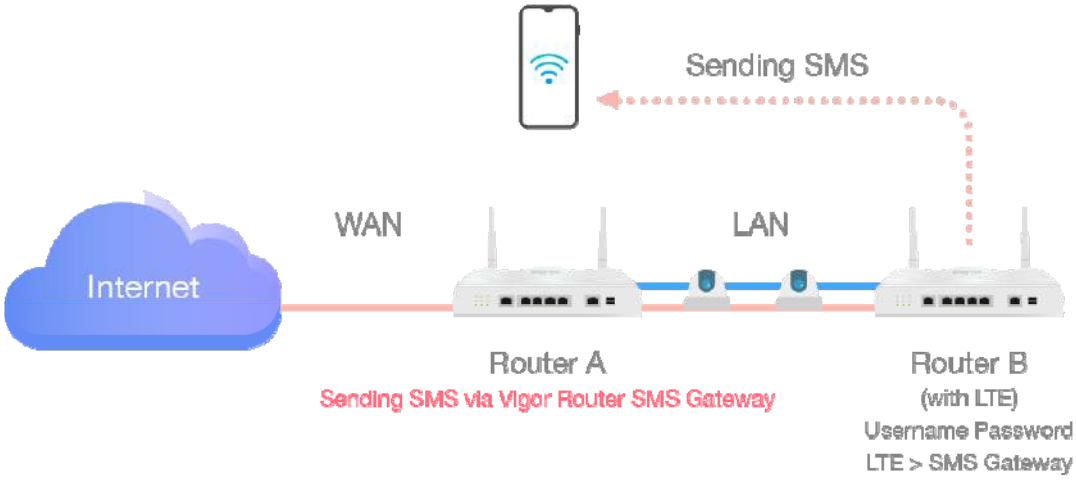
El enrutador Vigor puede servir como puerta de enlace SMS para enviar alertas a través de SMS a teléfonos móviles.

Fíjate en las dos imágenes siguientes.

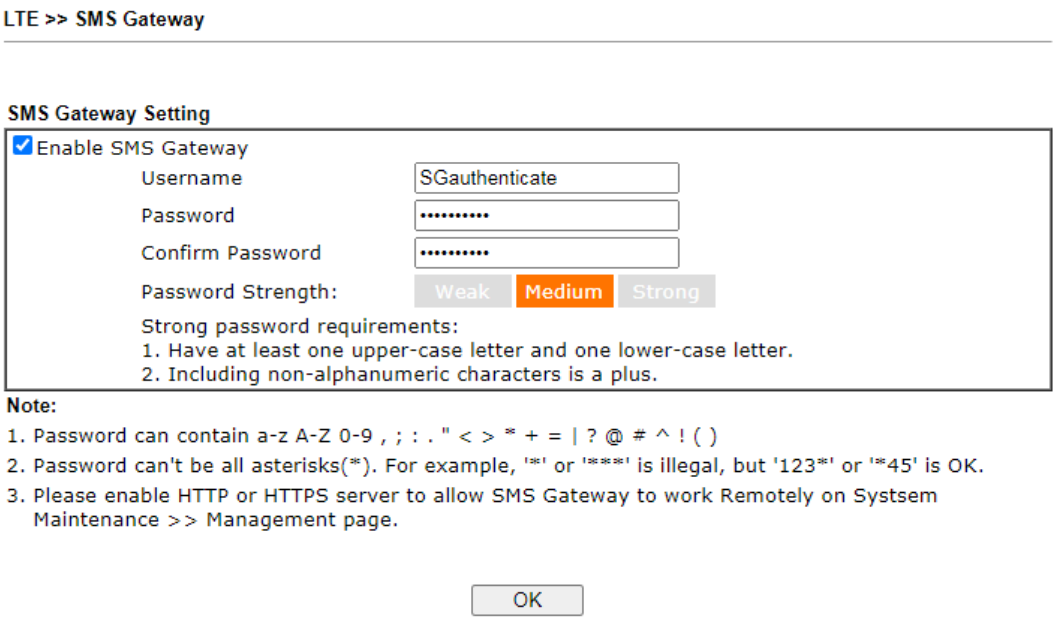
Las cámaras IP se conectan al enrutador A y al enrutador B a través de LAN. Cuando hay algún problema con la cámara IP, el enrutador A solo puede enviar el SMS con alertas/mensajes de advertencia a través de un proveedor de servicios específico en Internet.



Con la función de SMS Gateway en el enrutador B, incluso el enrutador A está fuera de línea, el enrutador B podría servir como una puerta de enlace SMS que puede enviar SMS (relacionados con alertas u otros eventos) a teléfonos móviles directamente.



Para el enrutador B, simplemente abra**LTE>>Puerta de enlace SMS**y establecer un par de nombre de usuario y contraseña.



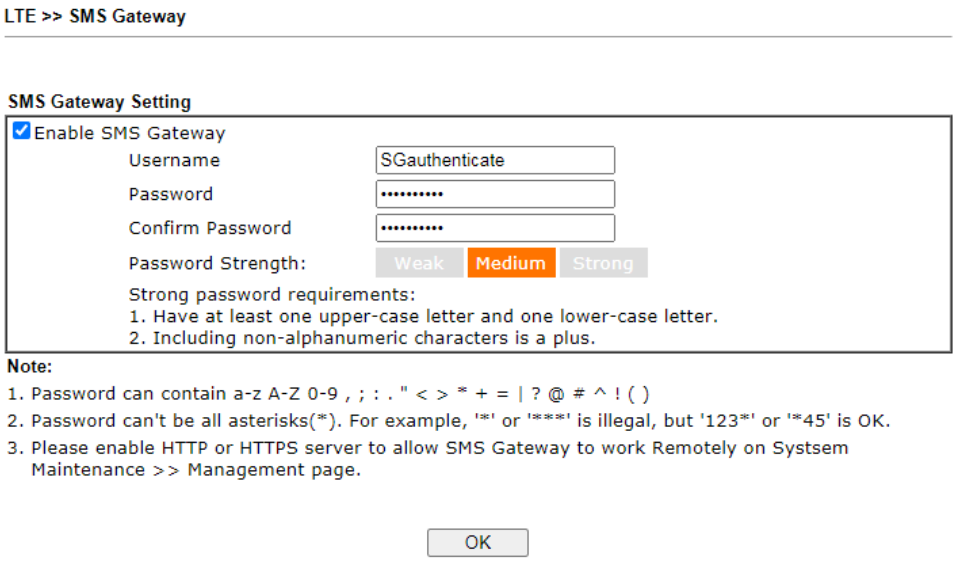
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar puerta de enlace SMS	Marque la casilla para habilitar la puerta de enlace SMS de este enrutador.
Nombre de usuario	Defina un nombre de usuario.
Contraseña	Defina una contraseña.
Confirmar contraseña	Introduzca la contraseña de nuevo.

A continuación se muestran los ajustes configurados en el enrutador A y el enrutador B.

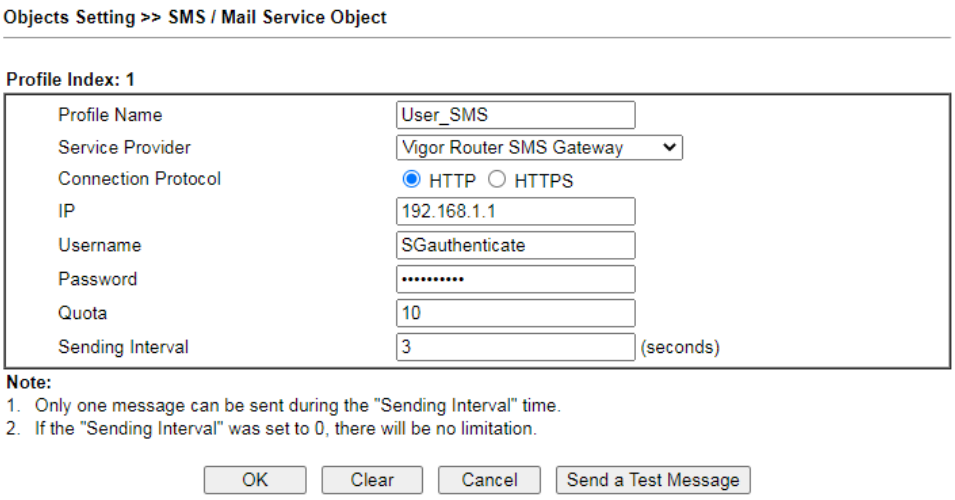
1. Conecte el enrutador A y el enrutador B (con módulo LTE).

2. En el enrutador B, establezca un par de nombre de usuario (por ejemplo, SGauthenticate) y contraseña en**LTE>>Puerta de enlace SMS**.



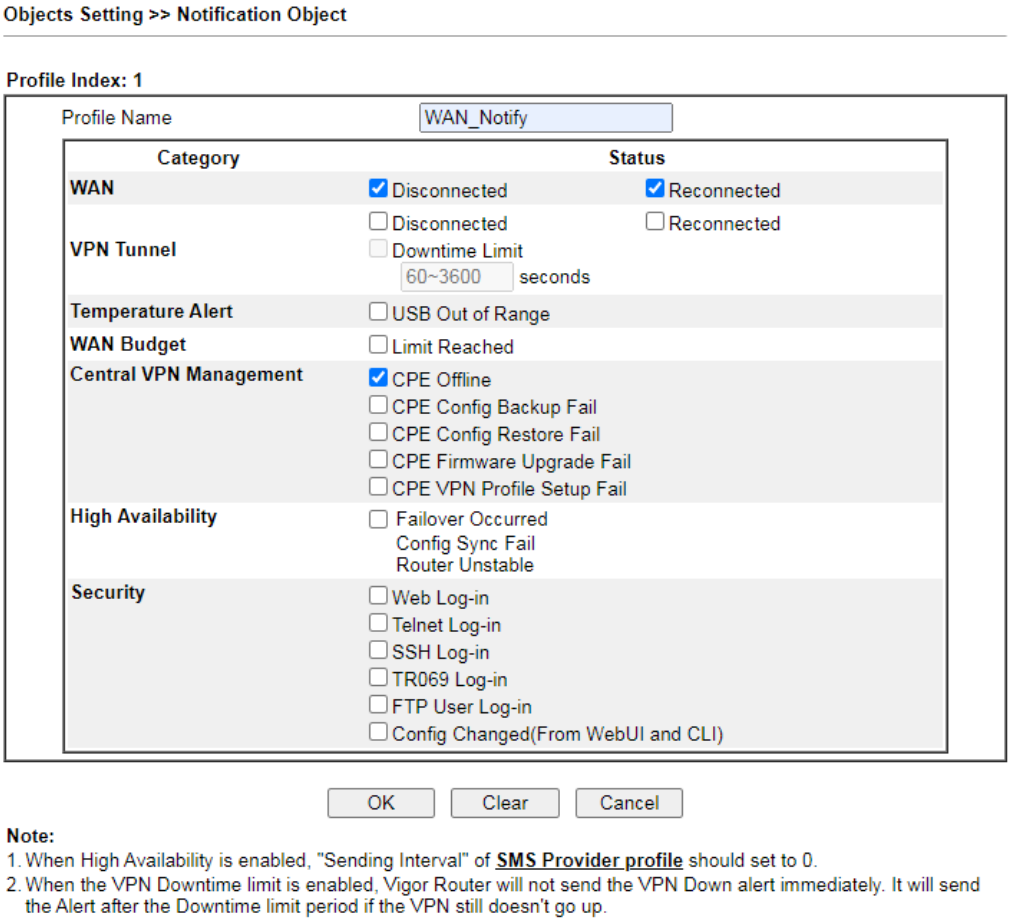
3. En el enrutador A, abra**Configuración de objetos >> Objeto de servicio de SMS/correo >> Proveedor de servicios**. Haga clic en cualquier número de índice (p. ej., #1 en este caso) para abrir la siguiente página. Seleccionar**Vigor**

Puerta de enlace SMS del enrutadorcomo proveedor de servicios. Establezca la IP de WAN o la IP de LAN de este enrutador en el campo IP.



En cuanto al nombre de usuario y la contraseña, ingrese los mismos valores que configuró en el Paso 2.

4. A continuación, vaya a**Configuración de objetos >> Objeto de notificación**. Seleccione desconexión o conexión de WAN, túnel VPN y haga clic en**DE ACUERDO**para guardar la configuración en el enrutador A.



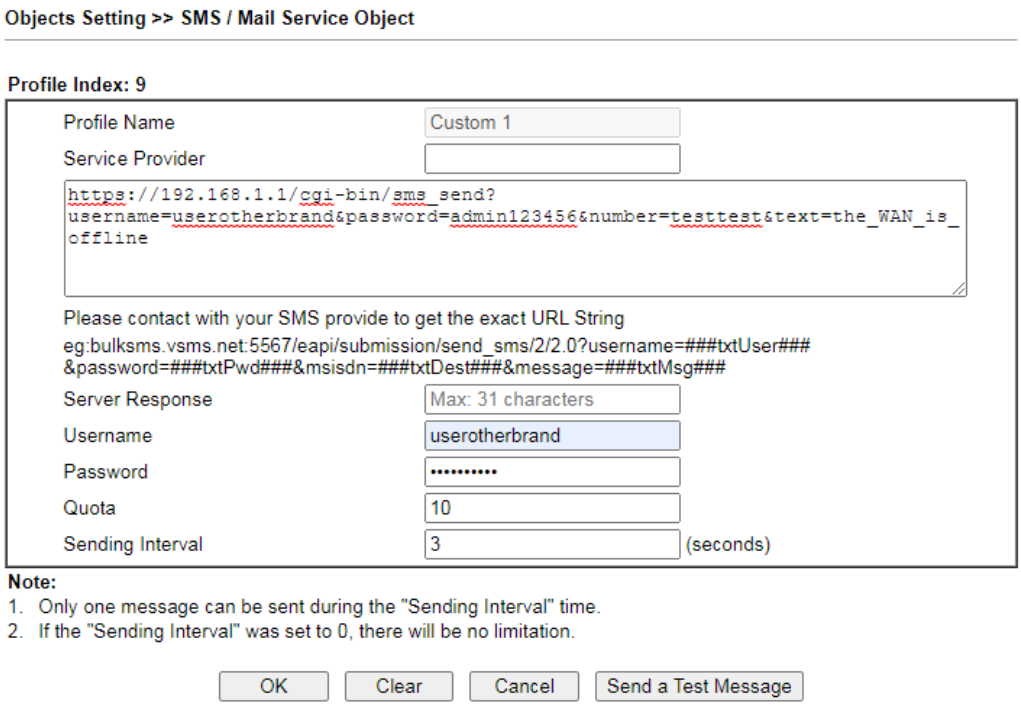
5. Una vez que el enrutador A encuentre la condición establecida anteriormente, el enrutador B (como puerta de enlace de SMS) enviará un SMS al destinatario.

Para un usuario que posee un enrutador LTE que no es DrayTek, hay una forma de enviar el SMS a teléfonos móviles a través del enrutador LTE que no es DrayTek y el enrutador DrayTek.

1. Asegúrese de que el enrutador DrayTek y el enrutador LTE que no sea DrayTek estén conectados a través de LAN.

2. Obtenga la cadena URL exacta del enrutador LTE que no sea DrayTek.

3. En el enrutador DrayTek, abra**Configuración de objetos>>Objeto de servicio de correo/SMS**y haga clic en el enlace numérico #9 o #10 para personalizar el objeto del servicio de SMS.



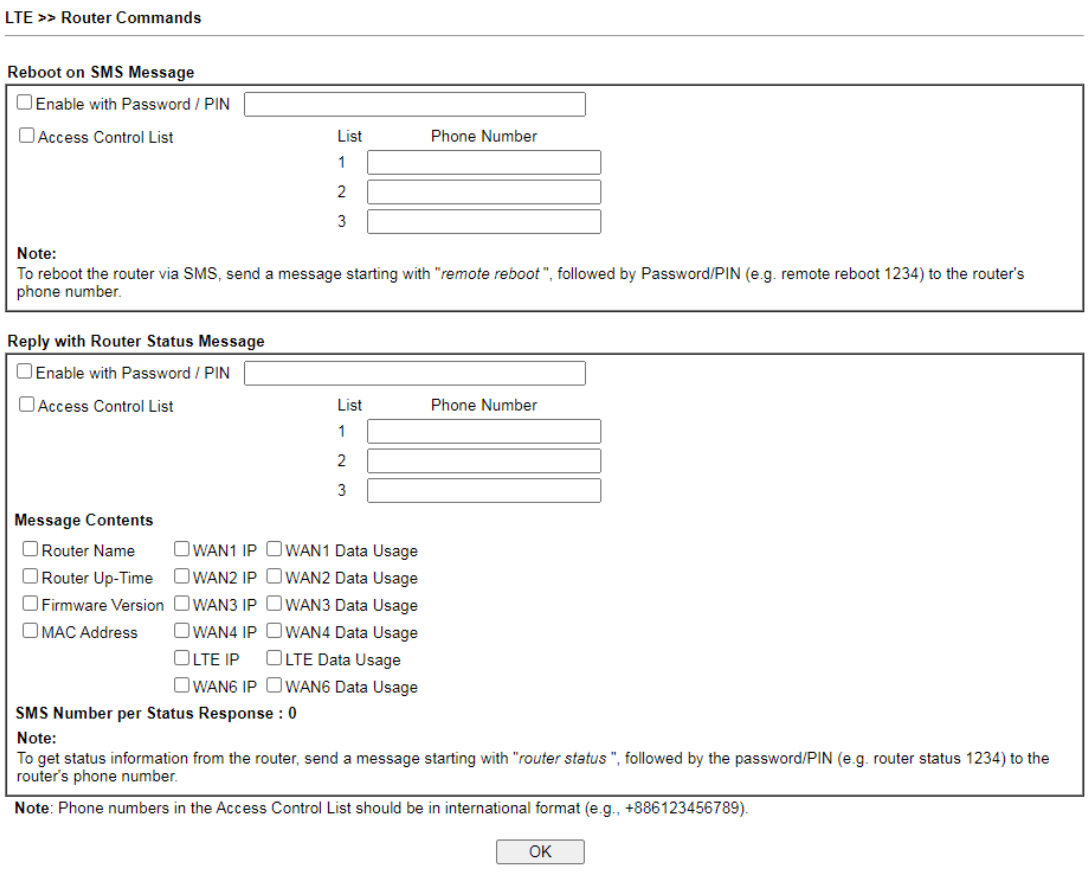
Ingrese los datos provenientes del enrutador LTE que no es DrayTek, por ejemplo, la cadena de URL, el nombre de usuario, la contraseña y el mensaje de advertencia en el cuadro de entrada.

4. Haga clic en**DE ACUERDO**para guardar la configuración.

II-7-5 Comandos del enrutador

Esta página le permite al usuario configurar la función para reiniciar el enrutador Vigor de forma remota y obtener el estado del enrutador a través de SMS.

Ir a**LTE>>Comandos del enrutador**para obtener la siguiente página.



Los ajustes disponibles se explican a continuación:

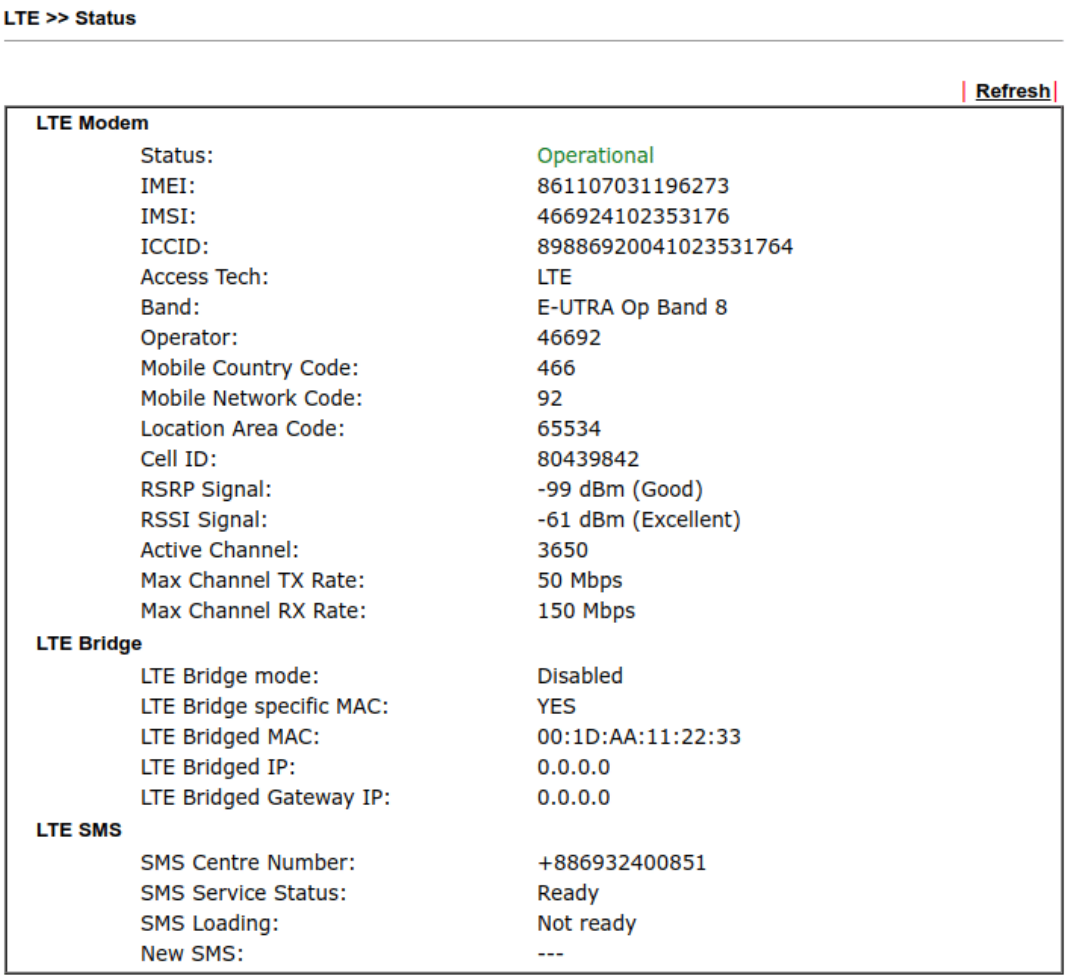
Artículo	Descripción
Reiniciar en mensaje SMS	
Habilitar con contraseña / PIN	Para reiniciar el enrutador Vigor de forma remota a través de SMS, marque dicha casilla e ingrese la contraseña/número PIN (tratado como autenticación para cualquier teléfono móvil). La contraseña estará compuesta por letras, números y línea base.

Lista de control de acceso	Marque la casilla para escribir o modificar (hasta 3) números de teléfono. El número de teléfono especificado aquí es capaz de enviar SMS para reiniciar dicho enrutador Vigor de forma remota. **Nota**: Si tal opción es**activado**, solo los teléfonos móviles especificados aquí pueden enviar SMS para reiniciar el enrutador Vigor si se proporciona la contraseña correcta. Es decir, si es**desactivado** (sin marcar), cualquier teléfono móvil puede enviar SMS para reiniciar dicho enrutador Vigor si se proporciona la contraseña correcta.
Responder con el mensaje de estado del enrutador	
Habilitar con contraseña / PIN	Los usuarios pueden obtener el uso de datos WAN e información básica sobre el enrutador Vigor (por ejemplo, dirección IP, dirección MAC) a través del teléfono móvil ingresando la contraseña/PIN especificado en este campo. La contraseña estará compuesta por letras, números y línea base.
Lista de control de acceso	Marque la casilla para escribir o modificar (hasta 3) números de teléfono. El número de teléfono especificado aquí es capaz de obtener información relacionada sobre el enrutador Vigor de forma remota. **Nota**: Si tal opción es**activado**, solo los teléfonos móviles especificados aquí pueden obtener información relacionada con el enrutador Vigor si se proporciona la contraseña correcta. Es decir, si es**desactivado** (sin marcar), cualquier teléfono móvil puede obtener los datos del enrutador Vigor si se proporciona la contraseña correcta.
Contenido del mensaje	Hay varios tipos de contenidos de mensajes para que usted seleccione. Elija y marque el elemento requerido, luego el enrutador Vigor ofrecerá la respuesta de estado sobre ese elemento a través de SMS.
Mensajes SMS por respuesta de estado	Muestra el número total del tipo para la respuesta de estado. Muestra el número total de SMS necesarios para enviar el mensaje de estado que contiene el contenido del mensaje seleccionado actualmente.

II-7-6 Estado

El enrutador Vigor con función LTE es capaz de acceder a Internet y enviar SMS a un teléfono móvil específico. Además, se puede tratar como un módem LTE.

Esta página mostrará información básica sobre el módulo LTE integrado y la conexión LTE actual.



Cada elemento se explica de la siguiente manera:

Artículo	Descripción
Módem LTE	
Estado	Estado de WAN LTE.
IMEI	Identidad de equipo móvil internacional del módulo LTE integrado.
IMSI	Identidad de suscriptor móvil internacional de la tarjeta SIM LTE.
Acceso a la tecnología	Tipo de conexión LTE (CDMA/GSM/ WCDMA/LTE/TD-SCDMA).
Banda	Banda de conexión LTE.
Operador	Nombre del ISP de la conexión LTE.

Código de país móvil / Código de red móvil / Código de área de ubicación / ID de celda:	Información de la estación base.
Señal	Intensidad de la señal de la conexión LTE.
Canal activo	Frecuencia de conexión LTE.
Interferencia con WLAN de 2,4 GHz	Si la frecuencia LTE actual causa interferencia con la conexión inalámbrica 2.4G. En caso afirmativo, se indicarán los canales inalámbricos 2.4G interferidos.
Velocidad máxima de TX del canal / Velocidad máxima de RX del canal	Velocidad máxima de enlace TX/RX de conexión LTE.
SMS LTE	
Número del centro de SMS	El número de teléfono para el servicio de SMS de la tarjeta SIM LTE.
Estado del servicio SMS	Si el servicio de SMS de la tarjeta SIM LTE está listo.
Cargando SMS	Si los mensajes SMS recibidos en la tarjeta SIM LTE se han cargado en el enrutador.
SMS nuevos	El número de SMS no leídos en la bandeja de entrada de SMS.

Parte III LAN inalámbrica

La LAN inalámbrica permite una alta movilidad para que los usuarios de WLAN puedan acceder simultáneamente a todas las instalaciones de LAN como en una LAN con cable, así como al acceso a Internet.

LAN inalámbrica III-1 (2,4 GHz/5 GHz)

Esta función está disponible solo en modelos inalámbricos (modelos con sufijos –ax o –ac).

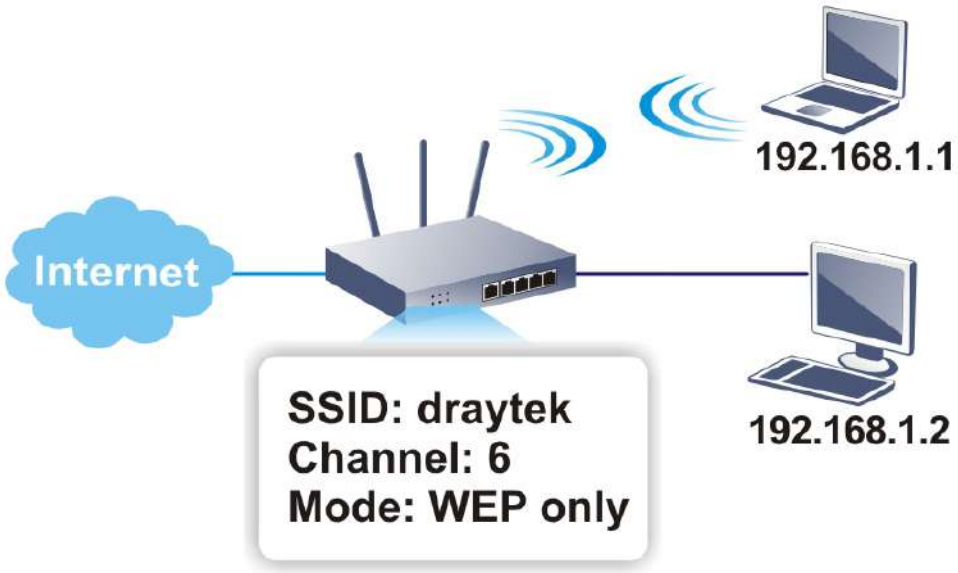
En los últimos años, el mercado de las comunicaciones inalámbricas ha disfrutado de un enorme crecimiento. La tecnología inalámbrica ahora llega prácticamente a todos los lugares del mundo. Miles de millones de personas intercambian información diariamente con productos de comunicación inalámbrica. La serie Vigor2927 de enrutadores inalámbricos (con "n", "n-plus" o "ac" en el nombre del modelo), diseñada teniendo en cuenta la máxima flexibilidad y eficiencia, es ideal para usar en una pequeña oficina o en el hogar. En un entorno empresarial, cualquier personal autorizado puede traer una tableta, PDA o computadora portátil equipada con WLAN a una sala de reuniones y conectarse a la red sin taladrar las paredes o romper el piso para tender un trozo de cableado LAN. Las redes inalámbricas permiten una alta movilidad para que los usuarios de WLAN puedan acceder a todos los recursos de LAN de la misma manera que lo harían en una LAN con cable, pero sin cables.

Todos los enrutadores inalámbricos Vigor2927 admiten 2,4 GHz. Los modelos ac agregan soporte para frecuencias de 5 GHz. Las operaciones de canal de 20 y 40 MHz son posibles en el espectro de 2,4 GHz, y las de 20, 40 y 80 MHz son compatibles con el espectro de 5 GHz. Los modelos “ac” (2865ac) admiten velocidades de datos de hasta 1,3 Gbps en canales 802.11ac de 80 MHz, mientras que los modelos “n” admiten velocidades de datos de hasta 300 Mbps en canales 802.11n de 40 MHz.

Información

El rendimiento real de los datos variará según las condiciones de la red y los factores ambientales, incluidos el volumen de tráfico de la red, la sobrecarga de la red y los materiales de construcción.

En un modo de infraestructura de red inalámbrica, el enrutador inalámbrico Vigor desempeña un papel como un punto de acceso (AP) que se conecta a muchos clientes inalámbricos o estaciones (STA). Todas las STA compartirán la misma conexión a Internet a través del enrutador inalámbrico Vigor. La configuración de la red inalámbrica, como SSID, canales, protocolo de cifrado, se puede configurar en Configuración general.



Múltiples SSID

Los enrutadores inalámbricos Vigor admiten hasta cuatro SSID (identificadores de conjunto de servicios) por banda para conexiones inalámbricas. Un conjunto de servicios es un grupo de clientes de red inalámbrica que tienen el mismo

parámetros de red. Cada conjunto de servicios puede configurarse para tener un nombre único (SSID) y tasas específicas de carga y descarga, y puede ser utilizado por diferentes categorías de usuarios.

Cifrado de hardware en tiempo real

Los enrutadores inalámbricos Vigor están equipados con un motor de cifrado AES de hardware para brindar la protección más eficaz y eficiente del tráfico inalámbrico, sin sacrificar la experiencia del usuario.

Selección completa de estándares de seguridad

Para garantizar la seguridad y privacidad de su comunicación inalámbrica, ofrecemos varios estándares vigentes en el mercado.

WEP (Privacidad equivalente por cable) es un método heredado para cifrar cada cuadro transmitido por radio utilizando una clave de 64 bits o de 128 bits. Por lo general, el punto de acceso preestablecerá un conjunto de cuatro teclas y se comunicará con cada estación usando solo una de las cuatro teclas.

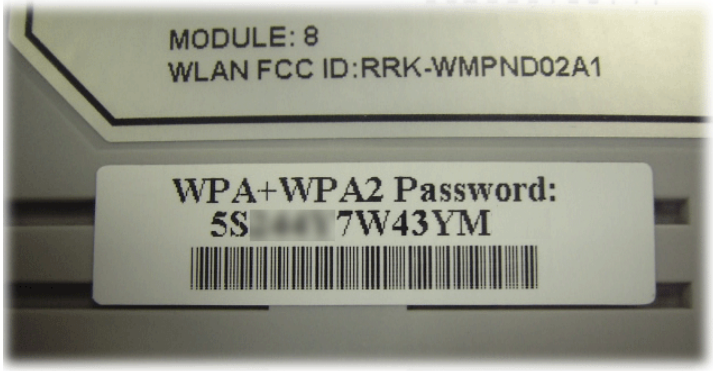
WPA (Wi-Fi Protected Access), el mecanismo de seguridad más dominante en la industria, se divide en dos categorías: WPA-personal o WPA Pre-Share Key (WPA/PSK) y WPA-Enterprise o WPA/802.1x.

En WPA-Personal, se utiliza una clave predefinida (PSK) para cifrar el tráfico durante la transmisión de datos. WPA utiliza el Protocolo de integridad de clave temporal (TKIP) para el cifrado de datos, mientras que WPA2 aplica AES (Estándar de cifrado avanzado). Una gran ventaja de WPA-Enterprise es que admite no solo el cifrado sino también la autenticación.

Debe seleccionar el mecanismo de seguridad apropiado según sus necesidades. Debido a que se ha demostrado que WEP es vulnerable a los ataques, debería considerar usar WPA en su lugar para obtener la conexión más segura. Independientemente del paquete de seguridad que seleccione, todos mejorarán la protección de datos por aire y/o la privacidad en su red inalámbrica. El enrutador inalámbrico Vigor es muy flexible y puede admitir múltiples conexiones seguras con WEP y WPA al mismo tiempo.

Información

La contraseña predeterminada (PSK) se encuentra en una etiqueta pegada en la parte inferior del enrutador. Dado que cualquiera que tenga acceso físico al enrutador puede descubrir la contraseña predeterminada, se recomienda encarecidamente que la cambie.



Separe la LAN inalámbrica y la cableada - Aislamiento de WLAN

El aislamiento de WLAN le permite separar los clientes de LAN inalámbrica de los cableados, ya sea con el fin de poner en cuarentena a ciertos usuarios o restringir su acceso a los recursos de LAN. Cuando el aislamiento de WLAN está habilitado en un SSID, sus usuarios solo podrán conectarse a la WAN (es decir, Internet). Esto es ideal para proporcionar a los visitantes acceso a Internet mientras se mantiene segura la red cableada.

Para obtener el mayor grado de seguridad, puede considerar agregar reglas de firewall para filtrar el acceso por dirección MAC.

Todas las estaciones en la red inalámbrica y su estado de conexión se muestran aquí.

Restricciones de DFS

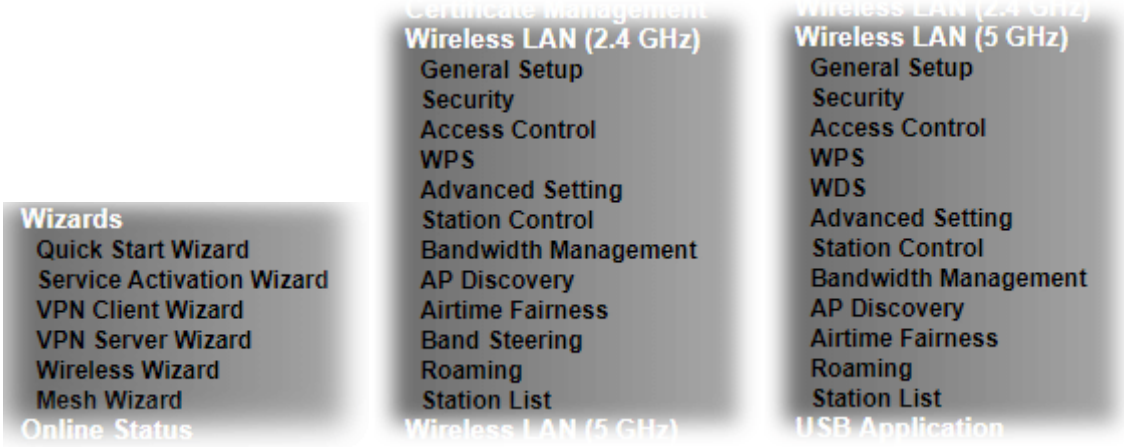
En ciertas partes del mundo, existen sistemas de radar que son los principales usuarios de la banda de 5 GHz. Los equipos WLAN en la banda de 5 GHz se consideran usuarios secundarios y no deben causar interferencias a los usuarios principales. Al utilizar una función llamada Selección de frecuencia dinámica, el enrutador inalámbrico detecta la presencia de señales de radar y reubica la red inalámbrica en un canal despejado. Los canales DFS varían según la región y debemos obtener la certificación de las autoridades antes de que estén disponibles para su uso en el enrutador Vigor. Estamos trabajando en la certificación DFS en Europa y abriremos esos canales lanzando un nuevo firmware una vez que pasemos la certificación. En Europa, estos canales DFS estarán disponibles 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 y 140.

En este momento, no tenemos planes de obtener la certificación DFS en los EE. UU., por lo que los canales DFS no estarán disponibles en un futuro previsible. Los canales DFS de EE. UU. 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 y 140 no estarán disponibles en los enrutadores vendidos en los Estados Unidos.

En el resto del mundo, también existen restricciones en los canales DFS. Los canales DFS no certificados no estarán disponibles para su selección según el código de país programado en el enrutador.

WPS

WPS (Configuración Wi-Fi Protegida)hace que la conexión de clientes inalámbricos a puntos de acceso y enrutadores inalámbricos sea un proceso simple.



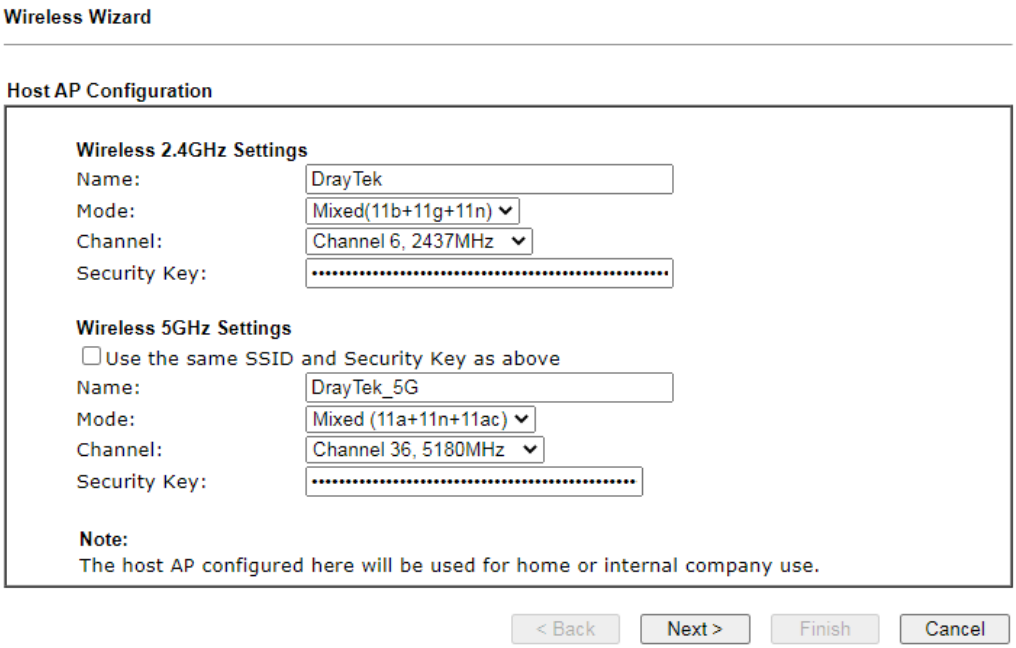
Asistente inalámbrico III-1-1

En los modelos equipados con Wi-Fi, puede configurar el punto de acceso inalámbrico (AP) utilizando el asistente inalámbrico. La Configuración del AP Anfitrión configura el SSID 1 para que lo usen los usuarios internos, a quienes se les permite acceder tanto a la LAN como a la WAN (Internet), mientras que la Configuración del AP Invitado configura el SSID 2 para que lo usen los visitantes, a quienes solo se les permite el acceso a la WAN y cuyas velocidades de acceso se pueden limitar opcionalmente.

El asistente inalámbrico le permite configurar rápidamente un SSID de host (para uso interno, como en un entorno doméstico o empresarial) y, opcionalmente, un SSID de invitado (para clientes inalámbricos que están restringidos al acceso a Internet únicamente, generalmente utilizados por los visitantes).

Siga los pasos que se enumeran a continuación:

1. En la barra de menú, haga clic en**magos**, y luego**Asistente inalámbrico**.
2. Aparecerá la página de configuración del punto de acceso del host. Esta página configura el SSID 1 para que lo usen los usuarios internos. El SSID 1 configurado mediante el asistente no tendrá limitación de la velocidad de acceso (por medio de la función Rate Control), y tanto la LAN como la WAN serán accesibles.



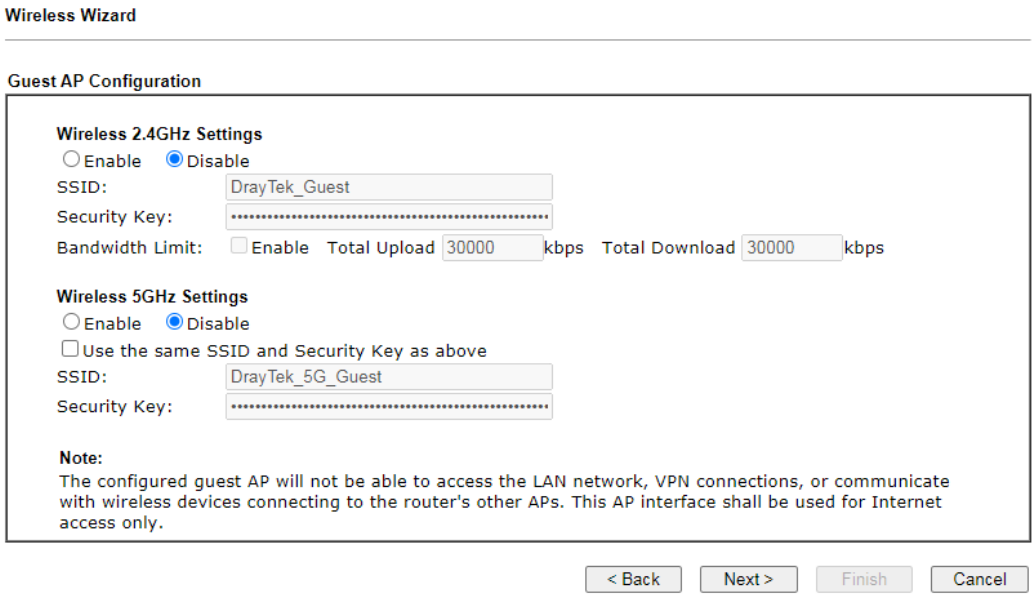
Los ajustes disponibles se explican a continuación:

Configurable por el usuario **Artículo**	**Descripción**
Configuración inalámbrica de 2,4 GHz	
Nombre	Identificación de conjunto de servicios (SSID), que aparece como el identificador de AP. La longitud máxima es de 32 caracteres.
Modo	Modos Wi-Fi permitidos. 802.11b es el modo Wi-Fi original en la banda de 2,4 GHz y admite velocidades de datos sin procesar de hasta 11 Mbit/s. 802.11g permite un rendimiento mejorado de hasta 54 Mbit/s. 802.11n proporciona un rendimiento de hasta 300 MHz. Las selecciones disponibles son • 11b solamente • Solo 11g • Solo 11n (2,4 GHz) • Mixto (11b+11g) • Mixto (11g+11n) • Mixta(11b+11g+11n) Las selecciones etiquetadas como "Mixtas" permiten múltiples modos activos simultáneamente.
Canal	Canal Wi-Fi utilizado para este SSID. Si se establece en Automático, el enrutador utiliza el mejor canal disponible.
Clave de seguridad	La clave precompartida (PSK) utilizada por WPA2/PSK (acceso protegido inalámbrico 2/clave precompartida) para cifrar el tráfico inalámbrico. La clave se compone de 8 a 63 caracteres ASCII. También puede especificar la clave utilizando 64 dígitos hexadecimales, con el prefijo 0x ("0x321253abcde...").
Configuración inalámbrica de 5 GHz	
Use el mismo SSID y clave de seguridad que el anterior	Si se selecciona, se usarán el nombre SSID y la clave de seguridad de la sección de 2,4 GHz.

Nombre	Identificación de conjunto de servicios (SSID), que aparece como el identificador de AP. La longitud máxima es de 32 caracteres.
Modo	Modos Wi-Fi permitidos. 802.11a es el modo Wi-Fi original en la banda de 5 GHz y admite velocidades de datos sin procesar de hasta 11 Mbit/s. 802.11n mejora el rendimiento y proporciona hasta 300 MHz. El estándar más reciente, 802.11ac, puede lograr un rendimiento de datos de 1,3 Gbit/s en la banda de 5 GHz. Las selecciones disponibles son • Solo 11a • Solo 11n (5 GHz) • Mixta(11a+11n) • Mixto (11a+11n+11ac) Las selecciones etiquetadas como "Mixtas" permiten múltiples modos activos simultáneamente.
Canal	Canal Wi-Fi utilizado para este SSID. Si se establece en Automático, el enrutador utiliza el mejor canal disponible.
Clave de seguridad	La clave precompartida (PSK) utilizada por WPA2/PSK (acceso protegido inalámbrico 2/clave precompartida) para cifrar el tráfico inalámbrico. La clave se compone de 8 a 63 caracteres ASCII. También puede especificar la clave utilizando 64 dígitos hexadecimales, con el prefijo 0x ("0x321253abcde...").
Próximo	Haga clic en él para acceder a la siguiente página de configuración.
Cancelar	Salga del asistente inalámbrico sin guardar ningún cambio.

3. Haga clic en**Próximo**para proceder a la página de configuración de AP invitado. Aparece la página Configuración de AP invitado. Esta página configura el SSID 2 para que lo usen los usuarios invitados. El SSID 2 configurado mediante el asistente se puede configurar opcionalmente con aceleración de la velocidad de acceso (por medio de la función Rate Control), y solo se podrá acceder a la WAN (Internet).

   El SSID 2 comparte la misma configuración de modo y canal que el SSID 1 configurado en la página anterior.



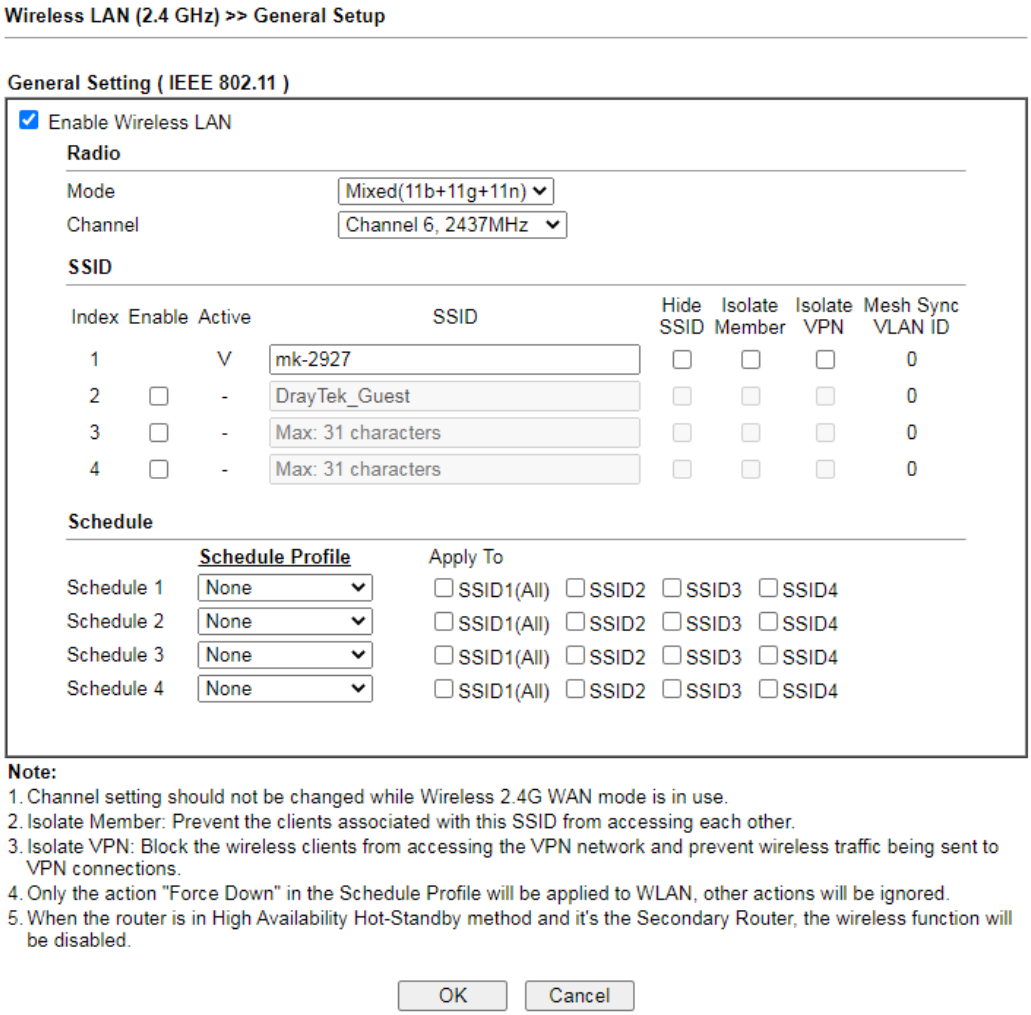
   Los ajustes disponibles se explican a continuación:

Configurable por el usuario Artículo	**Descripción**
Configuración inalámbrica de 2,4 GHz	
Habilitar deshabilitar	Habilite o deshabilite el SSID para uso de invitados.
SSID	Identificación de conjunto de servicios (SSID), que aparece como el identificador de AP. La longitud máxima es de 32 caracteres.
Clave de seguridad	La clave precompartida (PSK) utilizada por WPA2/PSK (acceso protegido inalámbrico 2/clave precompartida) para cifrar el tráfico inalámbrico. La clave se compone de 8 a 63 caracteres ASCII. También puede especificar la clave utilizando 64 dígitos hexadecimales, con el prefijo 0x ("0x321253abcde...").
Límite de ancho de banda	**Permitir**–Marque la casilla para establecer el límite de ancho de banda para la transmisión de datos en carga y descarga. Controla la tasa de transmisión de datos a través de la conexión inalámbrica. **Carga total**–Marque Habilitar e ingrese la velocidad de transmisión para la carga de datos. El valor predeterminado es 30.000 kbps. **Descarga total**–Introduzca la velocidad de transmisión para la descarga de datos. El valor predeterminado es 30.000 kbps.
Configuración inalámbrica de 5 GHz	
Habilitar deshabilitar	Haga clic para habilitar o deshabilitar la configuración en esta página.
Use el mismo SSID y clave de seguridad que el anterior	Si se selecciona, se usarán el nombre SSID y la clave de seguridad de la sección de 2,4 GHz.
SSID	Identificación de conjunto de servicios (SSID), que aparece como el identificador de AP. La longitud máxima es de 32 caracteres.
Clave de seguridad	La clave precompartida (PSK) utilizada por WPA2/PSK (acceso protegido inalámbrico 2/clave precompartida) para cifrar el tráfico inalámbrico. La clave se compone de 8 a 63 caracteres ASCII. También puede especificar la clave utilizando 64 dígitos hexadecimales, con el prefijo 0x ("0x321253abcde...").
Próximo	Haga clic en él para acceder a la siguiente página de configuración.
Cancelar	Salga del asistente inalámbrico sin guardar ningún cambio.

4. Haga clic en**Próximo**para pasar a la página Resumen de configuración.

5. El**Resumen de configuración**La página muestra todas las configuraciones que ha ingresado. Hacer clic**Finalizar** para guardar la configuración,**Atrás**para hacer cambios, o**Cancelar**para salir del asistente sin guardar la configuración.

El**LAN inalámbrica>>Configuración general**La sección le permite configurar los ajustes más básicos de su red inalámbrica, incluidos los SSID, los canales WLAN y el control de ancho de banda.



Los ajustes disponibles se explican a continuación:

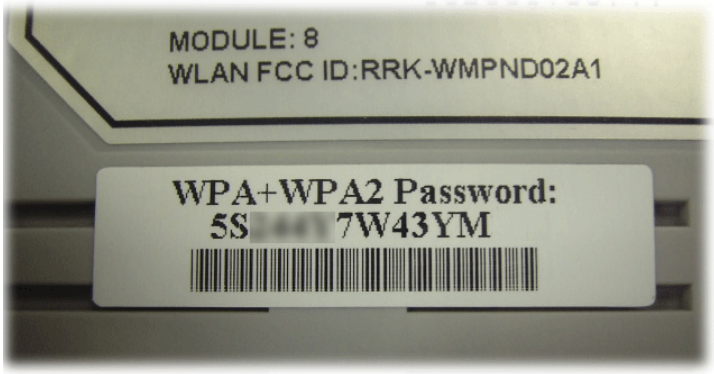
Artículo	Descripción
Habilitar LAN inalámbrica	Marque la casilla para habilitar la función inalámbrica.
Radio	
Modo	Seleccione el modo 802.11 permitido en la banda. En la banda de 2,4 GHz, están disponibles las siguientes opciones de modo inalámbrico: • 11b solamente • Solo 11g • Solo 11n (2,4 GHz) • Mixto (11b+11g) • Mixto (11g+11n) • Mixto (11b+11g+11n) En la banda de 5 GHz en modelos de CA (p. ej., 2927ac), están disponibles las siguientes opciones: • Solo 11a

	• Solo 11n (5 GHz) • Mixto (11a+11n) • Mixto (11a+11n+11ac)
Canal	Le permite especificar un canal inalámbrico en particular para usar, o dejar que el sistema determine el canal óptimo seleccionando "**Auto**". La lista de canales disponibles varía según la configuración regional a la que está destinado el enrutador.
SSID	
SSID	Identificación de conjunto de servicios (SSID), que aparece como el identificador de AP. La longitud máxima es de 32 caracteres.
Ocultar SSID	Seleccione para evitar que los SSID se muestren cuando los clientes inalámbricos realizan exploraciones, lo que dificulta que los clientes no autorizados o las STA se unan a su LAN inalámbrica. Según el cliente inalámbrico y el software utilizado, el usuario puede ver solo un AP en la lista sin el SSID, o es posible que el AP ni siquiera aparezca.
Aislar	**Miembro**–Marque esta casilla para no permitir la comunicación entre clientes inalámbricos (estaciones) en el mismo SSID. **vpn**–Marque esta casilla para bloquear el acceso de los clientes inalámbricos (estaciones) a los clientes VPN.
ID de VLAN de sincronización de malla	Muestre la ID de VLAN, que sincronizará la copia con el nodo de malla utilizando el mismo SSID.
Cronograma	
Programar perfil	Configure la LAN inalámbrica para que se deshabilite en ciertos intervalos de tiempo. Puede elegir hasta 4 horarios de los 15 horarios definidos en **Aplicaciones >> Horario**. Solo los perfiles de programación "Forzar abajo" tienen efecto, y la función inalámbrica se apagará durante la duración del perfil. La configuración predeterminada está en blanco para todos los horarios, lo que significa que la función inalámbrica siempre funcionará.
Aplicar para	El SSID seleccionado (2/3/4) se verá forzado hacia arriba/abajo según el perfil de programación utilizado. **Schedule** Schedule Profile / Apply To Schedule 1 None ☑ SSID1(All) ☑ SSID2 ☑ SSID3 ☑ SSID4 Schedule 2 None ☑ SSID1(All) ☑ SSID2 ☑ SSID3 ☑ SSID4 Schedule 3 None ☑ SSID1(All) ☑ SSID2 ☑ SSID3 ☑ SSID4 Schedule 4 None ☑ SSID1(All) ☑ SSID2 ☑ SSID3 ☑ SSID4

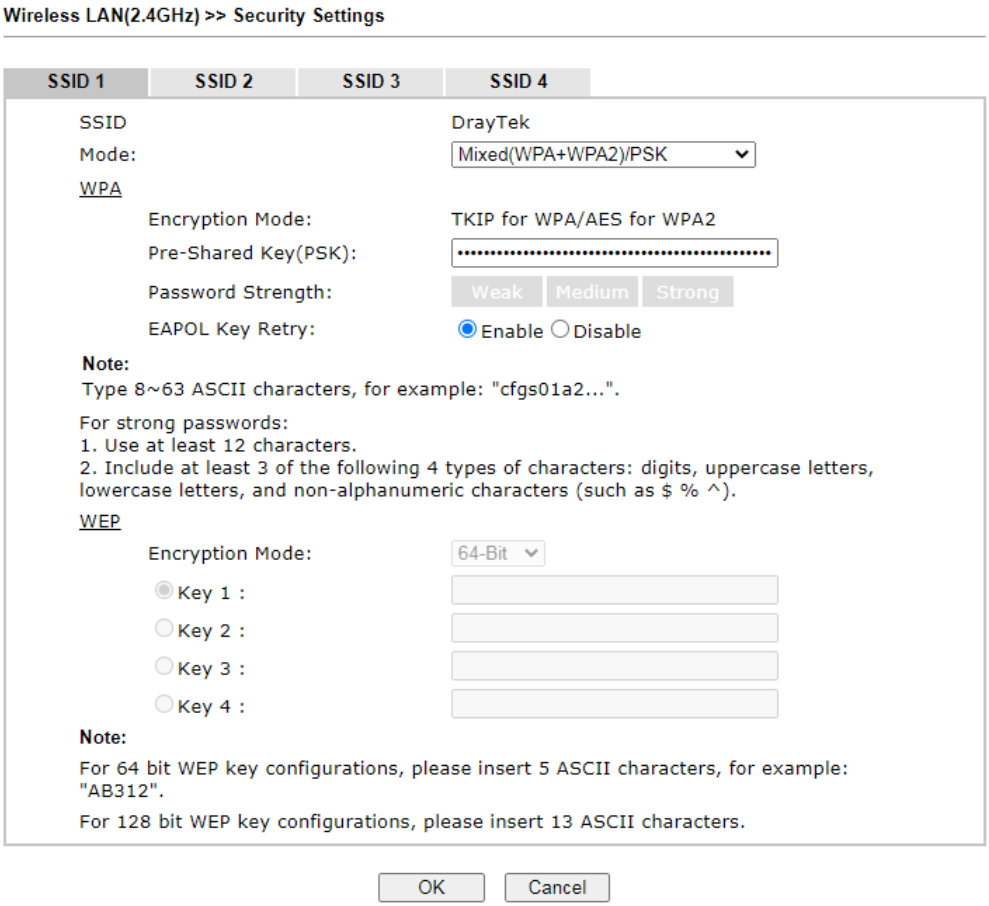
Para guardar los cambios en la página Configuración general, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**.

III-1-3 Seguridad

Cada enrutador tiene una contraseña inalámbrica predeterminada (PSK) que se proporciona en una etiqueta pegada en la parte inferior del enrutador. Para el cliente inalámbrico que desea acceder a Internet a través de dicho enrutador, ingrese el valor PSK predeterminado para la conexión.



Para mayor seguridad, puede establecer su propia contraseña inalámbrica haciendo clic en el**LAN inalámbrica>>Configuración de seguridad**entrada en la interfaz de usuario web. Cada uno de los 4 SSID se puede configurar de forma independiente utilizando su propia página de pestañas.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Modo	Este cuadro de diálogo enumera todos los modos de seguridad disponibles.

	Información: También debe establecer **Configuración de LAN inalámbrica (2,4 GHz) 802.1X** simultáneamente si se selecciona el modo 802.1x. **Desactivar**–El mecanismo de cifrado está deshabilitado. **WEP**–Permitir únicamente conexiones de clientes WEP. La clave de cifrado debe ingresarse en la sección Clave WEP. **Solo WEP/802.1x -**Acepta solo clientes WEP y la clave de cifrado se obtiene dinámicamente del servidor RADIUS con protocolo 802.1X. Permitir únicamente conexiones de clientes WEP. La clave de cifrado se obtiene de un servidor RADIUS utilizando el protocolo 802.1X. **Solo WPA/802.1x -**Permitir solo conexiones de clientes WPA. La clave de cifrado se obtiene de un servidor RADIUS utilizando el protocolo 802.1X. **Solo WPA2/802.1x-**Permitir solo conexiones de clientes WPA2. La clave de cifrado se obtiene de un servidor RADIUS utilizando el protocolo 802.1X. **Mixto (solo WPA+WPA2/802.1x) -**Permitir conexiones desde clientes WPA y WPA2. La clave de cifrado se obtiene de un servidor RADIUS utilizando el protocolo 802.1X. **PSK WPA -**Permitir conexiones solo desde clientes WPA. La clave de cifrado debe ingresarse en el campo PSK. **WPA2/PSK-**Permitir conexiones solo desde clientes WPA2. La clave de cifrado debe ingresarse en el campo PSK. **Mixto (WPA+ WPA2)/PSK -**Permitir conexiones desde clientes WPA y WPA2. La clave de cifrado debe ingresarse en el campo PSK. **WPA3/SAE-**Permitir conexiones solo desde clientes WPA3. La clave de cifrado debe ingresarse en el campo PSK. **Mixto (WPA2+ WPA3)/SAE -**Permitir conexiones desde clientes WPA2 y WPA3. La clave de cifrado debe ingresarse en el campo PSK. **DEBER**-WPA3 también presenta un nuevo modo de conexión abierta y segura; "Cifrado inalámbrico oportunista" (OWE). Permite que los clientes se conecten sin contraseña, lo que es ideal para redes de puntos de acceso, pero la conexión entre cada cliente individual está encriptada de forma única detrás de escena.
WPA	WPA encripta cada cuadro transmitido desde la radio utilizando la clave, que se ingresa en el campo PSK (clave precompartida) o se negocia automáticamente a través de 802.1x autenticación desde un servidor RADIUS. **Clave precompartida (PSK)**-Introduzca de 8 a 63 caracteres ASCII, por ejemplo, “012345678..”, o 64 dígitos hexadecimales con un “0x” inicial, por ejemplo, "0x321253abcde...". **seguridad de la contraseña**–El sistema mostrará la seguridad de la contraseña, indicada por las palabras "débil", "media" o "fuerte". **Reintento de clave EAPOL**-La configuración predeterminada es "Habilitar". Puede asegurarse de que la clave se instalará y usará una vez para evitar un ataque de reinstalación de clave.
WEP	Las claves WEP pueden ser de 64 bits o de 128 bits. **64 bits**-5 caracteres ASCII, por ejemplo, "12345", o 10 dígitos hexadecimales con un "0x" inicial, como

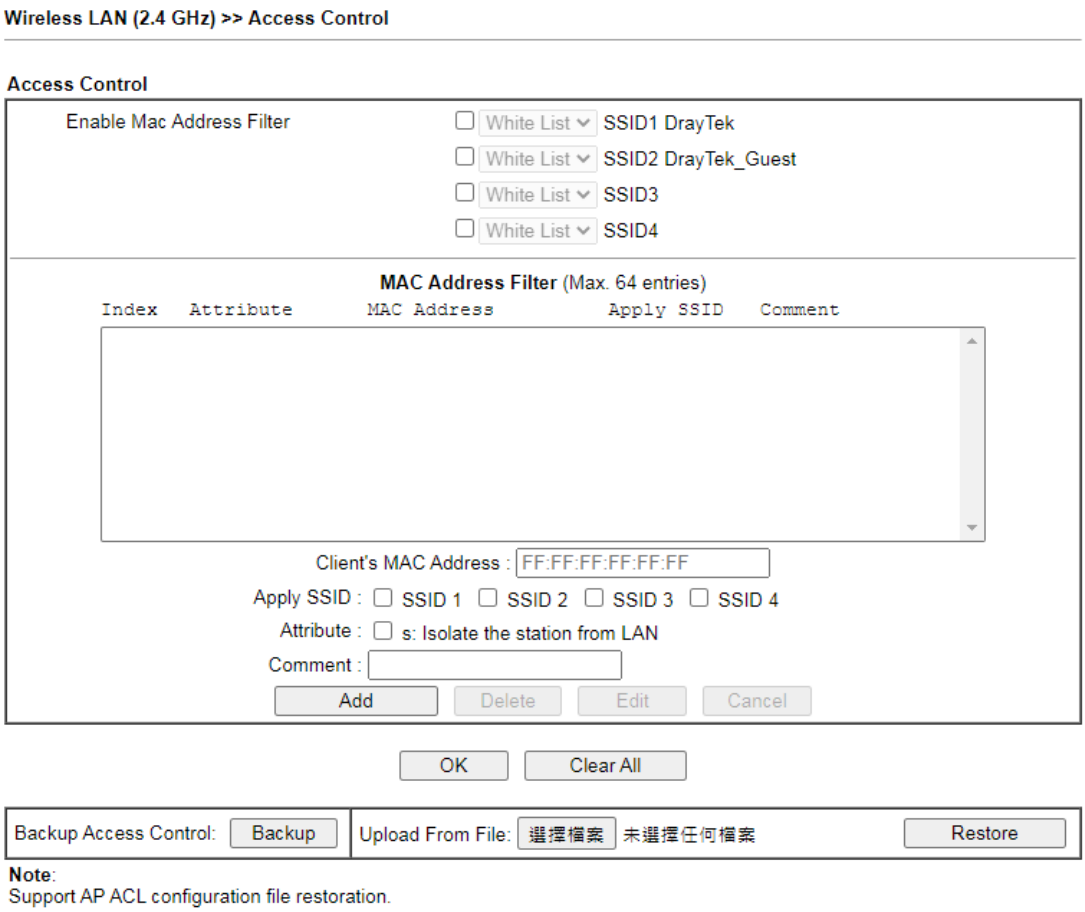
	“0x4142434445”. **128 bits**-13 caracteres ASCII, por ejemplo, "ABCDEFGHIJKLM", o 26 dígitos hexadecimales con un "0x" inicial, por ejemplo, "0x41424344454647484 94A4B4C4D". Aquí se pueden ingresar hasta cuatro claves, pero solo se puede seleccionar una clave en cualquier momento. Las claves se pueden ingresar en ASCII o Hexadecimal. Todos los dispositivos inalámbricos que pretendan conectarse al mismo SSID deben admitir el mismo tamaño de bit de encriptación WEP y tener la misma clave.

Para guardar los cambios en esta página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**.

III-1-4 Control de acceso

En el**Control de acceso**, el enrutador puede restringir el acceso inalámbrico a ciertos clientes inalámbricos solo al hacer referencia a una lista negra o blanca de direcciones MAC. El usuario puede bloquear clientes inalámbricos insertando sus direcciones MAC en una lista negra, o solo permitir que ciertos clientes inalámbricos se conecten insertando sus direcciones MAC en una lista blanca.

En la página web de Control de Acceso, los usuarios pueden configurar el**blanco negro**modos de lista utilizados por cada SSID y las direcciones MAC aplicadas a sus listas.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar el filtro de direcciones Mac	Seleccione los SSID que le gustaría tener activado el filtro de direcciones MAC. Seleccionar**Lista blanca**o**Lista negra**en el cuadro combinado junto a cada SSID habilitado.

	Lista blanca-Solo permita clientes inalámbricos cuyas direcciones MAC se encuentren en la lista de filtros de direcciones MAC. **Lista negra**-Solo permita clientes inalámbricos cuyas direcciones MAC no estén incluidas en la lista de filtros de direcciones MAC.
Filtro de direcciones MAC	Muestra todas las direcciones MAC en la lista de filtros.
Dirección MAC del cliente	Ingrese manualmente la dirección MAC del cliente inalámbrico.
Aplicar SSID	Seleccione los SSID a los que se aplicará el filtro de dirección MAC anterior.
Atributo	**s: Aislar la estación de LAN -**seleccione para aislar el cliente inalámbrico de la LAN.
Comentario	Ingrese una breve descripción para la dirección MAC del cliente especificado.
Agregar	Agregue una nueva entrada de filtro a la lista de filtros de direcciones MAC utilizando la información ingresada anteriormente.
Borrar	Elimine la dirección MAC seleccionada de la lista.
Editar	Actualice la dirección MAC seleccionada en la lista utilizando la información ingresada anteriormente.
Cancelar	Borre el contenido de todos los campos anteriores. Esto descartará todos los cambios sin guardarlos en la lista de filtros de direcciones MAC.
DE ACUERDO	Haga clic para guardar la lista de filtros de direcciones MAC.
Limpiar todo	Elimine todas las entradas de la lista de filtros de direcciones MAC.
Control de acceso de respaldo	La configuración de esta página web se puede guardar como un archivo que se puede restaurar en el futuro con este dispositivo u otro dispositivo.
Cargar desde archivo	Restaure la configuración de control de acceso inalámbrico y aplique en este dispositivo.

Para guardar los cambios en esta página, seleccione**DE ACUERDO**.

III-1-5 WPS

WPS (Configuración Wi-Fi Protegida)proporciona una manera fácil de conectar de forma inalámbrica a puntos de acceso inalámbricos y enrutadores con encriptación WPA o WPA2.

Información

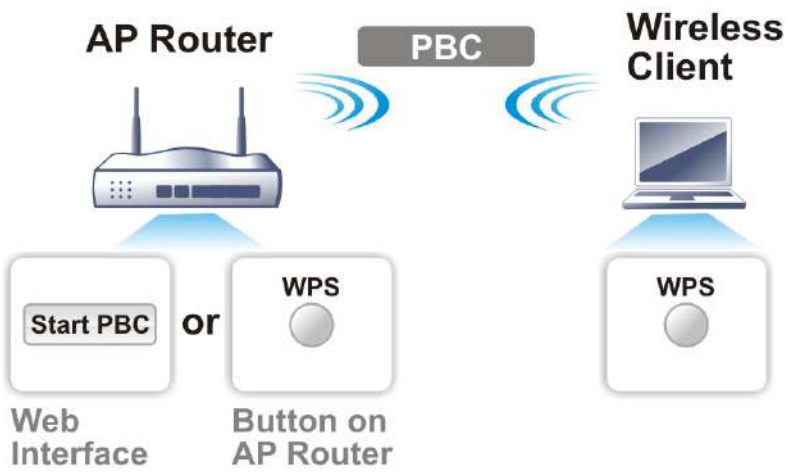
WPS funciona con estaciones inalámbricas compatibles con WPS o WPS2. No funciona con WEP.

Es la forma más sencilla de establecer una conexión entre los clientes de la red inalámbrica y el enrutador Vigor. Los usuarios no necesitan seleccionar ningún modo de encriptación ni escribir ninguna frase de contraseña de encriptación larga para configurar un cliente inalámbrico cada vez. Él / ella solo necesita presionar un botón en el cliente inalámbrico, y WPS se conectará automáticamente para el cliente y el enrutador.

Hay dos métodos para hacer conexión de red a través de WPS entre AP y Estaciones: presionando el botón***Iniciar PBC***botón o usando***Código PIN***.

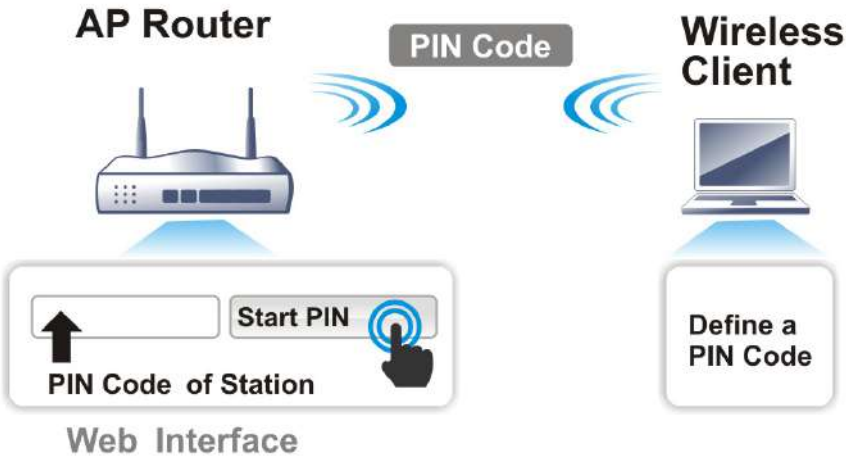
Uso del botón PBC

En el enrutador Vigor, presione y mantenga presionado el botón WPS en el panel frontal durante 2 segundos, o haga clic en el botón**Iniciar PBC**botón en el**LAN inalámbrica>>WPS**página en la interfaz de usuario web. En la estación inalámbrica (por ejemplo, una computadora portátil), presione el**WPS/Iniciar PBC**botón en la tarjeta de red.

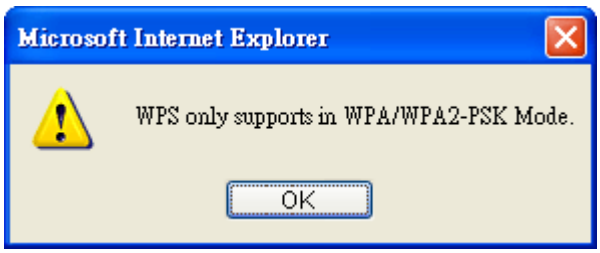


Usando un código PIN

Puede establecer una conexión inalámbrica ingresando un código PIN generado por un cliente inalámbrico compatible con WPS.

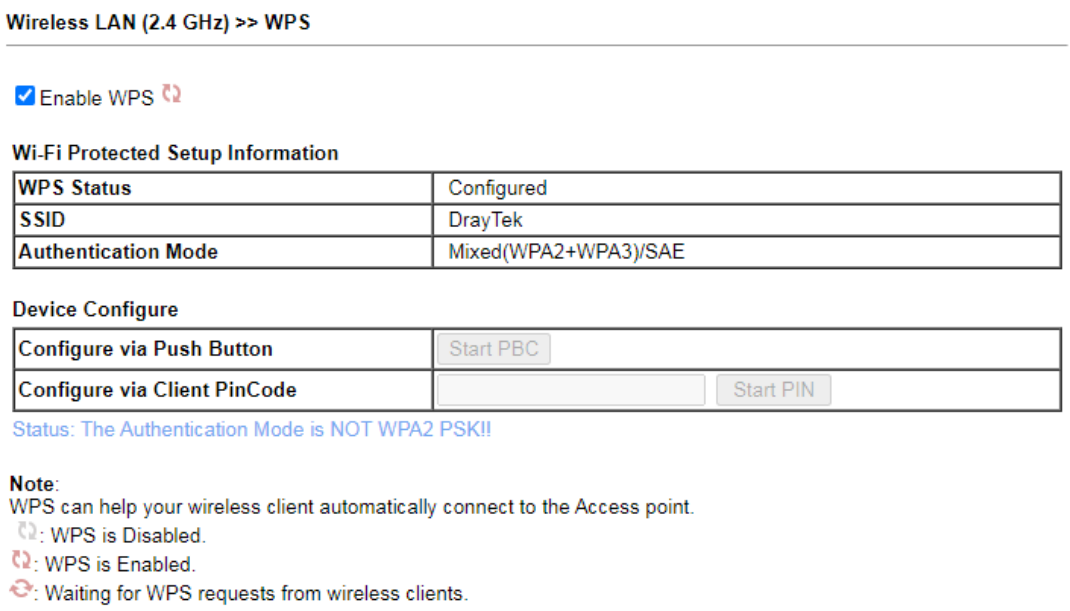


WPS solo es compatible cuando el protocolo de cifrado está configurado en WPA-PSK o WPA2-PSK. Si se han seleccionado otros protocolos (como WEP) en**LAN inalámbrica>>Seguridad**, verá el siguiente cuadro de mensaje:



Por favor haz click**DE ACUERDO**para cerrar el cuadro de diálogo, volver a**LAN inalámbrica>>Seguridad**y seleccione el modo WPA-PSK o WPA2-PSK antes de intentar habilitar WPS nuevamente.

A continuación se muestra**LAN inalámbrica>>WPS**Página web:



Los ajustes disponibles se explican a continuación:

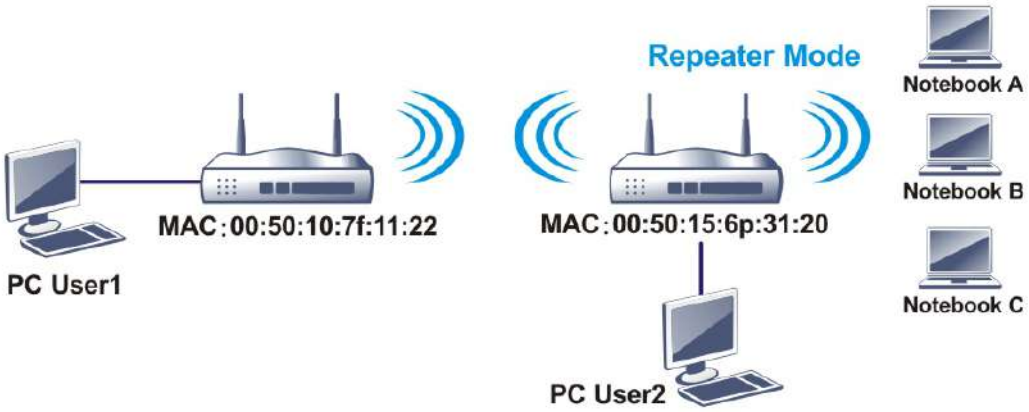
Artículo	Descripción
Habilitar WPS	Marque esta casilla para habilitar la configuración de WPS.
Estado WPS	Muestra información del sistema relacionada con WPS. El mensaje "Configurado" significa que la función de seguridad inalámbrica (cifrado) del enrutador está configurada correctamente y funciona correctamente.
SSID	Muestra el SSID1. WPS solo es compatible con SSID1.
modo de autenticación	Muestra el modo de autenticación actual del enrutador.
Configurar a través de un botón	Hacer clic**Iniciar PBC**para invocar el procedimiento de configuración de WPS estilo botón pulsador. El enrutador esperará aproximadamente 2 minutos para las solicitudes de conexión WPS de los clientes inalámbricos. El LED de WPS en el enrutador parpadeará rápidamente cuando WPS esté en progreso y volverá a su estado normal después de dos minutos.
Configurar a través del cliente Código PIN	Introduzca un código PIN y haga clic en el**PIN de inicio**botón. El LED de WPS en el enrutador parpadeará rápidamente cuando WPS esté en progreso, por hasta 2 minutos o hasta que se haya establecido una conexión WPS exitosa desde un cliente inalámbrico.

III-1-6 WDS (para 5 GHz)

El sistema de distribución inalámbrica (WDS) es un protocolo para vincular puntos de acceso (AP) de forma inalámbrica. WDS admite dos modos:

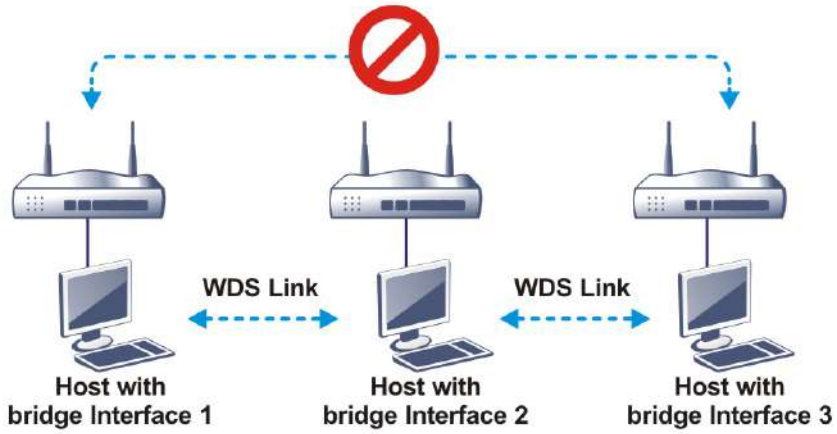
-**Modo Puente**, que une el tráfico entre dos LAN de forma inalámbrica.

-**Modo repetidor**, que amplía el rango de cobertura de una WLAN.

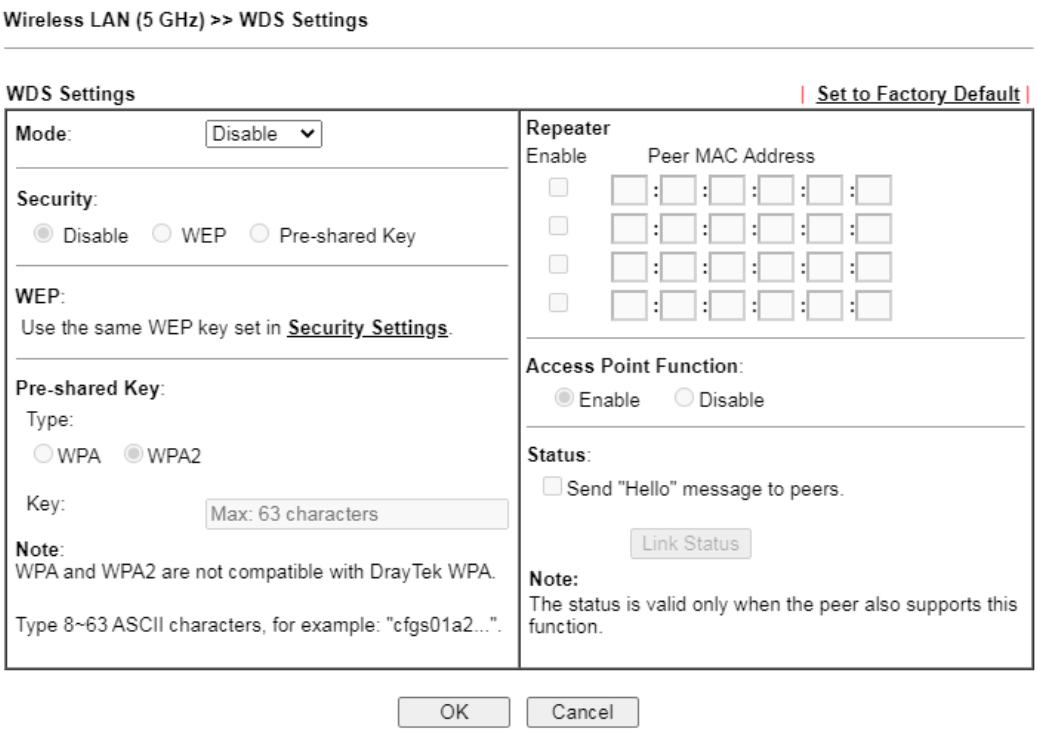


ElprincipalLa diferencia entre estos dos modos es que, en**Reloj de repetición**modo, los paquetes recibidos de un par AP se pueden repetir a otro par AP a través de enlaces WDS, mientras que en **Puente**modo, los paquetes recibidos de un enlace WDS solo se reenviarán a los hosts inalámbricos o cableados locales. En otras palabras, solo el modo repetidor puede hacer el reenvío de paquetes de WDS a WDS.

En el siguiente ejemplo, los hosts conectados al Puente 1 o 3 pueden comunicarse con los hosts conectados al Puente 2 a través de enlaces WDS. Sin embargo, los hosts conectados al Puente 1 no pueden comunicarse con los hosts conectados al Puente 3 a través del Puente 2.



Hacer clic**WDS**de**LAN inalámbrico**menú. Se mostrará la siguiente página.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Modo	Elija el modo WDS. **Desactivar**– WDS está deshabilitado. **Reloj de repetición**–WDS está habilitado en modo repetidor.
Seguridad	Elija uno de los tipos para el enrutador. La configuración que elija aquí hará que el siguiente campo de clave precompartida o WEP sea válido o no. **Desactivar**–La seguridad está desactivada. **WEP**-La seguridad está habilitada. **Clave precompartida**–La seguridad está habilitada.
Clave previamente compartida	**Tipo**–Seleccione WPA o WPA2 como protocolo de cifrado. **Llave**–Ingrese 8 ~ 63 caracteres ASCII o 64 dígitos hexadecimales con un “0x” inicial.
Reloj de repetición	Si se seleccionó Repetidor como el modo WDS, ingrese las direcciones MAC de pares en estos campos. En esta página se pueden ingresar hasta cuatro direcciones MAC de pares. Seleccione la casilla de verificación frente a una dirección MAC para habilitarla.
Función de punto de acceso	Seleccionar**Permitir**hacer que este enrutador sirva como punto de acceso; seleccionar **Desactivar**para deshabilitar la función de punto de acceso.
Estado	Haga clic para enviar un mensaje de "hola" a sus compañeros. Esto solo funciona si el compañero también admite esta función.

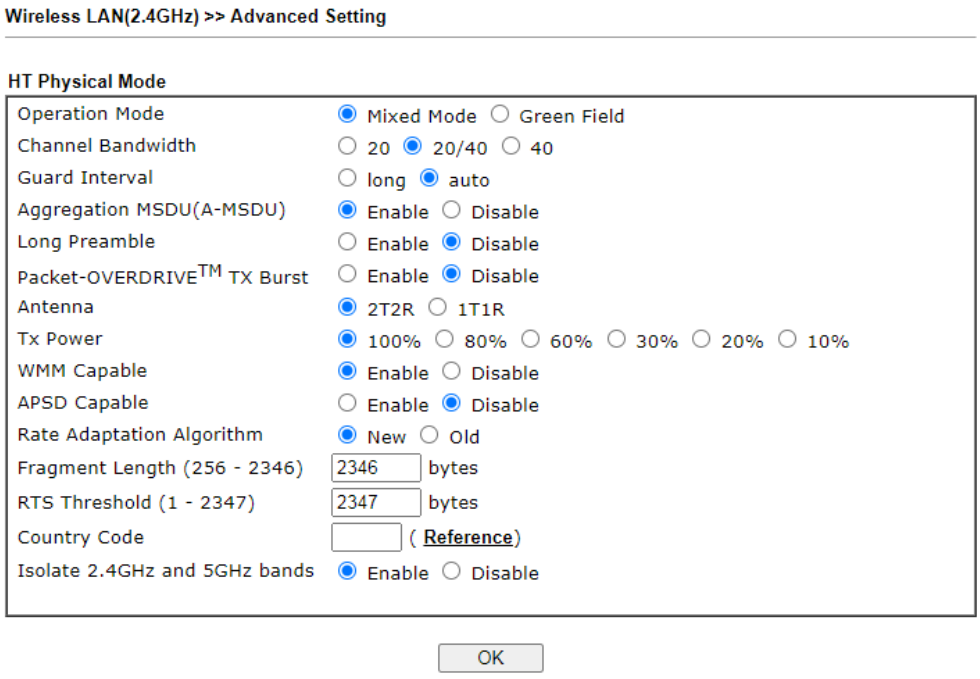
Para guardar los cambios en esta página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**.

III-1-7 Configuración avanzada

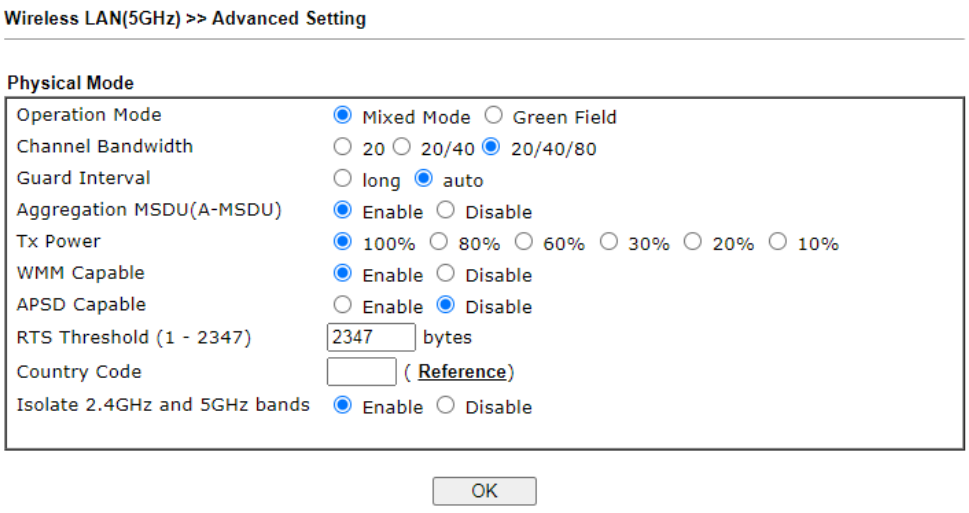
En esta página, puede configurar ajustes avanzados como el modo de operación, el ancho de banda del canal, el intervalo de protección y la MSDU de agregación para la transmisión inalámbrica de datos.

Si el enrutador Vigor es compatible con WLAN de doble banda, verá secciones de Configuración avanzada separadas para 2,4 GHz y 5 GHz.

Página de configuración avanzada de 2,4 GHz



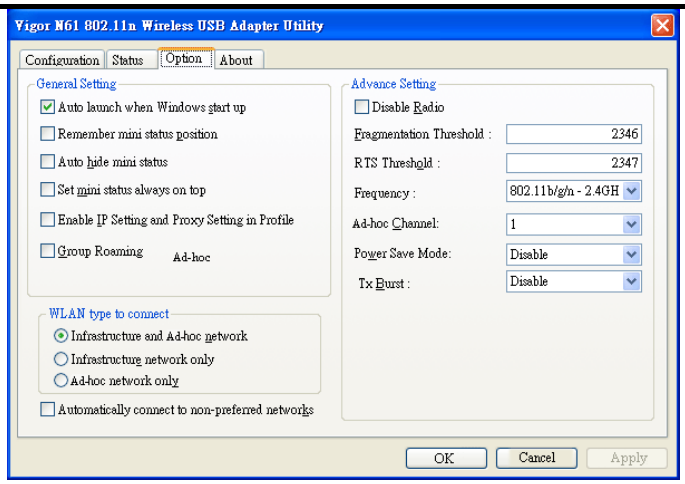
Página de configuración avanzada de 5 GHz:



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Modo de operación	**Modo mezclado**–El enrutador puede transmitir datos utilizando todos los protocolos admitidos por los estándares 802.11a/b/g y 802.11n. Sin embargo, todas las transmisiones inalámbricas se ralentizarán.

	cuando cualquier cliente inalámbrico 802.11go 802.11b está conectado. **campo verde**–Seleccione este modo para lograr el mayor rendimiento. Este modo solo admite la transmisión de datos entre sistemas 802.11n. Además, no tiene mecanismo de protección para evitar conflictos con dispositivos vecinos 802.11a/b/g.
Canal de Banda ancha	**20**–Vigor Router utilizará canales de 20 MHz para la transmisión y recepción de datos entre el AP y las estaciones inalámbricas. **40**–Vigor Router utilizará 40 MHz para la transmisión y recepción de datos entre el AP y las estaciones inalámbricas. **20/40**–Vigor Router utilizará 20 MHz o 40 MHz para la transmisión y recepción de datos dependiendo de la cantidad de puntos de acceso inalámbricos cercanos. Se utilizarán 20 MHz cuando haya más de 10 puntos de acceso inalámbricos; de lo contrario, se utilizarán 40 MHz. La selección de esta configuración garantiza el mejor rendimiento para el tránsito de datos en redes con clientes de 20 MHz y 40 MHz.
Intervalo de guardia	Habilitar esta configuración garantiza la integridad del tráfico inalámbrico mediante la inserción de intervalos de protección entre los símbolos para reducir los efectos adversos de los retrasos en la propagación y las rutas múltiples o los reflejos de la señal. Si elige automático como intervalo de vigilancia, el enrutador elegirá un intervalo de vigilancia corto (lo que aumenta el rendimiento inalámbrico) o un intervalo de vigilancia largo para la transmisión de datos, según la capacidad de la estación.
MSDU de agregación (A-MSDU)	Agregación MSDU puede combinar marcos de diferentes tamaños para mejorar el rendimiento en la capa MAC para clientes de ciertos fabricantes. La configuración predeterminada es**Permitir**.
largo preámbulo	Esta opción determina la longitud del campo de sincronización en un paquete 802.11. La mayoría de las redes inalámbricas modernas utilizan un preámbulo corto con campos de sincronización de 56 bits que producen mejores velocidades de transmisión. Sin embargo, algunos dispositivos inalámbricos 802.11b más antiguos solo admiten un preámbulo largo que utiliza campos de sincronización de 128 bits. Hacer clic**Permitir** utilizar Preámbulo largo para mantener la compatibilidad con estos dispositivos.
Paquete-OVERDRIVE	Esta función puede mejorar el rendimiento de la transmisión de datos en aproximadamente un 40 %* (al comprobar**Ráfaga de transmisión**). Está activo solo cuando tanto el punto de acceso como la estación (en el cliente inalámbrico) admiten e invocan esta función al mismo tiempo. **Nota:**El adaptador inalámbrico Vigor N61 admite esta función. Por lo tanto, puede instalarlo en su PC para aprovechar Packet-OVERDRIVE (consulte la siguiente imagen de la ventana de la utilidad inalámbrica Vigor N61: elija Habilitar para TxBURST en la**Opción** pestaña).

	 **Información** * La tasa de transmisión real depende del entorno de la red.
Antena	El enrutador Vigor se puede conectar con dos antenas para tener una buena transmisión de datos a través de una conexión inalámbrica. Sin embargo, si solo tiene una antena conectada, elija 1T1R.
Poder TX	Establece el porcentaje de potencia de la señal de transmisión del punto de acceso. Cuanto mayor sea el valor de TX Power, mayor será la intensidad de la señal.
Compatible con WMM	WMM significa Wi-Fi Multimedia. Proporciona calidad de servicio (QoS) básica al priorizar el tráfico en función de cuatro categorías de acceso definidas en el estándar IEEE 802.11e. Las categorías de acceso son AC_VO, AC_VI, AC_BE y AC_BK, que corresponden a los tipos de tráfico de voz, video, mejor esfuerzo y datos de baja prioridad (de fondo), respectivamente. Para aplicar parámetros WMM a la transmisión inalámbrica de datos, haga clic en el**Permitir**boton de radio.
Compatible con APSD	APSD (Automatic Power-Save Delivery) es una mejora sobre los mecanismos de ahorro de energía compatibles con las redes Wi-Fi. Permite que los puntos de acceso almacenen el tráfico antes de transmitirlo a los dispositivos inalámbricos, lo que permite que los dispositivos inalámbricos entren en modo de ahorro de energía, lo que reduce el consumo de energía. No todos los clientes inalámbricos admiten APSD correctamente, y la única forma de averiguar si APSD es apropiado para su red es experimentar. La configuración predeterminada es**Desactivar**.
Algoritmo de adaptación de velocidad	Establece la forma en que la tasa de transmisión inalámbrica se ajusta dinámicamente. En la mayoría de los casos, seleccionar "Nuevo" dará como resultado un mejor rendimiento que "Antiguo".
Longitud del fragmento (256 – 2346)	Establezca el umbral de Fragmento. Se recomienda dejar intacto el valor predeterminado, 2346.
Umbral RTS (1 – 2347)	Minimice la colisión (la unidad es bytes) entre estaciones ocultas para mejorar el rendimiento inalámbrico. Establezca el umbral de RTS. No modifique el valor predeterminado si

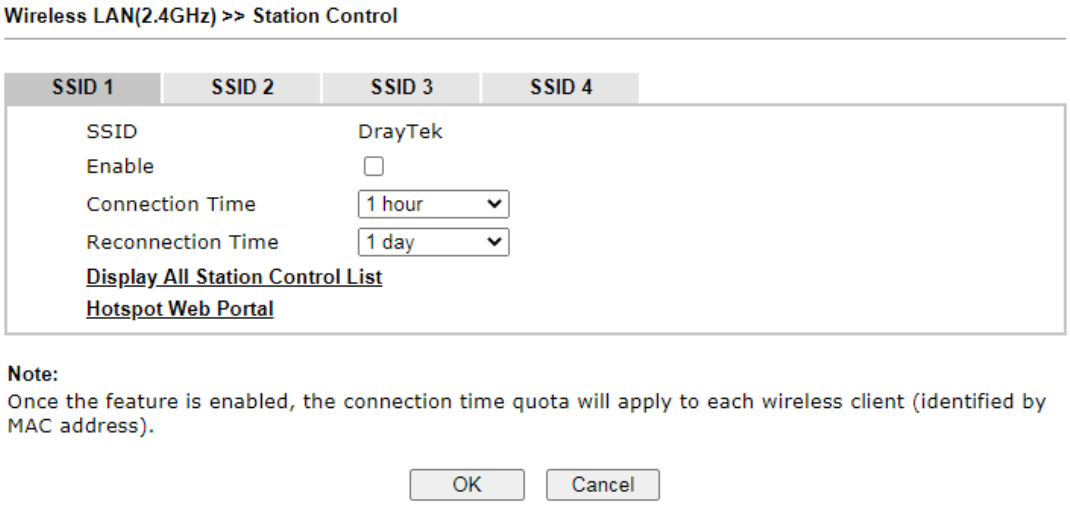
	no sé qué es, el valor predeterminado es 2347. Ajusta el tamaño máximo de trama de transmisión de 802.11, lo que podría reducir las posibilidades de colisión con estaciones ocultas. Se recomienda dejar intacto el valor predeterminado, 2347.
Código de país	El enrutador Vigor transmite códigos de países según el estándar 802.11d. Sin embargo, algunas estaciones inalámbricas detectarán/ explorarán los puntos de acceso en busca de códigos de países para determinar en qué país se encuentra y utilizar los canales apropiados para el país. El cliente inalámbrico puede confundirse si hay múltiples puntos de acceso en las cercanías que transmiten diferentes códigos de países. En tales casos, podría ser necesario cambiar el código de país del punto de acceso para garantizar que estos clientes puedan establecer una conexión inalámbrica con éxito.
Aislar las bandas de 2,4 GHz y 5 GHz	La configuración predeterminada es "Habilitar". Significa que el cliente inalámbrico que usa la banda de 2,4 GHz no puede conectarse al cliente inalámbrico con la banda de 5 GHz y viceversa. Para WLAN de 2,4 GHz y 5 GHz configurados con el mismo nombre de SSID: - No importa si dicha función está habilitada o deshabilitada, los clientes que usan WLAN de 2,4 GHz y 5 GHz pueden comunicarse entre sí si**Miembro aislado**(en**LAN inalámbrica>>Configuración general**) NO está habilitado para dicho SSID. - Sin embargo, si la función de**Miembro aislado**(en**LAN inalámbrica>>Configuración general**) está habilitado para dicho SSID, los clientes que utilizan WLAN de 2,4 GHz y 5 GHz no podrán comunicarse entre sí.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

III-1-8 Control de Estaciones

Station Control se usa para especificar la duración que el cliente inalámbrico puede conectarse al enrutador Vigor. Si esta función está deshabilitada, los clientes inalámbricos pueden conectarse al enrutador siempre que el enrutador esté encendido y la función inalámbrica esté habilitada.

Esta función es especialmente útil para el servicio WiFi gratuito. Por ejemplo, una cafetería puede ofrecer servicio de Wi-Fi gratuito a sus huéspedes durante una hora todos los días. En este escenario, el tiempo de conexión se puede establecer en "1 hora" y el tiempo de reconexión en "1 día". De esta forma, cada huésped puede navegar por la red durante una hora como máximo, liberando así recursos para otros huéspedes.



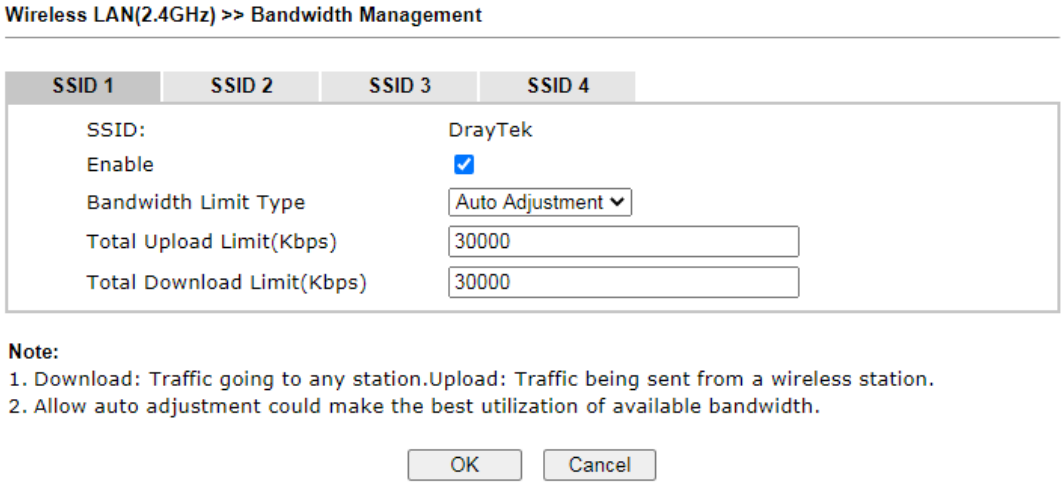
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
SSID	Muestra el SSID seleccionado.
Permitir	Seleccione para habilitar la función de control de estación para este SSID.
Tiempo de conección / Tiempo de reconexión	En el cuadro desplegable Tiempo de conexión, seleccione la cantidad máxima de tiempo que un cliente inalámbrico puede conectarse dentro del período de tiempo seleccionado en el cuadro desplegable Tiempo de reconexión. Seleccionar**Usuario definido**para introducir manualmente el tiempo en días, horas y minutos.
Mostrar la lista de control de todas las estaciones	Haga clic para mostrar todos los clientes inalámbricos que están bajo Control de estación.
Portal web de punto de acceso	Haga clic para saltar a la**Portal web de punto de acceso**página.

Para guardar los cambios en esta página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**.

III-1-9 Gestión de ancho de banda

El flujo descendente o ascendente desde FTP, HTTP o algunas aplicaciones P2P ocupará una gran parte del ancho de banda y afectará a las aplicaciones de otros programas. Utilice la gestión de ancho de banda para que el uso del ancho de banda sea más eficiente.



Los ajustes disponibles se explican a continuación:

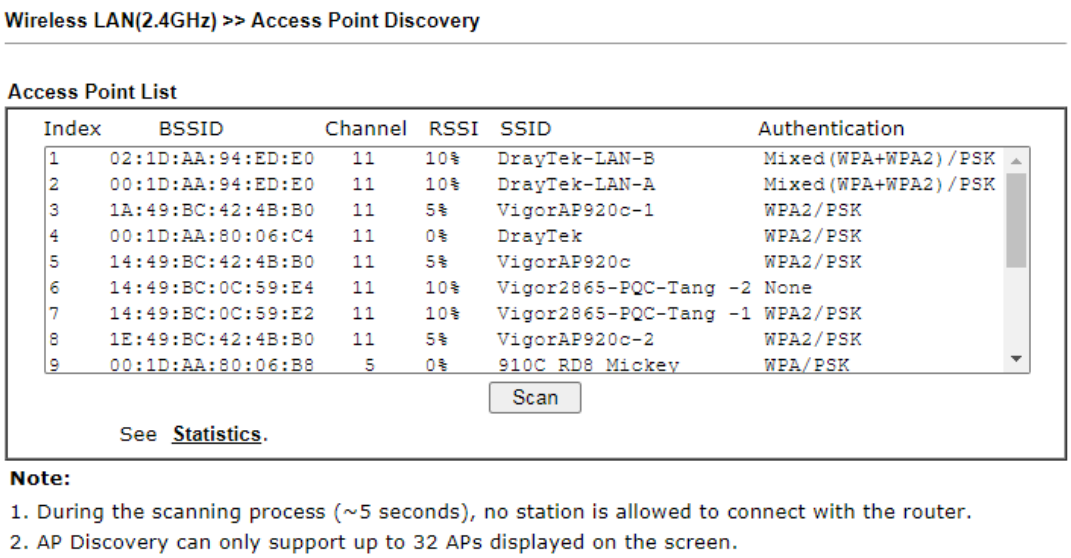
Artículo	Descripción
SSID	Muestra el nombre SSID específico.
Permitir	Marque esta casilla para habilitar la gestión del ancho de banda para los clientes.
Tipo de límite de ancho de banda	**Ajuste automático -**El límite de ancho de banda lo determina el sistema automáticamente. **Límite por estación**–El límite de ancho de banda se determina de acuerdo con la limitación del cliente inalámbrico.
Límite de carga total	Está disponible cuando se selecciona Ajuste automático. Escriba un valor para definir el tráfico de datos máximo (carga) para todos los clientes inalámbricos que se conectan a Vigor2927.
Límite total de descargas	Está disponible cuando se selecciona Ajuste automático. Escriba un valor para definir el número máximo de clientes de datos (estaciones) que se conectan a Vigor2927.
Límite de carga	Está disponible cuando se selecciona Límite por estación. Escriba un valor para definir el tráfico de datos máximo (carga) para cada cliente inalámbrico que se conecte a Vigor2927.
Límite de descarga	Está disponible cuando se selecciona Límite por estación Escriba un valor para definir el tráfico de datos máximo (descarga) para cada cliente inalámbrico que se conecte a Vigor2927.

Para guardar los cambios en esta página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**.

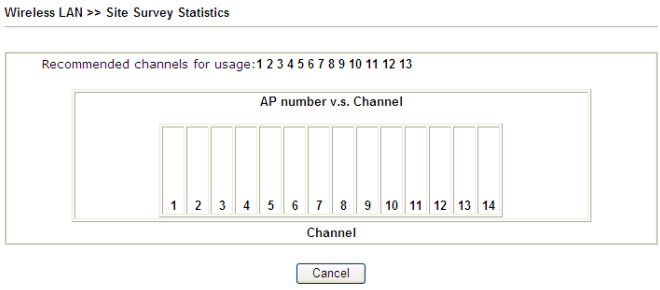
III-1-10 Descubrimiento AP

El enrutador Vigor puede escanear todos los canales regulatorios para encontrar AP que funcionen en el vecindario. El resultado del escaneo se puede usar para determinar el canal más deseable para usar o para ubicar un AP para establecer un enlace WDS. Tenga en cuenta que durante el proceso de escaneo (alrededor de 5 segundos), ningún cliente puede conectarse a Vigor. Solo se pueden descubrir los puntos de acceso que operan en la misma banda que el Vigor.

Haga clic en el**Escanear**botón para iniciar el proceso de descubrimiento de AP.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Escanear	Haga clic para iniciar el proceso de descubrimiento de AP. Los resultados se mostrarán en el cuadro encima de este botón.
Estadísticas	Muestra el uso del canal por parte de los puntos de acceso vecinos. 
Agregar a la configuración de WDS	Este campo está disponible para WLAN (5 GHz).
añadir	Para establecer un enlace WDS a un AP que se encontró en un escaneo de AP, haga clic en su entrada en la ventana Lista de puntos de acceso y su dirección MAC se copiará en el campo de dirección MAC del AP. Seleccione el modo WDS que desea utilizar y haga clic en**añadir**. El AP se configurará en **LAN inalámbrica >> Configuración de WDS**.

III-1-11 Equidad de tiempo aire

La equidad del tiempo aire es esencial en las redes inalámbricas que deben admitir aplicaciones empresariales críticas.

La mayoría de las aplicaciones son simétricas o requieren más capacidad de enlace descendente que de enlace ascendente; la telefonía y el correo electrónico envían la misma cantidad de datos en cada dirección, mientras que la transmisión de video y la navegación web involucran más tráfico enviado desde los puntos de acceso a los clientes que al revés. Esto es esencial para garantizar un rendimiento y una calidad de servicio predecibles, además de permitir que los clientes heredados y 802.11n coexistan en la misma red. Sin equidad en el tiempo aire, las oficinas que usan redes de modo mixto corren el riesgo de que los clientes heredados ralenticen toda la red o dejen que los clientes más rápidos desplacen a otros usuarios.

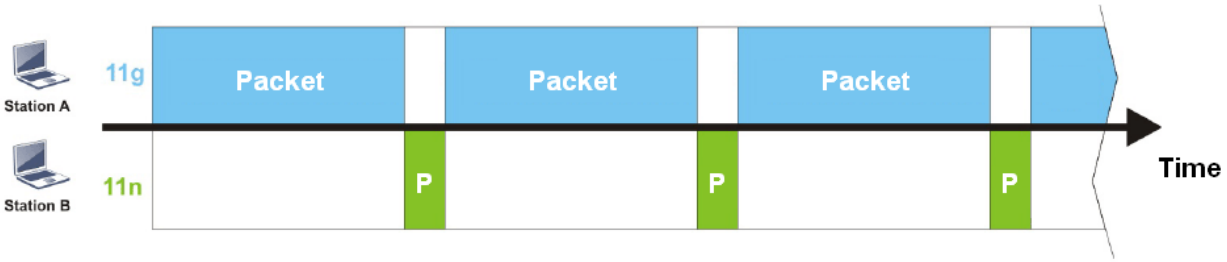
Con equidad en el tiempo aire, cada cliente en un nivel de calidad de servicio determinado tiene el mismo acceso al tiempo aire de la red.

Solo una estación inalámbrica puede acceder al canal inalámbrico al mismo tiempo.

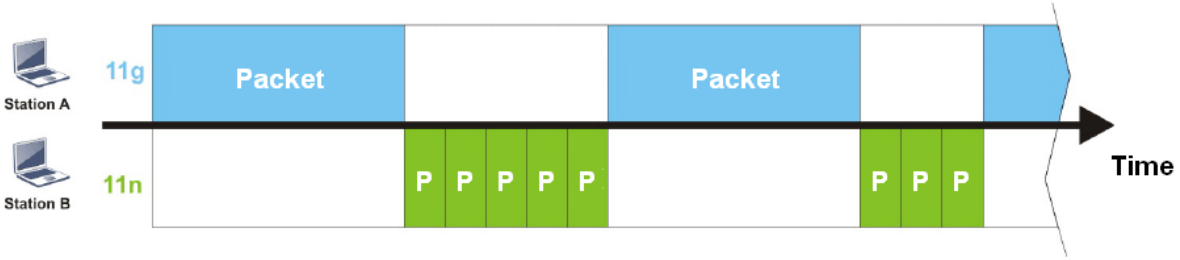
El principio detrás de los mecanismos de acceso al canal IEEE802.11 es que cada estación tiene ***igual probabilidad*** para acceder al canal. Cuando las estaciones inalámbricas tienen una tasa de datos similar, este principio conduce a un resultado justo. En este caso, las estaciones obtienen un tiempo de acceso al canal similar que se denomina tiempo aire.

Sin embargo, cuando las estaciones tienen varias tasas de datos (por ejemplo, 11g, 11n), el resultado no es justo. Las estaciones lentas (11g) funcionan en su tasa de datos lenta y ocupan demasiado tiempo aire, mientras que las estaciones rápidas (11n) se vuelven mucho más lentas.

Tome la siguiente figura como ejemplo, hay 2 estaciones inalámbricas en la red inalámbrica, la Estación A (11g) y la Estación B (11n), las cuales transmiten paquetes de datos al enrutador Vigor. A pesar de que tienen las mismas oportunidades de acceder al canal inalámbrico, la estación B (11n) obtiene poco tiempo de aire y espera demasiado porque la estación A (11g) tarda más en enviar un paquete. En otras palabras, la estación A (velocidad lenta) está acelerando efectivamente la transmisión desde la Estación B (velocidad rápida).



Para aliviar este problema, Airtime Fairness intenta asignar*tiempo aire similar*a cada estación (A y B) controlando el tráfico de TX. En la siguiente figura, la Estación B (11n) tiene mayores oportunidades de enviar paquetes de datos que la Estación A (11g). De esta manera, la estación B (tarifa rápida) obtiene su parte justa de tiempo aire y su velocidad no está limitada por la estación A (tarifa lenta).



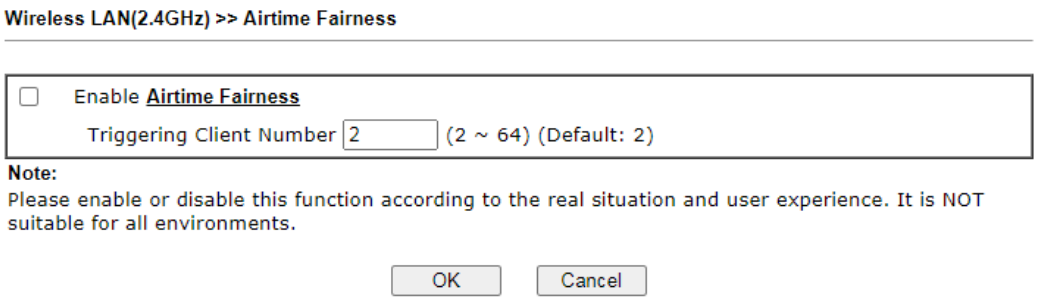
Esto es similar al límite de ancho de banda automático, donde el límite de ancho de banda dinámico de cada estación depende del número de estación activa instantánea y la asignación de tiempo aire. Tenga en cuenta que Airtime Fairness de las bandas de 2,4 GHz y 5 GHz son independientes, pero las estaciones conectadas a diferentes SSID en la misma banda tienen prioridad como grupo, porque todas usan el mismo canal inalámbrico. En determinados entornos, esta función puede reducir los efectos adversos de los dispositivos inalámbricos lentos y mejorar el rendimiento inalámbrico general.

Entornos que pueden beneficiarse al aplicar la equidad de tiempo aire:

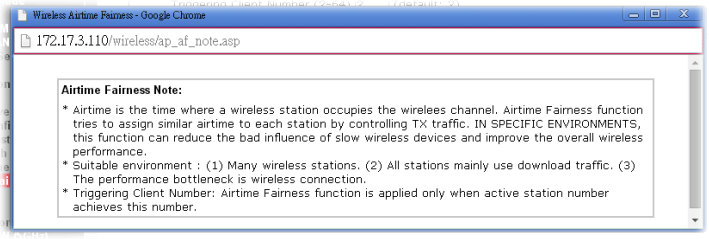
(1) Muchas estaciones inalámbricas.

(2) Todas las estaciones utilizan principalmente tráfico de descarga.

(3) El cuello de botella de rendimiento es la conexión inalámbrica.



Los ajustes disponibles se explican a continuación:

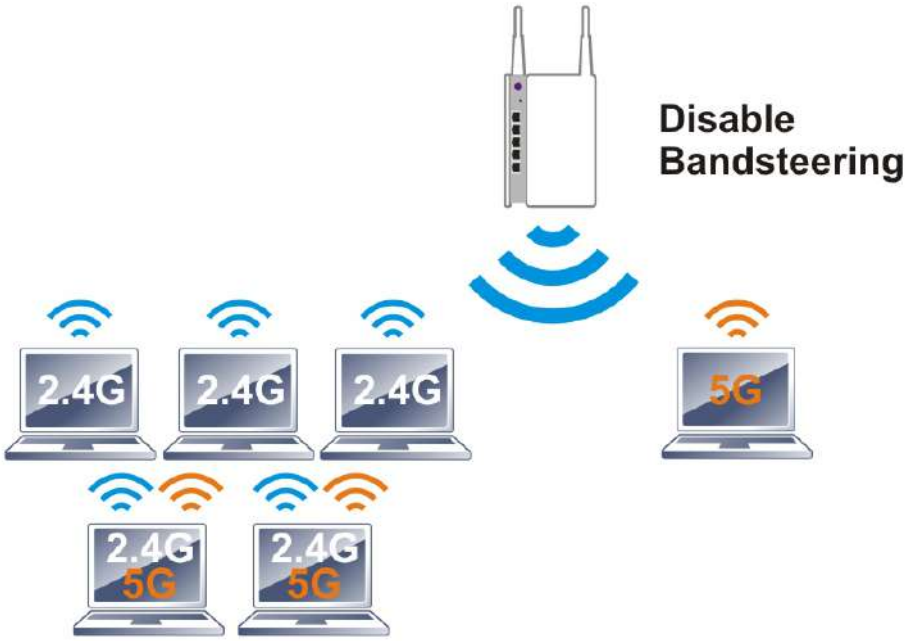
Artículo	Descripción
Habilitar la equidad de tiempo aire	Intente asignar un tiempo de aire similar a cada estación inalámbrica controlando el tráfico de TX. **Equidad de tiempo aire**–Haga clic en el enlace para mostrar la siguiente explicación de la nota de equidad de tiempo aire.  **Activación del número de cliente –**La función Airtime Fairness se aplica solo cuando hay al menos esta cantidad de estaciones inalámbricas activas.

Para guardar los cambios en esta página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**.

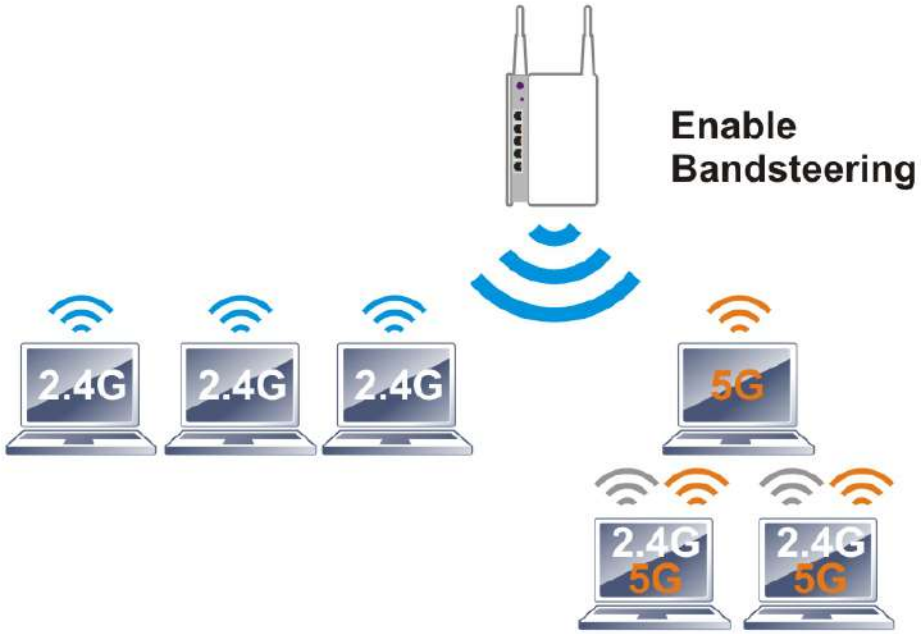
Información	La función Airtime Fairness y la función Bandwidth Limit deben ser mutuamente excluyentes. Por lo que sus webs tienen acciones extra para asegurar que estas dos funciones no estén habilitadas simultáneamente.

III-1-12 Dirección de banda (2,4 GHz)

Band Steering detecta si los clientes inalámbricos son capaces de funcionar a 5 GHz y los dirige a esa frecuencia. Ayuda a mantener libre la banda de 2,4 GHz para los clientes heredados y mejora la experiencia de los usuarios al reducir la utilización del canal de 2,4 GHz.



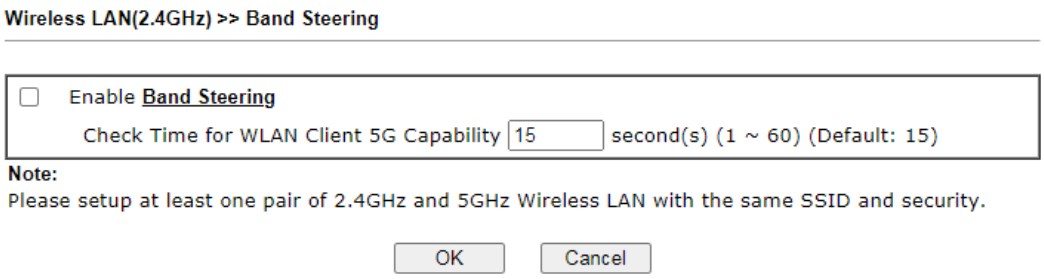
Si se detecta un cliente de doble banda, el AP permitirá que el cliente inalámbrico se conecte a la banda inalámbrica menos congestionada, como la banda de 5 GHz, para reducir la congestión de la red.



Información

Para que Band Steering funcione correctamente, se debe configurar el mismo SSID y la misma configuración de seguridad en las bandas de 2,4 GHz y 5 GHz.

Para configurar Band Steering, vaya a la**LAN inalámbrica (2,4 GHz)>>Dirección de banda**página:

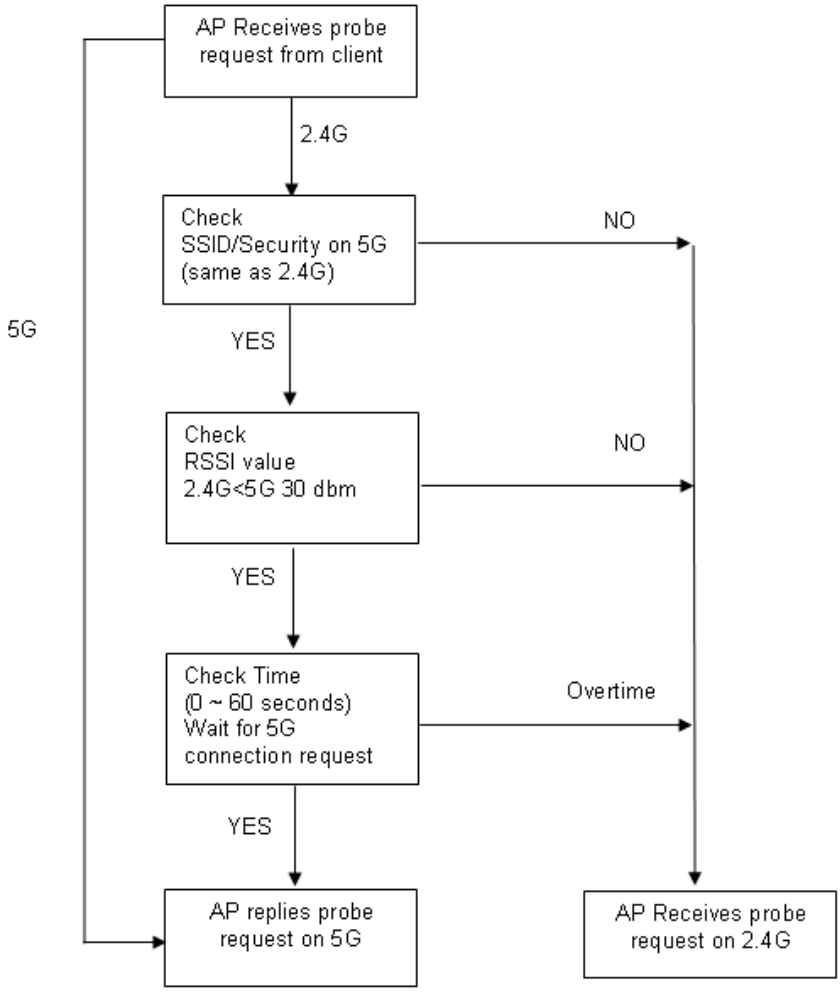


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar dirección de banda	Cuando está habilitado, el enrutador detectará si los clientes inalámbricos tienen capacidad de doble banda o no dentro del límite de tiempo. **Hora de revision...**. – Cuando un cliente inalámbrico intenta conectarse, el enrutador bloqueará los intentos de conectarse a la banda de 2,4 GHz durante el período de tiempo especificado (el valor predeterminado es de 30 segundos), lo que con suerte atraerá al cliente a conectarse a la banda de 5 GHz. Si el cliente no logra conectarse a la banda de 5 GHz dentro del intervalo especificado, podrá conectarse a la banda de 2,4 GHz.

Para guardar los cambios en esta página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**.

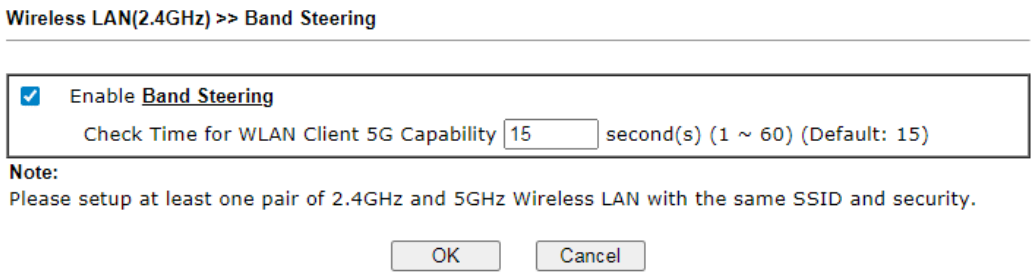
El siguiente diagrama muestra cómo funciona Band Steering.



Ejemplo: ¿Cómo usar la dirección de banda?

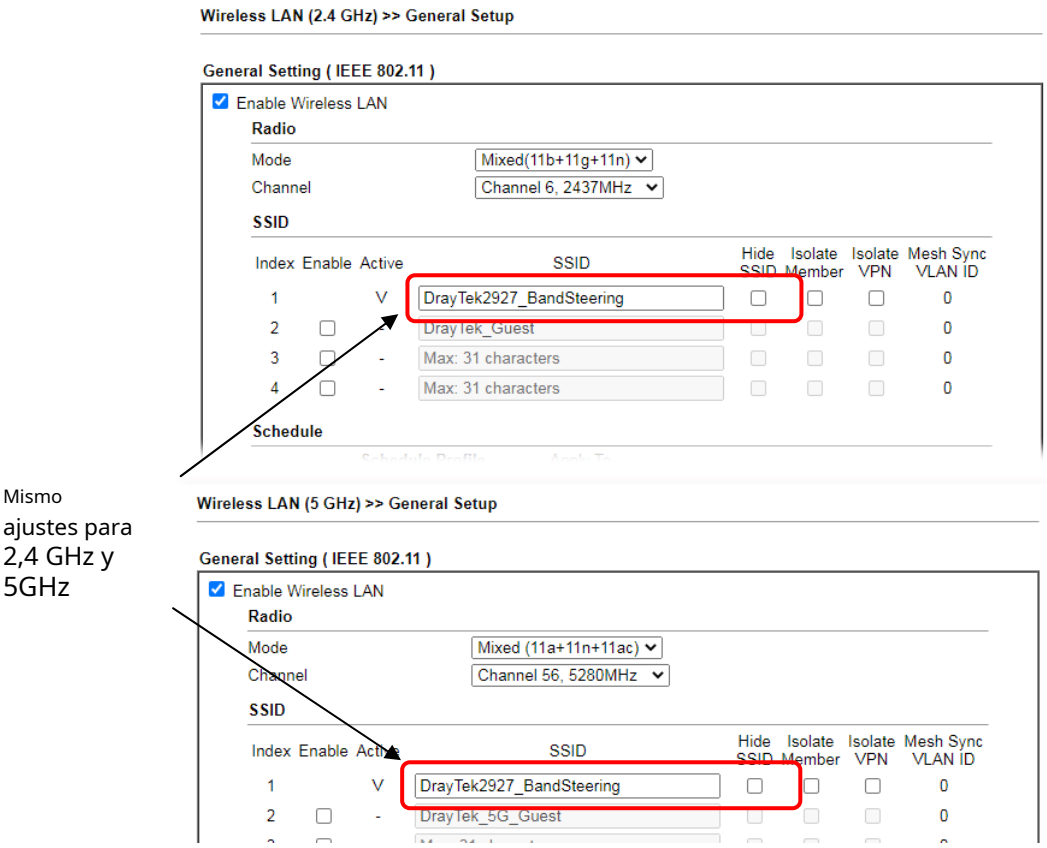
1. Abierto**LAN inalámbrica (2,4 GHz)>>Dirección de banda**.

2. Marque la casilla de**Habilitar dirección de banda**y use el valor predeterminado (15) para la configuración del tiempo de verificación.



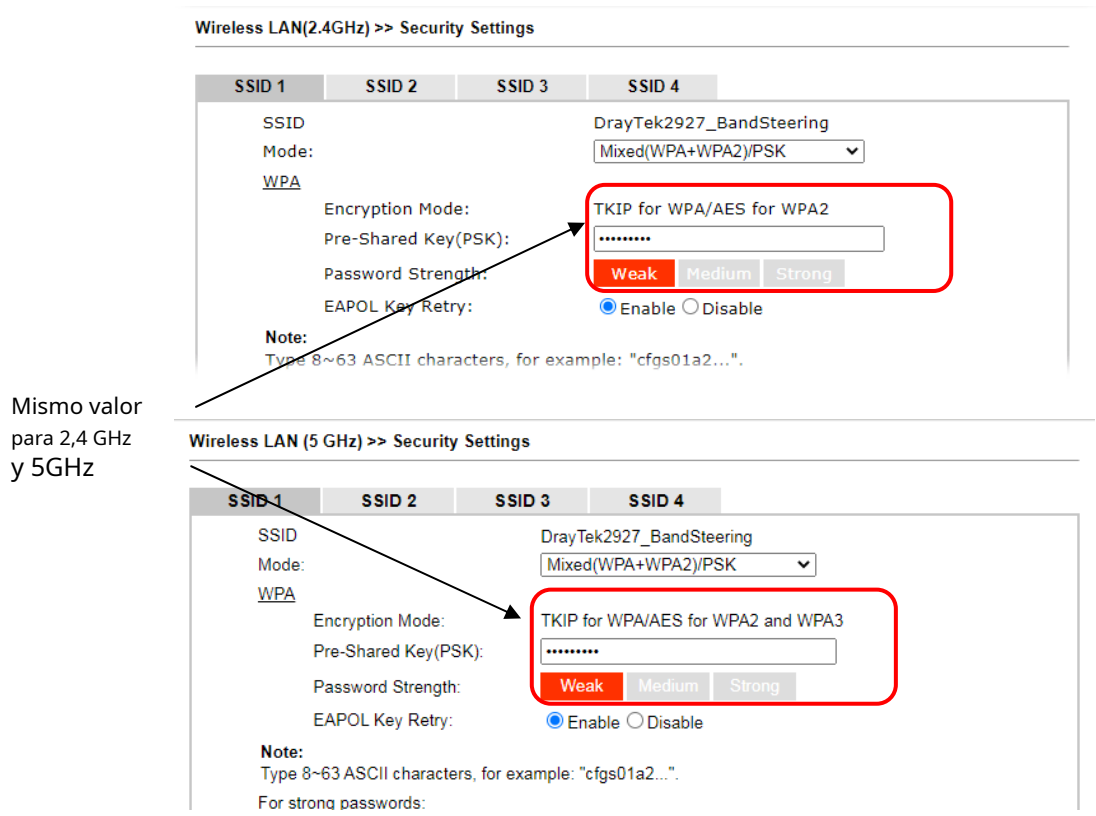
3. Haga clic en**DE ACUERDO**para guardar la configuración.

4. Abierto**LAN inalámbrica (2,4 GHz)>>Configuración general**y**LAN inalámbrica (5 GHz)>> Configuración general**. Configurar SSID como*DrayTek2927_BandSteerin*g para ambas páginas. Hacer clic**DE ACUERDO**para guardar la configuración.



Mismo ajustes para 2,4 GHz y 5GHz

5. Abierto**LAN inalámbrica (2,4 GHz)>>Seguridad**y**LAN inalámbrica (5GHz)>>Seguridad.**Configurar seguridad como *12345678*para ambas paginas. Hacer clic**DE ACUERDO**para guardar la configuración.



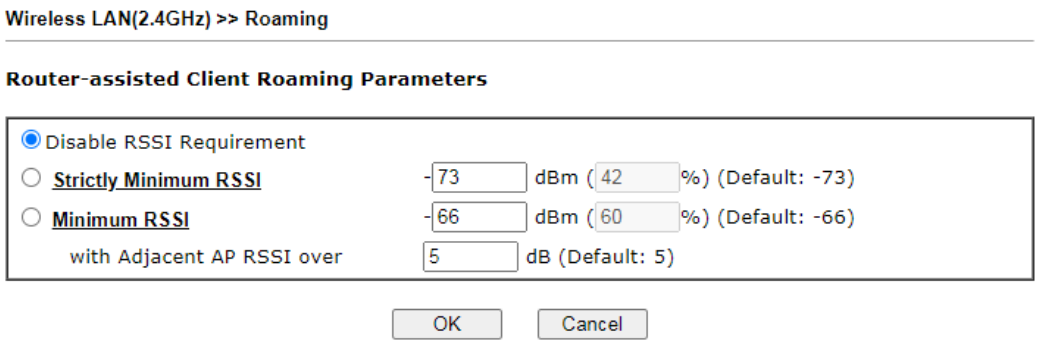
Mismo valor para 2,4 GHz y 5GHz

6. Vigor ahora dirigirá a los clientes inalámbricos a la banda inalámbrica menos congestionada, como 5GHz, para reducir la congestión de la red.

III-1-13 Itinerancia

El roaming WiFi permite que las estaciones inalámbricas cambien las conexiones entre los puntos de acceso dentro de un área para lograr una mejor cobertura y calidad de la señal. Por lo general, depende de la estación inalámbrica cambiar a otro punto de acceso con una intensidad de señal más fuerte mientras ya está conectado, pero los enrutadores inalámbricos Vigor tienen una función de roaming de cliente asistida por AP que podría facilitar el roaming en estaciones inalámbricas. Dependiendo de la configuración de roaming, Vigor monitorea el indicador de intensidad de la señal recibida (RSSI) de las estaciones inalámbricas y desconecta las estaciones cuyo RSSI cae por debajo de cierto umbral (configurable), lo que obliga a las estaciones a buscar otros hosts WiFi para conectarse.

Para configurar los ajustes de roaming inalámbrico, vaya a LAN inalámbrica >> Roaming.



Los ajustes disponibles se explican a continuación:

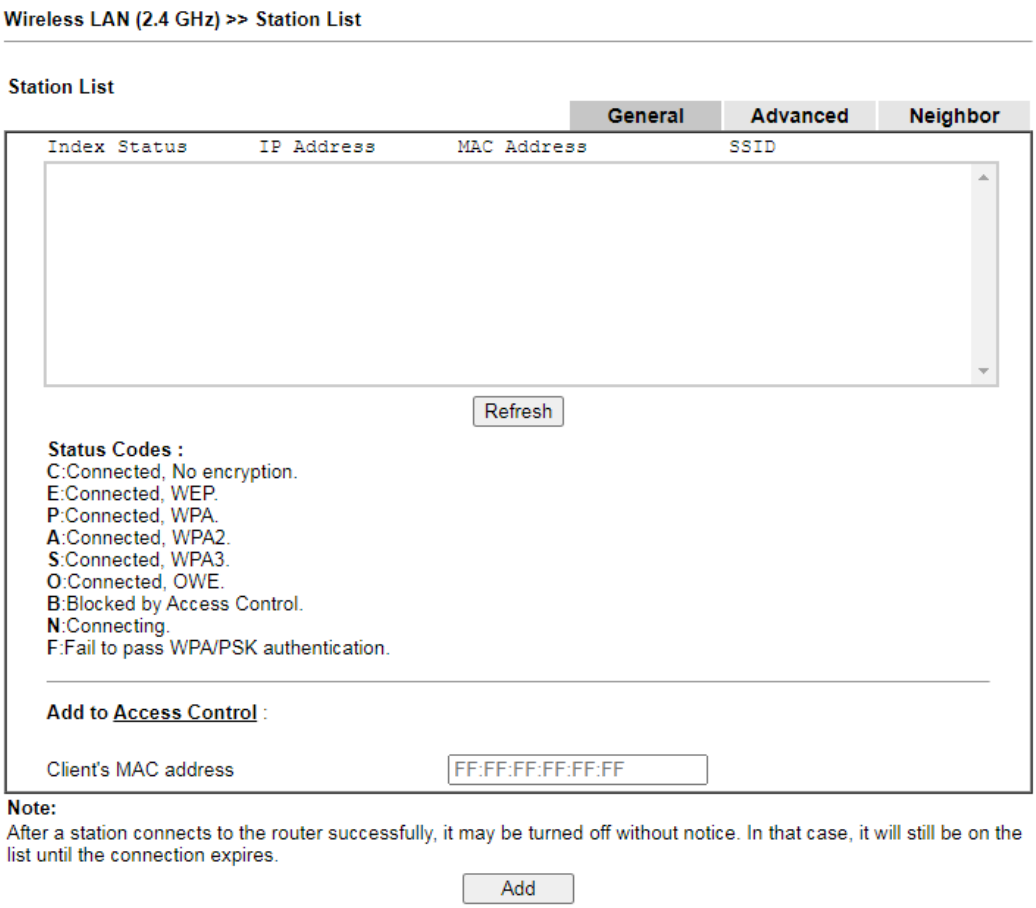
Artículo	Descripción
Deshabilitar el requisito de RSSI	El enrutador Vigor no presta atención al nivel RSSI de las estaciones inalámbricas. Seleccionar esta opción significa que el enrutador Vigor no interferirá con el comportamiento de roaming de las estaciones inalámbricas.
RSSI estrictamente mínimo	El enrutador Vigor desconectará inmediatamente la estación inalámbrica si su RSSI cae por debajo del valor configurado.
RSSI mínimo	**RSSI mínimo -**El enrutador Vigor desconectará a los clientes inalámbricos cuyo RSSI cae por debajo del umbral mínimo solo si también hay un host inalámbrico vecino (enrutador o AP) que tiene un valor de RSSI (definido en el campo Con RSSI de AP adyacente superado) superior a cierto umbral . Para que esta opción funcione, otros hosts inalámbricos conectados a la misma subred LAN deben admitir el intercambio de información RSSI con hosts inalámbricos pares a través de Ethernet. **Con AP adyacente RSSI terminado:**Especifique un valor como umbral.

Para guardar los cambios en esta página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**.

III-1-14 Lista de estaciones

Station List proporciona una descripción general de todos los clientes inalámbricos actualmente conectados y su estado. Como conveniencia adicional, puede optar por agregar un cliente inalámbrico en particular al control de acceso haciendo doble clic en su entrada en la lista para completar el campo de dirección MAC, y luego haciendo clic en el botón Agregar.

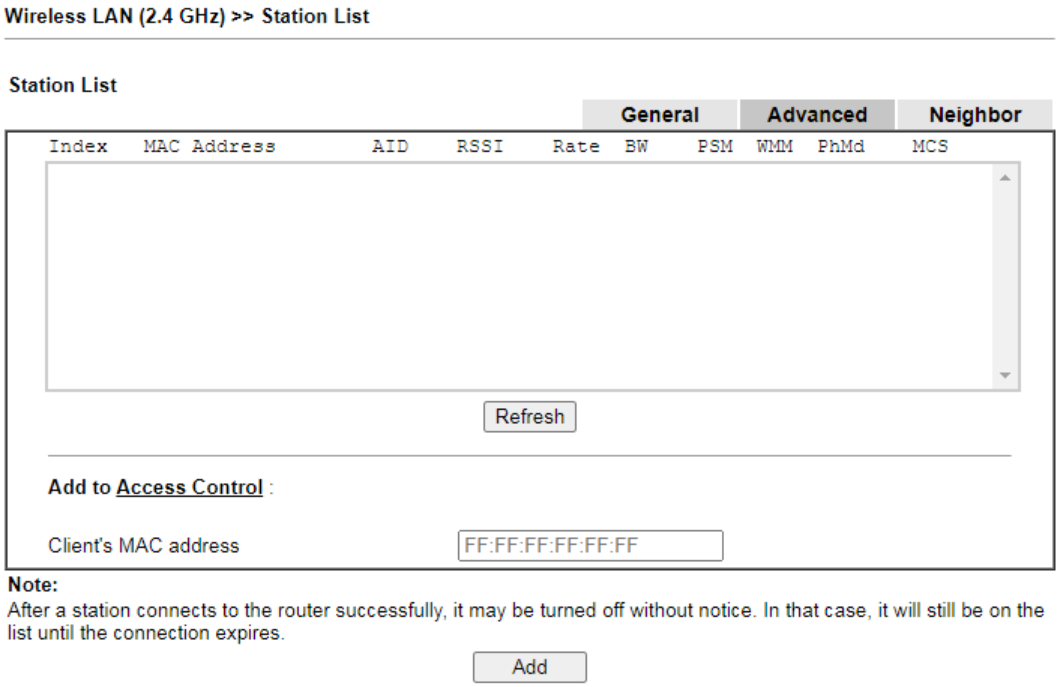
Hay 3 pestañas en la pantalla Lista de estaciones: General, Avanzado y Vecino. Tanto General como Avanzado muestran estaciones inalámbricas conectadas al enrutador Vigor, mientras que Vecino muestra estaciones inalámbricas cercanas conectadas a otros puntos de acceso detectados por el enrutador Vigor.



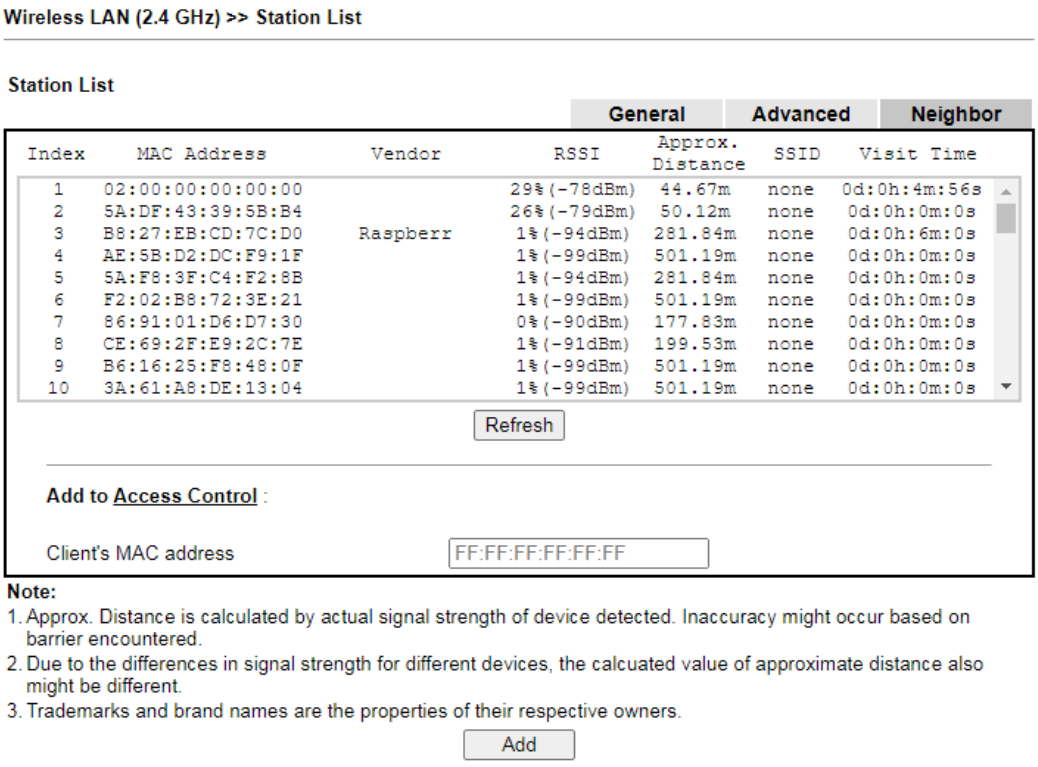
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Actualizar	Haga clic para actualizar la lista de estaciones.
Agregar	Haga clic para agregar la dirección en el campo de dirección MAC del cliente al control de acceso.

A continuación se muestra la pestaña Avanzado, que enumera los mismos clientes que la pestaña General, pero con información más detallada.



A continuación se muestra la pestaña Vecino, que enumera los clientes inalámbricos vistos por el enrutador pero que no están conectados al punto de acceso integrado del enrutador.



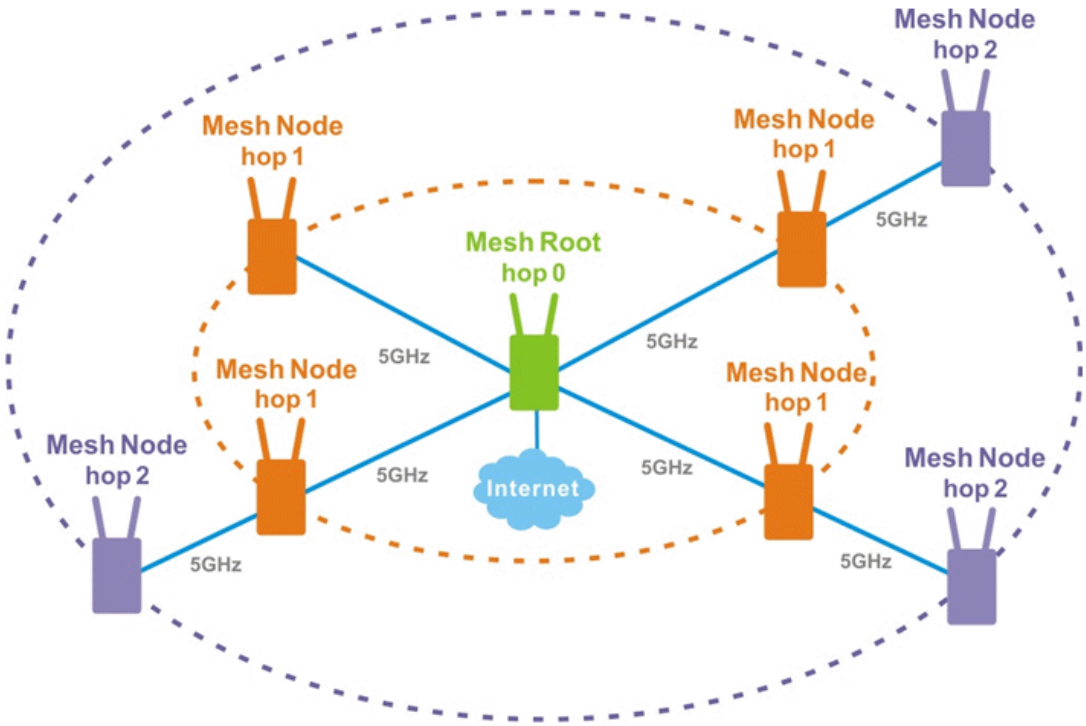
III-2 Red en malla

El enrutador Vigor juega un papel de raíz de malla en una red VigorMesh. Para configurar la red de malla, utilice el Asistente de malla o abra el menú Malla para configurar los ajustes detallados.

Tenga en cuenta que, dentro de la red VigorMesh,

- el número total permitido de nodos de malla es 8 (incluida la raíz de malla)
- el número máximo de saltos es 3

Consulte la siguiente figura:



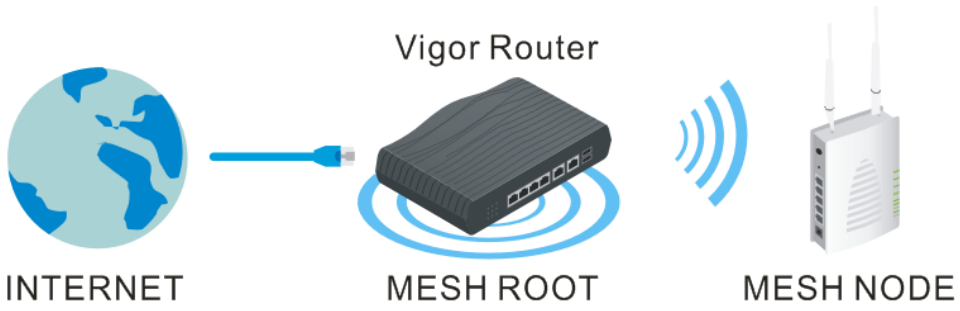
Para el conjunto de grupos de malla dentro de la red VigorMesh,

- Debe estar compuesto por "1" Mesh Root y "0 ~ 7" nodos de malla
- (Roaming) Normalmente, los miembros de un grupo de malla usan el mismo SSID inalámbrico/seguridad
- (Agregar) Solo la raíz de la malla puede agregar un nuevo nodo de malla al grupo de malla
- (Recuperar) Un nodo de malla desconectado intentará conectarse automáticamente a otro nodo de malla conectado del mismo grupo

Raíz de malla

Mesh Root indica que el enrutador Vigor sería la conexión de enlace ascendente de otro AP. Como Mesh Root, el enrutador Vigor debe conectarse a Internet a través de WAN para tener una conexión a Internet.

La siguiente figura muestra cómo el enrutador Vigor se ejecuta como MESH ROOT:

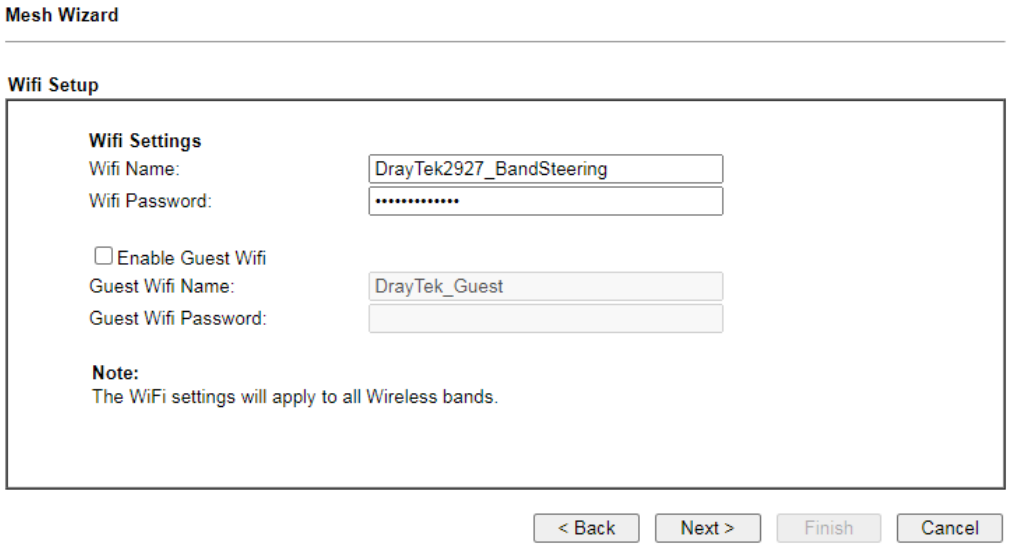


Asistente de malla III-2-1

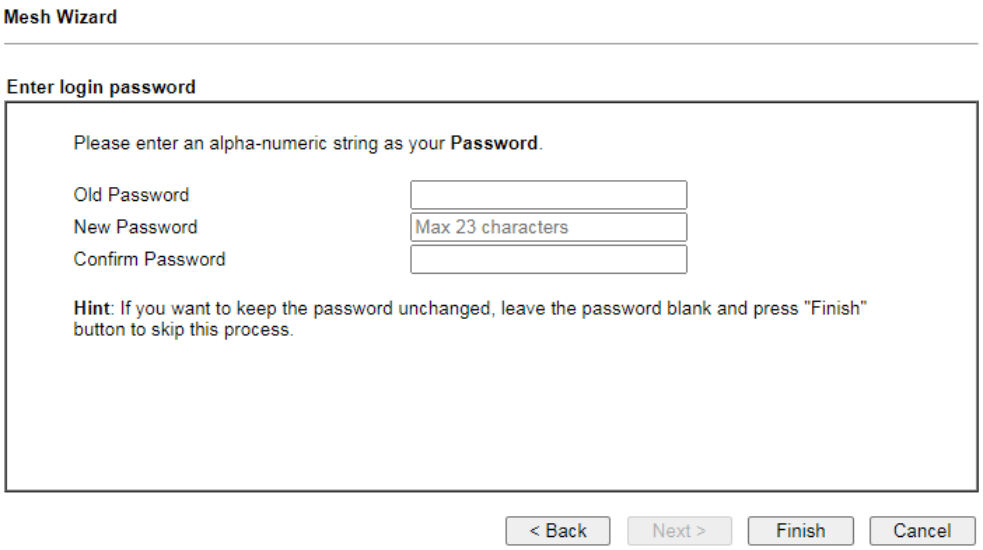
El asistente de malla ofrece una forma rápida de configurar la red de malla.

1. Ir a**Asistentes>Asistente de malla**.

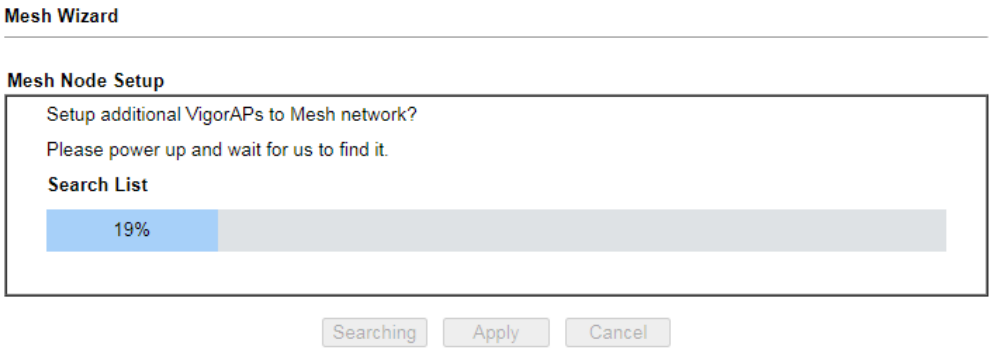
2. Verifique el**Habilitar malla**caja. Hacer clic**Próximo**para obtener la siguiente página.



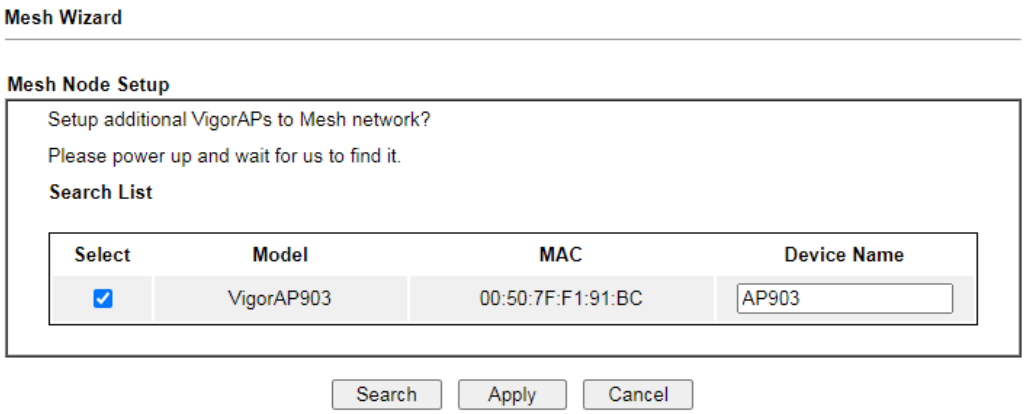
3. Establezca el nombre y la contraseña de Wifi; hacer clic**Próximo**para obtener la siguiente página.



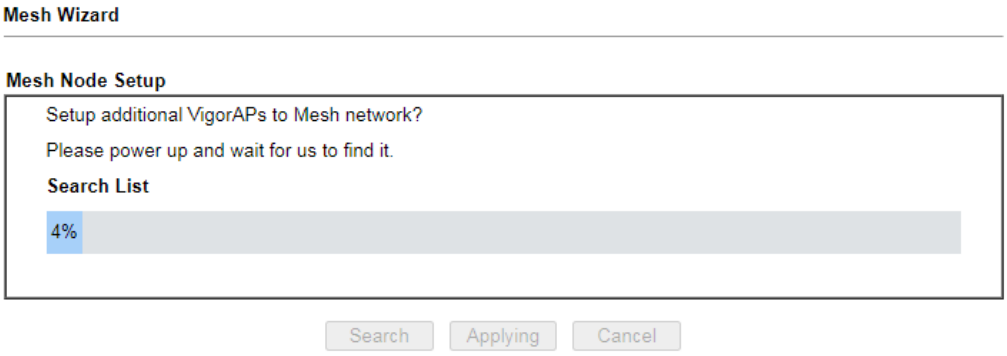
4. Establezca la contraseña, si es necesario. Luego, haga clic en**Finalizar**. El sistema comienza a buscar puntos de acceso disponibles.



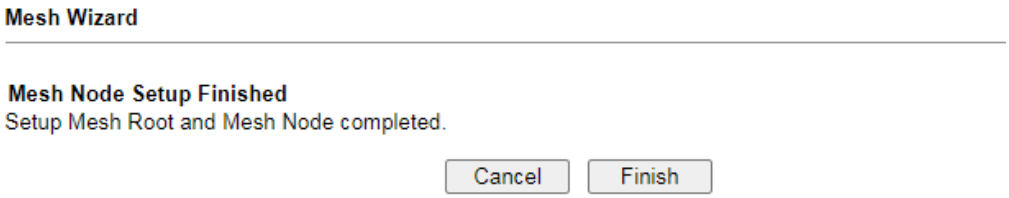
5. Espere unos minutos. Más tarde, los puntos de acceso alrededor del enrutador Vigor se mostrarán a continuación.



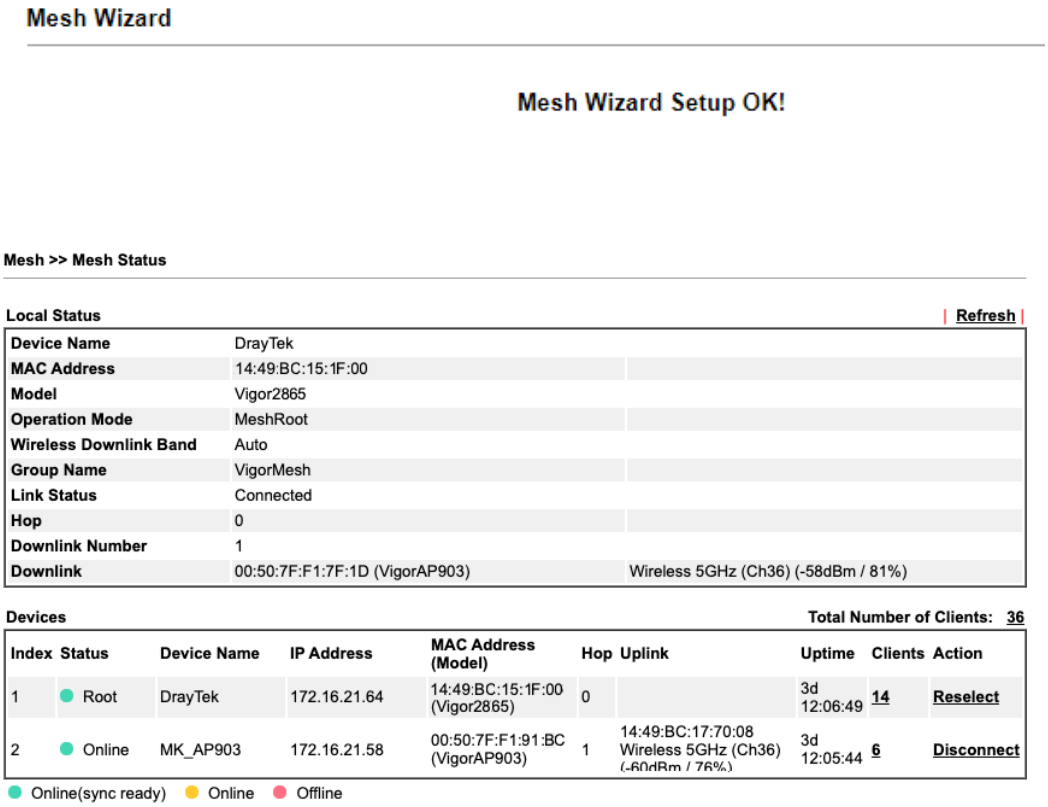
6. Seleccione el (por ejemplo, VigorAP903 en este caso) que desea agrupar en el enrutador Vigor. Luego, haga clic en**Aplicar**.



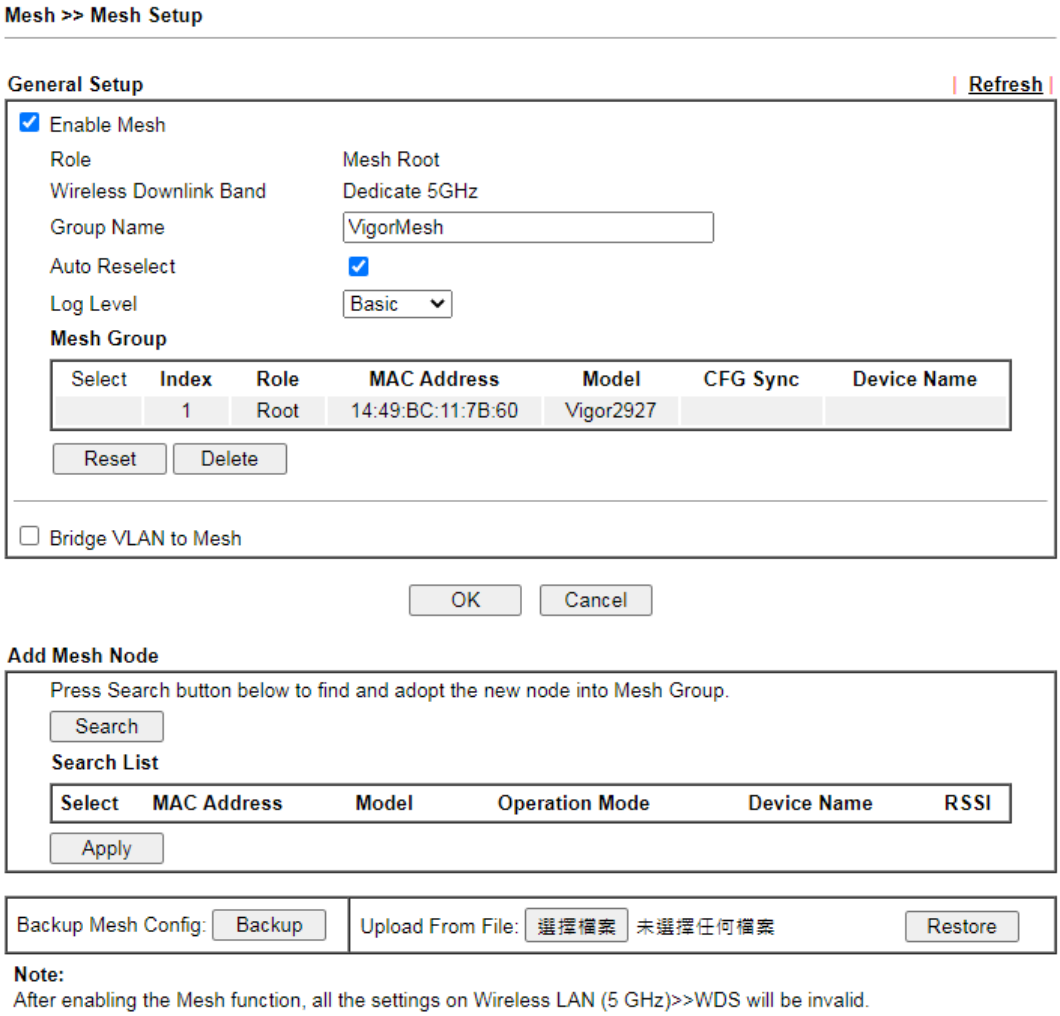
7. Cuando finalice la configuración del nodo de malla, haga clic en**Finalizar**.



8. Después de "Configuración del asistente de malla OK!" aparece, vaya a**Malla >> Estado de malla**. El nodo de malla (AP903) se ha agrupado bajo el enrutador Vigor.

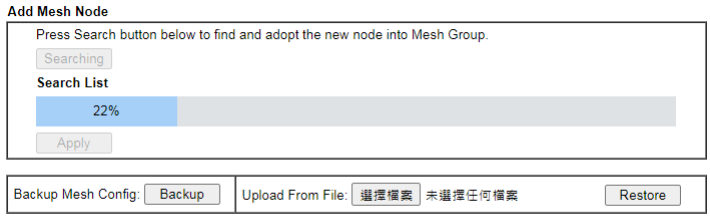
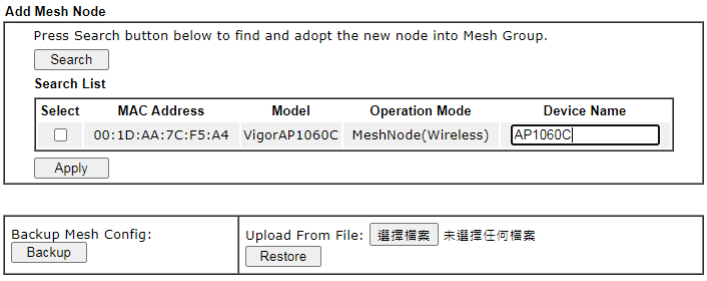
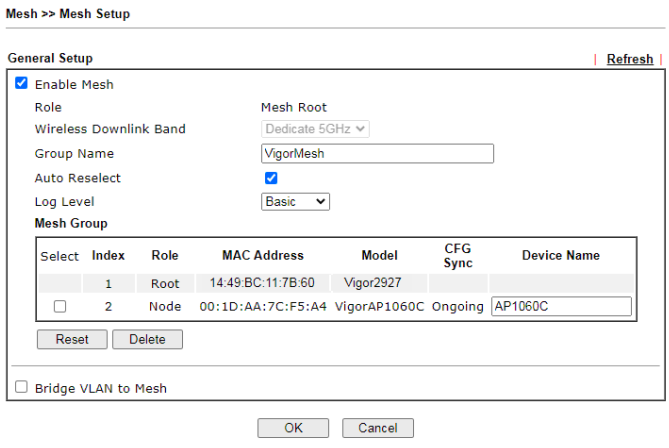


Esta página puede modificar la configuración relacionada con la malla. Puede buscar y especificar nodos de malla como miembros en el grupo de malla actual.



Los ajustes disponibles se explican a continuación:

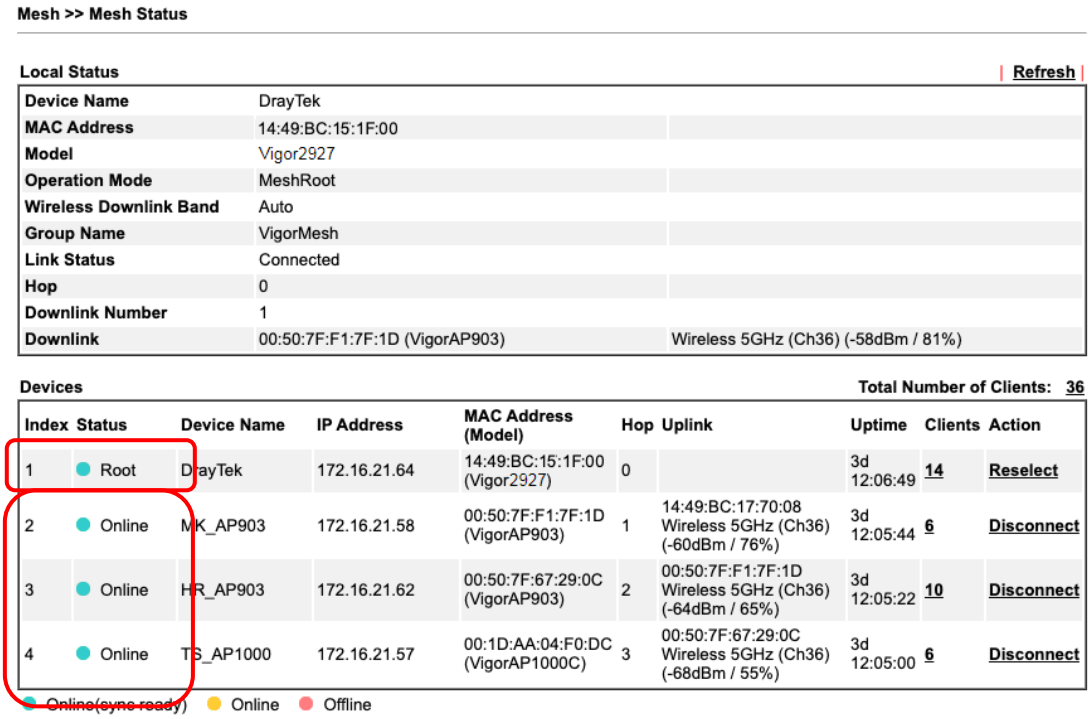
Artículo	Descripción
Configuración general	
Habilitar malla	Marque para habilitar la función de malla.
Role	Muestra la función del enrutador Vigor. El enrutador Vigor es una raíz de malla para proporcionar acceso a Internet para Mesh Network.
Banda de enlace descendente inalámbrico	En la actualidad, solo se dedican 5 GHz como banda de enlace descendente para conectarse con un nodo de malla de enlace ascendente.
Nombre del grupo	Muestra el nombre del grupo de malla actual.
Reselección automática	Está seleccionado por defecto. Para realizar la reselección automática, asegúrese de que el proceso de CFG Sync y CFG Check para nodos de malla sea exitoso. Si está habilitado, después de cambiar el entorno de la red en malla (p. ej., fuera de línea, desconexión), el dispositivo raíz realizará una reselección automática para reconstruir la red en malla.

Nivel de registro	Elegir**Básico**o**Detallado**. La información relacionada se mostrará en la **Diagnósticos >> Explorador de Syslog.**
Grupo de malla	La información básica, incluida la función, la dirección MAC y el nombre del modelo de la raíz y el nodo de malla (hasta 8 entradas, una raíz de malla y siete nodos de malla) se mostrará en este campo. **Reiniciar -**Haga clic en él para borrar la información del grupo de malla. **Borrar**-Haga clic en él para eliminar la entrada seleccionada.
Puente VLAN a malla	Seleccione para habilitar la función.
Agregar nodo de malla: solo está disponible si la función Malla está habilitada.	
Buscar	Haga clic para escanear los puntos de acceso disponibles alrededor de este enrutador Vigor.  Los puntos de acceso detectados se mostrarán en la lista de búsqueda. 
Aplicar	Seleccione el nodo de malla que desee y haga clic en este botón. El nuevo nodo de malla se mostrará en Grupo de malla. 
Configuración de malla de copia de seguridad	**Respaldo**–Haga clic en el botón para guardar la configuración como un archivo.
Seleccionar/Restaurar	Haga clic en el botón Cargar para especificar un archivo de configuración. Luego haga clic en Restaurar para aplicar la configuración. Cuando la dirección MAC del enrutador Vigor no es la raíz de malla del grupo de malla, la operación de restauración no tendrá éxito.

Estado de malla III-2-3

Esta página muestra el estado de la red de malla.

Un grupo de malla puede contener hasta 8 dispositivos. En la siguiente figura, el dispositivo con el salto 0 es un Backhaul Ethernet especial. Significa que este nodo usará un cable Ethernet para unirse al grupo de malla mientras que otros usan el enlace inalámbrico.



Mesh >> Mesh Status

Local Status | Refresh |

Device Name	DrayTek	
MAC Address	14:49:BC:15:1F:00	
Model	Vigor2927	
Operation Mode	MeshRoot	
Wireless Downlink Band	Auto	
Group Name	VigorMesh	
Link Status	Connected	
Hop	0	
Downlink Number	1	
Downlink	00:50:7F:F1:7F:1D (VigorAP903)	Wireless 5GHz (Ch36) (-58dBm / 81%)

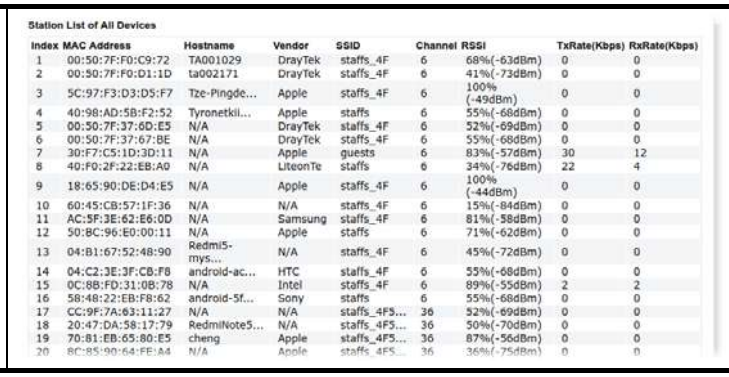
Devices **Total Number of Clients: 36**

Index	Status	Device Name	IP Address	MAC Address (Model)	Hop	Uplink	Uptime	Clients	Action
1	Root	DrayTek	172.16.21.64	14:49:BC:15:1F:00 (Vigor2927)	0		3d 12:06:49	14	Reselect
2	Online	MK_AP903	172.16.21.58	00:50:7F:F1:7F:1D (VigorAP903)	1	14:49:BC:17:70:08 Wireless 5GHz (Ch36) (-60dBm / 76%)	3d 12:05:44	6	Disconnect
3	Online	HR_AP903	172.16.21.62	00:50:7F:67:29:0C (VigorAP903)	2	00:50:7F:F1:7F:1D Wireless 5GHz (Ch36) (-64dBm / 65%)	3d 12:05:22	10	Disconnect
4	Online	TS_AP1000	172.16.21.57	00:1D:AA:04:F0:DC (VigorAP1000C)	3	00:50:7F:67:29:0C Wireless 5GHz (Ch36) (-68dBm / 55%)	3d 12:05:00	6	Disconnect

Online(sync ready) Online Offline

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Estado local	Muestra información general para este dispositivo.
Dispositivos	Muestre información detallada para este dispositivo (como raíz de malla) y los nodos de malla en el grupo. **Índice**–Muestra el número del dispositivo dentro de un grupo de malla. **Estado**–Muestra el rol y el estado de conexión del dispositivo. **Nombre del dispositivo**–Muestra el nombre del dispositivo (para identificación). **Dirección IP**–Muestra la dirección IP del dispositivo. **Dirección MAC**–Muestra la dirección MAC del dispositivo. **Brincar**–Muestra el nivel del dispositivo en Mesh Network. "0" significa que el dispositivo está conectado a Internet mediante un cable Ethernet (alámbrico). "1" a "3" significa cuántos enlaces inalámbricos debe atravesar el dispositivo para llegar a un dispositivo Hop 0. **enlace ascendente**–Muestra la dirección MAC del dispositivo al que se conecta el AP.
Número total de Clientes	Muestra la lista de estaciones de todos los dispositivos de malla.



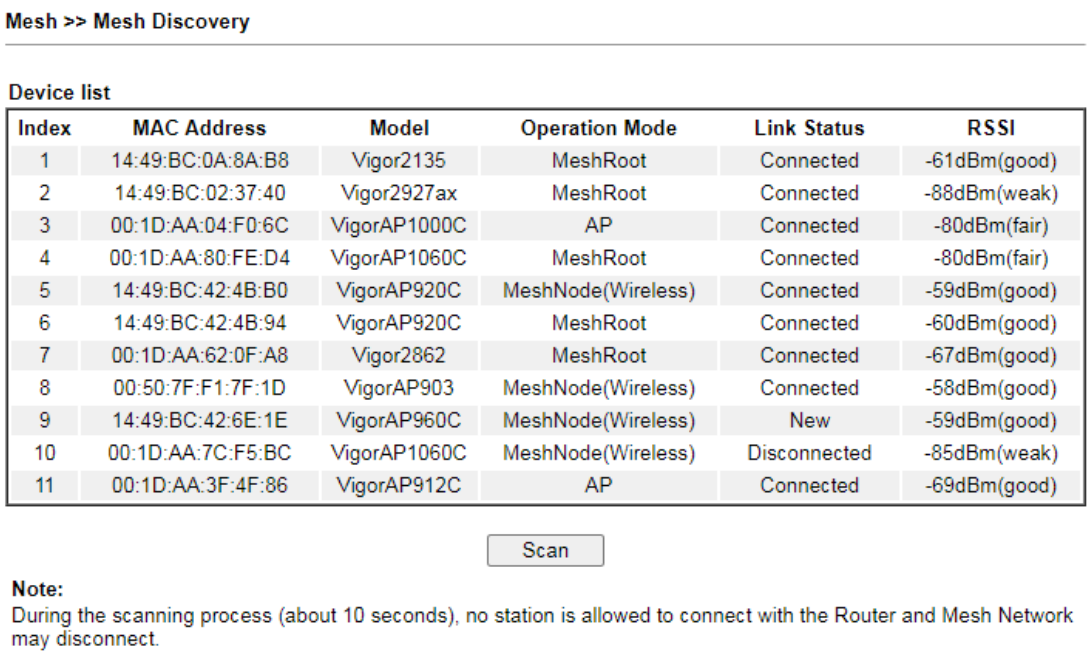
Station List of All Devices

Index	MAC Address	Hostname	Vendor	SSID	Channel	RSSI	TxRate(Kbps)	RxRate(Kbps)
1	00:50:7F:F0:C9:72	TA001029	DrayTek	staffs_4F	6	68%(-63dBm)	0	0
2	00:50:7F:F0:D1:1D	ta002171	DrayTek	staffs_4F	6	41%(-73dBm)	0	0
3	5C:97:F3:D3:D5:F7	Tze-Pingde...	Apple	staffs_4F	6	100% (-49dBm)	0	0
4	40:98:AD:5B:F2:52	Tyronetkii...	Apple	staffs	6	55%(-68dBm)	0	0
5	00:50:7F:37:6D:E5	N/A	DrayTek	staffs_4F	6	52%(-69dBm)	0	0
6	00:50:7F:37:67:BE	N/A	DrayTek	staffs_4F	6	55%(-68dBm)	0	0
7	30:F7:C5:1D:3D:11	N/A	Apple	guests	6	83%(-57dBm)	30	12
8	40:F0:2F:22:EB:A0	N/A	LiteonTe	staffs	6	34%(-76dBm)	22	4
9	18:65:90:DE:D4:E5	N/A	Apple	staffs_4F	6	100% (-44dBm)	0	0
10	60:45:CB:57:1F:36	N/A	N/A	staffs_4F	6	15%(-84dBm)	0	0
11	AC:5F:3E:62:E6:0D	N/A	Samsung	staffs_4F	6	81%(-58dBm)	0	0
12	50:8C:96:E0:00:11	N/A	Apple	staffs	6	71%(-62dBm)	0	0
13	04:B1:67:52:48:90	Redmi5-mys...	N/A	staffs_4F	6	45%(-72dBm)	0	0
14	04:C2:3E:3F:CB:F8	android-ac...	HTC	staffs_4F	6	55%(-68dBm)	0	0
15	0C:8B:FD:31:0B:78	N/A	Intel	staffs_4F	6	89%(-55dBm)	2	2
16	58:48:22:EB:F8:62	android-5f...	Sony	staffs	6	55%(-68dBm)	0	0
17	CC:9F:7A:63:11:27	N/A	N/A	staffs_4F5...	36	52%(-69dBm)	0	0
18	20:47:DA:58:17:79	RedmiNote5...	N/A	staffs_4F5...	36	50%(-70dBm)	0	0
19	70:81:EB:65:80:E5	cheng	Apple	staffs_4F5...	36	87%(-56dBm)	0	0
20	8C:85:90:64:FE:A4	N/A	Apple	staffs_4F5...	36	36%(-75dBm)	0	0

Descubrimiento de malla III-2-4

Antes de conectar un nodo de malla, no puede verificar el estado del dispositivo desde la raíz de malla. Esta página puede ayudar a descubrir todos los dispositivos Mesh y ofrecer el estado del enlace y el modo de funcionamiento de cada dispositivo Mesh.

Para obtener la lista de dispositivos alrededor de este enrutador Vigor, haga clic en**Escanear**. Más tarde, los dispositivos Mesh circundantes se mostrarán en esta página.



Mesh >> Mesh Discovery

Device list

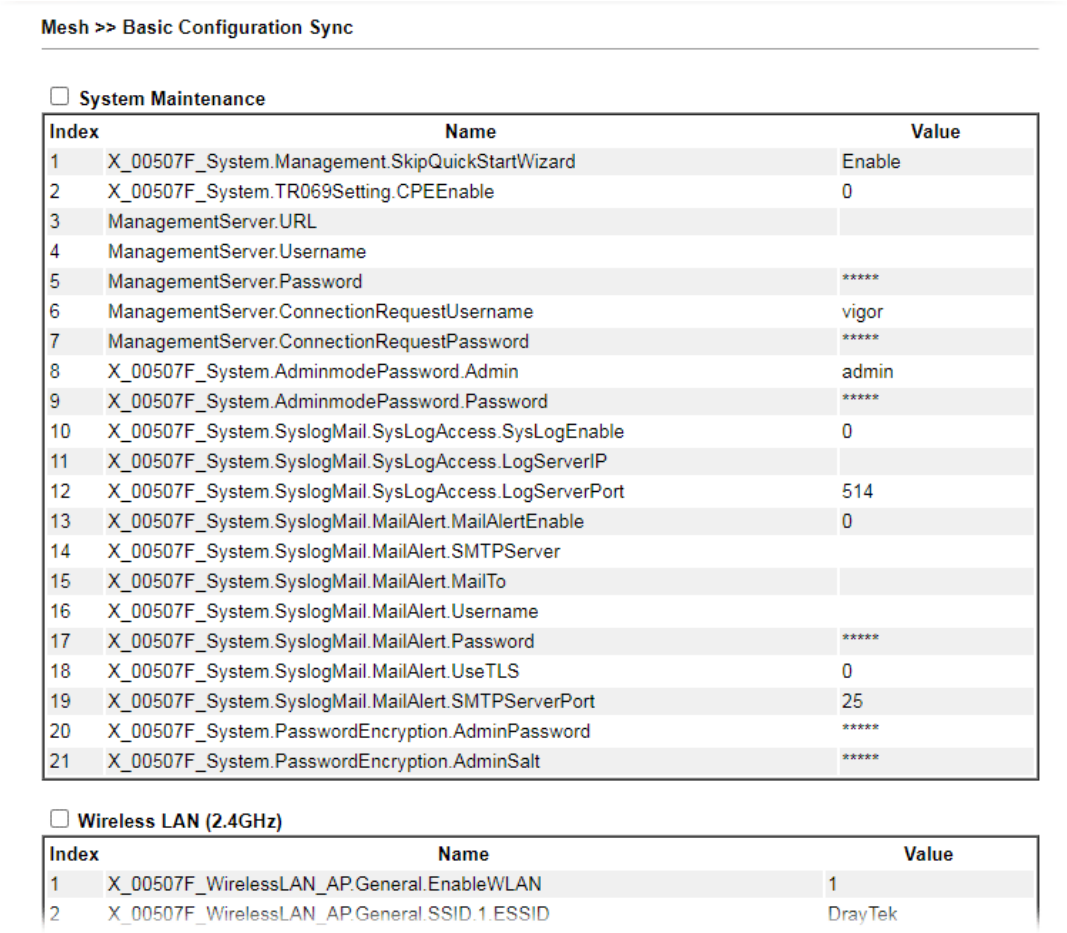
Index	MAC Address	Model	Operation Mode	Link Status	RSSI
1	14:49:BC:0A:8A:B8	Vigor2135	MeshRoot	Connected	-61dBm(good)
2	14:49:BC:02:37:40	Vigor2927ax	MeshRoot	Connected	-88dBm(weak)
3	00:1D:AA:04:F0:6C	VigorAP1000C	AP	Connected	-80dBm(fair)
4	00:1D:AA:80:FE:D4	VigorAP1060C	MeshRoot	Connected	-80dBm(fair)
5	14:49:BC:42:4B:B0	VigorAP920C	MeshNode(Wireless)	Connected	-59dBm(good)
6	14:49:BC:42:4B:94	VigorAP920C	MeshRoot	Connected	-60dBm(good)
7	00:1D:AA:62:0F:A8	Vigor2862	MeshRoot	Connected	-67dBm(good)
8	00:50:7F:F1:7F:1D	VigorAP903	MeshNode(Wireless)	Connected	-58dBm(good)
9	14:49:BC:42:6E:1E	VigorAP960C	MeshNode(Wireless)	New	-59dBm(good)
10	00:1D:AA:7C:F5:BC	VigorAP1060C	MeshNode(Wireless)	Disconnected	-85dBm(weak)
11	00:1D:AA:3F:4F:86	VigorAP912C	AP	Connected	-69dBm(good)

Scan

Note:
During the scanning process (about 10 seconds), no station is allowed to connect with the Router and Mesh Network may disconnect.

Solo el dispositivo con el Estado de enlace de "Nuevo" se puede seleccionar y agrupar en este enrutador.

Si agrega un nodo de malla en un grupo de malla, la raíz de malla enviará la configuración básica al dispositivo. Esta página podría ayudarlo a cambiar la configuración de Mesh Root y entregar la nueva configuración de Mesh Root a todos los nodos de malla "conectados".



Mesh >> Basic Configuration Sync

☐ **System Maintenance**

Index	Name	Value
1	X_00507F_System.Management.SkipQuickStartWizard	Enable
2	X_00507F_System.TR069Setting.CPEEnable	0
3	ManagementServer.URL	
4	ManagementServer.Username	
5	ManagementServer.Password	*****
6	ManagementServer.ConnectionRequestUsername	vigor
7	ManagementServer.ConnectionRequestPassword	*****
8	X_00507F_System.AdminmodePassword.Admin	admin
9	X_00507F_System.AdminmodePassword.Password	*****
10	X_00507F_System.SyslogMail.SysLogAccess.SysLogEnable	0
11	X_00507F_System.SyslogMail.SysLogAccess.LogServerIP	
12	X_00507F_System.SyslogMail.SysLogAccess.LogServerPort	514
13	X_00507F_System.SyslogMail.MailAlert.MailAlertEnable	0
14	X_00507F_System.SyslogMail.MailAlert.SMTPServer	
15	X_00507F_System.SyslogMail.MailAlert.MailTo	
16	X_00507F_System.SyslogMail.MailAlert.Username	
17	X_00507F_System.SyslogMail.MailAlert.Password	*****
18	X_00507F_System.SyslogMail.MailAlert.UseTLS	0
19	X_00507F_System.SyslogMail.MailAlert.SMTPServerPort	25
20	X_00507F_System.PasswordEncryption.AdminPassword	*****
21	X_00507F_System.PasswordEncryption.AdminSalt	*****

☐ **Wireless LAN (2.4GHz)**

Index	Name	Value
1	X_00507F_WirelessLAN_AP.General.EnableWLAN	1
2	X_00507F_WirelessLAN_AP.General.SSID.1.ESSID	DrayTek

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Mantenimiento del sistema / LAN inalámbrica (2,4 Hz) / LAN inalámbrica (5 GHz)	Marque los elementos que desea sincronizar en la configuración.
sincronizar	Este botón está disponible solo cuando cualquier nodo de malla en la red de malla está en línea y listo para sincronizar. Haga clic en él para aplicar la configuración configurada por este enrutador a todos los nodos de malla conectados.

Consejos para la configuración de la red Mesh

- Configure DOS dispositivos de malla con RSSI de enlace ascendente superior a -65dBm.
- Actualice la versión de firmware de los dispositivos Mesh a través de Mesh Link, comenzando desde el dispositivo Mesh con menos número de saltos. Por ejemplo, actualice el firmware desde la raíz, hop1 Mesh Node, luego hop2 Mesh Node, y así sucesivamente.

- La red VigorMesh admite hasta 3 saltos de dispositivos de malla. Sin embargo, se sugiere conectar el grupo de malla con menos o igual a 2 saltos.

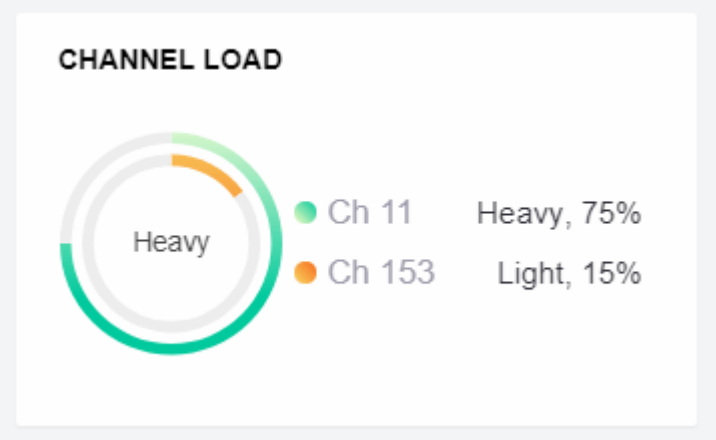
  Para su referencia, hacemos una prueba de entorno de malla real y obtenemos el siguiente registro. (Utilice la aplicación VigorAP para realizar pruebas de velocidad de Internet con diferentes nodos de malla de saltos).

  Velocidad de descarga de Internet (para root y hop1 ~ hop3):

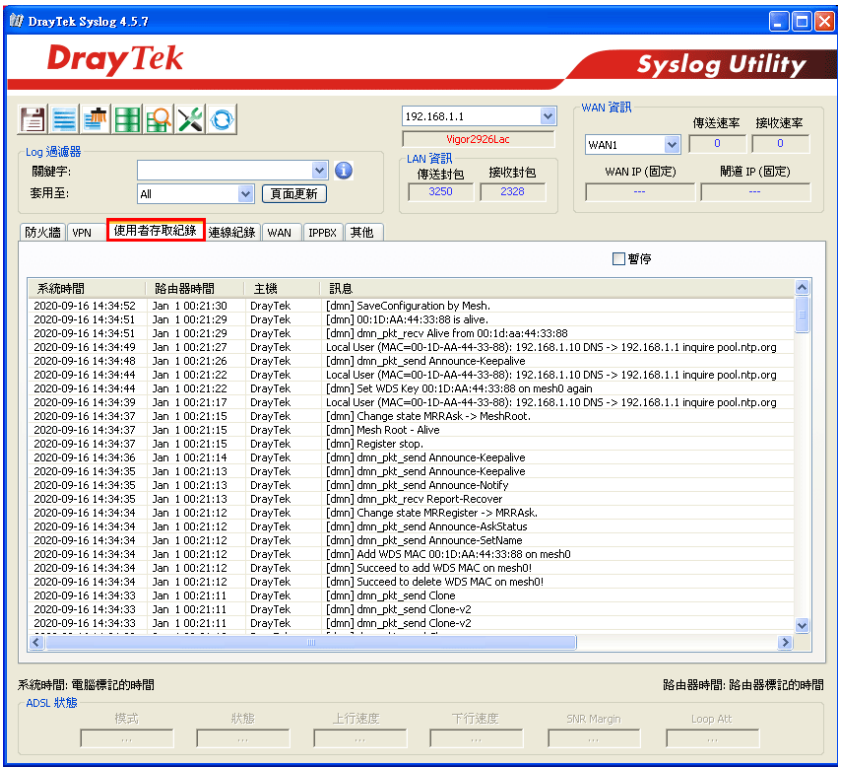
iPad se conecta a Root	: 80Mbps
El iPad se conecta al nodo hop1	: 49Mbps (Enlace ascendente RSSI : -55dBm)
El iPad se conecta al nodo hop2	: 41 Mbps (enlace ascendente RSSI: hop2 -64dBm / hop1 -55dBm)
iPad se conecta al nodo hop3	: 26Mbps (Enlace ascendente RSSI : hop3 -62dBm / hop2 -68dBm / hop1 - 55dBm)

- No se recomienda utilizar un Nodo de malla inalámbrico con un cable Ethernet conectado a una Raíz de malla.

- Si restablece una raíz de malla,
  - Se informará a todos los nodos de malla "conectados" para que se reinicien.
  - La lista de grupos y la clave de grupo también se restablecerán.
  - Para aquellos nodos de malla que no puedan restablecerse, restablézcalos manualmente. Restablezca la lista de grupos por defecto web o de fábrica.
- Si restablece un nodo de malla,
  - Se borrarán la lista de grupos y la clave de grupo.
  - El estado del enlace se convertirá en "Nuevo".
- Si Mesh Search / Apply / Discover funciona demasiado rápido o se realiza con un resultado vacío, su solicitud puede ser rechazada. Inténtalo de nuevo.
- Solución de problemas:
  - Compruebe la versión del firmware. Asegúrese de que todos los puntos de acceso dentro del grupo de malla tengan la versión de firmware más reciente.
  - Compruebe el modo OP (operación). Asegúrese de que el nuevo nodo de malla no obtenga accidentalmente una IP DHCP y se convierta en modo AP.
  - Consulta el código de país y los canales. Por ejemplo, es imposible conectar una raíz de malla VigorAP 912C con el canal 36 de 5G al nodo de malla inalámbrica VigorAP920R en el código de país de la UE.
  - Compruebe la carga del canal. Asegúrate de que no supere el 70 %.



  - Recopile algunos registros de malla y envíe el resultado a DrayTek para su análisis.



III-2-6 Lista de soporte

Mesh >> Support List

The following compatibility test lists DrayTek AP models supported by Vigor router Mesh.

Model	Status	Firmware Version
VigorAP 802	Y	1.3.6
VigorAP 903	Y	1.3.8
VigorAP 912C	Y	1.3.6
VigorAP 1000C	Y	1.3.5
VigorAP 960C	Y	1.4.0
VigorAP 1060C	Y	1.4.2

Y:Tested and is supported.
N:Not supported.

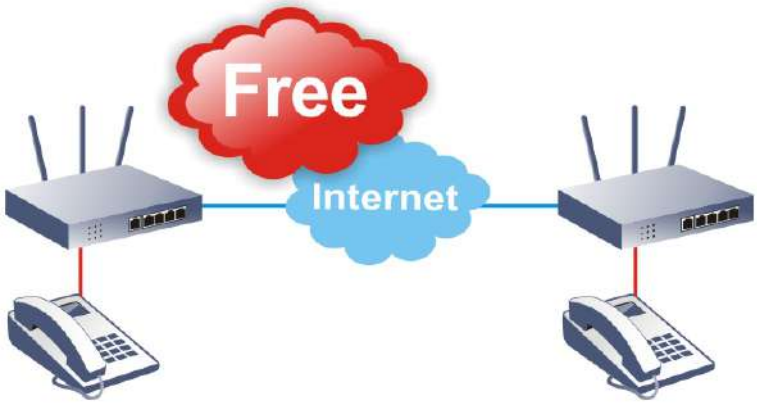
Esta página se deja en blanco.

Parte IV VoIP

La red de voz sobre IP (VoIP) le permite utilizar su conexión a Internet de banda ancha para realizar llamadas de voz con calidad de llamada de larga distancia a través de Internet.

IV-1VoIP

La red de voz sobre IP (VoIP) le permite utilizar su conexión a Internet de banda ancha para realizar llamadas de voz con calidad de llamada de larga distancia a través de Internet.



Información	Esta función se utiliza para los modelos “V”.

Existen muchos protocolos de señalización de llamadas diferentes, métodos mediante los cuales los dispositivos VoIP pueden comunicarse entre sí. Los protocolos más populares son SIP, MGCP, Megaco y H.323. Estos protocolos no son todos compatibles entre sí (excepto a través de un servidor de conmutación por software).

Los modelos Vigor V son compatibles con el protocolo SIP, ya que es una implementación ideal y conveniente para el ITSP (Proveedor de servicios de telefonía por Internet) y el softphone, y es ampliamente compatible. SIP es un protocolo de señalización de extremo a extremo que establece la presencia y la movilidad del usuario en la estructura de VoIP. Todo aquel que quiera hablar utilizando su Identificador Uniforme de Recursos SIP, “Dirección SIP”. El formato estándar de SIP URI es

sorbo: usuario: contraseña @ host: puerto

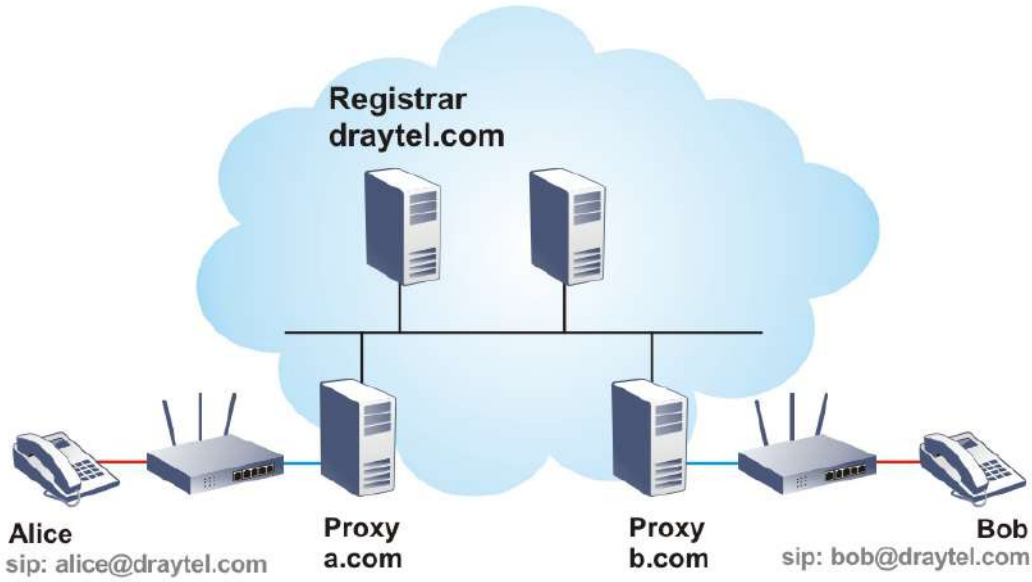
Algunos campos pueden ser opcionales en diferentes usos. En general, "host" se refiere a un dominio. La "información de usuario" incluye el campo de usuario, el campo de contraseña y el signo @ que los sigue. Esto es muy similar a una URL, por lo que algunos pueden llamarla "URL SIP". SIP admite pares -llamadas directas a pares y también llamadas a través de un servidor proxy SIP (una función similar a la del gatekeeper en las redes H.323), mientras que el protocolo MGCP utiliza una arquitectura cliente-servidor, siendo el escenario de llamadas muy similar a la red PSTN actual.

Después de configurar una llamada, los flujos de voz se transmiten a través de RTP (Protocolo de transporte en tiempo real). Se pueden incorporar diferentes códecs (métodos para comprimir y codificar la voz) en los paquetes RTP. Los modelos Vigor V ofrecen varios códecs, incluidos G.711 A/ley μ, G.723, G.726 y G.729 A y B. Cada códec utiliza un ancho de banda diferente y, por lo tanto, proporciona diferentes niveles de calidad de voz. Cuanto más ancho de banda utilice un códec, mejor será la calidad de la voz; sin embargo, el códec utilizado debe ser apropiado para su ancho de banda de Internet.

Llamadas a través de servidores SIP

En primer lugar, sus modelos Vigor V deberán registrarse en un registrador SIP mediante el envío de mensajes de registro para validar. Luego, los servidores proxy SIP de ambas partes reenviarán la secuencia de mensajes a la persona que llama para establecer la sesión.

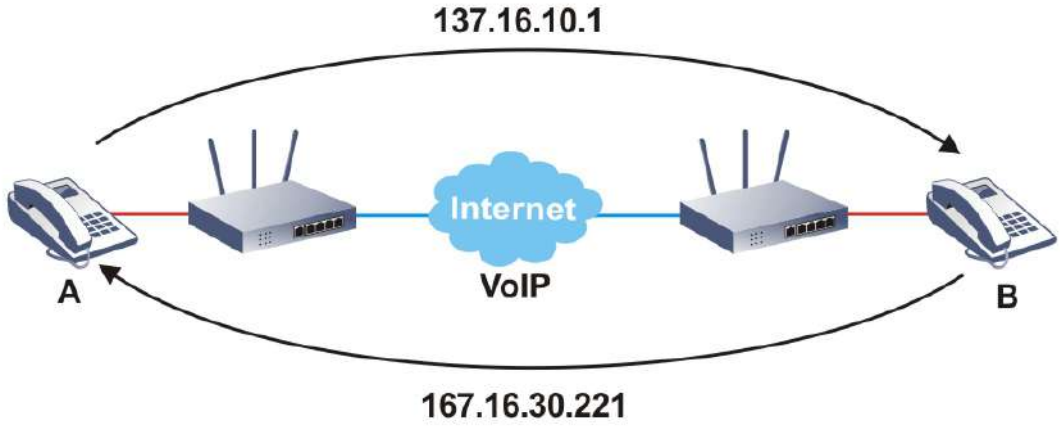
Si ambos se registran en el mismo registrador SIP, se ilustrará a continuación:



El principal beneficio de este modo es que no tiene que memorizar la dirección IP de su amigo, que puede cambiar con mucha frecuencia si es dinámica. En lugar de eso, solo tendrás que usar**plan de marcado**o marque directamente el de su amigo**nombre de la cuenta**si estás con el mismo Registrador SIP.

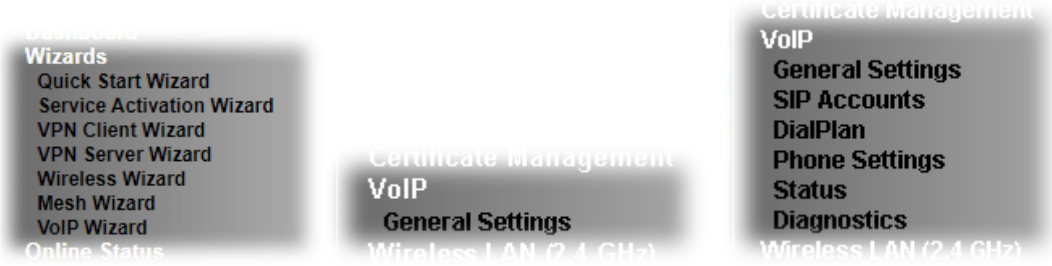
De igual a igual

Antes de llamar, debe conocer la dirección IP de su amigo. Los enrutadores VoIP de Vigor crearán una conexión entre ellos.



Los modelos Vigor V primero aplican códecs eficientes diseñados para hacer el mejor uso del ancho de banda disponible, pero los modelos Vigor V también están equipados con garantía QoS automática. QoS Assurance ayuda a asignar alta prioridad al tráfico de voz a través de Internet. Siempre tendrá el ancho de banda de entrada y salida requerido que se prioriza exclusivamente para el tráfico de voz a través de Internet, pero solo obtiene sus datos un poco más lentos y es tolerable para el tráfico de datos.

Nuestros modelos Vigor V primero aplican códecs eficientes diseñados para hacer el mejor uso del ancho de banda disponible, pero los modelos Vigor V también cuentan con garantía de QoS automática. QoS Assurance ayuda a asignar alta prioridad al tráfico de voz a través de Internet. Siempre tendrá el ancho de banda de entrada y salida requerido que se prioriza exclusivamente para el tráfico de voz a través de Internet, pero solo obtiene sus datos un poco más lentos y es tolerable para el tráfico de datos.



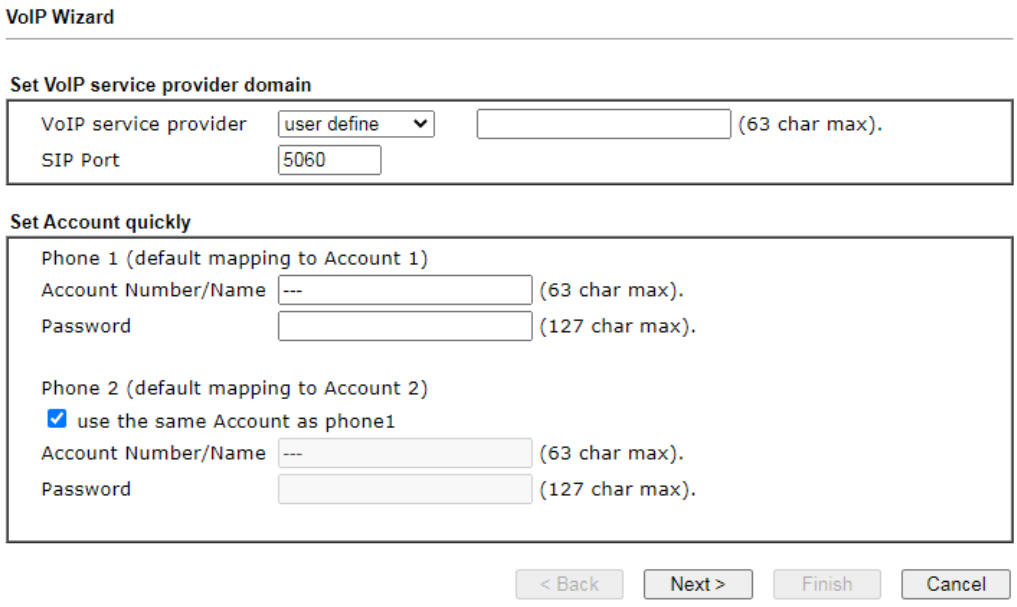
Asistente de VoIP IV-1-1

El enrutador Vigor ofrece un método rápido para configurar los ajustes de la aplicación VoIP. Siga los pasos que se enumeran a continuación.

Información	Este asistente está disponible solo para el modelo "V".

1. Abierto**Asistentes>>Asistente de VoIP**.

2. La pantalla de**Asistente VoIP**se mostrará de la siguiente manera.

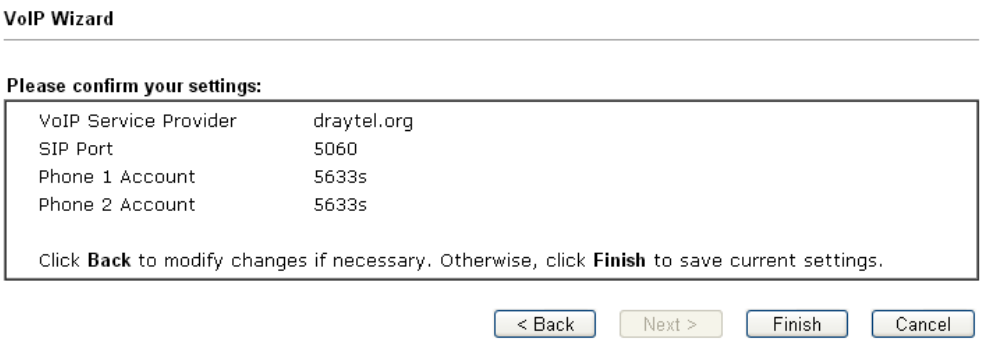


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Establecer servicio VoIP dominio del proveedor	**proveedor de servicios VoIP**-Utilice la lista desplegable para elegir el ISP que ofrece el servicio de VoIP para su enrutador. **Puerto SIP**–Utilice la configuración predeterminada (5060).
Establecer cuenta rápidamente	**Número de cuenta/Nombre**–Ingrese el número de cuenta/ nombre registrado en su ISP. **Contraseña**–Introduzca la contraseña de la cuenta registrada en su ISP.

	Usar la misma cuenta que el teléfono 1–Si no necesita configurar los ajustes del Teléfono 2, simplemente marque esta casilla.
Próximo	Haga clic en él para acceder a la siguiente página de configuración.
Cancelar	Haga clic en él para abandonar el asistente de VoIP.

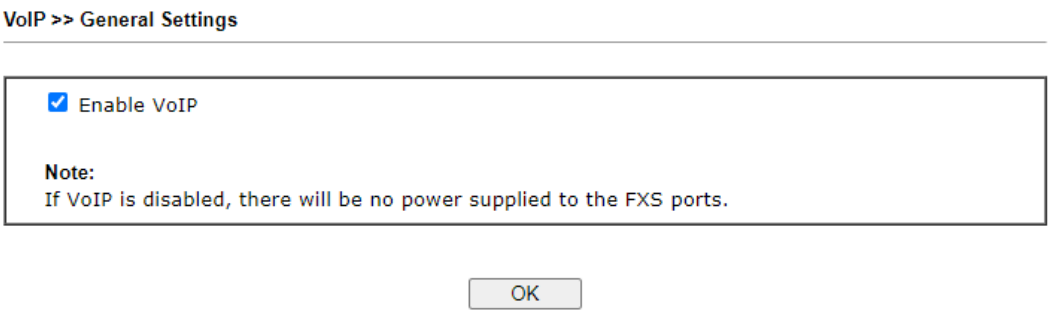
3. Después de terminar la configuración anterior, haga clic en**Próximo**para ver el resumen de dicha conexión.



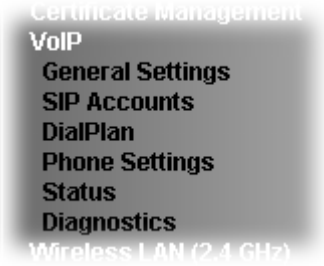
4. Haga clic en**Finalizar.**una pagina de**¡Configuración del asistente de VoIP OK!**aparecerá.

IV-1-2 Configuración general

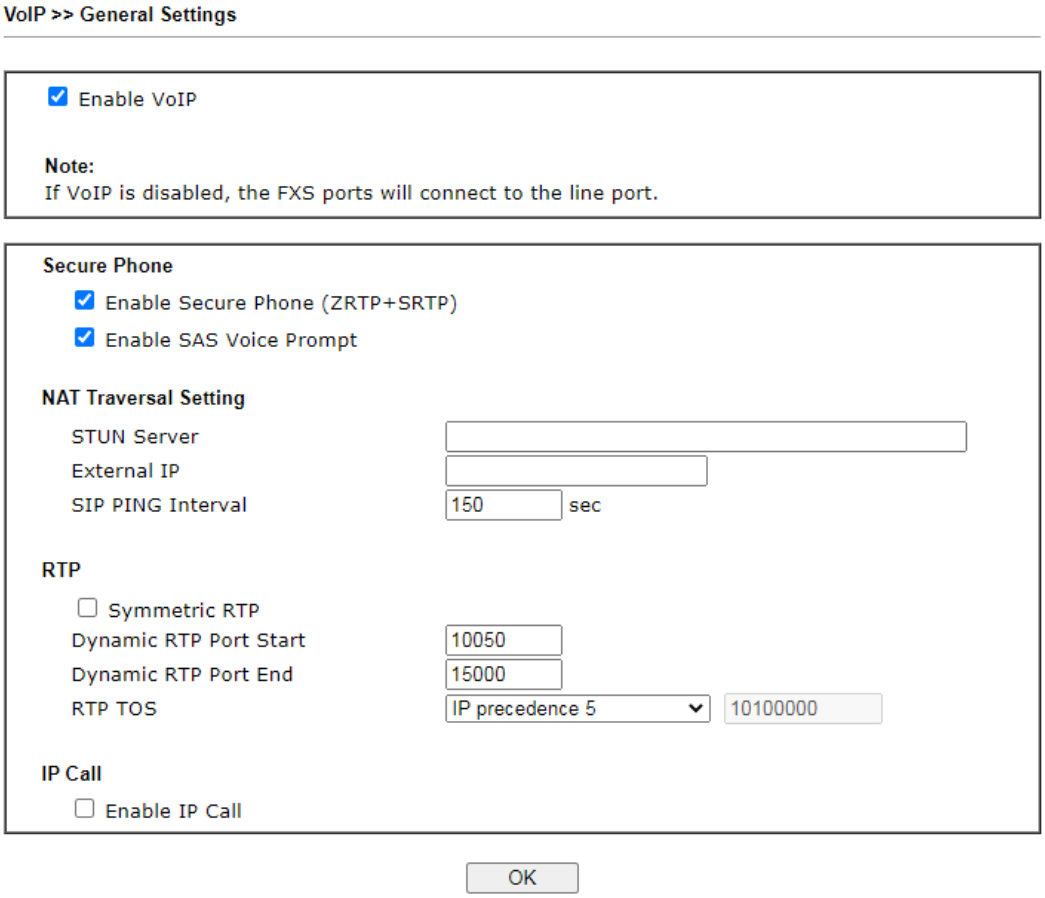
Abierto**VoIP>>Configuraciones generales**. Aparecerá la siguiente página. Marque la casilla de**Habilitar VoIP** y haga clic**DE ACUERDO**para abrir la página de configuración. De lo contrario, no se mostrará ninguna configuración.



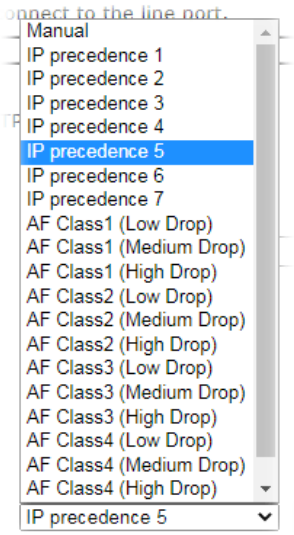
Después de marcar la casilla y hacer clic**DE ACUERDO**, los elementos del menú bajo VoIP se mostrarán de la siguiente manera.



De nuevo, abre**VoIP>>Configuraciones generales**. Aparece la siguiente página para configurar teléfono seguro, llamada IP; y establezca NAT Traversal Setting, RTP para la función VoIP.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
teléfono seguro	**Habilitar teléfono seguro**-Permite a los usuarios tener un flujo RTP encriptado con el lado del par usando el mismo protocolo (ZRTP+SRTP). Marque esta casilla para tener una llamada segura. **Habilitar mensaje de voz SAS -**Si está habilitado, se escuchará el aviso de SAS para ambos extremos cada vez. Si está deshabilitado, ya no se escuchará ningún aviso de SAS.
Configuración transversal de NAT	**Servidor STUN -**Escriba la dirección IP o el dominio del servidor STUN. **IP externa -**Escriba la dirección IP de la puerta de enlace. **Intervalo SIP PING -**El valor predeterminado es 150 (seg). Es útil para un servidor Nortel NAT Traversal Support.
RTP	**RTP simétrico**–Marque esta casilla para invocar la función. Para que la transmisión de datos a través de ambos extremos del enrutador local y del enrutador remoto no sea engañosa debido a la pérdida de IP (por ejemplo, enviar datos desde la IP pública del enrutador remoto a la IP privada del enrutador local), puede marcar esta casilla para resuelve este problema. **Inicio de puerto RTP dinámico**-Especifica el puerto de inicio para la transmisión RTP. El valor predeterminado es 10050. **Extremo de puerto RTP dinámico**-Especifica el puerto final para la transmisión RTP. El valor predeterminado es 15000. **Condiciones de servicio de RTP**–Decide el nivel del paquete de VoIP. Utilice la lista desplegable para elegir cualquiera de ellos. 
Llamada IP	**Habilitar llamada IP –**Permite que un usuario pueda marcar Llamadas IP salientes; y el enrutador Vigor podría recibir las llamadas IP entrantes.

Solicitud de Teléfono Seguro

Habilite el mensaje de voz de SAS, por ejemplo: si el enrutador vigor A llama al enrutador vigor B con verificación**Habilitar teléfono seguro**y**Habilitar mensaje de voz SAS**, entonces:

1. Después de establecer la conexión, el enrutador vigor A enviará el mensaje de voz SAS a A y el enrutador vigor B enviará el mensaje de voz SAS a B.
2. Luego, el tráfico RTP se asegura hasta que finaliza la llamada.

3. Si el enrutador vigor A quiere volver a llamar al enrutador vigor B la próxima vez, tanto A como B no volverán a escuchar ninguna indicación de voz, incluso comprobando**Habilitar mensaje de voz SAS**en la interfaz de usuario web. Significa que solo la primera llamada entre ellos tendrá un mensaje de voz.

Habilite el mensaje de voz de SAS, por ejemplo: si el enrutador vigor A llama al enrutador vigor B con verificación**Habilitar teléfono seguro**pero no**Habilitar mensaje de voz SAS**, entonces:

1. Una vez establecida la conexión, el vigor router A**NO**envíe la indicación de voz SAS al enrutador vigor A y el enrutador vigor B NO enviará la indicación de voz SAS al enrutador vigor B.

2. Incluso sin aviso de voz, pero el tráfico RTP aún está seguro hasta que finaliza la llamada.

Información

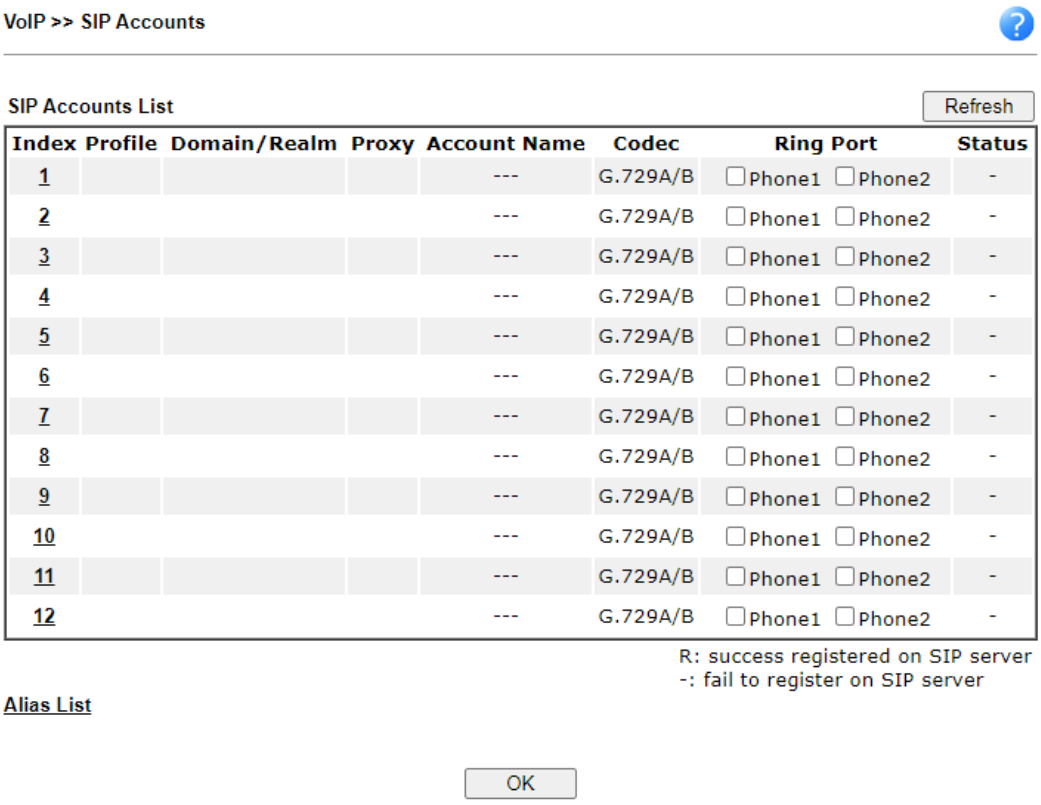
Si las llamadas entrantes o salientes no coinciden con ninguna entrada de la agenda, el router intentará que la llamada "esté protegida". Pero, si la llamada termina "desprotegida" (por ejemplo, el lado del par no es compatible con ZRTP+SRTP), el enrutador no reproducirá un mensaje de advertencia.

IV-1-3 Cuentas SIP

En esta sección, configura su propia configuración de SIP. Cuando solicite una cuenta, su proveedor de servicios SIP le dará una**Nombre de la cuenta**o usuario,**Registrador SIP, Proxy,**y **Nombre de dominio**. (Los tres últimos podrían ser los mismos en algún caso). Luego puede decirle a sus amigos su dirección SIP como en **Nombre de cuenta @ Nombre de dominio**

Cuando el enrutador Vigor VoIP está encendido, primero se registrará con el registrador usando AuthorizationUser@Domain /Realm. Después de eso, SIP Proxy desviará su llamada al destino utilizando AccountName@Domain /Realm como identidad.

Información	Los elementos de selección para Ring Port diferirán según el enrutador que tenga.

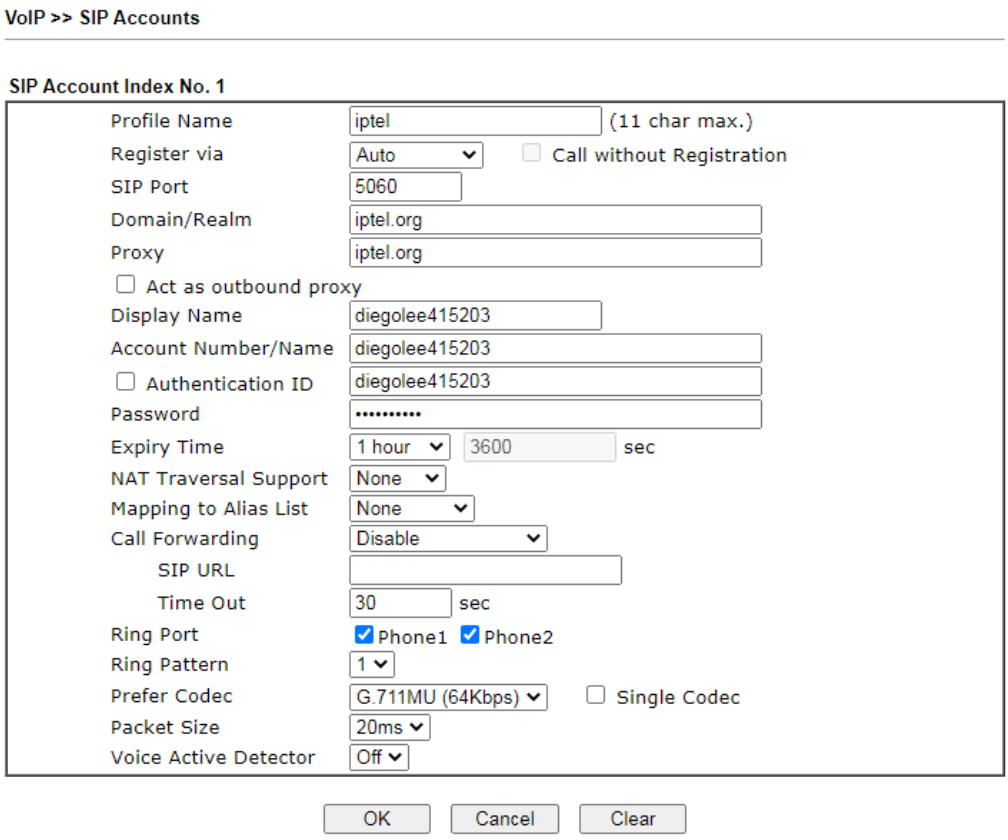


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Índice	Haga clic en este enlace para acceder a la página siguiente para configurar la cuenta SIP.
Perfil	Muestra el nombre de perfil de la cuenta.
Dominio/Reino	Muestra el nombre de dominio o la dirección IP del servidor de registro SIP.
Apoderado	Muestra el nombre de dominio o la dirección IP del servidor proxy SIP.
Nombre de la cuenta	Muestra el nombre de cuenta de la dirección SIP antes de @.
códec	Muestra el tipo de códec para la cuenta.
Puerto de anillo	Especifique qué puerto sonará cuando reciba una llamada telefónica.

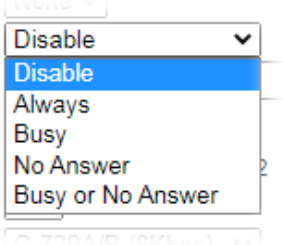
Estado	Muestra el estado de la cuenta SIP correspondiente.**R**significa que dicha cuenta está registrada en el servidor SIP con éxito.**–**significa que la cuenta no se pudo registrar en el servidor SIP.
Lista de alias	Le permite establecer múltiples nombres de alias SIP.

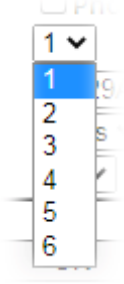
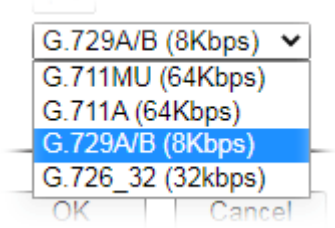
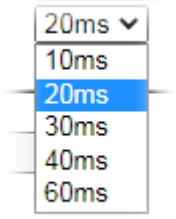
Haga clic en cualquier enlace de índice para acceder a la página siguiente para configurar la cuenta SIP.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre de perfil	Asigne un nombre a este perfil para identificarlo. Puede escribir un nombre similar con el dominio. Por ejemplo, si el nombre de dominio es*Draytel.org*, entonces podría establecer*Draytel-1*en este campo.
Regístrese a través de	Si desea realizar una llamada VoIP sin registrar información personal, elija**Ninguno**y marque la casilla para lograr el objetivo. Algunos servidores SIP permiten al usuario utilizar la función VoIP sin registrarse. Para dicho servidor, marque la casilla de**Llame sin registro**. Elegir**Auto**es recomendado. El sistema seleccionará una forma adecuada para su llamada VoIP.
Puerto SIP	Configure el número de puerto para enviar/recibir mensajes SIP para crear una sesión. El valor predeterminado es**5060.**Su compañero debe establecer el mismo valor en su Registrador.
Dominio/Reino	Configure el nombre de dominio o la dirección IP del servidor SIP Registrar.
Apoderado	Establezca el nombre de dominio o la dirección IP del servidor proxy SIP. Para cuando puedas escribir**:número de puerto**después del nombre de dominio para especificar ese puerto como el destino de la transmisión de datos

	(p.ej,**nat.draytel.org:5065**)
Actuar como proxy saliente	Marque esta casilla para que el proxy actúe como proxy de salida.
Nombre para mostrar	El identificador de llamadas que desea que se muestre en la pantalla de su amigo.
Número de cuenta/Nombre	Ingrese su nombre de cuenta de dirección SIP, por ejemplo, cada texto antes de @.
ID de autenticación	Marque la casilla para invocar esta función e ingrese el nombre o el número utilizado para la Autorización SIP con el Registrador SIP. Si este valor de configuración es el mismo que el Nombre de la cuenta, no es necesario que marque la casilla y establezca ningún valor en este campo.
Contraseña	La contraseña que se le proporcionó cuando se registró en un servicio SIP.
Tiempo de expiración	La duración de tiempo que su servidor SIP Registrar mantiene su registro. Antes de que expire el tiempo, el enrutador volverá a enviar otra solicitud de registro al registrador SIP.
Compatibilidad con NAT transversal	Si el enrutador (p. ej.,enrutador de banda ancha) que utiliza se conecta a Internet mediante otro dispositivo, debe configurar esta función para su necesidad. **Ninguno -**Desactive esta función. **Aturdir**–Elija esta opción si se proporciona un servidor Stun para su enrutador. **Manual**–Elija esta opción si desea especificar una dirección IP externa como soporte transversal de NAT. **Nortel**–Si el conmutador de software que utiliza es compatible con la solución de Nortel, puede elegir esta opción.
Asignación a la lista de alias	Seleccione uno de los perfiles de alias.
Reenvío de llamadas	Hay cuatro opciones para que usted elija.**Desactivar**es cerrar la función de desvío de llamadas.**Siempre**significa que todas las llamadas entrantes se reenviarán a la URL de SIP sin ningún motivo.**Ocupado** significa que las llamadas entrantes se reenviarán a la URL de SIP solo cuando el sistema local esté ocupado.**Sin respuesta**significa que si las llamadas entrantes no reciben ninguna respuesta, se reenviarán a la URL de SIP cuando finalice el tiempo.  **URL SIP**–Escriba la URL de SIP (p. ej., aaa@draytel.org o abc@iptel.org) como el sitio para el desvío de llamadas. **Se acabó el tiempo**–Configure el tiempo de espera para el desvío de llamadas. La configuración predeterminada es 30 seg.
Puerto de anillo	Configure el Teléfono 1 y/o el Teléfono 2 como los puertos de timbre predeterminados para esta cuenta SIP.
patrón de anillo	Elija un tipo de tono de llamada para la llamada telefónica VoIP.

	
Preferir códec	Seleccione uno de los cinco códecs como predeterminado para sus llamadas VoIP. El códec utilizado para cada llamada se negociará con la otra parte antes de cada sesión y, por lo tanto, es posible que no sea su opción predeterminada. El códec predeterminado es G.729A/B; ocupa poco ancho de banda manteniendo una buena calidad de voz. Si su velocidad de subida es de solo 64 Kbps, no use el códec G.711. Es mejor que tenga al menos 256 Kbps de subida si desea utilizar G.711.  **Códec único**–Si la casilla está marcada, solo se aplicará el códec seleccionado.
Tamaño del paquete	La cantidad de datos contenidos en un solo paquete. El valor predeterminado es 20 ms, lo que significa que el paquete de datos contendrá 20 ms de información de voz. 
Detector activo de voz	Esta función puede detectar si la voz en ambos lados está activa o no. De lo contrario, el enrutador hará algo para guardar el ancho de banda para otros usos. Hacer clic**En**para invocar esta función; hacer clic**Apagado** para cerrar la función.

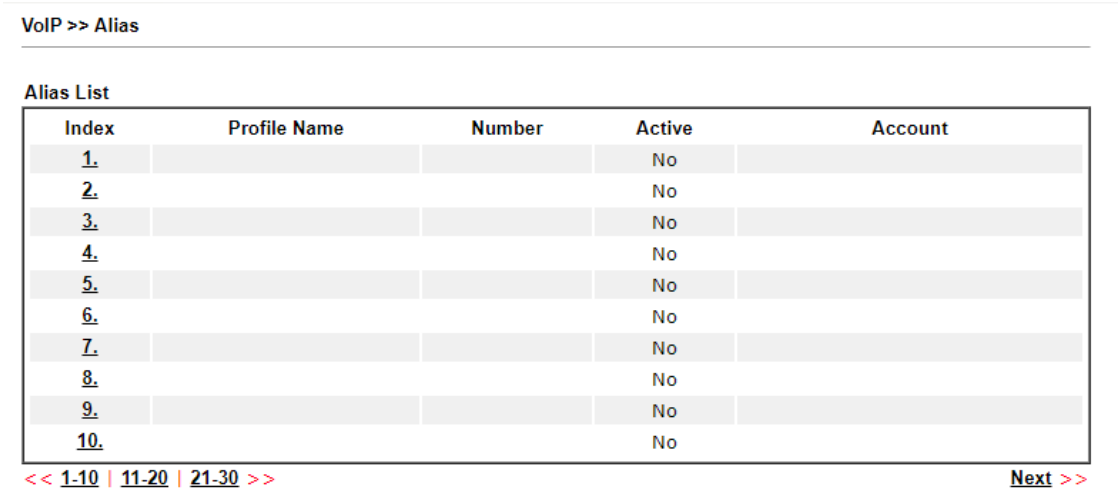
Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

IV-1-3-1 Lista de alias

Esta página enumera todos los perfiles de alias SIP.

Un alias SIP es como un número de extensión en el que las personas pueden marcarlo para comunicarse directamente con una persona específica. Normalmente, cuando tiene una cuenta de usuario para un ITSP, el ITSP le proporcionará una cuenta SIP. Sin embargo, con esta función, puede tener varios alias SIP en una cuenta SIP. Cuando se registra con una cuenta de usuario regular, el alias se registra así como la cuenta SIP principal. Luego, cuando alguien marque el alias, sonará el SIP URI vinculado al alias.

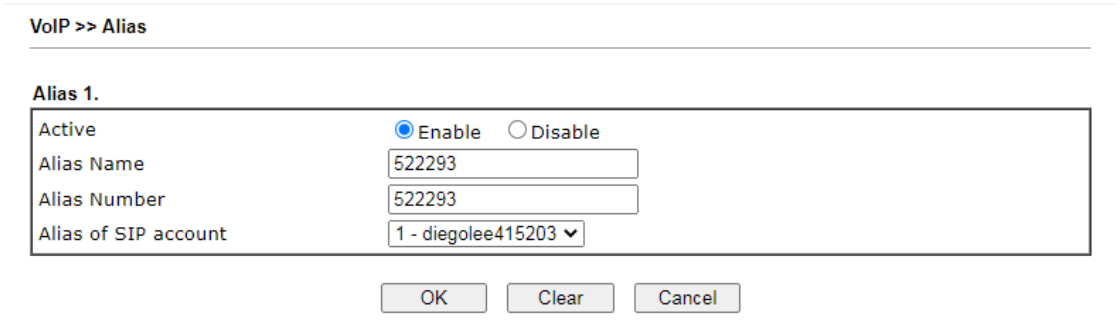
Haga clic en el**Lista de alias**enlace para acceder a la página de configuración como se muestra a continuación.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Índice	Haga clic en el enlace del número para cada perfil.
Nombre de perfil	Muestra el nombre de alias para dicha subcuenta.
Número	Muestra el número de teléfono de dicha cuenta.
Activo	Muestra el estado de activación actual de dicha cuenta, habilitada o deshabilitada.
Cuenta	Muestra el número de cuenta SIP para dicha subcuenta adjunta.

Puede configurar 30 perfiles como alias. Haga clic en el número debajo de Índice para establecer una configuración detallada.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Activo	Hacer clic**Permitir**para activar esta entrada. O haga clic en**Desactivar**para inactivar esta entrada.
Apodo	Especifique un nombre para un número de alias.
Número de alias	Introduzca un número de alias. Los números de alias se obtienen de su ITSP.
Alias de cuenta SIP	Elija uno de los elementos enumerados en la lista de cuentas SIP para este perfil de alias.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

VoIP >> Alias

Alias List

Index	Profile Name	Number	Active	Account
1.	522293	522293	Yes	diegolee415203
2.			No	
3.			No	
4.			No	
5.			No	
6.			No	
7.			No	
8.			No	
9.			No	
10.			No	

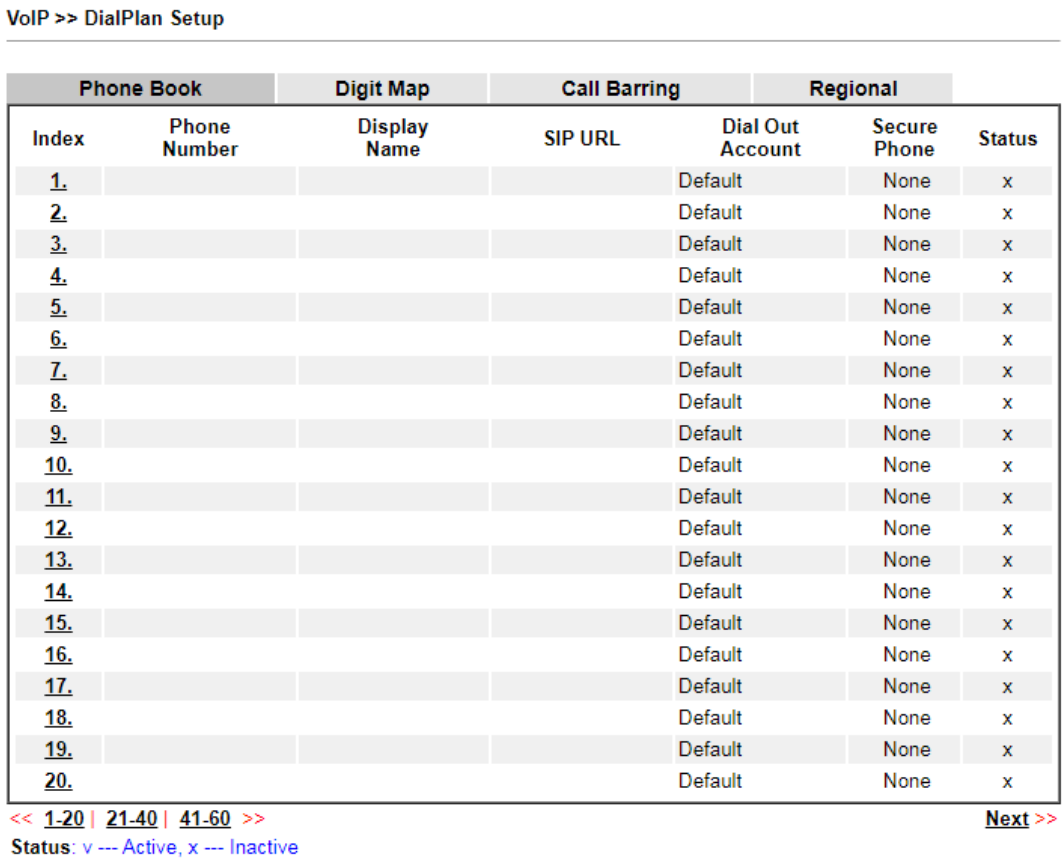
<< 1-10 | 11-20 | 21-30 >> Next >>

Plan de marcación IV-1-4

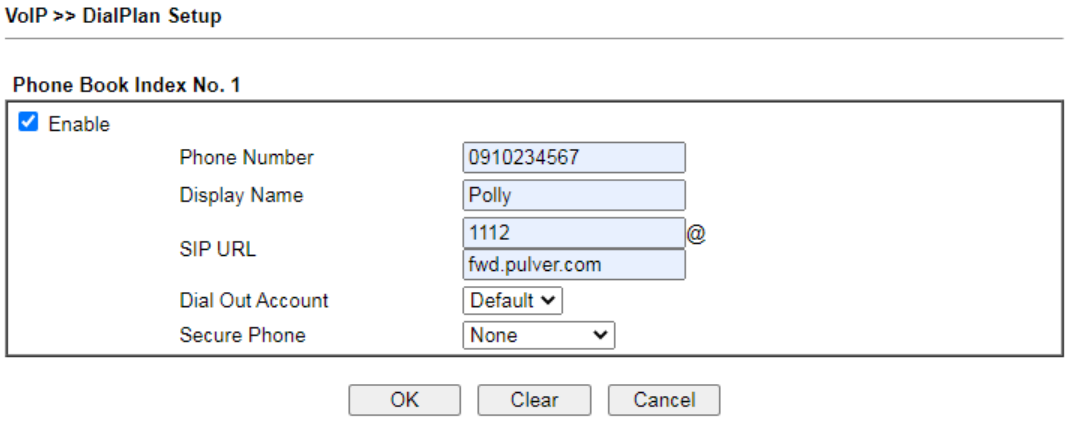
Esta página le permite establecer la guía telefónica, el mapa de dígitos, la restricción de llamadas y la configuración regional para la función VoIP. Haga clic en los enlaces de esta página para acceder a las siguientes páginas para obtener configuraciones detalladas.

IV-1-4-1 Directorio telefónico

En esta sección, puede configurar sus contactos de VoIP en la “agenda telefónica”. Puede ayudarlo a realizar llamadas de forma rápida y sencilla mediante el uso de "marcación rápida"**Número de teléfono**. Hay un total de 60 entradas de índice en la agenda telefónica para que almacene todas las direcciones SIP de sus amigos y familiares.**Bucle a través**y **Número de teléfono de respaldo**se mostrará si está utilizando la serie Vigor2927 para configurar la guía telefónica.



Haga clic en cualquier número de índice para mostrar la página de configuración del plan de marcación.



Los ajustes disponibles se explican a continuación:

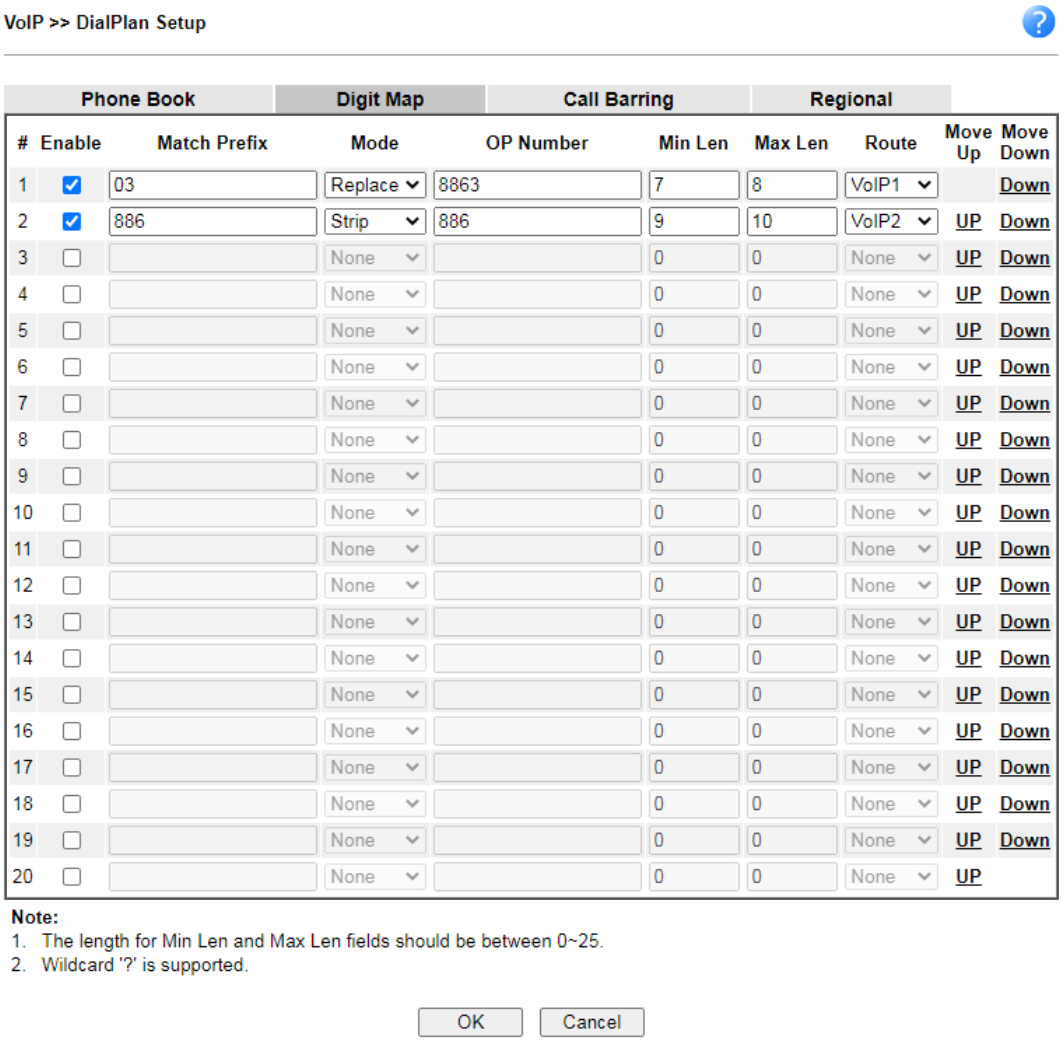
Artículo	Descripción
Permitir	Haga clic aquí para habilitar esta entrada.
Número de teléfono	El número de marcación rápida de este índice. Puede ser cualquier número que elijas, usando dígitos**0-9**y*****.
Nombre para mostrar	El identificador de llamadas que desea que se muestre en la pantalla de su amigo. Esto le permite a su amigo saber fácilmente quién está llamando sin tener que memorizar muchas direcciones URL SIP.
URL SIP	Ingrese la dirección SIP de su amigo.
Cuenta de marcación	Elija una de las cuentas SIP para este perfil para marcar. Es útil para ambos lados (persona que llama y persona que llama) que se registraron en diferentes servidores SIP Registrar. Si la persona que llama y la persona que llama no usan el mismo servidor SIP, a veces, la conexión de la llamada telefónica VoIP puede no tener éxito. Mediante el uso de la cuenta de acceso telefónico especificada, se puede asegurar la conexión exitosa.
teléfono seguro	**ZRTP+SRTP**-Permite a los usuarios tener un flujo RTP encriptado con el lado del par usando el mismo protocolo (ZRTP+SRTP). Marque esta casilla para tener una llamada segura.
Cancelar	Volver a la página web anterior.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

Información	Si las llamadas entrantes o salientes no coinciden con ninguna entrada de la agenda, el router intentará que la llamada "esté protegida". Pero, si la llamada termina "desprotegida" (por ejemplo, el lado del par no es compatible con ZRTP+SRTP), el enrutador no reproducirá un mensaje de advertencia.

Mapa de IV-1-4-2 dígitos

Para comodidad del usuario, esta página permite a los usuarios editar el número de prefijo para la cuenta SIP agregando un número, eliminando un número o reemplazando un número. Se utiliza para ayudar al usuario a tener una forma rápida y fácil de marcar a través de la interfaz de VoIP.



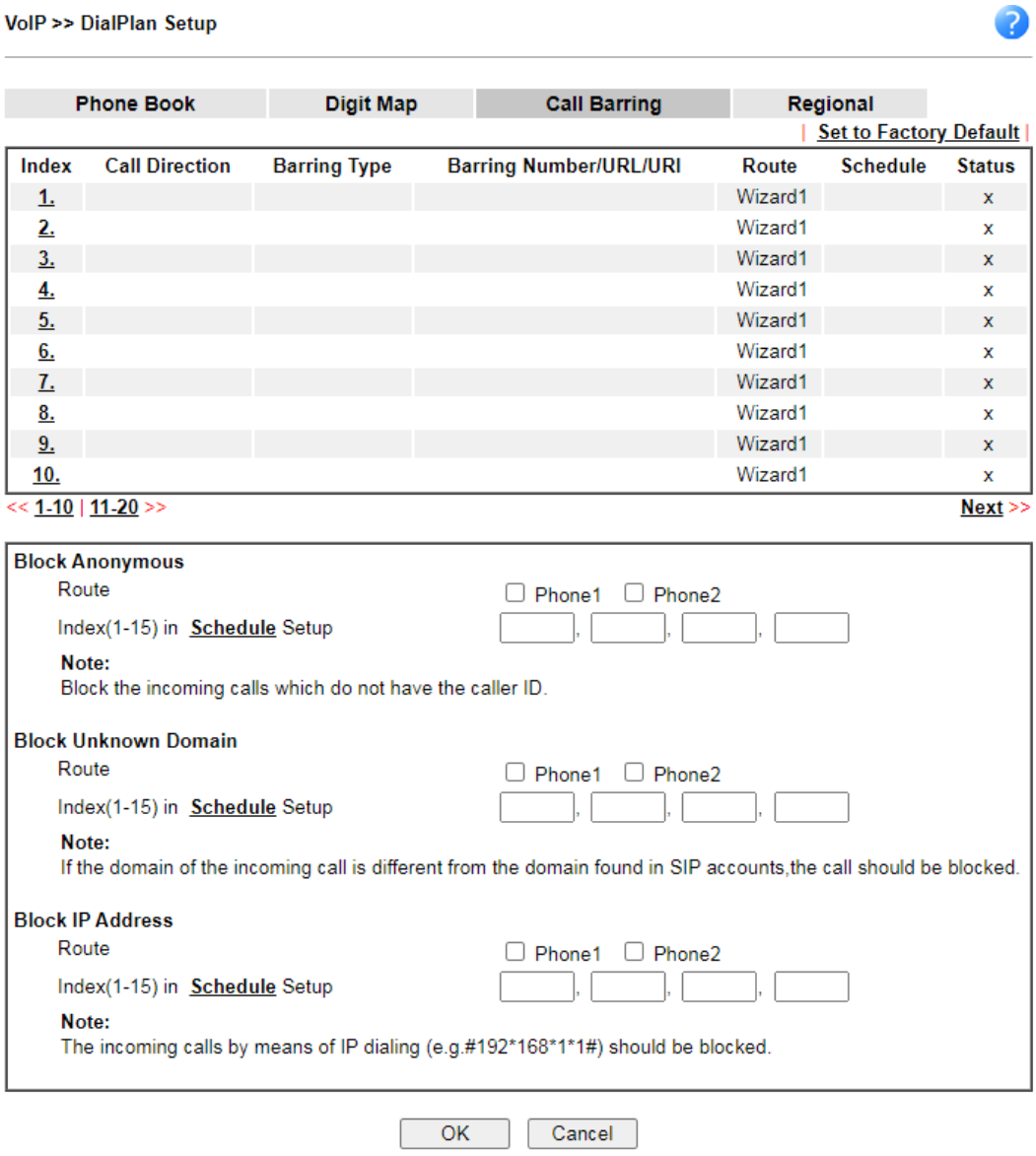
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Marque esta casilla para invocar esta configuración.
Prefijo de coincidencia	Se usa para coincidir con el número que marcó y puede ser modificado por la acción (agregar, quitar o reemplazar) con el **Número OP**.
Modo	**Ninguno**-Sin acción **Agregar**-Cuando elige este modo, el número OP se agregará antes del número de prefijo de coincidencia para llamar a través de la ruta específica. **Banda**-Cuando elige este modo, el número de prefijo de coincidencia parcial o total se eliminará de acuerdo con el número de OP. Tome la imagen de arriba (página web de configuración de la tabla de prefijos) como ejemplo, el número OP de*886*se eliminará por completo para el número de prefijo de coincidencia se establece con*886*. **Reemplazar**-Cuando elige este modo, el número OP será reemplazado por el número de prefijo para llamar a través de la interfaz VoIP específica. Tome la imagen de arriba (página web de configuración de la tabla de prefijos) como ejemplo, el número de prefijo 03 se reemplazará por 8863. Por ejemplo: el número de marcación de "031111111" se cambiará a "88631111111" y se enviará al servidor SIP.

Número OP	El número frontal que ingresa aquí es la primera parte del número de cuenta que desea ejecutar una función especial (según el modo elegido) utilizando el número de prefijo.
Duración mínima	Establezca la longitud mínima del número de marcación para aplicar la configuración del número de prefijo. Tome la imagen de arriba (página web de configuración de la tabla de prefijos) como ejemplo, si el número de marcado está entre 7 y 9, ese número puede aplicar la configuración de número de prefijo aquí.
max len	Establezca la longitud máxima del número de marcación para aplicar la configuración del número de prefijo.
Ruta	Elija el que desea habilitar la configuración del número de prefijo de las cuentas SIP guardadas. Primero configure una cuenta SIP para que esta interfaz esté disponible. Este elemento se cambiará de acuerdo con la configuración del puerto configurada en **VoIP>> Configuración del teléfono**.
Mover ARRIBA / Mover Abajo	Haga clic en el enlace para mover la entrada seleccionada hacia arriba o hacia abajo.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

La restricción de llamadas se utiliza para bloquear las llamadas telefónicas que provienen del que no es bienvenido.



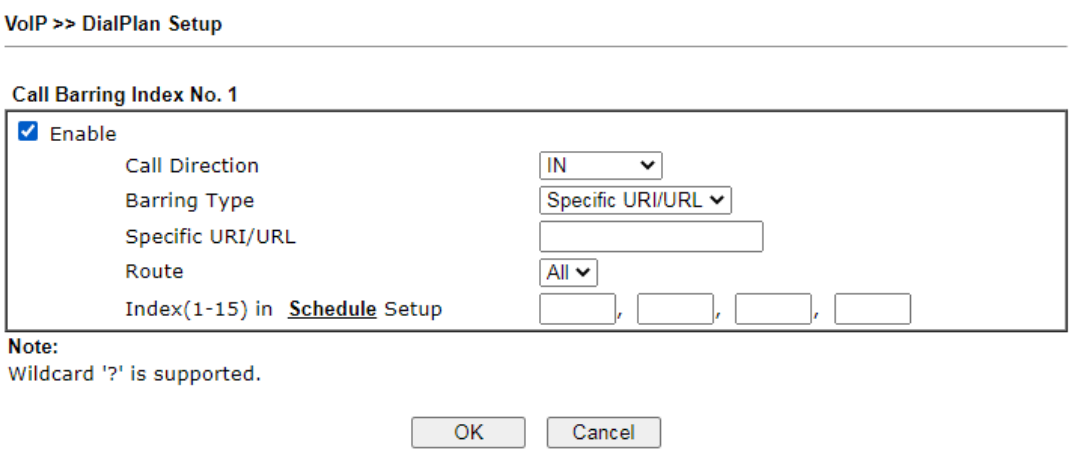
Además, puede establecer configuraciones avanzadas para la restricción de llamadas, como**Bloquear anónimo**,**Bloquear dominio desconocido**o**Bloquear dirección IP**.

Para**Bloquear anónimo -**esta función puede bloquear las llamadas entrantes sin identificador de llamadas en la interfaz (Puerto del teléfono) especificada en la siguiente ventana. Dicho control también se puede realizar en base a horarios preconfigurados.

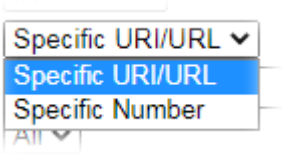
Para**Bloquear dominio desconocido –**esta función puede bloquear las llamadas entrantes (a través del puerto del teléfono) de un dominio no reconocido que no está especificado en las cuentas SIP. Dicho control también se puede realizar en base a horarios preconfigurados.

Para**Bloquear dirección IP –**esta función puede bloquear las llamadas entrantes (a través del puerto del teléfono) provenientes de la dirección IP. Dicho control también se puede realizar en base a horarios preconfigurados.

Haga clic en cualquier número de índice para mostrar la página de configuración de restricción de llamadas.

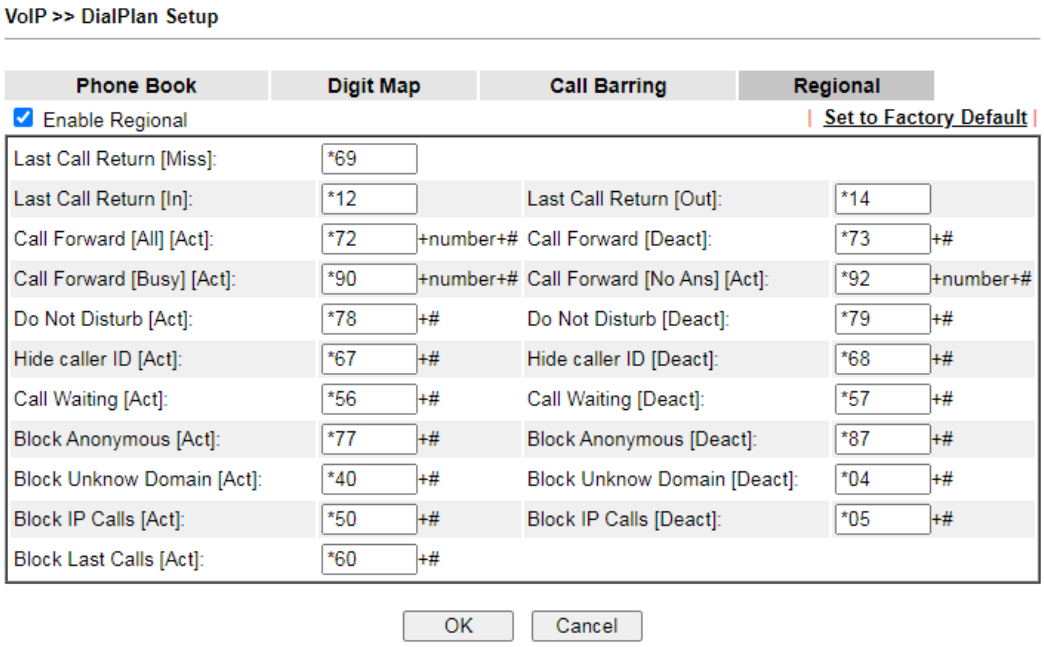


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Márquelo para habilitar esta entrada.
Dirección de llamada	Determine la dirección de la llamada telefónica, ENTRADA: llamada entrante, SALIDA-llamada saliente, ENTRADA y SALIDA: llamadas entrantes y salientes.
Tipo de restricción	Determine el tipo de llamada telefónica VoIP, URI/URL o número. 
URI/URL específico o Número específico	Este campo se cambiará según el tipo que haya seleccionado para Tipo de restricción.
Ruta	**Todo**significa que todas las llamadas telefónicas se bloquearán con dicho mecanismo.
Índice (1-15) en Horario	Ingrese al índice de perfiles de horarios para controlar la restricción de llamadas de acuerdo con los horarios preconfigurados. Consulte la sección **Aplicaciones>>Horario**para una configuración detallada.

IV-1-4-4 Regionales

Esta página le permite procesar llamadas telefónicas entrantes o salientes por región. Los valores predeterminados (usados comúnmente en la mayoría de las áreas) se mostrarán en esta página web. Tú***puede cambiar***el número según la región en la que se encuentra el enrutador.



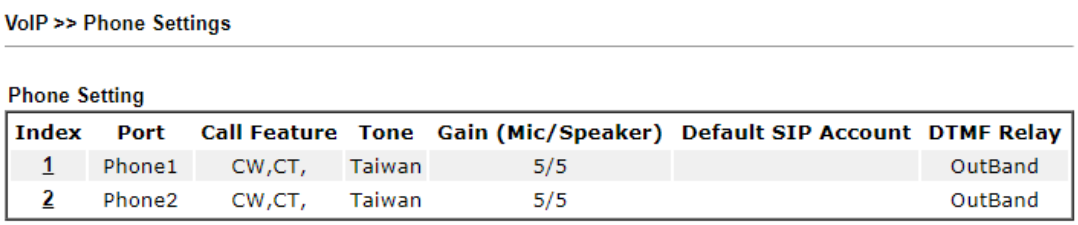
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar regional	Marque esta casilla para habilitar esta función.
Devolución de última llamada [Señorita]	A veces, las personas pueden perder algunas llamadas telefónicas. Marque el número escrito en este campo para saber de dónde proviene la última llamada telefónica y vuelva a llamar a esa.
Devolución de última llamada [En]	Ha finalizado una llamada telefónica entrante, sin embargo, desea volver a llamar por algún motivo. Marque el número escrito en este campo para volver a llamar a ese.
Devolución de última llamada [Fuera]	Marque el número escrito en este campo para volver a llamar a la llamada telefónica saliente anterior.
Desvío de llamadas [Todo][Act]	Marque el número escrito en este campo para desviar todas las llamadas entrantes al lugar especificado.
Desvío de llamadas [desactivar]	Marque el número escrito en este campo para liberar la función de desvío de llamadas.
Desvío de llamadas [Ocupado][Act.]	Marque el número escrito en este campo para desviar todas las llamadas entrantes al lugar especificado mientras el teléfono está ocupado.
Desvío de llamadas [No Respuesta][Acto]	Marque el número escrito en este campo para desviar todas las llamadas entrantes al lugar especificado mientras no haya respuesta del teléfono conectado.
No molestar [Act.]	Marque el número escrito en este campo para invocar la función de DND.
No molestar [Desactivar]	Marque el número escrito en este campo para liberar la función DND.

Ocultar identificador de llamadas [Act]	Marque el número escrito en este campo para que su número de teléfono (ID) no se muestre en el panel de visualización del extremo remoto.
Ocultar identificador de llamadas [Desactivar]	Marque el número escrito en este campo para liberar esta función.
Llamada en espera [actuar]	Marque el número escrito en este campo para que todas las llamadas entrantes esperen su respuesta.
Llamada en espera [desactivar]	Marque el número escrito en este campo para liberar esta función.
Bloquear Anónimo[Act]	Marque el número escrito en este campo para bloquear todas las llamadas entrantes con identificación desconocida.
Bloquear Anónimo[Desactivar]	Marque el número escrito en este campo para liberar esta función.
Bloquear dominio desconocido [Acto]	Marque el número escrito en este campo para bloquear todas las llamadas entrantes de un dominio desconocido.
Bloquear dominio desconocido [Desactivar]	Marque el número escrito en este campo para liberar esta función.
Bloquear llamadas IP [Act]	Marque el número escrito en este campo para bloquear todas las llamadas entrantes desde la dirección IP.
Bloquear llamadas IP [Desactivar]	Marque el número escrito en este campo para liberar esta función.
Bloquear últimas llamadas [Act]	Marque el número escrito en este campo para bloquear la última llamada telefónica entrante.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

Esta página permite al usuario establecer la configuración del teléfono para el Teléfono 1 y el Teléfono 2 respectivamente. Sin embargo, cambia ligeramente según el modelo que tenga.



VoIP >> Phone Settings

Phone Setting

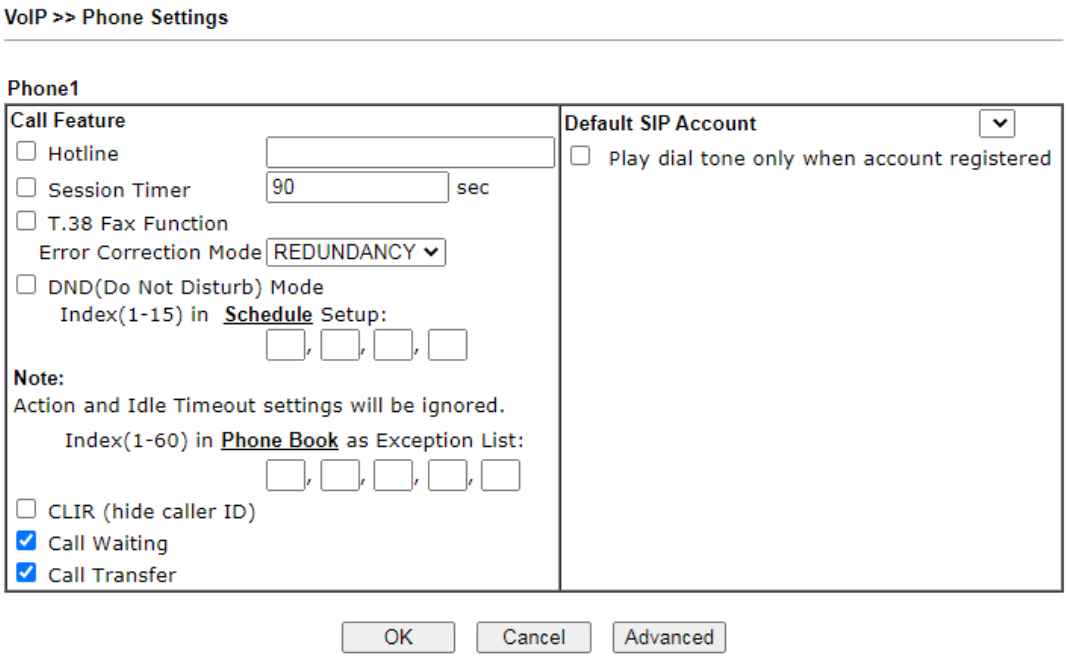
Index	Port	Call Feature	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay
1	Phone1	CW,CT,	Taiwan	5/5		OutBand
2	Phone2	CW,CT,	Taiwan	5/5		OutBand

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Configuración del teléfono	**Índice –**aquí se proporcionan dos puertos telefónicos para que los configure. **Puerto -**Muestra phone1 y phone2. **función de llamada**–Se mostrará una breve descripción de la función de llamada en este campo para su referencia. **Tono**-Muestra la configuración de tono que se configuró en la página de configuración avanzada de Phone Index. **Ganar**-Muestra la configuración de ganancia de volumen para Micrófono/Altavoz que se configuró en la página de configuración avanzada de Phone Index. **Cuenta SIP predeterminada**– "draytel_1" es la cuenta SIP predeterminada. Puede hacer clic en el número debajo del campo Índice para cambiar la cuenta SIP para cada puerto telefónico. **Relé DTMF**–Muestra el modo DTMF que se configuró en la página de configuración avanzada de Phone Index.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

Haga clic en el enlace del número de índice para el puerto del teléfono, puede acceder a la siguiente página para configurar los ajustes del teléfono.

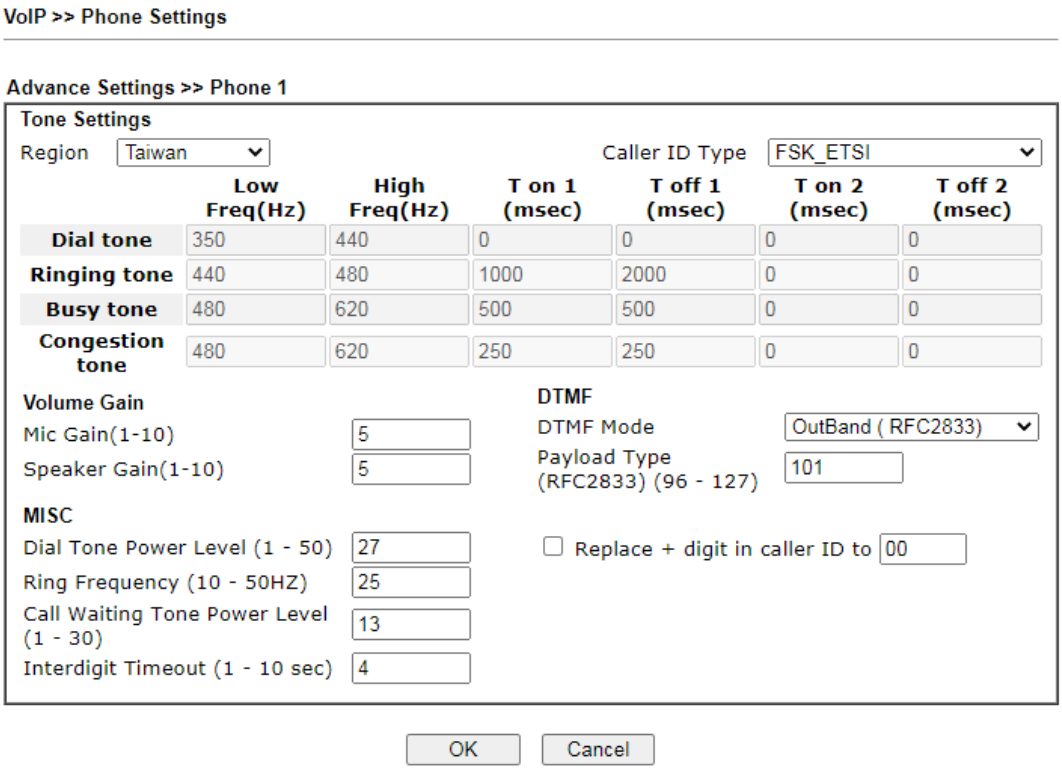


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
línea directa	Marque la casilla para habilitarlo. Escriba la URL de SIP en el campo para marcar automáticamente cuando descuelgue el teléfono.
Temporizador de sesión	Marque la casilla para habilitar la función. En el tiempo limitado que establezca en este campo, si no hay respuesta, la llamada de conexión se cerrará automáticamente.
Función de fax T.38	Marque la casilla para habilitar la función de fax T.38. **Modo de corrección de errores –**elija un modo para la corrección de errores.
Modo DND (No molestar)	Establezca un período de tiempo de paz sin molestar por llamadas telefónicas VoIP. Durante el período, el que marque escuchará el tono de ocupado, pero el usuario local no escuchará ningún tono de llamada. **Índice (1-15) en Horario -**Ingrese al índice de perfiles de horarios para controlar cuándo sonará el teléfono y cuándo no de acuerdo con los horarios preconfigurados. Consulte la sección**Aplicación >>Horario**para una configuración detallada. **Índice (1-60) en la guía telefónica -**Introduzca el índice de los perfiles de la guía telefónica. Consulte la sección**DialPlan – Directorio telefónico**para una configuración detallada.
CLIR (ocultar identificador de llamadas)	Marque esta casilla para ocultar el identificador de llamadas en el panel de visualización del teléfono.
Llamada en espera	Marque esta casilla para invocar esta función. Aparecerá un sonido de aviso para decirle al usuario que hay una nueva llamada telefónica esperando su respuesta. Haga clic en gancho flash para atender la llamada telefónica en espera.
Transferencia de llamada	Marque esta casilla para invocar esta función. Haga clic en gancho flash para iniciar otra llamada telefónica. Cuando la conexión de la llamada telefónica se realice correctamente, cuelgue el teléfono. Entonces, los otros dos lados pueden comunicarse.

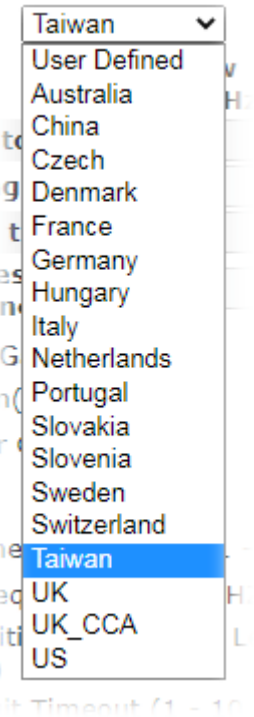
Cuenta SIP predeterminada	Puede configurar cuentas SIP (hasta seis grupos) en la página Cuenta SIP. Use la lista desplegable para elegir uno de los nombres de perfil para las cuentas como predeterminado para esta configuración de teléfono. **Reproducir tono de marcación solo cuando la cuenta esté registrada -**Marque esta casilla para invocar la función.

Además, puede pulsar el botón**Avanzado**botón para configurar los ajustes de tono, ganancia de volumen, MISC y modo DTMF.**Avanzado**Se proporciona una configuración para ajustar la costumbre de telecomunicaciones para el área local del enrutador instalado. Los ajustes de tono incorrectos pueden causar molestias a los usuarios. Para configurar el patrón de sonido del teléfono, simplemente elija una región adecuada para permitir que el sistema encuentre automáticamente la configuración de tono preestablecida y el tipo de identificador de llamadas. O puede ajustar la configuración de tono manualmente si elige Definido por el usuario. TOn1, TOff1, TOn2 y TOff2 significan la cadencia del patrón de tono. TOn1 y TOn2 representan sonido encendido; TOff1 y TOff2 representan el sonido apagado.



Los ajustes disponibles se explican a continuación:

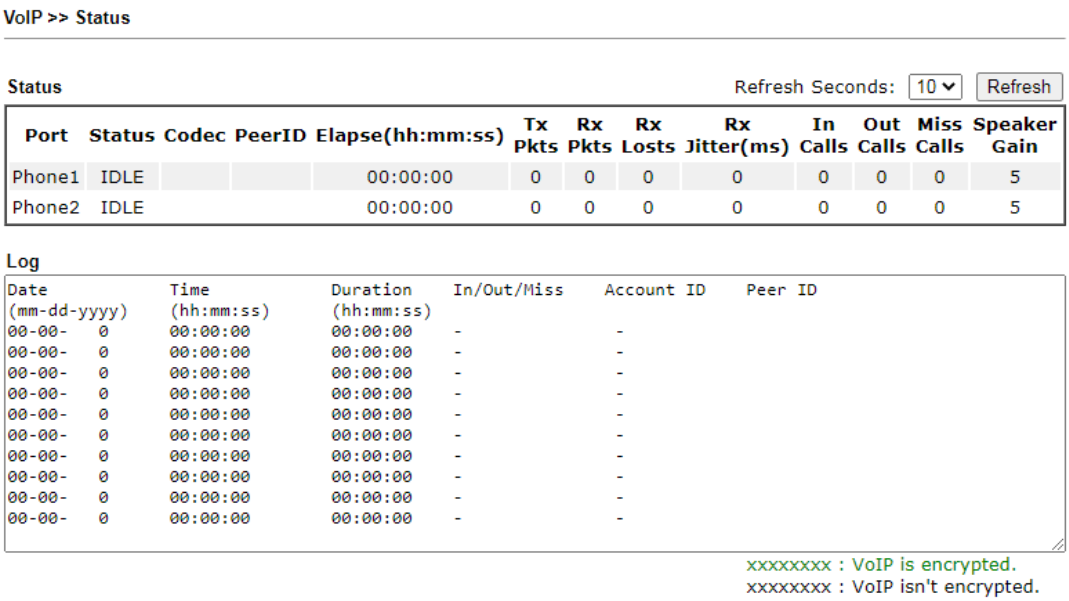
Artículo	Descripción
Región	Seleccione la región adecuada en la que se encuentra. Los ajustes comunes de**Tipo de identificador de llamadas**,**Tono de marcación**,**Tono de llamada**, **Tono ocupado**y**Tono de congestión**se mostrará automáticamente en la página. Si no puede encontrar uno adecuado, elija **Usuario definido**y complete los valores correspondientes para el tono de marcación, el tono de llamada, el tono de ocupado, el tono de congestión para el teléfono VoIP.

	 Además, puede especificar cada campo para su necesidad. Se recomienda que utilice la configuración predeterminada para la comunicación VoIP.
Ganancia de volumen	**Ganancia de micrófono (1-10)/Ganancia de altavoz (1-10)**-Ajuste el volumen del micrófono y el altavoz ingresando un número del 1 al 10. Cuanto mayor sea el número, mayor será el volumen.
VARIOS	**Nivel de potencia del tono de marcación**l - Esta configuración se utiliza para ajustar el volumen del tono de marcación. Cuanto más pequeño es el número, más fuerte es el tono de marcación. Se recomienda que utilice la configuración predeterminada. **Frecuencia de timbre**-Esta configuración se utiliza para controlar la frecuencia del tono de llamada. Se recomienda que utilice la configuración predeterminada. **Nivel de potencia del tono de llamada en espera**-Esta configuración se utiliza para ajustar el volumen del tono de llamada en espera. Cuanto más pequeño es el número, más fuerte es el tono. Se recomienda que utilice la configuración predeterminada. **Tiempo de espera entre dígitos**–Escriba un valor en este campo para especificar el límite de tiempo para interdígito.
DTMF	**Modo DTMF –**Hay cuatro modos DTMF para que elijas. - ***En banda***-Elija este y Vigor enviará el tono DTMF como audio directamente cuando presione el teclado del teléfono. - ***fuera de banda***-Elija este, luego el Vigor capturará el número del teclado que presionó y lo transformará a forma digital y luego lo enviará al otro lado; el receptor generará el tono de acuerdo con la forma digital que reciba. Esta función es muy útil cuando se produce una congestión de tráfico en la red y aún puede mantener la precisión del tono DTMF. - ***INFORMACIÓN SIP***-Elija este y Vigor capturará el tono DTMF y lo transferirá a formato SIP. Luego se enviará al extremo remoto con un mensaje SIP.

	Tipo de carga útil (rfc2833)-Escriba un número del 96 al 127; el valor predeterminado era 101. Esta configuración está disponible para el modo OutBand (RFC2833). **Reemplace + dígito en el identificador de llamadas para**-Para llamadas telefónicas internacionales, el número de teléfono podría agregar un signo '+', por ejemplo, + 8865972727. Sin embargo, el identificador de llamadas (especialmente el tipo DTMF) no puede mostrar '+' en absoluto. Por lo tanto, esta función se puede habilitar para dar otro número para reemplazar el signo más, por ejemplo, "+" se puede reemplazar por "00". Luego, el número de teléfono anterior se convertirá en 008865972727. Cuando la persona que llama recibe dicho número, puede usar la función de volver a marcar para volver a llamar a la persona que llama.

IV-1-6 Estado

Desde esta página, puede encontrar el códec, la conexión y otros estados de llamadas importantes para cada puerto.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Actualizar segundos	Especifique el intervalo (5, 10 o 30) del tiempo de actualización para obtener la información de llamadas VoIP más reciente. La información se actualizará inmediatamente cuando se haga clic en el botón Actualizar.
Puerto	Muestra el estado de conexión actual para los puertos de teléfono(s).
Estado	Muestra el estado de la conexión VoIP. **INACTIVO -**Indica que la función VoIP está inactiva. **COLGAR -**Indica que no se ha establecido la conexión (tono de ocupado). **CONECTANDO -**Indica que el usuario está llamando. **ESPERA_ANS -**Indica que se inició una conexión y está esperando la respuesta del usuario remoto. **ALERTA -**Indica que está llegando una llamada. **ACTIVO-** Indica que se ha iniciado la conexión VoIP.

códec	Indica el códec de voz empleado por el canal actual.
ID de compañero	El ID de compañero de llamada entrante o saliente actual (el formato puede ser IP o Dominio).
Transcurrir(hh:mm:ss)	El formato se representa como horas:minutos:segundos.
paquetes de transmisión	Número total de paquetes de voz transmitidos durante esta sesión de conexión.
paquetes recetados	Número total de paquetes de voz recibidos durante esta sesión de conexión.
Recetas perdidas	Número total de paquetes perdidos durante esta sesión de conexión.
Fluctuación de Rx	La fluctuación de los paquetes de voz recibidos.
En llamadas	Acumulación por los tiempos de in call.
Llamadas salientes	Acumulación para los tiempos de llamada fuera.
Llamadas perdidas	Acumulación por los tiempos de llamada perdida.
Ganancia del altavoz	El volumen de la llamada actual.
Registro	Mostrar registros de llamadas VoIP.

IV-1-7 Diagnóstico

VoIP Diagnostics se usa para diagnosticar si la falla del teléfono VoIP es causada por un tono o ID de llamada diferente.

VoIP >> Diagnostics

VoIP Diagnostics

Caller ID Tone

IV-1-7-1 Identificador de llamadas

VoIP >> VOIP Diagnostics

Send Caller ID

FXS 1 | FXS 2 | FXO

Current type: **FSK_ETSI**

Caller ID used to send : _____

Item	Types	Status
◉	FSK_ETSI	Untest
○	FSK_ETSI (UK)	Untest
○	FSK_BELLCORE (US/AU)	Untest
○	DTMF	Untest
○	DTMF (DK)	Untest
○	DTMF (SE/NL/FIN)	Untest

Set Test

IV-1-7-2 Tono

VoIP >> VOIP Diagnostics

Send Tone

FXS 1 | FXS 2

Region Taiwan

	Low Freq(Hz)	High Freq(Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dial tone	350	440	0	0	0	0
Ringing tone	440	480	1000	2000	0	0
Busy tone	480	620	500	500	0	0
Congestion tone	480	620	250	250	0	0

Item	Types	Status
○	Dial Tone	Untest
○	Busy Tone	Untest
○	Congestion Tone	Untest

Set Test

Esta página se deja en blanco.

Parte V VPN

VPN

Una red privada virtual (VPN) es la extensión de una red privada que abarca enlaces a través de redes compartidas o públicas como Internet. En resumen, mediante la tecnología VPN, puede enviar datos entre dos computadoras a través de una red pública o compartida de una manera que emule las propiedades de un enlace privado punto a punto.

Certificate Management

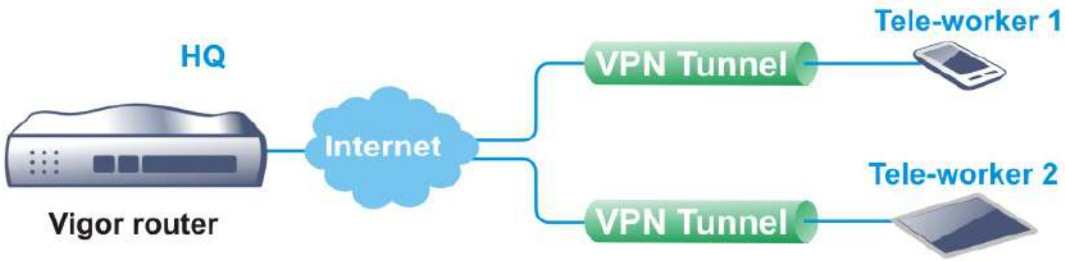
Un certificado digital funciona como una identificación electrónica, que es emitida por una autoridad de certificación (CA). Contiene información como su nombre, un número de serie, fechas de vencimiento, etc., y la firma digital de la autoridad emisora del certificado para que un destinatario pueda verificar que el certificado es real. Aquí, el enrutador Vigor admite certificados digitales que cumplen con el estándar X.509.

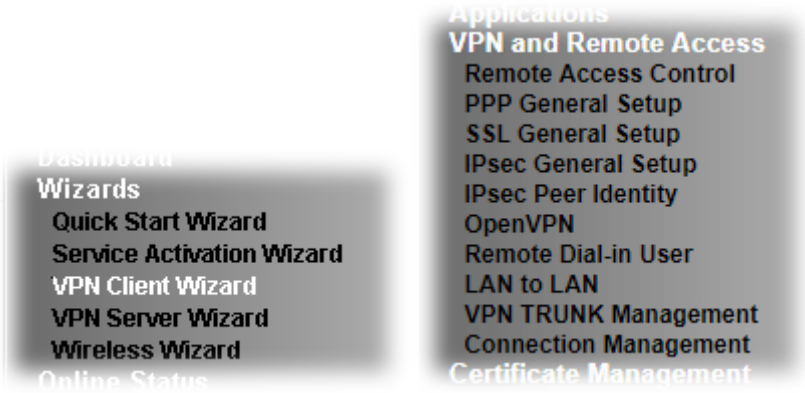
VPN V-1 y acceso remoto

Una red privada virtual (VPN) es una extensión de una red privada que permite a los usuarios acceder a los recursos de red que están disponibles en la red privada a través de redes públicas o compartidas como Internet, como si los usuarios estuvieran conectados directamente a la red privada.

Estos son algunos usos de las VPN:

- Comunicación entre home office y cliente.
- Conexión segura entre Teletrabajador, personal en viaje de negocios y oficina principal.
- Intercambio de datos entre la oficina remota y la oficina principal.
- POS entre la cadena de tiendas y la sede.
- Elusión de la censura en Internet que filtra sitios web o contenidos.
- Elusión de técnicas de geolocalización empleadas por proveedores de servicios o vendedores para bloquear o restringir servicios a los usuarios.
- Comunicaciones seguras a través de puntos de acceso público

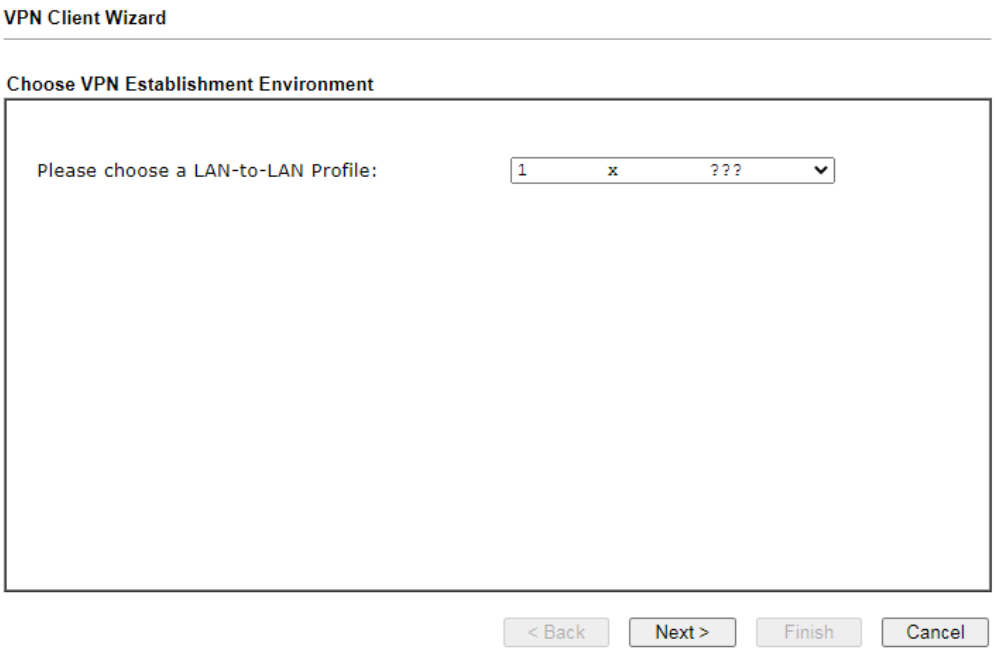




Asistente de cliente VPN V-1-1

El asistente del cliente VPN configurará el enrutador como un***cliente***para conectarse a un servidor VPN remoto utilizando un túnel VPN de LAN a LAN. El asistente lo guiará a través del proceso de configuración.

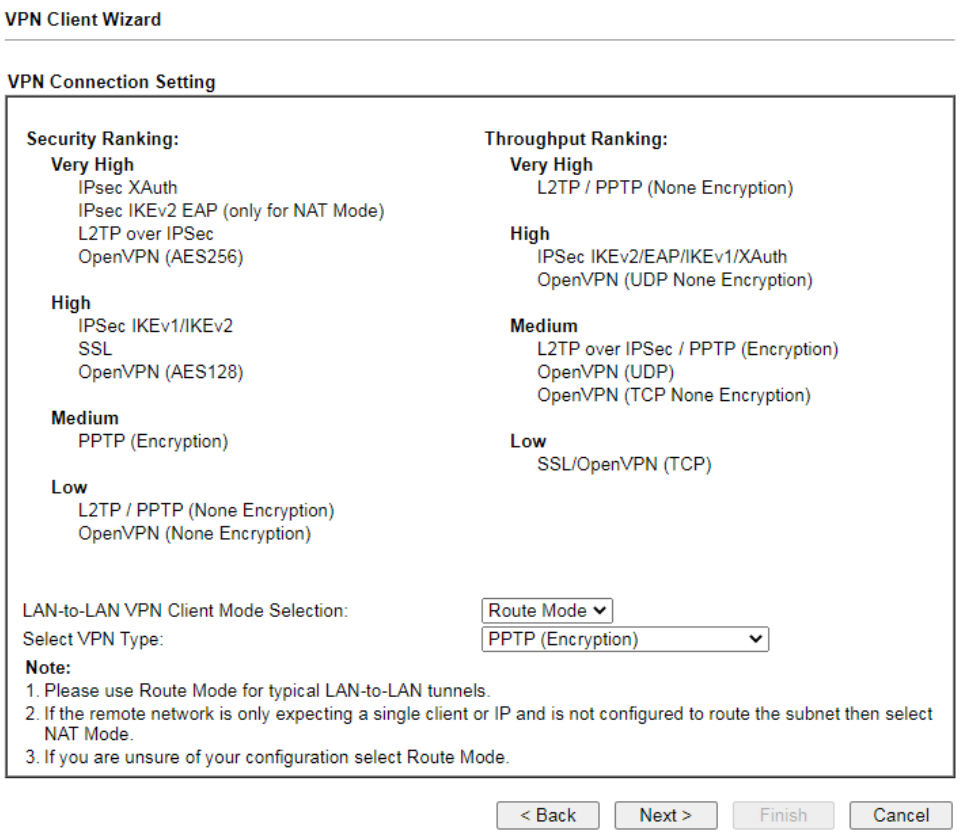
1. En la barra de menú, haga clic en**magos,**y luego**Asistente de cliente VPN**.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Por favor elige un Perfil de LAN a LAN	El perfil utilizado para almacenar esta configuración de túnel. Si selecciona un índice que ya se ha configurado anteriormente, el asistente sobrescribirá la configuración existente.

2. Cuando finalice la selección de modo y perfil, haga clic en**Próximo**para abrir la página siguiente.

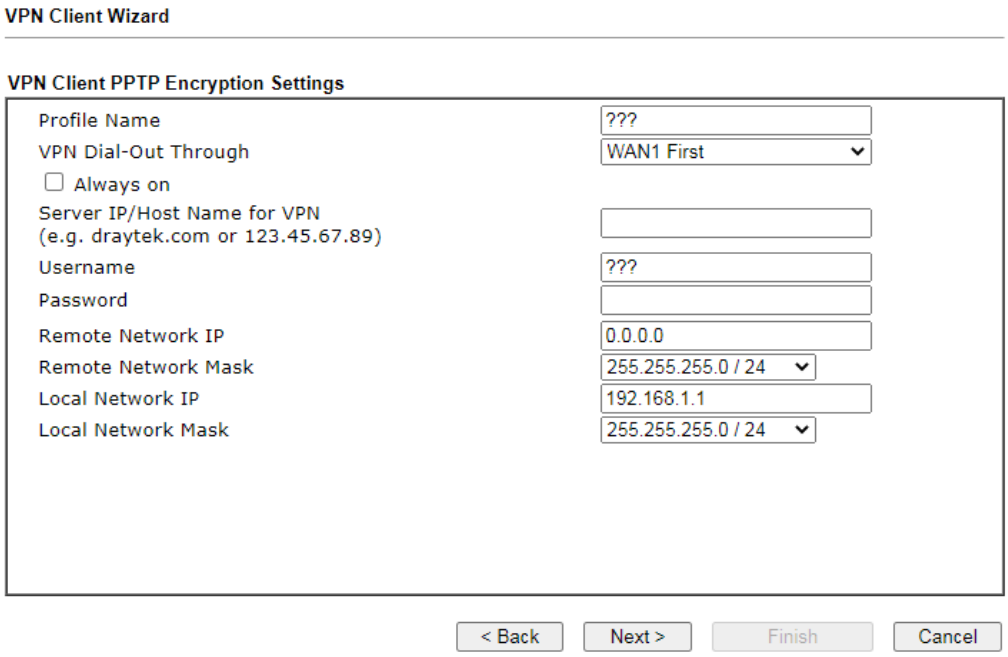


Los ajustes disponibles se explican a continuación:

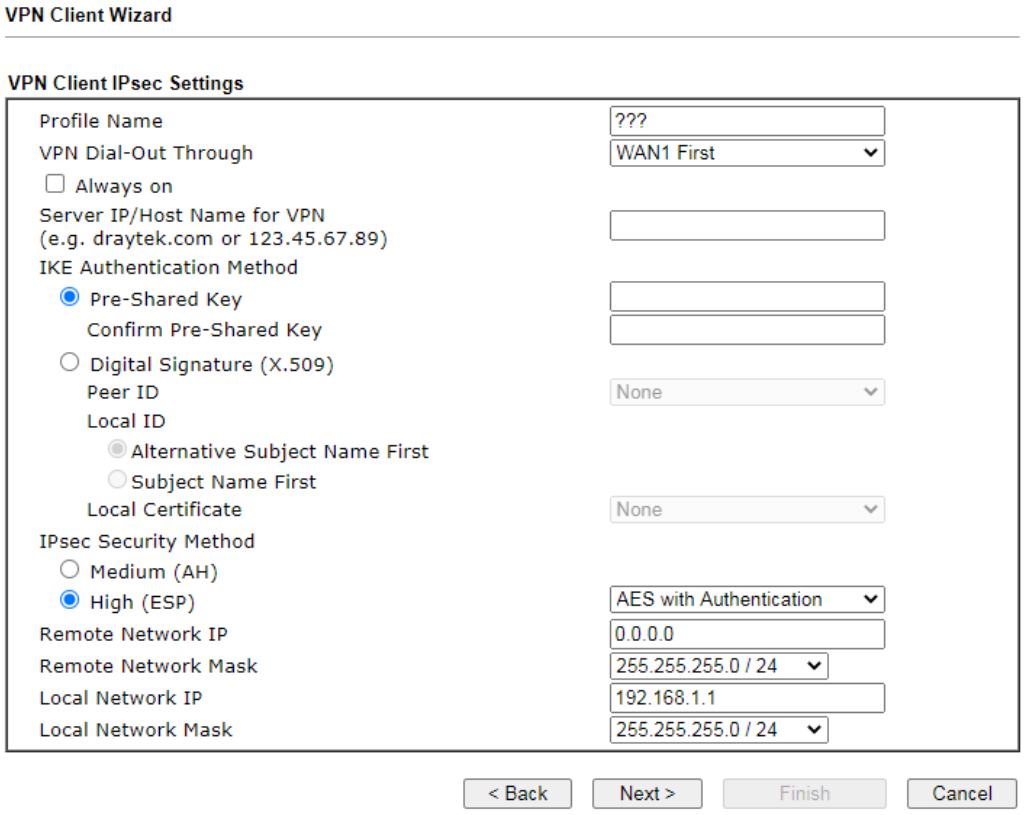
Artículo	Descripción
Cliente de LAN a LAN Selección de modo	**Modo de ruta –**Todo el tráfico entre la red local y la red remota lleva las direcciones IP de origen. Seleccione esto si el servidor VPN puede establecer rutas para manejar el enrutamiento de tráfico entre LAN. **Modo NAT –**El cliente VPN (enrutador local) usa una sola dirección IP asignada por el servidor VPN (enrutador remoto) y usa NAT para realizar un seguimiento de las conexiones. Seleccione esto si el servidor VPN espera que solo una dirección IP en la red local se comunique con la red remota.
Seleccione el tipo de VPN	Seleccione un protocolo VPN para el túnel de LAN a LAN. Los diferentes protocolos VPN ofrecen diferentes niveles de seguridad y rendimiento.

Información	Las siguientes descripciones para el tipo de VPN se basan en el**Modo de ruta** especificado en Selección de modo de cliente de LAN a LAN.

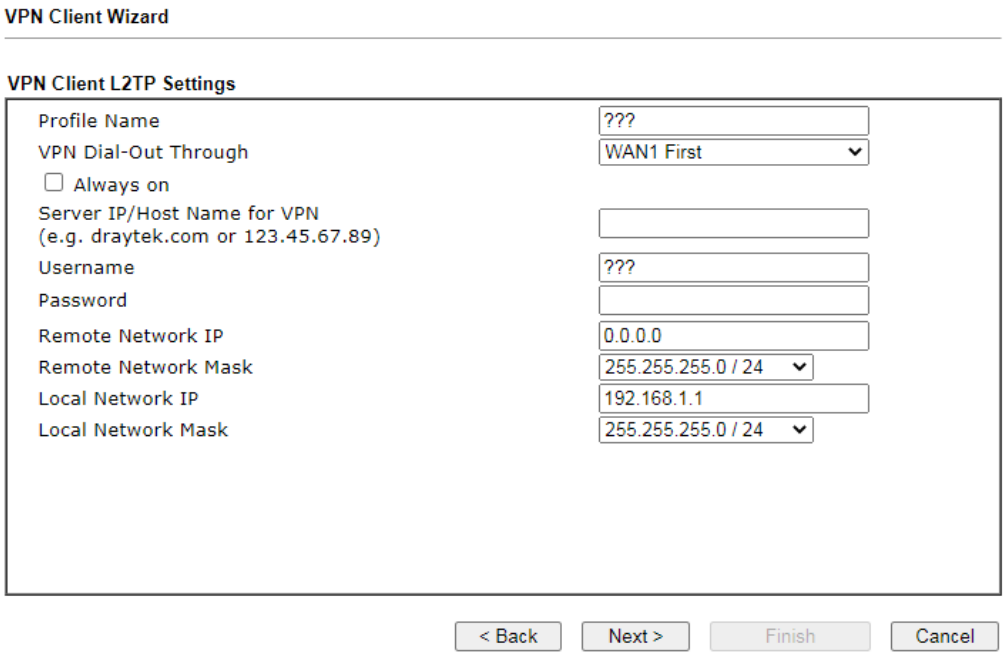
Si ha seleccionado**PPTP (sin cifrado)**o**PPTP (Cifrado)**, aparece la siguiente pantalla de configuración.



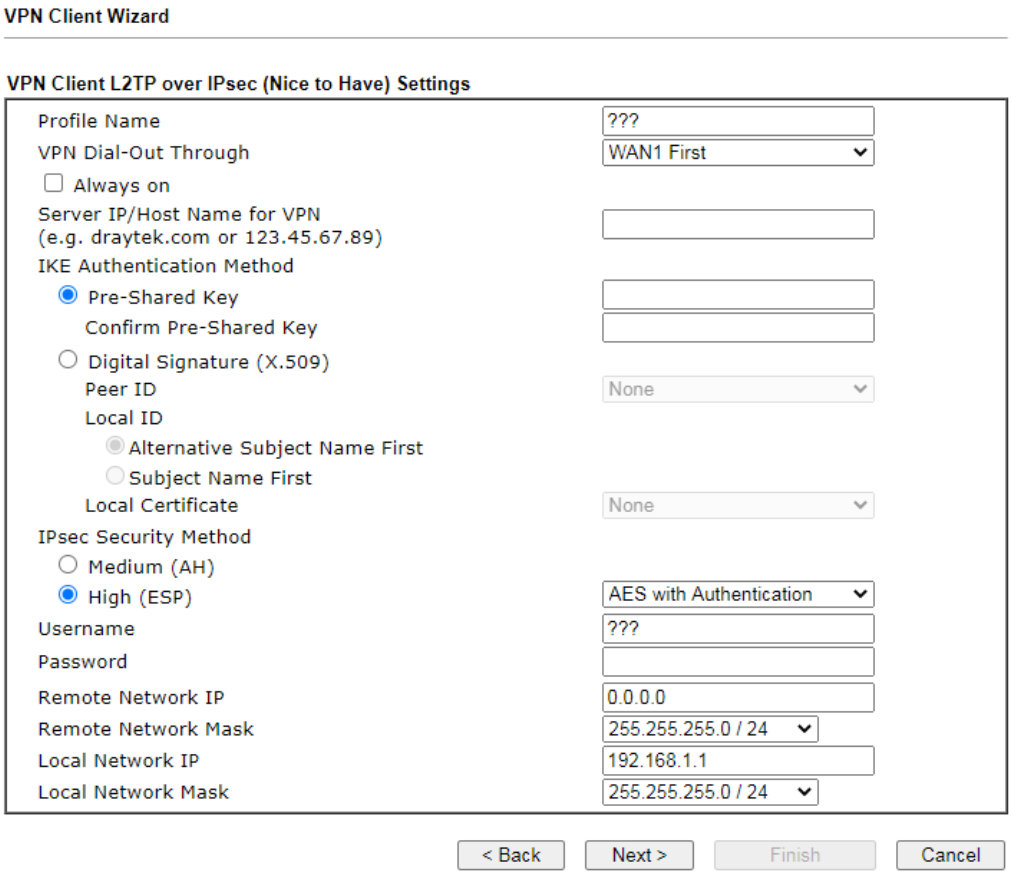
Si ha seleccionado**IPsec**, aparece la siguiente pantalla de configuración.



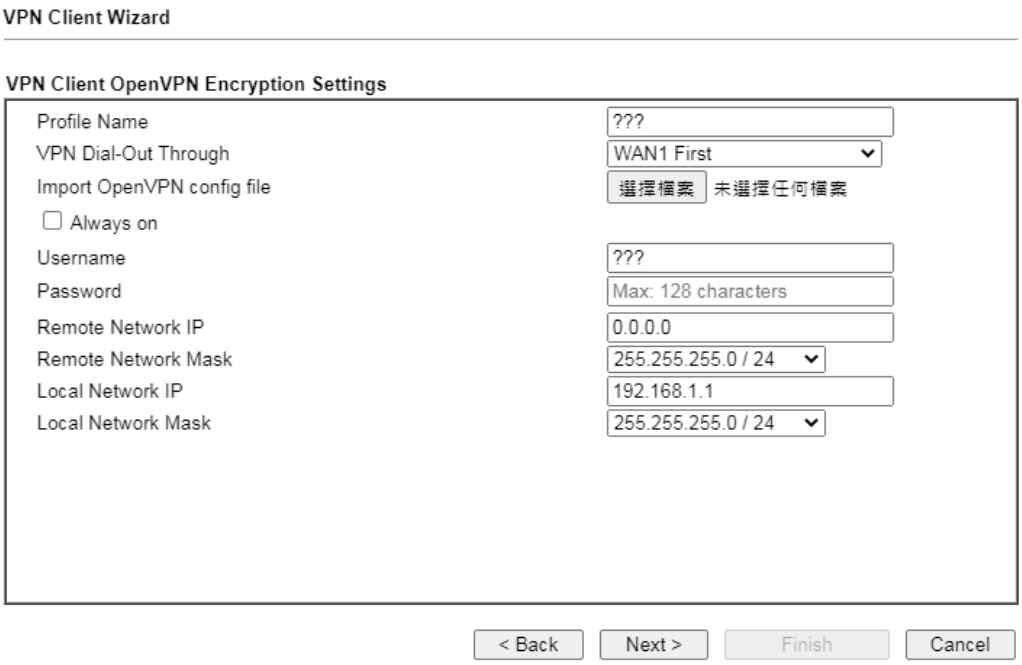
Si ha seleccionado**SSL/L2TP**, aparece la siguiente pantalla de configuración.



Si ha seleccionado**L2TP sobre IPsec (agradable tener)**o**L2TP sobre IPsec (Obligatorio)**, aparece la siguiente pantalla de configuración.



Si ha seleccionado**OpenVPN**, aparece la siguiente pantalla de configuración.

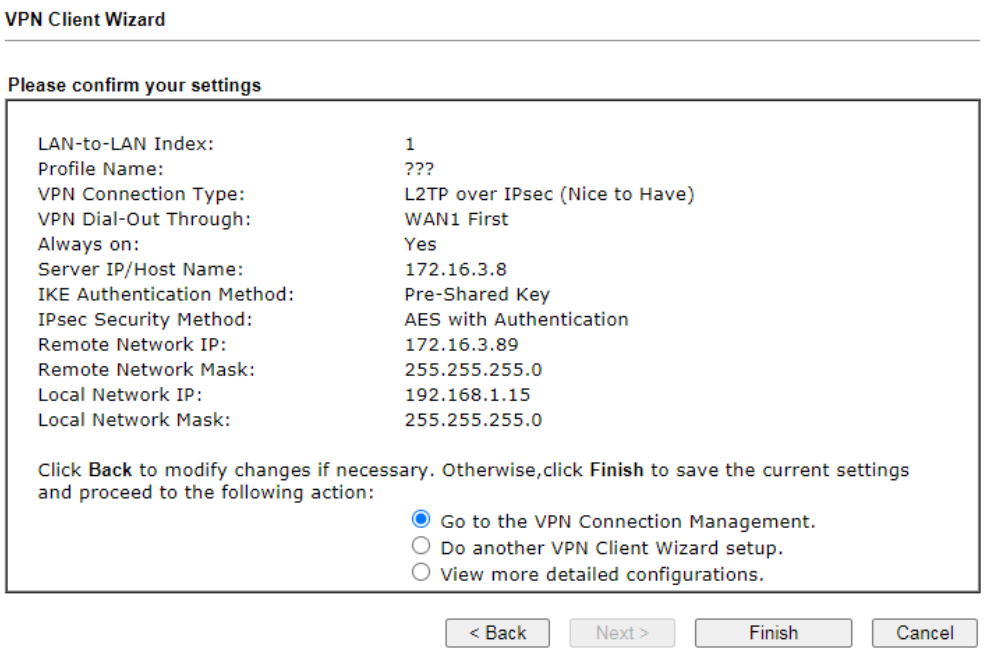


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre de perfil	Nombre que identifica a este perfil. La longitud máxima del nombre del perfil es de 10 caracteres.
Llamada de salida VPN a través	La interfaz WAN que se usará para marcar para establecer el túnel VPN. **WANx primero (o LTE primero)**-El enrutador primero intenta establecer el túnel VPN utilizando esta interfaz WAN. Cuando eso no tiene éxito, intentará usar otras interfaces WAN. **Solo WANx (o solo LTE)**-El enrutador establecerá el túnel VPN utilizando solo esta interfaz WAN. **Solo WANx: solo establezca VPN si WANy está inactivo**-El enrutador establecerá el túnel VPN utilizando esta interfaz WAN si la otra interfaz WAN está fuera de línea.
siempre encendido	Si se selecciona, el enrutador mantendrá la conexión VPN.
Servidor IP/Nombre de host para VPN	Ingrese la dirección IP o el nombre de host del servidor del servidor VPN remoto.
Autenticación IKE Método	Método de autenticación IKE que se utilizará. Escoger entre **Clave previamente compartida**y**Firma Digital (X.509)**. **Clave previamente compartida** - **Clave precompartida-**Especifique una clave para la autenticación IKE. - **Confirmar clave precompartida-**Confirme la clave precompartida. **Firma Digital (X.509)** - **ID de compañero**–Seleccione ID de compañero de la lista desplegable. Las ID de pares se administran mediante VPN y acceso remoto >> Identidad de pares IPsec. - **ID local**–Seleccionar**Nombre alternativo del sujeto primero**o **Nombre del sujeto Abetos**t. - **Certificado local**–Seleccione un certificado de la lista desplegable. Los certificados locales se gestionan mediante

	Gestión de Certificados >> Certificado Local.
Método de seguridad IPsec	**Medio**-El encabezado de autenticación (AH) significa que los datos se autenticarán, pero no se cifrarán. Por defecto, esta opción está activa. **Alto**-La carga útil de seguridad encapsulada (ESP) significa que la carga útil (datos) se cifrará y autenticará. Puede seleccionar el algoritmo de cifrado de Estándar de cifrado de datos (DES), Triple DES (3DES) y AES.
Importar OpenVPN archivo de configuración	Seleccione para importar un archivo de configuración de OpenVPN desde un servidor OpenVPN específico (p. ej., enrutador Vigor, PC, otro proveedor de VPN, etc.) al enrutador Vigor. Más tarde, como cliente VPN, este enrutador puede acceder al servidor VPN a través del nombre de usuario y la contraseña.
Nombre de usuario	Este campo se utiliza para autenticar la conexión cuando selecciona PPTP o L2TP con o sin la política IPsec anterior. La longitud del nombre de usuario está limitada a 11 caracteres.
Contraseña	Este campo se utiliza para autenticar la conexión cuando selecciona PPTP o L2TP con o sin la política IPsec anterior. La longitud de la contraseña está limitada a 11 caracteres.
IP de red remota	Ingrese una dirección IP de LAN (según la ubicación real del host remoto) para establecer una conexión VPN.
Red remota Mascarilla	Ingrese la máscara de red (según la ubicación real del host remoto) para crear una conexión VPN.
IP de red local	Introduzca la IP de la red local para la configuración de TCP/IP.
Máscara de red local	Introduzca la máscara de red local para la configuración de TCP/IP.

3. Una vez que haya ingresado toda la información requerida, haga clic en**Próximo**para pasar a la página de confirmación. La página de confirmación muestra un resumen de todas las configuraciones. Si necesita realizar ajustes en la configuración, haga clic en**Atrás**para volver a la página anterior. De lo contrario, seleccione una de las siguientes acciones y haga clic en**Finalizar**para guardar los cambios en el perfil VPN de LAN a LAN.



Los ajustes disponibles se explican a continuación:

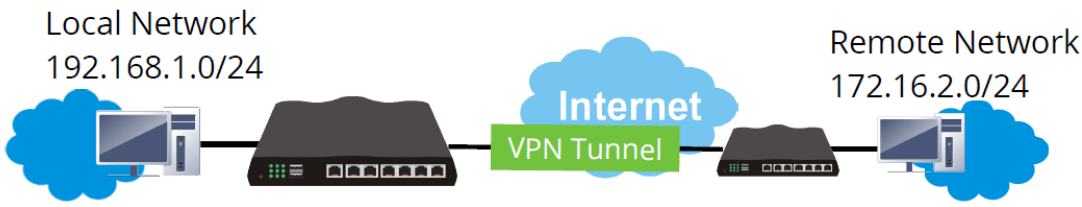
Artículo	Descripción
Ir a la VPN Conexión Gestión	Proceder a**VPN y acceso remoto>>Gestión de conexiones**para administrar las sesiones de VPN.
Haz otra VPN Configuración del asistente del cliente	Vuelva a ejecutar el asistente de cliente de VPN para configurar otro perfil de VPN de LAN a LAN.
Ver más detallado configuración	Abre este perfil en**VPN y acceso remoto>>LAN a LAN** para realizar cambios de configuración adicionales.

Asistente del servidor VPN V-1-2

El asistente del servidor VPN se puede utilizar para configurar el enrutador como un***servidor***que acepta conexiones VPN entrantes desde un servidor VPN utilizando un túnel VPN de LAN a LAN.

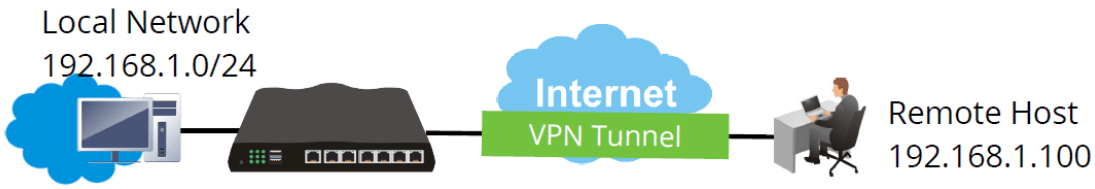
Sitio a sitio (LAN a LAN)

- Una conexión entre las redes LAN de dos enrutadores.
- Permite que los empleados de las sucursales y la oficina central compartan los mismos recursos de red.



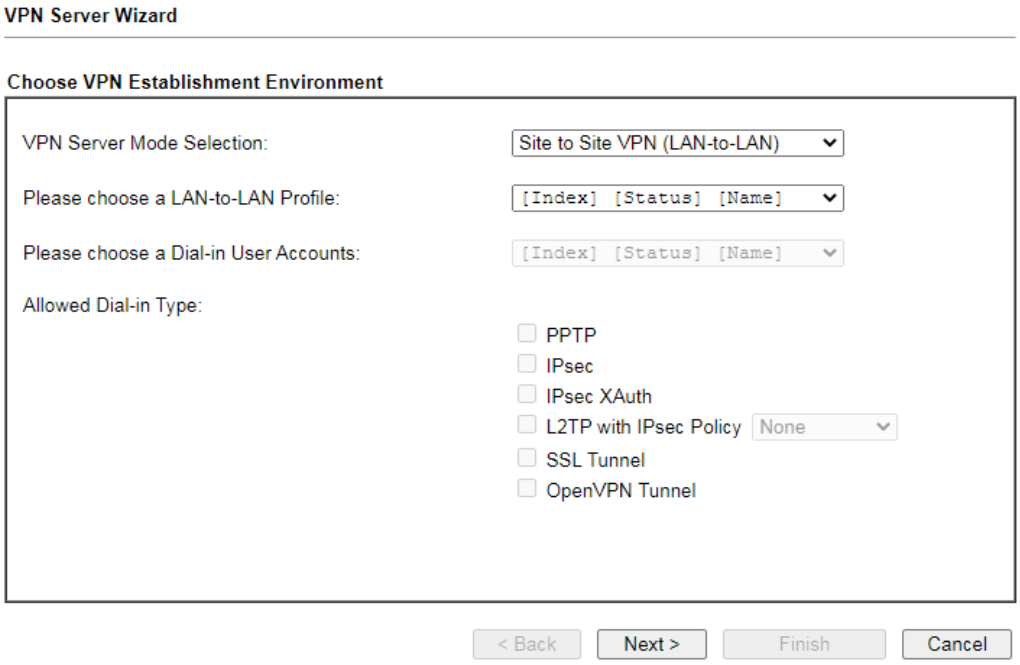
Acceso remoto (marcación remota)

- Una conexión entre el host remoto y la red LAN del enrutador. El host utilizará una dirección IP en la subred local.
- Permite a los empleados acceder a los recursos internos de la empresa cuando se encuentran de viaje.



El asistente lo guiará paso a paso a través del proceso de configuración.

1. En la barra de menú, haga clic en**magos,**y luego**Asistente del servidor VPN**.

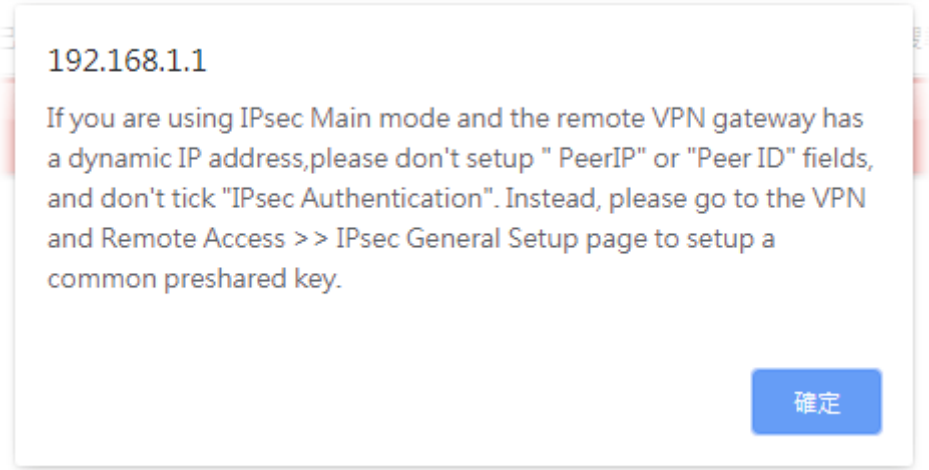


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Modo de servidor VPN **Selección**	Tipo de Servidor VPN a configurar. **VPN de sitio a sitio (LAN a LAN)**-Configura el servidor VPN para conexiones entrantes desde otros enrutadores. **Usuario de marcación remota (teletrabajador)**-Configura el servidor VPN para conexiones entrantes de usuarios remotos.
Por favor elige un **Perfil de LAN a LAN**	Si el modo de servidor VPN seleccionado fue**VPN de sitio a sitio (LAN a LAN)**, elija un perfil de LAN a LAN para almacenar esta configuración.
Por favor elige un **Cuentas de usuario de acceso telefónico**	Si el modo de servidor VPN seleccionado fue**Usuario de marcación remota (teletrabajador)**, elija un perfil de usuario de acceso telefónico para almacenar esta configuración.
Tipo de acceso telefónico permitido	Seleccione todos los protocolos VPN permitidos para este perfil de LAN a LAN o cuenta de usuario de acceso telefónico. Un tipo de marcación diferente conducirá a una página de configuración diferente. Además, los elementos ajustables para cada tipo de acceso telefónico se cambiarán de acuerdo con el modo de servidor VPN (**VPN de sitio a sitio**y**Usuario de marcación remota**) seleccionado.

2. Después de elegir el perfil del servidor, haga clic en**Próximo**.

3. Aparecerá el siguiente cuadro de diálogo, recordándole que no configure los campos IPsec si la ubicación remota tiene una dirección IP dinámica.

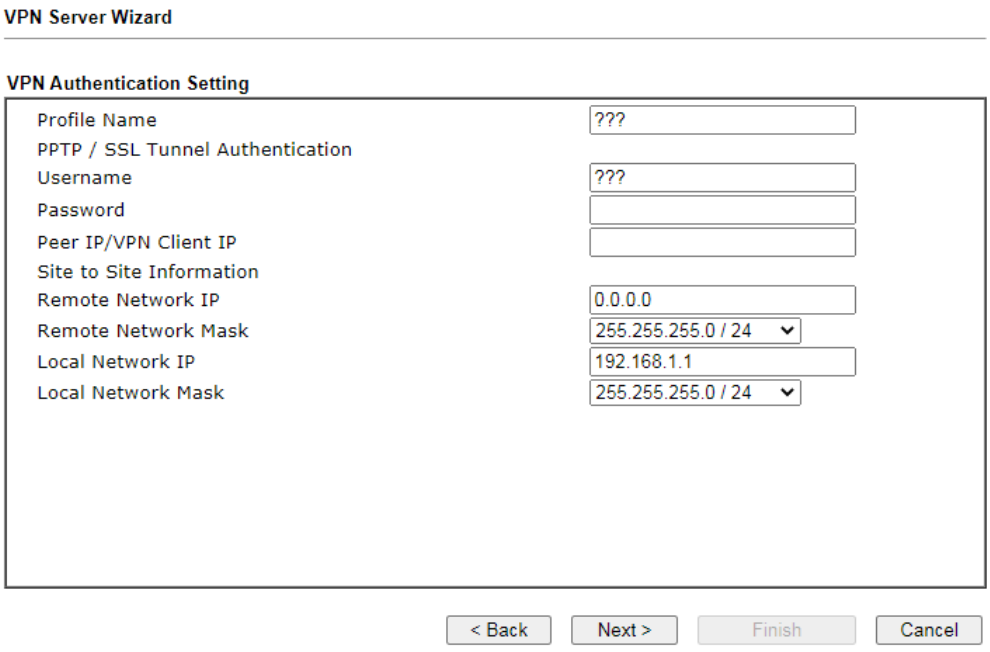


Hacer clic**DE ACUERDO**para descartar el cuadro de diálogo y pasar a la página siguiente.

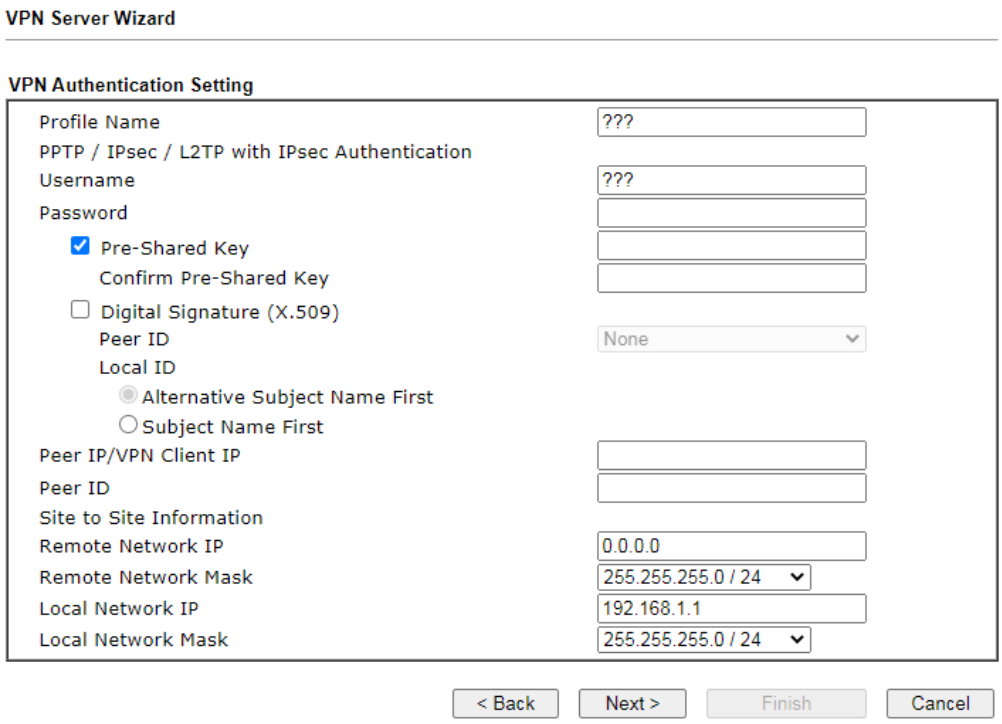
Si ha elegido configurar un perfil VPN de LAN a LAN, vaya al paso 4.

Si ha elegido configurar un perfil de VPN de usuario de marcación remota, vaya al paso 5.

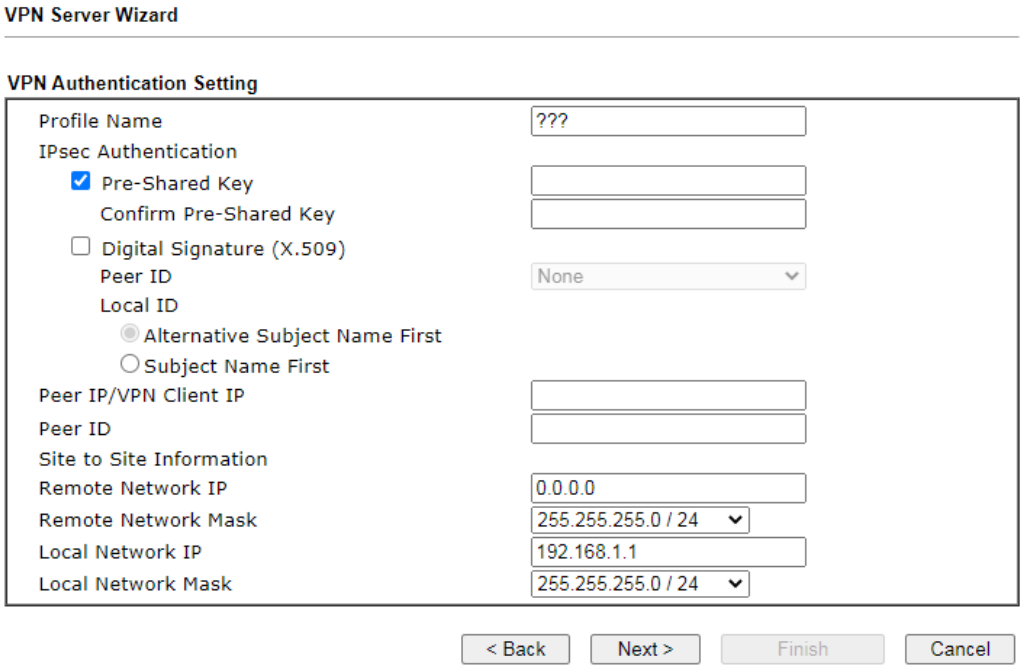
4. El**VPN de sitio a sitio (LAN a LAN)**la página de configuración aparece de la siguiente manera si ha seleccionado**PPTP/SSL**.



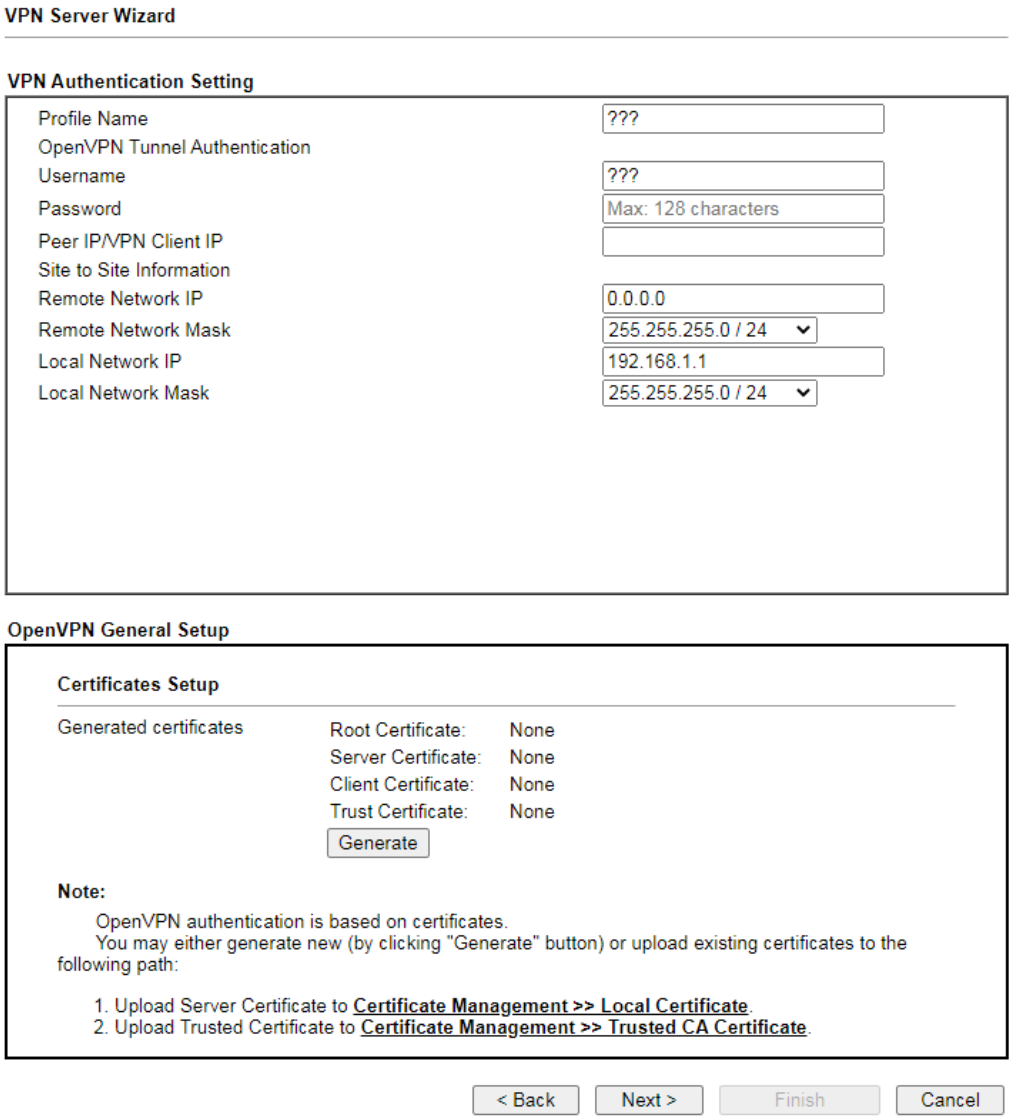
Si ha seleccionado**PPTP e IPsec y L2TP**(tres tipos) o**PPTP e IPsec**(dos tipos) o **L2TP con política (agradable tener/imprescindible),**aparece la siguiente pantalla de configuración.



Si ha seleccionado**IPsec,**aparece la siguiente pantalla de configuración.



Si ha seleccionado**VPN abierta,**aparece la siguiente pantalla de configuración.

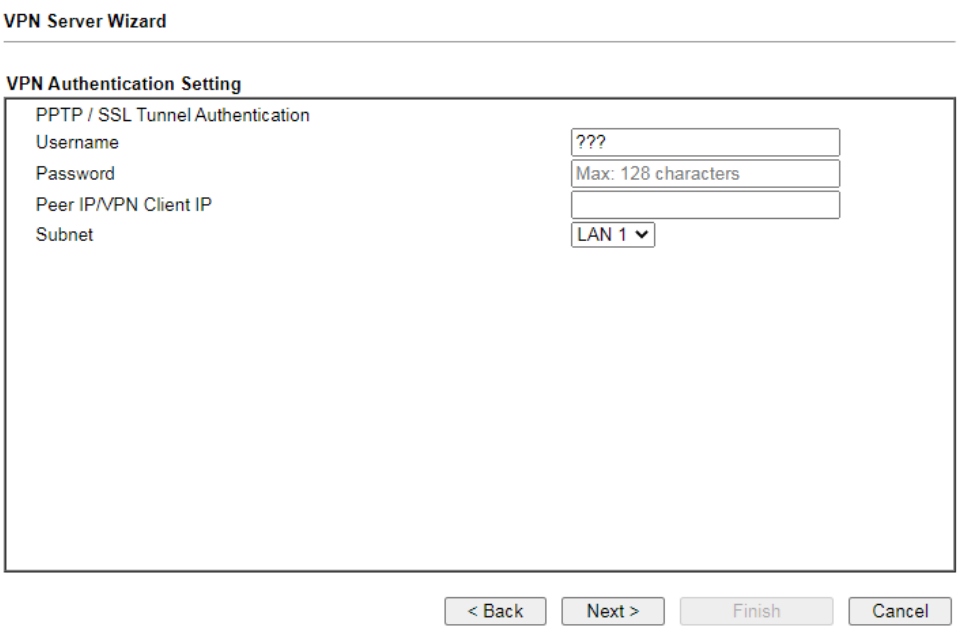


Los ajustes disponibles se explican a continuación:

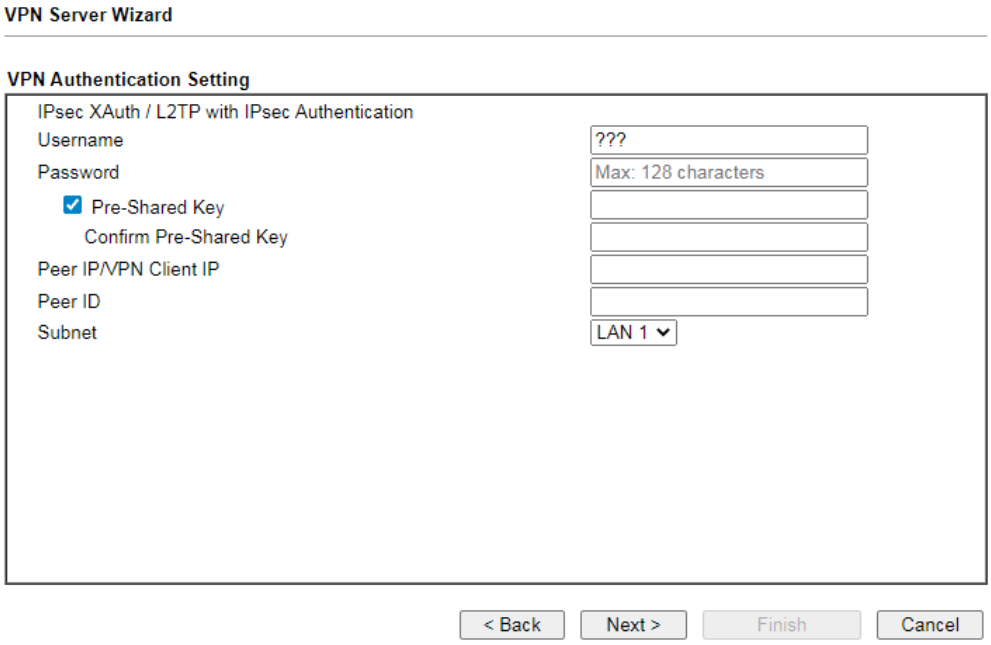
Artículo	Descripción
Nombre de perfil	Nombre para identificar este perfil VPN.
Nombre de usuario	Utilizado por la LAN remota para establecer una conexión VPN. La longitud del nombre de usuario está limitada a 11 caracteres.
Contraseña	Utilizado por la LAN remota para establecer una conexión VPN. La longitud de la contraseña está limitada a 11 caracteres.
IPsec / IPsec XAuth / L2TP con autenticación de túnel IPsec / SSL	
Clave precompartida	Para la autenticación PPTP / IPsec / IPsec XAuth / L2TP con IPsec / SSL Tunnel, debe configurar una clave precompartida y/o una firma digital. Tenga en cuenta que, si el cliente remoto tiene una dirección IP dinámica, no habilite ninguna de las configuraciones (PSK / Firma digital) en esta sección. En su lugar, configure los ajustes globales de IPsec mediante VPN y acceso remoto>>Configuración general de IPsec. **Clave precompartida**-Seleccione para ingresar una clave precompartida IPsec específica para este perfil. La longitud del PSK está limitada a 64 caracteres.

	Confirmar clave precompartida-Vuelva a ingresar la clave precompartida nuevamente para confirmar.
Firma digital (X.509)	**Firma Digital (X.509) -**Seleccione para habilitar la firma digital X.509. **ID de compañero**–Seleccione una firma digital X.509 predefinida como ID de homólogo. Las ID de pares deben configurarse primero mediante VPN y acceso remoto>>Identidad de pares IPsec. **ID local**–Especifica si se debe comprobar primero el nombre del sujeto o el nombre del sujeto alternativo de la ID del par X.509. Seleccione cualquiera**Nombre alternativo del sujeto primero** o**Nombre del sujeto primero**.
IP del mismo nivel/IP del cliente VPN	Ingrese la dirección IP de WAN o la dirección IP del cliente VPN para el cliente remoto. Si se especifican valores, solo se aceptarán las conexiones que provengan de la dirección IP especificada y/o que tengan la ID de par especificada.
ID de compañero	Ingrese el nombre de ID para el cliente remoto. La longitud máxima de la ID de par es de 47 caracteres. Si se especifican los valores, solo se aceptarán las conexiones que provengan de la dirección IP especificada y/o que tengan la ID de par especificada.
Información de sitio a sitio	
IP de red remota	Introduzca la dirección IP de la red remota.
Red remota **Mascarilla**	Introduzca la máscara de subred de la red remota.
IP de red local	Introduzca la IP de la red local para la configuración de TCP/IP.
Máscara de red local	Introduzca la máscara de red local para la configuración de TCP/IP.
Open VPN General **Configuración**	**Generar**-Haga clic para generar un certificado para la autenticación OpenVPN. O cargue un certificado existente de**Certificado local**o **Certificado de CA de confianza**página.

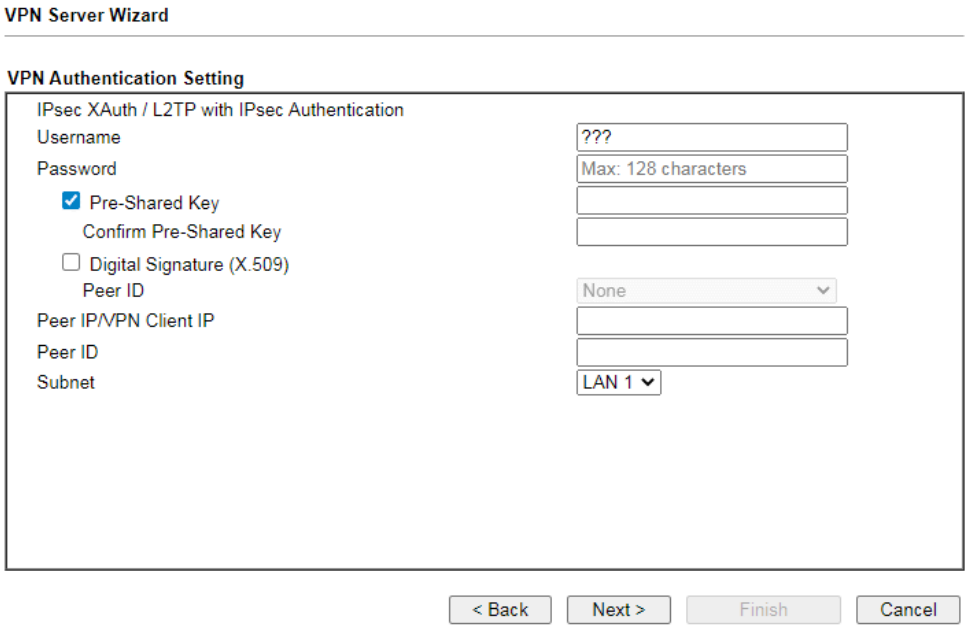
5. La página de configuración VPN de usuario de marcación remota (teletrabajador) aparece de la siguiente manera si ha seleccionado**PPTP/SSL**.



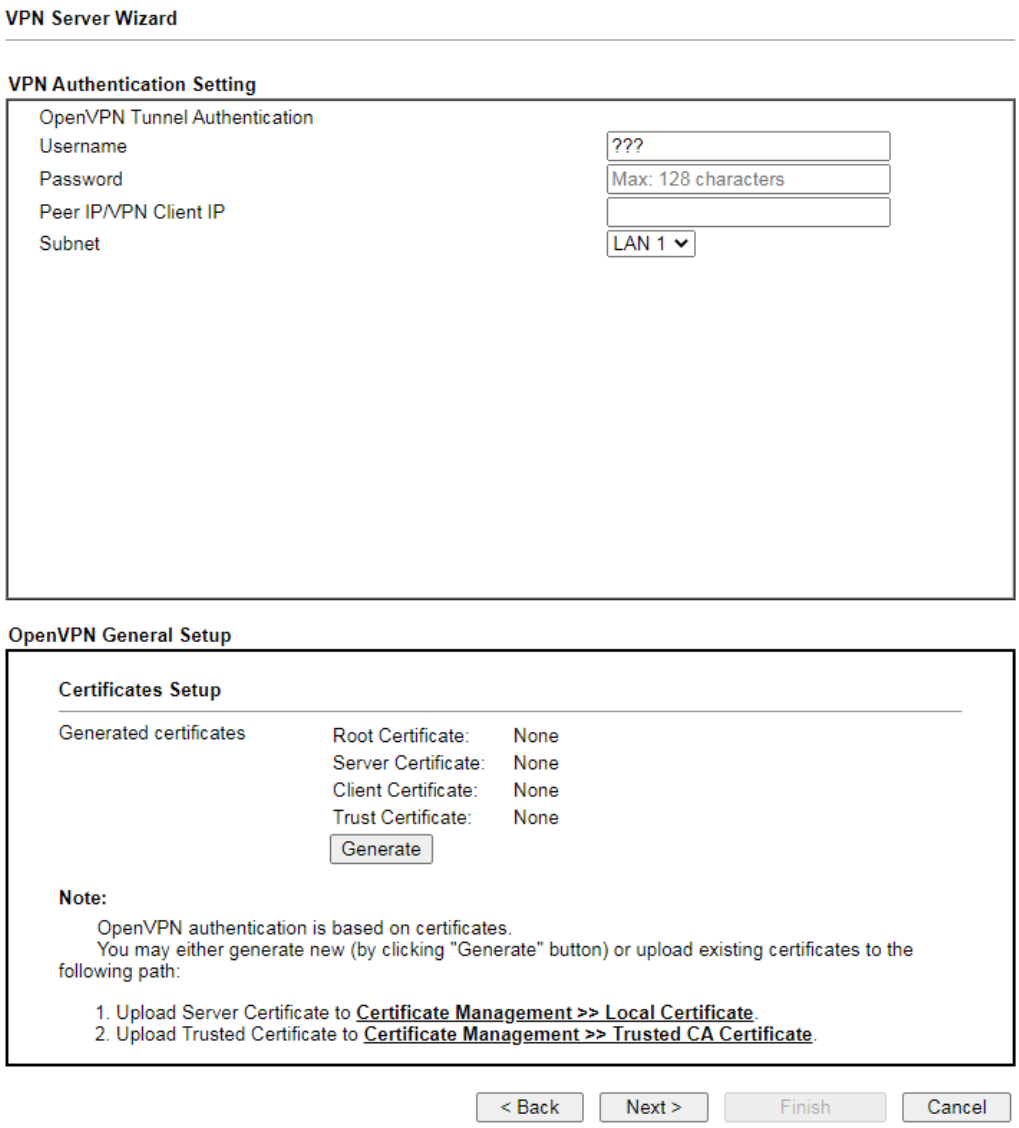
Si ha seleccionado**IPsec XAuth/L2TP con política IPsec (ninguno),**aparece la siguiente pantalla de configuración.



Si ha seleccionado**IPsec XAuth/L2TP con política IPsec (agradable tener)/L2TP con política IPsec (imprescindible),**aparece la siguiente pantalla de configuración.



Si ha seleccionado**Túnel OpenVPN,**aparece la siguiente pantalla de configuración.

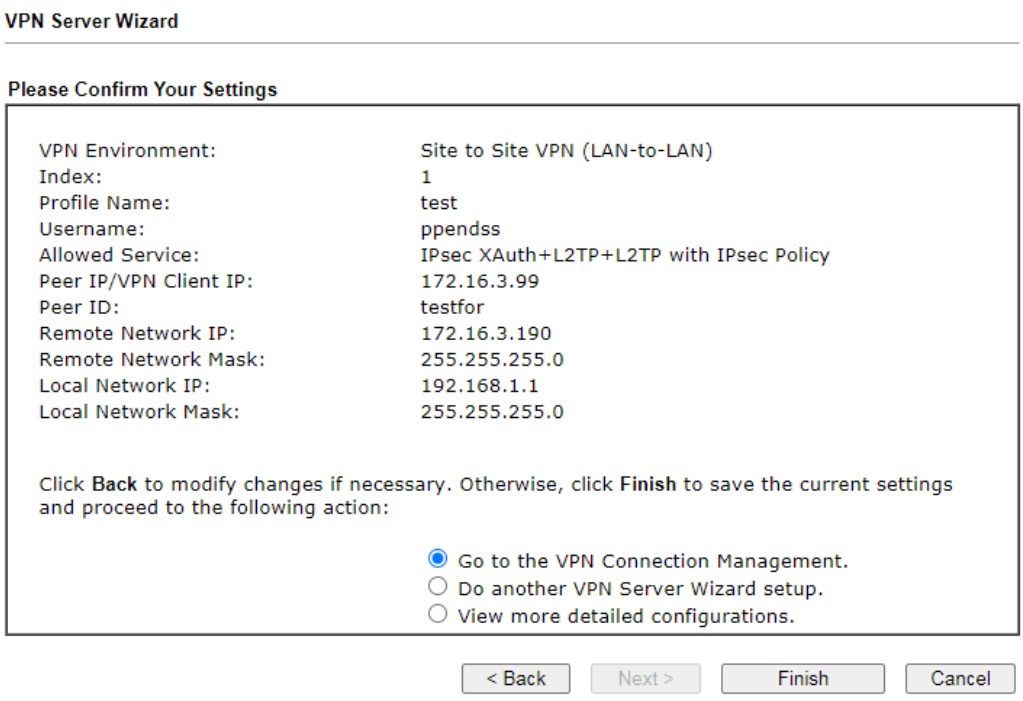


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre de usuario	Utilizado por la LAN remota para establecer una conexión VPN. La longitud del nombre de usuario está limitada a 11 caracteres.
Contraseña	Utilizado por la LAN remota para establecer una conexión VPN. La longitud de la contraseña está limitada a 11 caracteres.
IKEv1/IKEv2/IPsec XAuth/L2TP con autenticación de túnel IPsec/SSL	
Clave precompartida	Para IKEv1/IKEv2 / IPsec / IPsec XAuth / L2TP con autenticación de túnel IPsec / SSL, debe configurar una clave precompartida y/o una firma digital. Tenga en cuenta que, si el cliente remoto tiene una dirección IP dinámica, no habilite ninguna de las configuraciones (PSK / Firma digital) en esta sección. En su lugar, configure los ajustes globales de IPsec mediante VPN y acceso remoto>>Configuración general de IPsec. **Clave precompartida**-Seleccione para ingresar una clave precompartida IPsec específica para este perfil. La longitud del PSK está limitada a 64

	caracteres. **Confirmar clave precompartida**-Vuelva a ingresar la clave precompartida nuevamente para confirmar.
Firma digital (X.509)	**Firma Digital (X.509) -**Seleccione para habilitar la firma digital X.509. **ID de compañero**–Seleccione una firma digital X.509 predefinida como ID de homólogo. Las ID de pares deben configurarse primero mediante VPN y acceso remoto>>Identidad de pares IPsec.
IP del mismo nivel/IP del cliente VPN	Ingrese la dirección IP de WAN o la dirección IP del cliente VPN para el cliente remoto. Si se especifican valores, solo se aceptarán las conexiones que provengan de la dirección IP especificada y/o que tengan la ID de par especificada.
ID de compañero	Ingrese el nombre de ID para el cliente remoto. La longitud máxima de la ID de par es de 47 caracteres. Si se especifican los valores, solo se aceptarán las conexiones que provengan de la dirección IP especificada y/o que tengan la ID de par especificada.
subred	Seleccione una interfaz.
Open VPN General **Configuración**	**Generar**-Haga clic para generar un certificado para la autenticación OpenVPN. O cargue los certificados existentes de**Certificado local**o **Certificado de CA de confianza**página.

6. Después de finalizar la configuración, haga clic en**Próximo**para pasar a la página de confirmación.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Ir a la VPN Conexión	Proceder a**VPN y acceso remoto>>Gestión de conexiones**para administrar las sesiones de VPN.

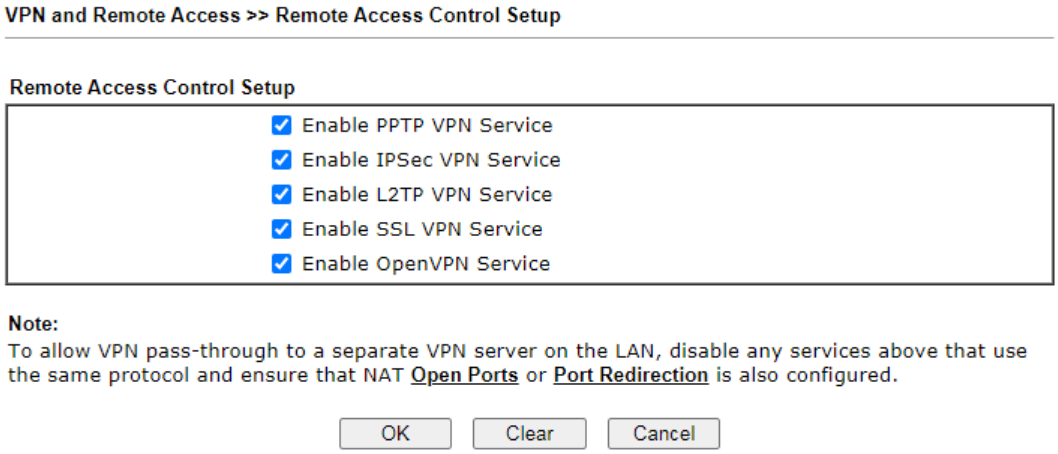
Gestión	
Haz otra VPN Configuración del asistente del servidor	Vuelva a ejecutar el asistente del servidor VPN para configurar otro perfil VPN de LAN a LAN.
Ver más detallado configuración	Abre este perfil en**VPN y acceso remoto>>LAN a LAN** para realizar cambios de configuración adicionales.

7. Haga clic en**Finalizar**para guardar el perfil, o**Atrás**para hacer cambios, o**Cancelar**para salir del asistente sin guardar.

Control de acceso remoto V-1-3

El enrutador Vigor admite varios protocolos para VPN, todos los cuales se pueden habilitar o deshabilitar de forma independiente.

Si tiene la intención de ejecutar un servidor VPN dentro de su LAN, debe deshabilitar el servicio VPN de Vigor Router para permitir el paso del túnel VPN, así como la configuración NAT adecuada, como DMZ o puerto abierto. Abierto**VPN y Acceso Remoto>>Control de Acceso Remoto**.

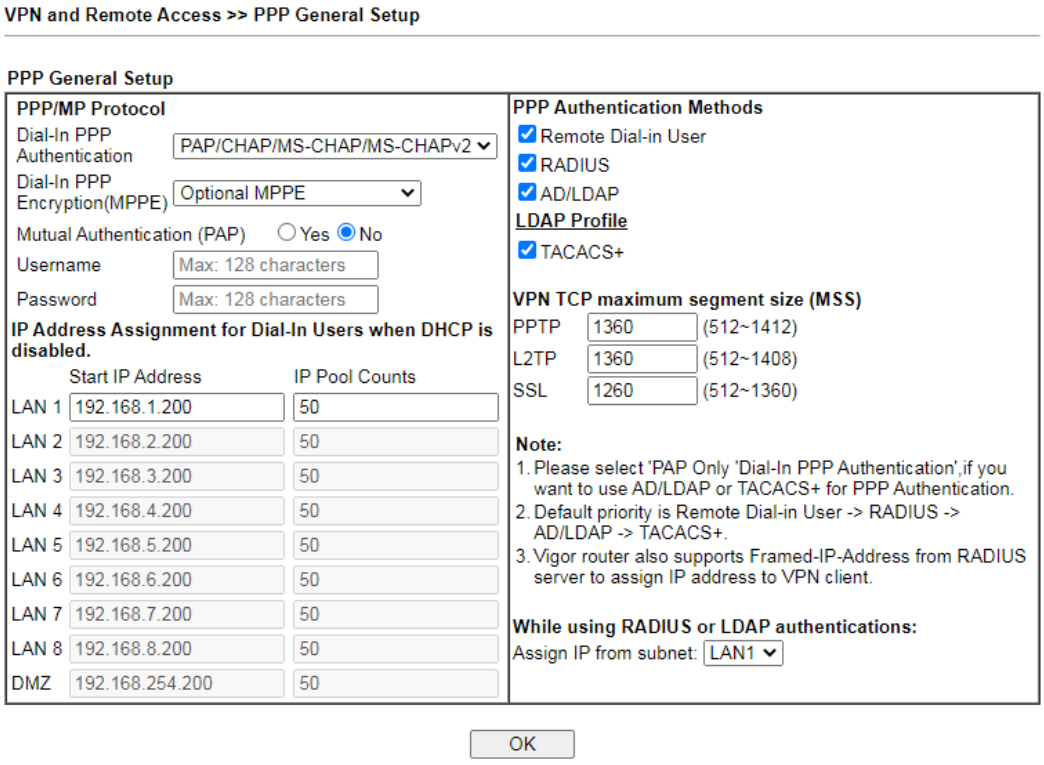


Artículo	Descripción
Habilitar el servicio VPN PPTP	Este es uno de los primeros protocolos VPN y es compatible de forma nativa con todas las versiones de Microsoft Windows desde Windows 95, todos los dispositivos Android, iOS antes de la versión 10 y Mac OS X antes de la versión 10.12. Es fácil de configurar, tiene una sobrecarga baja y es moderadamente seguro.
Habilitar el servicio VPN IPSec	Este es un protocolo de red que cifra el tráfico entre dos ubicaciones de red. Windows, por medio de Windows Firewall, admite de forma nativa túneles IPsec entre puntos finales con direcciones IP estáticas. Para computadoras con direcciones IP asignadas dinámicamente, DrayTek proporciona el cliente SmartVPN.
Habilitar el servicio VPN L2TP	Este es un protocolo de tunelización utilizado en las VPN. No encripta el tráfico de red a menos que se use junto con IPsec.
Habilitar el servicio VPN SSL	Este tipo de VPN utiliza la capa de conexión segura (SSL) y la seguridad de la capa de transporte (TLS), que también se utilizan para cifrar el tráfico hacia y desde los sitios web. Dado que SSL y TLS funcionan sobre TCP y UDP, que son los protocolos de Internet más comunes, es menos probable que tengan problemas con los firewalls y las puertas de enlace.
Habilitar el servicio OpenVPN	Este tipo de VPN ofrece una manera conveniente para que los usuarios creen una VPN entre el extremo local y el extremo remoto.

Para guardar los cambios en la página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**; para borrar la configuración de esta página y volver a la configuración predeterminada, seleccione**Claro**.

V-1-4 Configuración general de PPP

Esta página permite la configuración del Protocolo punto a punto (PPP) utilizado por las conexiones VPN PPTP y L2TP. Desde el menú principal seleccione**VPN y acceso remoto >> Configuración general de PPP**para que aparezca la siguiente página de configuración.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Autenticación PPP de acceso telefónico	**Solo PAP**-Autentique a los usuarios de acceso telefónico utilizando únicamente el protocolo PAP. **PAP/CHAP/MS-CHAP/MS-CHAPv2**-Intente autenticar a los usuarios de acceso telefónico utilizando varios protocolos CHAP y, si el cliente VPN remoto no puede autenticarse, recurra a PAP.
Cifrado PPP de acceso telefónico (MPPE)	Especifica si se utilizará el cifrado PPP (MPPE) para las conexiones VPN de acceso telefónico. **MPPE opcional**-MPPE es opcional. Si el cliente VPN es compatible con MPPE, los datos de PPP se cifrarán. **Requiere MPPE (40/128 bits) -**Requerir cifrado PPP para conexiones VPN de acceso telefónico. Se permiten esquemas de cifrado de 40 y 128 bits. El usuario de acceso telefónico remoto utilizará 40 bits para realizar el cifrado antes de utilizar 128 bits para el cifrado. En otras palabras, si el método de cifrado MPPE de 128 bits no está disponible, se aplicará un esquema de cifrado de 40 bits para cifrar los datos. **MPPE máximo -**Requiere encriptación PPP de 128 bits para todas las conexiones VPN de acceso telefónico.
Autenticacion mutua (PAPILLA)	Especifica si se va a utilizar la autenticación mutua. Algunos pares de VPN (por ejemplo, ciertos enrutadores Cisco) requieren bidireccional

	autenticación utilizada para proporcionar mayor seguridad. Cuando la autenticación mutua está habilitada, los campos Nombre de usuario y Contraseña también deben completarse con valores del par VPN. La longitud máxima de estos campos es de 23 y 19 caracteres, respectivamente. **Sí**–Habilite la autenticación mutua. **No** –Deshabilite la autenticación mutua.
Asignación de dirección IP para usuarios de acceso telefónico cuando DHCP está deshabilitado	**LAN1**-Cuando el servidor DHCP del enrutador está deshabilitado, el enrutador asignará direcciones IP a los usuarios de VPN de acceso telefónico comenzando con la dirección IP especificada en Dirección IP de inicio. El número total de direcciones IP de VPN de marcación de entrada que se proporcionarán se especifica en Recuentos de grupos de IP. LAN2 ~ LAN8 y DMZ estarán disponibles si está habilitado. Consulte LAN>>Configuración general para habilitar la interfaz LAN.
Autenticación PPP Métodos	Las credenciales que se utilizarán para la autenticación PPP se obtendrán de las fuentes seleccionadas, en el siguiente orden: **Usuario de marcación remota**–Se utilizarán los nombres de usuario y las contraseñas de la sección VPN y acceso remoto >> Usuario de marcación remota. **RADIO**–Se utilizará un servidor RADIUS externo para la autenticación. Asegúrese de configurar el servidor RADIUS en la sección Aplicaciones >> RADIUS/TACACS+. **ANUNCIO/LDAP**–Se utilizará un servidor Active Directory/LDAP para la autenticación. Asegúrese de configurar los ajustes de AD y LDAP en Aplicaciones >> Active Directory/LDAP. **TACACS+**–Se utilizará un servidor TACACS+ para la autenticación. Asegúrese de configurar el servidor RADIUS en la sección Aplicaciones >> RADIUS/TACACS+.
Perfil PPTP LDAP	Los perfiles LDAP configurados se enumerarán en dicho elemento. Simplemente marque el que desee para habilitar la autenticación PPP mediante perfiles de servidor LDAP. Sin embargo, si no hay ningún perfil en la lista, simplemente haga clic en el enlace de **Perfil PPTP LDAP**para crear/agregar algunos perfiles LDAP nuevos que desee.
VPN TCP máximo **tamaño del segmento (MSS)**	Establezca el tamaño máximo de segmento (MSS) para diferentes tipos de VPN. Especifique los valores de MSS para cada tipo para evitar paquetes cortados por MTU durante el período de transmisión de datos a través de la conexión VPN IPsec.
Mientras usa la autenticación Radius o LDAP	Cuando el usuario de VPN de marcación de entrada se autentica con las credenciales de la sección Usuario de marcación de entrada remota, se asignará una dirección IP de la LAN especificada en el perfil de usuario. Cuando el usuario se autentica con credenciales de otras fuentes (RADIUS, AD, TACACS+), la dirección IP asignada se extraerá del grupo de direcciones de la LAN especificada aquí.

Para guardar los cambios en la página, seleccione**DE ACUERDO**.

Configuración general de SSL V-1-5

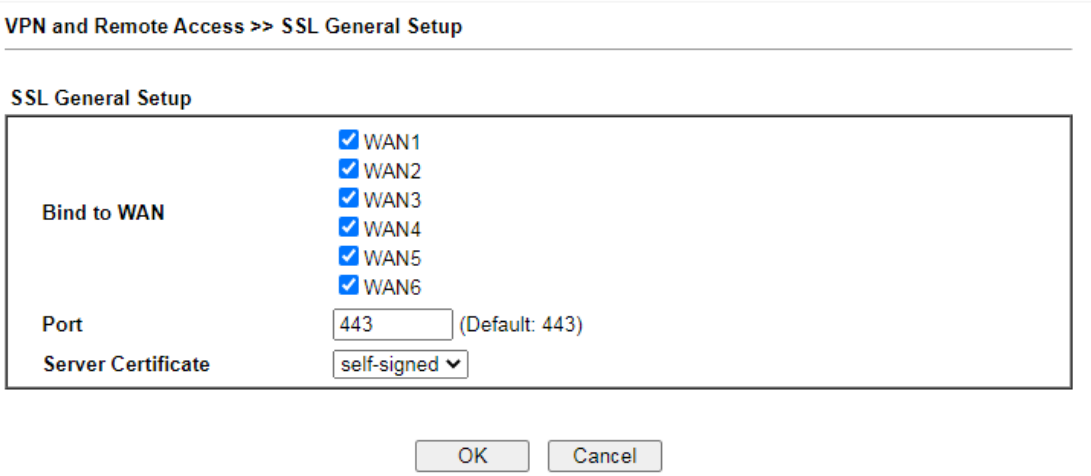
SSL VPN (red privada virtual de capa de conexión segura) es una forma de VPN que encripta el tráfico usando SSL, que es la misma tecnología que se usa en los sitios web seguros. Debido a la importancia de SSL como protocolo de encriptación en Internet, la mayoría de las redes tienen pocas restricciones en el tráfico SSL y, como resultado, es más probable que SSL VPN funcione cuando otras tecnologías VPN experimentan dificultades debido a obstáculos como firewalls y traducción de direcciones de red (NAT).).

En breve,

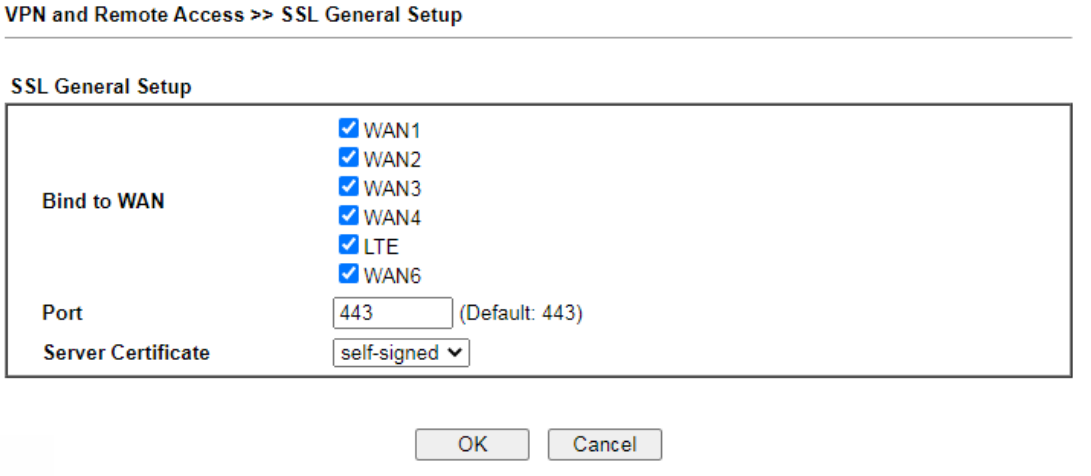
-No es necesario que los usuarios preinstalen el software del cliente VPN para ejecutar la conexión SSL VPN.

-Hay menos restricciones para los datos cifrados a través de SSL VPN en comparación con la VPN tradicional.

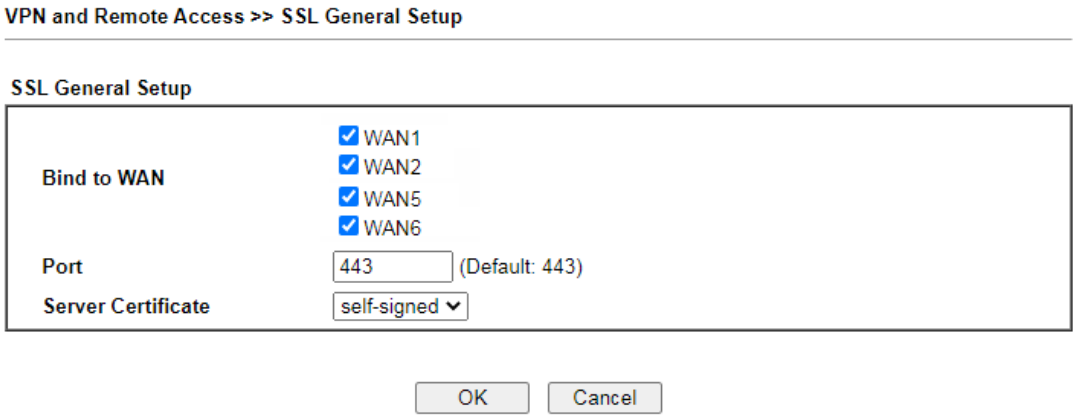
Esta página determina la configuración general para SSL VPN Server y SSL Tunnel.



o



O



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Vincular a WAN	Seleccione las interfaces WAN para aceptar conexiones SSL VPN entrantes.
Puerto	El puerto que se utilizará para el servidor SSL VPN. Es independiente del puerto de gestión (Puerto HTTPS) que está configurado en **Mantenimiento del Sistema>>Gestión.**La configuración predeterminada es 443.
Certificado de servidor	Especifique el certificado que se utilizará para las conexiones SSL. Seleccione un certificado de los certificados importados o generados en el enrutador, o elija Autofirmado para usar el certificado predeterminado integrado del enrutador. El certificado seleccionado se puede utilizar en el servidor VPN SSL y el proxy web HTTPS.

Para guardar los cambios en esta página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**.

En**Configuración general de IPsec,**hay dos partes principales de

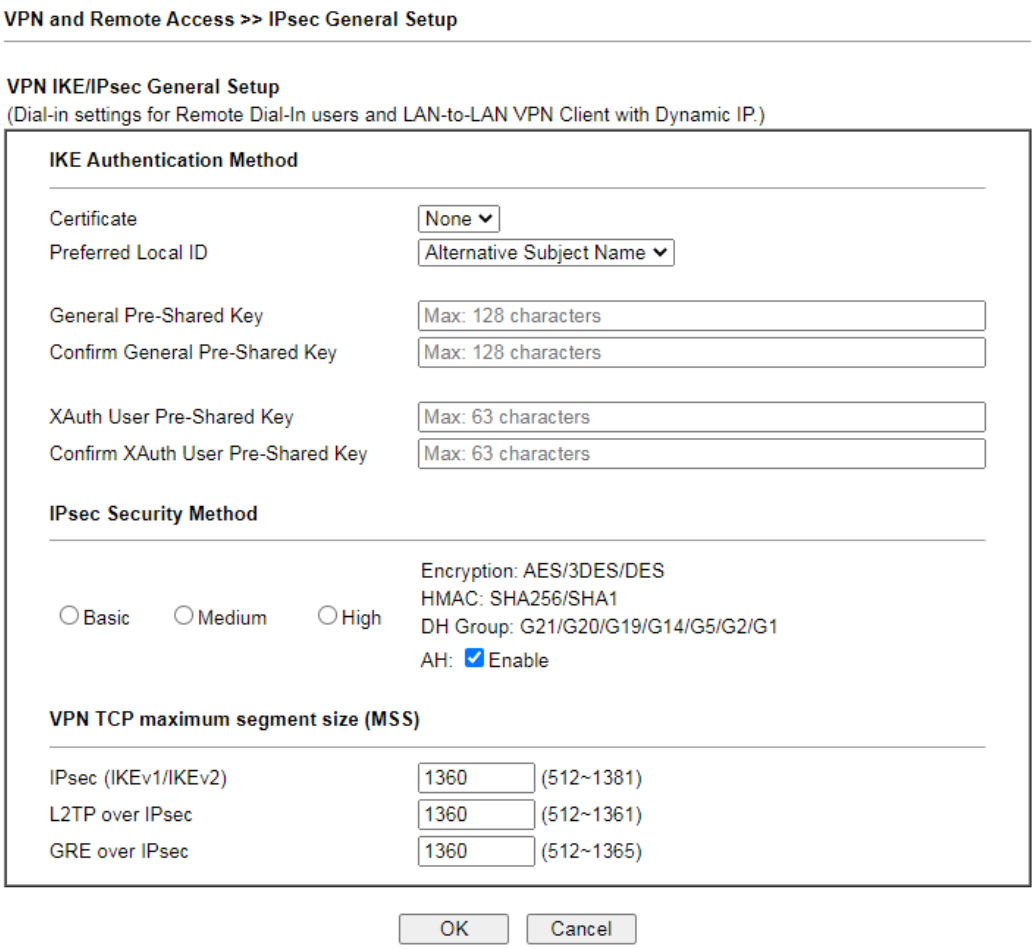
configuración. Hay dos fases de IPsec.

- Fase 1: negociación de parámetros IKE que incluyen cifrado, hash, valores de parámetros Diffie-Hellman y vida útil para proteger el siguiente intercambio IKE, autenticación de ambos pares mediante una clave precompartida o una firma digital (x.509). El par que inicia la negociación propone todas sus políticas al par remoto y luego el par remoto intenta encontrar una coincidencia de mayor prioridad con sus políticas. Eventualmente para configurar un túnel seguro para IKE Fase 2.
- Fase 2: negociación de métodos de seguridad IPsec, incluido el encabezado de autenticación (AH) o la carga útil de seguridad encapsulada (ESP) para el siguiente intercambio IKE y el examen mutuo del establecimiento del túnel seguro.

Hay dos métodos de encapsulación utilizados en IPsec,**Transporte**y**Túnel**. El**Transporte** agregará la carga útil AH/ESP y usará el encabezado IP original para encapsular la carga útil de datos únicamente. Solo se puede aplicar al paquete local, por ejemplo, L2TP sobre IPsec. El**Túnel**El modo no solo agregará la carga útil AH/ESP, sino que también usará un nuevo encabezado IP (encabezado IP tunelizado) para encapsular todo el paquete IP original.

AH (Encabezado de autenticación) proporciona autenticación e integridad de datos para los paquetes IP que se pasan entre pares de VPN. Esto se logra mediante una función hash unidireccional con clave en el paquete para crear un resumen del mensaje. Este resumen se colocará en el AH y se transmitirá junto con los paquetes. En el lado receptor, el par realizará el mismo hash unidireccional en el paquete y comparará el valor con el del AH que recibe.

ESP (Encapsulating Security Payload) es un protocolo de seguridad que brinda confidencialidad y protección de datos con autenticación opcional y servicio de detección de reproducción.



Los ajustes disponibles se explican a continuación:

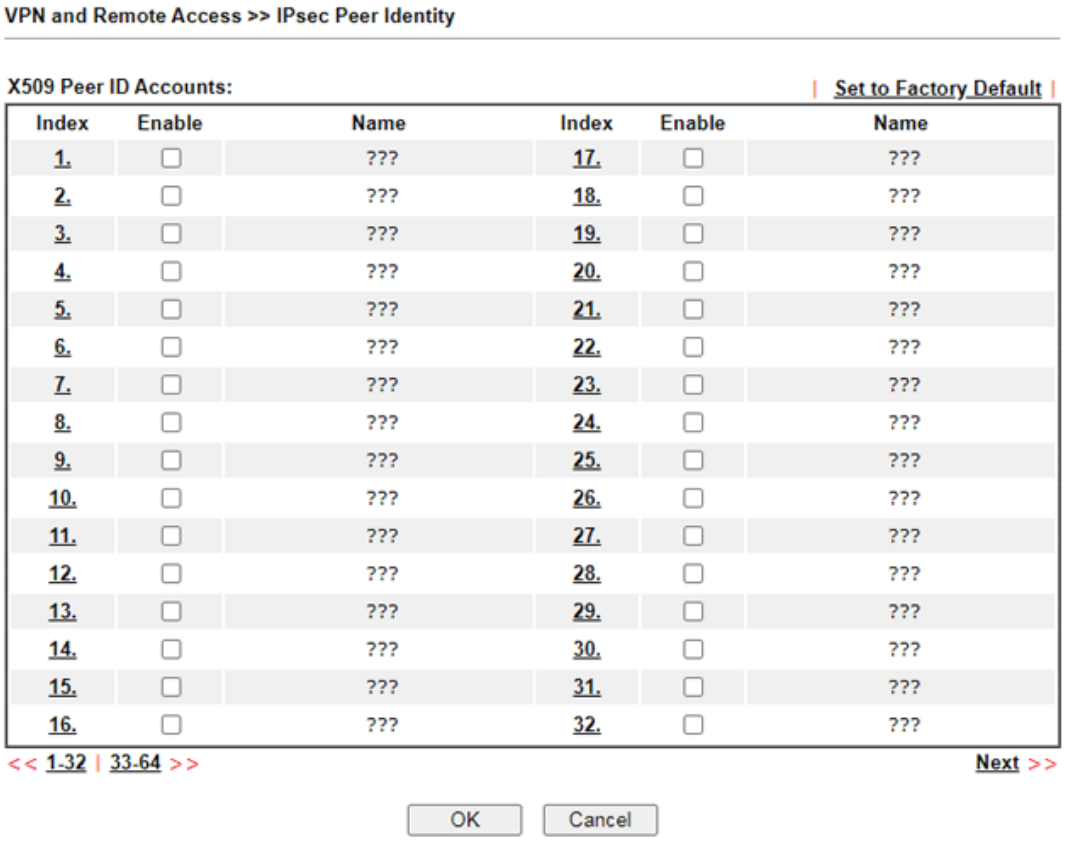
Artículo	Descripción
Autenticación IKE **Método**	Esto generalmente se aplica a aquellos que son usuarios o nodos de marcación remota (LAN a LAN) que utilizan una dirección IP dinámica y conexiones VPN relacionadas con IPsec, como L2TP sobre IPsec y túnel IPsec. Hay dos métodos ofrecidos por el enrutador Vigor para que usted autentique los datos entrantes provenientes del usuario de marcación remota, **Certificado (X.509)**y**Clave precompartida**. **Certificado**–Los certificados X.509 se pueden usar para la autenticación IKE. Para configurar certificados en el enrutador, vaya a la sección Administración de certificados. **Identificación local preferida**-Especifique la información de identificación local preferida**(Nombre alternativo del sujeto primero**o**Nombre del sujeto primero**) para la autenticación de IPsec mientras el cliente está usando la configuración general (sin una IP o ID de par específica en el perfil de VPN). **Clave precompartida general-**Defina la clave PSK para la autenticación general. **Confirmar clave precompartida general-**Vuelva a ingresar los caracteres para confirmar la clave precompartida. **Clave precompartida de usuario XAuth -**Defina la clave PSK para la autenticación IPsec XAuth. **Confirmar clave precompartida de usuario XAuth-**Vuelva a ingresar los caracteres para confirmar la clave precompartida para IPsec XAuth

	autenticación. **Nota**: cualquier paquete del usuario de marcado remoto que no coincida con la regla definida en**VPN y acceso remoto>>Usuario de marcado remoto**se aplicará con el método especificado aquí.
Método de seguridad IPsec	Los métodos disponibles incluyen**Básico, Medio**y**Alto**. Cada método ofrece diferentes cifrados, HMAC y DH Group. **Básico -**El encabezado de autenticación (AH) significa que los datos se autenticarán, pero no se cifrarán. Por defecto, esta opción está activa. **Medio -**Cuando se selecciona esta opción, el protocolo de encabezado de autenticación (AH) se puede usar para proporcionar autenticación al tráfico IPsec. **Alto**-Cuando se selecciona esta opción, el protocolo de carga útil de seguridad encapsulada (ESP) se puede utilizar para proporcionar autenticación y cifrado al tráfico IPsec. Se admiten tres estándares de cifrado para ESP: DES, 3DES y AES, en orden ascendente de seguridad.
VPN TCP máximo **tamaño del segmento (MSS)**	Establezca el tamaño máximo de segmento (MSS) para diferentes tipos de VPN. Especifique los valores de MSS para cada tipo para evitar paquetes cortados por MTU durante el período de transmisión de datos a través de la conexión VPN IPsec.

Para guardar los cambios en la página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**.

V-1-7 Identidad de pares IPsec

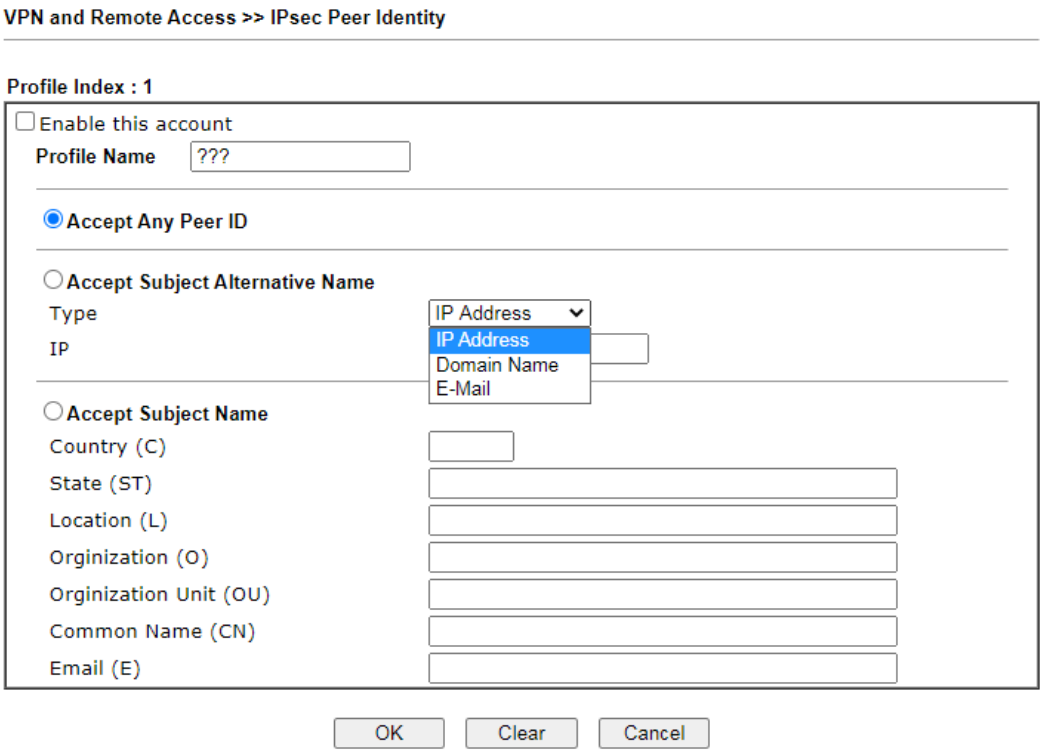
Esta pantalla permite crear perfiles de nombres alternativos de sujeto (SAN) y nombres distinguidos/nombres de sujeto que se pueden usar para la autenticación de pares IPsec en conexiones VPN de LAN a LAN o de usuario remoto.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Establecer como predeterminado de fábrica	Haga clic en él para borrar todos los índices.
Índice	Haga clic en el número de índice del perfil para ver o editar su configuración.
Permitir	Marque para habilitar el perfil.
Nombre	Nombre ingresado por el usuario que identifica el perfil.

La siguiente pantalla de configuración se muestra después de hacer clic en un índice de perfil.

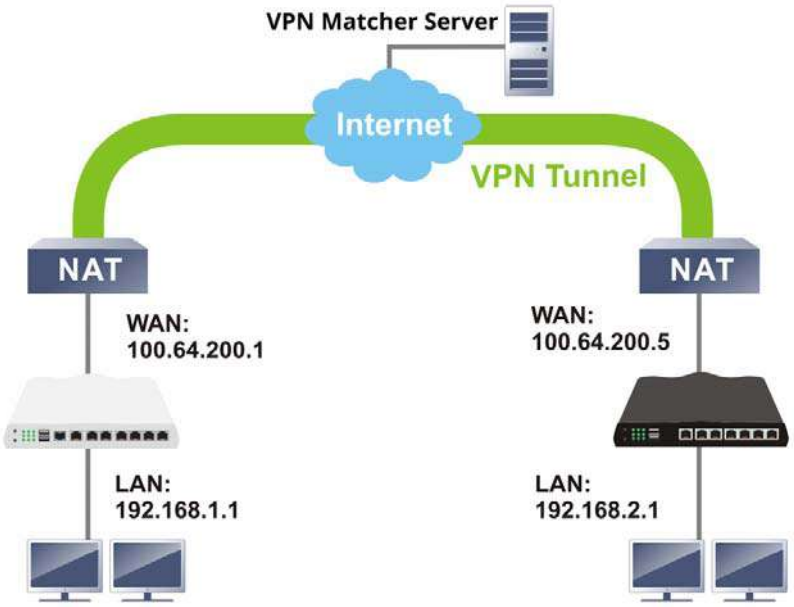


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar esta cuenta	Marque para habilitar dicho perfil de cuenta.
Nombre de perfil	Un nombre que le permita identificar este perfil. La longitud máxima del nombre que puede establecer es de 32 caracteres.
Aceptar cualquier ID de compañero	Cuando se selecciona esta opción, el enrutador acepta cualquier nombre alternativo de sujeto o nombre de sujeto como válido, independientemente del tipo y el valor.
Aceptar Asunto Nombre alternativo	Cuando se selecciona esta opción, el enrutador acepta el tipo y el valor del nombre alternativo del sujeto especificado como autenticación válida. Los tipos alternativos de materias admitidos son**Dirección IP**,**Nombre de dominio**y**Correo electrónico**.
Aceptar nombre del sujeto	Cuando se selecciona esta opción, el enrutador realiza la autenticación de pares haciendo coincidir los valores de los diferentes campos de nombre de sujeto. Estos campos incluyen**País (C), Estado (ST), Ubicación (L), Organización (O), Unidad de organización (OU), Nombre común (CN),**y**Correo electrónico (E)**.

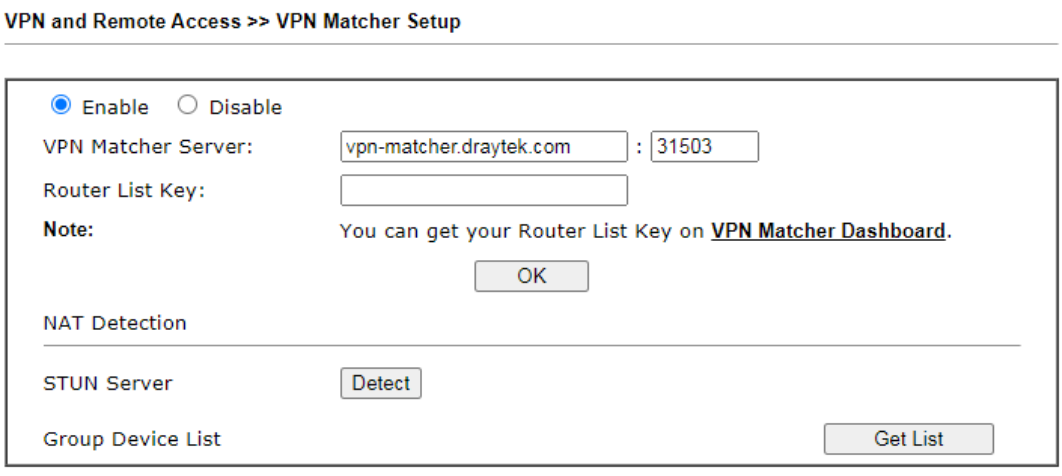
Para guardar los cambios en la página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**; para borrar la configuración de esta página y volver a la configuración predeterminada, seleccione**Claro**.

Normalmente, para establecer una conexión VPN, al menos un compañero debe tener una dirección IP pública. El servidor VPN Matcher puede ayudar a dos enrutadores Draytek detrás de NAT a establecer un túnel VPN seguro para la transmisión de datos entre ellos. Consulte la siguiente figura.



Hay una limitación para la conexión VPN. Ambos enrutadores deben estar detrás de un NAT de cono, pero no de un NAT simétrico.

Ir a**VPN y acceso remoto>>Configuración de VPN Matcher**para abrir la página siguiente.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar deshabilitar	Haga clic para activar/desactivar la función de configuración de VPN Matcher.
Servidor de comparación de VPN	La dirección IP del servidor DrayTek VPN Matcher se define como "vpn-matcher.draytek.com" con el número de puerto "31503".
Clave de la lista de enrutadores	Ingrese la clave de autenticación para encontrar un enrutador Vigor con el mismo grupo de este dispositivo desde el servidor de comparación de VPN. Luego configure un enlace VPN entre los enrutadores Vigor en ambos extremos a través de

	Asistente de VPN.
DE ACUERDO	Haga clic para guardar la configuración.
Servidor STUN	**Detectar**-Haga clic para verificar si el NAT utilizado por el enrutador Vigor es NAT central o no. De lo contrario, no se puede establecer una VPN.
Lista de dispositivos de grupo	**Obtener lista**-Después de ingresar la Authkey anterior, haga clic para obtener el enrutador Vigor disponible que se encuentra dentro del mismo grupo que este dispositivo.

V-1-9 VPN abierta

El protocolo OpenVPN utiliza claves públicas, certificados y nombres de usuario y contraseñas para autenticar al cliente. El tráfico se transporta a través de canales seguros basados en protocolos de encriptación SSL/TLS estándar de la industria.

Con la integración de OpenVPN, el enrutador Vigor puede ayudar a los usuarios a lograr conexiones privadas más sólidas, confiables y seguras para las necesidades comerciales.

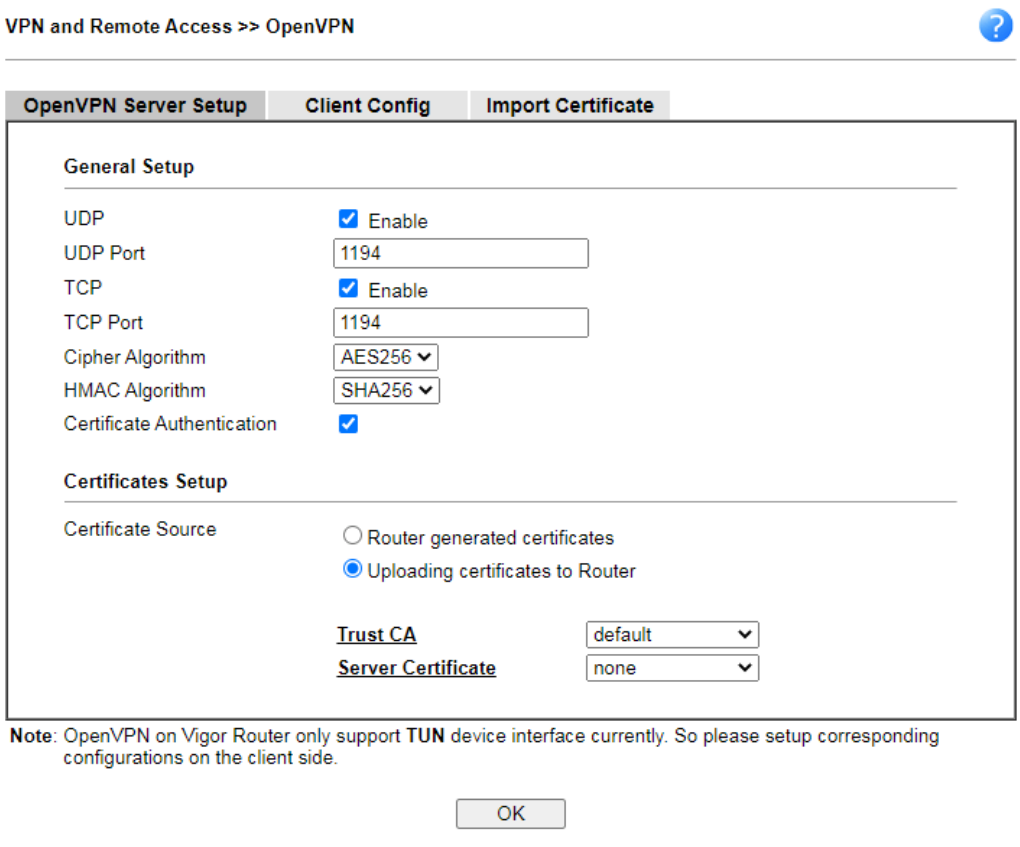
OpenVPN ofrece una manera conveniente para que los usuarios construyan una VPN entre el extremo local y el extremo remoto. Hay dos ventajas de OpenVPN:

- Se puede operar en diferentes sistemas como Windows, Linux y MacOS.
- Basado en el protocolo estándar de encriptación SSL, OpenVPN puede proporcionarle un modo cliente/servidor escalable, lo que permite que varios clientes se conecten a un solo proceso de servidor OpenVPN a través de un solo puerto TCP o UDP.

En términos de credenciales, el administrador puede optar por dejar que el enrutador genere los certificados o importar certificados emitidos por autoridades de certificación (CA) de terceros. Cuando el enrutador genera los certificados, actúa como la CA raíz para emitir los certificados de CA de confianza (almacenados en Administración de certificados >> Certificado de CA de confianza), que se utilizan para generar los certificados de servidor y cliente utilizados por OpenVPN (almacenados en Administración de certificados > > Certificado local). Sin embargo, si se utiliza un certificado emitido por una CA de terceros, tanto el certificado de la CA como el certificado emitido deben importarse al enrutador en las secciones Certificado de CA de confianza y Certificado local, respectivamente.

Configuración del servidor V-1-9-1 OpenVPN

OpenVPN requiere el uso de certificados. Antes de establecer la conexión OpenVPN, primero se deben configurar los ajustes generales para el servicio OpenVPN.

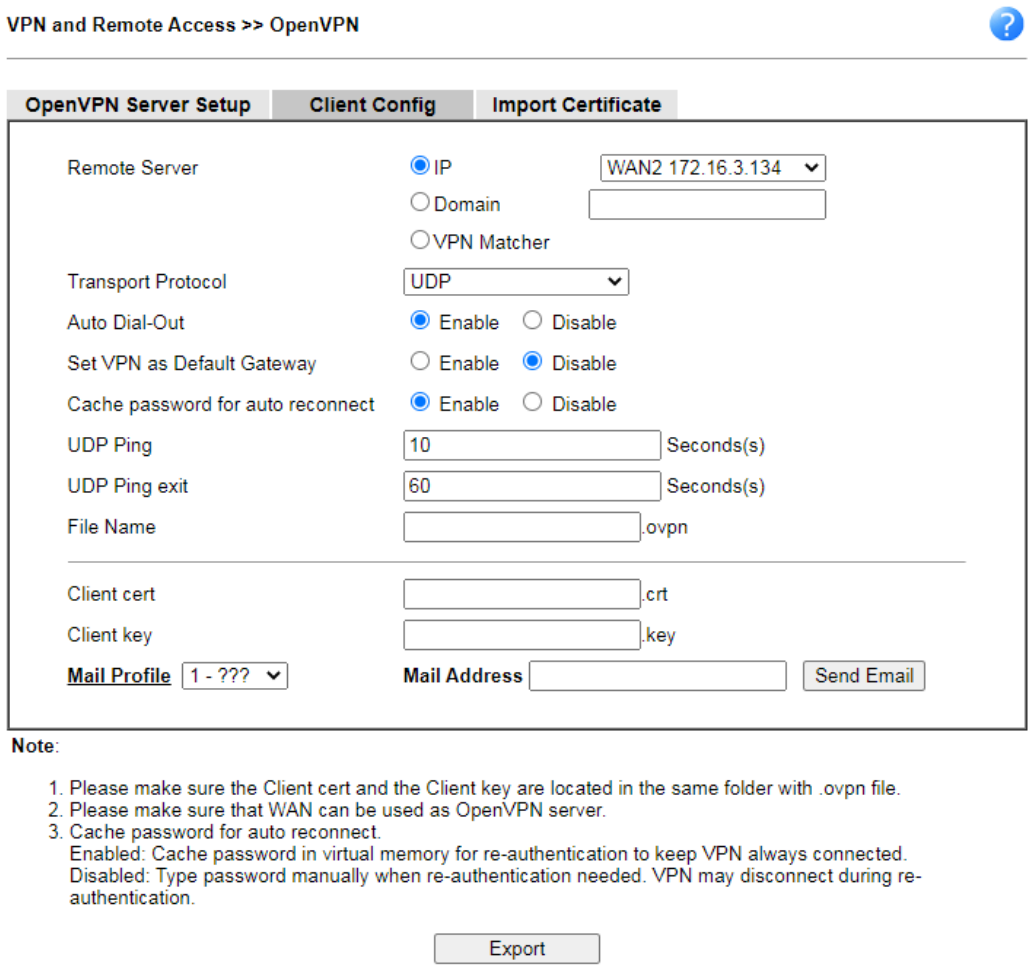


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Configuración general	
UDP	**Permitir -**Seleccione la casilla de verificación para habilitar el protocolo UDP para conexiones OpenVPN. **El puerto UDP**–Introduzca el número de puerto UDP.
TCP	**Permitir -**Seleccione la casilla de verificación para habilitar el protocolo TCP para conexiones OpenVPN. **Puerto TCP**–Introduzca el número de puerto TCP.
Algoritmo de cifrado	Seleccione el algoritmo de cifrado deseado. Se admiten dos algoritmos de cifrado: AES128 y AES256. AES256 es más seguro que AES128, pero puede resultar en un menor rendimiento porque incurre en una mayor sobrecarga computacional.
Algoritmo HMAC	HMAC significa Código de autenticación de mensajes basado en hash. Se utiliza para validar la integridad de los datos y la autenticidad de los datos de la VPN. Seleccione el algoritmo hash HMAC deseado. Se admiten dos algoritmos hash, SHA1 y SHA256. Se prefiere SHA256 porque es más robusto y confiable que SHA1.
Autenticación de certificados	Seleccione esta casilla de verificación si desea validar que el certificado de cliente fue emitido por una CA de confianza.
Configuración del certificado	
Origen del certificado	Seleccione una fuente para el certificado que se usará para OpenVPN. **Certificados generados por el enrutador**-Certificados generados por el enrutador que se utilizarán para OpenVPN. - **GENERAR**-Haga clic para generar un certificado. - **Eliminar todos los certificados**-Haga clic para eliminar todos los certificados generados por el enrutador. **Subir certificados al enrutador**-Se utilizarán certificados de terceros para OpenVPN. - **Confiar en CA**-Utilice la lista desplegable para seleccionar un certificado de CA de confianza que ya se haya cargado en el enrutador. Para cargar certificados de Trusted CA en el enrutador, haga clic en el enlace Trust CA y accederá al **Gestión de certificados >> Certificado de CA de confianza** página para realizar la operación. - **Certificado de servidor**-Utilice la lista desplegable para seleccionar un certificado de servidor que ya se haya cargado en el enrutador. Para cargar certificados de servidor en el enrutador, haga clic en el enlace Certificado de servidor y accederá a la**Gestión de certificados >> Certificado local** página para realizar la operación.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

En esta página, puede crear y exportar la configuración requerida para que un cliente OpenVPN remoto se conecte al enrutador.



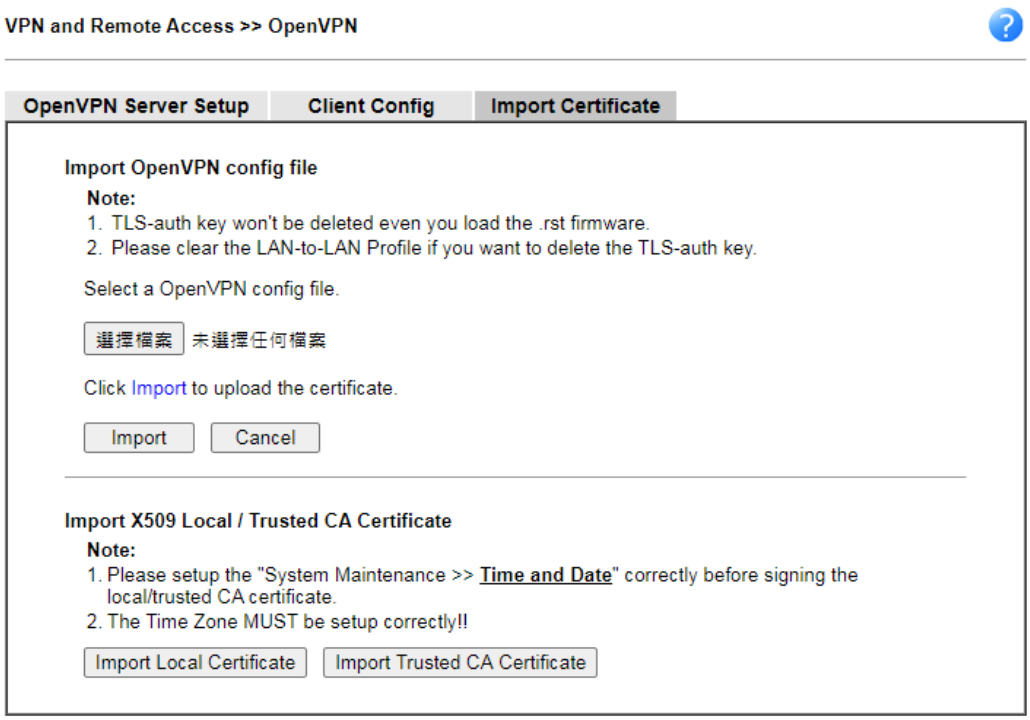
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Servidor remoto	El cliente OpenVPN utilizará la dirección IP o el nombre de dominio para conectarse al enrutador. Seleccione IP o Dominio. **IP**–El archivo de configuración de OpenVPN utilizará la dirección IP numérica como la dirección del servidor. **Dominio**–El archivo de configuración de OpenVPN utilizará el dominio como dirección del servidor. Debe asegurarse de que el dominio se resuelva en la dirección IP de un puerto WAN del enrutador. **Comparador de VPN**-El archivo de configuración de OpenVPN utilizará el comparador de VPN como la dirección del servidor.
Protocolo de transporte	Seleccione UDP o TCP para el protocolo que utilizará el cliente OpenVPN para conectarse al enrutador.
Llamada de salida automática	**Permitir**-Si se selecciona, el cliente remoto puede marcar automáticamente a este enrutador Vigor para construir un túnel OpenVPN. **Desactivar**-Seleccione para deshabilitar la función.
Establecer VPN como puerta de enlace predeterminada	**Permitir**-Si se selecciona, el enrutador Vigor se tratará como una puerta de enlace "predeterminada" para los clientes de OpenVPN. El cliente OpenVPN redirigirá todo el tráfico al enrutador Vigor a través del

	Túnel OpenVPN. **Desactivar**-Seleccione para deshabilitar la función.
Contraseña de caché para reconexión automática	**Permitir**-OpenVPN se volverá a conectar cada hora. Durante la reconexión, se requiere la contraseña. Si la función está habilitada, la contraseña para la conexión OpenVPN será guardada y utilizada por el sistema Vigor para la reconexión cada vez. **Desactivar**-Seleccione para deshabilitar la función.
Ping de UDP	Haga ping al dispositivo remoto a través del canal de control UDP, si no se han enviado paquetes durante la cantidad de segundos configurada aquí.
Salida de ping UDP	Deje que OpenVPN salga después de los segundos establecidos aquí si no se recibe un ping u otro paquete desde el dispositivo remoto.
Nombre del archivo	Ingrese el nombre de archivo del archivo de configuración que se descargará del enrutador.
certificado de cliente	Ingrese el nombre de archivo del certificado de cliente obtenido del proveedor externo.
clave de cliente	Ingrese el nombre de archivo de la clave privada obtenida del proveedor externo.
Perfil de correo	Utilice la lista desplegable para especificar un perfil de correo. **Correo Electronico**-Ingrese la dirección de correo para recibir el correo de notificación. **Enviar correo electrónico**-Haga clic para enviar el correo.
Exportar	Haga clic en este botón para descargar la configuración de esta página como un archivo, que se puede importar a un cliente VPN para establecer conexiones OpenVPN.

Certificado de Importación V-1-9-3

En esta página, puede importar el certificado desde otros lugares para que un cliente OpenVPN remoto se conecte al enrutador.



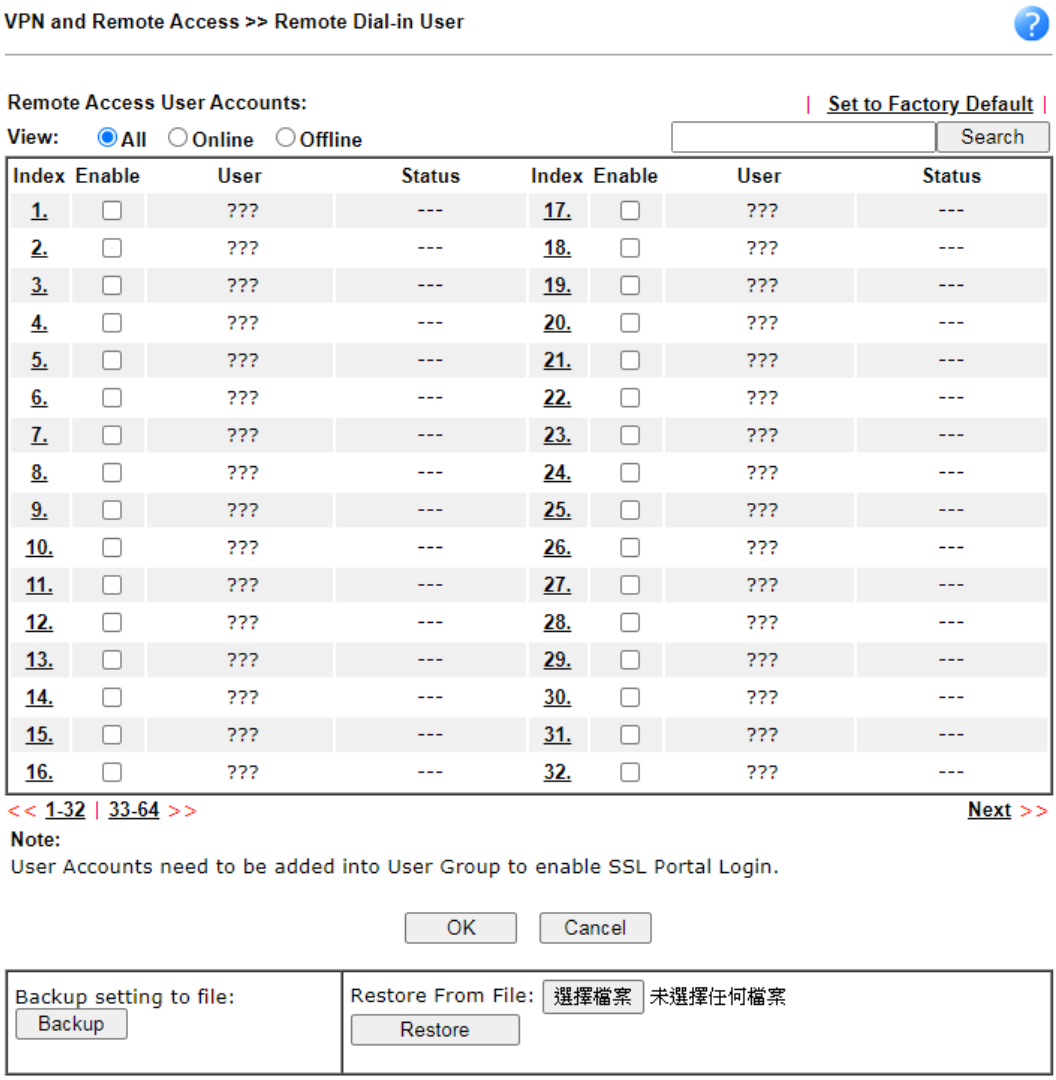
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Importar configuración de OpenVPN	
Seleccione un archivo de configuración de OpenVPN	**Navegar**-Haga clic para seleccionar un archivo. **Importar**-Haga clic para importar un archivo de configuración.
Importar certificado de CA de confianza/local X509	
Importar certificado local	Haga clic para acceder a la página Certificado local para importar un certificado.
Importar CA de confianza Certificado	Haga clic para acceder a la página Certificado de CA de confianza para importar un certificado.

V-1-10 Usuario de marcado remoto

Puede administrar el acceso remoto manteniendo una tabla de perfiles de usuarios remotos, de modo que los usuarios puedan autenticarse a través de una conexión VPN.

Los perfiles de usuario de marcación remota se pueden configurar en esta pantalla.



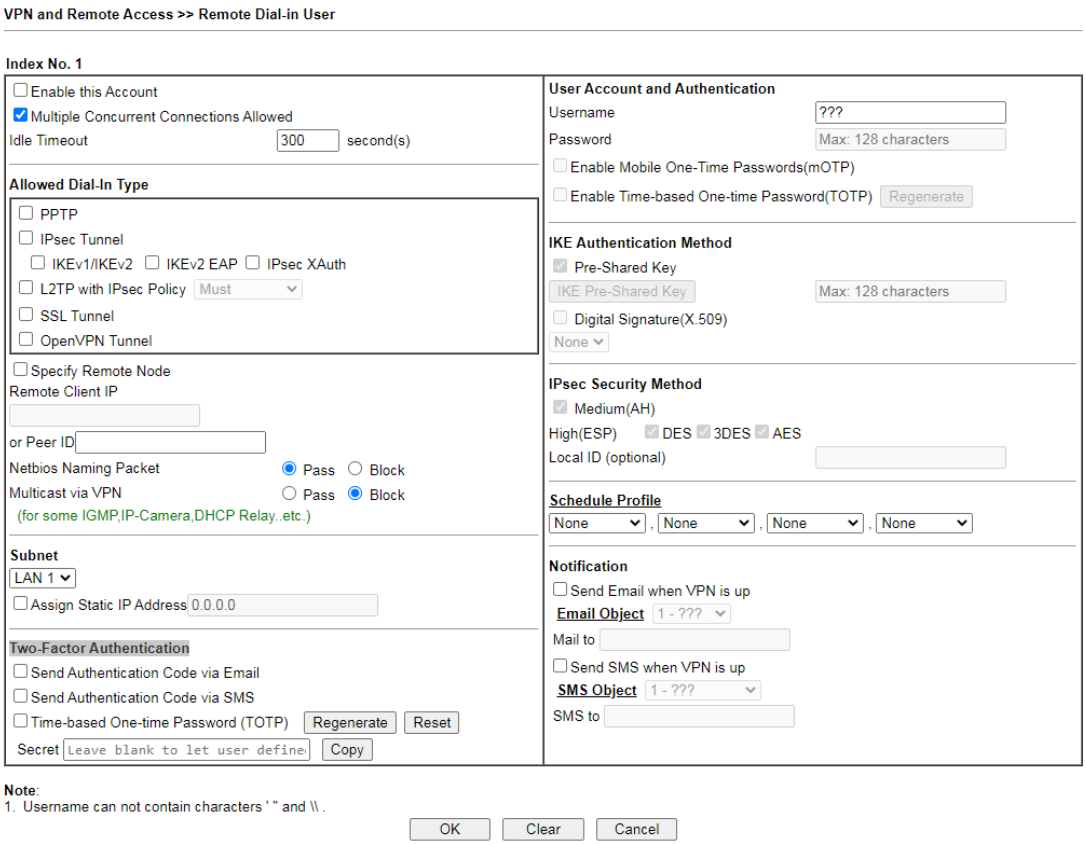
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Establecer como predeterminado de fábrica	Haga clic para borrar todos los perfiles de usuario de marcado remoto.
Índice	Haga clic en el número de índice del perfil para ver o editar su configuración.
Permitir	Marque para habilitar el perfil de usuario.
Usuario	Muestre el nombre de usuario para el usuario de acceso telefónico específico del perfil de LAN a LAN. El símbolo**???**representa que el perfil está vacío.
Estado	Muestra la subred LAN y el método de asignación de direcciones IP. Ejemplo: LAN1-DHCP significa que la dirección IP de la VPN

	la conexión se extraerá del grupo DHCP de la subred LAN1. El color del estado indica el estado actual del perfil: Verde: el perfil está siendo utilizado por una conexión VPN de acceso telefónico. Rojo: el perfil no se está utilizando. Negro: el perfil está deshabilitado.
Respaldo	Hacer clic**Respaldo**para guardar la configuración.
Restaurar	Hacer clic**Seleccionar**para elegir un archivo de configuración. Luego haga clic **Restaurar**para aplicar el archivo.

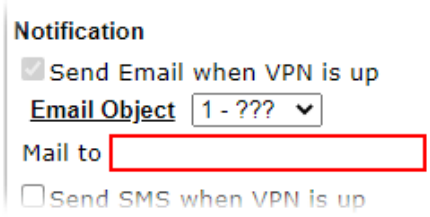
Para guardar los cambios en la página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione

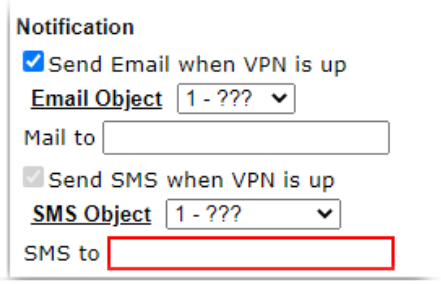
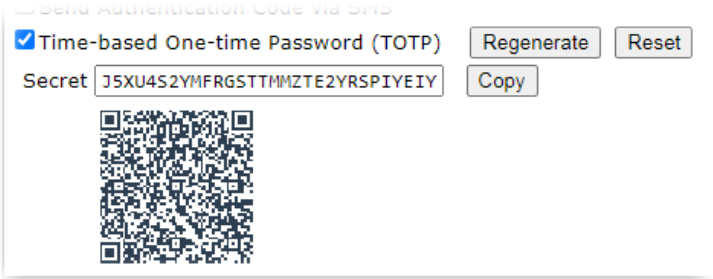
Cancelar. La siguiente pantalla de configuración se muestra después de hacer clic en un índice de perfil.

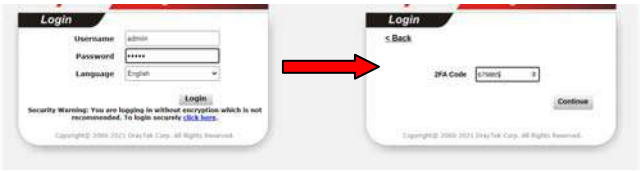


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar esta cuenta	Seleccione esta opción para habilitar este perfil para que lo utilicen los usuarios de acceso telefónico remoto.
múltiples concurrentes Conexiones permitidas	Seleccione para hacer que varios clientes VPN se conecten al dispositivo Vigor con el mismo nombre de usuario/contraseña. **Tiempo de inactividad**-Tiempo de inactividad permitido antes de que el enrutador desconecte la conexión VPN. El valor de tiempo de espera predeterminado es de 300 segundos.
Tipo de acceso telefónico permitido	Seleccione todos los protocolos VPN permitidos para este perfil. Para L2TP, especifique cómo se debe aplicar IPsec. Las opciones son: -**Ninguno**–IPsec no se puede utilizar con conexiones L2TP.

	- **Agradable tener**–Se prefiere IPsec pero no es obligatorio para las conexiones L2TP. - **Debe**–Se requiere IPsec cuando se establecen conexiones L2TP. **Especificar nodo remoto**-La dirección IP del cliente VPN remoto (IP de cliente remoto) o la ID de pares (utilizada en el modo agresivo de IKE) se pueden especificar opcionalmente. El enrutador rechazará la conexión si cualquiera de estos valores se ingresa en el perfil pero el cliente remoto no pasa el valor o pasa el valor incorrecto. **Paquete de nombres de Netbios -**Especifica si se permite que los paquetes de nombres de NetBIOS atraviesen el túnel VPN. - **Aprobar**–Haga clic en él para consultar la transmisión de datos entre los hosts ubicados a ambos lados del Túnel VPN mientras se conecta. - **Bloquear**–Cuando se produce un conflicto entre los hosts en ambos lados del túnel VPN al conectarse, dicha función puede bloquear la transmisión de datos del paquete de nombres de Netbios dentro del túnel. **Multidifusión a través de VPN**-Especifica si permitir que los paquetes de multidifusión atraviesen el túnel VPN. - **Aprobar**–Haga clic en este botón para permitir que los paquetes de multidifusión pasen a través del enrutador. - **Bloquear**–Esta es la configuración predeterminada. Haga clic en este botón para permitir que el enrutador bloquee los paquetes de multidifusión.
subred	El cliente VPN recibirá una dirección IP del conjunto de DHCP o el rango de direcciones IP especificado en Asignación de direcciones IP para usuarios de acceso telefónico para la subred LAN seleccionada. **Asignar dirección IP estática**–Como alternativa, se puede configurar una dirección IP estática seleccionando la casilla de verificación Asignar dirección IP estática. **Nombre de usuario**-Se utiliza para el tipo de marcación de túnel PPTP, L2TP o SSL. La longitud del nombre está limitada a 23 caracteres. **Contraseña**-Se utiliza para el tipo de marcación de túnel PPTP, L2TP o SSL. La longitud de la contraseña está limitada a 19 caracteres.
dos factores Autenticación	Cuando un usuario remoto dal-in intenta iniciar sesión en el enrutador Vigor desde la VPN, debe pasar la autenticación de dos factores. **Enviar código de autenticación por correo electrónico**-Seleccione para enviar el código de autenticación a través de un correo electrónico. La dirección de correo electrónico se puede especificar en el campo de**Correo a**bajo la**Notificación**área.  **Enviar código de autenticación por SMS**-Seleccione para enviar el código de autenticación a través de un SMS. El número de teléfono se puede especificar en el campo de**SMS a**bajo la**Notificación** área.

	 **Contraseña de un solo uso basada en el tiempo (TOTP)**-Seleccione para mostrar un secreto generado por el enrutador Vigor. **Regenerado**-Haga clic para generar un nuevo código QR secreto y correspondiente. **Reiniciar**-Haga clic para borrar el secreto. **Secreto**-Muestra un número secreto de 32 dígitos generado por el enrutador Vigor. El código correspondiente también se mostrará en esta área.  **Copiar**-Haga clic para copiar el secreto.
Cuenta de usuario y Autenticación	**Nombre de usuario**-Se utiliza para el tipo de marcación de túnel PPTP, L2TP o SSL. La longitud del nombre está limitada a 23 caracteres. **Contraseña**-Se utiliza para el tipo de marcación de túnel PPTP, L2TP o SSL. La longitud de la contraseña está limitada a 19 caracteres. **Habilitar contraseñas móviles de un solo uso (mOTP) -**Seleccione para habilitar las contraseñas de un solo uso (Mobile-OTP). Introduzca el código PIN y el secreto. El cliente SmartVPN de DrayTek tiene soporte incorporado para mOTP. Los clientes mOTP de terceros se pueden usar para generar contraseñas cuando se usan otros clientes VPN. Para obtener más información sobre mOTP, visite la página de inicio de Mobile-OTP. - **Código PIN**–Introduzca el código de autenticación (p. ej., 1234). - **Secreto**–Utilice el número secreto de 32 dígitos generado por mOTP en el teléfono móvil (p. ej., e759bb6f0e94c7ab4fe6). **Habilitar contraseña de un solo uso basada en el tiempo (TOTP) -** Asegúrese de que la zona horaria de su enrutador sea correcta. Luego, instale la aplicación Google Authenticator en su teléfono celular. Abra la aplicación para escanear el código QR en esta página. Se mostrará una contraseña de un solo uso en su teléfono. en el archivado de**Código de validación**, ingrese la contraseña de un solo uso

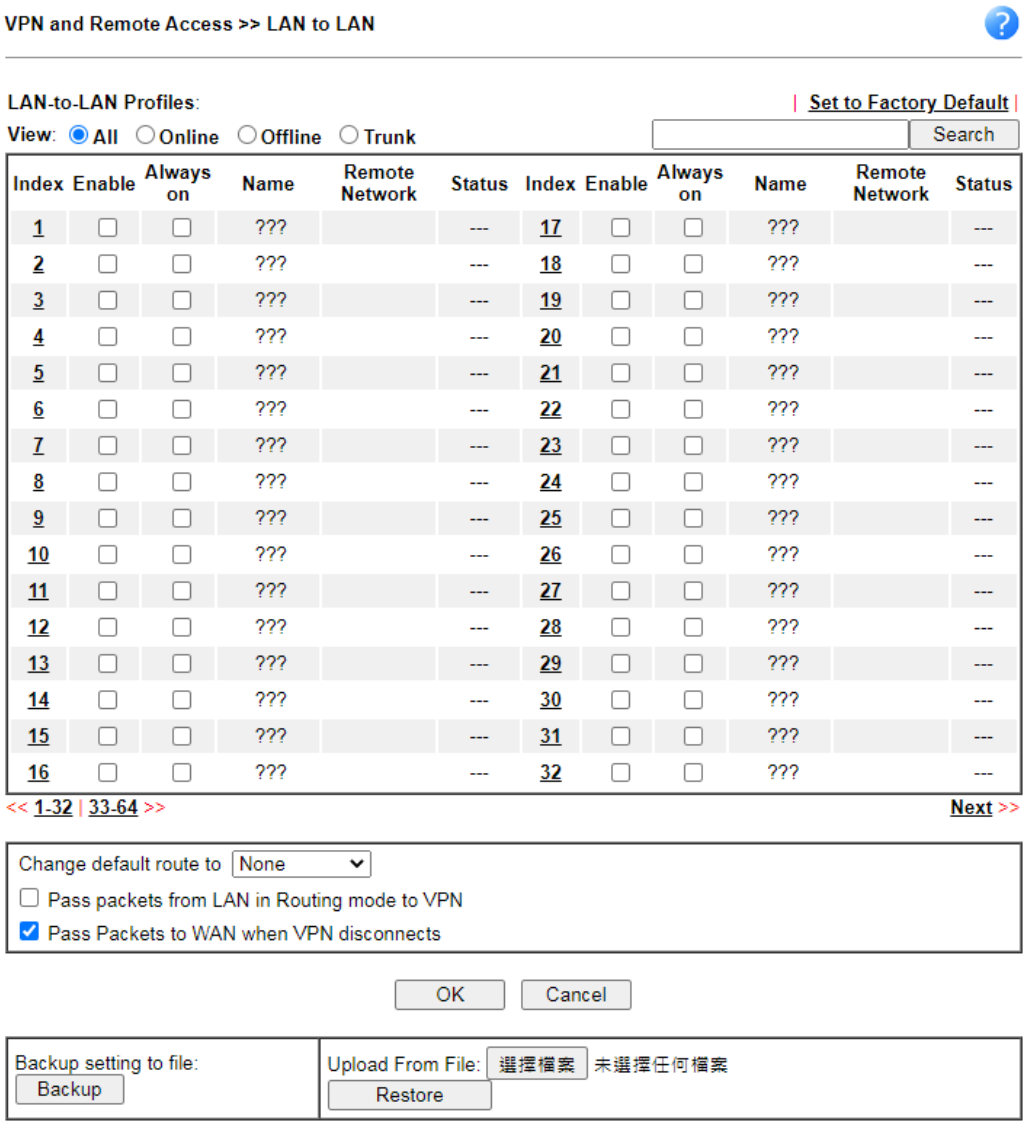
	y haga clic**Verificar**. Ahora, la configuración ha terminado. Se le pedirá que ingrese el código 2FA después de pasar la autenticación de nombre de usuario y contraseña. 
Autenticación IKE **Método**	**Clave precompartida**-Esta casilla de verificación está disponible cuando se especifica IP de cliente remoto o ID de homólogo. Marque la casilla de verificación y haga clic en Clave precompartida de IKE para ingresar un PSK de IKE (de 1 a 63 caracteres) que se usará solo para este perfil. **Firma Digital (X.509) –**Para habilitar la autenticación usando ID de pares X.509, marque la casilla de verificación y luego seleccione un perfil X.509. Los perfiles X.509 se pueden configurar en**VPN y acceso remoto >> Identidad de pares IPsec**.
Método de seguridad IPsec	Seleccione todos los protocolos IPsec que se pueden usar para este perfil. **Encabezado de autenticación media (AH)**significa que los datos se autenticarán, pero no se cifrarán. De forma predeterminada, se invoca esta opción. Puede desmarcarlo para deshabilitarlo. **Alta (ESP) -**Carga útil de seguridad de alta encapsulación (ESP) significa que la carga útil (datos) se cifrará y autenticará. Puede seleccionar el algoritmo de cifrado de Estándar de cifrado de datos (DES), Triple DES (3DES) y AES. **Identificación local (Opcional)-**Especifique una ID local que se usará al establecer una conexión VPN de LAN a LAN usando el modo agresivo IKE.
Programar perfil	Se pueden configurar hasta cuatro perfiles de programación.
Notificación	**Enviar correo electrónico cuando VPN esté activo**-Se enviará un correo electrónico al usuario definido en Objeto de correo electrónico cuando la VPN esté conectada y activa. - **Correo a**-Introduzca una dirección de correo electrónico. **Enviar SMS cuando la VPN esté activa**-Se enviará un SMS al usuario definido en Objeto SMS cuando la VPN esté conectada y activa. - **SMS a**-Ingresa un número de teléfono.

Para guardar los cambios en la página, seleccione**DE ACUERDO**; para descartar los cambios, seleccione**Cancelar**; para borrar la configuración de esta página y volver a la configuración predeterminada, seleccione**Claro**.

V-1-11 LAN a LAN

Esta sección le permite configurar hasta 64 conexiones VPN de LAN a LAN. Las conexiones de LAN a LAN se pueden configurar para permitir solo acceso telefónico de entrada, solo acceso telefónico de salida o tanto acceso telefónico de entrada como acceso telefónico de salida.

La siguiente figura muestra la tabla resumen según el ítem (Todo/Troncal) seleccionado para **Vista**.

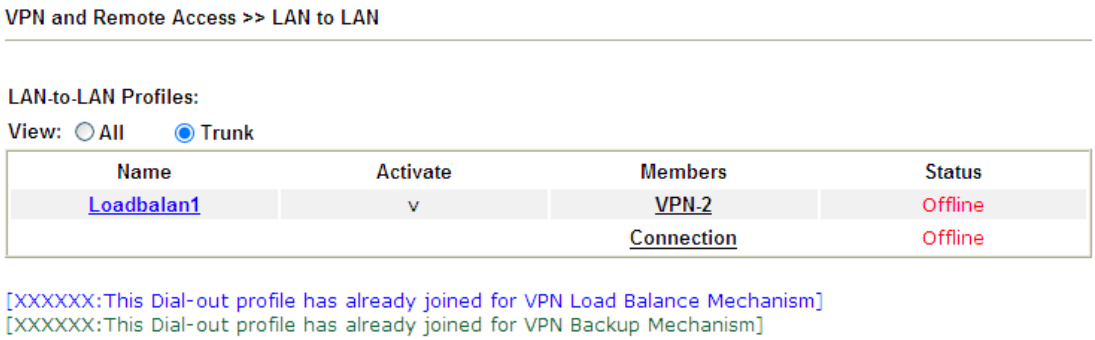


Los ajustes disponibles se explican a continuación:

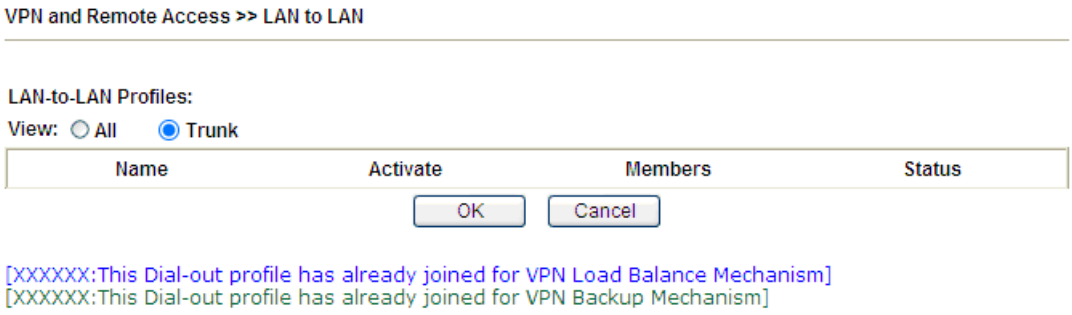
Artículo	Descripción
Establecer como predeterminado de fábrica	Haga clic para borrar todos los índices.
Vista	**Todo -**Muestra todos los perfiles VPN de LAN a LAN. **Trompa -**Muestra todos los perfiles troncales (consulte VPN y acceso remoto > > Gestión de TRONCO VPN).
Índice	Haga clic en el número de índice del perfil para ver o editar su configuración.
Permitir	Marque para habilitar el perfil VPN de LAN a LAN.
siempre encendido	Marque la casilla para habilitar la marcación de salida VPN de LAN a LAN

	perfil.
Nombre	Muestra el nombre del perfil de LAN a LAN. El símbolo**???** representa que el perfil está vacío.
Red remota	Muestra el nombre de la red remota.
Estado	Muestra el estado del perfil. En línea: la VPN de LAN a LAN está conectada. Fuera de línea: la VPN de LAN a LAN está desconectada. - - - – El perfil está deshabilitado.
Cambiar ruta predeterminada a	Cambie la ruta predeterminada al túnel VPN seleccionado.
Pasar paquetes de LAN en modo de enrutamiento a VPN	Si está habilitado, los paquetes del enrutamiento LAN pasarán a través del túnel VPN.
Pasar paquetes a WAN cuando VPN se desconecta	Si está habilitado, los paquetes pueden pasar a través de WAN cuando la VPN se desconecta.
Respaldo	Hacer clic**Respaldo**para guardar la configuración.
Restaurar	Hacer clic**Seleccionar**para elegir un archivo de configuración. Luego haga clic **Restaurar**para aplicar el archivo.

La siguiente figura muestra los perfiles unidos al balance de carga de VPN y al mecanismo de copia de seguridad de VPN.

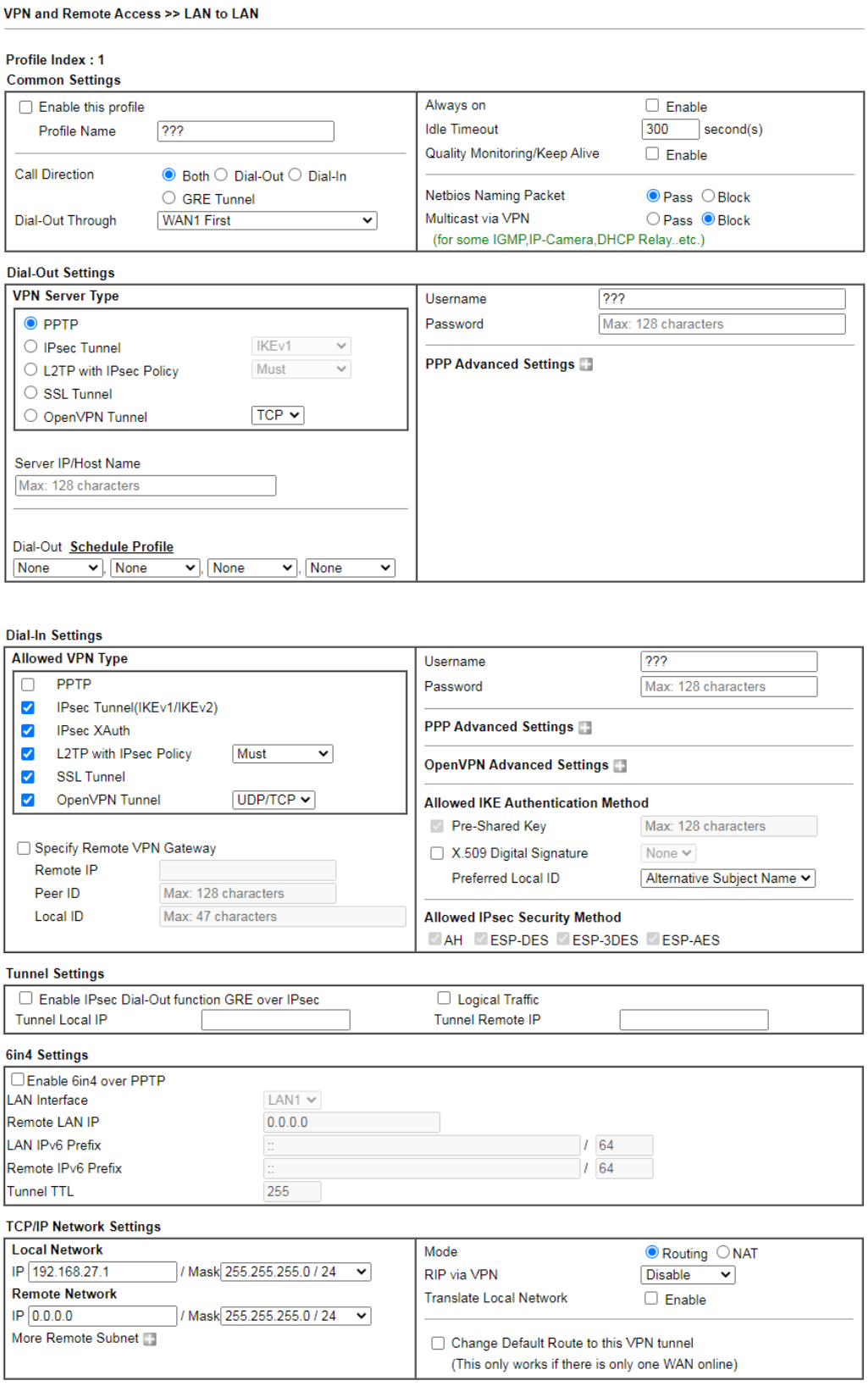


Si aún no hay un perfil unido, esta página se mostrará de la siguiente manera:



Para editar cada perfil, haga clic en cada índice para editar cada perfil.

1. La pantalla de configuración se muestra después de hacer clic en un índice de perfil. Hay 6 secciones: Configuración común, Configuración de marcación de salida, Configuración de marcación de entrada, Configuración de túnel, Configuración de 6 en 4 y Configuración de red TCP/IP.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Configuraciones comunes	
Habilitar este perfil	Seleccione para habilitar el perfil.

	Nombre de perfil -Especifique un nombre que le permita identificar este perfil. **Dirección de llamada -**Especifique la dirección de llamada permitida de este perfil de LAN a LAN. Hay cuatro opciones disponibles para el modo de conexión: - **Ambos**–El perfil se utilizará para iniciar (marcar) o aceptar (marcar) conexiones. - **Marcar hacia afuera**–El perfil se utilizará para iniciar conexiones salientes. - **Marcar**–El perfil se utilizará para aceptar conexiones entrantes. - **Túnel GRE**–La conexión se realiza mediante un túnel GRE. **Llamada de salida a través -**Seleccione la conexión WAN para las conexiones realizadas con este perfil. Esta configuración es útil solo para marcación de salida. - **WANx primero**-Mientras se conecta, el enrutador utilizará WANx o LTE como el primer canal para la conexión VPN. Si WANx o LTE fallan, el enrutador usará otra interfaz WAN en su lugar. - **Solo WANx o solo LTE**-Mientras se conecta, el enrutador utilizará WANx o LTE como el único canal para la conexión VPN. - **Solo WAN1: solo establece VPN si WAN2 está inactivo**-Si WAN2 falla, el enrutador utilizará WAN1 para la conexión VPN. - **Solo WAN2: solo establece VPN si WAN1 está inactivo**-Si WAN1 falla, el enrutador utilizará WAN2 para la conexión VPN. **siempre encendido**-Seleccione esta opción para mantener una conexión de acceso telefónico siempre activa. **Tiempo de inactividad**-El enrutador cerrará la conexión si no se observa actividad en la conexión VPN durante tantos segundos. El valor predeterminado es 300 segundos. **Monitoreo de calidad/Mantener vivo**-Seleccione esta opción para mantener la conexión VPN para la función de monitoreo de calidad SD-WAN. **Paquete de nombres de Netbios**-Especifica si permitir que los paquetes de nombres de NetBIOS atraviesen el túnel VPN**.** - **Aprobar**–haga clic en él para consultar la transmisión de datos entre los hosts ubicados a ambos lados del Túnel VPN mientras se conecta. - **Bloquear**–Cuando se produce un conflicto entre los hosts en ambos lados del túnel VPN al conectarse, dicha función puede bloquear la transmisión de datos del paquete de nombres de Netbios dentro del túnel. **Multidifusión a través de VPN -**Especifica si permitir que los paquetes de multidifusión atraviesen el túnel VPN. - **Aprobar**–Haga clic en este botón para permitir que los paquetes de multidifusión pasen a través del enrutador. - **Bloquear**–Esta es la configuración predeterminada. Haga clic en este botón para permitir que el enrutador bloquee los paquetes de multidifusión.

Configuración de marcación de salida

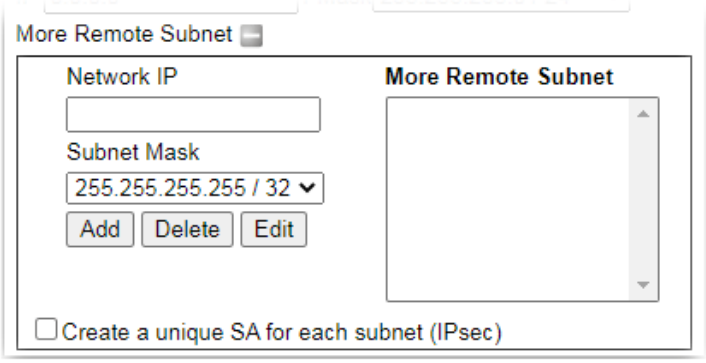
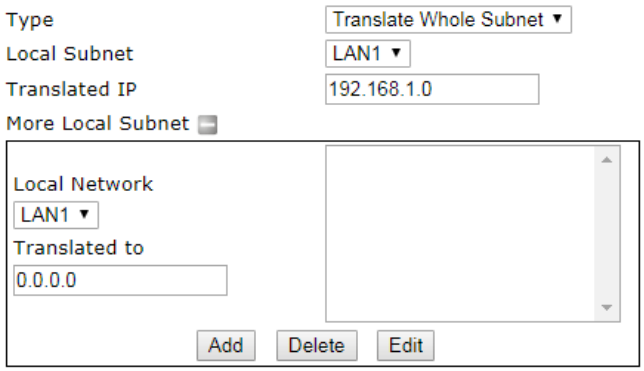
Tipo de servidor VPN	Seleccione el protocolo VPN que se utilizará**.**
Servidor IP/Nombre de host	Dirección IP o nombre de host DNS del host VPN remoto.

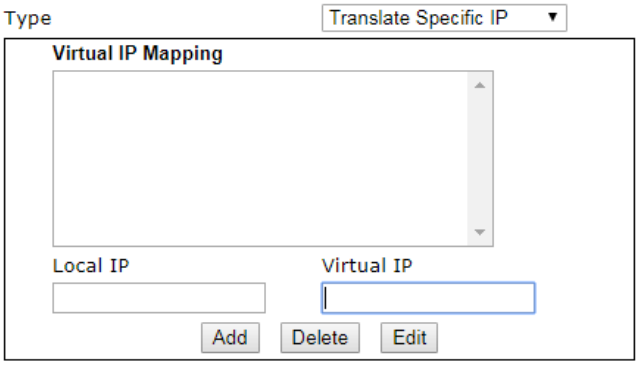
Calendario de marcación de salida **Perfil**	Conectar y desconectar según perfiles horarios. La configuración predeterminada de este campo está en blanco y la función siempre funcionará.
Nombre de usuario	Ingrese un nombre de usuario para establecer la conexión VPN.
Contraseña	Introduzca la contraseña para establecer la conexión VPN.
Si PPTP / **L2TP con IPsec** **Política /** **Túnel SSL /** **se selecciona como tipo de servidor VPN**	**Configuración avanzada de PPP**-Haga clic en él para expandir la configuración avanzada de PPP. - **Autenticación PPP -** Solo PAP: autentica a los usuarios de acceso telefónico utilizando solo el protocolo PAP. PAP/CHAP/MS-CHAP/MS-CHAPv2: intente autenticar a los usuarios de acceso telefónico utilizando varios protocolos CHAP y, si el cliente VPN remoto no se autentica, recurra a PAP. - **compresion vj -**Especifica si habilitar la compresión de encabezado Van Jacobson (VJ), que mejora el rendimiento en conexiones lentas. - **Solicitar dirección IP**-Introduzca la dirección IP.
Si se selecciona IPsec/ L2TP con política IPsec como VPN **Tipo de servidor**	**Configuración de la fase 1 de IKE -**Seleccionar de**Principal**modo y **Agresivo**modo. El resultado final es intercambiar propuestas de seguridad para crear un canal seguro protegido. **Principal**el modo es más seguro que**Agresivo**ya que se realizan más intercambios en un canal seguro para configurar la sesión IPsec. sin embargo, el**Agresivo**El modo es más rápido. El valor predeterminado en el enrutador Vigor es el modo principal. - **Autenticación - Firma digital (X.509)** - **ID de compañero -**Seleccione uno de los perfiles predefinidos establecidos en**VPN y acceso remoto >> Identidad de pares IPsec.** - **ID local -**Usar**Nombre de sujeto alternativo**o **Nombre del tema**de certificado local como identificación local. - **Certificado Local -**Seleccione uno de los perfiles establecidos en **Gestión de certificados>>Certificado local**. - **Autenticación: clave precompartida** - **Clave precompartida -**Ingrese de 1 a 128 caracteres como clave precompartida. - **ID local -**Ingrese la identidad IKE local para enviar en el intercambio para establecer la conexión IPsec. - **Cifrado de propuesta -**Utilice Auto/AES/3DES/DES para el cifrado de paquetes. - **propuesta Grupo ECDH -**Especifique un grupo si Automático no está seleccionado como Cifrado de propuesta. - **propuesta Autenticación -**Seleccione SHA256 o SHA1 para la autenticación de paquetes. - **Forzar encapsulación UDP -**Seleccione para hacer la encapsulación UDP a la fuerza. Todos los paquetes IPsec se encapsularán con el encabezado UDP. **Configuración de la fase 2 de IKE -**Especifique el protocolo de seguridad, el cifrado de propuestas y la autenticación de propuestas. - **Protocolo de seguridad**-AH (Medio) significa que los datos se autenticarán, pero no se cifrarán. Por defecto, esta opción está activa. ESP (Alto) significa que la carga útil (datos) se cifrará y autenticará. - **Cifrado de propuestas**-Utilice el algoritmo de cifrado AES/3DES y aplique la autenticación MD5 o SHA-1

	algoritmo. - **Autenticación de propuestas**-Seleccione Todos, SHA o Ninguno. **Configuración avanzada de IKE -**Especifique la vida útil de la clave de cada fase IKE, ID de red, etc. - **Vida útil de la clave de la fase 1 de IKE-**Por razones de seguridad, se debe definir la vida útil de la clave. El valor predeterminado es 28800 segundos. Puede especificar un valor entre 900 y 86400 segundos. - **Vida útil de la clave IKE fase 2-**Por razones de seguridad, se debe definir la vida útil de la clave. El valor predeterminado es 3600 segundos. Puede especificar un valor entre 600 y 86400 segundos. - **ID de red de fase 2 -**Esto es opcional. Cambie la dirección IP de origen del tráfico VPN a la dirección IP especificada para el modo NAT seleccionado en el campo Configuración de red TCP/IP. - **Habilitar Perfect Forward Secret (PFS) -**La clave IKE Fase 1 se reutilizará para evitar la complejidad de cálculo en la fase 2. El valor predeterminado es inactiva esta función. **Hacer ping para mantenerse vivo -**Seleccione para habilitar la función de PING para mantener vivo. **PING IP de destino -**Ingrese la dirección IP para mantener vivo.
Si el túnel OpenVPN con la política IPsec se selecciona como VPN **Tipo de servidor**	**Configuración avanzada de OpenVPN - C**Haga clic para establecer la configuración avanzada de OpenVPN. - **Algoritmo de cifrado -**Seleccione un algoritmo para cifrar los paquetes a través de OpenVPN. - **Algoritmo HMAC -**Seleccione un algoritmo para autenticar los paquetes a través de OpenVPN. - **Certificado de cliente -**Seleccione un certificado de cliente o autofirme un nuevo certificado o un certificado DrayDDNS. - **Confiar en CA -**Seleccione un certificado de CA de confianza. - **Comprimir -**Seleccione un método para comprimir los paquetes para reducir el uso de ancho de banda mientras transfiere los paquetes comprimidos. - **TLS - autorización -**Seleccionar**En**para utilizar el método de autenticación TLS. La información clave relacionada se puede comprobar haciendo clic en**Vista**. **Importar archivo de configuración de OpenVPN -**Se puede importar un archivo de configuración OpenVPN de otro enrutador Vigor y aplicarlo a este enrutador. - **Seleccione Archivo -**Seleccione un archivo de su disco duro. - **Importar -**Haga clic para cargar el archivo de configuración seleccionado en este enrutador Vigor.
Configuración de acceso telefónico	
Tipo de VPN permitido	Seleccione los protocolos VPN permitidos para las conexiones de acceso telefónico. - **PPTP -**Permita que el usuario de acceso telefónico remoto realice una conexión VPN PPTP a través de Internet. Debe configurar el Nombre de usuario y la Contraseña del usuario de marcación remota a continuación. - **Túnel IPsec (IKEv1/IKEv2)-**Permita que el usuario de acceso telefónico remoto active una conexión VPN IPsec a través de Internet. - **IPsec XAuth** - **L2TP con política IPsec -**Permita que el usuario de acceso telefónico remoto realice una conexión VPN L2TP a través de Internet.

	Puede seleccionar usar L2TP solo o con IPsec. Seleccione de abajo: - **Ninguno -**No aplique la política IPsec. En consecuencia, la conexión VPN que empleó la política L2TP sin IPsec puede verse como una conexión L2TP pura. - **Agradable tener**-Primero aplique la política IPsec, si es aplicable durante la negociación. De lo contrario, la conexión VPN de acceso telefónico se convierte en una conexión L2TP pura. - **Debe -**Especifique la política IPsec que se aplicará definitivamente en la conexión L2TP. - **Túnel SSL-**Permita que el usuario de marcación remota active una conexión SSL VPN a través de Internet. - **Túnel OpenVPN**
Especificar VPN remota **Puerta**	Puede especificar la dirección IP del usuario de marcación remota o la ID del compañero (debe ser la misma que la configuración de ID en el tipo de marcación) marcando la casilla. Además, debe especificar más los métodos de seguridad correspondientes en el lado derecho. Si desmarcas la casilla**,**el tipo de conexión que seleccione arriba aplicará los métodos de autenticación y métodos de seguridad en la configuración general. **Nombre de usuario -**Este campo se aplica cuando selecciona PPTP o L2TP con o sin la política IPsec anterior. La longitud del nombre está limitada a 11 caracteres. **Contraseña -**Este campo se aplica cuando selecciona PPTP o L2TP con o sin la política IPsec anterior. La longitud de la contraseña está limitada a 11 caracteres.
PPP Avanzado Ajustes	Haga clic en él para expandir la configuración avanzada de PPP. **Compresión VJ -**Especifica si habilitar la compresión de encabezado Van Jacobson, que mejora el rendimiento en conexiones lentas. **Asignar dirección IP de pares**-Ingrese la dirección IP del par.
OpenVPN Avanzado Ajustes	**Algoritmo de cifrado -**Seleccione un algoritmo para cifrar los paquetes a través de OpenVPN. **Algoritmo HMAC -**Seleccione un algoritmo para autenticar los paquetes a través de OpenVPN.
IKE permitido **Autenticación** **Método**	Esta sección está disponible cuando se selecciona el túnel IPsec como protocolo de marcado. Las opciones disponibles son la clave precompartida IKE y la firma digital X.509. **Clave precompartida**-Para usar una clave precompartida, seleccione este botón de opción y luego haga clic en el botón Clave precompartida de IKE para ingresar al PSK. **Firma digital X.509**-Para usar una firma digital X.509, seleccione este botón de opción y luego seleccione un perfil de identidad de pares IPsec X.509. Para habilitar la autenticación usando ID de pares X.509. Los perfiles X.509 se pueden configurar en**VPN y acceso remoto >> Identidad de pares IPsec**. - **ID local**–Seleccione si desea hacer coincidir primero el nombre alternativo del sujeto o el nombre del sujeto durante la autenticación. **- Nombre de sujeto alternativo**–El nombre de sujeto alternativo (configurado en**Gestión de certificados>>Certificado local**) será inspeccionado primero.

	- Nombre del tema–El nombre del sujeto (configurado en **Gestión de certificados>>Certificado local**) será inspeccionado primero.
IPsec permitido **Método de seguridad**	Esta configuración está disponible cuando se selecciona Túnel IPsec como protocolo de marcación de salida. - **AH-**El encabezado de autenticación (AH) significa que los datos se autenticarán, pero no se cifrarán. Seleccione para usar el protocolo de encabezado de autenticación. Por defecto, esta opción está activa. - **ESP-DES/ESP-3DES/ESP-AES -**La carga útil de seguridad encapsulada (ESP) significa que la carga útil (datos) se cifrará y autenticará. Puede seleccionar el algoritmo de cifrado de Estándar de cifrado de datos (DES), Triple DES (3DES) y AES.
Configuración del túnel	
Habilitar marcación IPsec función GRE sobre IPsec	Marque esta casilla para verificar los datos y transmitirlos encriptados con GRE sobre el paquete IPsec después de configurar la configuración de Llamada IPsec. Ambos extremos deben coincidir configurando la misma dirección IP virtual para la comunicación.
Tráfico Lógico	Tal técnica proviene de RFC2890. Defina el tráfico lógico para la transmisión de datos entre ambos lados del túnel VPN utilizando la característica de GRE. Incluso el pirata informático puede descifrar el cifrado IPsec, pero aún no puede pedirle al sitio LAN que realice la transmisión de datos con ninguna información. Dicha función puede garantizar que los datos transmitidos en el túnel VPN se envíen realmente desde ambos lados. Esta es una función opcional. Sin embargo, si un lado quiere usarlo, el compañero también debe habilitarlo.
IP local del túnel	Ingrese la IP virtual del enrutador para que sea verificada por pares.
IP remota del túnel	Ingrese la IP virtual del host del mismo nivel para que la verifique el enrutador.
Ajustes 6 en 4	
Habilitar 6 en 4 sobre PPTP	Transmita los paquetes IPv6 desde el sitio local al sitio remoto a través del túnel VPN IPv4 con la tecnología de encapsulación 6in4. Marque para habilitar la función. Los paquetes IPv6 pueden pasar a través del túnel WAN PPTP VPN al sitio remoto.
Interfaz LAN	Especifique una interfaz LAN para transmitir los paquetes.
IP de LAN remota	Especifique la dirección IP del sitio remoto.
Prefijo IPv6 de LAN	Especifique el prefijo (con longitud) del sitio local.
Prefijo IPv6 remoto	Especifique el prefijo (con la longitud) del sitio remoto.
Túnel TTL	Introduzca un valor.
Configuración de red TCP/IP	
Red local	El valor predeterminado es 0.0.0.0, lo que significa que el enrutador Vigor obtendrá una dirección IP PPP del enrutador remoto durante la fase de negociación de IPCP. Si la dirección IP de PPP está fijada por el lado remoto, especifique aquí la dirección IP fija. No cambies

	el valor predeterminado si no selecciona PPTP o L2TP. **IP / Máscara -**Muestra la IP de la red local y la máscara para la configuración de TCP/IP. Puede modificar la configuración si es necesario.
Red remota	El valor predeterminado es 0.0.0.0, lo que significa que el enrutador Vigor obtendrá una dirección IP PPP de puerta de enlace remota del enrutador remoto durante la fase de negociación de IPCP. Si la dirección IP de PPP está fijada por el lado remoto, especifique aquí la dirección IP fija. No cambie el valor predeterminado si no selecciona PPTP o L2TP. **IP/ Máscara -**Agregue una ruta estática para dirigir todo el tráfico destinado a esta dirección IP de red remota/máscara de red remota a través de la conexión VPN. Para IPsec, estos son los ID de clientes de destino del modo rápido de fase 2.
Más subred remota	Haga clic para abrir un cuadro de diálogo para ingresar rutas estáticas adicionales para las subredes destinadas a la red remota. 
Modo	Si la red remota solo permite una dirección IP para la red local, seleccione**NAT**; de lo contrario, seleccione**Ruta**.
Cuando el Modo está configurado en Enrutamiento	Cuando**Enrutamiento**está seleccionado, los campos disponibles en la sección Configuración de red TCP/IP se mostrarán como: **Traducir red local**-Marque la casilla para habilitar la función. Agregue una ruta estática para dirigir todo el tráfico destinado a más direcciones IP de red remota/máscara de red remota a través de la conexión VPN. Esto generalmente se usa cuando encuentra que hay varias subredes detrás del enrutador VPN remoto. - **Tipo**-Hay dos tipos (**Traducir toda la subred**, **Traducir IP específica**) para que usted elija. Cuando**Traducir toda la subred**se selecciona como**Tipo**, las configuraciones disponibles se enumeran a continuación:  - **Subred local**-Seleccione la LAN cuyas direcciones IP se van a traducir. - **IP traducida**-Especifique una dirección IP. - **Más subred local**-Haga clic en él para agregar más subredes.

	Cuando**Traducir IP específica**se selecciona como**Tipo**, las configuraciones disponibles se enumeran a continuación:  - **Asignación de IP virtuales:**Aparecerá un cuadro de diálogo emergente para que especifique la dirección IP local y la dirección IP virtual de asignación.
Cuando el modo está configurado en NAT	Cuando**NAT**está seleccionado, los campos disponibles en la sección Configuración de red TCP/IP se mostrarán como: **RIP a través de VPN -**Especifica la dirección de los paquetes del Protocolo de información de enrutamiento (RIP). Las opciones disponibles son: - TX/RX Ambos: puede transmitir o recibir paquetes RIP Solo TX: - solo puede transmitir pero no recibir paquetes RIP Solo RX: - solo puede recibir pero no transmitir paquetes RIP - Deshabilitar: RIP está deshabilitado. **Cambiar la ruta predeterminada a este túnel VPN -**Seleccione esta opción para dirigir todo el tráfico que no esté vinculado a la LAN a este túnel VPN. Esta opción es funcional cuando solo hay una WAN activa.

2. Para guardar los cambios en la página de perfil de LAN a LAN, seleccione**DE ACUERDO**; para restablecer toda la página en blanco, seleccione**Claro**; para descartar los cambios, seleccione**Cancelar**.

V-1-12 Gestión de troncales VPN

Un troncal VPN combina DOS túneles VPN de LAN a LAN para proporcionar funcionalidades de respaldo de VPN o equilibrio de carga de VPN.

Respaldo VPN

VPN Backup proporciona conectividad VPN redundante e ininterrumpida al monitorear constantemente el estado de un túnel VPN y conmuta por error al túnel VPN secundario cuando falla el túnel principal.

En un tronco VPN de respaldo, solo uno de los dos túneles VPN de LAN a LAN está conectado en un momento dado. Cuando falla un túnel, el enrutador se iniciará automáticamente y dirigirá todo el tráfico VPN destinado al enlace troncal al otro túnel.

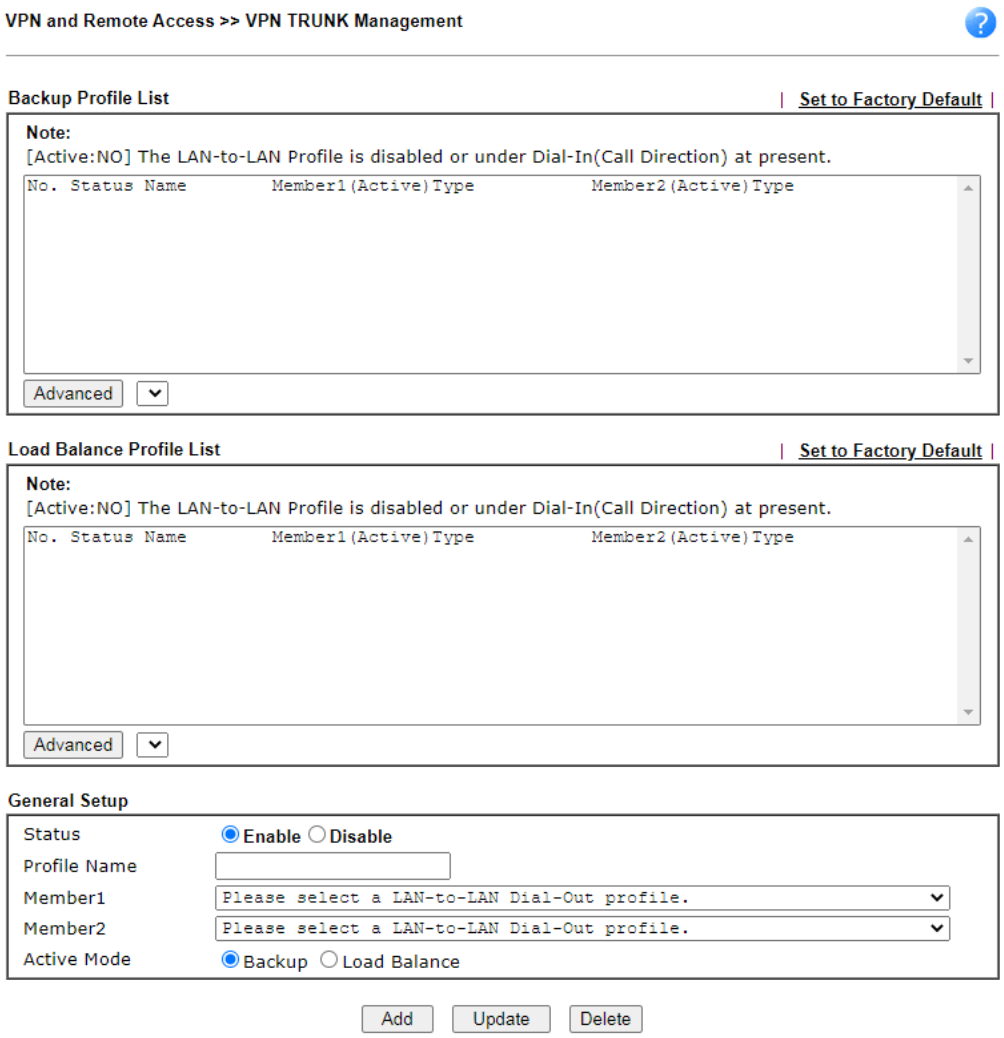
Equilibrio de carga de VPN

VPN Load Balance aumenta el ancho de banda de una conexión de LAN a LAN al combinar y equilibrar la carga de dos túneles, con la opción de dirigir el tráfico a túneles específicos por dirección de origen, dirección de destino o puerto.

En un enlace troncal VPN de equilibrio de carga, ambos túneles VPN de LAN a LAN están conectados simultáneamente. El enrutador primero intenta hacer coincidir el tráfico con una regla de política de equilibrio de carga y enviarlo por el túnel especificado en la regla coincidente. El tráfico que no coincida con ninguna política se equilibrará en la carga por turnos, y la relación de tráfico entre los dos túneles la determina automáticamente el enrutador o la especifica el usuario.

Para configurar un Troncal VPN, primero se deben haber configurado 2 perfiles VPN de LAN a LAN. Para detalles sobre la configuración de túneles VPN de LAN a LAN, consulte la sección V-1-10 LAN a LAN. Cuando los 2 perfiles VPN de LAN a LAN estén listos, siga los pasos a continuación para configurar un enlace troncal VPN.

Para crear un nuevo Troncal VPN, primero configure la sección Configuración general.



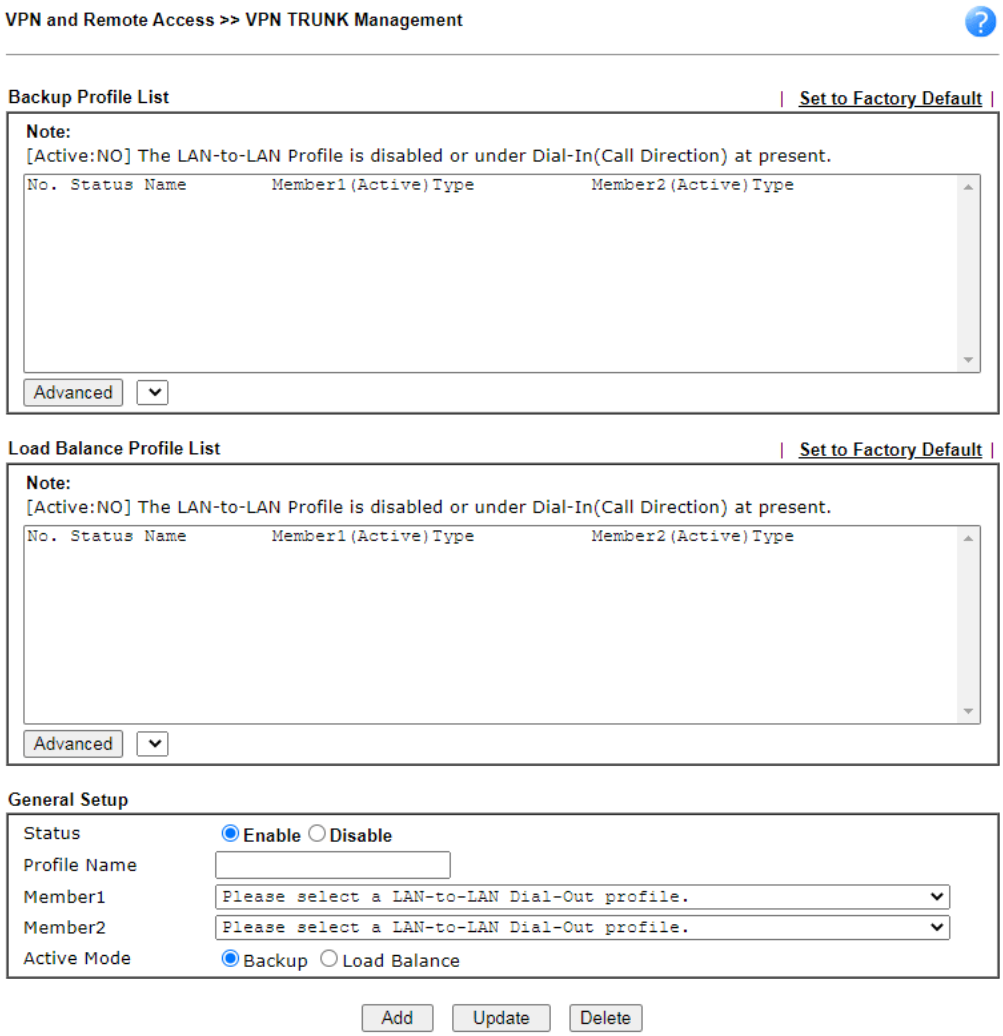
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Configuración general	**Estado**-Habilite o deshabilite el Troncal VPN. - **Permitir**–Seleccione esto para habilitar este troncal VPN. - **Desactivar**-Seleccione esto para deshabilitar este troncal VPN. **Nombre de perfil**-Ingrese un nombre para identificar este perfil de Troncal VPN. **Miembro 1/Miembro 2**-Seleccione los perfiles VPN de LAN a LAN para que sean el primer y segundo miembro de este tronco VPN. **Modo activo**-Seleccione el modo de operación del Troncal VPN. **Copia de seguridad / Balance de carga**–Seleccione esto para configurar un enlace troncal VPN de respaldo/equilibrio de carga. **Agregar**-Selecciónelo para agregar un perfil de troncal VPN usando la información ingresada. **Actualizar -**Selecciónelo para guardar los cambios en el**Estado**(Habilitar o deshabilitar), nombre de perfil, miembro1 o miembro2. **Borrar -**Selecciónelo para eliminar el perfil VPN TRUNK seleccionado. Los miembros correspondientes (perfiles de LAN a LAN) agrupados

	en el perfil VPN TRUNK eliminado se liberará y los perfiles en LAN-to-LAN se mostrarán en negro.

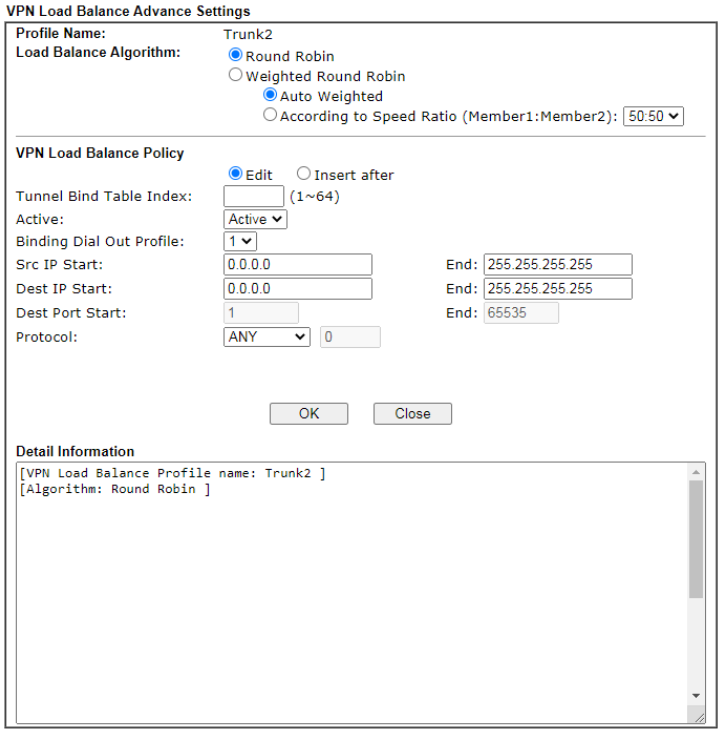
Configuración, modificación o eliminación de un troncal VPN

Para configurar o modificar un Troncal VPN, vaya a la sección Lista de Perfiles que corresponda al tipo de Troncal VPN (Copia de Seguridad o Equilibrio de Carga).



Los ajustes disponibles se explican a continuación:

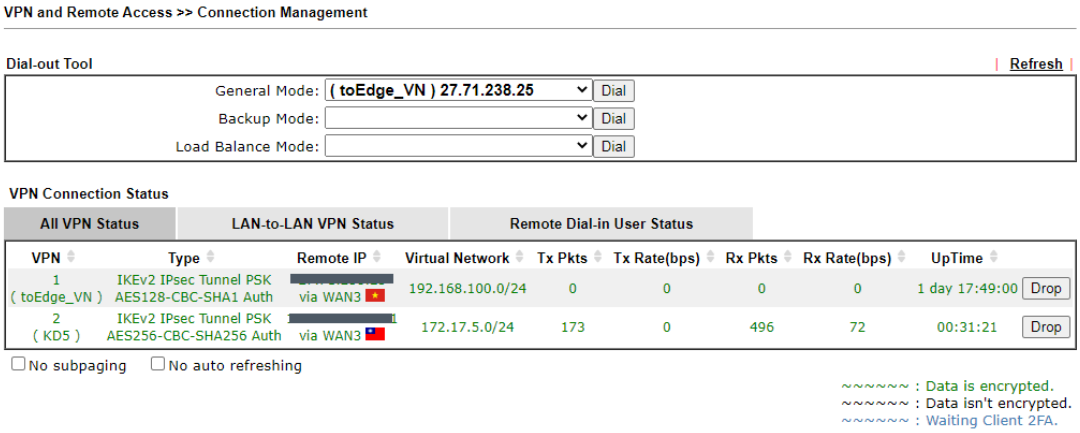
Artículo	Descripción
Lista de perfiles de copia de seguridad **y** **Lista de perfiles de equilibrio de carga**	**Establecido a los valores predeterminados de fábrica -**Elimina todos los perfiles de Troncal VPN en la Lista de perfiles. **No. -**El número de índice del perfil VPN. **Estado**-Muestra si el Troncal VPN está habilitado o deshabilitado. - v – VPN Trunk está habilitado. x: - VPN Trunk está deshabilitado. **Nombre -**El nombre ingresado por el usuario que identifica el perfil de troncal. **Tipo de miembro 1 (activo) / Tipo de miembro 2 (activo) -**Muestra el índice del perfil, si está habilitado o deshabilitado, y el protocolo VPN de los 2 perfiles VPN de LAN a LAN. Ejemplo: 1(YES)PPTP: el miembro troncal está configurado para usar el

	primer perfil que actualmente está habilitado y utiliza el protocolo PPTP. **Avanzado**-Para configurar los ajustes avanzados de un perfil de Troncal VPN, seleccione su nombre de la lista desplegable y haga clic en Avanzado.
Avanzado para copia de seguridad **Lista de perfiles**	Si se seleccionó un perfil de copia de seguridad, aparecerá la siguiente pantalla Configuración avanzada: **Nombre de perfil**-Nombre definido por el usuario que identifica este perfil. **Modo ERD**-Establece el modo de detección de recuperación del entorno (ERD). - **Normal**–Ambos túneles VPN tienen una prioridad equivalente. - **Reanudar**–Los túneles VPN de miembro 1 y miembro 2 son conexiones primarias y secundarias, respectivamente. El enrutador siempre intentará usar el miembro 1 primero y solo conmutará por error al miembro 2 si el miembro 1 está inactivo. **Información detallada**-Proporciona una explicación detallada del modo ERD. Para guardar la configuración avanzada del perfil, seleccione**DE ACUERDO**; para cerrar sin guardar los cambios, seleccione**Cerca**.
Avanzado para carga **Lista de perfiles de saldo**	Si se seleccionó un perfil de equilibrio de carga, aparece la siguiente pantalla Configuración avanzada:  **Nombre de perfil**e - Nombre definido por el usuario que identifica este perfil. **Algoritmo de equilibrio de carga**-Configura cómo se realiza el equilibrio de carga.

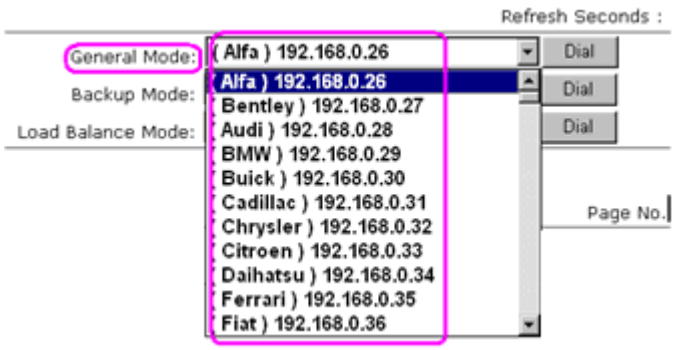
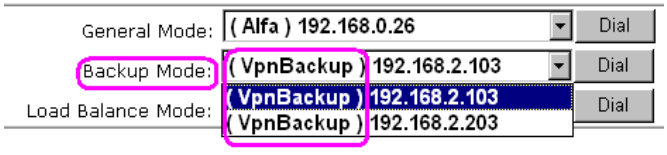
	- **ronda robin**–Todas las conexiones salientes que no coinciden con ninguna política de equilibrio de carga se distribuyen uniformemente entre los túneles. - **Round Robin Ponderado**--Todas las conexiones salientes que no coinciden con ninguna política de equilibrio de carga se distribuyen entre los túneles en función de una proporción determinada automáticamente por el enrutador (Ponderación automática) o especificada por el usuario (Según la proporción de velocidad). **Política de equilibrio de carga de VPN**-Esta sección permite la modificación o adición de perfiles de política de equilibrio de carga. **Editar / Insertar después**-Seleccione Editar para modificar el perfil de equilibrio de carga existente con el índice especificado en el índice de la tabla de enlace de túnel o Insertar después para insertar un nuevo perfil de equilibrio de carga inmediatamente después de la posición de índice especificada en el índice de la tabla de enlace de túnel. **Índice de tabla de vinculación de túnel**- Este dispositivo proporciona 64 tablas de túnel de enlace. En el modo de edición, se actualizará el perfil que coincida con este índice. En el modo Insertar después, se insertará un nuevo perfil inmediatamente después de la política que tenga este índice. **Activo**–Incluye Activo y Claro. En el cual, - **Activo**-Toda la información se guardará en un perfil de equilibrio de carga. - **Claro**–Se eliminará el perfil con índice de índice de tabla de vinculación de túnel coincidente. **Perfil de marcación vinculante**–El túnel VPN de LAN a LAN al que se enviará el tráfico que coincida con esta política. **Scr IP inicio/fin**– Especifique las direcciones IP de origen como punto de inicio y punto final. **Destino IP Inicio/Fin**–Especifique las direcciones IP de destino como punto de partida y punto final. **Puerto de destino inicio/fin**– Especifique el intervalo de puertos de destino si el protocolo es TCP o UDP. **Protocolo**–Especifique el protocolo del tráfico. **Información detallada**-Muestra toda la información sobre el perfil de Load Balance. Para guardar la configuración avanzada del perfil, seleccione**DE ACUERDO**; para cerrar sin guardar los cambios, seleccione**Cerca**.
Agregar	Selecciónelo para agregar un perfil de troncal VPN usando la información ingresada.
Actualizar	Realice las modificaciones necesarias en la sección Configuración general. Selecciónelo para guardar los cambios en el Estado (Habilitar o Deshabilitar), nombre de perfil, miembro1 o miembro2.
Borrar	Selecciónelo para eliminar el perfil VPN TRUNK. Los miembros correspondientes (perfiles de LAN a LAN) agrupados en el perfil TRUNK VPN eliminado se liberarán y los perfiles de LAN a LAN se mostrarán en negro.

V-1-13 Gestión de conexiones

Puede iniciar sesiones de VPN de LAN a LAN salientes y ver y desconectar todas las sesiones de VPN de acceso telefónico y de LAN a LAN actuales.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Actualizar	Haga clic para volver a cargar manualmente la página para actualizar la información de conexión VPN.
Herramienta de marcado	La sección Herramienta de marcación de salida se puede utilizar para iniciar sesiones VPN de LAN a LAN salientes. **Modo General -**Enumera todos los perfiles de VPN de LAN a LAN que no pertenecen a los perfiles de troncales de VPN habilitados. Para marcar manualmente un perfil VPN de LAN a LAN, selecciónelo en el cuadro combinado y haga clic en el**Marcar**botón a la derecha. La conexión VPN creada por el modo general no es compatible con la función de copia de seguridad de VPN.  **Modo de copia de seguridad -**Enumera todos los perfiles de Backup VPN Trunk. Para marcar manualmente un perfil de Troncal VPN de respaldo, selecciónelo en el cuadro combinado y haga clic en el botón**Marcar**botón a la derecha. La conexión VPN creada por el modo de copia de seguridad admite la función de copia de seguridad de VPN.  **Modo de equilibrio de carga -**Enumera todos los troncales VPN de equilibrio de carga

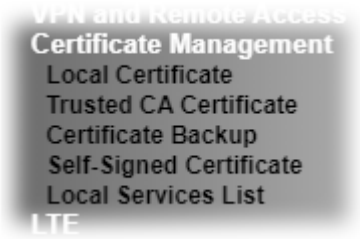
	perfiles. Para marcar manualmente un perfil de troncal VPN de equilibrio de carga, selecciónelo en el cuadro combinado y haga clic en el**Marcar**botón a la derecha. **Marcar -**Haga clic en este botón para ejecutar la función de marcar. Si la conexión se realiza con éxito, aparecerá en la sección Estado de la conexión VPN a continuación.
Estado de la conexión VPN	**vpn**-Muestra el número de perfil VPN y el nombre del perfil. **Tipo** -Muestra el protocolo VPN utilizado para la conexión **IP remota**-Muestra la dirección IP remota de la conexión VPN. **red virtual**-Muestra la subred IP utilizada por la conexión VPN. **paquetes de transmisión**-Muestra la cantidad de paquetes que se han transmitido a través de la conexión VPN. **Tasa de transmisión (bps)**-Muestra la velocidad ascendente actual de la conexión VPN. **paquetes recetados**-Muestra el número de paquetes que se han recibido a través de la conexión VPN. **Tasa de Rx (bps)**-Muestra la velocidad descendente actual de la conexión VPN. **tiempo de actividad**-Muestra el tiempo transcurrido de la conexión VPN. **Gota**-Haga clic en este botón para desconectar esta conexión VPN.

Gestión de certificados V-2

Un certificado digital es un documento electrónico emitido por una autoridad de certificación (CA) a una entidad para demostrar la propiedad de una clave pública. Contiene información de identificación, incluido el nombre de la parte a la que se emite, un número de serie, fechas de vencimiento, etc., y la firma digital de la autoridad emisora del certificado para que el destinatario pueda verificar que el certificado es real. El enrutador Vigor admite certificados digitales que cumplen con el estándar X.509.

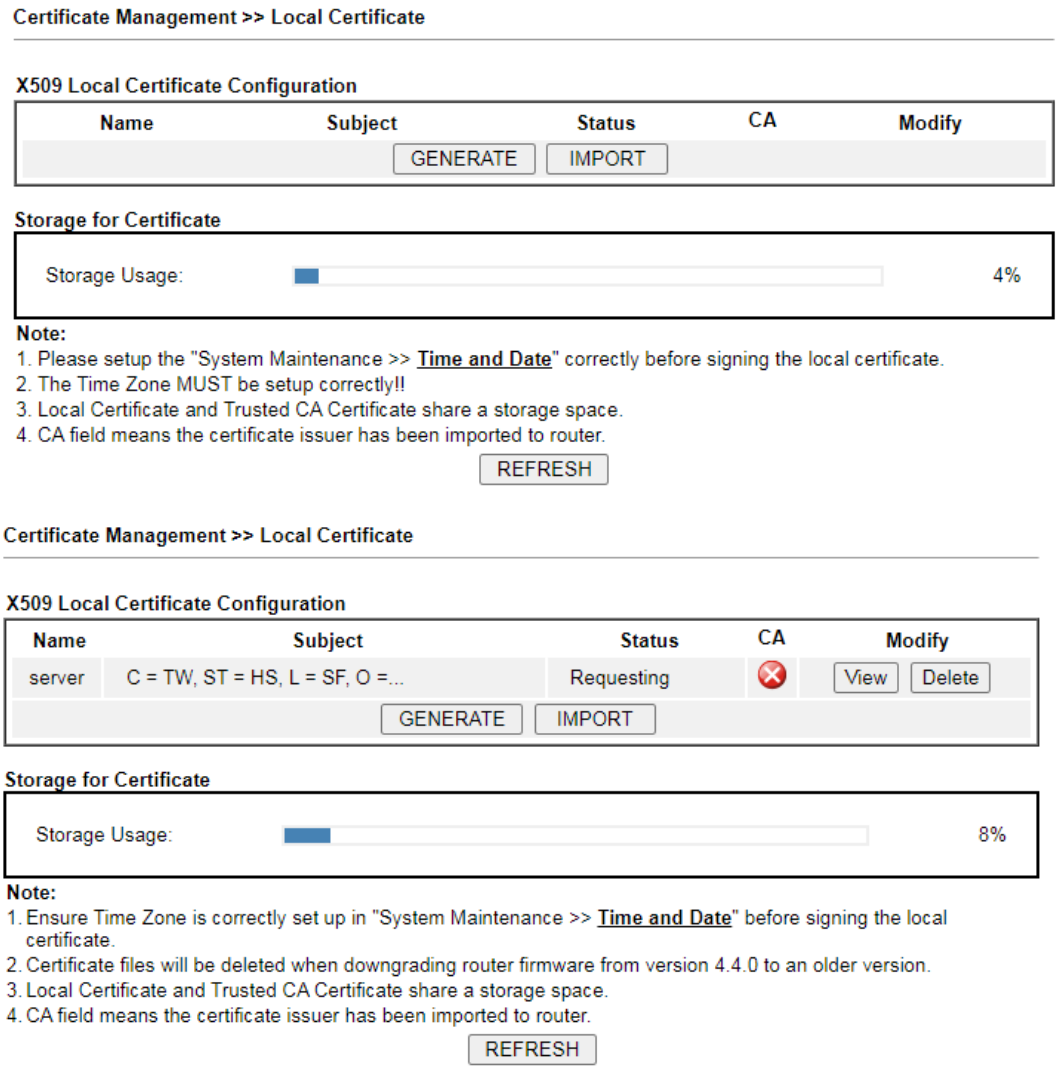
En esta sección, puede generar y administrar certificados digitales locales e importar certificados de CA de confianza. Asegúrese de que la hora del sistema sea correcta en el enrutador para que los certificados no se consideren erróneamente como no válidos debido a que una hora del sistema incorrecta cae fuera del período de validez del certificado. La forma más fácil de lograr esto es sincronizar periódicamente la hora del sistema con un servidor NTP (Network Time Protocol).

La siguiente imagen muestra los elementos del menú para la gestión de certificados.



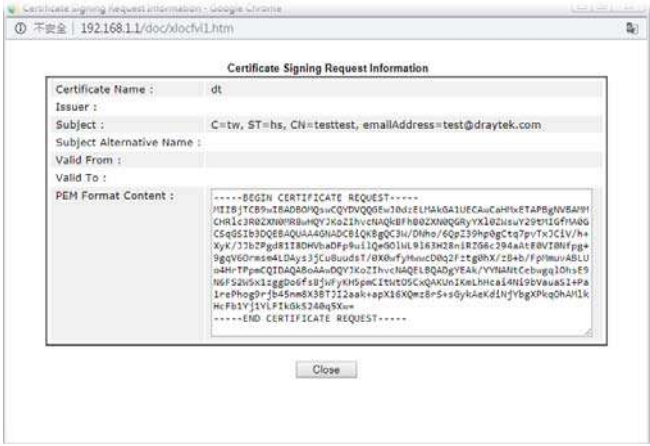
Certificado Local V-2-1

Puede generar, importar o ver certificados locales en esta página.



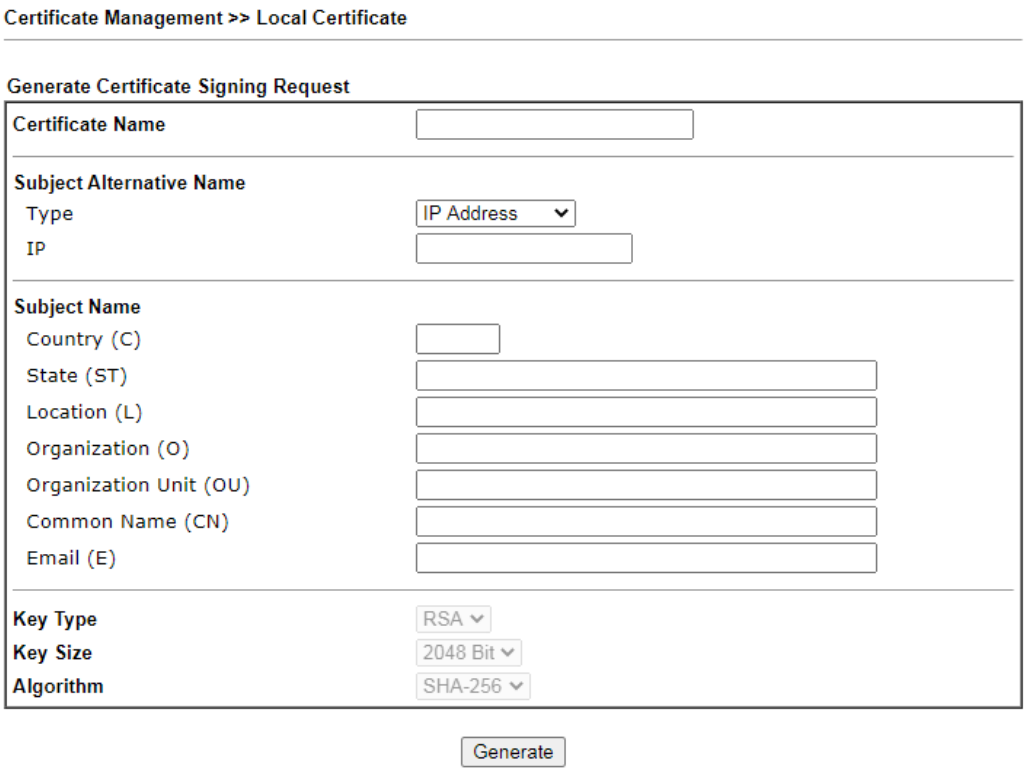
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre	Muestra el Nombre que identifica el certificado.
Sujeto	Muestra las entradas del nombre del sujeto del certificado.

Estado	Muestra el estado del certificado.
Modificar	**Vista**–Haga clic para ver los detalles del certificado. Aparecerá una pantalla similar a la siguiente, que muestra el nombre del sujeto, el nombre alternativo del sujeto y el contenido del certificado. **Borrar**-Haga clic para eliminar el nombre seleccionado.  **Borrar**–Haga clic para eliminar el certificado.
Generar	Haga clic para completar los detalles sobre un certificado e inicie el proceso de generación.
Almacenamiento para Certificado	Muestra el porcentaje del uso del almacenamiento.
Actualizar	Haga clic en este botón para actualizar la información de esta página.

GENERAR

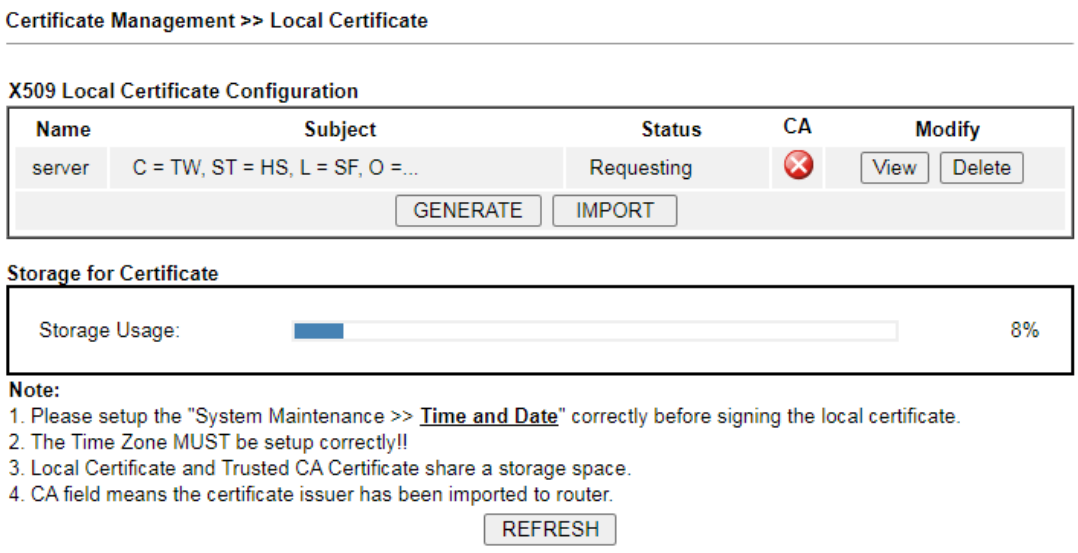
Utilice esta pantalla para enviar una solicitud a su CA raíz para generar un certificado.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre del certificado	Nombre que identifica al certificado.
Tipo	Seleccione el tipo (dirección IP, nombre de dominio, correo electrónico o ninguno) de nombre alternativo del sujeto e ingrese su valor.
País (C)	País en el que se encuentra su organización.
Estado (ST)	Estado o provincia donde se encuentra su organización.
Ubicación (L)	Ciudad donde se encuentra su organización.
Organización (O)	Nombre legal de su organización.
Unidad organizativa (OU)	Departamento dentro de su organización que desea asociar con este certificado.
Nombre común (CN)	Nombre de dominio totalmente calificado/IP WAN que se utilizará para llegar a su servidor.
Correo electrónico (E)	Dirección de correo electrónico de la entrada.
Tipo de clave	El tipo de clave está configurado de forma rígida en RSA.
Tamaño de clave	Elija entre 1024 y 2048 bits.
Algoritmo	Elija entre SHA-1 y SHA-256.
Generar	Haga clic para enviar una solicitud de generación al servidor de CA.

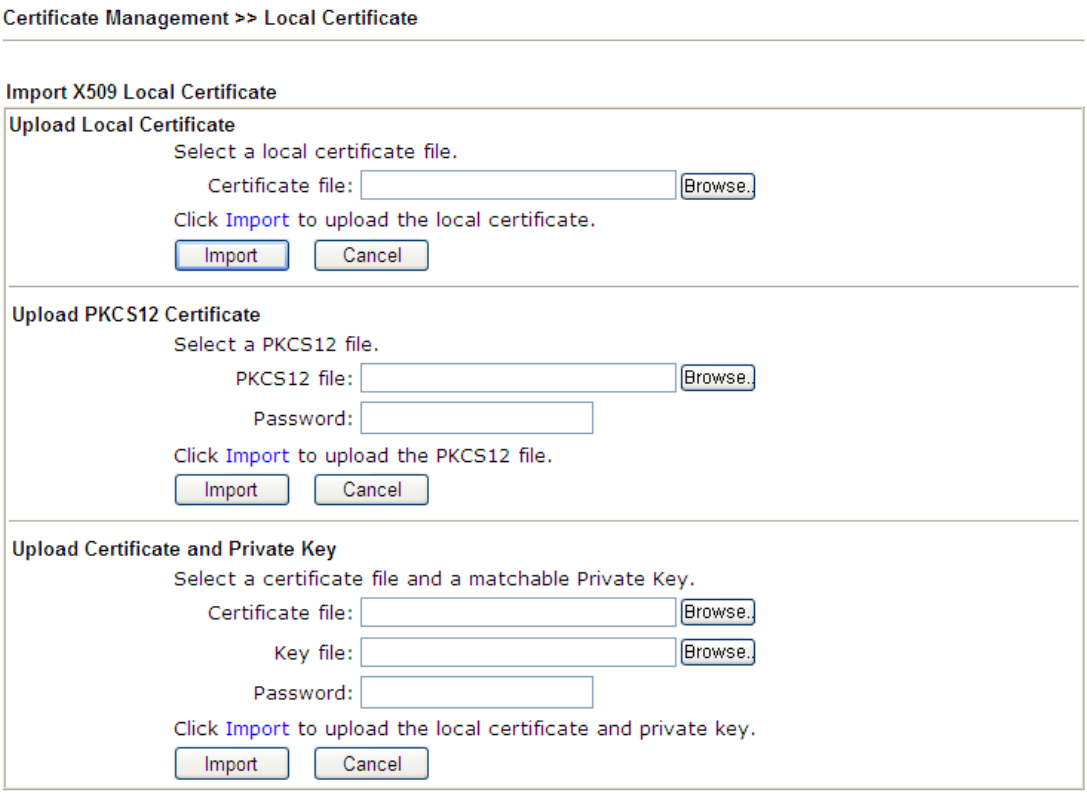
Después de hacer clic en el**Generar**botón, volverá a la pantalla principal Certificado local, que muestra la solicitud de certificado en curso:



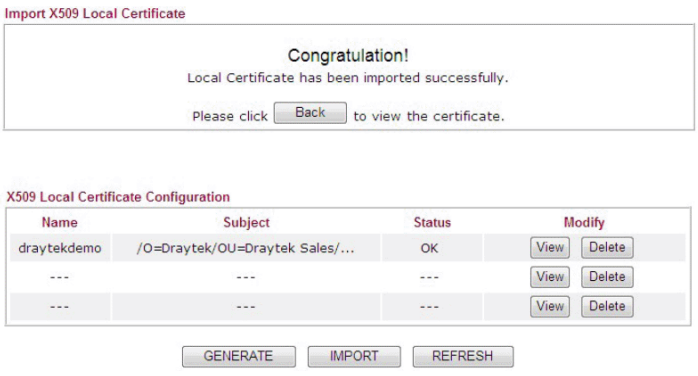
IMPORTAR

El enrutador Vigor le permite generar una solicitud de certificado y enviarla al servidor de CA, luego importarla como "Certificado local". Si ya obtuvo un certificado de un tercero, puede importarlo directamente. Los tipos admitidos son Certificado PKCS12 y Certificado con clave privada.

Haga clic en este botón para importar un archivo guardado como información de certificación. Hay tres tipos de certificados locales compatibles con el enrutador Vigor.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Cargar certificado local	**archivo de certificado -**Hacer clic**Navegar**para seleccionar un archivo de certificado local. **Importar -**Haga clic para importar el archivo de certificado seleccionado al enrutador. **Cancelar -**Haga clic para volver a la pantalla principal Certificado local. Si lo ha hecho bien en la generación de certificados, el estado del certificado se mostrará como "**DE ACUERDO**". 
Subir PKCS12 Certificado	Permite a los usuarios importar el certificado cuyas extensiones suelen ser .pfx o .p12. Y estos certificados suelen necesitar contraseñas. Tenga en cuenta que PKCS12 es un estándar para almacenar certificados y claves privadas de forma segura. Se utiliza (entre otras cosas) en Netscape y Microsoft Internet Explorer con sus opciones de importación y exportación. **archivo PKCS12**-Hacer clic**Navegar**para seleccionar un archivo de certificado PKCS12. **Contraseña**-Ingrese la contraseña asociada con el certificado y los archivos clave. **Importar**-Haga clic para importar el archivo de certificado seleccionado al enrutador.

	Cancelar-Haga clic para volver a la pantalla principal Certificado local.
Subir certificado y **Llave privada**	Es útil cuando los usuarios tienen certificados separados y claves privadas. Y la contraseña es necesaria si la clave privada está cifrada. **archivo de certificado -**Hacer clic**Navegar**para seleccionar un archivo de certificado local. **Archivo de clave**-Hacer clic**Navegar**para seleccionar un archivo clave. **Contraseña**-Ingrese la contraseña asociada con el certificado y los archivos clave. **Importar -**Haga clic para importar el archivo de certificado seleccionado al enrutador. **Cancelar -**Haga clic para volver a la pantalla principal Certificado local.

Certificado de CA de confianza V-2-2

El usuario puede crear certificados RootCA (hasta tres) si es necesario.

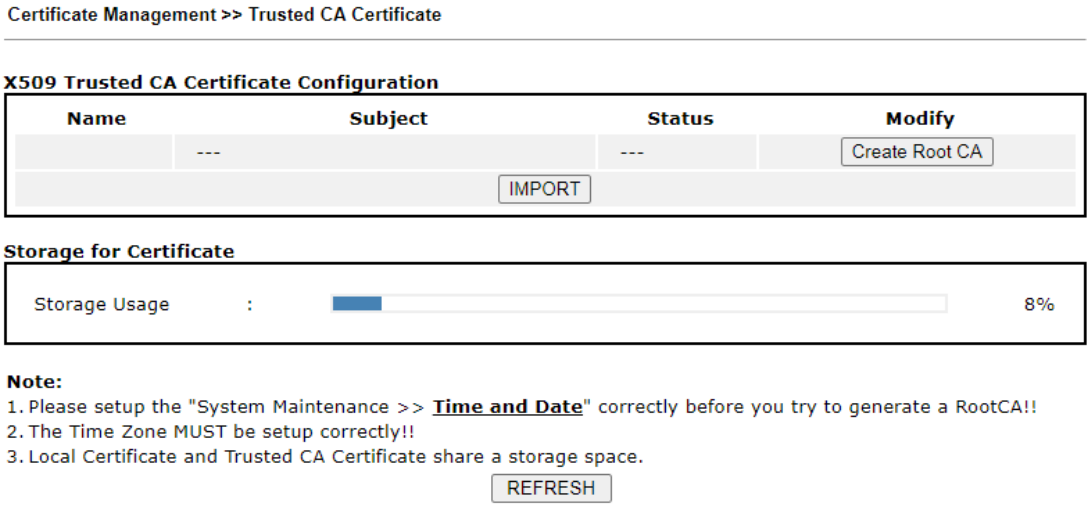
Cuando se requiere que el cliente local y el cliente remoto realicen una autenticación de certificado (p. ej., IPsec X.509) para los datos que pasan a través del túnel SSL y evitan el ataque de MITM, se utilizará una autoridad de certificación raíz confiable (CA raíz) para autenticar el digital. certificados ofrecidos por ambos extremos.

Sin embargo, el procedimiento de solicitud de un certificado digital de una autoridad de certificación raíz de confianza es complicado y requiere mucho tiempo. Por lo tanto, el enrutador Vigor ofrece un mecanismo que le permite generar una CA raíz para ahorrar tiempo y brindar comodidad al usuario general. Posteriormente, dicha CA raíz generada por el servidor DrayTek puede realizar la emisión del certificado local.

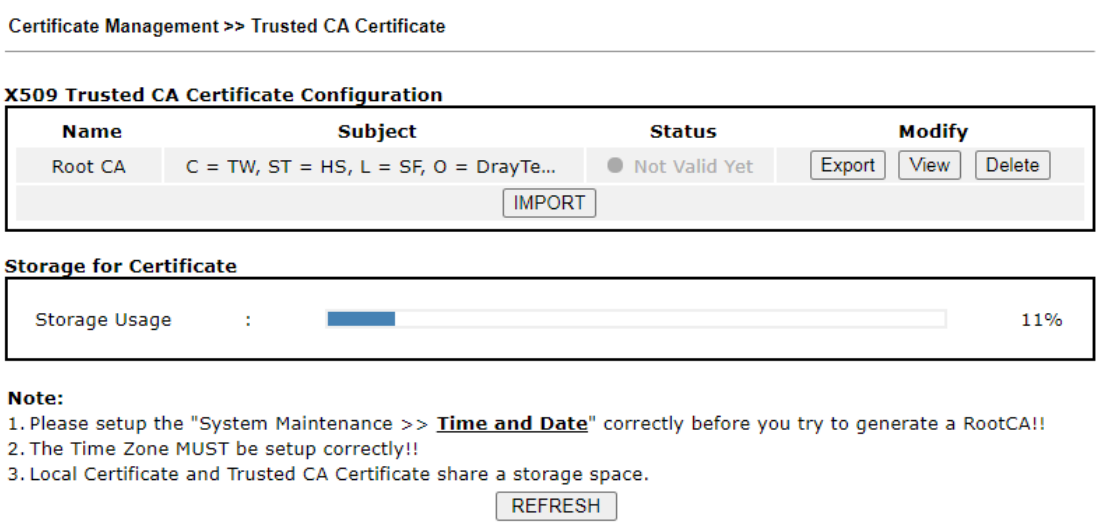
Información

La CA raíz se puede eliminar pero no editar. Si desea modificar la configuración de una CA raíz, elimínela y cree otra haciendo clic en Crear CA raíz.

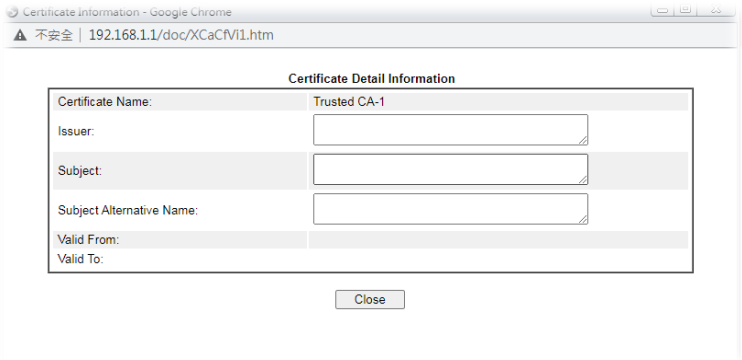
Cree, importe o exporte, vea la raíz de los certificados de la autoridad certificadora de confianza en esta página. No existía una CA raíz



Existía una CA raíz

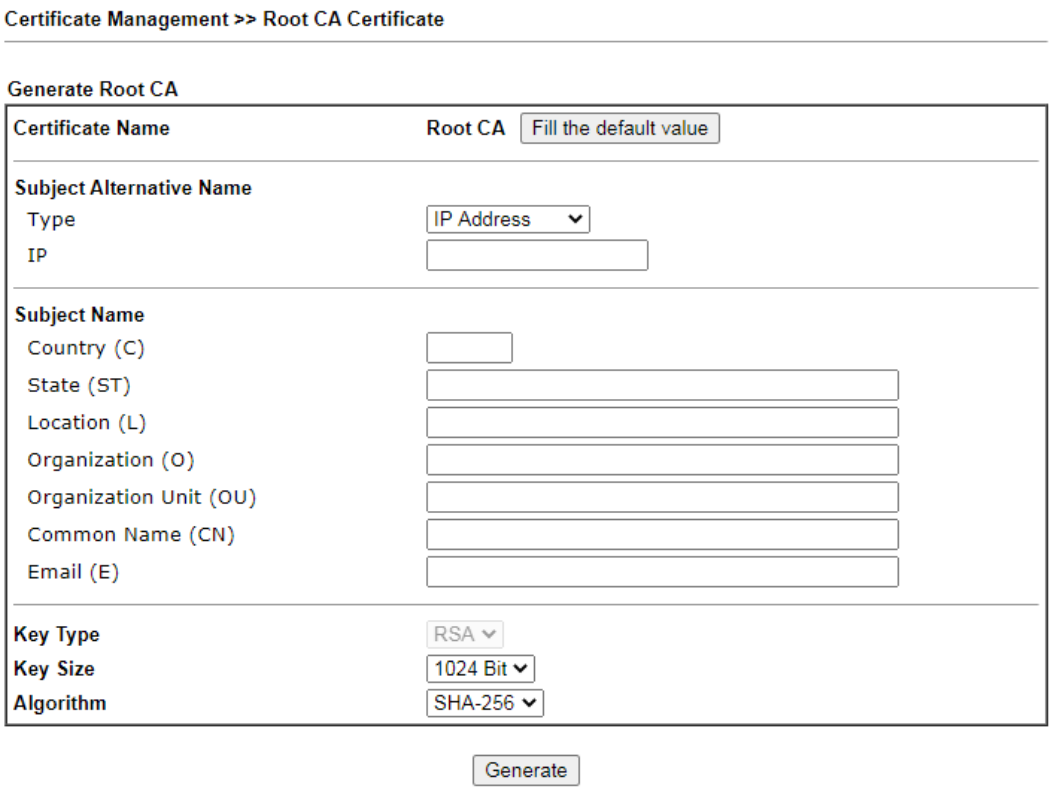


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Crear CA raíz	Haga clic para crear una nueva CA raíz.
Nombre	Nombre que identifica al certificado.
Sujeto	Muestra el nombre del sujeto del certificado.
Estado	Muestra el estado del certificado.
Modificar	Cuando no existía ninguna CA raíz: - **Crear CA raíz –**Haga clic para completar los detalles sobre un certificado e inicie el proceso de generación. Cuando existía una CA raíz: - **Exportar -**Haga clic para exportar el certificado como un - archivo. **Vista -**Haga clic para ver los detalles del certificado.  - **Borrar -**Haga clic para eliminar el certificado.
Importar	Haga clic para importar un certificado existente.
Actualizar	Haga clic para actualizar la página para mostrar la información más reciente del certificado.

Creación de una CA raíz

Hacer clic**Crear CA raíz**para abrir la página siguiente.

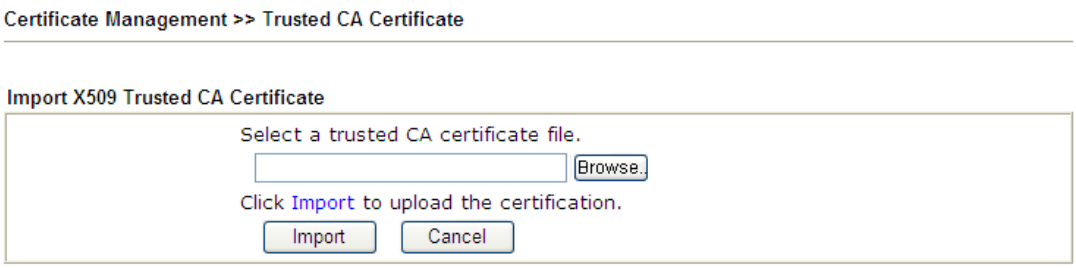


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre del certificado	Muestra el nombre de la CA raíz. **Rellene el valor predeterminado**-Haga clic para ingresar el valor predeterminado para esta CA raíz.
Tipo	Seleccione el tipo de Nombre alternativo del sujeto e ingrese su valor.
País (C)	País en el que se encuentra su organización.
Estado (ST)	Estado o provincia donde se encuentra su organización.
Ubicación (L)	Ciudad donde se encuentra su organización.
Organización (O)	Nombre legal de su organización.
Unidad organizativa (OU)	Departamento dentro de su organización que desea asociar con este certificado.
Nombre común (CN)	Nombre de dominio totalmente calificado/IP WAN que se utilizará para llegar a su servidor.
Correo electrónico (E)	Dirección de correo electrónico de la entrada.
Tipo de clave	El tipo de clave está configurado de forma rígida en RSA.
Tamaño de clave	Elija entre 1024 y 2048 bits.
Algoritmo	Elija entre SHA-1 y SHA-256.
Generar	Haga clic para enviar una solicitud de generación al servidor de CA.

Importación de una CA de confianza

Para importar un certificado de CA de confianza previamente guardado, haga clic en**IMPORTAR**para abrir la siguiente ventana.

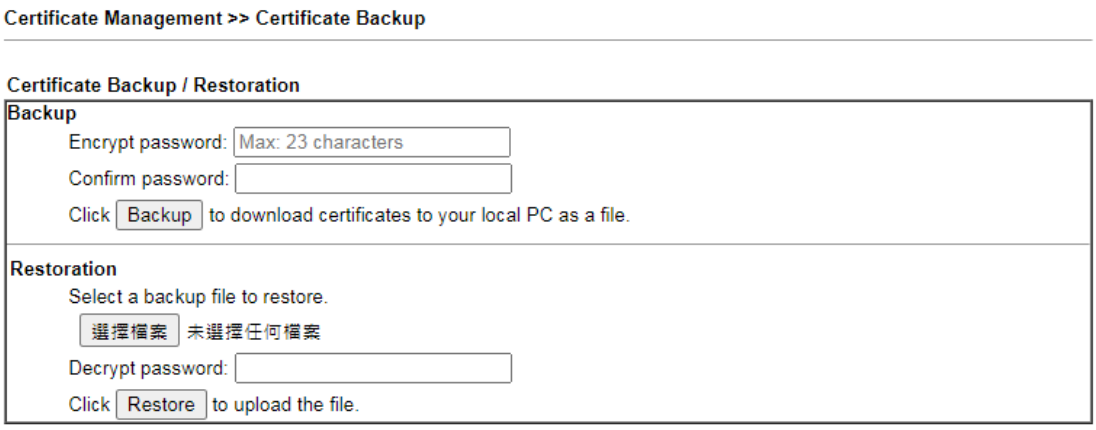


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Navegar	Haga clic en Examinar para seleccionar un archivo de certificado de CA.
Importar	Haga clic para importar el archivo de certificado seleccionado al enrutador. El que importó aparecerá en la ventana Certificado de CA de confianza.
Cancelar	Haga clic para volver a la pantalla principal Certificado de CA de confianza.

Copia de seguridad del certificado V-2-3

Puede hacer una copia de seguridad de los certificados de CA locales y de confianza en el enrutador en un archivo.



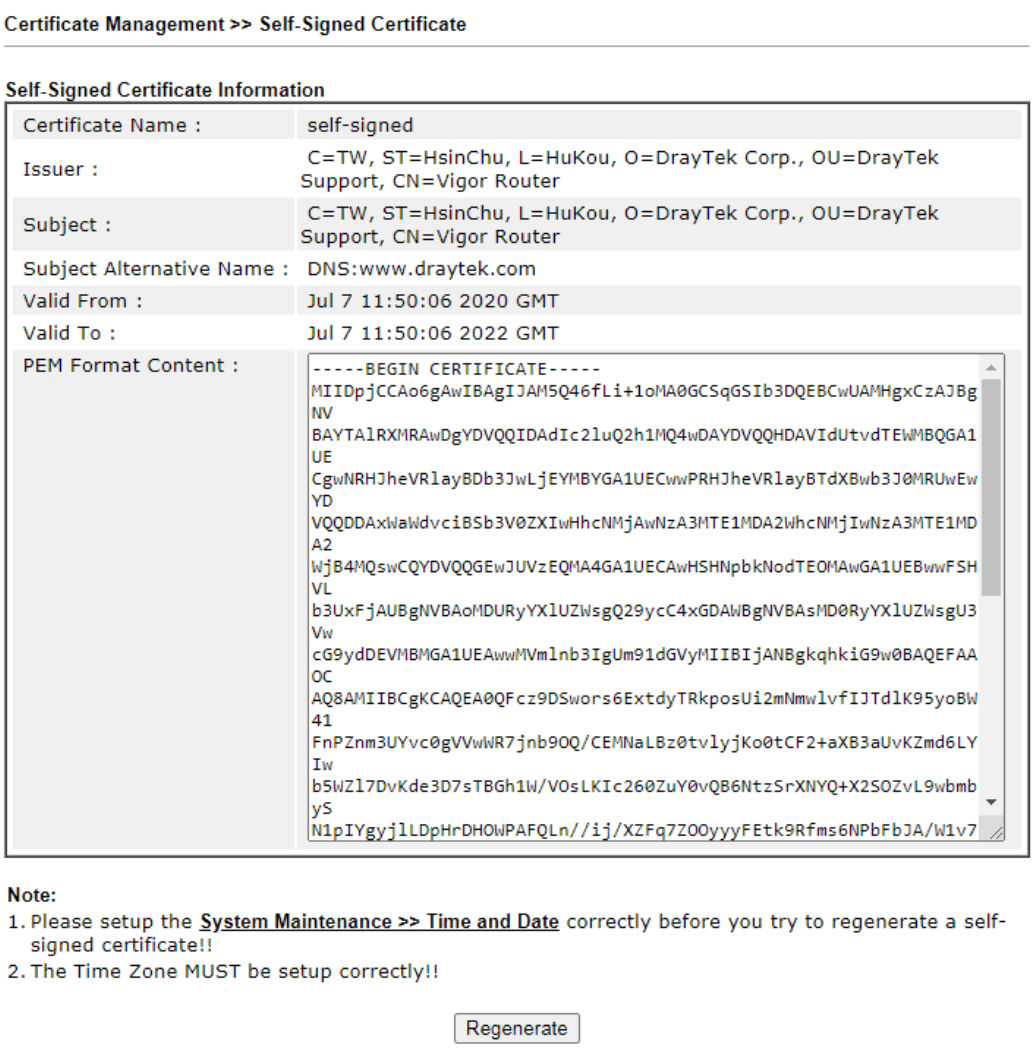
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Respaldo	
cifrar **contraseña confirmada** **contraseña**	Introduzca la contraseña con la que desea cifrar el certificado.
Respaldo	Haga clic para descargar el certificado.
Restauracion	
Seleccione un archivo de copia de seguridad para restaurar	Haga clic en Examinar para seleccionar el archivo de copia de seguridad que desea restaurar.
Descifrar contraseña	Introduzca la contraseña que se utilizó para cifrar los certificados.
Restaurar	Haga clic para recuperar el certificado.

Certificado autofirmado V-2-4

Un certificado autofirmado es un*único*identificación para el dispositivo (por ejemplo, enrutador Vigor) que genera el certificado por sí mismo para garantizar la seguridad del enrutador. Dicho certificado autofirmado se firma con su propia clave privada.

El certificado autofirmado se aplicará en SSL VPN, HTTPS, etc. Además, se puede crear de forma gratuita utilizando una amplia variedad de herramientas.



Hacer clic**Regenerado**para abrir la ventana Regenerar certificado autofirmado. Ingrese toda la información solicitada, incluido el nombre del certificado (utilizado para diferenciar diferentes certificados), el tipo de nombre alternativo del sujeto y la configuración relacional para el nombre del sujeto. Luego haga clic en GENERAR.

Lista de servicios locales V-2-5

Esta página muestra el certificado utilizado por los servicios locales. Los usuarios pueden hacer clic para crear un certificado autofirmado.

Certificate Management >> Local Services List

Default Certificate: self-signed

Certificate Name	Local Services
Default Certificate	Router Management -- Web Access from LAN or WAN
	Router Management -- SSH
	VPN and Remote Access >> LAN to LAN -- SSL VPN
	VPN and Remote Access >> Remote Dial-in User -- SSL VPN
	VPN and Remote Access >> OpenVPN -- OpenVPN
	Hotspot Web Portal
	Applications >> Internal RADIUS
	Applications >> Local 802.1X General Setup
	Applications >> High Availability
	CSM >> DNS Filter -- block page
	USB Application >> USB User Management
server	
None	**VPN and Remote Access >> IPsec General Setup**

OK

Esta página se deja en blanco.

Parte VI Seguridad

Firewall

Si bien los usuarios de banda ancha demandan más ancho de banda para multimedia, aplicaciones interactivas o aprendizaje a distancia, la seguridad siempre ha sido la principal preocupación. El firewall del enrutador Vigor ayuda a proteger su red local contra ataques de personas externas no autorizadas. También restringe el acceso a Internet de los usuarios de la red local.

CSM

CSM es una abreviatura de Administración de seguridad central que se utiliza para controlar el uso de IM/P2P, filtrar el contenido web y el contenido de URL para alcanzar un objetivo de administración de seguridad.

Básico

Un firewall de red monitorea el tráfico que viaja entre redes, con la capacidad de permitir o bloquear el tráfico de manera selectiva mediante un conjunto predefinido de reglas de seguridad. Esto ayuda a mantener la integridad de las redes al detener el acceso no autorizado y el intercambio de información confidencial.

Instalaciones de cortafuegos

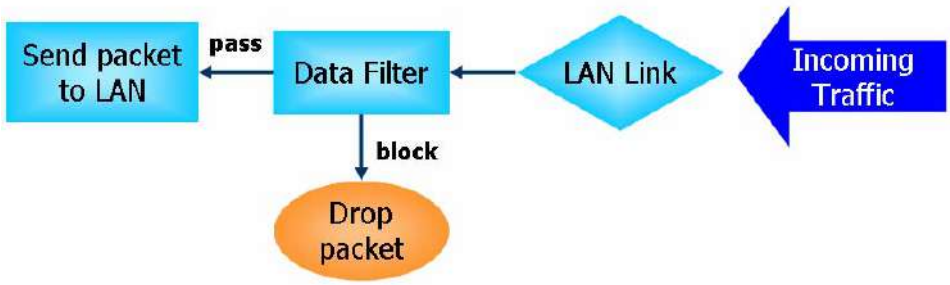
Los usuarios de LAN cuentan con protección segura mediante las siguientes instalaciones de firewall:

- Filtro IP configurable por el usuario (filtro de datos).
- Stateful Packet Inspection (SPI): realiza un seguimiento de los paquetes y niega los datos entrantes no solicitados
- Protección contra ataques seleccionables de denegación de servicio (DoS)/Distributed DoS (DDoS)

Filtro de datos

Todo el tráfico, tanto entrante como saliente, que no desencadena un intento de conexión PPP (ya sea porque no es necesaria una conexión PPP o porque la conexión PPP requerida ya se ha establecido) se compara con el filtro de datos y se permitirá o bloqueará según a las reglas configuradas dentro.

Los siguientes diagramas de flujo muestran cómo el enrutador trata el tráfico entrante y el tráfico saliente, respectivamente.



Inspección de paquetes con estado (SPI)

La inspección con estado es una arquitectura de firewall que funciona en la capa de red. A diferencia del filtrado de paquetes estáticos heredado, que examina un paquete en función de la información de su encabezado, la inspección de estado construye una máquina de estado para rastrear cada conexión que atraviesa todas las interfaces del firewall y se asegura de que sean válidas. El firewall con estado del enrutador Vigor no solo examina la información del encabezado, sino que también monitorea el estado de la conexión.

Defensa de denegación de servicio (DoS)

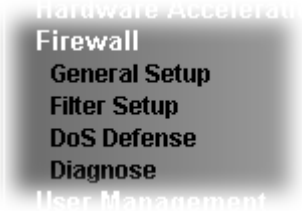
Los ataques DoS se clasifican en dos tipos: ataques de inundación y ataques de vulnerabilidad. Los ataques de tipo inundación intentan agotar los recursos del sistema, mientras que los ataques de vulnerabilidad intentan paralizar el sistema explotando las vulnerabilidades de los protocolos o sistemas operativos.

La funcionalidad DoS Defense de Vigor detecta ataques DoS y mitiga su daño al inspeccionar cada paquete entrante, y los paquetes maliciosos serán bloqueados. Si Syslog está habilitado, también se enviarán mensajes de alerta. También se bloquea el flujo de tráfico anómalo, como los ataques de inundación y exploración de puertos que superan los umbrales permitidos.

A continuación se muestran los tipos de ataques que la función de defensa DoS/DDoS puede detectar:

1. Ataque de inundación SYN
2. Ataque de inundación UDP
3. Ataque de inundación ICMP
4. Ataque de escaneo de puertos
5. Opciones de IP
6. Ataque terrestre
7. Ataque de pitufo
8. Trazar ruta
9. Fragmento SYN
10. Ataque Fraggle
11. Escaneo de bandera TCP
12. Ataque de lágrimas
13. Ataque de ping de la muerte
14. Fragmento ICMP
15. Números no asignados

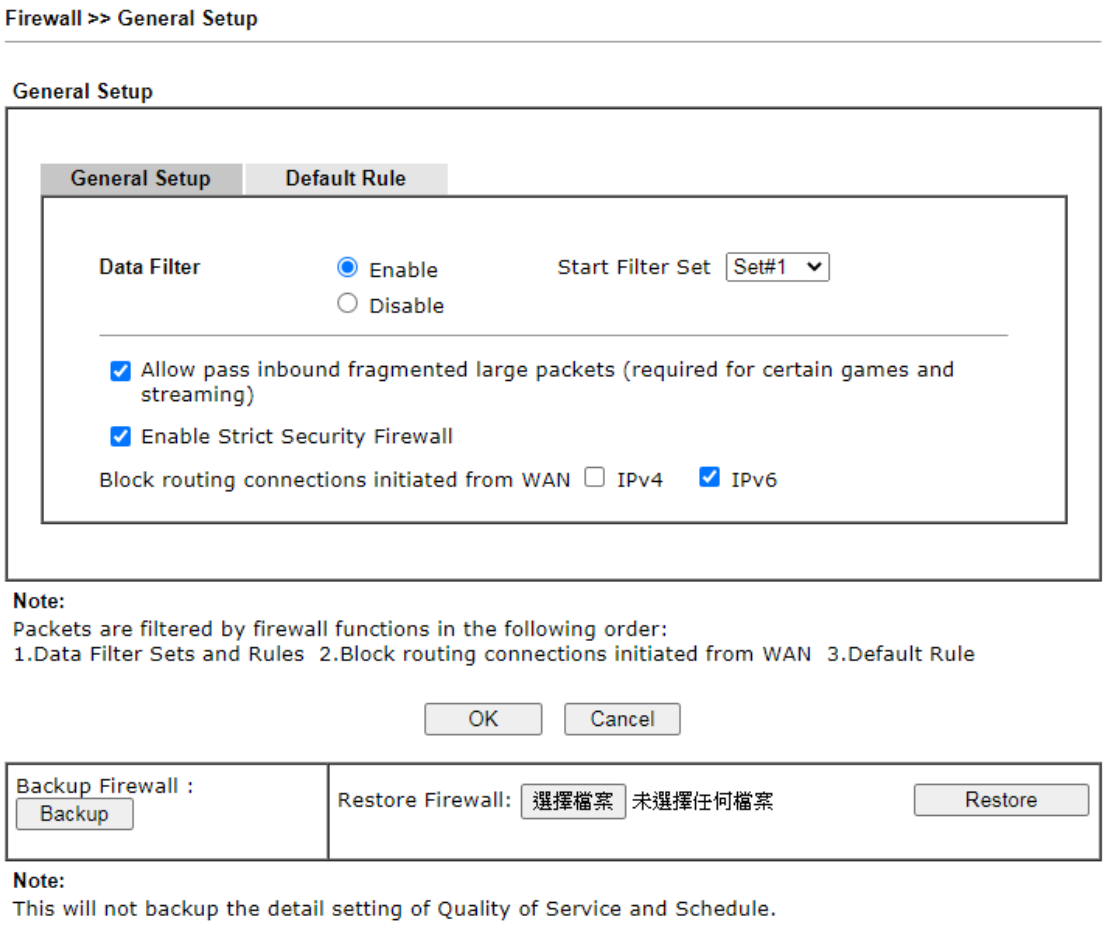
A continuación se muestran los elementos del menú para Firewall.



VI-1-1 Configuración general

Página de configuración general

Dicha página le permite habilitar / deshabilitar el filtro de datos, determinar la regla general para filtrar los datos entrantes y salientes.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Filtro de datos	Seleccionar**Permitir**para activar la función Filtro de datos y, a continuación, seleccione Iniciar conjunto de filtros.

Pasar siempre entrante paquetes grandes fragmentados	Ciertos juegos y servicios de transmisión de video usan paquetes UDP fragmentados para transferir datos. Habilitar esta opción permite que estas aplicaciones funcionen correctamente. Si esta opción no está habilitada, el enrutador intentará volver a ensamblar los paquetes fragmentados hasta cierto valor (p. ej., 15xx~2102) kilobytes de longitud. Los paquetes más grandes que el valor determinado serán descartados. Si esta opción está habilitada, el enrutador siempre pasa paquetes fragmentados sin volver a ensamblarlos, independientemente del tamaño del paquete.
Habilitar seguridad estricta cortafuegos	Si esta opción y el Filtro de contenido web (WCF) están habilitados, el tráfico web se bloqueará si el servidor WCF no responde a las solicitudes de búsqueda.
Bloquear conexiones de enrutamiento iniciadas desde WAN	**IPv6**-IPv6 no utiliza la traducción de direcciones de red (NAT), por lo que todos los hosts de LAN reciben direcciones IP IPv6 públicas que están expuestas a la WAN. Habilite esta opción para impedir que los hosts WAN se conecten a los hosts LAN mediante IPv6. **IPv4**-Para los hosts de LAN que reciben direcciones IPv4 de WAN mediante la subred enrutada por IP, habilite esta opción para evitar que los hosts de WAN se conecten a los hosts de LAN. Esta opción no tiene efecto en hosts LAN en subredes LAN privadas.
Cortafuegos de respaldo	Hacer clic**Respaldo**para guardar la configuración del cortafuegos.
Restaurar cortafuegos	Hacer clic**Seleccionar**para elegir un archivo de configuración de cortafuegos. Luego haga clic**Restaurar**para aplicar el archivo.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en

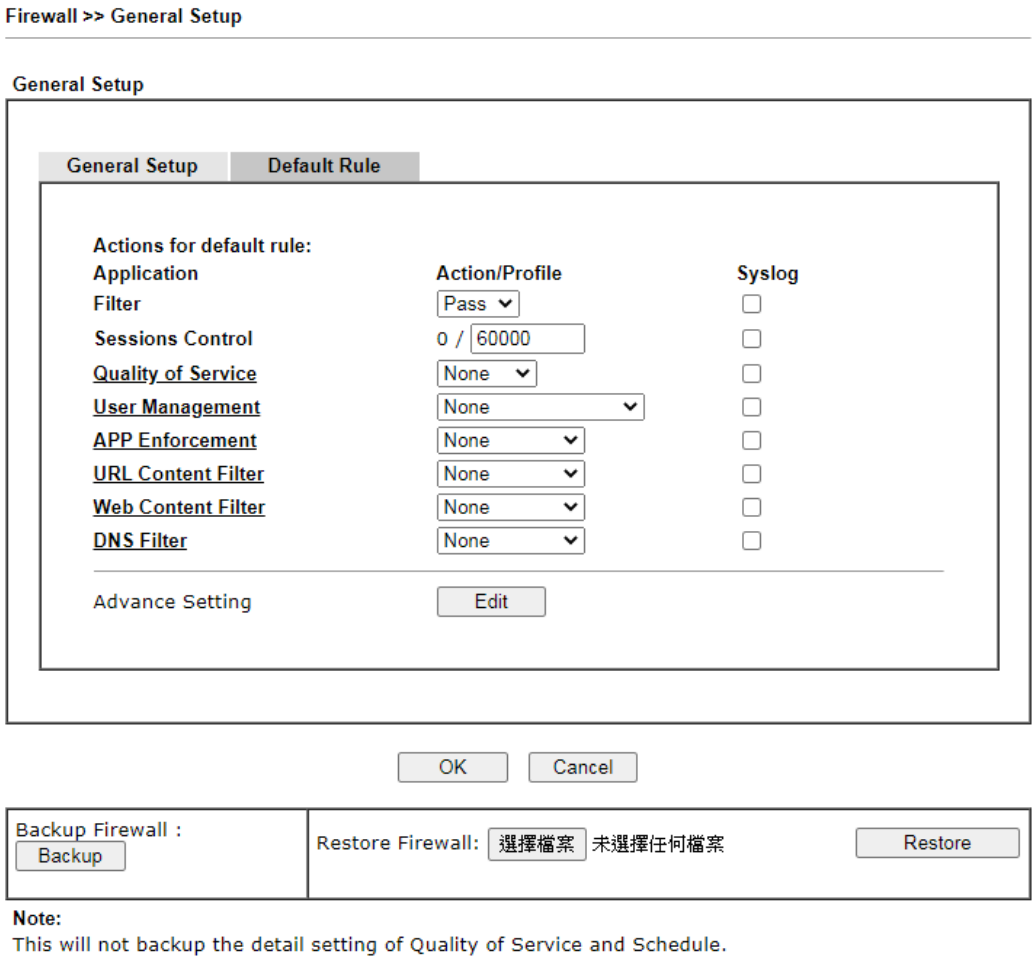
Cancelar. El tráfico se filtra por las funciones del cortafuegos en el siguiente orden:

1. Conjuntos de filtros de datos y reglas
2. Bloquear conexiones iniciadas desde WAN
3. Regla por defecto

Página de regla predeterminada

Dicha página le permite elegir perfiles de filtrado que incluyen QoS, política de equilibrio de carga, WCF, cumplimiento de aplicaciones, filtro de contenido de URL, para la transmisión de datos a través del enrutador Vigor.

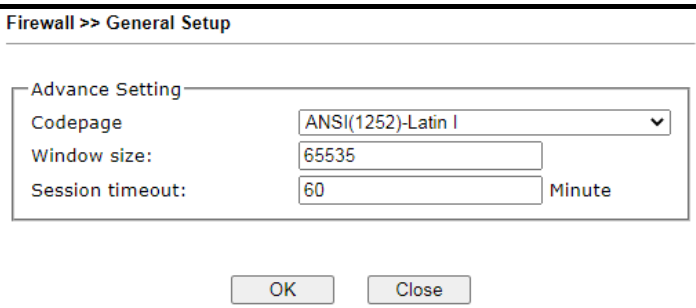
La regla predeterminada se aplica a todo el tráfico que no está restringido por otros filtros o reglas.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Filtrar	Seleccionar**Aprobar**o**Bloquear**para los paquetes que no coinciden con las reglas de filtrado. Cuando la configuración es Bloquear, todos los demás campos de la página están deshabilitados porque no son aplicables.
Control de sesiones	El número actual de sesiones se muestra antes de la barra inclinada, seguido del número máximo de sesiones simultáneas permitidas, que es configurable. El máximo predeterminado es 60000, que también es el límite superior del valor.
Calidad de servicio	Elija una de las reglas de QoS para aplicarla como regla de firewall. Para obtener información detallada sobre la configuración de QoS, consulte la sección relacionada más adelante.
Gestión de usuarios	Esta configuración solo está disponible cuando**Basado en reglas**se selecciona en **Gestión de usuarios>>Configuración general**. La regla de firewall predeterminada se aplicará al usuario o grupo de usuarios seleccionado. Consulte el capítulo sobre Gestión de usuarios para obtener más detalles sobre la función. - **Ninguno**: La gestión de usuarios no se aplica al valor predeterminado

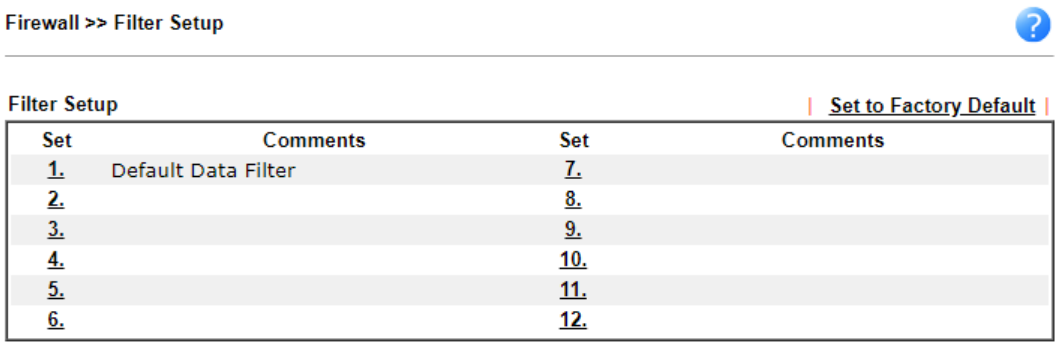
	regla. - **Objeto de usuario**: La regla predeterminada solo se aplica al usuario seleccionado. - [**Crear nuevo usuario**]: Seleccione esto para crear un nuevo usuario. - Grupo de usuarios: la regla predeterminada solo se aplica al grupo de usuarios seleccionado. - [**Crear nuevo grupo**]: Seleccione esto para crear un nuevo grupo de usuarios. - **TODO**: la regla predeterminada se aplica a todos los usuarios definidos. - **Crear nuevo usuario**o**Crear nuevo grupo**Aparecerá un elemento para que haga clic para crear uno nuevo si no existe un perfil de usuario o un perfil de grupo. **registro del sistema**-Seleccione para permitir que la administración de usuarios registre mensajes en Syslog.
Cumplimiento de la aplicación	Seleccione un perfil de Cumplimiento de aplicaciones para el bloqueo de aplicaciones o Ninguno para deshabilitar el Cumplimiento de aplicaciones para la regla predeterminada. Seleccionar**[Crear nuevo]**de la lista desplegable para crear un nuevo perfil. Consulte el capítulo sobre Cumplimiento de aplicaciones para obtener más detalles sobre la función. **registro del sistema**-Seleccione para permitir el cumplimiento de aplicaciones para registrar mensajes en Syslog.
Filtro de contenido de URL	Seleccione un perfil de filtro de contenido de URL para usar, o Ninguno para deshabilitar el filtro de contenido de URL para la regla predeterminada. Seleccionar **[Crear nuevo]**de la lista desplegable para crear un nuevo perfil. Consulte el capítulo sobre Filtro de contenido de URL para obtener más detalles sobre la función. **registro del sistema**-Seleccione para permitir que el filtro de contenido de URL registre mensajes en Syslog. La acción de registro se configura en el nivel de perfil en CSM>>Perfil de filtro de contenido de URL, Registro.
Filtro de contenido web	Seleccione un perfil de Filtro de contenido web para usar, o Ninguno para deshabilitar el Filtro de contenido web para la regla predeterminada. Seleccionar **[Crear nuevo]**de la lista desplegable para crear un nuevo perfil. **registro del sistema**-Seleccione para permitir que Web Content Filter registre mensajes en Syslog. La acción de registro se configura en el nivel de perfil en la sección Tabla de perfil de filtro de contenido web en CSM>>Perfil de filtro de contenido web, Registro.
Filtro DNS	Seleccione el perfil de filtro DNS que se usará o Ninguno para deshabilitar el filtro DNS para la regla predeterminada. Seleccionar**[Crear nuevo]**de la lista desplegable para crear un nuevo perfil. **registro del sistema**-Seleccione para permitir que el filtro DNS registre mensajes en Syslog. La acción de registro se configura en el nivel de perfil en la sección Tabla de perfil de filtro DNS en CSM>>Perfil de filtro DNS, SysLog.
Configuración avanzada	Hacer clic**Editar**para abrir la ventana de configuración de Configuración avanzada. Sin embargo lo és**recomendado**para utilizar la configuración predeterminada.

	 **Página de código**–Establece la página de códigos utilizada por el filtro de contenido de URL para hacer coincidir las URL con las palabras clave en los perfiles. La elección de la página de códigos adecuada puede aumentar la precisión del filtro de contenido de URL. El valor predeterminado es ANSI 1252 Latin I. Si la configuración es Ninguno, no se realizará la decodificación de URL. Si no está seguro de qué página de códigos usar, inicie la aplicación Syslog y la página de códigos recomendada se mostrará en la pestaña Información de la página de códigos en el cuadro de diálogo Configuración. **Tamaño de ventana**–Establece el tamaño de la ventana TCP como se describe en RFC 1323. Los valores válidos son de 0 a 65535. Cuanto mayor sea el valor, mejor será el rendimiento. Sin embargo, si la red no es estable, el valor pequeño será apropiado. **Hora de término de la sesión**–Establece el tiempo de espera que las sesiones pueden estar inactivas antes de que se eliminen del sistema.
Cortafuegos de respaldo	Hacer clic**Respaldo**para guardar la configuración del cortafuegos.
Restaurar cortafuegos	Hacer clic**Seleccionar**para elegir un archivo de configuración de cortafuegos. Luego haga clic**Restaurar**para aplicar el archivo.

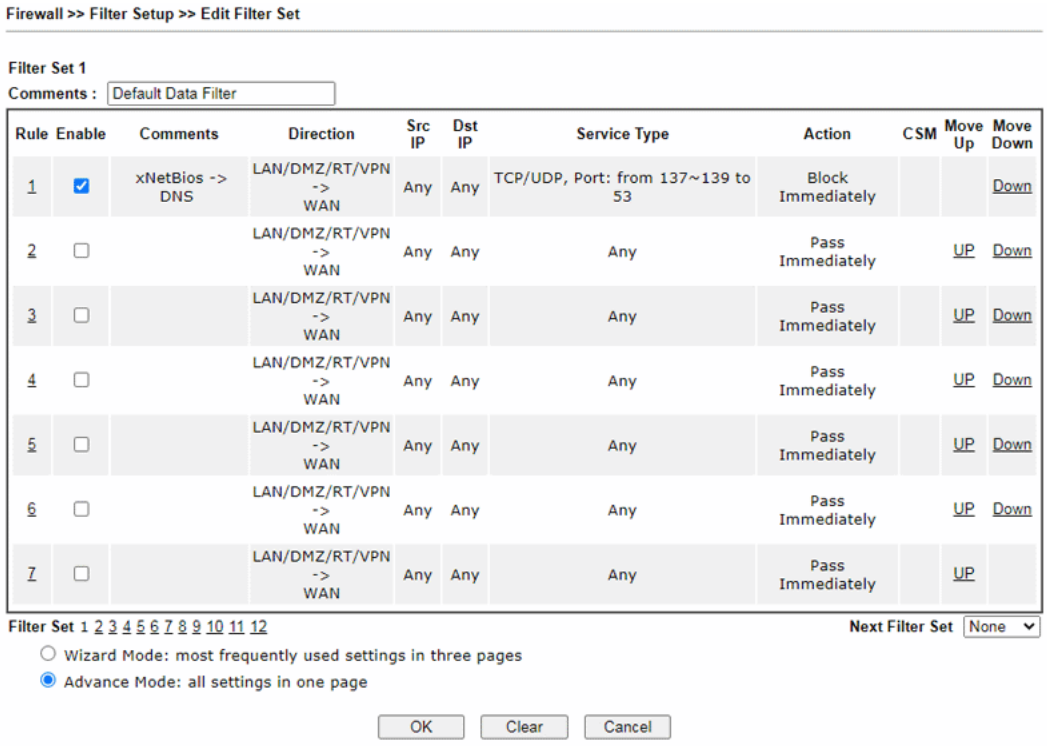
Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

Configuración del filtro VI-1-2

Hacer clic**cortafuegos**y haga clic**Configuración del filtro**para abrir la página de configuración.



Para editar un conjunto de filtros, haga clic en su número de conjunto. Se mostrará la siguiente página de Conjunto de filtros. Cada conjunto de filtros contiene hasta 7 reglas.



Los ajustes disponibles se explican a continuación:

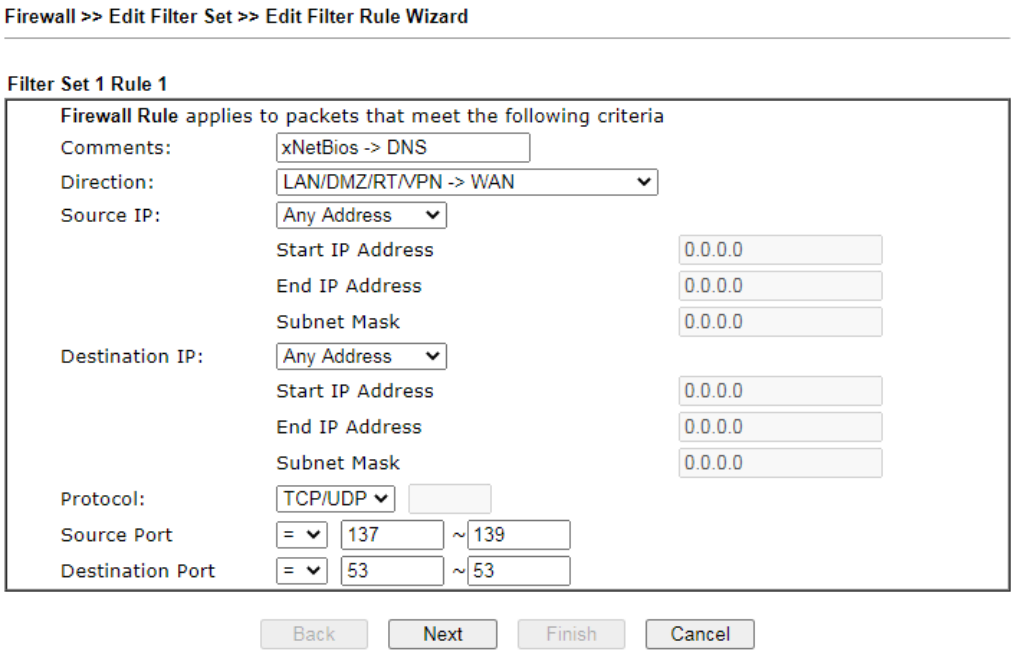
Artículo	Descripción
Regla de filtro	Para editar la regla de filtro, haga clic en el número de la regla de filtro para abrir la página Editar regla de filtro. Consulte la siguiente sección para obtener detalles sobre la página Editar regla de filtro.
Permitir	Seleccione para habilitar la regla de filtrado.
Comentarios	Comentario opcional ingresado en la página de configuración para identificar la regla.
Dirección	Muestra la dirección del paquete.
IP de origen / IP de horario	Muestra la dirección IP de origen/destino.
Tipo de servicio	Muestra el tipo y número de puerto del paquete.

Acción	Muestra los paquetes a pasar/bloquear.
CSM	Muestra la seguridad del contenido gestionado
Mover arriba/abajo	Usar**Arriba**o**Abajo**enlace para cambiar el orden de las reglas de filtrado.
Siguiente conjunto de filtros	Seleccione el conjunto de filtros para que el cortafuegos procese después del conjunto de filtros actual, o Ninguno si el conjunto de filtros actual es el último en procesarse. Tenga cuidado de no crear un bucle al configurar los siguientes conjuntos de filtros.
Modo mago	Permita configurar los ajustes de uso frecuente para la regla de filtro a través de varias páginas de configuración.
Modo avanzado	Permitir configurar ajustes detallados de la regla de filtro.

Para usar el Modo Asistente, simplemente siga los siguientes pasos:

1. Haga clic en el**Modo mago**boton de radio.

2. Haga clic en**Índice 1**. La página de configuración aparecerá de la siguiente manera:



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Comentarios	Ingrese los comentarios/la descripción del conjunto de filtros. La longitud máxima es de 14 caracteres.
Dirección	Establece la dirección del flujo de paquetes. **Nota:**RT significa dominio de enrutamiento para la segunda subred u otra LAN.
IP de origen/destino	Para configurar la dirección IP manualmente, elija**Cualquier dirección/ Dirección única/Dirección de rango/Dirección de subred**como el tipo de dirección e introdúzcalos en este cuadro de diálogo.
Protocolo	Especifique los protocolos a los que se aplicará esta regla de filtrado.

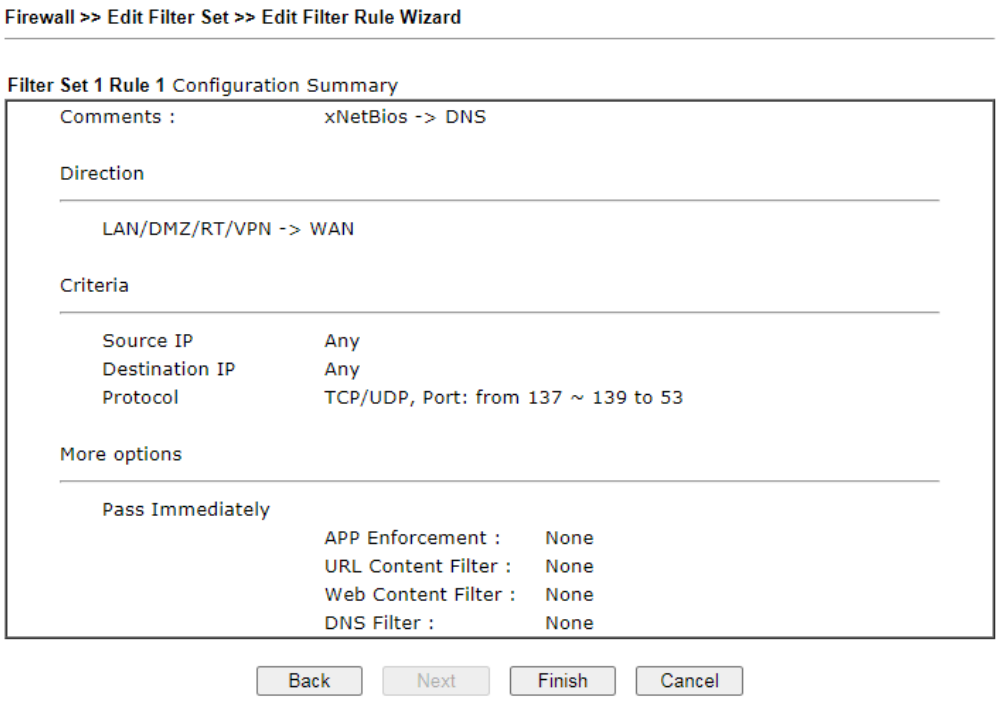
Puerto de origen / Puerto de destino	***(=)***-cuando el primer y el último valor son iguales, indica un puerto; cuando el primer y el último valor son diferentes, indica un rango para el puerto y disponible para este tipo de servicio. ***(!=)***-cuando el primer y último valor son iguales, indica todos los puertos excepto el puerto aquí definido; cuando el primer y el último valor son diferentes, indica que todos los puertos excepto el rango definido aquí están disponibles para este tipo de servicio. ***(>)***-el número de puerto mayor que este valor está disponible. ***(<)***-el número de puerto menor que este valor está disponible para este perfil.

3. Haga clic en**Próximo**para obtener la siguiente página.

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Pase inmediatamente	Los paquetes que coincidan con la regla se pasarán inmediatamente. **Cumplimiento de la aplicación -**Seleccione un perfil de Cumplimiento de aplicaciones para el bloqueo de aplicaciones o Ninguno para deshabilitar el Cumplimiento de aplicaciones para la regla predeterminada. Seleccionar**[Crear nuevo]**de la lista desplegable para crear un nuevo perfil. Consulte el capítulo sobre Cumplimiento de aplicaciones para obtener más detalles sobre la función. **Filtro de contenido URL -**Seleccione un perfil de filtro de contenido de URL para usar, o Ninguno para deshabilitar el filtro de contenido de URL para la regla predeterminada. Seleccionar**[Crear nuevo]**de la lista desplegable para crear un nuevo perfil. Consulte el capítulo sobre Filtro de contenido de URL para obtener más detalles sobre la función. **Filtro de contenido web -**Seleccione un perfil de Filtro de contenido web para usar, o Ninguno para deshabilitar el Filtro de contenido web para la regla predeterminada. Seleccionar**[Crear nuevo]**de la lista desplegable para crear un nuevo perfil. **Filtro DNS -**Seleccione el perfil de filtro DNS que se usará o Ninguno para deshabilitar el filtro DNS para la regla predeterminada. Seleccionar **[Crear nuevo]**de la lista desplegable para crear un nuevo perfil.
Bloquear inmediatamente	Los paquetes que coincidan con la regla se eliminarán inmediatamente.

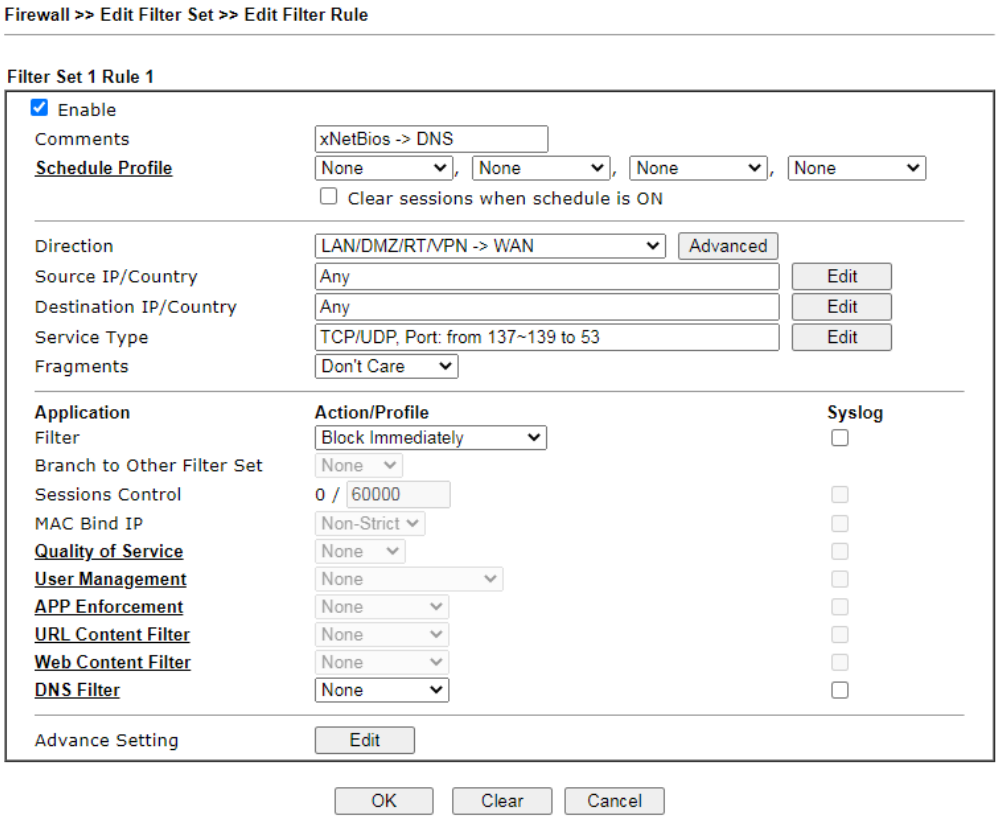
4. Después de elegir el mecanismo, haga clic en**Próximo**para obtener la página de resumen como referencia.



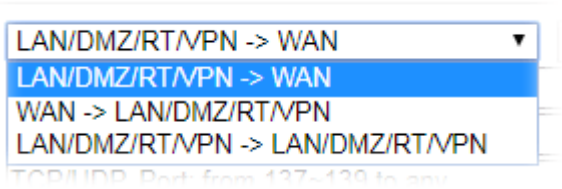
5. Si no hay ningún error, haga clic en**Finalizar**para completar la configuración del asistente.

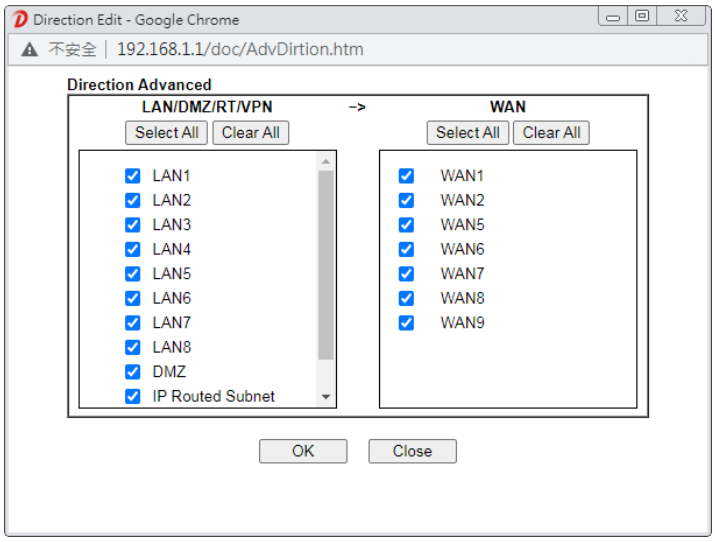
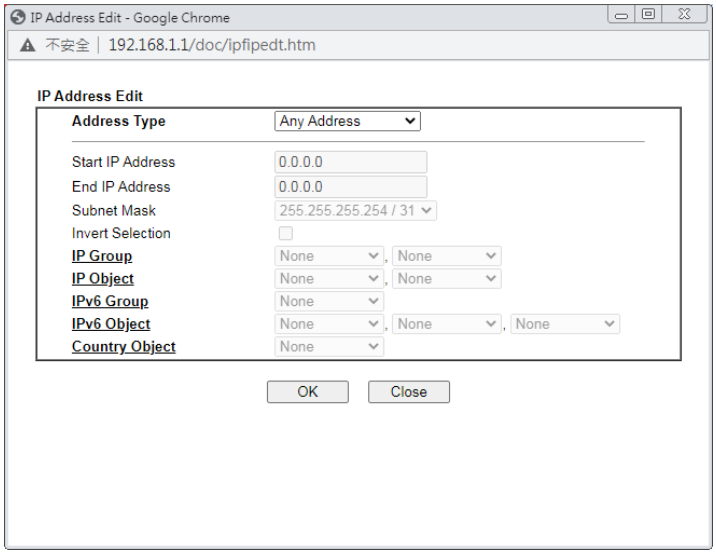
Usar**Avance**modo, siga los siguientes pasos:

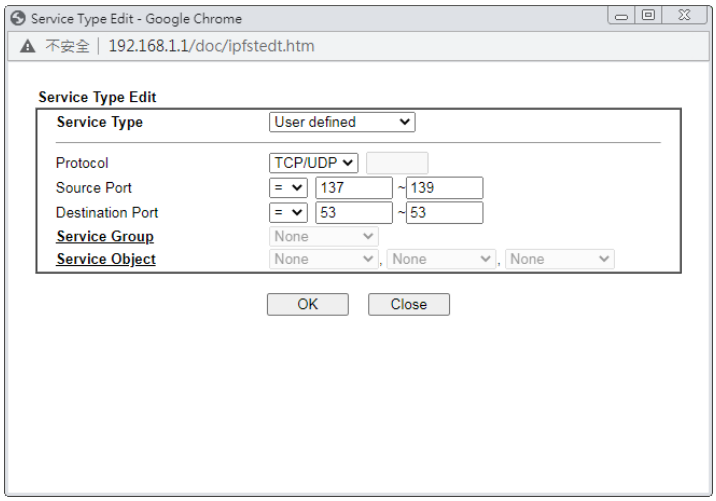
1. Haga clic en el**Modo avanzado**boton de radio.
2. Haga clic en**Índice 1**para acceder a la página siguiente.



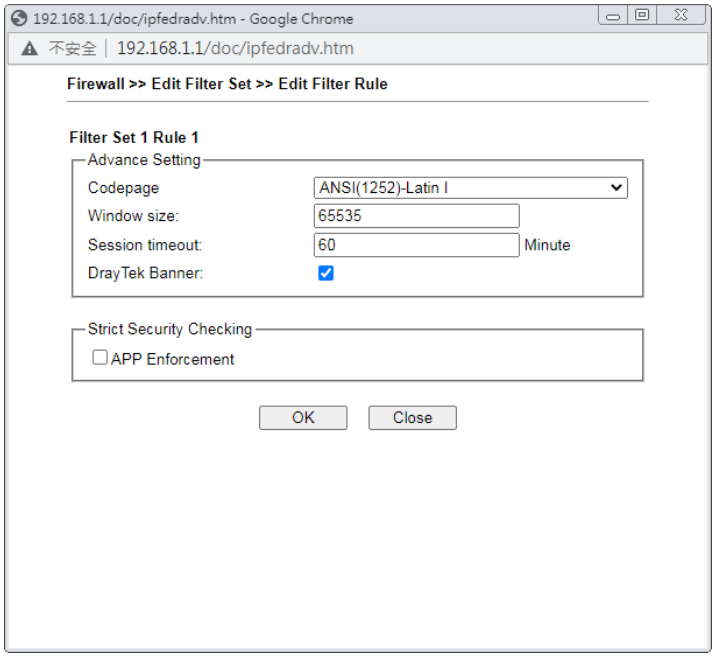
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Marque esta casilla para habilitar la regla de filtro.
Comentarios	Ingrese los comentarios/la descripción del conjunto de filtros. La longitud máxima es de 14 caracteres.
Programar perfil	Seleccione Programar índices para permitir que la regla se habilite en momentos específicos. Puede elegir hasta 4 de los 15 horarios en Aplicaciones >> Horario. La regla siempre está habilitada cuando no se han seleccionado índices.
Borrar sesiones cuando programar ON	Seleccione esta opción para borrar las sesiones existentes cuando la regla cambia está habilitada por un perfil de programación. Todas las conexiones se restablecerán.
Dirección	Especifique la dirección del flujo de tráfico a la que se aplica esta regla de filtro.  **Nota:**RT representa el dominio de enrutamiento para la segunda subred u otra LAN.

	Avanzado-Después de elegir la dirección, haga clic en el botón Avanzado para especificar interfaces para el flujo de tráfico. 
IP de origen/ País y IP de destino / País	Hacer clic**Editar**para abrir el siguiente cuadro de diálogo para configurar las direcciones IP de origen y destino o los objetos de país.  Para configurar la dirección IP manualmente, elija un tipo de dirección e ingrese la información requerida. **Tipo de dirección**–Seleccione uno de los siguientes: - **Cualquier dirección**–Todas las direcciones IP - **Dirección única**–Ingrese una dirección IP en la dirección IP de inicio - **Dirección de rango**–Ingrese las direcciones IP de inicio y finalización - **Dirección de subred**–Ingrese la dirección IP de inicio y la máscara de subred. Ejemplo: Dirección IP de inicio 192.168.1.1 y Máscara de subred 255.255.255.128 significa que es lo mismo que tener la Dirección IP de inicio como 192.168.1.1 y la Dirección IP final como 192.168.1.127. - **Grupo y Objetos**–Permite la selección de grupos de IP y objetos de IP predefinidos. Para obtener detalles sobre los grupos de IP y los objetos, consulte el capítulo sobre configuración de objetos. - **Objeto País**-Permite la selección de objetos de país predefinidos.
Tipo de servicio	Hacer clic**Editar**para que aparezca el siguiente cuadro de diálogo para configurar

	el tipo de servicio.  **Tipo de servicio**-Para configurar el tipo de servicio manualmente, elija**Usuario definido**como el tipo de servicio. - **Usuario definido**–Configure los puertos de protocolo, origen y destino manualmente. - **Grupo y Objetos**–Seleccione grupos de servicios u objetos preconfigurados. **Protocolo -**Especifique los protocolos a los que se aplicará esta regla de filtrado. **Puerto de origen/destino –** - (=) – cualquier puerto que se encuentre dentro del rango especificado (!=) - – cualquier puerto que se encuentre fuera del rango especificado - (>) – un puerto cuyo número es mayor que el valor especificado - (<) – un puerto cuyo número es menor que el valor especificado **Grupo de servicio/objeto**-Utilice la lista desplegable para seleccionar los grupos de servicios u objetos deseados.
Fragmentos	Acción a tomar para paquetes fragmentados. Esta opción es válida para **Filtro de datos**reglas solamente. - **no me importa**–No se tomarán medidas con respecto a los paquetes fragmentados. - **sin fragmentar**–Aplicar la regla a los paquetes no fragmentados. - **Fragmentado**–Aplicar la regla a los paquetes fragmentados. - **Demasiado corto**–Aplique la regla solo a los paquetes que son demasiado cortos para contener un encabezado completo.
Filtrar	Acción a tomar cuando los paquetes coinciden con la regla. **Bloquear inmediatamente**–Los paquetes que coincidan con la regla se eliminarán inmediatamente. **Pase inmediatamente**–Los paquetes que coincidan con la regla se pasarán inmediatamente. **Bloquear si no hay más coincidencias**–Bloquee el paquete si esta es la última regla coincidente para este paquete en el filtro. **Pase si no hay más coincidencias**–Pase el paquete si esta es la última regla coincidente para este paquete en el filtro.
Rama a otro conjunto de filtros	Si el paquete coincide con la regla de filtrado y la acción Filtrar es **Bloquear si no hay más coincidencias**o**Pase si no hay más coincidencias**, tú

	puede especificar el siguiente conjunto de filtros que se aplicará, omitiendo así el resto de las reglas en el conjunto de filtros actual.
Control de sesiones	El número actual de sesiones se muestra antes de la barra inclinada, seguido del número máximo de sesiones simultáneas permitidas, que es configurable. El máximo predeterminado es 60000, que también es el límite superior del valor.
IP de enlace MAC	**Estricto**–Asegúrese de que tanto la dirección MAC como la dirección IP de los clientes de origen y/o destino. **no estricto**–No verifique la dirección IP cuando procese objetos IP que especifican direcciones MAC.
Calidad de servicio	Elija una de las reglas de QoS para aplicarla como regla de firewall. Para obtener información detallada sobre la configuración de QoS, consulte la sección relacionada más adelante.
Gestión de usuarios	Esta configuración solo está disponible cuando**Basado en reglas**se selecciona en **Gestión de usuarios>>Configuración general**. La regla de firewall predeterminada se aplicará al usuario o grupo de usuarios seleccionado. Consulte el capítulo sobre Gestión de usuarios para obtener más detalles sobre la función. - **Ninguno**: La gestión de usuarios no se aplica a la regla predeterminada. - **Objeto de usuario**: La regla predeterminada solo se aplica al usuario seleccionado. - [**Crear nuevo usuario**]: Seleccione esto para crear un nuevo usuario. - Grupo de usuarios: la regla predeterminada solo se aplica al grupo de usuarios seleccionado. - [**Crear nuevo grupo**]: Seleccione esto para crear un nuevo grupo de usuarios. - **TODO**: la regla predeterminada se aplica a todos los usuarios definidos. - **Crear nuevo usuario**o**Crear nuevo grupo**Aparecerá un elemento para que haga clic para crear uno nuevo si no existe un perfil de usuario o un perfil de grupo. **registro del sistema**-Seleccione para permitir que la administración de usuarios registre mensajes en Syslog.
Cumplimiento de la aplicación	Seleccione un perfil de Cumplimiento de aplicaciones para el bloqueo de aplicaciones o Ninguno para deshabilitar el Cumplimiento de aplicaciones para la regla predeterminada. Seleccionar**[Crear nuevo]**de la lista desplegable para crear un nuevo perfil. Consulte el capítulo sobre Cumplimiento de aplicaciones para obtener más detalles sobre la función. **registro del sistema**-Seleccione para permitir el cumplimiento de aplicaciones para registrar mensajes en Syslog.
Filtro de contenido de URL	Seleccione un perfil de filtro de contenido de URL para usar, o Ninguno para deshabilitar el filtro de contenido de URL para la regla predeterminada. Seleccionar **[Crear nuevo]**de la lista desplegable para crear un nuevo perfil. Consulte el capítulo sobre Filtro de contenido de URL para obtener más detalles sobre la función. **registro del sistema**-Seleccione para permitir que el filtro de contenido de URL registre mensajes en Syslog. La acción de registro se configura en el nivel de perfil en CSM>>Perfil de filtro de contenido de URL, Registro.
Filtro de contenido web	Seleccione un perfil de Filtro de contenido web para usar, o Ninguno para deshabilitar el Filtro de contenido web para la regla predeterminada. Seleccionar **[Crear nuevo]**de la lista desplegable para crear un nuevo perfil. **registro del sistema**-Seleccione para permitir que Web Content Filter registre mensajes en Syslog. La acción de registro se configura en el nivel de perfil en

	la sección Tabla de perfil de filtro de contenido web en CSM>>Perfil de filtro de contenido web, Registro.
Filtro DNS	Seleccione el perfil de filtro DNS que se usará o Ninguno para deshabilitar el filtro DNS para la regla predeterminada. Seleccionar**[Crear nuevo]**de la lista desplegable para crear un nuevo perfil. **registro del sistema**-Seleccione para permitir que el filtro DNS registre mensajes en Syslog. La acción de registro se configura en el nivel de perfil en la sección Tabla de perfil de filtro DNS en CSM>>Perfil de filtro DNS, SysLog.
Configuración avanzada	Hacer clic**Editar**para abrir la ventana de configuración de Configuración avanzada. Sin embargo, se recomienda utilizar la configuración predeterminada.  **Página de código**–Establece la página de códigos utilizada por el filtro de contenido de URL para hacer coincidir las URL con las palabras clave en los perfiles. La elección de la página de códigos adecuada puede aumentar la precisión del filtro de contenido de URL. El valor predeterminado es ANSI 1252 Latin I. Si la configuración es Ninguno, no se realizará la decodificación de URL. Si no está seguro de qué página de códigos usar, inicie la aplicación Syslog y la página de códigos recomendada se mostrará en la pestaña Información de la página de códigos en el cuadro de diálogo Configuración. **Tamaño de ventana**–Establece el tamaño de la ventana TCP como se describe en RFC 1323. Los valores válidos son de 0 a 65535. Cuanto más

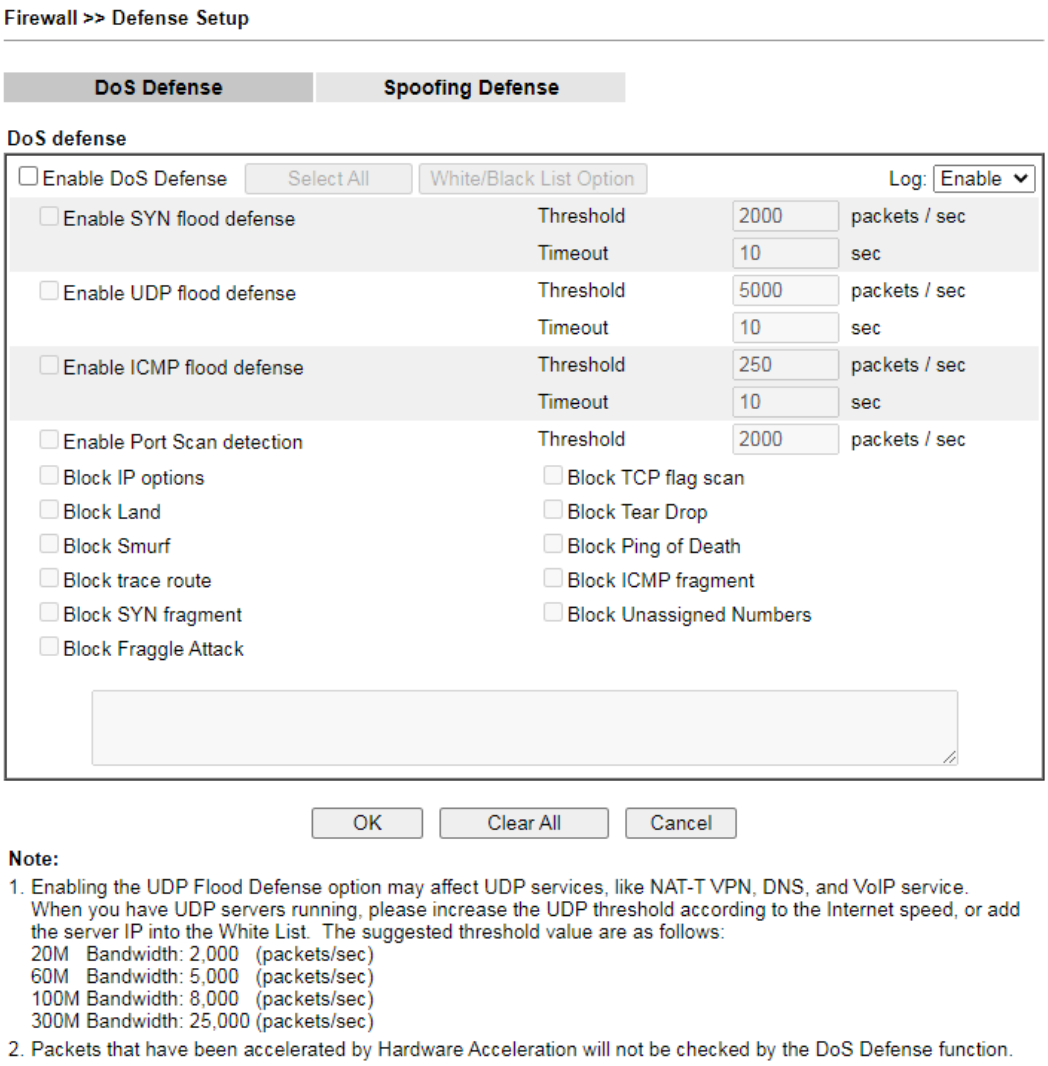
	es el valor, mejor será el rendimiento. Sin embargo, si la red no es estable, el valor pequeño será apropiado. **Hora de término de la sesión**–Establece el tiempo de espera que las sesiones pueden estar inactivas antes de que se eliminen del sistema. **Banner DrayTek**–Seleccione para mostrar la siguiente pantalla para las páginas web que están bloqueadas por el Firewall. La configuración por defecto está activada. **Estricto control de seguridad** **Cumplimiento de la aplicación**–Si se selecciona esta opción, cuando el enrutador no pueda identificar la aplicación que generó el tráfico saliente debido a los recursos limitados del sistema, la sesión se bloqueará; si no se selecciona esta opción, se permitirá la sesión.

3. Cuando termine la configuración, haga clic en**DE ACUERDO**para guardar y salir de esta página.

Como una sub-funcionalidad de IP Filter/Firewall, hay 15 tipos de funciones de detección/defensa en el**Defensa DoS**configuración. La funcionalidad DoS Defense está deshabilitada por defecto.

VI-1-3-1 Defensa DoS

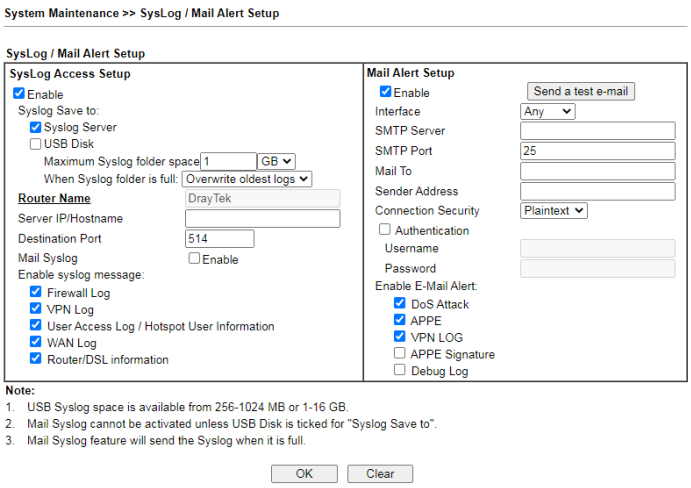
Para configurar DoS Defense, seleccione DoS Defense en el elemento de menú Firewall en la barra de menú de la interfaz de usuario web.

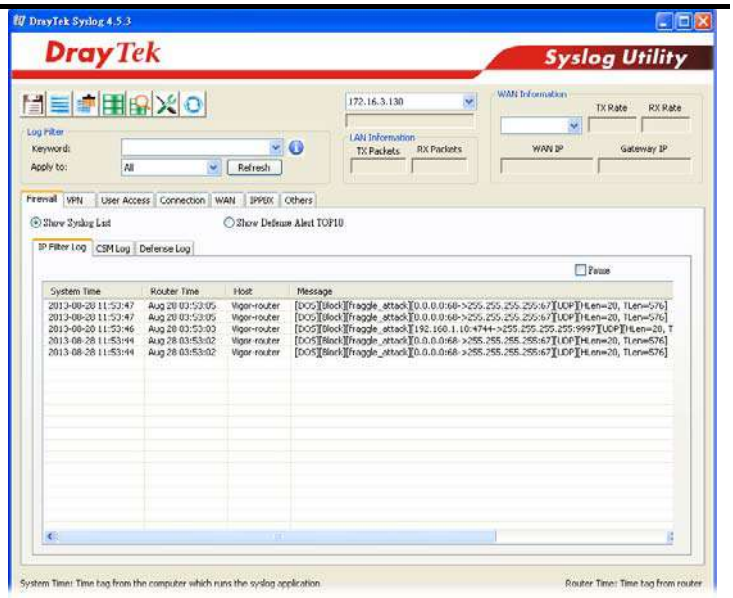


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar defensa DOS	Seleccione para habilitar DoS Defense. **Seleccionar todo -**Haga clic para seleccionar todas las opciones de DoS Defense. **Opción de lista blanca/negra**–Configure la lista blanca/negra de direcciones IPv4/IPv6.
Habilitar la defensa contra inundaciones SYN	Seleccione para habilitar la defensa contra inundaciones SYN. Cuando la tasa de llegada de los paquetes SYN supera el valor del Umbral, el enrutador comenzará a descartar aleatoriamente los paquetes TCP SYN durante un período de tiempo definido en Tiempo de espera. Esto es para evitar que los paquetes TCP SYN agoten los recursos del enrutador.

	Los valores predeterminados de umbral y tiempo de espera son 2000 paquetes por segundo y 10 segundos, respectivamente.
Habilitar la defensa contra inundaciones UDP	Seleccione para habilitar la defensa contra inundaciones UDP. Cuando la tasa de llegada de los paquetes UDP supera el valor del Umbral, el enrutador comenzará a descartar aleatoriamente los paquetes TCP SYN durante un período de tiempo definido en Tiempo de espera. Los valores predeterminados de umbral y tiempo de espera son 2000 paquetes por segundo y 10 segundos, respectivamente.
Habilitar la defensa contra inundaciones ICMP	Seleccione para habilitar la defensa contra inundaciones ICMP. Cuando la tasa de llegada de los paquetes ICMP supera el valor del Umbral, el enrutador comenzará a descartar aleatoriamente los paquetes TCP SYN durante un período de tiempo definido en Tiempo de espera. Los valores predeterminados de umbral y tiempo de espera son 250 paquetes por segundo y 10 segundos, respectivamente.
Habilitar exploración de puertos detección	Seleccione para habilitar la detección de exploración de puertos. Los escaneos de puertos atacan su red enviando paquetes a una variedad de puertos en un intento de encontrar servicios que respondan. Cuando la detección de exploración de puertos está habilitada, el enrutador envía mensajes de advertencia cuando detecta actividades de exploración de puertos que superan la tasa de umbral. El umbral predeterminado es de 2000 paquetes por segundo.
Bloquear opciones de IP	Seleccione para habilitar las opciones de Bloquear IP. El enrutador Vigor ignorará los paquetes IP con el campo de opción IP establecido en el encabezado del datagrama. Las opciones de IP rara vez se usan y los atacantes podrían abusar de ellas, ya que contienen información sobre la red privada que de otro modo no estaría disponible para la red externa, como seguridad, parámetros de TCC (grupo cerrado de usuarios), una serie de direcciones de Internet, mensajes de enrutamiento, etc. que los espías externos pueden usar para descubrir detalles sobre la red privada.
Bloque de tierra	Seleccione para bloquear ataques LAND. Los ataques LAND ocurren cuando un atacante envía paquetes SYN falsificados con direcciones de origen y de destino configuradas en las del sistema objetivo, lo que hace que el objetivo se responda a sí mismo continuamente.
Pitufo bloque	Seleccione para bloquear los ataques de Smurf. El enrutador ignorará cualquier solicitud de eco ICMP de transmisión.
Bloquear ruta de rastreo	Seleccione para bloquear rutas de seguimiento. El enrutador no reenviará paquetes de ruta de rastreo.
Bloquear fragmento SYN	Seleccione Bloquear fragmentos de paquetes SYN. El enrutador eliminará cualquier paquete que tenga configurados los bits SYN y más fragmentos.
Ataque de bloques Fraggle	Seleccione para bloquear ataques Fraggle. Los paquetes UDP de difusión recibidos de Internet están bloqueados. La activación de esta función podría bloquear algunos paquetes legítimos. Dado que todos los paquetes UDP de difusión que provienen de Internet están bloqueados, los paquetes RIP de Internet también podrían descartarse.
Bloquear escaneo de bandera TCP	Seleccione para bloquear escaneos de bandera TCP. Se eliminarán los paquetes TCP con configuraciones de banderas anormales. Las actividades de escaneo de bandera TCP que están bloqueadas incluyen escaneo sin bandera, escaneo FIN sin ACK, escaneo SYN FIN, escaneo de Navidad y escaneo de Navidad completo.
Gota de lágrima de bloque	Seleccione para bloquear los ataques de lágrima. Algunos clientes pueden fallar cuando reciben datagramas ICMP (paquetes) que exceden

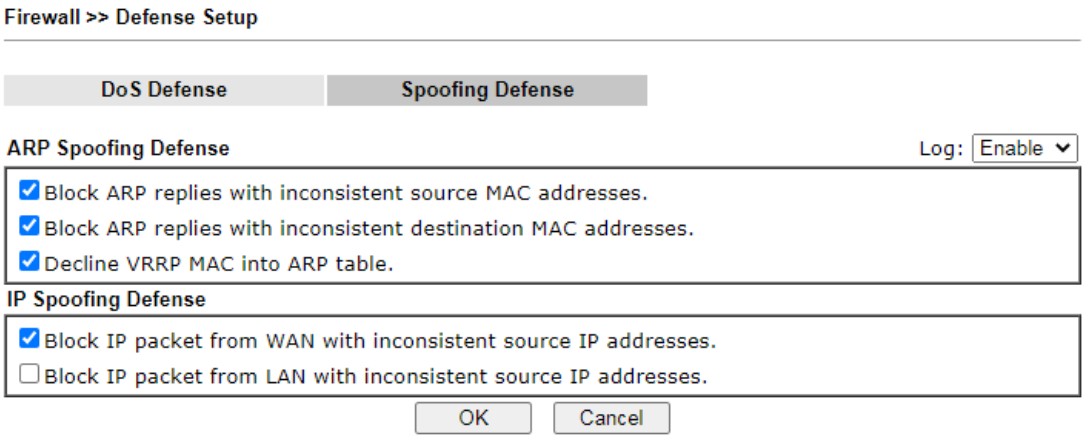
	la longitud máxima. El enrutador descarta cualquier paquete ICMP fragmentado que tenga una longitud superior a 1024 octetos.
Bloquear ping de la muerte	Seleccione para bloquear el ping de la muerte, donde los paquetes de ping fragmentados se envían a los hosts de destino para que esos hosts puedan bloquearse al volver a ensamblar los paquetes de ping mal formados.
Bloquear fragmento ICMP	Seleccione para bloquear fragmentos ICMP. Los paquetes ICMP con el conjunto de bits de más fragmentos se eliminan.
Bloquear números no asignados	Seleccione Bloquear números de protocolo no asignados y el enrutador bloqueará los paquetes que tengan números de protocolo no asignados. El paquete IP individual tiene un campo de protocolo en el encabezado del datagrama para indicar el tipo de protocolo que se ejecuta en la capa superior. Sin embargo, los tipos de protocolo superiores a 100 están reservados y sin definir en este momento. Por lo tanto, el enrutador debe tener la capacidad de detectar y rechazar este tipo de paquetes.
Mensajes de advertencia	Proporcionamos la función Syslog para que el usuario recupere el mensaje del enrutador Vigor. El usuario, como servidor Syslog, recibirá el envío del informe desde el enrutador Vigor, que es un cliente Syslog. Todos los mensajes de advertencia relacionados con**Defensa DoS**se enviará al usuario y el usuario puede revisarlo a través del demonio Syslog. Busque la palabra clave**DoS**en el mensaje, seguido de un nombre para indicar qué tipo de ataques se detectan. 



Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

Defensa de suplantación de identidad VI-1-3-2

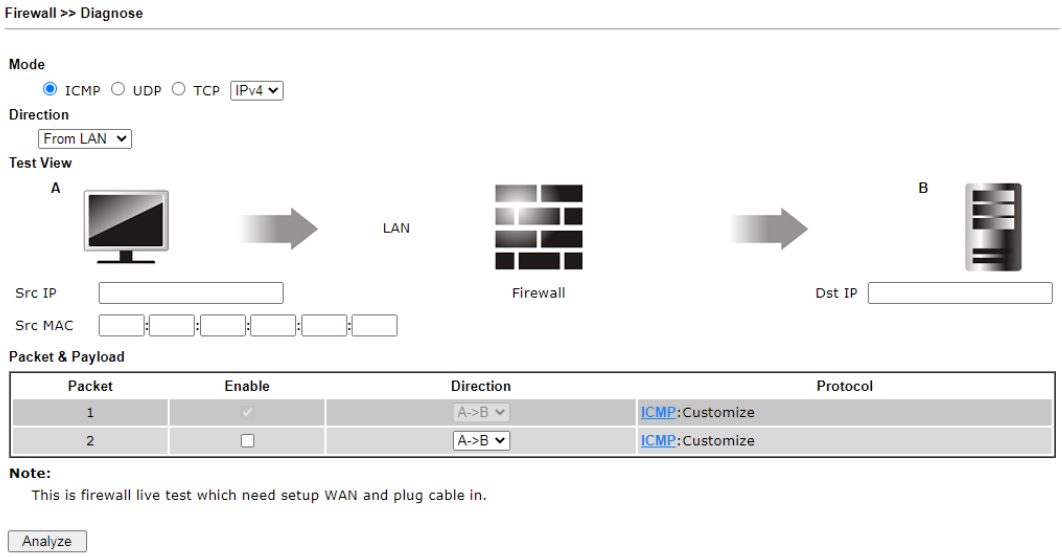
Haga clic en el**Defensa contra la suplantación de identidad**pestaña para abrir la página de configuración.



VI-1-4 Diagnosticar

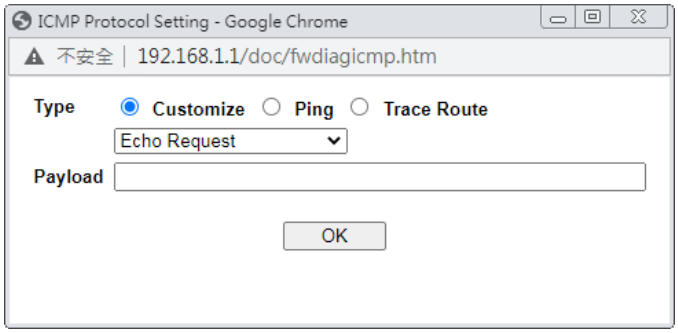
El propósito de esta función es probar cuando el enrutador recibe un paquete entrante, qué regla de firewall se aplicará a ese paquete. El resultado de la prueba, incluido el perfil de la regla del cortafuegos, la traducción de la dirección IP en la transmisión de paquetes, el estado de las funciones del cortafuegos, etc., también se mostrará en esta página.

Información	El resultado obtenido al usar Diagnosticar se ofrece para la depuración de RD. Será diferente según el estado actual, como la conexión de red, la configuración de LAN/WAN, etc.

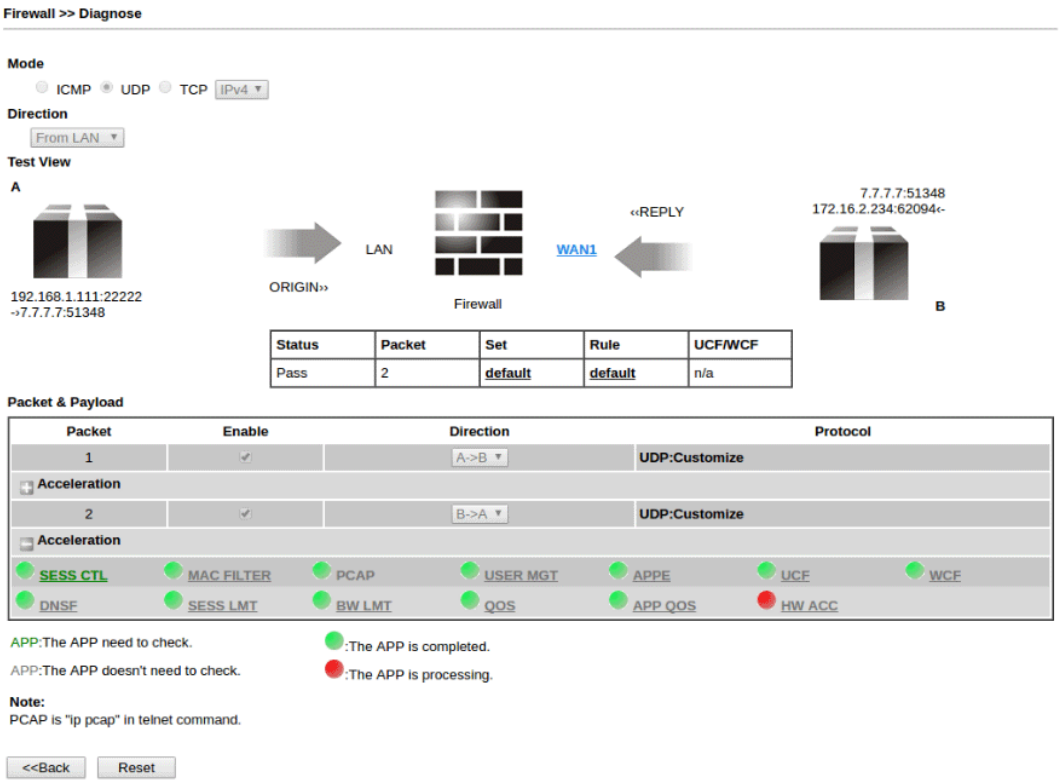


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Modo	Para tener una prueba de regla de firewall, especifique el tipo de servicio (ICMP, UDP, TCP) del paquete y el tipo de dirección IP (IPv4/IPv6).
Dirección	Establezca la forma (desde WAN o desde LAN) que el enrutador Vigor recibe el primer paquete para la prueba. Manera diferente significa que el cortafuegos procesará la conexión iniciada desde LAN o desde WAN.
Vista de prueba	Esta es una página de visualización dinámica. De acuerdo con la dirección especificada, la vista de prueba mostrará la figura para guiarlo al escribir la dirección IP, el número de puerto y la dirección MAC. Más tarde, después de hacer clic en el botón Analizar, la información para el perfil de la regla del firewall y la traducción de la dirección se mostrarán en esta página.
IP de origen	Introduzca la dirección IPv4/IPv6 del origen del paquete.
Puerto origen	Introduzca el número de puerto de origen del paquete.
Fuente MAC	Ingrese la dirección MAC de la fuente del paquete.
DST IP	Introduzca la dirección IPv4/IPv6 del destino del paquete.

puerto de horario de verano	Introduzca el número de puerto de destino del paquete.
Paquete y carga útil	En el diagnóstico de firewall, dos paquetes pertenecen a una conexión. En general, dos paquetes son suficientes para que el enrutador Vigor realice esta prueba. **Permitir**–Marque la casilla para enviar el paquete de prueba. **Dirección**–El primer paquete de la prueba de cortafuegos seguirá la dirección especificada anteriormente. Sin embargo, la dirección del segundo paquete puede ser diferente. Simplemente elija la dirección (de la computadora A a la B o de la B a la A) para el segundo paquete. **Protocolo**–Muestra el modo seleccionado arriba y el estado. Si es necesario, haga clic en el enlace de modo para configurar la configuración avanzada. El tipo de servicio común (Personalizar, Ping, Rastrear ruta/Personalizar, DNS, Rastrear ruta/Personalizar, Http(GET) relacionado con ese modo (ICMP/UDP/TCP) se mostrará en el siguiente cuadro de diálogo.  - **Tipo**–Elija Personalizar, Ping, Rastrear ruta/ Personalizar, DNS, Rastrear ruta/Personalizar, Http (GET). - **Carga útil**–Está disponible cuando se selecciona Personalizar. Simplemente escriba 16 caracteres HEX que representan cierto paquete (por ejemplo, paquete DNS) si desea configurar los datos transferidos con el protocolo (ICMP/UDP/TCP) que es diferente a la configuración de Tipo.
Analizar	Ejecute la prueba y analice el resultado.

La siguiente figura muestra el resultado de la prueba después de hacer clic en**Analizar**. El estado de procesamiento de las funciones (Filtro MAC, QoS, Gestión de usuarios, etc.) relacionadas con el cortafuegos se mostrará mediante un LED verde o rojo.



VI-2 Gestión de seguridad central (CSM)

Content Security Management (CSM) permite al administrador de la red restringir el tráfico de Internet según el tipo de contenido, lo que garantiza el uso adecuado de los recursos de la red y también reduce la probabilidad de amenazas de contenido de red malicioso.

Filtro de cumplimiento de aplicaciones

El filtro de cumplimiento de aplicaciones se puede utilizar para evitar que los usuarios utilicen aplicaciones de red indeseables o inapropiadas, como el chat en línea y los programas de igual a igual. El filtro funciona detectando y bloqueando el tráfico de red de las aplicaciones mediante patrones de tráfico.

Filtro de contenido de URL

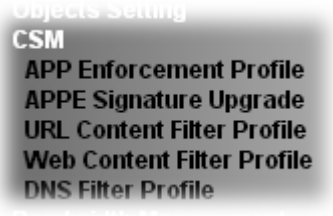
El filtro de contenido de URL escanea cadenas de URL en solicitudes HTTP en busca de palabras clave predefinidas para restringir las actividades de navegación.

Filtro de contenido web

También se puede evitar que los usuarios naveguen por ciertos tipos de sitios web utilizando el Filtro de contenido web. Este filtro clasifica los nombres de dominio de sitios web en diferentes categorías, que se pueden bloquear de forma selectiva.

Primero se deben crear perfiles de filtro antes de poder habilitar estos filtros CSM. Una vez que se han configurado los perfiles, se pueden aplicar a la Regla predeterminada en Cortafuegos>>Configuración general o Reglas de filtrado en Conjuntos de filtros en Cortafuegos>>Configuración de filtros.

Información	La prioridad del filtro de contenido de URL es mayor que la del filtro de contenido web.



VI-2-1 Perfil de aplicación de la aplicación

Se pueden configurar hasta 32 perfiles de políticas para el cumplimiento de aplicaciones.

CSM >> APP Enforcement Profile

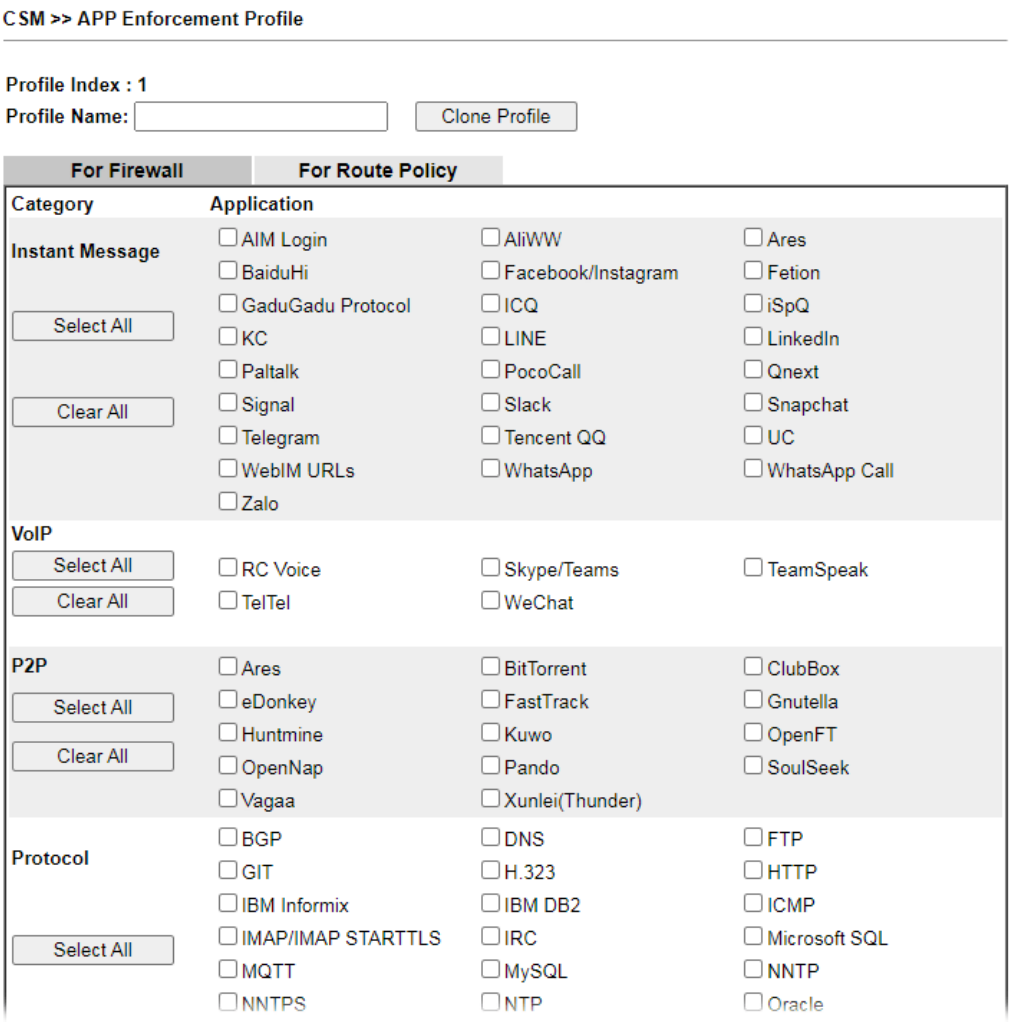
APP Enforcement Profile Table: | Set to Factory Default |

Profile	Name	Profile	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Establecer como predeterminado de fábrica	Borre todas las configuraciones de perfil.
Perfil	Índice del perfil. Haga clic para abrir la página de configuración del perfil.
Nombre	Nombre del perfil.

Para configurar un perfil, haga clic en su número de perfil y aparecerá la siguiente página de configuración de perfil:



Los ajustes disponibles se explican a continuación:

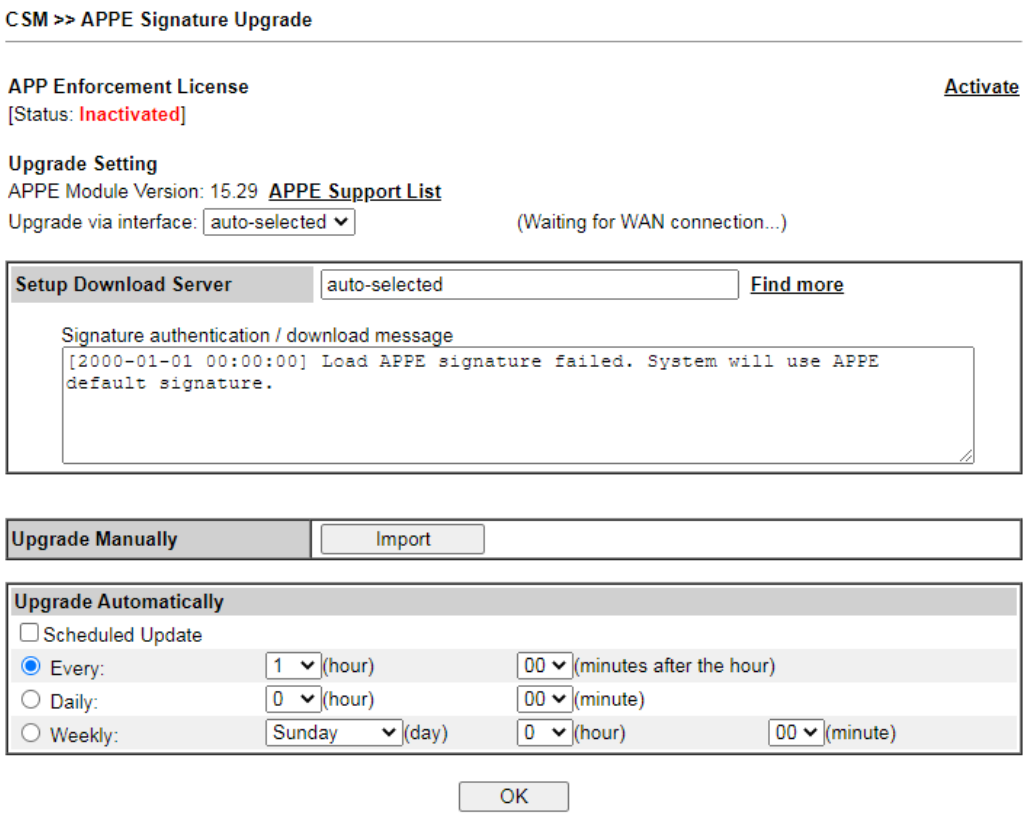
Artículo	Descripción
Nombre de perfil	Nombre que identifica a este perfil. La longitud máxima es de 15 caracteres.
Categoría	Las aplicaciones se clasifican en varias categorías. Cada categoría contiene varias aplicaciones para bloquear.
Perfil de clonación	Haga clic en él para clonar la configuración configurada por un perfil existente.
Seleccionar todo	Haga clic para seleccionar todos los elementos de esta página.
Limpiar todo	Haga clic para anular la selección de todos los elementos seleccionados.
☐	Seleccione esta casilla de verificación para bloquear la aplicación.

Para guardar los cambios en la página, haga clic en**O**K. Para descartar los cambios, haga clic en**Cancelar**.

VI-2-2 Actualización de la firma APPE

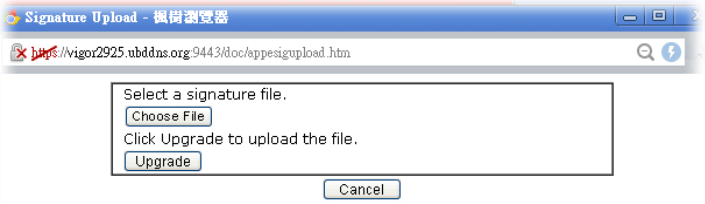
La función Perfil de cumplimiento de aplicaciones identifica las aplicaciones haciendo coincidir su tráfico de red con las firmas. DrayTek lanza periódicamente actualizaciones de firma APPE para garantizar que se puedan detectar nuevas aplicaciones o nuevas versiones.

Las comprobaciones de actualización se pueden realizar de forma manual o automática.



Los ajustes disponibles se explican a continuación:

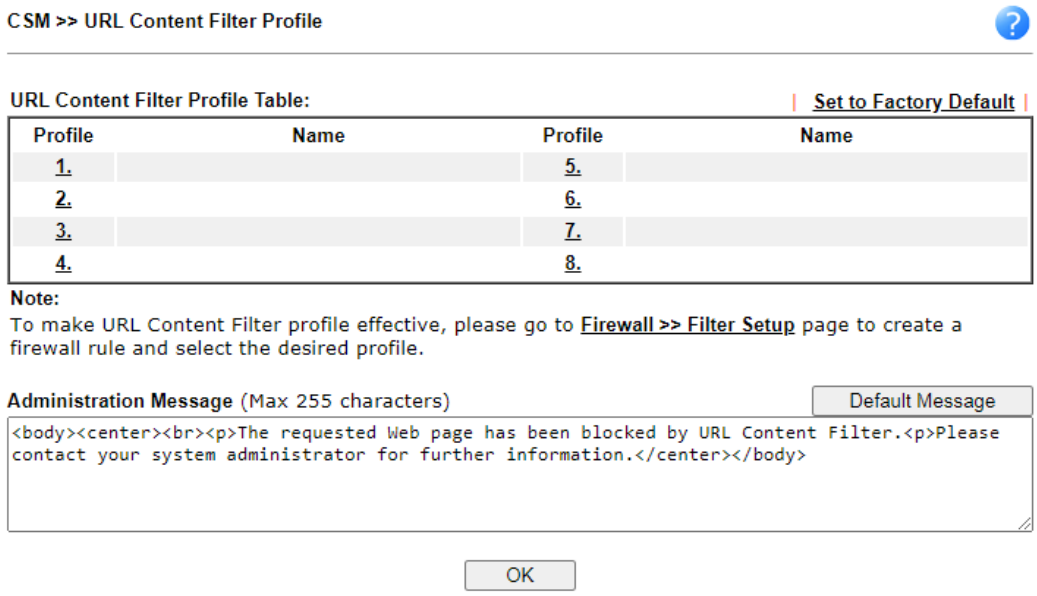
Artículo	Descripción
Licencia de aplicación de la aplicación	**Estado -**Muestra el estado actual de la licencia.
Configuración de actualización	**Versión del módulo APPE**–Muestra la versión actual de la firma APPE. **Nueva versión de Internet**–El**Descargar**El botón está habilitado solo cuando hay una versión más nueva de la firma APPE que la presente en el enrutador. Después de hacer clic en el botón Descargar, aparecerá un cuadro de diálogo que muestra la información de lanzamiento de la nueva versión. Hacer clic**DE ACUERDO**en el cuadro de diálogo para continuar con la descarga. **Actualizar a través de la interfaz**–Seleccione una interfaz WAN para descargar la nueva firma APPE.
Configurar servidor de descarga	Especifique un servidor de descarga escribiendo su URL del servidor. Haga clic en elEncuentra más para obtener una lista de servidores de descarga. Cuando se usa el valor predeterminado seleccionado automáticamente, el servidor se determina automáticamente al buscar la ubicación geográfica de la dirección IP WAN. **Autenticación de firma/mensaje de descarga**–Muestra mensajes de estado de descarga.

Actualizar manualmente	Utilice esta funcionalidad si desea actualizar utilizando un archivo de firma descargado previamente. **Importar**–Al hacer clic en el botón, aparece la página siguiente.  Hacer clic**Elija el archivo**para seleccionar el archivo de firma. Hacer clic**Mejora** para iniciar el proceso de actualización.
Actualizar automáticamente	**Actualización programada -**Seleccione para habilitar la verificación periódica automática de actualizaciones de firmas.

Hacer clic**DE ACUERDO**para guardar los cambios en la página.

VI-2-3 Perfil de filtro de contenido de URL

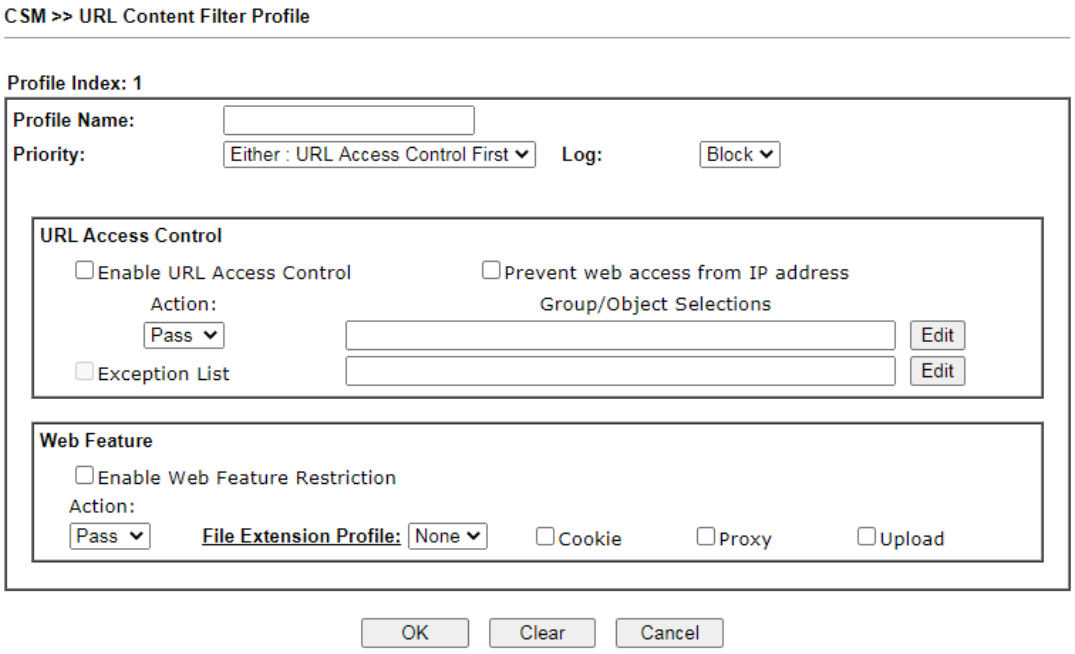
Para configurar perfiles de filtro de contenido de URL, haga clic en**CSM**en la barra del menú principal y luego haga clic en**Perfil de filtro de contenido de URL**para abrir la página de configuración del perfil.



Cada elemento se explica de la siguiente manera:

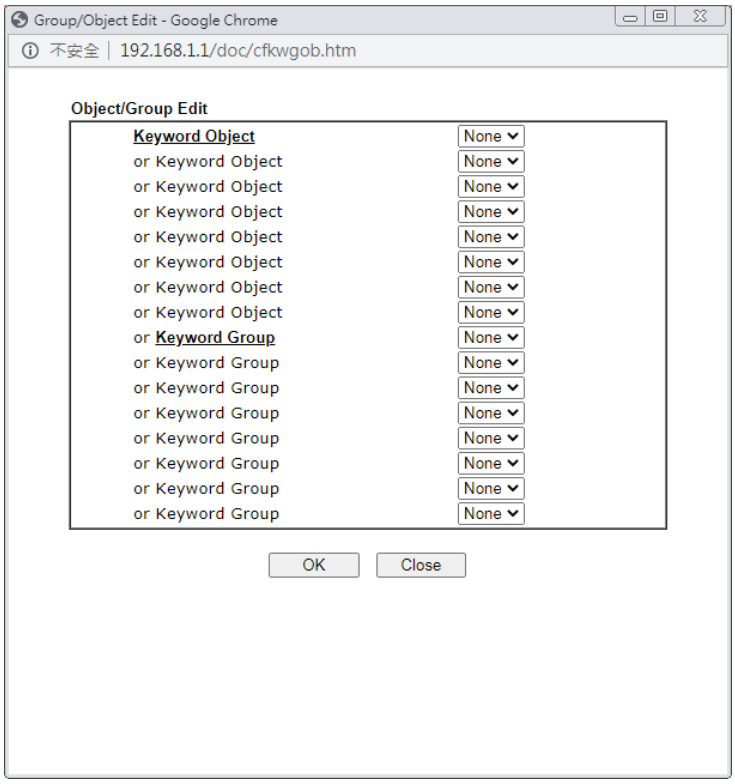
Artículo	Descripción
Establecer como predeterminado de fábrica	Borre todas las configuraciones de perfil.
Perfil	Número de índice del perfil.
Nombre	Nombre que identifica al perfil.
Mensaje de administración	El mensaje que se muestra en el navegador cuando se bloquea el acceso a una URL. Se puede ingresar un mensaje personalizado con formato HTML en el cuadro de texto. **Mensaje predeterminado**-Haga clic para restablecer el mensaje de administración a los valores predeterminados de fábrica.

Para configurar un perfil, haga clic en el número de perfil en la columna Índice para abrir la página de configuración.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre de perfil	Nombre que identifica el perfil de filtro de contenido de URL. La longitud máxima del nombre del perfil es de 15 caracteres.
Prioridad	El orden de evaluación de URL Access Control y Web Feature a continuación: **Ambos: Pasar**–El enrutador permitirá el acceso solo a los recursos web que coincidan con las condiciones especificadas tanto en el Control de acceso URL como en la Función web. La configuración de Acción tanto del Control de acceso de URL como de la Función web se deshabilitará y los valores se establecerán en Aprobado. **Ambos: Bloquear**–El enrutador bloqueará el acceso a los recursos web que coincidan con las condiciones especificadas tanto en el Control de acceso URL como en la Función web. La configuración de Acción tanto del Control de acceso de URL como de la Función web se desactivará y los valores se establecerán en Bloquear. **O bien: control de acceso URL primero**–El enrutador bloqueará o permitirá el acceso a los recursos web que coincidan con las condiciones especificadas en Control de acceso URL o Función web. Primero se aplica el control de acceso URL, seguido de la característica web. **Ya sea: característica web primero**–El enrutador bloqueará o permitirá el acceso a los recursos web que coincidan con las condiciones especificadas en Control de acceso URL o Función web. La característica web se aplica primero, seguida del control de acceso de URL.
Registro	**Ninguno**–No se creará ningún archivo de registro para este perfil. **Aprobar**–Solo los intentos de acceso aprobados se registrarán en Syslog. **Bloquear**–Solo los intentos de acceso bloqueados se registrarán en Syslog. **Todo**–Tanto los intentos de acceso aprobados como los bloqueados se registrarán en Syslog.
Control de acceso a URL	**Habilitar control de acceso a URL**-Seleccione para activar el acceso a la URL

	Control. **Impedir el acceso a la web desde la dirección IP**-Se bloquearán las URL que contengan direcciones IP (p. ej., 192.168.1.1). Solo se permitirán URL con direcciones de dominio (p. ej., www.draytek.com). Esto es para evitar que los usuarios eludan el control de acceso de URL. **Acción**–Esta configuración está habilitada solo cuando la Prioridad está configurada en Ya sea: Control de acceso URL primero o Cualquiera: Característica web primero. - **Aprobar -**Permite el acceso a páginas web con URL que contienen palabras clave que se encuentran en los grupos u objetos de palabras clave seleccionados. El acceso a otras URL está bloqueado. - **Bloquear -**Bloquea el acceso a páginas web con direcciones URL que contienen palabras clave que se encuentran en los grupos u objetos de palabras clave seleccionados. Se permite el acceso a otras URL. **Lista de excepciones**–Especifique los perfiles de objeto como la lista de excepción que se procesará de manera opuesta a la acción seleccionada anteriormente. **Selecciones de grupo/objeto**–Muestra los grupos de palabras clave y/u objetos seleccionados para este perfil de filtro de contenido de URL. Para agregar o quitar grupos de palabras clave y objetos a la selección, haga clic en el**Editar**botón para abrir la siguiente pantalla.  Se pueden seleccionar hasta 8 objetos de palabras clave y 8 grupos de palabras clave. Para agregar, eliminar o modificar grupos u objetos, haga clic en los hipervínculos Objeto de palabra clave o Grupo de palabras clave para que aparezca el**Configuración de objetos >> Objeto de palabra clave**o**Configuración de objetos > > Grupo de palabras clave**paginas
Característica web	**Habilitar función de restricción web -**Marque para habilitar la restricción de funciones web. **Acción -**Esta configuración está habilitada solo cuando Prioridad está configurada en **O bien: control de acceso URL primero**o**O bien: función web**

	Primero. - **Aprobar**–Permite el acceso a páginas web con URL que contienen palabras clave que se encuentran en los grupos u objetos de palabras clave seleccionados. El acceso a otras URL está bloqueado. - **Bloquear**–Bloquea el acceso a páginas web con direcciones URL que contienen palabras clave que se encuentran en los grupos u objetos de palabras clave seleccionados. Se permite el acceso a otras URL. **Perfil de extensión de archivo –**Elija uno de los perfiles que configuró en**Configuración de objetos>> Objetos de extensión de archivo** previamente para pasar o bloquear la descarga del archivo. **Galleta**-Seleccione para bloquear las cookies de los sitios web de Internet. **Apoderado**-Seleccione para bloquear servidores proxy web que retransmiten tráfico HTTP. **Subir**–Seleccione para bloquear cargas HTTP desde la LAN a Internet.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para borrar todas las configuraciones, haga clic en**Claro**.

VI-2-4 Perfil de filtro de contenido web

El servicio WCF de prueba se puede activar usando el**Asistente de activación de servicios**.

Si desea continuar usando WCF más allá del período de prueba, puede obtener una suscripción WCF completa comunicándose con su distribuidor o socio de canal DrayTek local. Las suscripciones de WCF se pueden activar usando el**Activar**enlace en**CSM >> Perfil de filtro de contenido web**(descrito en esta sección) o **Mantenimiento del sistema**.

Desde el menú principal, haga clic en**CSM**, seguido por**Perfil de filtro de contenido web**para cargar la página de configuración del perfil.

Información 1	El filtro de contenido web (WCF) no es un servicio integrado del enrutador Vigor, sino un servicio impulsado por Commtouch. Si desea utilizar dicho servicio (edición de prueba o formal), primero debe realizar el procedimiento de activación. Para el servicio de edición formal, póngase en contacto con su distribuidor/vendedor para obtener información detallada.
Información 2	Cyren fusiona Commtouch y los servicios de GlobalView continuarán brindando potentes soluciones de seguridad de la información basadas en la nube. Referirse a: http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239025151.html

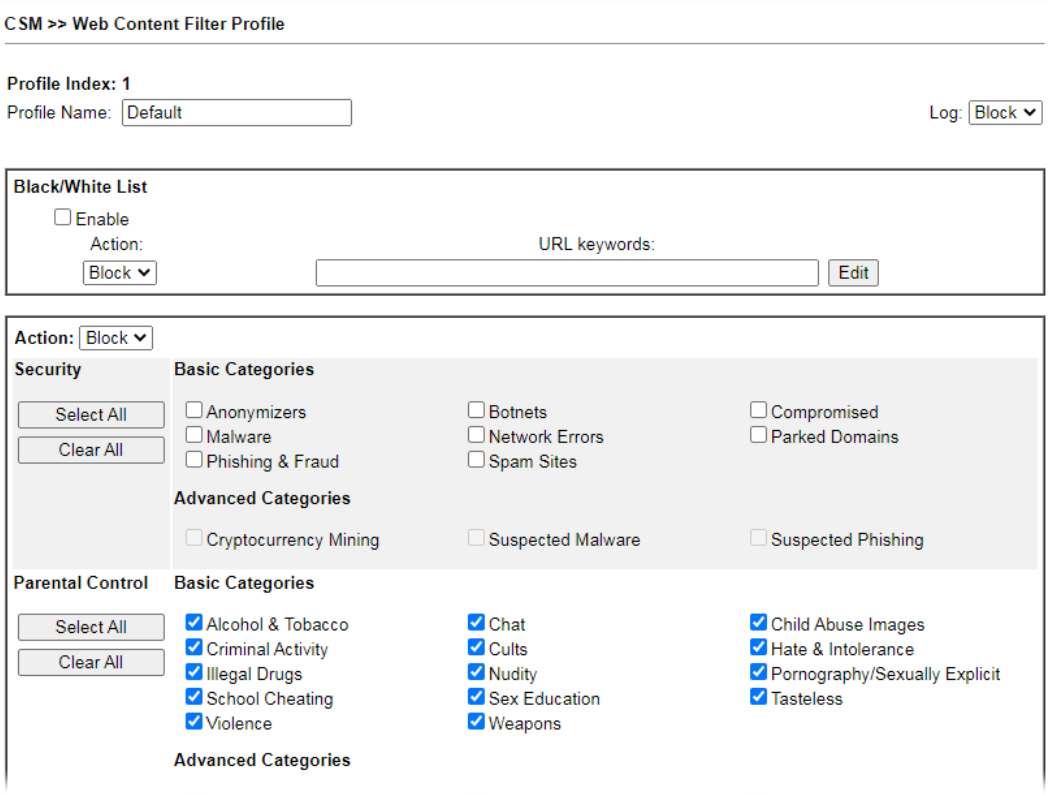
Los ajustes disponibles se explican a continuación:

Artículo	Descripción

Activar	Haga clic para visitar el sitio web MyVigor para activar el servicio WCF. Deberá iniciar sesión en su cuenta MyVigor para continuar con el proceso de activación. Si aún no tiene una cuenta MyVigor, puede crear una en este momento.
Configurar servidor de consultas	Especifique un servidor de consultas WCF escribiendo la dirección del servidor. Haga clic en elEncuentra más para obtener una lista de servidores de consultas. Cuando se usa el valor predeterminado seleccionado automáticamente, el servidor se determina automáticamente al buscar la ubicación geográfica de la dirección IP WAN. Se recomienda utilizar la configuración predeterminada seleccionada automáticamente.
Configurar servidor de prueba	Especifique un servidor de prueba WCF escribiendo la dirección del servidor. Haga clic en elEncuentra más para obtener una lista de servidores de prueba. Cuando se usa el valor predeterminado seleccionado automáticamente, el servidor se determina automáticamente al buscar la ubicación geográfica de la dirección IP WAN. Se recomienda utilizar la configuración predeterminada seleccionada automáticamente.
Cache	**Ninguno**–El enrutador verifica cada URL HTTP solicitada comunicándose con el servidor WCF en Internet. Este modo proporciona la coincidencia de URL más precisa, pero tiene el rendimiento más bajo. **L1**–El enrutador almacena en caché las URL HTTP que se han verificado con el servidor WCF. Las direcciones URL se buscarán en la memoria caché L1 antes de llegar al servidor WCF. Cuando la memoria caché esté llena, la entrada más antigua se eliminará para acomodar las nuevas URL. **L2**–Una vez que se ha verificado una URL y se ha encontrado que pasa WCF, las direcciones IP de origen y destino se almacenan en caché durante aproximadamente 1 segundo en la memoria caché L2. Esto es para permitir que se cargue una página web sin verificar más las mismas URL con la caché L1 o el servidor WCF. **Caché L1+L2**–El enrutador utilizará cachés L1 y L2.
Establecer como predeterminado de fábrica	Borre todas las configuraciones de perfil.
Perfil	Número de índice del perfil.
Nombre	Nombre que identifica al perfil.
Mensaje de administración	El mensaje que se muestra en el navegador cuando se bloquea el acceso a un sitio web. Se puede ingresar un mensaje personalizado con formato HTML en el cuadro de texto. Puede incrustar las siguientes variables en el mensaje: %SIP%: la dirección IP de origen que intentó el acceso HTTP. %DIP%: la dirección IP de destino a la que se intentó acceder. %URL%: la URL del sitio web de destino. %CL%: la categoría a la que pertenece la URL. %RNAME%: el nombre del enrutador. **Mensaje predeterminado**-Haga clic para restablecer el mensaje de administración a los valores predeterminados de fábrica.

Se pueden configurar hasta 8 perfiles WCF. Para configurar un perfil, haga clic en su número de perfil para abrir su página de configuración. La configuración del perfil de filtro es específica de los proveedores de WCF. si ya

tiene una suscripción WCF activa, la activación de una suscripción WCF a un proveedor diferente de su proveedor actual borrará todas las configuraciones de perfil existentes.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre de perfil	Nombre que identifica el perfil de WCF. La longitud máxima del nombre del perfil es de 15 caracteres.
Registro	**Aprobar**–Solo los intentos de acceso aprobados se registrarán en Syslog. **Bloquear**–Solo los intentos de acceso bloqueados se registrarán en Syslog. **Todo**–Tanto los intentos de acceso aprobados como los bloqueados se registrarán en Syslog.
Lista blanca/negra	Los objetos y grupos de palabras clave se pueden aplicar a la dirección URL para anular el filtrado de categorías de WCF. **Permitir -**Seleccione para habilitar la lista negra o la lista blanca. **Acción**-Acción a realizar cuando una URL coincide con selecciones de objetos y grupos de palabras clave. - **Aprobar**–Permitir el acceso a la URL. - **Bloquear**–No permitir el acceso a la URL. **Palabras clave de URL –**Muestra el grupo de palabras clave y los objetos seleccionados. Haga clic en el**Editar**botón para modificar las selecciones de palabras clave.
Grupos y Categorías	Seleccione las categorías que se incluirán en el filtro. **Acción**-Acción a realizar cuando una URL coincide con selecciones de objetos y grupos de palabras clave. - **Aprobar**–permitir el acceso a la URL. - **Bloquear**–no permitir el acceso a la URL. **Seleccionar todo -**Haga clic para seleccionar todas las categorías dentro del grupo.

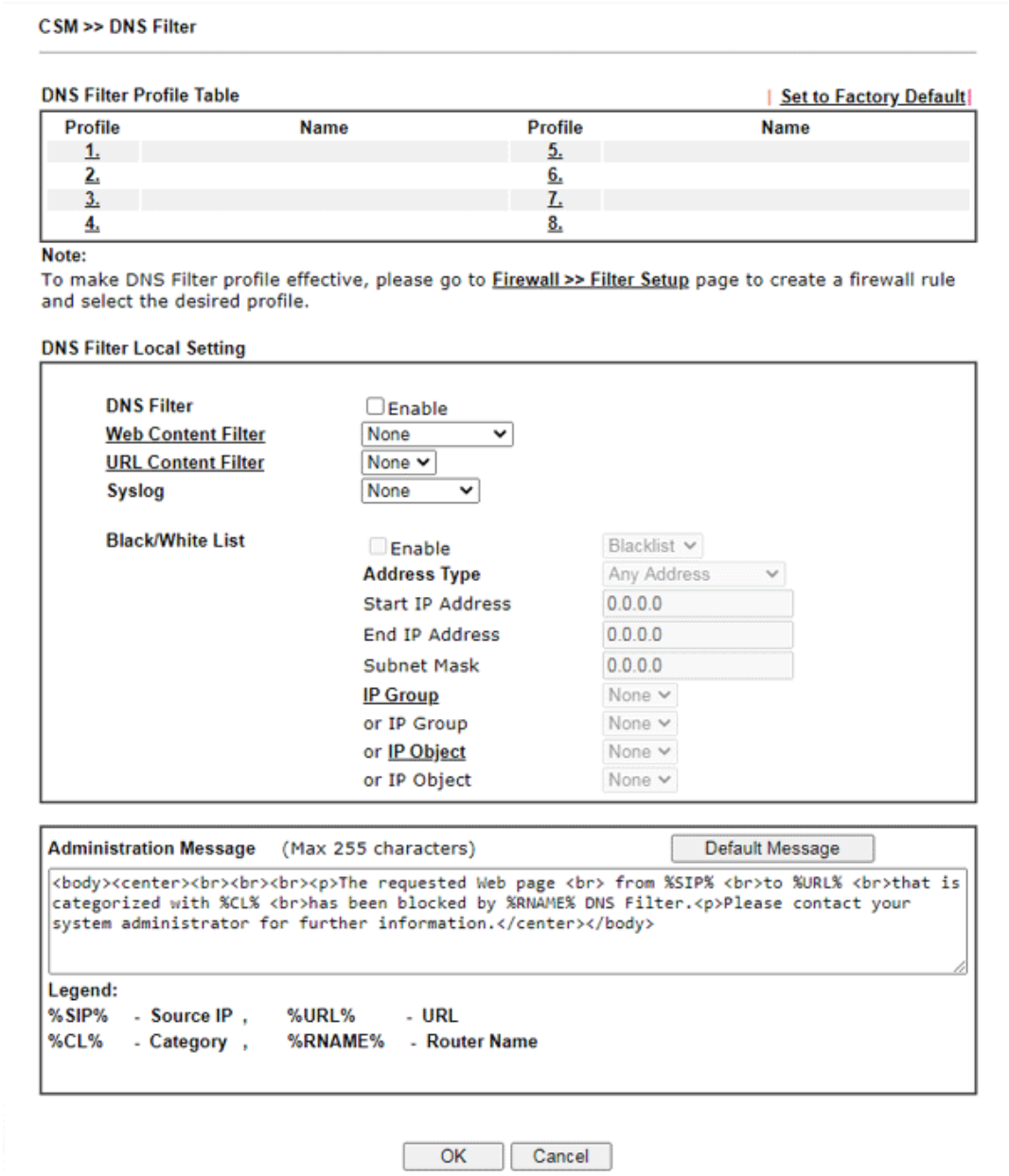
	Limpiar todo -Haga clic para anular la selección de todas las categorías dentro del grupo.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**.

VI-2-5 Perfil de filtro DNS

El filtro DNS bloquea o permite el tráfico a la WAN interceptando consultas de DNS y aplicando reglas UCF y WCF a los nombres de host. El filtrado de DNS es especialmente útil cuando desea restringir el acceso a protocolos que no sean HTTP, como HTTPS. Tenga en cuenta que ya se debe haber activado una licencia de WCF antes de que se puedan usar las reglas de WCF.

Para configurar perfiles de filtro DNS, seleccione**CSM >> Perfil de filtro de contenido web**desde el menú principal.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Tabla de perfil de filtro DNS	Los perfiles de filtro DNS surten efecto cuando se utilizan servidores DNS en la WAN para consultas DNS. El enrutador intercepta todas las consultas DNS salientes en el puerto UDP 53 y aplica las reglas WCF y UCF en los nombres de dominio antes de pasar las consultas a los servidores DNS. A continuación, las direcciones IP de los dominios se bloquean o

	permitido según las reglas aplicables de WCF y UCF. Los perfiles de filtro DNS se pueden aplicar seleccionando las reglas de filtro de Firewall. **Perfil -**Número de índice del perfil. Haga clic para abrir la página de configuración de la entrada de perfil. **Nombre -**Nombre que identifica al perfil.
Establecer como predeterminado de fábrica	Borre todas las configuraciones del perfil del filtro DNS.
Configuración local del filtro DNS	Al establecer la dirección IP del servidor de búsqueda de DNS en la dirección del enrutador, el enrutador sirve como un servidor proxy de búsqueda de DNS. Cuando la configuración local del filtro DNS está habilitada, todas las consultas DNS enviadas al enrutador tendrán reglas WCF y UCF aplicadas a los nombres de host, y el acceso a las direcciones IP resueltas se permitirá o bloqueará según lo configurado en las reglas. **Filtro DNS -**Seleccione para habilitar la configuración local del filtro DNS. **Filtro de contenido web -**Seleccione un perfil de WCF. **Filtro de contenido de URL**-Seleccione un perfil UCF. **Registro del sistema -**El resultado del filtrado se puede registrar de acuerdo con la configuración seleccionada para Syslog. - **Ninguno -**No se creará ningún archivo de registro para este perfil. - **Pase solamente -**Solo los intentos de acceso aprobados se registrarán en Syslog. - **Solo bloque–**Solo los intentos de acceso bloqueados se registrarán en Syslog. - **Ambos -**Tanto los intentos de acceso aprobados como los bloqueados se registrarán en Syslog. **Lista blanca/negra –**Especifique la dirección IP, la máscara de subred, el objeto IP o el grupo IP como una lista negra o una lista blanca para los paquetes DNS que pasan o son bloqueados por el enrutador Vigor.
Mensaje de administración	El mensaje que se muestra en el navegador cuando se bloquea el acceso a un sitio web. Se puede ingresar un mensaje personalizado con formato HTML en el cuadro de texto. Puede incrustar las siguientes variables en el mensaje: - %SIP%: la dirección IP de origen que intentó el acceso HTTP. - %DIP%: la dirección IP de destino a la que se intentó acceder. - %URL%: la URL del sitio web de destino. %CL%: - la categoría a la que pertenece la URL. - %RNAME%: el nombre del enrutador. **Mensaje predeterminado**-Haga clic para restablecer el mensaje de administración a los valores predeterminados de fábrica.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**.

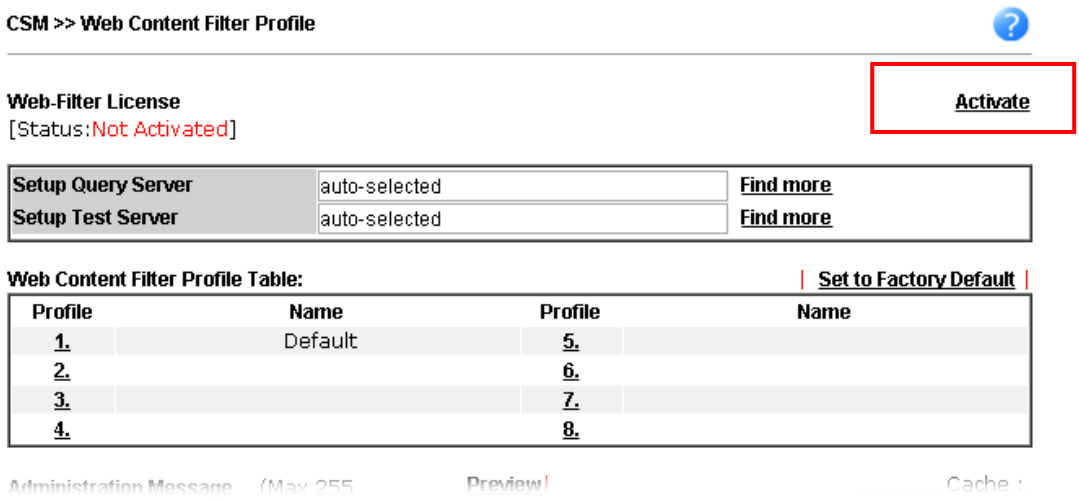
A-1 Cómo crear una cuenta para MyVigor

El sitio web de MyVigor (un servidor ubicado en http://myvigor.draytek.com) proporciona varios servicios útiles (como Anti-Spam, Web Content Filter, Anti-Intrusion, etc.) para filtrar las páginas web por el bien de proteger su sistema.

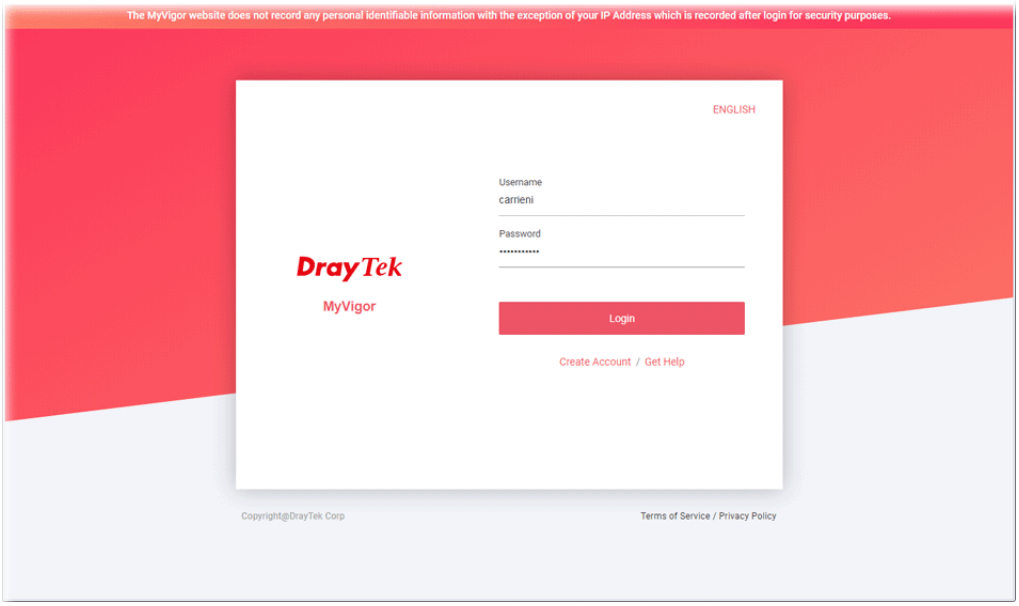
Para acceder a MyVigor y obtener más información, cree una cuenta en MyVigor.

Crear una cuenta a través del enrutador Vigor

1. Haga clic en**CSM>> Perfil de filtro de contenido web**. Aparecerá la siguiente página.



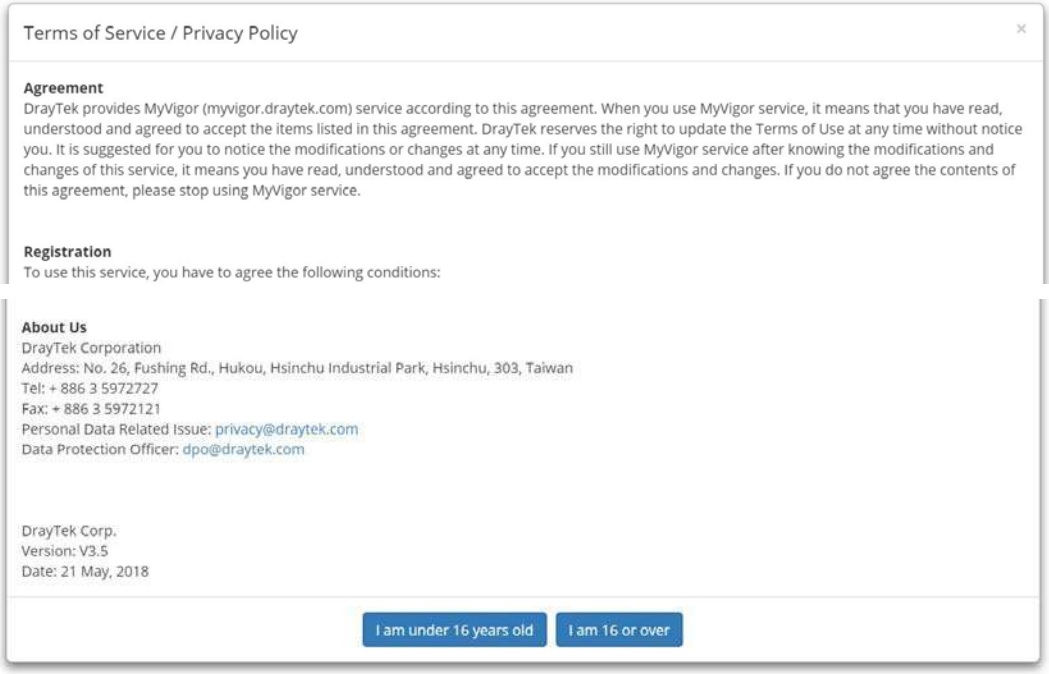
2. Haga clic en el**Activar**enlace. Aparecerá automáticamente una página de inicio de sesión para el sitio web de MyVigor.



3. Haga clic en el enlace de**Crear una cuenta**.

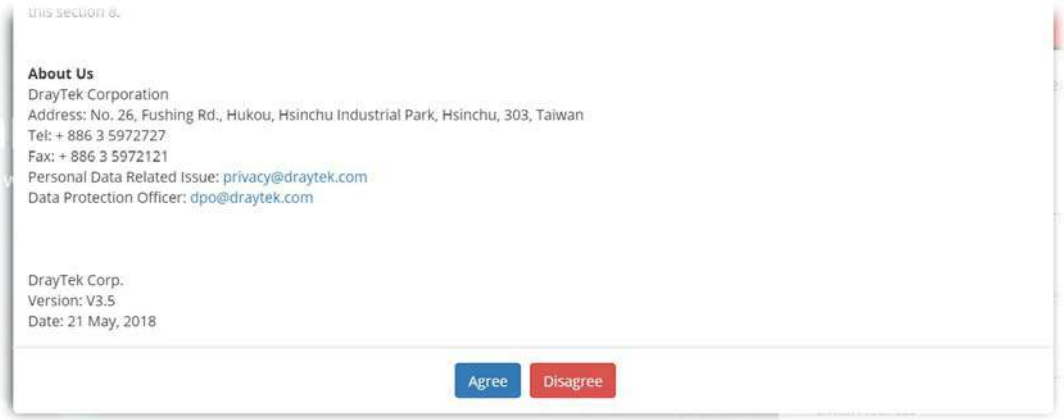
4. El sistema le preguntará si tiene 16 años o más.

-Si es así, haga clic**tengo 16 años o más**.

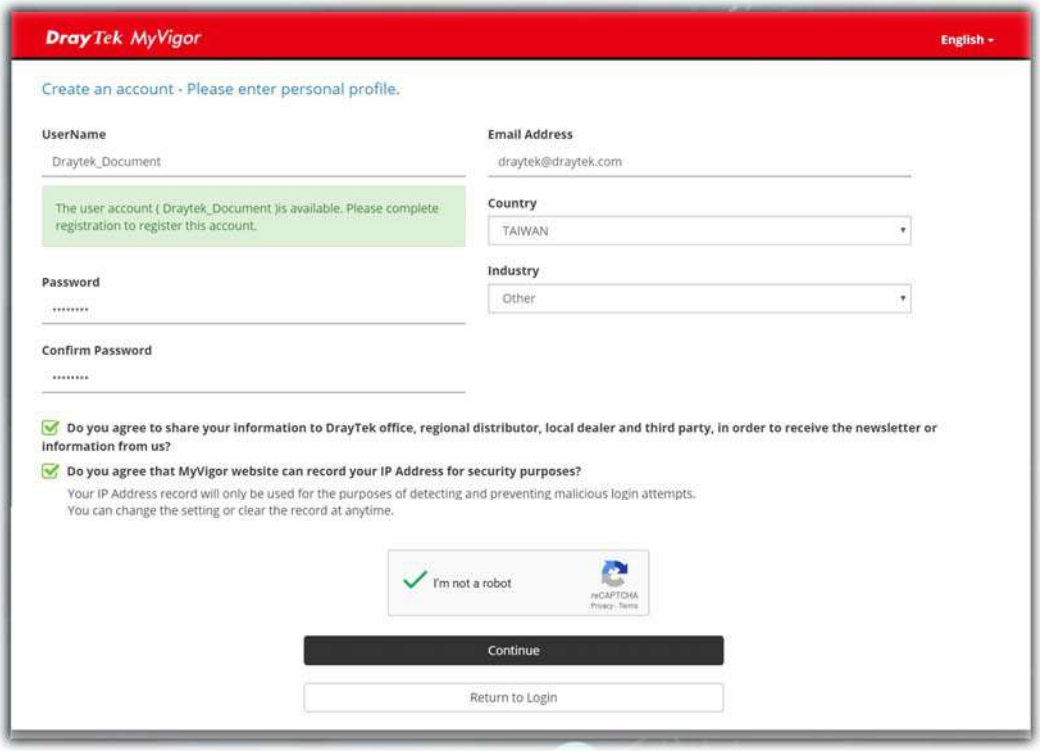


-Si no, haga clic en**tengo menos de 16 años**para obtener la siguiente página. Luego, haga clic en**Yo y mi tutor legal estamos de acuerdo**.

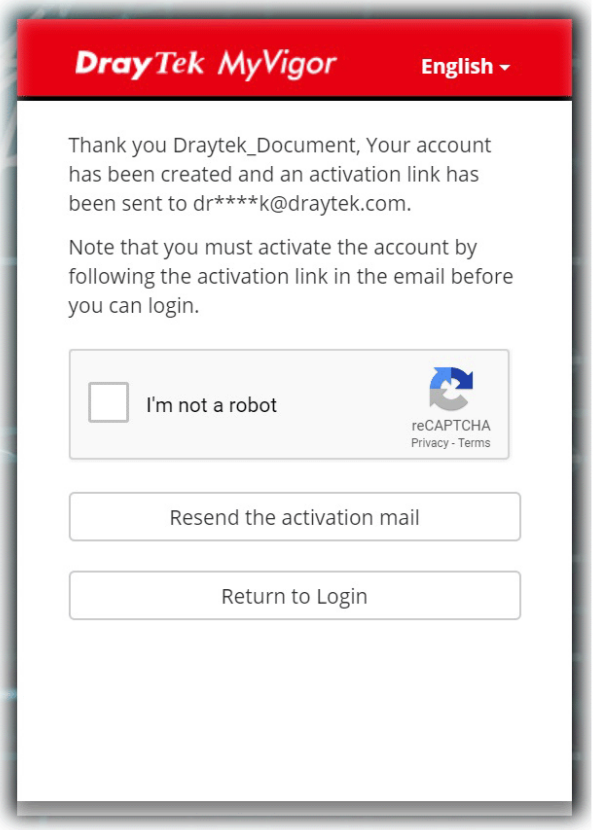
5. Después de leer los términos de servicio/política de privacidad, haga clic en**Aceptar**.



6. En la página siguiente, ingrese su información personal en esta página y luego haga clic en **Continuar**.

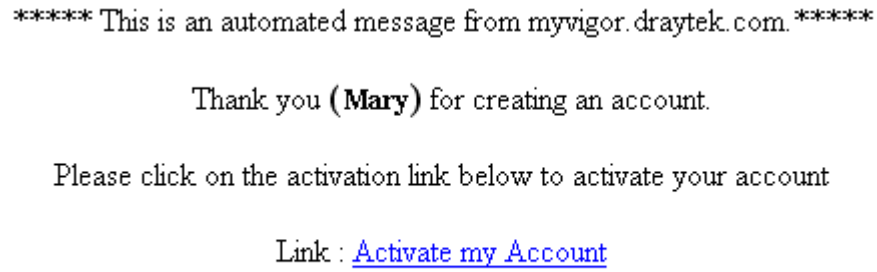


7. Elija la selección adecuada para su computadora y haga clic en**Continuar**.

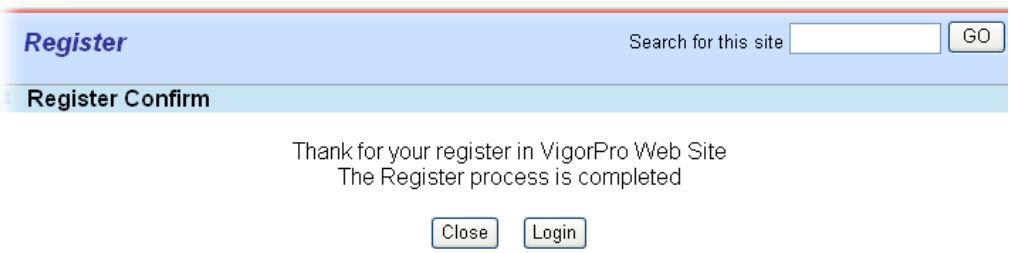


8. Ahora ha creado una cuenta con éxito.

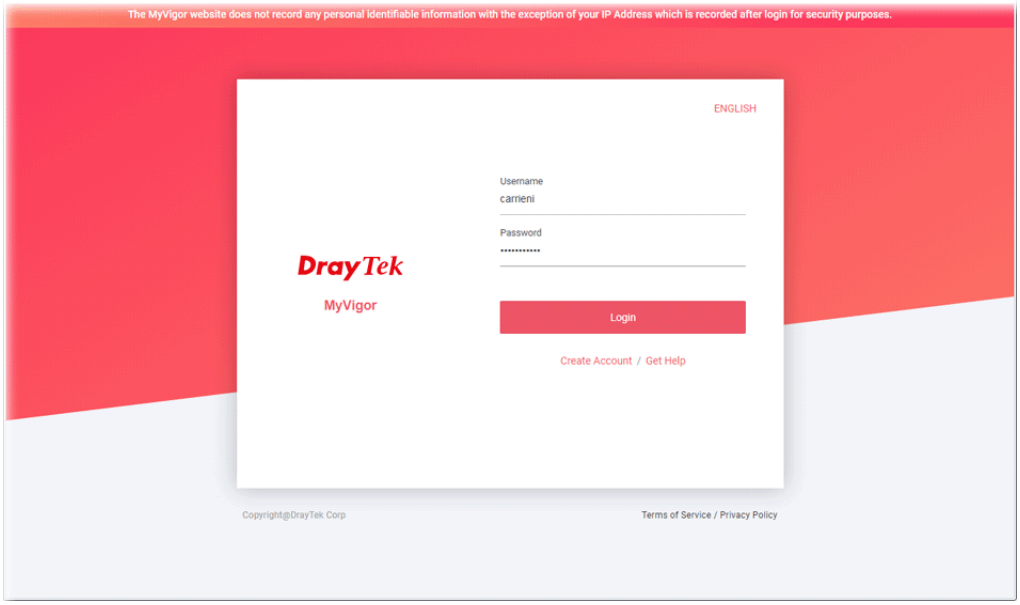
9. Verifique para ver la confirmación***correo electrónico***con el titulo de**Carta de confirmación de cuenta nueva de myvigor.draytek.com**.



10. Haga clic en el**Activar mi cuenta**enlace para habilitar la cuenta que ha creado. Se mostrará la siguiente pantalla para verificar que el proceso de registro haya finalizado. Por favor haz click**Acceso**.



11. Cuando vea la siguiente página, ingrese la cuenta y la contraseña (que acaba de crear) en los campos de**Nombre de usuario**y**Contraseña**.



12. Ahora, haz clic**Acceso**. Tu cuenta ha sido activada. Puede acceder al servidor MyVigor para activar el servicio (por ejemplo, WCF) que desee.

A-2 Cómo bloquear el servicio de Facebook al que acceden los usuarios a través del filtro de contenido web/ filtro de contenido URL

Hay dos formas de bloquear el servicio de Facebook, el filtro de contenido web y el filtro de contenido URL.

filtro de contenido web,

Beneficios: Implemente fácil y rápidamente la categoría/sitio web que desea bloquear.

Nota: Se requiere licencia.

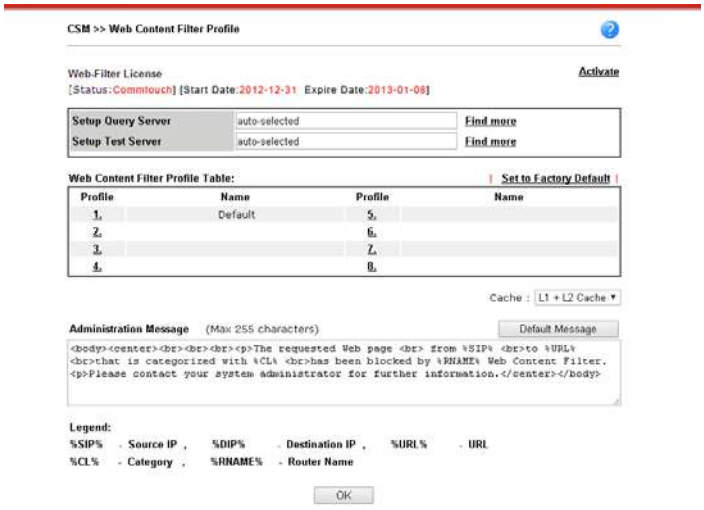
filtro de contenido de URL,

Beneficios: Gratis, flexible para personalizar la página web. Nota:

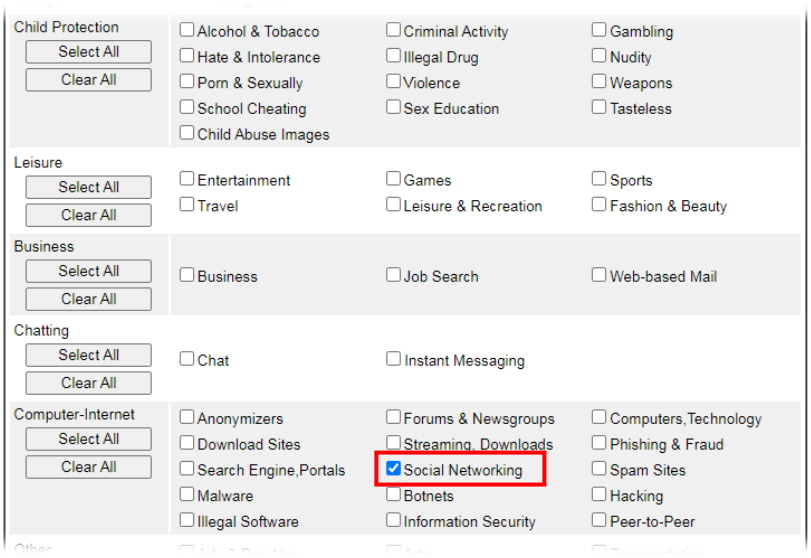
configuración manual (p. ej., una palabra clave para un sitio web).

I. A través del filtro de contenido web

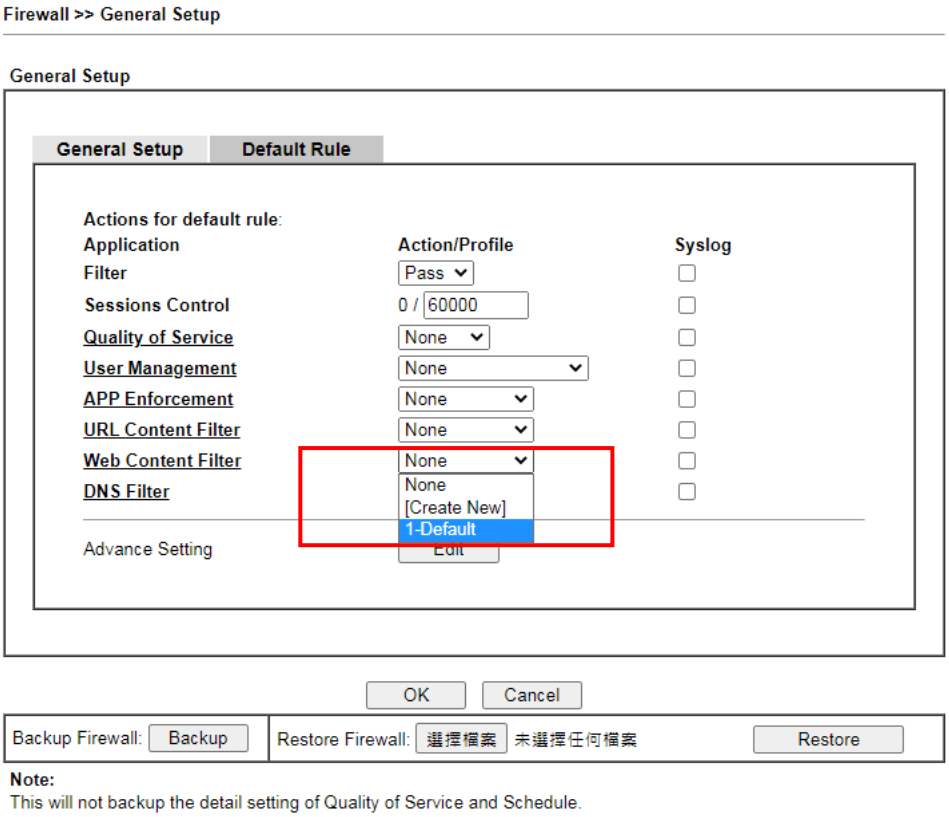
1. Asegúrese de que la licencia de Web Content Filter sea válida.



2. Abierto**CSM >> Perfil de filtro de contenido web**para crear un perfil WCF. Controlar**Redes sociales**con acción**, Bloquear**.



3. Habilite este perfil en**Cortafuegos>>Configuración general>>Regla predeterminada**.



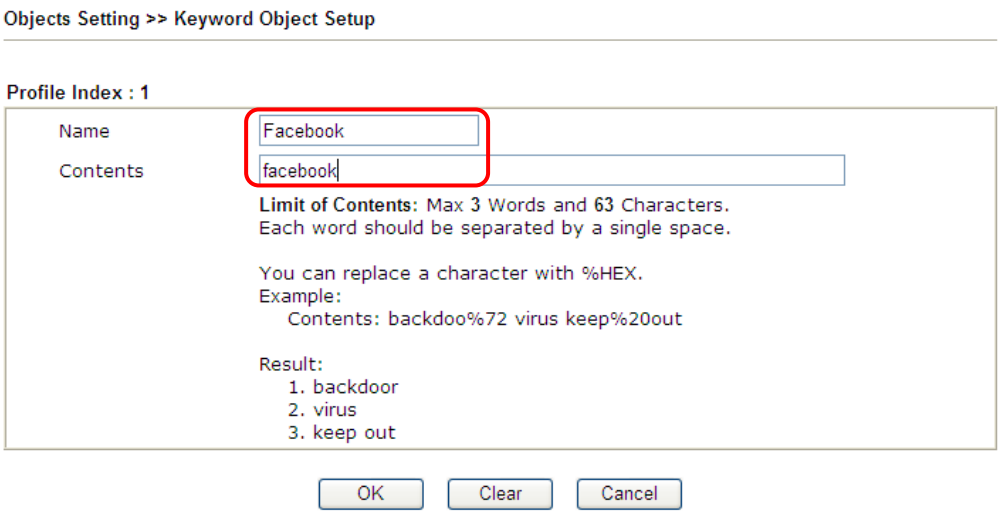
4. La próxima vez que alguien acceda a Facebook a través de este enrutador, la página web se bloqueará y en su lugar se mostrará el siguiente mensaje.

II. A través del filtro de contenido de URL

A. Bloquear la página web que contiene la palabra de “Facebook”

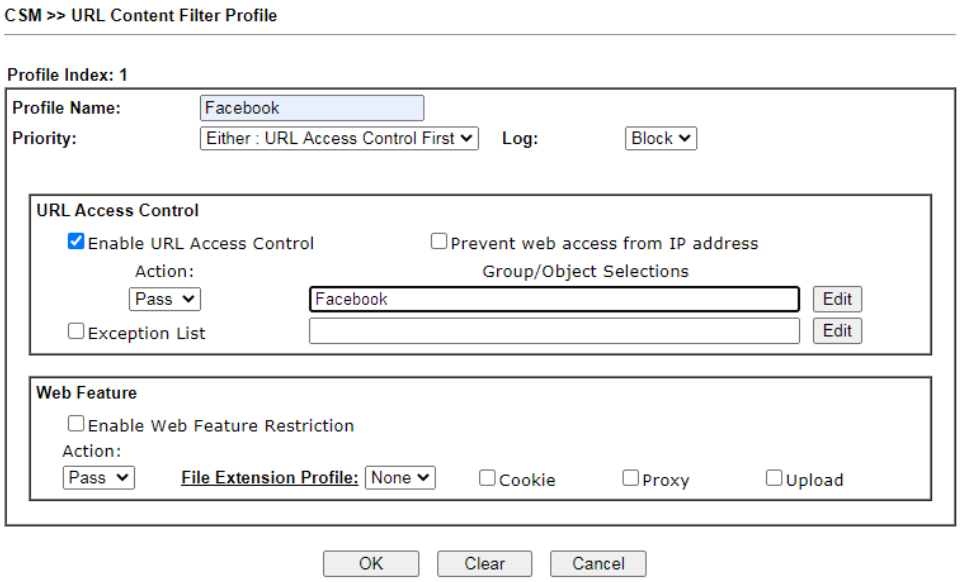
1. Abierto**Configuración de objeto>>Objeto de palabra clave**. Haga clic en un número de índice para abrir la página de configuración.

2. En el campo de**Contenido**, por favor escribe*Facebook*. Configure los ajustes como se muestra en la siguiente figura.



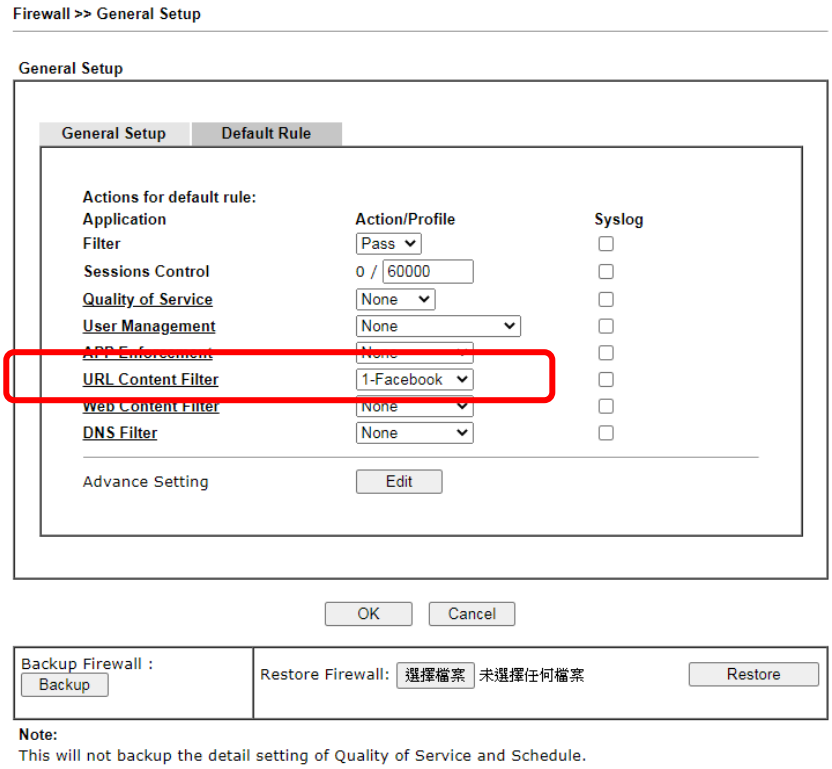
3. Abierto**CSM>>Perfil de filtro de contenido de URL**. Haga clic en un número de índice para abrir la página de configuración.

4. Configure los ajustes como se muestra en la siguiente figura.



5. Cuando haya terminado los pasos anteriores, haga clic en**DE ACUERDO**. Entonces, abre**Cortafuegos>>Configuración general**.

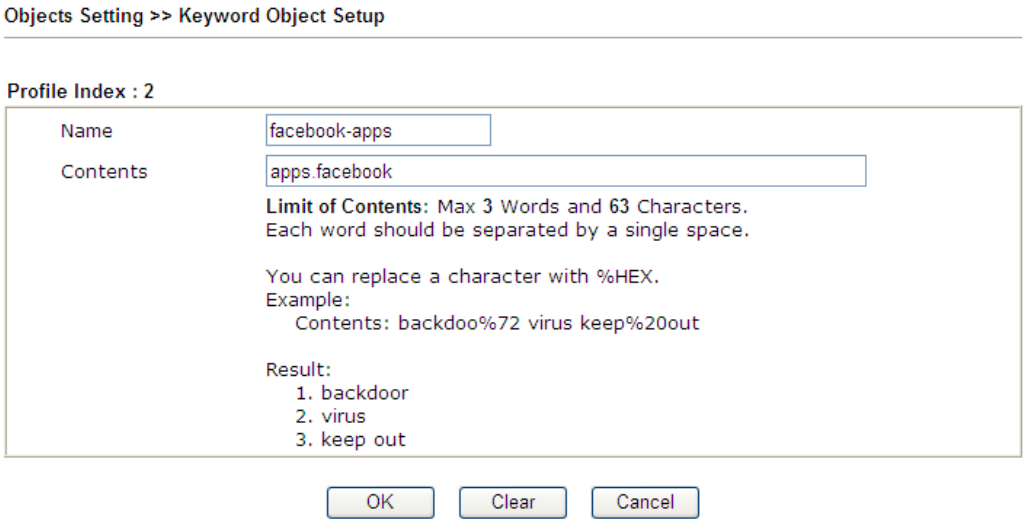
6. Haga clic en el**Regla predeterminada**pestaña. Elija el perfil recién configurado de la lista desplegable en el campo de**Filtro de contenido de URL**. Ahora, los usuarios no pueden abrir ninguna página web que tenga la palabra “facebook” adentro.



B. Prohibir que los usuarios jueguen en Facebook

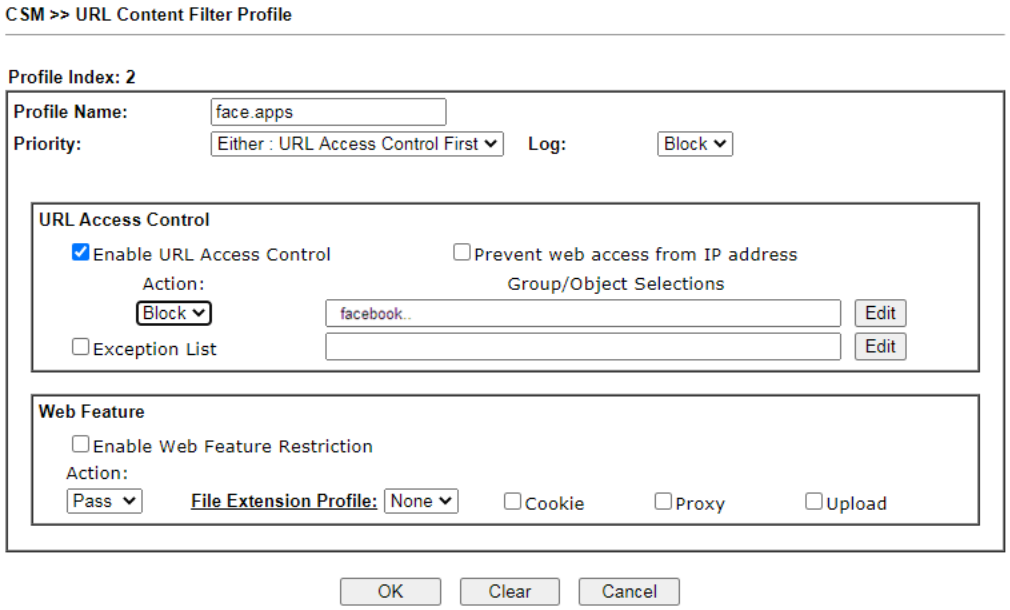
1. Abierto**Configuración de objeto>>Objeto de palabra clave**. Haga clic en un número de índice para abrir la página de configuración.

2. En el campo de**Contenido**, por favor escribe*aplicaciones.facebook*. Configure los ajustes como se muestra en la siguiente figura.



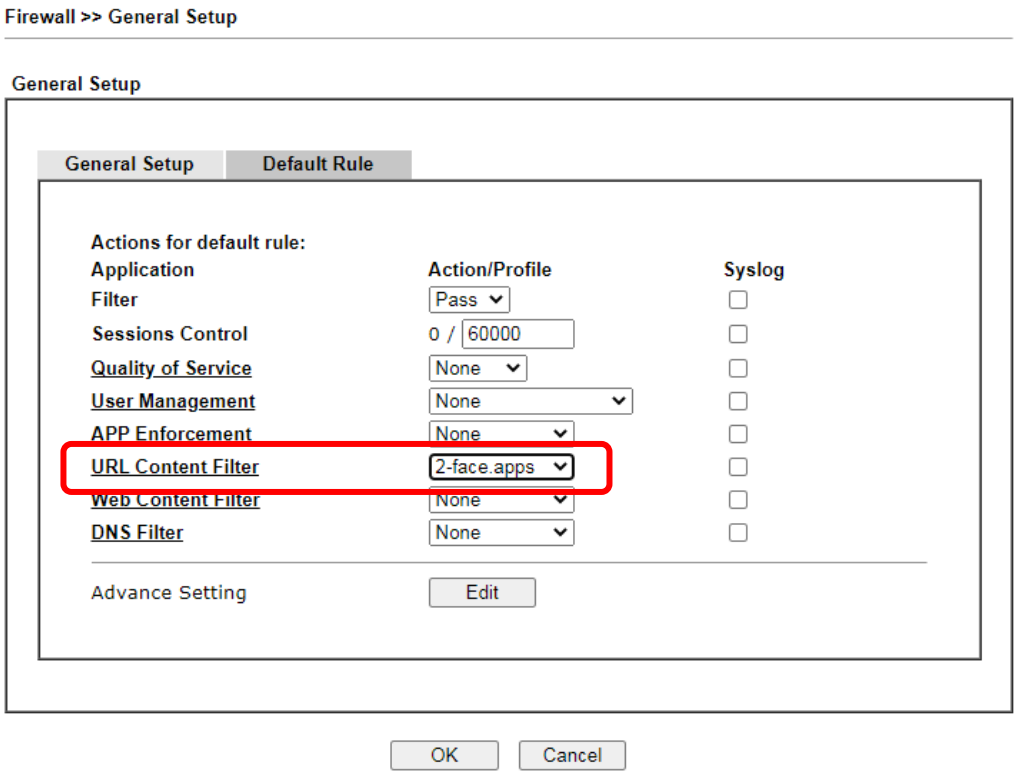
3. Abierto**CSM>>Perfil de filtro de contenido de URL**. Haga clic en un número de índice para abrir la página de configuración.

4. Configure los ajustes como se muestra en la siguiente figura.



5. Cuando haya terminado los pasos anteriores, abra**Cortafuegos>>Configuración general**.

6. Haga clic en el**Regla predeterminada**pestaña. Elija el perfil recién configurado de la lista desplegable en el campo de filtro de contenido de URL. Ahora, los usuarios no pueden abrir ninguna página web que tenga la palabra “facebook” adentro.



Parte VII Gestión

System Maintenance

Se ofrecen varios elementos para la configuración del sistema del enrutador Vigor: Estado del sistema, TR-069, Contraseña del administrador, Contraseña del usuario, Saludo de la página de inicio de sesión, Copia de seguridad de la configuración, Syslog/ Alerta de correo, Hora y fecha, Gestión, Reinicio del sistema, Actualización y activación del firmware .

Bandwidth Management

Se utiliza para controlar el ancho de banda de la transmisión de datos a través de la configuración del límite de sesiones, el límite de ancho de banda y la calidad del servicio (QoS).

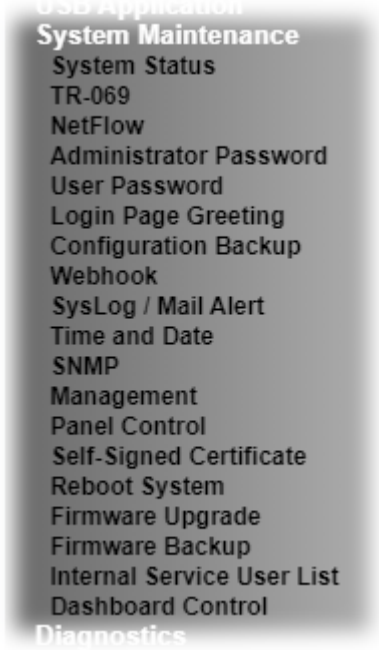
User Management

Es una función de seguridad que no permite ningún tráfico IP (excepto los paquetes relacionados con DHCP) de un host en particular hasta que ese host haya proporcionado correctamente un nombre de usuario y una contraseña válidos.

Mantenimiento del sistema VII-1

Para la configuración del sistema, hay varios elementos que debe conocer en la forma de configuración: Estado del sistema, TR-069, NetFlow, Contraseña del administrador, Contraseña del usuario, Saludo de la página de inicio de sesión, Copia de seguridad de la configuración, Webhook, Syslog/Alerta de correo, Hora y Fecha, SNMP, Gestión, Control de panel, Certificado autofirmado, Reinicio del sistema, Actualización de firmware, Copia de seguridad de firmware, Lista de usuarios de servicios internos y Control de panel.

A continuación se muestran los elementos del menú para el mantenimiento del sistema.



VII-1-1 Estado del sistema

El**Estado del sistema**muestra información básica de la red del enrutador Vigor, incluido el estado de la interfaz LAN y WAN. También está disponible la versión actual del firmware y la información relacionada con el firmware.

System Maintenance >> System Status

Model Name : Vigor2927Vac
Firmware Version : 4.4.2.2
Build Date/Time : Nov 11 2022 11:59:09

LAN

	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	14-49-BC-11-7B-60	192.168.1.1	255.255.255.0	ON	8.8.8.8
LAN2	14-49-BC-11-7B-60	192.168.2.1	255.255.255.0	ON	8.8.8.8
LAN3	14-49-BC-11-7B-60	192.168.3.1	255.255.255.0	ON	8.8.8.8
LAN4	14-49-BC-11-7B-60	192.168.4.1	255.255.255.0	ON	8.8.8.8
LAN5	14-49-BC-11-7B-60	192.168.5.1	255.255.255.0	ON	8.8.8.8
LAN6	14-49-BC-11-7B-60	192.168.6.1	255.255.255.0	ON	8.8.8.8
LAN7	14-49-BC-11-7B-60	192.168.7.1	255.255.255.0	ON	8.8.8.8
LAN8	14-49-BC-11-7B-60	192.168.8.1	255.255.255.0	ON	8.8.8.8
DMZ PORT	14-49-BC-11-7B-60	192.168.254.1	255.255.255.0	ON	8.8.8.8
IP Routed Subnet	14-49-BC-11-7B-60	192.168.0.1	255.255.255.0	ON	8.8.8.8

Wireless LAN(2.4GHz)

MAC Address	Frequency Domain	Firmware Version	SSID
16-49-BC-41-7B-60	Europe	5.0.4.0	DrayTek

Wireless LAN(5GHz)

MAC Address	Frequency Domain	Firmware Version	SSID
14-49-BC-11-7B-60	Europe	5.0.4.0	DrayTek_5G

WAN

	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	14-49-BC-11-7B-61	DHCP Client	---	---
WAN2	Disconnected	14-49-BC-11-7B-62	DHCP Client	---	---
WAN3	Disconnected	12-59-BC-11-7B-60	---	---	---
WAN4	Disconnected	12-49-BC-11-7B-60	---	---	---
WAN5	Disconnected	14-49-BC-11-7B-65	---	---	---
WAN6	Disconnected	14-49-BC-11-7B-66	---	---	---

IPv6

	Address	Scope	Internet Access Mode
LAN	FE80::1649:BCFF:FE11:7B60/64	Link	---

VoIP

Port	Profile	Reg.	In/Out
Phone1		No	0/0
Phone2		No	0/0

Los ajustes disponibles se explican a continuación:

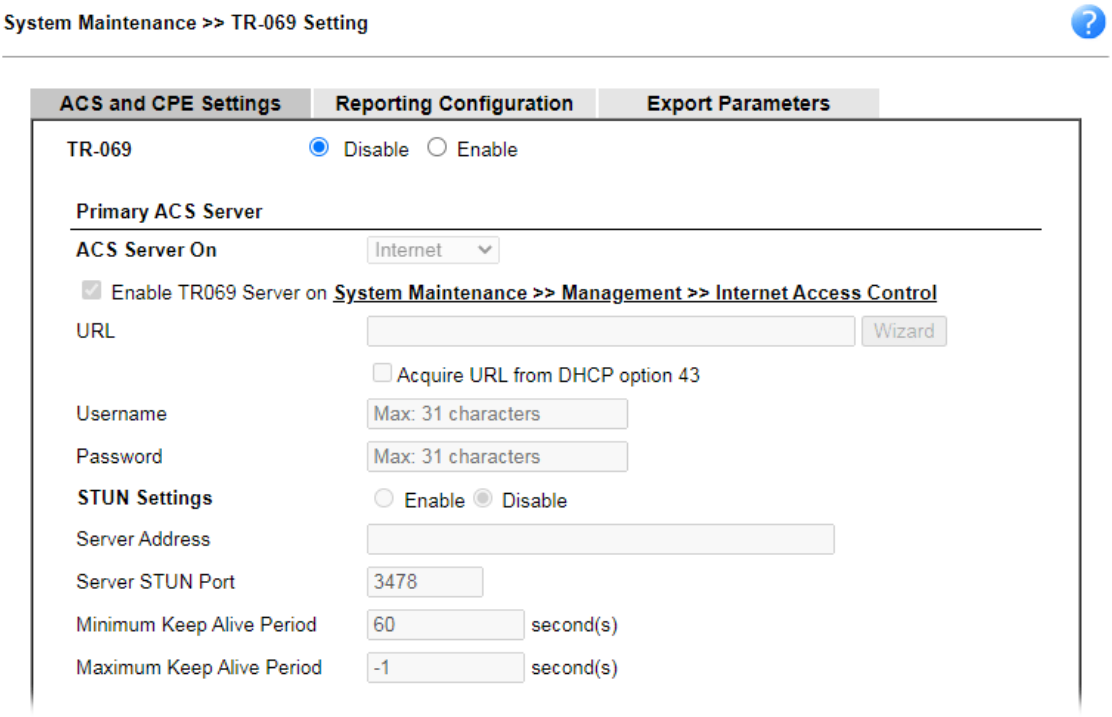
Artículo	Descripción
Nombre del modelo	Muestra el nombre del modelo del enrutador.
Versión de firmware	Muestra la versión de firmware del enrutador.
Fecha/hora de compilación	Muestra la fecha y la hora de la compilación de firmware actual.
LAN	**Dirección MAC** - Muestra la dirección MAC de la interfaz LAN. **Dirección IP** - Muestra la dirección IP de la interfaz LAN. **Máscara de subred**

	- Muestra la dirección de la máscara de subred de la interfaz LAN. **servidor DHCP** - Muestra el estado actual del servidor DHCP de la interfaz LAN. **DNS** - Muestra la dirección IP asignada del DNS primario.
LAN inalámbrico	**Dirección MAC** - Muestra la dirección MAC de la interfaz LAN. **Dominio de la frecuencia** - Muestra el dominio de la frecuencia. **Versión de firmware** - Muestra la versión del firmware. **SSID** - Muestra el nombre del SSID.
PÁLIDO	**Estado del enlace** - Muestra el estado de conexión actual de la interfaz WAN. **Dirección MAC** - Muestra la dirección MAC de la interfaz WAN. **Conexión** - Muestra el tipo de conexión de la interfaz WAN.. **Dirección IP** - Muestra la dirección IP de la interfaz WAN. **Puerta de enlace predeterminada** - Muestra la dirección IP asignada de la puerta de enlace predeterminada.
IPv6	**DIRECCIÓN -**Muestra la dirección IPv6 para LAN. **Alcance -**Muestra el alcance de la dirección IPv6. Por ejemplo, **Enlace IPv6 local**no es enrutable y solo se puede usar para conexiones locales. **Modo de acceso a Internet –**Muestra el modo de conexión de la interfaz WAN.

VII-1-2 TR-069

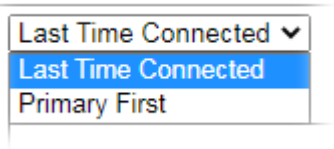
Este dispositivo es compatible con el estándar TR-069 para la gestión remota de equipos en las instalaciones del cliente (CPE) a través de un servidor de configuración automática, como VigorACS.

Configuración de VII-1-2-1 ACS y CPE



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
TR-069	Habilita o deshabilita la funcionalidad TR-069.
Servidor ACS primario	Esta sección especifica la configuración del servidor ACS. **Servidor ACS activado -**Elija la interfaz para conectar el enrutador al servidor de configuración automática. **Habilite el servidor TR069 en Mantenimiento del sistema>>Administración>>Control de acceso a Internet**-Si está habilitado, un usuario podrá acceder a TR-069 desde WAN. **URL-**Ingrese la URL para conectarse al ACS. **Mago**–Haga clic para ingresar la dirección IP del servidor VigorACS, el número de puerto y el controlador. **Adquirir URL desde DHCP opción 43**–Marque la casilla para obtener la URL de la opción 43 de DHCP. **Usuario Contraseña -**Ingrese las credenciales requeridas para conectarse al servidor ACS. **Configuración de STUN -**El valor predeterminado es**Desactivar**. Si selecciona**Permitir**, escriba la configuración relacional que se detalla a continuación: - **Dirección del servidor -**Escriba la dirección IP del servidor STUN. - **Servidor STUN Puerto –**Escriba el número de puerto del servidor STUN.

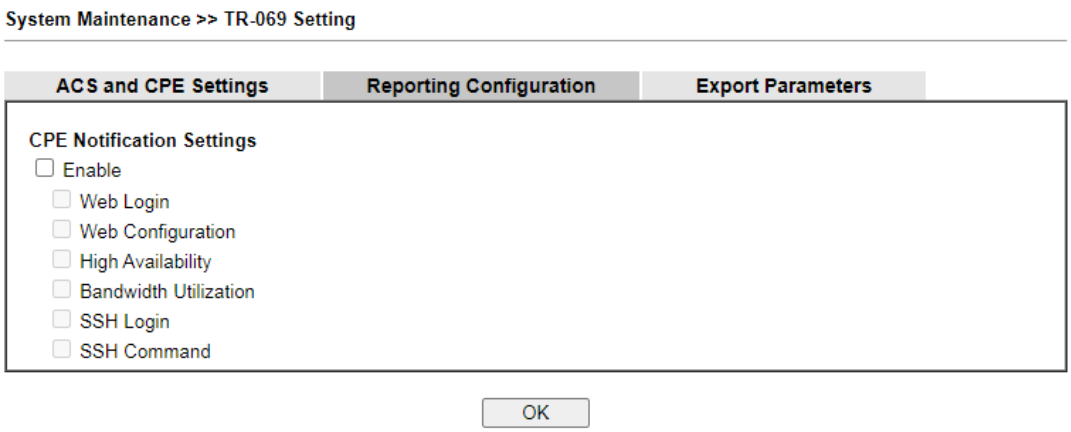
	- **Período mínimo de mantenimiento de vida:**Si STUN está habilitado, el CPE debe enviar una solicitud de vinculación al servidor con el fin de mantener la vinculación en el Gateway. Escriba un número como período mínimo. La configuración predeterminada es "60 segundos". - **Período Máximo de Keep Alive –**Si STUN está habilitado, el CPE debe enviar una solicitud de vinculación al servidor con el fin de mantener la vinculación en el Gateway. Escriba un número como período máximo. Un valor de "-1" indica que no se especifica un período máximo.
Servidor ACS secundario	**Modo -**Elegir**Primaria Primero**si este servidor actuará como un servidor de respaldo.  **Servidor ACS activado -**Elija la interfaz para conectar el enrutador al servidor de configuración automática. **Habilite el servidor TR069 en Mantenimiento del sistema>>Administración>>Control de acceso a Internet**-Si está habilitado, un usuario podrá acceder a TR-069 desde WAN. **URL-**Ingrese la URL para conectarse al ACS. **Mago**–Haga clic para ingresar la dirección IP del servidor VigorACS, el número de puerto y el controlador. **Usuario Contraseña -**Dichos datos deben escribirse de acuerdo con el ACS (Servidor de configuración automática) que desea vincular. **Configuración de STUN -**El valor predeterminado es**Desactivar**. Si selecciona**Permitir**, escriba la configuración relacional que se detalla a continuación: - **Dirección del servidor -**Escriba la dirección IP del servidor STUN. - **Servidor STUN Puerto –**Escriba el número de puerto del servidor STUN. - **Período mínimo de mantenimiento de vida:**Si STUN está habilitado, el CPE debe enviar una solicitud de vinculación al servidor con el fin de mantener la vinculación en el Gateway. Escriba un número como período mínimo. La configuración predeterminada es "60 segundos". - **Período Máximo de Keep Alive –**Si STUN está habilitado, el CPE debe enviar una solicitud de vinculación al servidor con el fin de mantener la vinculación en el Gateway. Escriba un número como período máximo. Un valor de "-1" indica que no se especifica un período máximo.
Estado	**Tiempo de respuesta de la última información**–Muestra la hora en que el servidor VigorACS respondió al recibir el mensaje de información de CPE la última vez. **Prueba con informe**–Haga clic para enviar un mensaje basado en la selección del código de evento para probar si dicho CPE puede comunicarse con el servidor VigorACS SI. **Código de evento**–Utilice el menú desplegable para especificar un evento para realizar la prueba.
Cliente CPE	Esta sección especifica la configuración del Cliente CPE. **Protocolo**–Seleccione Https si la conexión está encriptada;

	de lo contrario, seleccione Http. **Puerto**–En caso de conflictos de puerto, cambie el número de puerto del CPE. **Nombre de usuario**y**Contraseña**–Ingrese el nombre de usuario y la contraseña que utilizará VigorACS para conectarse al CPE.
Configuración de información periódica	**Permitir**–La configuración predeterminada es Activar, lo que significa que el Cliente CPE se conectará periódicamente al Servidor ACS para actualizar sus parámetros de conexión en los intervalos especificados en el campo Intervalo de tiempo. - **Intervalo de tiempo**-Establezca el tiempo de intervalo o programe el tiempo para que el enrutador envíe una notificación al CPE. **Desactivar**-Seleccionar**Desactivar**para desactivar las notificaciones periódicas.
Aplicar configuraciones a los puntos de acceso	Esta función puede aplicar la configuración TR-069 (incluida la configuración del servidor STUN y ACS) a todos los AP administrados por Vigor2927 al mismo tiempo. **Desactivar**–TR-069 y las configuraciones relacionadas no se aplicarán a los VigorAP. **Permitir**–La configuración de TR-069 se aplicará a los VigorAP después de hacer clic en**DE ACUERDO**. Se debe especificar la contraseña de VigorAP. - **Contraseña AP**–Ingrese la contraseña del VigorAP al que desea aplicar la configuración TR-069 de Vigor2135. - **Especifique la configuración de STUN para AP**–Después de hacer clic en el **Permitir**botón de radio para Aplicar configuraciones a AP, si desea aplicar configuraciones específicas de STUN (es decir, diferentes de las configuraciones de Vigor2865 STUN) a VigorAP para cumplir con requisitos específicos, marque esta casilla e ingrese la dirección IP del servidor, el puerto del servidor y el valor mínimo y máximo mantener períodos vivos respectivamente.

Seleccionar**DE ACUERDO**para guardar los cambios en la página, o**Claro**para restablecer todas las configuraciones a los valores predeterminados de fábrica.

VII-1-2-2 Configuración de informes

La información relacionada con el estado del enrutador se divide en varias categorías y se enumera en este campo. Después de verificar los elementos, el enrutador Vigor organizará y enviará los datos correspondientes a VigorACS como referencia para el administrador del sistema.



Los ajustes disponibles se explican a continuación:

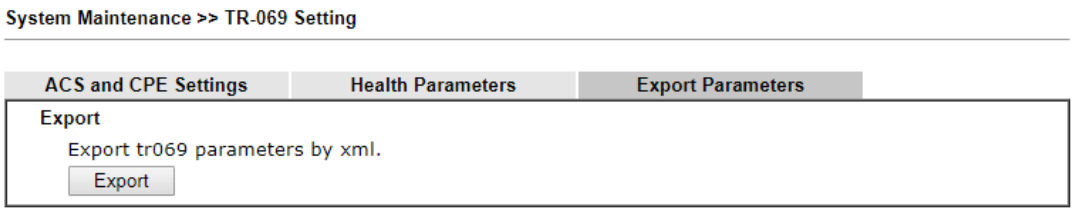
Artículo	Descripción
Configuración de notificaciones de CPE	**Permitir**-Marque la casilla para seleccionar los elementos de notificación.

	El enrutador Vigor enviará el estado de utilización a VigorACS.

Hacer clic**DE ACUERDO**para guardar los cambios en la página.

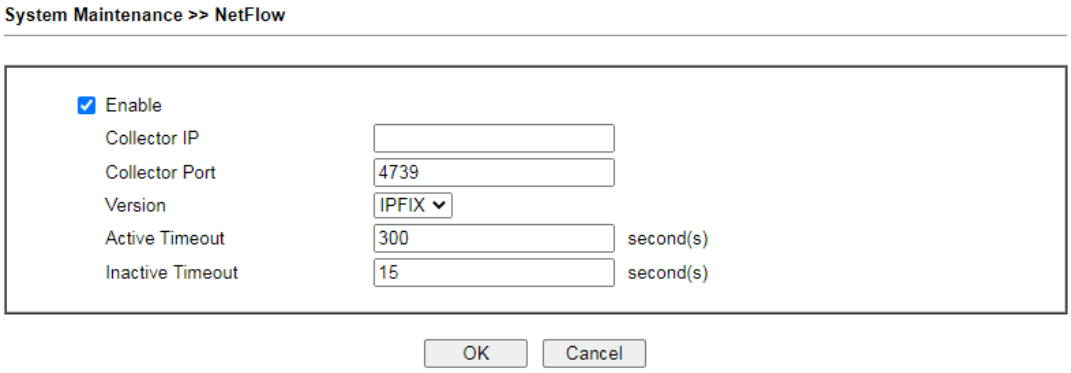
VII-1-2-3 Parámetros de exportación

Hacer clic**Exportar**para guardar la configuración del parámetro TR-069 como un ".xml".



VII-1-3 Flujo de red

Esta página le permite configurar la dirección IP, el número de puerto, las versiones y el tiempo de espera para recopilar información de paquetes supervisada por la función NetFlow.



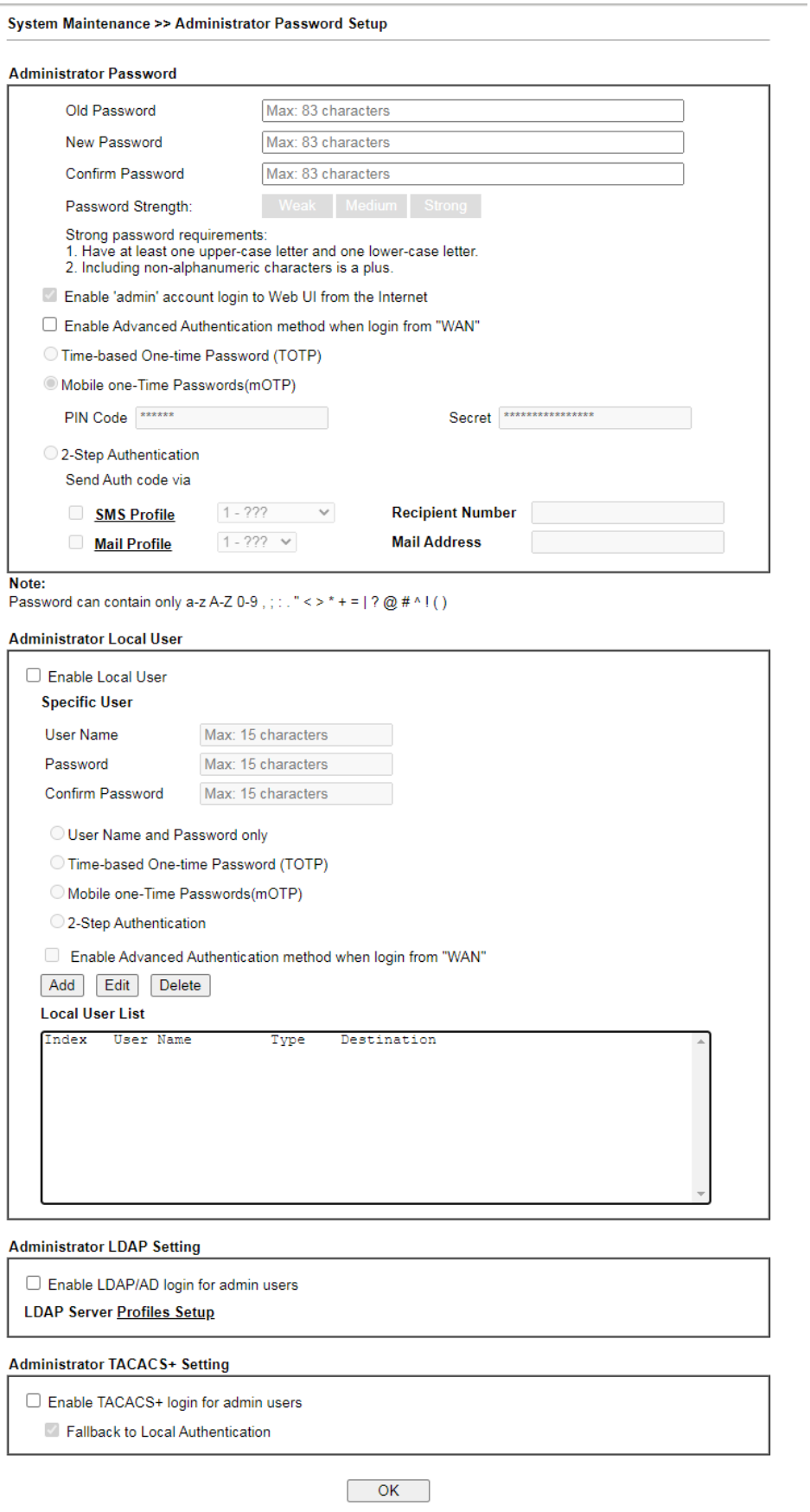
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	**Permitir**-Marque la casilla para habilitar la función NetFlow.
IP del recopilador	Ingrese la dirección IP de un servidor (p. ej., VigorConnect) que se puede usar como colector de flujo.
Puerto colector	Introduzca el número de puerto del servidor.
Versión	El enrutador admite tres versiones (v5, v9 e IPFIX) de la función NetFlow.
Tiempo de espera activo	Rango de 60 a 1800 segundos. El valor predeterminado es 300 (segundos). Establece el intervalo de tiempo de actividad que marca un flujo activo. La información del flujo de datos se recopilará continuamente hasta el tiempo de espera activo.
Tiempo de espera inactivo	Rango de 15 a 1800 segundos. Establece el intervalo de tiempo de inactividad que marca un flujo inactivo. La información de los datos recopilados se exportará después del intervalo de tiempo inactivo.

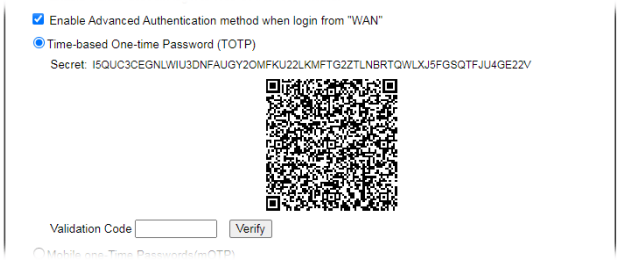
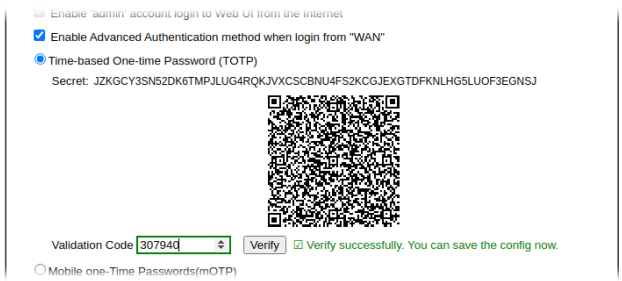
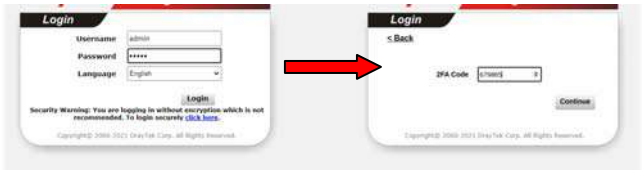
Hacer clic**DE ACUERDO**para guardar los cambios en la página.

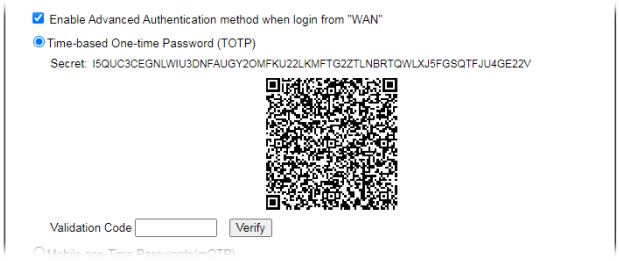
VII-1-4 Contraseña del administrador

Esta página le permite establecer o cambiar la contraseña de administrador.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Contraseña de administrador	El administrador puede iniciar sesión en la interfaz de usuario web del enrutador Vigor para modificar todas las configuraciones para cumplir con los requisitos. **Contraseña anterior**-Introduzca la contraseña actual. El valor predeterminado de fábrica es "administrador". **Nueva contraseña**–Introduzca la nueva contraseña. La longitud máxima de la contraseña es de 23 caracteres. **confirmar Contraseña**–Ingrese la nueva contraseña nuevamente para confirmar. **seguridad de la contraseña**-Muestra el nivel de seguridad de la contraseña especificada anteriormente. **Habilite el inicio de sesión de la cuenta 'admin' en la interfaz de usuario web desde Internet**– Seleccione para permitir que el administrador inicie sesión desde Internet. Esta opción está habilitada cuando está habilitado el Administrador de usuario local (ver a continuación). **Use solo el método de autenticación avanzada para el inicio de sesión de administrador "WAN"**–El método de autenticación avanzada puede ofrecer una **más seguro**conexión de red. Seleccione para requerir TOTP, mOTP o autenticación de 2 pasos al iniciar sesión desde la WAN. - **Contraseña de un solo uso basada en el tiempo (TOTP) -**Asegúrese de que la zona horaria de su enrutador sea correcta. Luego, instale la aplicación Google Authenticator en su teléfono celular. Abra la aplicación para escanear el código QR en esta página. Se mostrará una contraseña de un solo uso en su teléfono.  en el archivado de**Código de validación**, ingrese la contraseña de un solo uso y haga clic en**Verificar**.  Ahora, la configuración ha terminado. Se le pedirá que ingrese el código 2FA después de pasar la autenticación de nombre de usuario y contraseña.  - **Contraseña móvil de un solo uso (mOTP)**–Seleccionar para permitir

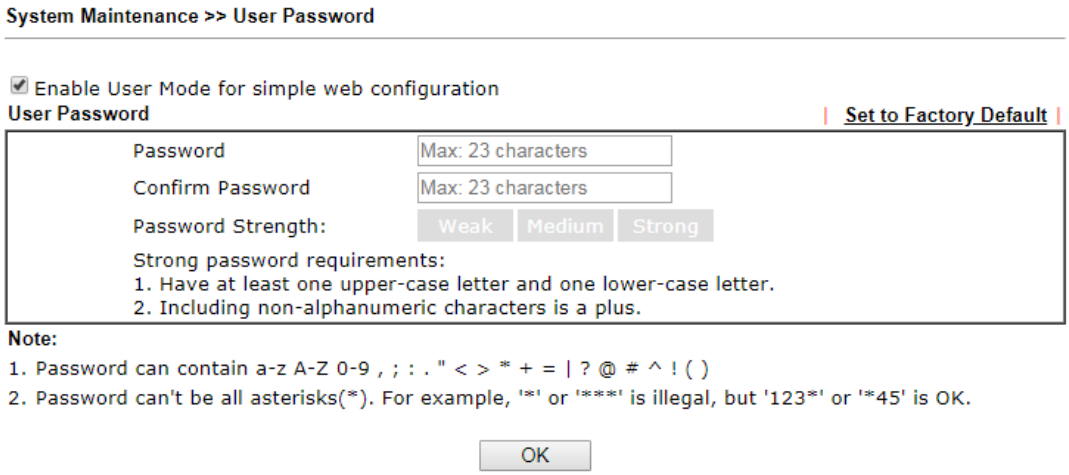
	el uso de contraseñas mOTP. Ingrese el código PIN y la configuración secreta para obtener contraseñas de un solo uso. - **2-Paso Código de autenticación a través de<u>Perfil SMS</u> y/o<u>Perfil de correo</u> –** Seleccione los perfiles de SMS y/o Correo y el número de SMS de destino y/o la dirección de correo electrónico para transmitir la contraseña.
Administrador Usuario local	Por lo general, el administrador del sistema tiene el privilegio más alto para modificar la configuración en la interfaz de usuario web del enrutador Vigor. Sin embargo, en algunos casos, puede ser necesario tener otros usuarios en la LAN para acceder a la interfaz de usuario web del enrutador Vigor. Esta función le permite agregar más administradores que luego pueden iniciar sesión en la interfaz web, con los mismos privilegios que el administrador. **Habilitar usuario local**–Marque la casilla para permitir que otros usuarios administren el enrutador. **Usuario específico –**Cree la nueva cuenta de usuario como usuario local. Luego especifique el método de autenticación (dividido en Básico y Avanzado) para la cuenta de usuario. - **Nombre de usuario**–Introduzca un nombre de usuario. - **Contraseña**–Ingrese la contraseña para el usuario local. - **confirmar Contraseña**-Ingrese la nueva contraseña nuevamente para confirmar. - **Solo nombre de usuario y contraseña**-Si se selecciona, debe ingresar un nombre de usuario y una contraseña. - **Contraseña de un solo uso basada en el tiempo (TOTP) -**Asegúrese de que la zona horaria de su enrutador sea correcta. Luego, instale la aplicación Google Authenticator en su teléfono celular. Abra la aplicación para escanear el código QR en esta página. Se mostrará una contraseña de un solo uso en su teléfono.  en el archivado de**Código de validación**, ingrese la contraseña de un solo uso y haga clic en**Verificar**. Ahora, la configuración ha terminado. Se le pedirá que ingrese el código 2FA después de pasar la autenticación de nombre de usuario y contraseña.

	  - **Contraseña móvil de un solo uso (mOTP)**–Seleccione para permitir el uso de contraseñas mOTP. Ingrese el código PIN mOTP y el secreto que se usará para generar las contraseñas de un solo uso. - **2-Paso Autenticación vía<u>Perfil SMS</u> e y/o<u>Perfil de correo</u> –** Seleccione los perfiles de SMS y/o Correo y el número de SMS de destino y/o la dirección de correo electrónico para transmitir la contraseña. - **Habilite el método de autenticación avanzada cuando inicie sesión desde "WAN"**– El método de autenticación avanzada puede ofrecer una**más seguro**conexión de red. Seleccione para requerir mOTP o TOTP o autenticación de 2 pasos al iniciar sesión desde la WAN. - **Agregar**–Después de ingresar el nombre de usuario y la contraseña anteriores, haga clic en este botón para crear un nuevo usuario local. El nuevo usuario se mostrará en la Lista de usuarios locales inmediatamente. - **Editar**–Si desea cambiar un usuario en la Lista de usuarios locales, selecciónelo, realice las modificaciones necesarias y haga clic en este botón para actualizar el usuario. - **Borrar**–Si desea eliminar un usuario de la Lista de usuarios locales, selecciónelo y haga clic en este botón para eliminarlo. - **Lista de usuarios locales**–Muestra todos los usuarios que están configurados para administrar el enrutador.
Administrador LDAP **Configuración**	**Habilitar inicio de sesión LDAP/AD para usuarios administradores**–Seleccione para permitir la autenticación mediante un servidor LDAP/Active Directory. **Servidor LDAP<u>Configuración de perfiles</u>** –Haga clic para configurar el servidor LDAP/Active Directory.
Administrador TACACS+ **Configuración**	**Habilite el inicio de sesión de TACACS+ para usuarios administradores**–Si está habilitado, cualquier usuario puede acceder a la interfaz de usuario web del enrutador Vigor a través de la autenticación del servidor TACACS+. - **Alternativa a la autenticación local**-Si está habilitado, el administrador puede usar otros métodos de inicio de sesión para la autenticación una vez que el servidor TACACS+ no responde.

Hacer clic**DE ACUERDO**para guardar los cambios en la página y se le dirigirá a la pantalla de inicio de sesión. Inicie sesión con la nueva contraseña.

VII-1-5 Contraseña de usuario

Esta página le permite establecer una nueva contraseña para la operación del usuario.



Los ajustes disponibles se explican a continuación:

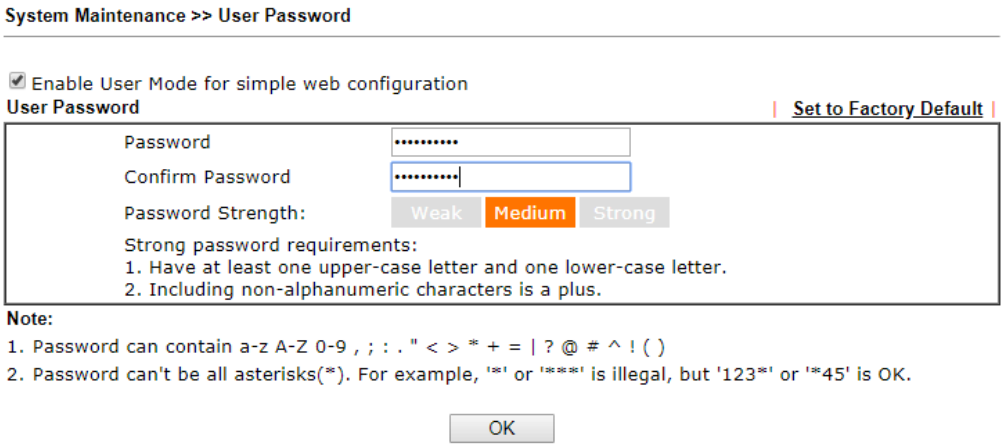
Artículo	Descripción
Habilite el modo de usuario para una configuración web simple	Marque esta casilla para habilitar el modo de usuario para la interfaz de usuario web con la contraseña ingresada aquí para una configuración web simple. La configuración de la interfaz de usuario web simple difiere de la interfaz de usuario web completa que se ve cuando se inicia sesión con la contraseña de administrador.
Contraseña	Introduce la contraseña. La longitud máxima de la contraseña es de 31 caracteres.
confirmar Contraseña	Introduzca la contraseña de nuevo para la verificación.
seguridad de la contraseña	Muestra el nivel de seguridad de la contraseña especificada anteriormente.
Establecer como predeterminado de fábrica	Haga clic para volver a la configuración predeterminada de fábrica.

Hacer clic**DE ACUERDO**para guardar los cambios en la página y se le dirigirá a la pantalla de inicio de sesión. Aparecerá una ventana. Inicie sesión con la nueva contraseña.

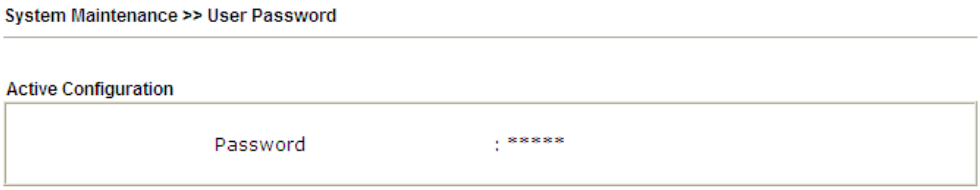
Estos son los pasos necesarios para configurar el enrutador para el acceso en modo de usuario:

1. Navegue hasta**Mantenimiento del sistema>>Contraseña de usuario**en la interfaz de usuario web.

2. Marque la casilla de**Habilite el modo de usuario para una configuración web simple**n para habilitar la operación en modo usuario. Introduzca una nueva contraseña en el campo Contraseña y haga clic en Aceptar.

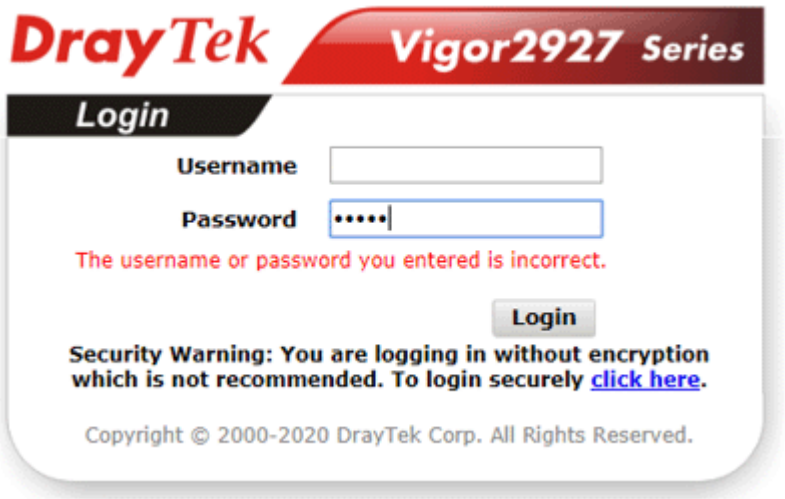


3. Aparecerá la siguiente pantalla. Hacer clic**DE ACUERDO**.

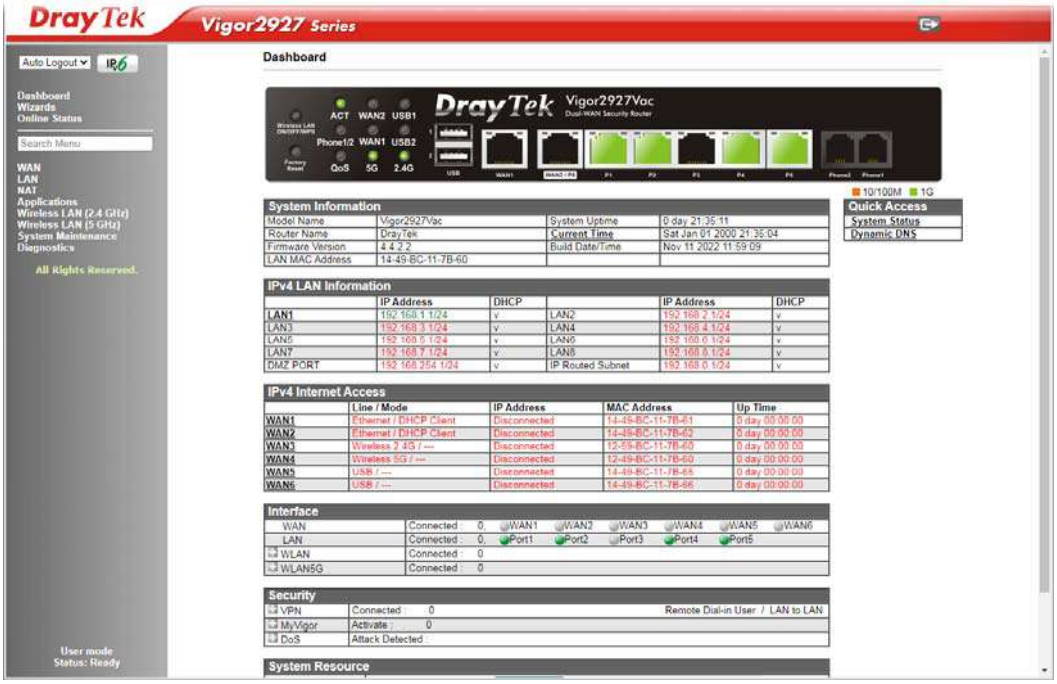


4. Cierre sesión en la interfaz de usuario web del enrutador Vigor haciendo clic en el botón Cerrar sesión.

5. Se mostrará la siguiente ventana. Introduzca la nueva contraseña de usuario en el**Contraseña**campo y haga clic**Acceso**.



6. La pantalla principal con el modo de usuario se mostrará de la siguiente manera:



Solo la configuración básica está disponible en el modo de usuario. Estos son un subconjunto de la configuración del modo de administración.

Información	La configuración en el modo de usuario se puede configurar de la misma manera que en el modo de administrador.

Cuando desee acceder a la interfaz de usuario web del enrutador Vigor, el sistema le pedirá que proporcione primero el nombre de usuario y la contraseña. En ese momento, el fondo de la página web está en blanco y no se mostrará ningún encabezado en la ventana de inicio de sesión. Esta página le permite especificar la URL de inicio de sesión y el encabezado de la ventana de inicio de sesión si tiene dicho requisito.

Esta sección le permite personalizar la página de inicio de sesión agregando un mensaje y/o configurando el título de la página.

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Logotipo de la página de inicio de sesión	Establezca una imagen que se mostrará encima de la ventana de inicio de sesión. **Por defecto -**El**Habilitar saludo**La función está disponible para establecer el título de la página de inicio de sesión. **Blanco -**Sin imagen / sin saludo. **Cargar un archivo -**Elija un archivo de imagen y haga clic en Cargar. Más tarde, la imagen seleccionada se mostrará en la ventana de inicio de sesión.
Habilitar saludo	Marque esta casilla para habilitar la función de personalización de inicio de sesión.
Título de la página de inicio de sesión	Ingrese una breve descripción (p. ej., Bienvenido a DrayTek) que se mostrará en el encabezado del cuadro de diálogo de inicio de sesión.
mensaje de bienvenida y Boletín	Ingrese palabras u oraciones aquí. Se mostrará para el mensaje de boletín. Además, se puede mostrar en el cuadro de diálogo de inicio de sesión en la parte inferior. Tenga en cuenta que no ingrese el enlace de redirección de URL aquí.
Avance	Haga clic para obtener una vista previa de la ventana de inicio de sesión personalizada según la configuración ingresada en esta página.
Establecer como predeterminado de fábrica	Haga clic para volver a la configuración predeterminada de fábrica.

A continuación se muestra un ejemplo de una página de inicio de sesión personalizada con los valores ingresados en el**Título de la página de inicio de sesión**y**Mensaje de Bienvenida y Boletín**campos.

Welcome Message

This welcome message is displayed in the Login page of the router. Replace this text with your own message.

1. The welcome message can be written in HTML so lists such as this one can be created
2. Other markup tags such as p, font or img can be used

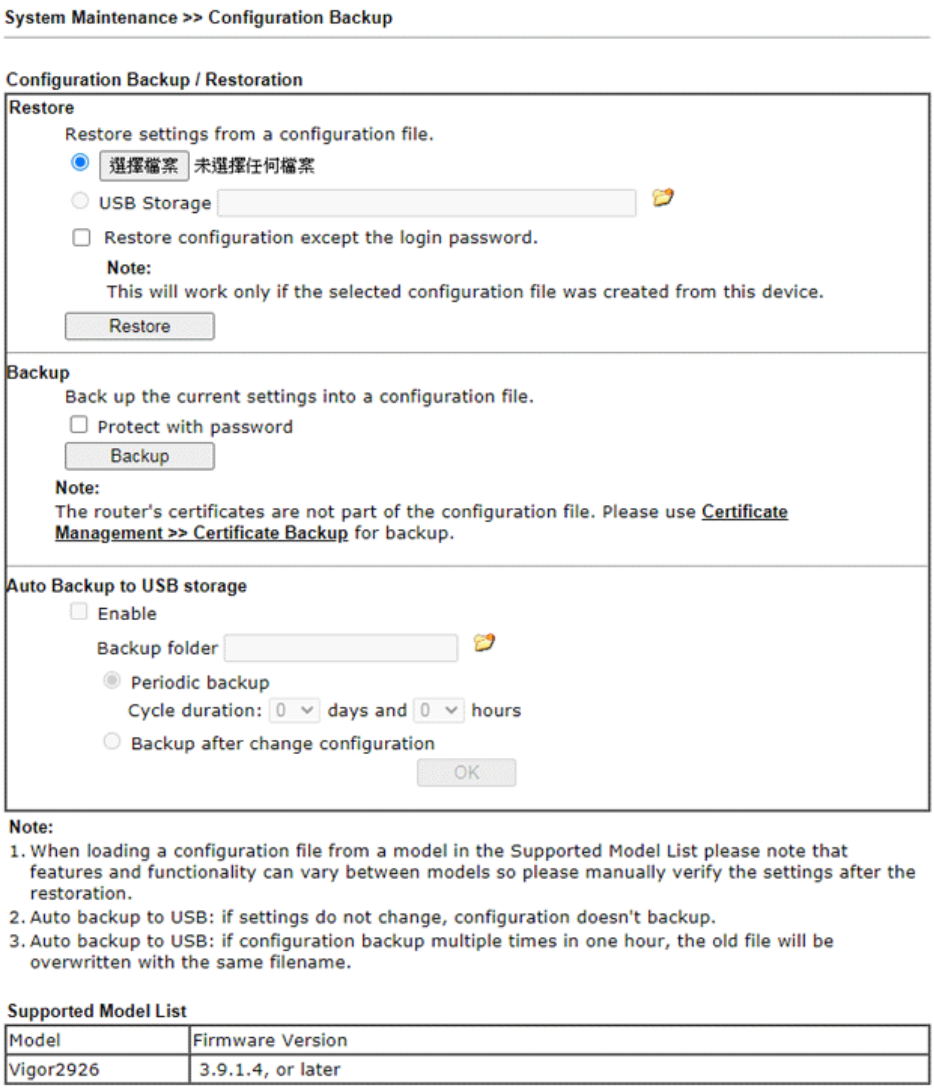
VII-1-7 Copia de seguridad de la configuración

Esta función permite la copia de seguridad y la restauración de la configuración del enrutador. Además de restaurar la copia de seguridad de configuración propia de Vigor2927, es posible restaurar copias de seguridad de ciertos enrutadores DrayTek como las series Vigor2820, Vigor2830 y Vigor2850 en Vigor2927.

Copia de seguridad de la configuración

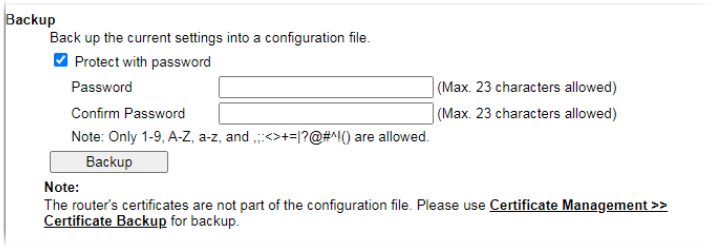
Siga los pasos a continuación para hacer una copia de seguridad de su configuración.

1. Ir a**Mantenimiento del sistema**>>**Copia de seguridad de la configuración**. Se mostrará la siguiente página.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Restaurar	**Restaurar ajustes desde un archivo de configuración**–Haga clic en el**Seleccione Archivo**para especificar un archivo a restaurar o haga clic en**Almacenamiento USB**(si hay un disco de almacenamiento USB conectado) para elegir el archivo de configuración. **Restaurar configuración excepto la contraseña de inicio de sesión**–Seleccione para excluir la contraseña de la restauración de la copia de seguridad. **Restaurar**-Haga clic para iniciar la restauración de la configuración. Si el

	el archivo de respaldo está encriptado, se le pedirá que ingrese la contraseña.
Respaldo	Haga clic en él para realizar la copia de seguridad de la configuración de este enrutador. **Proteger con contraseña-**Seleccione para cifrar la copia de seguridad con una contraseña. Se le pedirá que ingrese la contraseña como se muestra a continuación:  - **Contraseña**–Introduzca una nueva contraseña para cifrar el archivo de configuración. - **confirmar Contraseña**–Ingrese la nueva contraseña nuevamente para confirmar. **Respaldo**-Haga clic para iniciar el proceso de copia de seguridad.
Copia de seguridad automática en almacenamiento USB	La configuración se puede almacenar en un USB conectado al enrutador Vigor como respaldo. **Permitir**-Marque la casilla para habilitar la función. **carpeta de copia de seguridad**–Establezca la ruta para la descarga. **Copia de seguridad periódica** –Establezca la duración del círculo para la copia de seguridad. **Copia de seguridad después de cambiar la configuración**–La copia de seguridad se ejecutará cada vez que se cambie la configuración.

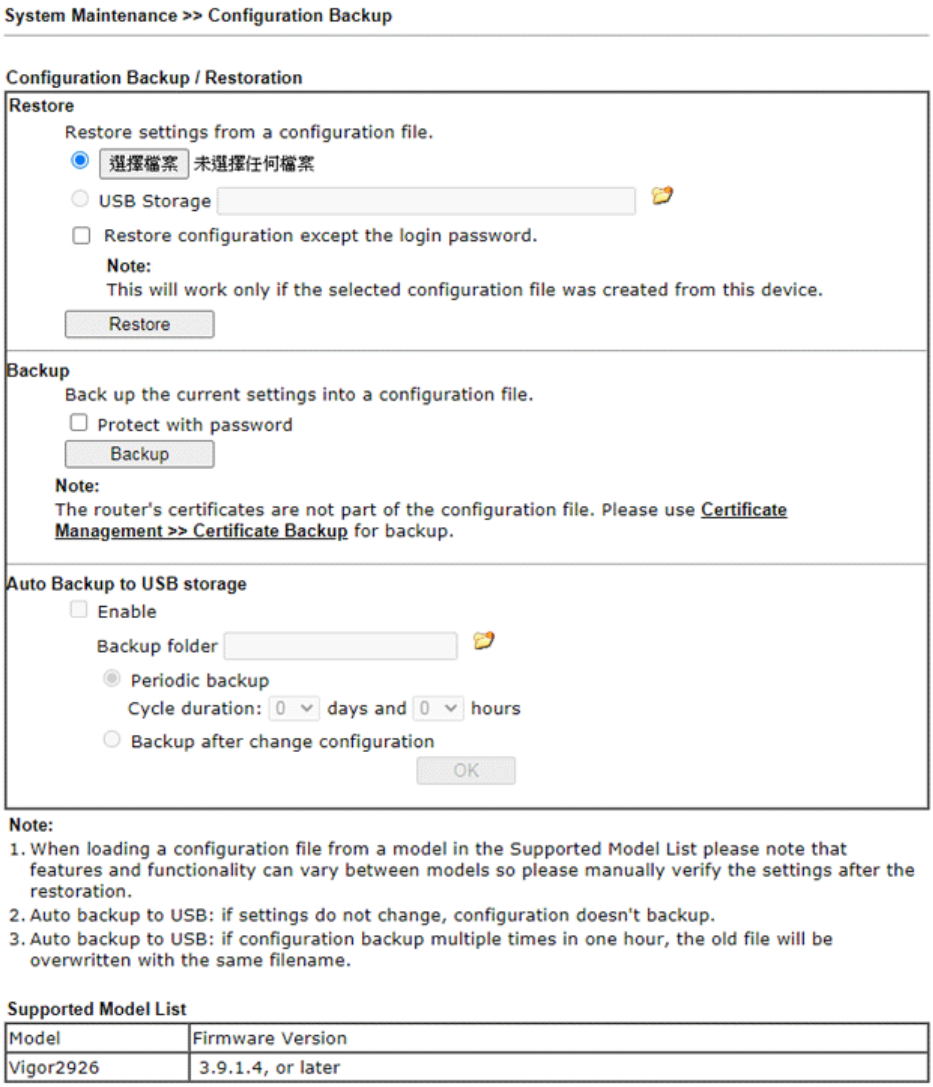
2. Haga clic en el**Respaldo**y se mostrará el cuadro de diálogo Descargar archivo. Dependiendo de su navegador, se le puede pedir que seleccione una ubicación para guardar el archivo, o el archivo se puede guardar en la ubicación de descarga predeterminada de su navegador.TLa configuración se descargará automáticamente a su computadora como un archivo llamado**config.cfg**.

El ejemplo anterior está usando**ventanas**plataforma para demostrar ejemplos. El**Mac**o**linux** plataforma aparecerán diferentes ventanas, pero la función de copia de seguridad todavía está disponible.

Información	La copia de seguridad de la configuración no incluye certificados almacenados en el enrutador. Haga una copia de seguridad de los certificados por separado yendo a**Gestión de certificados > > Copia de seguridad del certificado**.

Restauración de la configuración

1. Ir a**Mantenimiento del sistema**>>**Copia de seguridad de la configuración**. Se mostrarán las siguientes ventanas.

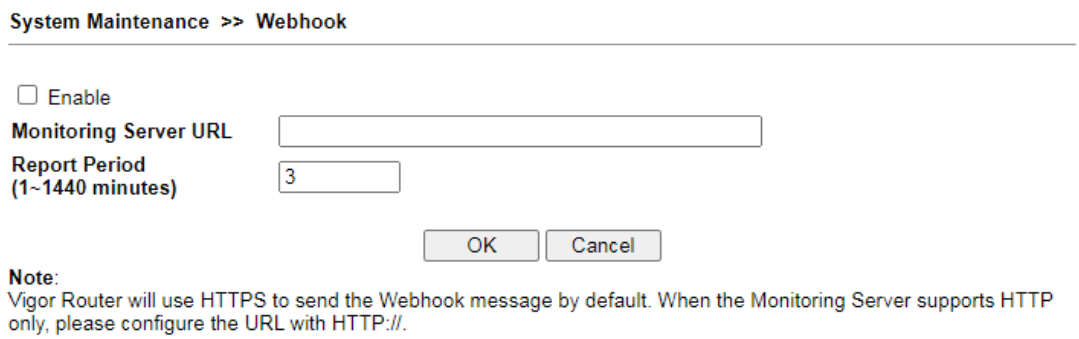


2. Haga clic en el**Elija el archivo**botón debajo**Respaldo**para abrir el cuadro de diálogo de archivo abierto para seleccionar el archivo de configuración que se va a cargar y restaurar.

3. Haga clic en el**Restaurar**y espere unos segundos.

Webhook VII-1-8

El enrutador Vigor enviará un informe (mensaje de webhook) que incluye WAN arriba, abajo, uso de CPU, uso de memoria, etc. a un servidor de monitoreo periódicamente.



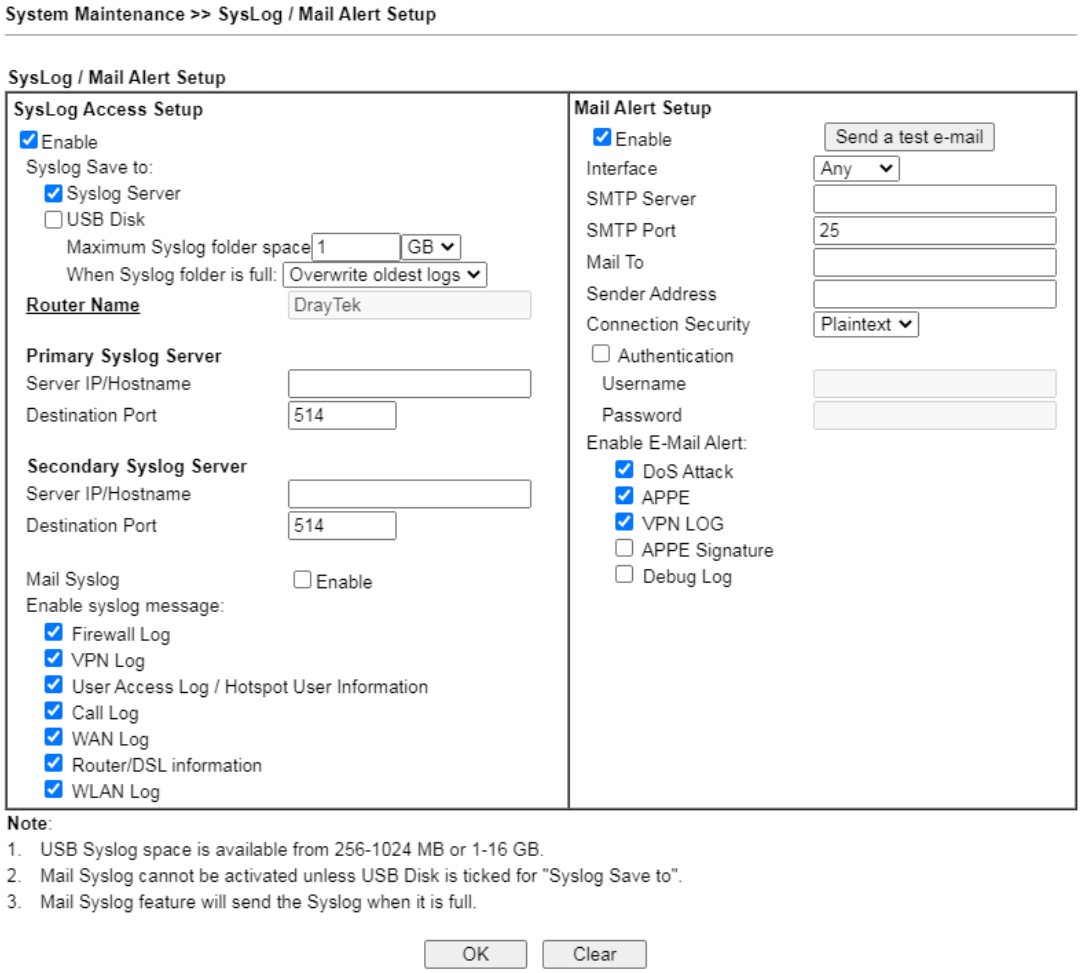
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Selecciónelo para habilitar esta función.
URL del servidor de supervisión	Introduzca la URL de un servidor.
Período de informe	Defina el tiempo de intervalo para que se envíe cada informe.

Seleccionar**DE ACUERDO**para guardar los cambios en la página.

VII-1-9 Syslog/Alerta de correo

La función SysLog se proporciona para que los usuarios supervisen el enrutador.



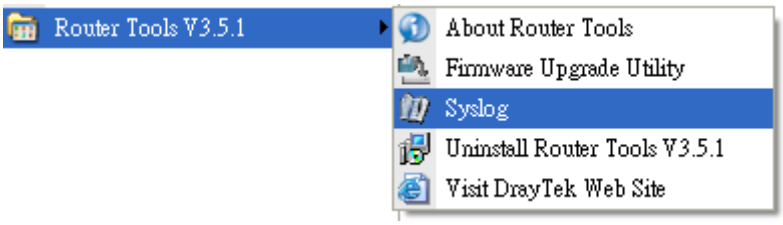
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Configuración de acceso a SysLog	**Permitir**-Seleccione para habilitar la función Syslog. **Registro del sistema** **Guardar en**–Compruebe el servidor Syslog y/o el disco USB. - **Servidor Syslog**–Los eventos se enviarán a un servidor Syslog. - **Disco USB**–Los eventos se guardarán en un dispositivo de almacenamiento USB conectado al enrutador. - **Espacio máximo de carpeta Syslog**-Establezca un espacio (unidad GB/MB) para almacenar registros de eventos. - **Cuando la carpeta Syslog está llena**-Especifique la acción (sobrescribir los registros más antiguos o detener el registro) que se ejecutará.
Nombre del enrutador	Muestra el nombre del enrutador configurado en**Mantenimiento del Sistema >> Gestión**. Este nombre se utilizará para identificar el enrutador en las entradas de Syslog. Para establecer o modificar el nombre del enrutador, haga clic en el hipervínculo y se le llevará a**Mantenimiento del Sistema >> Gestión**dónde

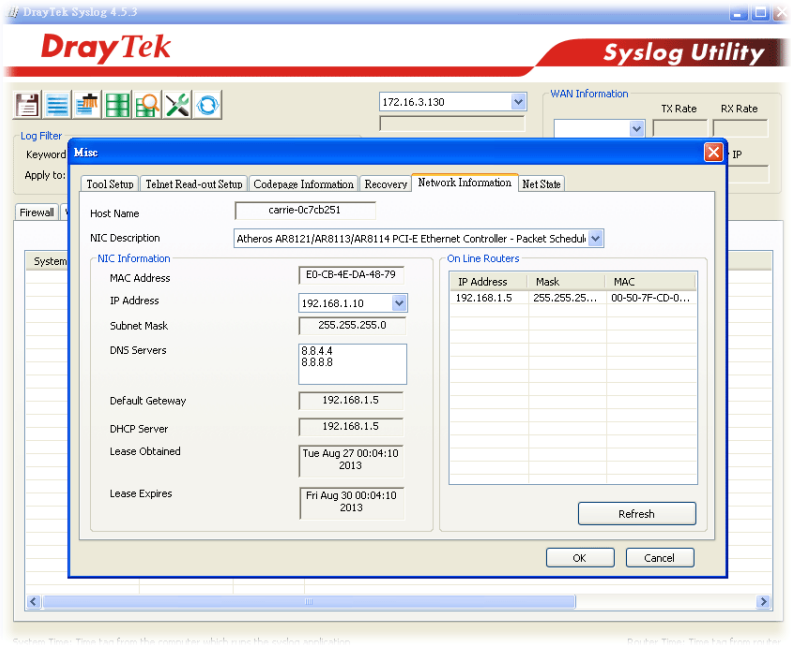
	puede ingresar el valor.
Servidor Syslog primario / Servidor Syslog secundario	**Servidor Syslog primario / Servidor Syslog secundario -**El enrutador Vigor enviará los datos al servidor Syslog para su análisis según la configuración del servidor configurada aquí. Puede enviar a ambos servidores simultáneamente si se configuran servidores primarios y secundarios; o enviar a cualquiera de los servidores que se han configurado aquí. **IP del servidor/nombre de host -**La dirección IP o el nombre de host del servidor Syslog. **Puerto de destino -**Asigne un puerto para el protocolo Syslog. **Registro del sistema de correo:**Marque la casilla para recodificar el evento de correo en Syslog. **Habilitar mensaje de syslog -**Marque la casilla que aparece en esta página web para enviar el mensaje correspondiente de firewall, VPN, acceso de usuario, llamada, WAN, información de enrutador/DSL a Syslog.
Configuración de alerta de correo	**Permitir**-Seleccione para habilitar la alerta de correo. **Enviar un correo electrónico de prueba -**Haga clic para enviar un mensaje de correo electrónico de prueba usando la configuración a continuación. **Interfaz**-Especifique la interfaz WAN para el paso de un correo. **Servidor SMTP**-Introduzca la dirección del servidor SMTP utilizado para enviar correos electrónicos. **Puerto SMTP-**Introduzca el puerto del servidor SMTP. La configuración predeterminada es 25. **Enviar a -**Introduzca la dirección de correo electrónico del destinatario. **Dirección del remitente -**Introduzca la dirección de correo electrónico del remitente. **Seguridad de conexión**-Seleccione un método (Texto sin formato, SSL o StartTLS) para garantizar la seguridad de la conexión. SSL significa usar el puerto 465 para el servidor SMTP porque algunos servidores de correo electrónico usan https como método de transmisión. - Acepte el uso de texto sin formato si falla la conexión StartTLS. - Forzar inicio de TLS. Deténgase si falla la conexión StartTLS. **Autenticación -**Seleccione esta casilla de verificación e ingrese el nombre de usuario y la contraseña si el servidor SMTP requiere autenticación. - **Nombre de usuario -**Introduzca el nombre de usuario para la autenticación. - **Contraseña -**Introduzca la contraseña para la autenticación. **Habilitar alerta de correo electrónico -**Seleccione los tipos de eventos que activarán las alertas por correo electrónico.

Seleccionar**DE ACUERDO**para guardar los cambios en la página, o**Claro**para restablecer todas las configuraciones a los valores predeterminados de fábrica. Para ver el mensaje de Syslog, siga los pasos a continuación:

1. En el**Configuración de Syslog/Alerta de correo**pantalla, ingrese la dirección IP de la PC del monitor en el**Dirección IP del servidor**campo.
2. Instale las herramientas del enrutador desde el sitio web de DrayTek. Después de la instalación, inicie Syslog haciendo clic en**Herramientas de enrutador>>Syslog**en el menú Inicio de Windows.

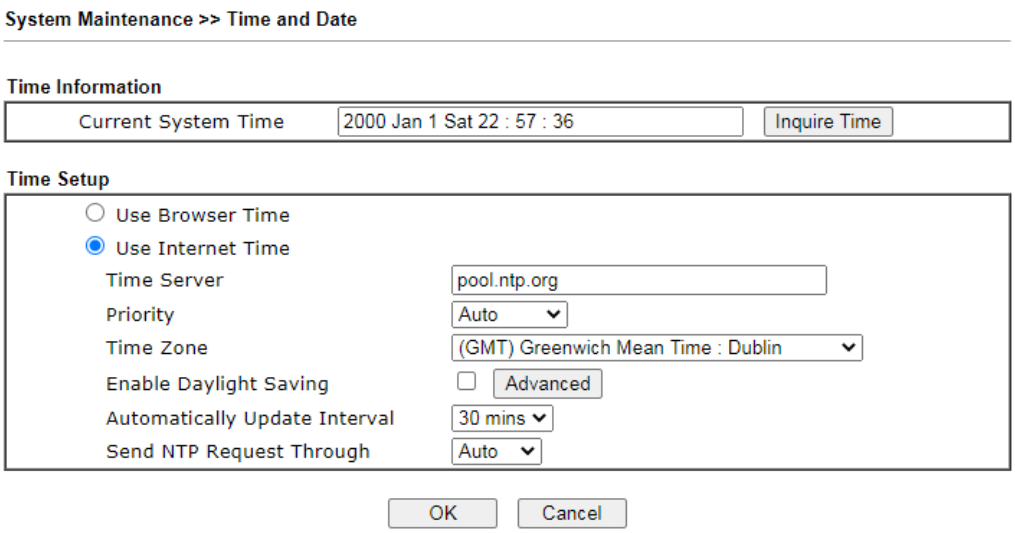


3. En la aplicación Syslog, seleccione el enrutador que desea monitorear. Recuerde seleccionar el adaptador de red que se usará para conectarse al enrutador en Información de red, de lo contrario, el tráfico de Syslog no se puede recibir desde el enrutador.

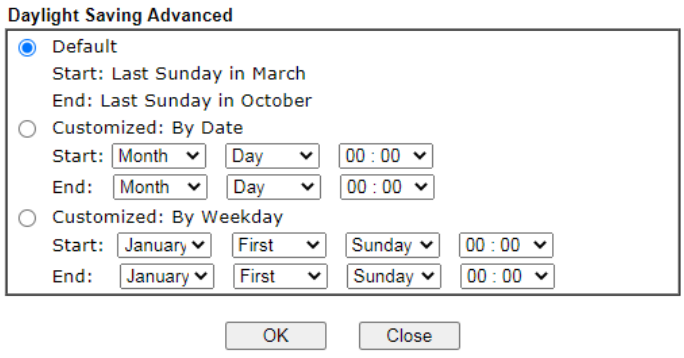


VII-1-10 Hora y fecha

Esta sección le permite configurar los ajustes relacionados con la fecha y la hora del sistema.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Hora actual del sistema	Hacer clic**Consultar tiempo**para recuperar la hora actual del servidor horario.
Usar la hora del navegador	Seleccione esta opción para permitir que el enrutador establezca la hora del sistema usando la hora informada por el navegador web.
Usar tiempo de Internet	Seleccione esta opción para permitir que el navegador configure la hora de su sistema recuperando la información de la hora del servidor de hora de la red especificado usando el Protocolo de hora de la red (NTP).
Servidor de tiempo	Introduzca la dirección del servidor horario.
Prioridad	Seleccionar**Auto**o**IPv6 primero**como la prioridad.
Zona horaria	Seleccione la zona horaria donde se encuentra el enrutador.
Habilitar Horario de Verano	Marque la casilla para habilitar el horario de verano (DST) si es aplicable a su ubicación. **Avanzado**–Haga clic para ingresar un horario personalizado para habilitar el horario de verano.  Utilice la configuración de tiempo predeterminada o establezca el tiempo definido por el usuario para sus necesidades. **Por defecto**–Utiliza el programa DST predeterminado para la zona horaria.

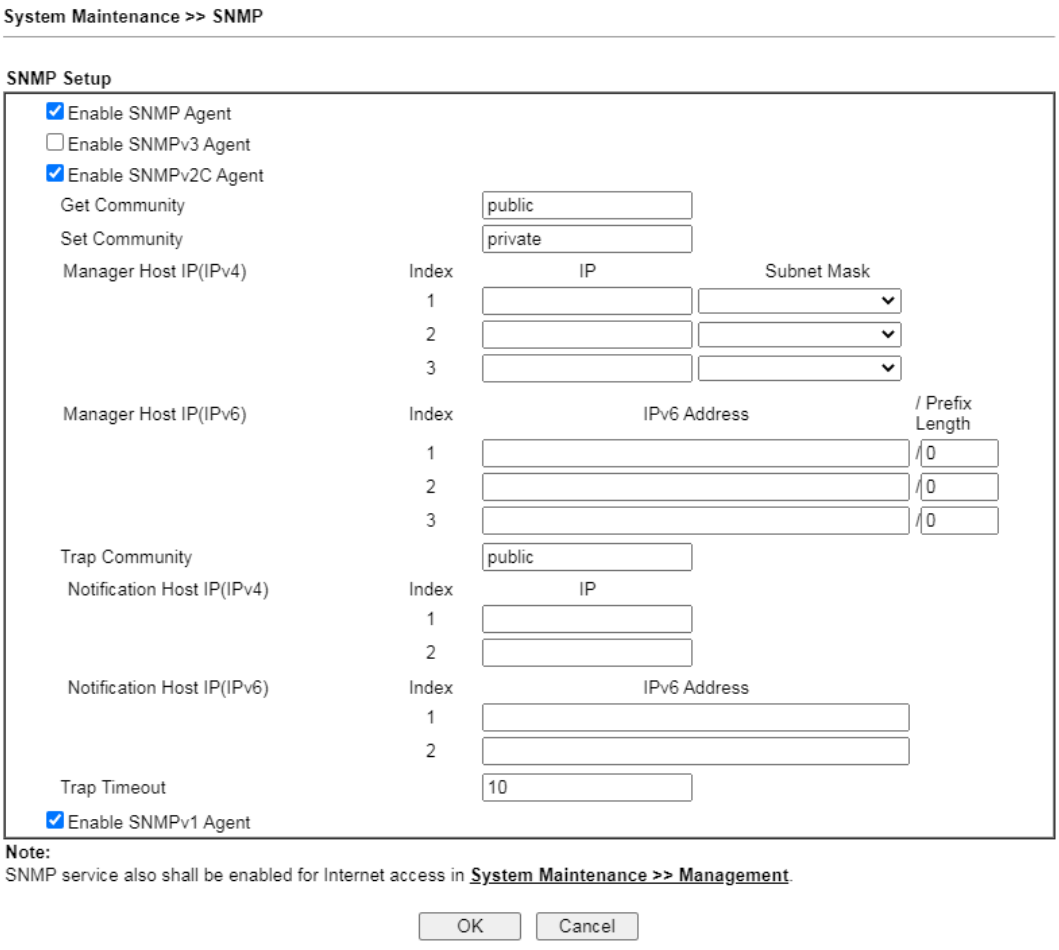
	Rango de fechas–Seleccione esta opción si el horario de verano comienza y finaliza en fechas fijas. **Anual**–Seleccione esta opción si el horario de verano comienza y termina en ciertos días de la semana.
Actualizar automáticamente Intervalo	Seleccione el intervalo de tiempo en el que el enrutador actualiza la hora del sistema.
Enviar solicitud NTP A través de	Especifique una interfaz WAN para enviar una solicitud NTP para sincronización de tiempo.

Seleccionar**DE ACUERDO**para guardar los cambios en la página, o**Cancelar**para descartar los cambios sin guardar.

VII-1-11 SNMP

Esta sección le permite configurar los ajustes para los servicios SNMP y SNMPv3.

SNMPv3 es más seguro que SNMP mediante el uso de cifrado (admite AES y DES) y autenticación (admite MD5 y SHA) para las necesidades de administración.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar agente SNMP	Marque para habilitar la función SNMP. Luego, habilite el Agente SNMPv3 / Agente SNMPv2C / Agente SNMPv1.
Obtener comunidad	Introduzca la cadena Obtener comunidad. La configuración predeterminada es **público**. Los dispositivos que envían solicitudes para recuperar información usando comandos get deben pasar el Get Community correcto.

	cadena. La longitud máxima permitida es de 23 caracteres.
Establecer comunidad	Introduzca la cadena Establecer comunidad. La configuración predeterminada es **privado**. Los dispositivos que envían solicitudes para cambiar la configuración mediante los comandos set deben pasar la cadena Set Community correcta. La longitud máxima del texto es de 23 caracteres.
IP del host del administrador (IPv4)	Ingrese la dirección IPv4 de los hosts que pueden emitir comandos SNMP. Si este campo se deja en blanco, cualquier host de LAN IPv4 puede emitir comandos SNMP.
IP del host del administrador (IPv6)	Ingrese la dirección IPv6 de los hosts que pueden emitir comandos SNMP. Si este campo se deja en blanco, cualquier host de LAN IPv6 puede emitir comandos SNMP.
Comunidad trampa	Ingrese la cadena Trap Community. La configuración predeterminada es pública. Los dispositivos que envían mensajes no solicitados a la consola SNMP deben pasar la cadena Trap Community correcta. La longitud máxima del texto es de 23 caracteres.
IP del host de notificación (IPv4)	Ingrese la dirección IPv4 de los hosts a los que se les permite enviar trampas SNMP.
IP del host de notificación (IPv6)	Ingrese la dirección IPv6 de los hosts a los que se les permite enviar trampas SNMP.
Tiempo de espera de trampa	La configuración predeterminada es de 10 segundos.
Habilitar agente SNMPV3	Marque para habilitar la función SNMPV3.
Usuario USM	USM significa modo de seguridad basado en el usuario. Introduzca el nombre de usuario que se utilizará para la autenticación. La longitud máxima permitida es de 23 caracteres.
Algoritmo de autenticación	Elija uno de los métodos hash que se utilizará con el algoritmo de autenticación.
Contraseña de autenticación	Introduzca una contraseña para la autenticación. La longitud máxima permitida es de 23 caracteres.
Algoritmo de privacidad	Elija un método de cifrado como algoritmo de privacidad.
Contraseña de privacidad	Introduzca una contraseña para la privacidad. La longitud máxima permitida es de 23 caracteres.

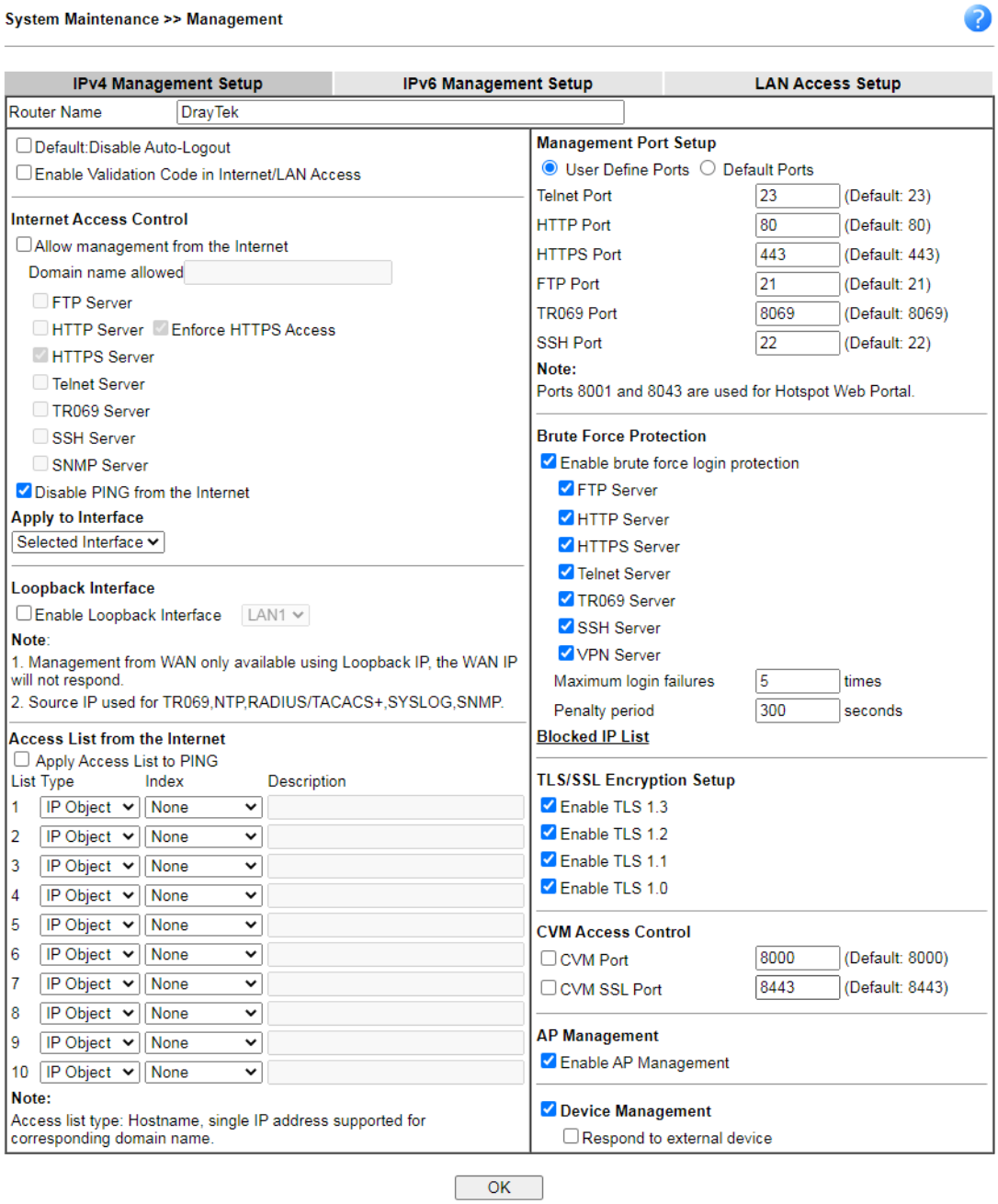
Seleccionar**DE ACUERDO**para guardar los cambios en la página, o**Cancelar**para descartar los cambios sin guardar.

Gestión VII-1-11

Esta página le permite administrar la configuración de Control de acceso a Internet/LAN, Lista de acceso desde Internet, Configuración del puerto de administración, Configuración de cifrado TLS/SSL, Control de acceso CVM y Administración de dispositivos.

La configuración de administración para IPv4 e IPv6 se encuentra en páginas de pestañas separadas.

Configuración de la gestión de IPv4



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre del enrutador	Ingrese el nombre del enrutador proporcionado por el ISP.

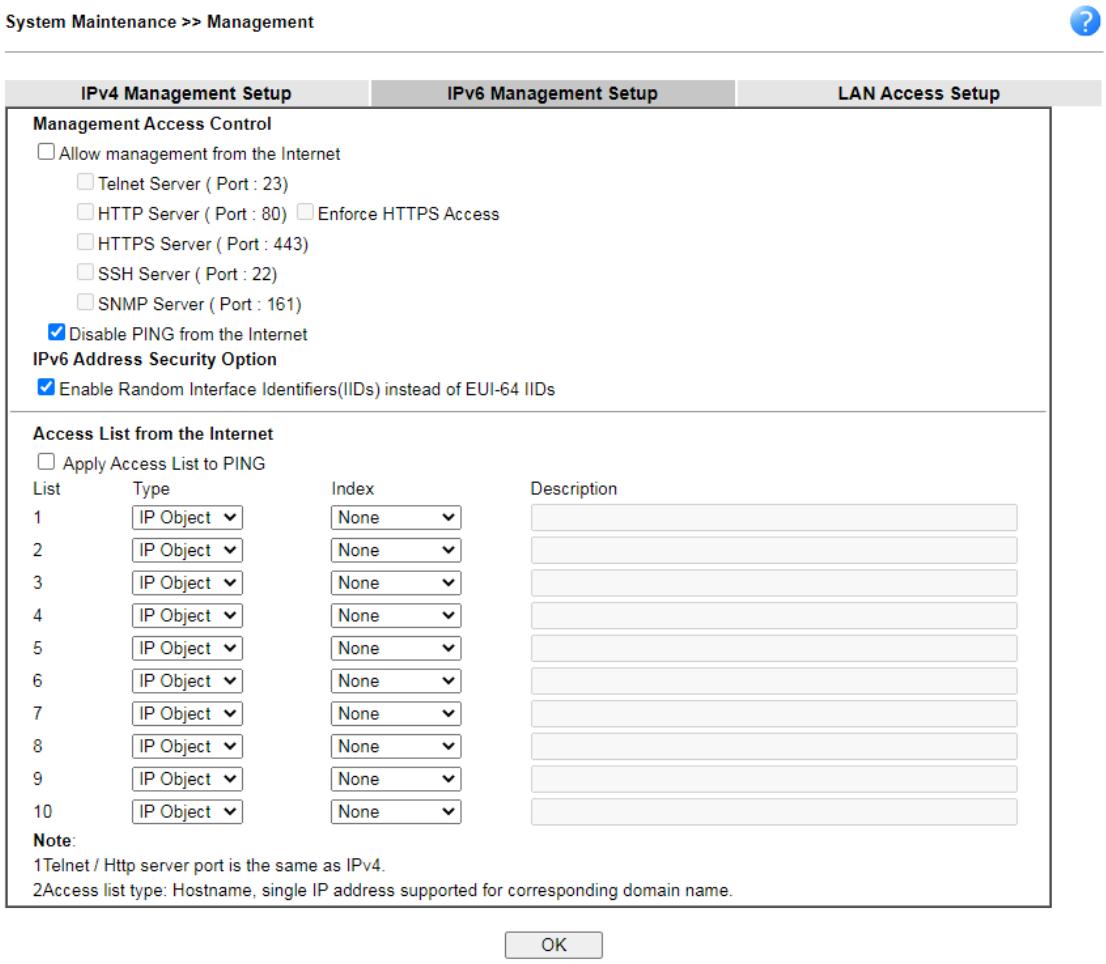
Predeterminado: Deshabilitar **Cierre de sesión automático**	Si está habilitado, la función de cierre de sesión automático para la interfaz de usuario web estará deshabilitada. La interfaz de usuario web no finalizará hasta que haga clic manualmente en el icono Cerrar sesión.
Habilitar código de validación en acceso a Internet/LAN	Si está habilitado, el enrutador Vigor requerirá que los usuarios ingresen un código de validación como se muestra en una imagen cuando inicien sesión.
Control de acceso a Internet	**Permitir la gestión desde Internet**-Active la casilla de verificación para permitir que los administradores del sistema inicien sesión desde Internet y luego seleccione los servicios específicos que se pueden administrar de forma remota. **nombre de dominio permitido**–Esta configuración solo está disponible si el filtrado de DNS está habilitado, aplicando el perfil de filtro de DNS en las reglas del firewall o habilitando la configuración local del filtro de DNS. El enrutador solo permitirá conexiones a WebUI usando direcciones de dominio configuradas en perfiles DDNS o en esta sección. Si el filtrado de DNS está deshabilitado, esta configuración se deshabilitará y cualquier dirección de dominio que se resuelva en la dirección IP de WAN del enrutador se puede usar para conectarse a WebUI. **Deshabilitar PING desde Internet -**Seleccione para rechazar todos los paquetes PING de Internet. Para mayor seguridad, esta configuración está habilitada de forma predeterminada. **Aplicar a la interfaz**-Permita que el usuario acceda al enrutador a través de las interfaces WAN seleccionadas.
Interfaz de bucle invertido	Una interfaz loopback es una interfaz virtual lógica creada en un enrutador que simula una interfaz real. Esto se puede usar para conectarse a servicios de administración como Web (HTTPS), SNMP, ACS (TR069), Syslog o SSH, así como a servicios de autenticación como TACACS+ o RADIUS en lugar de usar una IP de LAN. Para la función de autenticación, el uso de la dirección de bucle invertido dedicada reducirá la sobrecarga administrativa, ya que no es necesario agregar varias direcciones IP de enrutador al servidor AAA. Además, se mejorará la seguridad al aislar la autenticación de la red del usuario. El uso de una dirección de loopback significa que la interfaz virtual siempre está activa, especialmente cuando el CPE tiene múltiples interfaces WAN. Por ejemplo, si BGP conectado en WAN1 está inactivo, la administración y el tráfico AAA se pueden enrutar a la interfaz de bucle invertido definida a través del túnel VPN conectado en WAN2. Otro beneficio es que la IP de loopback puede ser una dirección IP (con una máscara de 32 bits). Esto significa que la interfaz no está asignada a ningún puerto LAN, lo que mejora la seguridad y ahorra mucho espacio de direcciones IP. Podemos imaginar que si asignamos IP de máscara de 24 bits a muchos enrutadores administrados, habrá IP de red insuficientes.

	Habilitar interfaz de bucle invertido -Seleccione para habilitar la función de la interfaz de bucle invertido. **LAN#**- Seleccione una subred LAN como interfaz de bucle invertido.
Lista de acceso desde Internet	La capacidad de los administradores del sistema para iniciar sesión en el enrutador se puede restringir a hasta 10 hosts o redes específicos. **Aplicar lista de acceso a PING**–Cuando esta opción está marcada y **Deshabilitar PING desde Internet**está desmarcada, los pings que se originan en Internet solo se aceptarán si provienen de una de las direcciones IP y/o máscaras de subred que se especifican a continuación. Esta opción no tiene efecto si**Deshabilitar PING desde Internet**está marcado, lo que bloquea todos los pings de Internet. **Tipo**-Seleccionar**Objeto IP**. **Índice**-Seleccione el número de índice de un objeto IP configurado. **Descripción**-Muestra un breve comentario para el objeto IP seleccionado (con máscara de subred).
Configuración del puerto de administración	**Puertos definidos por el usuario -**Marque para especificar números de puerto definidos por el usuario para los servidores Telnet, HTTP, HTTPS, FTP, TR-069 y SSH. **Puertos predeterminados -**Marque para usar números de puerto estándar para los servidores.
Protección de fuerza bruta	A cualquier cliente que intente acceder a Internet a través del enrutador Vigor se le pedirá que pase por la autenticación de usuario. Esta función puede evitar que el enrutador Vigor sea atacado cuando un hacker prueba todas las combinaciones posibles de letras, números y símbolos hasta encontrar la combinación correcta de contraseña. **Habilite la protección de inicio de sesión de fuerza bruta –**Seleccione para habilitar la detección de intentos de inicio de sesión de fuerza bruta. **Máxima falla de inicio de sesión:**Especifique el número máximo de intentos fallidos de inicio de sesión antes de que se bloqueen más inicios de sesión. **Período de penalización –**Configure el tiempo de bloqueo después de que se haya excedido el número máximo de intentos de inicio de sesión. El usuario no podrá intentar iniciar sesión hasta que haya pasado el tiempo especificado. **Lista de IP bloqueadas –**Muestre, en una nueva ventana del navegador, las direcciones IP que actualmente están bloqueadas para iniciar sesión en el enrutador.
Configuración de cifrado TLS/SSL	**Habilitar TLS 3.0/1.0/1.1/1.2/1.3 –**Marque la casilla para habilitar los protocolos de cifrado TLS 3.0/1.0/1.1/1.2/1.3. Para mejorar la seguridad, los servidores HTTPS y SSL VPN integrados en el enrutador se actualizaron al protocolo TLS 1.x. Si está utilizando un navegador web antiguo (por ejemplo, IE 6.0) o una versión antigua del cliente SmartVPN, es posible que deba habilitar SSL 3.0 para conectarse al enrutador. Sin embargo, se recomienda que, en su lugar, actualice su navegador web o cliente SmartVPN a una versión compatible con los protocolos TLS que son mucho más seguros que SSL.
Control de Acceso CVM	**Puerto CVM –**Marque la casilla para habilitar la configuración del puerto de administración de VPN central. **Puerto CVM SSL –**Marque la casilla para habilitar la configuración del puerto SSL de Central VPN Management.
Gestión de puntos de acceso	**Habilitar la gestión de puntos de acceso:**Marque para habilitar la función de administración del punto de acceso. Si no, los elementos del menú relacionados con**Central**

	Gestión>>APestará oculto.
Gestión de dispositivos	Marque para habilitar la función de administración de dispositivos. **Responder a un dispositivo externo –**Si se selecciona, Vigor2927 funcionará como un dispositivo esclavo. Cuando un dispositivo externo (dispositivo maestro) envía paquetes a Vigor2927 para intentar administrarlo, Vigor2927 responderá a la solicitud proveniente del dispositivo externo que puede administrar Vigor2927.

Seleccionar**DE ACUERDO**para guardar los cambios en la página.

Configuración de la gestión de IPv6



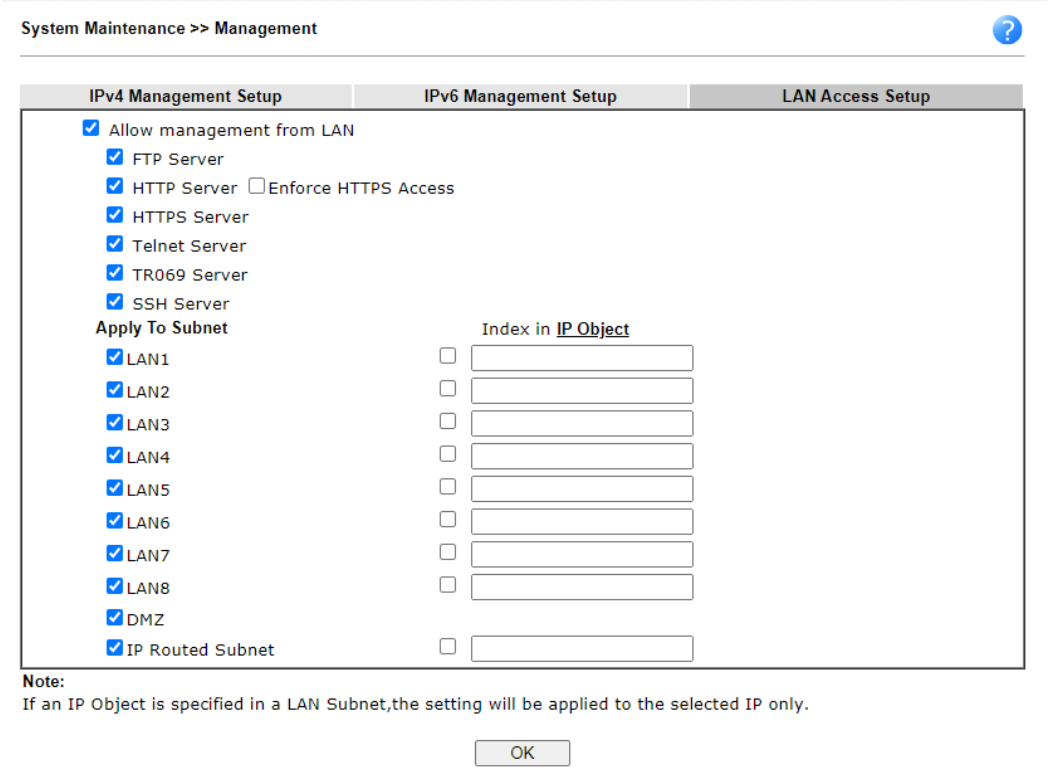
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Acceso de gestión Control	**Permitir la gestión desde Internet**-Marque para habilitar la función. Seleccione los servidores que los administradores del sistema pueden administrar desde Internet. **Deshabilitar PING desde Internet**-Marque para rechazar todos los paquetes PING de Internet. Para mayor seguridad, esta configuración está habilitada de manera predeterminada.
Seguridad de direcciones IPv6 Opción	**Habilitar identificadores de interfaz aleatorios (IID)... -**La dirección IPv6 se generará aleatoriamente, pero no se utilizará LAN/WAN MAC para evitar el ataque del hacker.
Lista de acceso desde Internet	Puede especificar que el administrador del sistema solo pueda iniciar sesión desde un host o red específicos definidos en la lista. Se permite un máximo de tres IP/máscaras de subred.

	Aplicar lista de acceso a PING–Cuando esta opción está marcada y **Deshabilitar PING desde Internet**está desmarcada, los pings que se originan en Internet solo se aceptarán si provienen de una de las direcciones IP y/o máscaras de subred que se especifican a continuación. Esta opción no tiene efecto si**Deshabilitar PING desde Internet**está marcado, lo que bloquea todos los pings de Internet. **Tipo**-Seleccionar**Objeto IP**o**nombre de host**. **Índice**-Seleccione el número de índice de un objeto IPv6 configurado.

Seleccionar**DE ACUERDO**para guardar los cambios en la página.

Configuración de acceso LAN



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir la gestión desde LAN	Active la casilla de verificación para permitir que los administradores del sistema inicien sesión desde la interfaz LAN. El sistema proporciona varios servidores que le permiten administrar el enrutador desde la interfaz LAN. Marque la(s) casilla(s) para especificar.
Aplicar a subred	Verifique la interfaz LAN para que el administrador la use para acceder a la interfaz de usuario web del enrutador Vigor. **Índice en Objeto IP** - Marque la casilla e ingrese el número de índice del perfil del objeto IP. Tenga en cuenta que el Tipo de dirección seleccionado para ese objeto IP no debe ser Cualquier dirección.

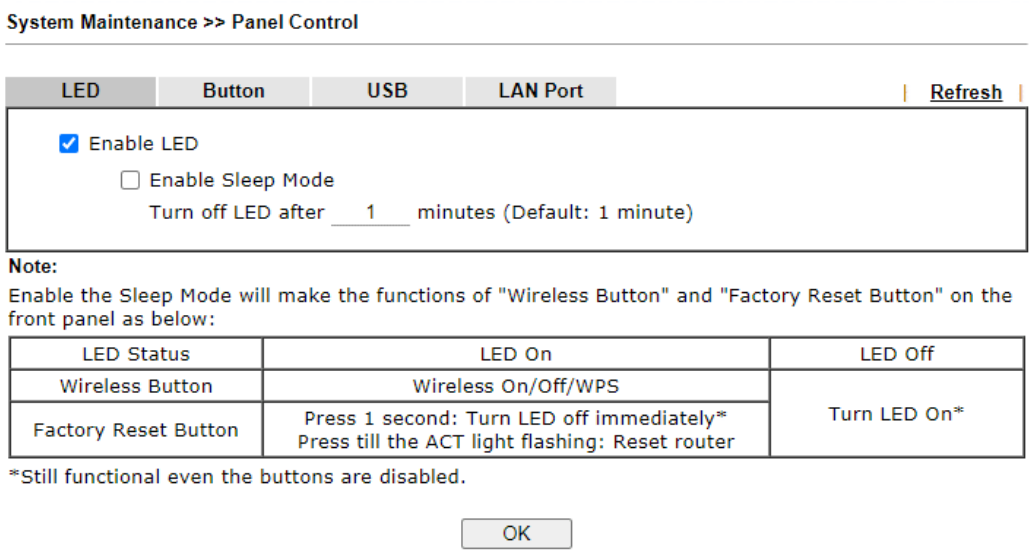
Seleccionar**DE ACUERDO**para guardar los cambios en la página.

VII-1-12 Panel de control

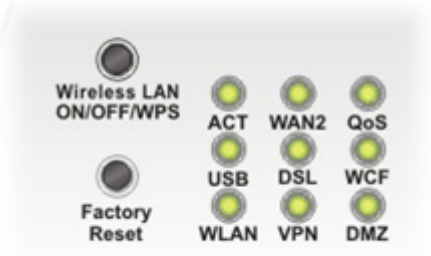
Puede personalizar el comportamiento de los LED, los botones, los puertos WLAN, USB y LAN en el panel frontal.

para LED

De forma predeterminada, los LED del panel frontal se iluminan o parpadean durante el funcionamiento para mostrar el estado de las diversas funciones del enrutador. Sin embargo, puede configurarlos para que permanezcan apagados en todo momento, o permanezcan apagados hasta que se presione un botón para despertarlos.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Actualizar	Haga clic para actualizar la página para mostrar la información más reciente.
LED de activación	Seleccione para permitir que los LED funcionen de acuerdo con los ajustes configurados. Anule la selección para desactivar los LED por completo.
Habilitar el modo de suspensión	Seleccione para permitir que el sistema apague los LED después de que haya transcurrido el número de minutos especificado. Cuando el modo de suspensión está habilitado, los LED se pueden activar presionando uno de los siguientes botones: - LAN inalámbrica ON/OFF/WPS en el panel frontal - Restablecimiento de fábrica en el panel frontal - Wake up LED en esta página de configuración 
Estado	Muestra el estado de los LED. Cuando se muestra lo siguiente, los LED están en modo de suspensión.

	Status : Sleep [Wake up LED] Para despertarlos, realice una de las siguientes acciones: - presione el**LED de despertador**en esta página presione el botón**Conexión** - **inalámbrica activada/desactivada/WPS**botón en el panel frontal - presione el**Restablecimiento de fábrica**botón en el panel frontal. Cuando se muestra lo siguiente, los LED están activos. **Status :** Awake, sleep after 1 minutes [LED sleep immediately] Para ponerlos a dormir inmediatamente, realice una de las siguientes acciones: - presione el**LED dormir inmediatamente**en esta página - presione el botón Factory Reset en el panel frontal
LED de despertador	Haga clic para reanudar el funcionamiento del LED después de que se hayan ido a dormir.

Seleccionar**DE ACUERDO**para guardar los cambios en la página.

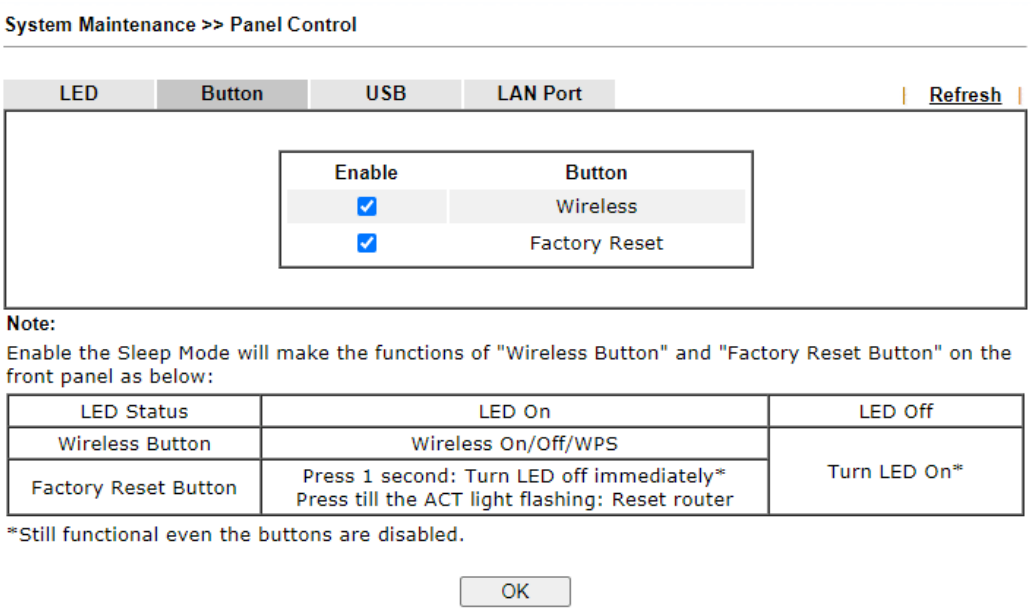
Para botón

Las funciones primarias de la**Restablecimiento de fábrica**y**Encendido/apagado inalámbrico/WPS**Los botones del panel frontal (restablecimiento a los valores predeterminados de fábrica y control inalámbrico, respectivamente) están habilitados de forma predeterminada, pero se pueden habilitar o deshabilitar según sea necesario.

Cuando el**Restablecimiento de fábrica**el botón está configurado para**Desactivado**, el enrutador no se puede restablecer durante el funcionamiento normal. Todavía se pueden usar otras funciones del botón de reinicio (como iniciar el servidor TFTP para cargar el firmware durante el encendido y controlar la iluminación de los LED del panel frontal cuando el modo de suspensión de LED está habilitado).

Cuando el**Encendido/apagado inalámbrico/WPS**el botón está configurado para**Desactivado**, el botón no se puede usar para encender o apagar la red inalámbrica, ni se puede usar para iniciar el proceso de emparejamiento WPS. Sin embargo, los LED del panel frontal se pueden activar cuando el modo de suspensión de LED está habilitado.

Haga clic en el**Botón**pestaña para obtener la página siguiente.



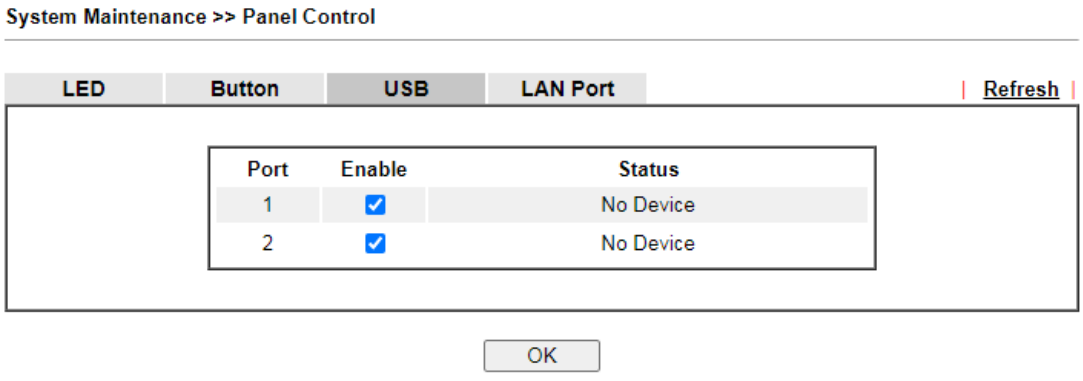
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Actualizar	Haga clic para actualizar la página para mostrar la información más reciente.
Habilitar restablecimiento de fábrica **Botón**	El valor predeterminado es**Activado**. Anule la selección para desactivar la función de reinicio del botón de reinicio de fábrica. Deshabilitar el botón Restablecimiento de fábrica solo evita que se use para reiniciar el enrutador Vigor con la configuración predeterminada. Todavía se puede usar para activar los LED cuando el modo de suspensión de LED está habilitado.
Habilitar botón inalámbrico	El valor predeterminado es**Activado**. Anule la selección para desactivar la capacidad del botón Inalámbrico para controlar las funciones WLAN y WPS. Deshabilitar el botón inalámbrico solo evita que se use para controlar las funciones de WLAN. Todavía se puede usar para activar los LED cuando el modo de suspensión de LED está habilitado.

Seleccionar**DE ACUERDO**para guardar los cambios en la página.

para USB

Los puertos USB se pueden habilitar o deshabilitar individualmente. Cuando un puerto USB está deshabilitado, el enrutador no reconocerá los dispositivos conectados.



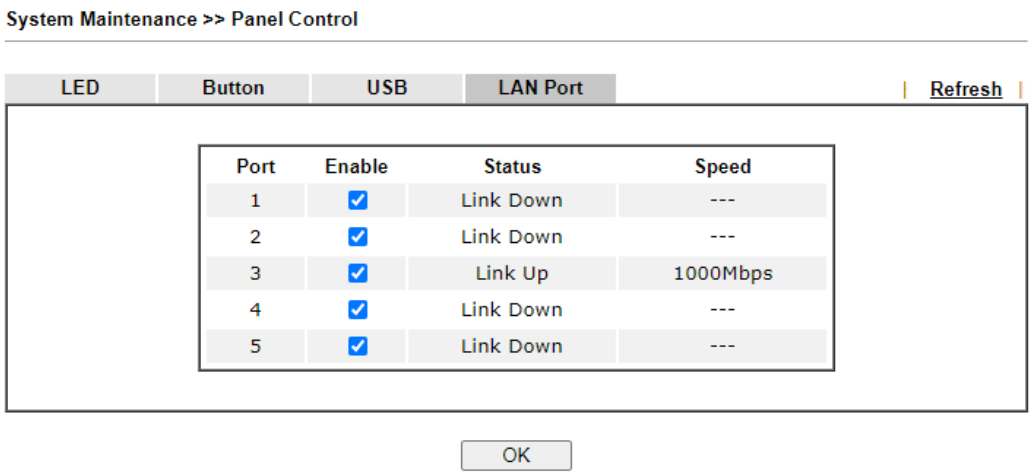
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Actualizar	Haga clic para actualizar la página para mostrar la información más reciente**.**
Puerto	El número corresponde al número de puerto USB que se muestra en el panel frontal.
Permitir	Anule la selección para desactivar el puerto USB. El valor predeterminado está habilitado.
Estado	Muestra el estado del puerto USB. **Sin dispositivo**–ningún dispositivo USB está conectado al puerto. **Conectado**–un dispositivo USB está conectado al puerto. **- - --** el puerto USB está deshabilitado.

Seleccionar**DE ACUERDO**para guardar los cambios en la página.

Para puerto LAN

Los 5 puertos LAN se pueden habilitar o deshabilitar individualmente. Cuando un puerto LAN está deshabilitado, el enrutador no reconocerá los dispositivos conectados.



Los ajustes disponibles se explican a continuación:

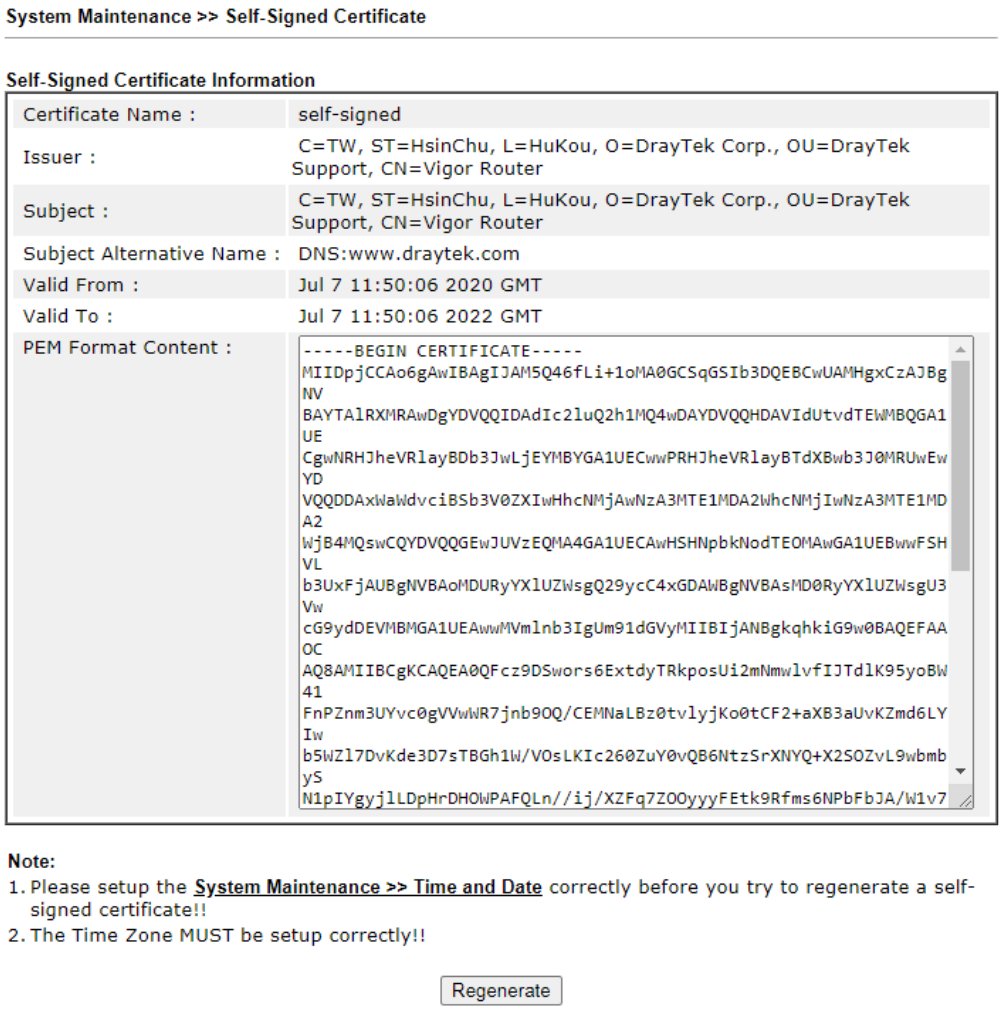
Artículo	Descripción
Actualizar	Haga clic para actualizar la página para mostrar la información más reciente.
Puerto	El número corresponde al número de puerto LAN que se muestra en el panel frontal.
Permitir	Anule la selección para deshabilitar el puerto LAN. El valor predeterminado está habilitado.
Estado	Muestra el estado del puerto USB. **Vincularse**–Un dispositivo Ethernet activo está conectado al puerto. **Enlace caído**–No se detecta ningún dispositivo Ethernet activo. **- - -** El puerto LAN está deshabilitado.
Velocidad	Muestra la velocidad negociada del puerto LAN. **1000Mbps**–La velocidad negociada del puerto LAN es de 1000 Mbps. **100Mbps**–La velocidad negociada del puerto LAN es de 100 Mbps. **10Mbps**–La velocidad negociada del puerto LAN es de 10 Mbps. **- - -** El puerto LAN está deshabilitado o no hay ningún dispositivo activo conectado.

Seleccionar**DE ACUERDO**para guardar los cambios en la página.

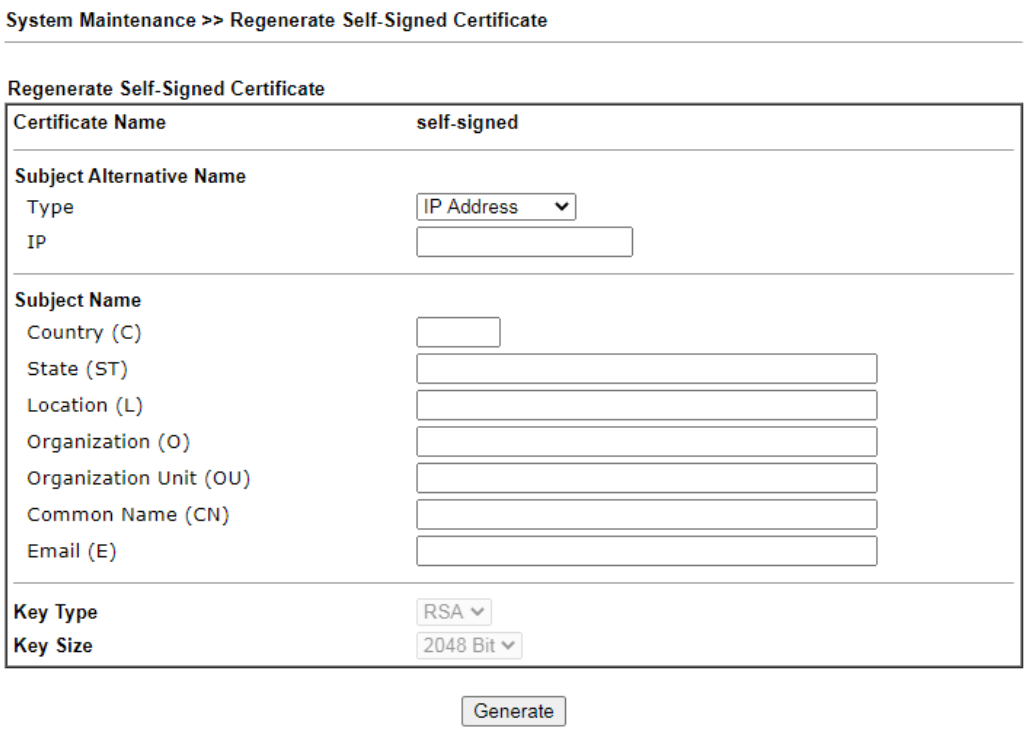
VII-1-13 Certificado autofirmado

Un certificado autofirmado es un*único*identificación para el dispositivo (por ejemplo, enrutador Vigor) que genera el certificado por sí mismo para garantizar la seguridad del enrutador. Dicho certificado autofirmado se firma con su propia clave privada.

El certificado autofirmado se puede utilizar para servicios como SSL VPN y HTTPS. Además, se puede crear de forma gratuita utilizando una amplia variedad de herramientas.



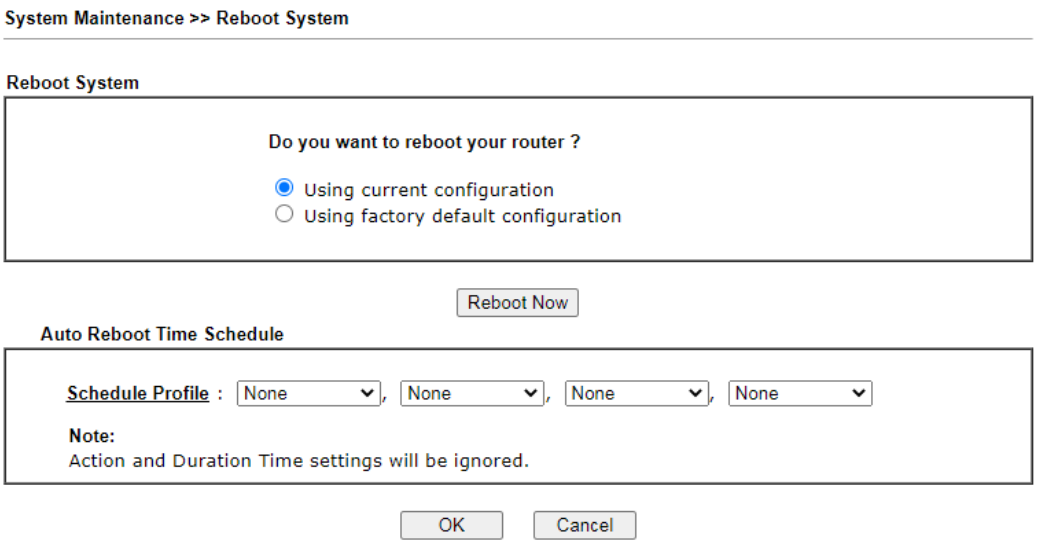
Hacer clic**Regenerado**abrir**Regenerar certificado autofirmado**ventana.



Ingrese toda la información solicitada, incluido el nombre del certificado (utilizado para diferenciar diferentes certificados), el tipo de nombre alternativo del sujeto y la configuración relacional para el nombre del sujeto. Luego haga clic**GENERAR**.

Sistema de reinicio VII-1-14

La interfaz de usuario web se puede usar para reiniciar su enrutador. Hacer clic**Reiniciar el sistema**de **Mantenimiento del sistema**para abrir la página siguiente.



Los ajustes disponibles se explican a continuación:

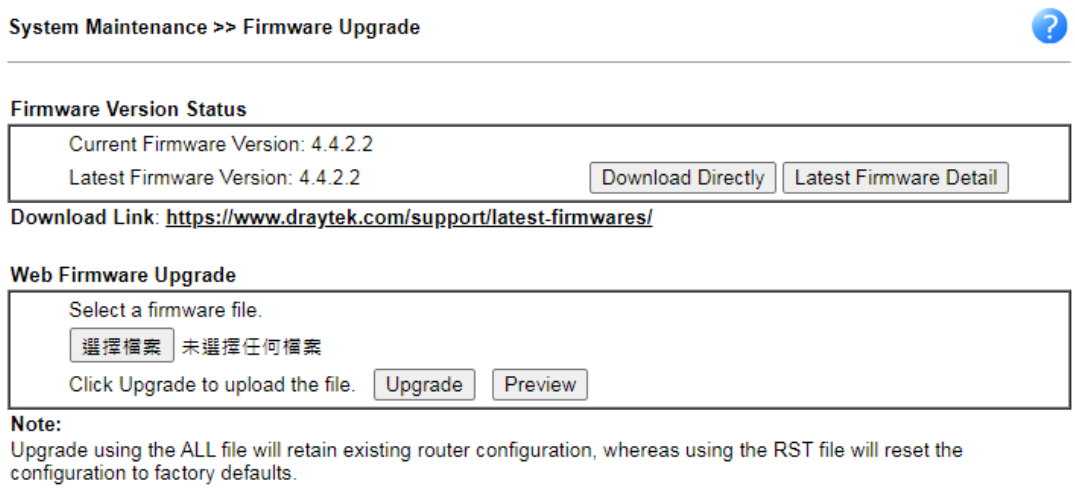
Artículo	Descripción
Reiniciar el sistema	Seleccione una de las siguientes opciones y presione el botón**Reinicie ahora**botón para reiniciar el enrutador. **Usando la configuración actual**–Seleccione esta opción para reiniciar el enrutador usando la configuración actual. **Uso de la configuración predeterminada de fábrica**–Seleccione esta opción para restablecer la configuración del enrutador a los valores predeterminados de fábrica antes de reiniciar.
Tiempo de reinicio automático **Cronograma**	**Programar perfil**-Seleccione hasta 4 horarios configurados por el usuario para reiniciar el enrutador de forma programada.

Seleccionar**DE ACUERDO**para guardar los cambios en la página, o**Cancelar**para descartar los cambios sin guardar.

Información
Cuando el sistema muestre la página web Reiniciar sistema después de configurar los ajustes web, haga clic en Reiniciar ahora para reiniciar su enrutador para garantizar un funcionamiento normal y evitar errores inesperados del enrutador en el futuro.

Actualización de firmware VII-1-15

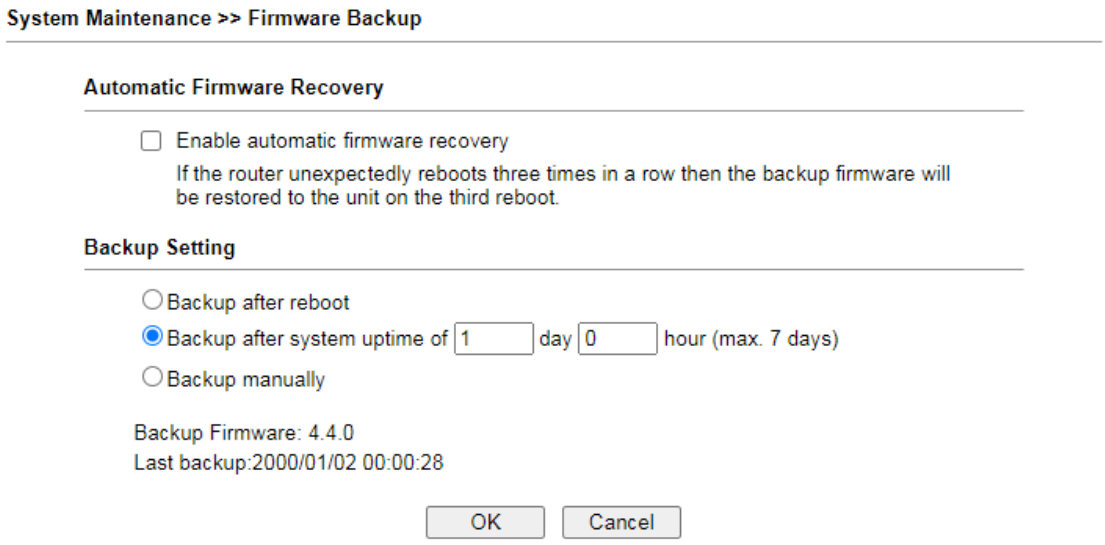
Hacer clic**Mantenimiento del sistema>> Actualización de firmware**para actualizar la actualización del firmware.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Estado de la versión del firmware	**Compruebe el firmware más reciente**–Haga clic para buscar firmware actualizado. Se mostrarán todos los nuevos archivos de firmware disponibles y puede descargar cualquiera de ellos haciendo clic en**Descargar**. Una vez descargado el archivo, haga clic en Seleccionar seguido de Actualizar para realizar la actualización del firmware.
Actualización de firmware web	Hacer clic**Navegar...**para seleccionar el archivo de firmware, seguido de **Mejora**para iniciar el proceso de actualización, o**Avance**para mostrar información detallada sobre el archivo de firmware seleccionado:

El firmware para el enrutador Vigor se puede guardar en el host como un firmware de respaldo. Después de eso, si el enrutador falla debido a un error de firmware, se aplicará el firmware de respaldo para que el enrutador funcione normalmente.



Los ajustes disponibles se explican a continuación:

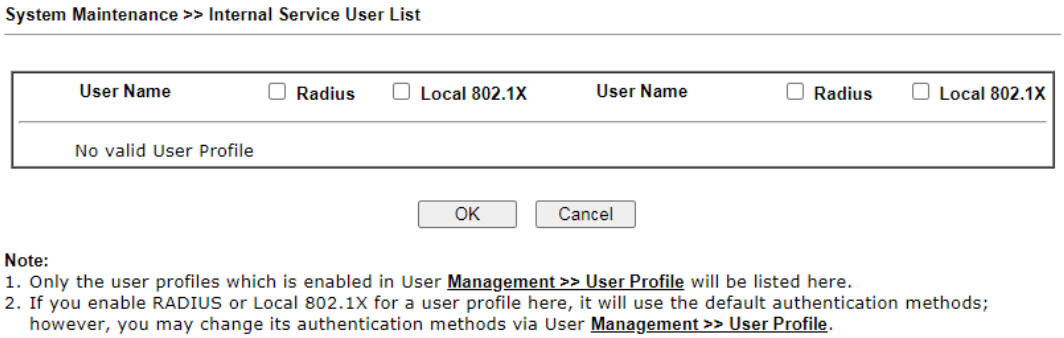
Artículo	Descripción
Firmware automático Recuperación	**Habilitar la recuperación automática de firmware**- Si esta opción está habilitada, el enrutador restaurará el firmware respaldado más recientemente después de que el enrutador se reinicie inesperadamente tres veces.
Configuración de copia de seguridad	Esta opción controla el comportamiento de respaldo del enrutador. - **Copia de seguridad después de reiniciar -**El enrutador hace una copia del firmware actual inmediatamente después de que se reinicia - **Copia de seguridad después del tiempo de actividad del sistema... -**El enrutador hace una copia del firmware actual después de que se haya ejecutado durante el período de tiempo especificado después del arranque. - **Copia de seguridad manualmente -**el enrutador no creará automáticamente una copia de seguridad del firmware. Haga clic en esta opción y haga clic en Aceptar, la copia de seguridad del firmware se realizará de inmediato. **Firmware de copia de seguridad**-Muestra la versión de copia de seguridad de firmware más reciente. **Última copia de seguridad**-Muestra la hora de la última copia de seguridad del firmware.

Seleccionar**DE ACUERDO**para guardar los cambios en la página, o**Cancelar**para descartar los cambios sin guardar.

VII-1-17 Lista de Usuarios del Servicio Interno

Perfiles de usuario (clientes) definidos y habilitados en**Gestión de usuarios>>Perfil de usuario**se mostrará en esta página.

Dicha página le permite activar o desactivar el servicio de autenticación de seguridad (ofrecido por RADIUS interno y/o Local 802.1X) para cada perfil de usuario sin acceder a la página de configuración de Administración de usuarios.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre de usuario	Muestra el nombre del perfil de usuario existente. Para modificar la configuración detallada, simplemente haga clic en el enlace del nombre de usuario para acceder a la página web para su modificación.
Radio	Marque la casilla para activar el servicio de autenticación de seguridad que ofrece el servidor RADIUS interno para el perfil de usuario. Desmarque la casilla para desactivar el servicio de autenticación de seguridad que ofrece el servidor RADIUS interno para el perfil de usuario. Si marca la casilla junto a dicho elemento, todos los perfiles de usuario enumerados en esta página se habilitarán con el servicio RADIUS habilitado y viceversa.
802.1X locales	Marque la casilla para activar el servicio de autenticación de seguridad ofrecido por el servidor Local 802.1X para el perfil de usuario. Desmarque la casilla para desactivar el servicio de autenticación de seguridad ofrecido por el servidor Local 802.1X para el perfil de usuario. Si marca la casilla junto a dicho elemento, todos los perfiles de usuario enumerados en esta página se habilitarán con el servicio Local 802.1X habilitado; viceversa.

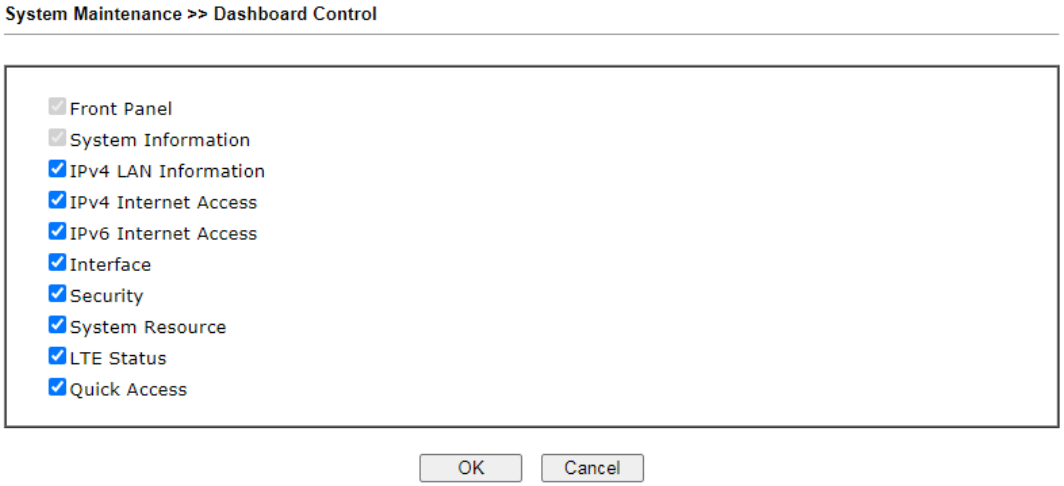
Información

Para conocer la configuración detallada (como la dirección IP, el número de puerto) del RADIUS interno, consulte**Aplicaciones>>RADIUS/TACACS+**.

Para conocer la configuración detallada (como la dirección IP, el número de puerto) de Local 802.1X, consulte**LAN>>Alámbrico 802.1X**y**LAN inalámbrica>>Seguridad**.

VII-1-18 Tablero de Control

Hay nueve grupos de información de configuración que se pueden mostrar en el Tablero como referencia para el administrador/usuario. A excepción de la información del sistema y del panel frontal, la información de configuración relacionada con los grupos enumerados en esta página se puede ocultar si es necesario.



Límite de sesiones

Cuando los clientes de LAN comparten una dirección IP pública común mediante la traducción de direcciones de red (NAT), el enrutador debe realizar un seguimiento de las sesiones NAT para que el tráfico hacia y desde la WAN pueda llegar a los destinos previstos. Hay un número finito de sesiones que el enrutador puede rastrear, y al establecer límites de sesión se asegurará de que el enrutador no se quede sin recursos. Esto es especialmente importante cuando se utilizan aplicaciones P2P. Aplicaciones P2P, como BitTorrent, que intentan establecer conexiones simultáneamente con tantos hosts WAN como sea posible.

Límite de ancho de banda

El límite de ancho de banda garantiza que los clientes de LAN obtengan su parte justa del ancho de banda de la red al imponer restricciones en las velocidades de red ascendentes y descendentes.

Calidad de servicio (QoS)

QoS (Calidad de servicio) garantiza que todos los clientes de LAN reciban la parte justa del ancho de banda que se requiere para que las aplicaciones funcionen de manera adecuada y eficiente.

Sin QoS, es posible que ciertas aplicaciones consuman recursos de red excesivos y degraden el rendimiento de aplicaciones más importantes, especialmente aquellas que son menos tolerantes a la fluctuación (variación de retraso) o paquetes perdidos o retrasados. Además, en momentos de congestión de la red, QoS puede priorizar diferentes tipos de tráfico de acuerdo con su prioridad predefinida, lo que garantiza que el tráfico de mayor importancia se procese primero.

Una implementación típica de QoS consta de dos componentes:

- Clasificación: identificar aplicaciones cruciales o de baja latencia y marcarlas para la aplicación de nivel de servicio de alta prioridad en toda la red.
- Programación: priorización de paquetes asignándolos a diferentes colas y tipos de servicio según los niveles de servicio.

Calidad de servicio de la aplicación

APP QoS permite aplicar QoS a determinados protocolos y aplicaciones.

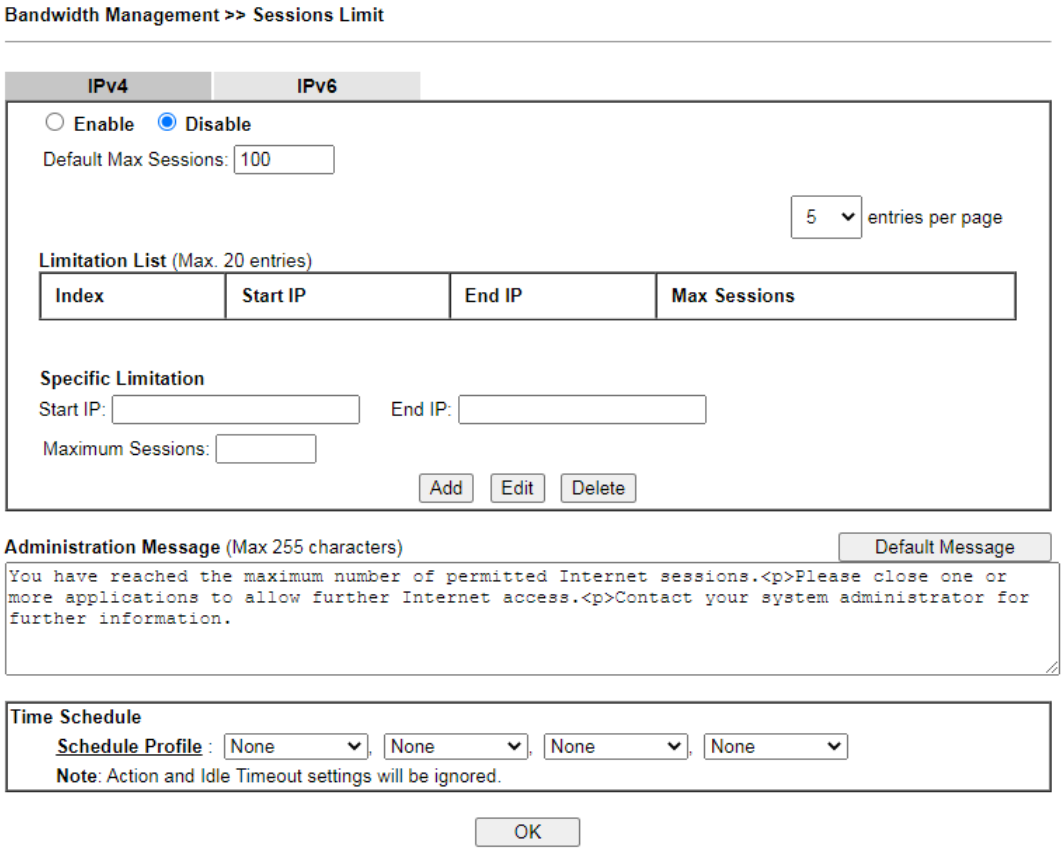
Los protocolos y las aplicaciones se dividen en dos categorías: rastreables e imposibles de rastrear. Las aplicaciones rastreables son aquellas cuyo tráfico se puede rastrear al 100 % y se les puede asignar una clase de QoS específica. Las aplicaciones imposibles de rastrear, por otro lado, se detectan cuando intentan establecer conexiones con hosts remotos, y todo el tráfico entre los hosts remotos y la red local se colocará bajo QoS, dentro de la misma clase de QoS.

La gestión del ancho de banda garantiza una asignación eficiente del ancho de banda de la red para varias aplicaciones.

Para configurar la Gestión de ancho de banda, desde el Menú principal, seleccione**Gestión de ancho de banda**.

VII-2-1 Límite de sesiones

Para configurar el Límite de Sesiones, desde la**Gestión de ancho de banda**menú, seleccione**Límite de sesiones**para abrir la página de configuración.



Los ajustes disponibles se explican a continuación:

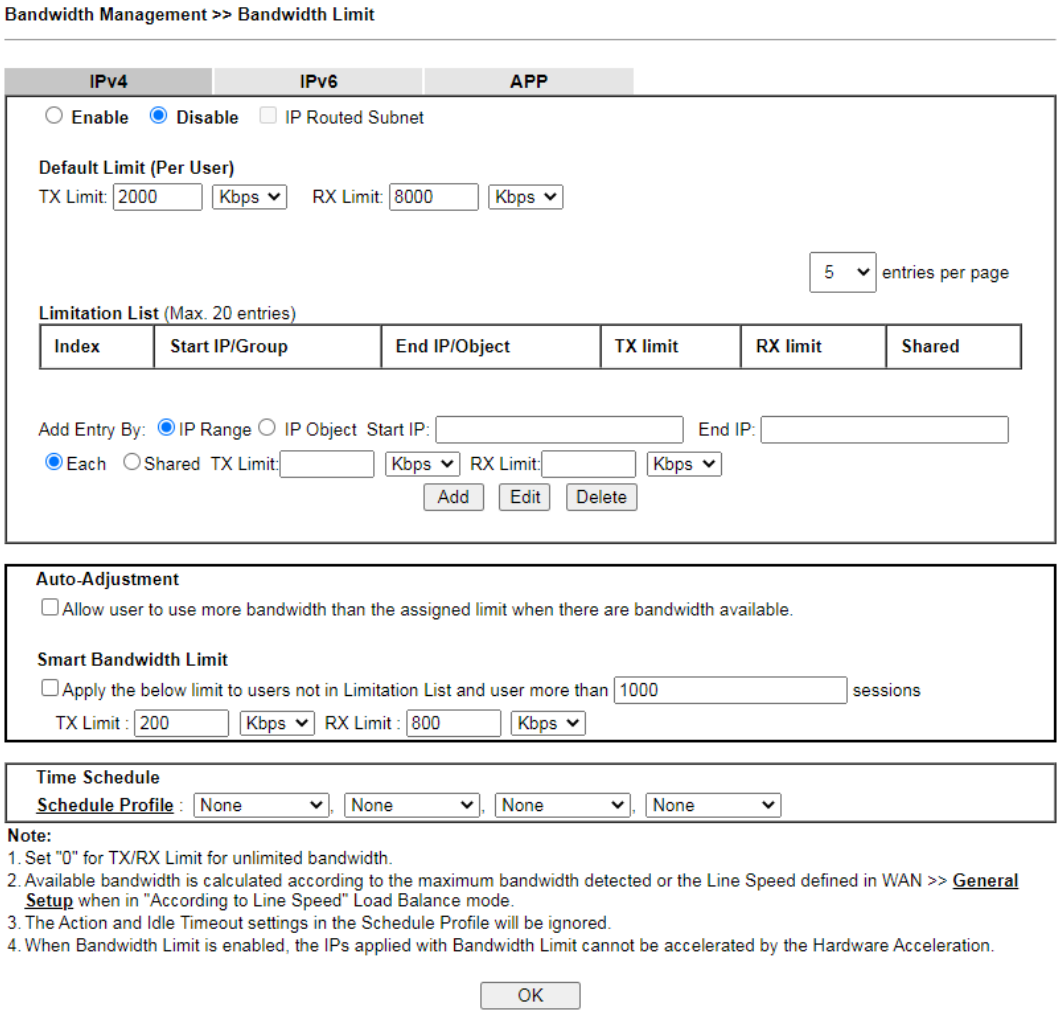
Artículo	Descripción
Habilitar deshabilitar	**Permitir -**Seleccione para activar la función de límite de sesión. **Desactivar -**Seleccione para desactivar la función de límite de sesión. **Sesión máxima predeterminada -**El número máximo predeterminado de sesiones permitidas por cliente LAN, a menos que se anule especificando un número diferente en la Lista de limitaciones.

Lista de limitaciones	Muestra entradas de limitaciones específicas.
Limitación específica	**IP de inicio -**La dirección IP inicial para esta entrada de límite. **IP final -**La dirección IP final para la entrada de límite. **Máximo de sesiones -**El número máximo de sesiones NAT permitidas por cliente LAN. Si no se ingresa ningún valor, se usa el valor de Sesiones máximas predeterminadas. **Agregar -**Crea una nueva entrada de límite utilizando los valores de limitación específica anteriores. **Editar -**Para editar una entrada existente, seleccione la entrada de la Lista de limitaciones, realice los cambios apropiados en Limitación específica y luego haga clic en Editar. **Borrar -**Para eliminar una entrada, selecciónela de la Lista de limitaciones y luego haga clic en el botón Eliminar.
Mensaje de administración	Mensaje que se mostrará en un navegador web en el cliente LAN cuando se haya alcanzado el número máximo de sesiones NAT. **Mensaje predeterminado**-Haga clic para restablecer el mensaje de administración a los valores predeterminados de fábrica.
Horario	**Programar perfil**-Especifique hasta 4 entradas de horario para habilitar o deshabilitar la WAN.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**.

VII-2-2 Límite de ancho de banda

Para configurar la función Límite de ancho de banda, desde la**Gestión de ancho de banda**menú, seleccione **Límite de ancho de banda**para abrir las páginas de configuración de IPv4, IPv6 y APP. Aquí tomamos IPv4 como ejemplo.



Los ajustes disponibles se explican a continuación:

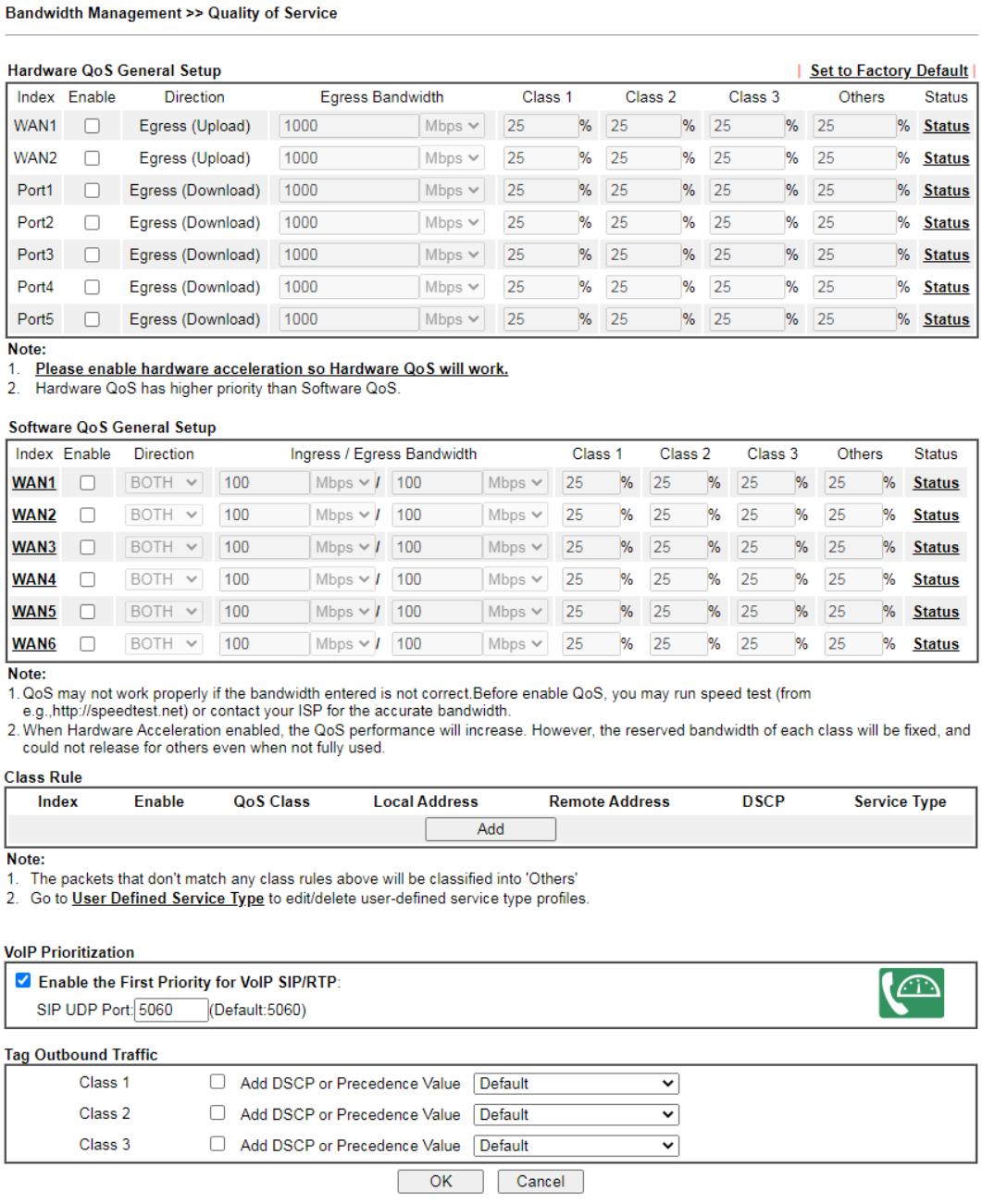
Artículo	Descripción
Habilitar deshabilitar	**Permitir**-Seleccione para activar la función de límite de ancho de banda. **Desactivar**-Seleccione para desactivar la función de límite de ancho de banda. **Límite predeterminado (por usuario)** - **LÍMITE TX -**Límite de velocidad ascendente predeterminado para cada cliente LAN. La unidad puede ser Kbps o Mbps. El valor debe estar entre 0 (ilimitado) y 30000. - **Límite de RX -**Límite de velocidad descendente predeterminado para cada cliente LAN. La unidad puede ser Kbps o Mbps. El valor debe estar entre 0 (ilimitado y 30000).
Lista de limitaciones	Muestra entradas de limitaciones específicas.
Agregar entrada por	**Rango IP -**Todas las IP dentro del rango definido estarán restringidas por el límite de ancho de banda definido por el Límite de TX y el Límite de RX a continuación.

	- **IP de inicio -**La dirección IP inicial para esta entrada de límite. **IP** - **final -**La dirección IP final para la entrada de límite. **Objeto IP -**Todas las IP especificadas por el objeto de IP seleccionado o el grupo de IP estarán restringidas por el límite de ancho de banda definido por el Límite de TX y el Límite de RX a continuación. - **Grupo de PI –**Especifique un grupo de IP utilizando la lista desplegable. - **Objeto IP -**Especifique un objeto de IP utilizando la lista desplegable. **Cada**-El ancho de banda especificado es el límite por cliente LAN. **Compartido -**Los límites de ancho de banda especificados son el total permitido para todos los clientes LAN dentro del rango de direcciones IP. - **límite de transmisión -**El límite aguas arriba. La unidad puede ser Kbps o Mbps. El valor debe estar entre 0 (ilimitado) y 30000. - **Límite de RX -**El límite aguas abajo. La unidad puede ser Kbps o Mbps. El valor debe estar entre 0 (ilimitado) y 30000. **Agregar -**Crea una nueva entrada de límite utilizando los valores de limitación específica anteriores. **Editar -**Para editar una entrada existente, seleccione la entrada de la Lista de limitaciones, realice los cambios apropiados en Limitación específica y luego haga clic en Editar. **Borrar -**Para eliminar una entrada, selecciónela de la Lista de limitaciones y luego haga clic en el botón Eliminar.
Ajuste automático	**Permitir que el usuario use más ancho de banda...-**Seleccione para permitir que el enrutador ajuste automáticamente los límites de flujo ascendente y descendente según el ancho de banda disponible.
Límite de ancho de banda inteligente	Esta opción restringe el ancho de banda de los clientes LAN que no están en la lista de limitaciones cuando las sesiones de red superan un umbral predefinido. **Aplique el siguiente límite a...**-El número de sesiones que un cliente LAN puede tener antes de que se active el límite de ancho de banda inteligente. - **límite de transmisión -**Límite de velocidad ascendente para cada cliente LAN. La unidad puede ser Kbps o Mbps. El valor debe estar entre 0 (ilimitado) y 30000. - **Límite de RX -**Límite de velocidad descendente para cada cliente LAN. La unidad puede ser Kbps o Mbps. El valor debe estar entre 0 (ilimitado y 30000).
Horario	**Programar perfil**-Especifique hasta 4 entradas de horario para habilitar o deshabilitar la WAN.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**.

VII-2-3 Calidad de Servicio

Para configurar**Calidad de servicio**, en el menú principal, seleccione**Gestión de ancho de banda**menú, luego haga clic en**Calidad de servicio**para abrir la página de configuración.



Los ajustes disponibles se explican a continuación:

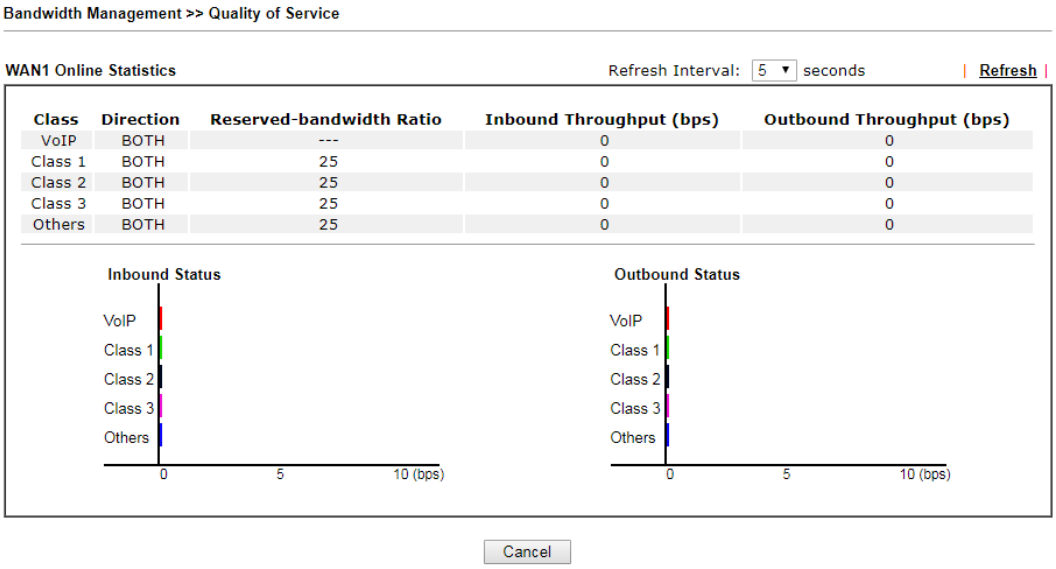
Artículo	Descripción
Hardware QoS general Configuración	Antes de usar Hardware QoS, habilite**Aceleracion de hardware** primero. **Índice**–Enlace de la interfaz WAN/LAN. **Permitir**–Marque la casilla para habilitar la función QoS para la interfaz WAN/LAN. Si está habilitado, puede configurar la configuración general de QoS para cada interfaz. - **Dirección**–Aplique QoS solo al tráfico saliente.

	- **Salida de ancho de banda**–El ancho de banda de salida de la WAN/LAN. - **Clase 1 ~ 3 / Otros**–Porcentaje de ancho de banda reservado para cada clase. - **Estado**–Haga clic para abrir la página Estadísticas en línea que muestra instantáneas de estadísticas para la interfaz WAN/LAN dada.
Software QoS general **Configuración**	**Índice**–Enlace de interfaz WAN/LTE. **Permitir**–Marque la casilla para habilitar la función QoS para la interfaz WAN/LTE. Si está habilitado, puede configurar la configuración general de QoS para cada interfaz WAN/LTE. - **Dirección**–Dirección del tráfico al que se aplicará QoS (entrante, saliente o ambos). - **EN -**Aplique QoS solo al tráfico entrante. - **AFUERA -**Aplique QoS solo al tráfico saliente. - **AMBOS -**Se aplica tanto al tráfico entrante como saliente. - **Ancho de banda de entrada/salida**– El ancho de banda de entrada/salida de la WAN. - **Clase 1 ~ 3 / Otros**–Porcentaje de ancho de banda reservado para cada clase. **Estado**–Haga clic para abrir la página Estadísticas en línea que muestra instantáneas de estadísticas para la interfaz WAN dada.
regla de clase	Defina y enumere las reglas de la clase. **Índice**–Muestre el número de clase que puede editar. **Permitir**-Muestra el estado de esta regla de clase. **Clase de** **QoS**-Muestra el nivel de clase de QoS. **Dirección local**-Muestra la dirección IP local para la regla. **Dirección remota**-Muestra la dirección IP remota para la regla. **DSCP**-Muestra los niveles de los datos para procesar con control QoS. **Tipo de servicio**–Muestra la configuración detallada para el tipo de servicio. **Agregar**-Haga clic en él para crear una regla de clase para QoS.
Priorización de VoIP	**Habilite la primera prioridad para VoIP SIP/RTP**-Seleccione para permitir que el tráfico de VoIP reciba la prioridad más alta. **Puerto SIP UDP –**Número de puerto que se supervisará para el tráfico SIP. - Haga clic en este icono para mostrar el estado de VoIP QoS.
Etiquetar tráfico saliente	Etiquete el tráfico saliente con el valor DSCP o Precedencia. **Agregue DSCP o valor de precedencia para la clase 1 a la clase 3**-Marque para aplicar el DSCP o el valor de precedencia para cada clase.

Para guardar los cambios, haga clic en**DE ACUERDO**; para descartar los cambios, haga clic en**Cancelar**.

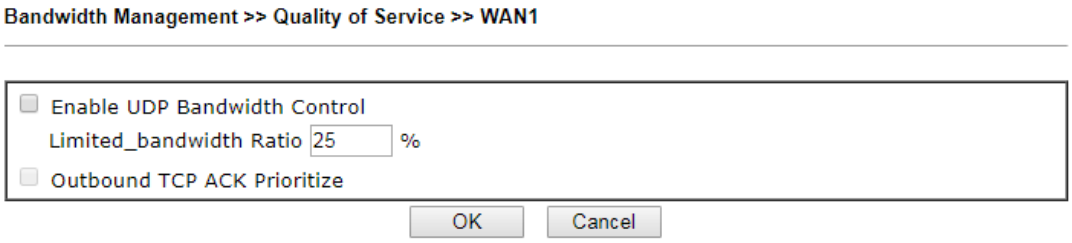
Estadísticas en línea

Haga clic en el enlace Estado en la sección Configuración general para mostrar estadísticas en línea en tiempo real de la interfaz WAN.



Configuración general para la interfaz WAN (Software QoS)

Haga clic en el vínculo del número de interfaz WAN/LTE para configurar la proporción de ancho de banda limitado para QoS de la interfaz WAN.



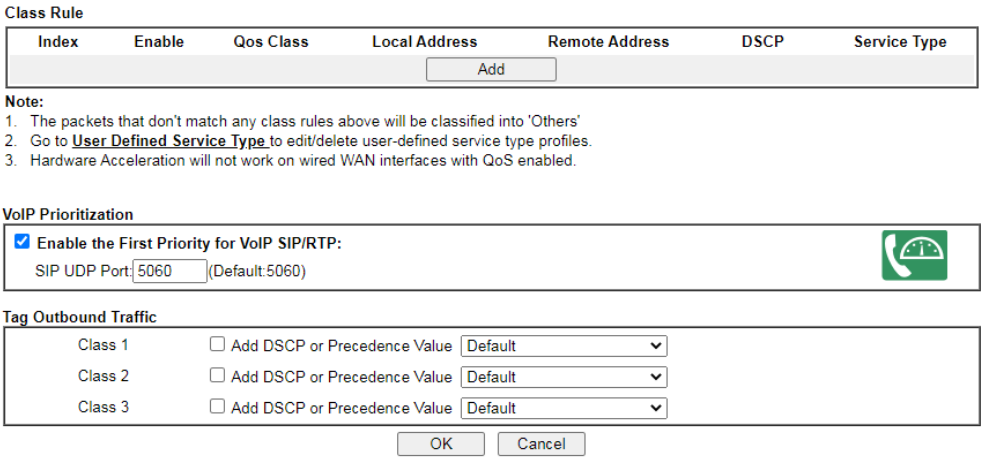
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar ancho de banda UDP Control	Seleccione para restringir el ancho de banda disponible para el tráfico UDP. El **Relación de ancho de banda limitado**El valor es el porcentaje máximo de ancho de banda que puede utilizar el tráfico UDP. - **Relación de ancho de banda limitado -**Introduzca un valor porcentual.
Acuse de recibo de TCP saliente priorizar	Seleccione para dar prioridad a los paquetes ACK salientes sobre otros paquetes para garantizar que el tráfico no se ralentice porque el host remoto está esperando paquetes ACK antes de que se envíe más tráfico.

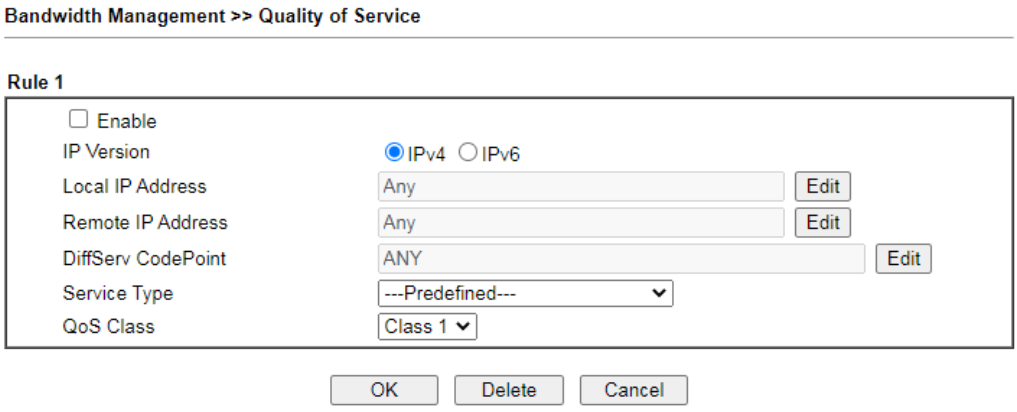
Información	
	La tasa de salida/entrada debe ser menor que el ancho de banda real para garantizar el cálculo correcto de QoS. Se sugiere establecer el valor de ancho de banda para entrada/salida como 80% - 85% de la velocidad de la red física proporcionada por el ISP para maximizar el rendimiento de QoS.

Puede configurar hasta 20 reglas para una clase. Si desea editar una regla existente, seleccione el botón de opción de esa regla y haga clic en Editar para abrir la página de edición de la regla para su modificación.

1. Para agregar una regla, haga clic en**Agregar**para abrir la página de configuración. Para editar una regla existente, seleccione la regla haciendo clic en el botón de radio delante de la regla y luego haga clic en**Editar** para abrir la página de configuración.

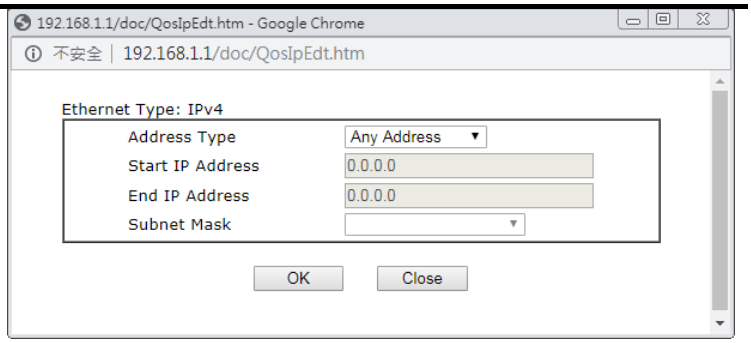


2. Para agregar una nueva regla, haga clic en**Agregar**para abrir la página siguiente.

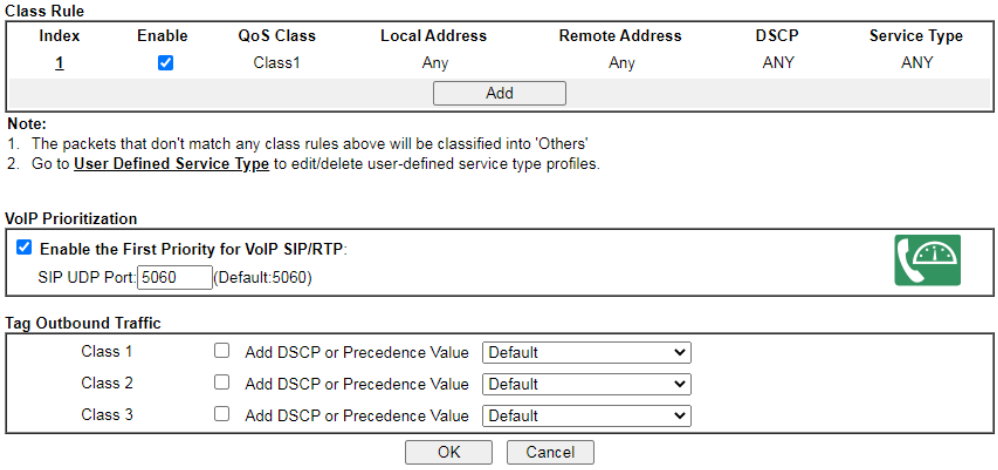


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Seleccione para habilitar esta regla.
Versión IP	Protocolo (IPv4 o IPv6) al que se aplica esta regla.
Dirección IP local	Haga clic en el**Editar**para configurar la dirección IP local (LAN) o el rango de direcciones para la regla.
Dirección IP remota	Haga clic en el**Editar**para configurar la dirección IP remota (WAN) o el rango de direcciones para la regla.

	 **Tipo de dirección**–Tipo de dirección: cualquier dirección, dirección única, dirección de rango, dirección de subred. - **Dirección única**-Especifique la dirección IP. - **Dirección de rango**-Especifique la dirección IP inicial y la dirección IP final. - **Dirección de subred**-Especifique la dirección IP de inicio y la máscara de subred.
Punto de código DiffServ	Precedencia DSCP o ToS de los paquetes a los que se aplica esta regla.
Tipo de servicio	Tipo de servicio al que se aplica esta regla. El servicio es un tipo de tráfico predefinido o definido por el usuario que utiliza ciertos protocolos o puertos. Para configurar un servicio personalizado, seleccione Definido por el usuario para configurar el nombre del servicio, el protocolo y el número de puerto.
Clase de QoS	Especifique la clase de QoS (1, 2 o 3) para esta regla.

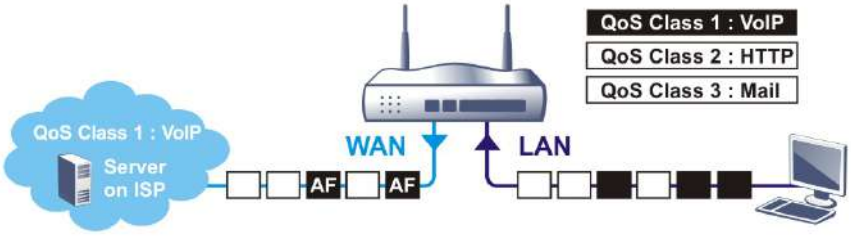
3. Después de finalizar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.



Vuelva a etiquetar los paquetes para su identificación

Los paquetes que se originan en la LAN que están destinados a la WAN pueden tener el indicador DS cambiado a un valor diferente habilitando Tag Packet y especificando el valor DSCP o IP Precedence.

En la siguiente ilustración, los paquetes de VoIP salientes de la LAN llegan al enrutador Vigor con el valor de QoS sin configurar. El enrutador establece el valor DSCP en AF antes de reenviarlos al servidor ISP a través de la interfaz WAN.



Class Rule

Index	Enable	Qos Class	Local Address	Remote Address	DSCP	Service Type
1	☑	Class 1	Any	Any	ANY	SIP(UDP:5060)
2	☑	Class 1	Any	Any	ANY	HTTP(TCP:80)
3	☑	Class 1	Any	Any	ANY	SMTP(TCP:25)

Add

Note:
1. The packets that don't match any class rules above will be classified into 'Others'
2. Go to **User Defined Service Type** to edit/delete user-defined service type profiles.
3. Hardware Acceleration will not work on wired WAN interfaces with QoS enabled.

VoIP Prioritization

☑ Enable the First Priority for VoIP SIP/RTP:
SIP UDP Port: 5060 (Default:5060)

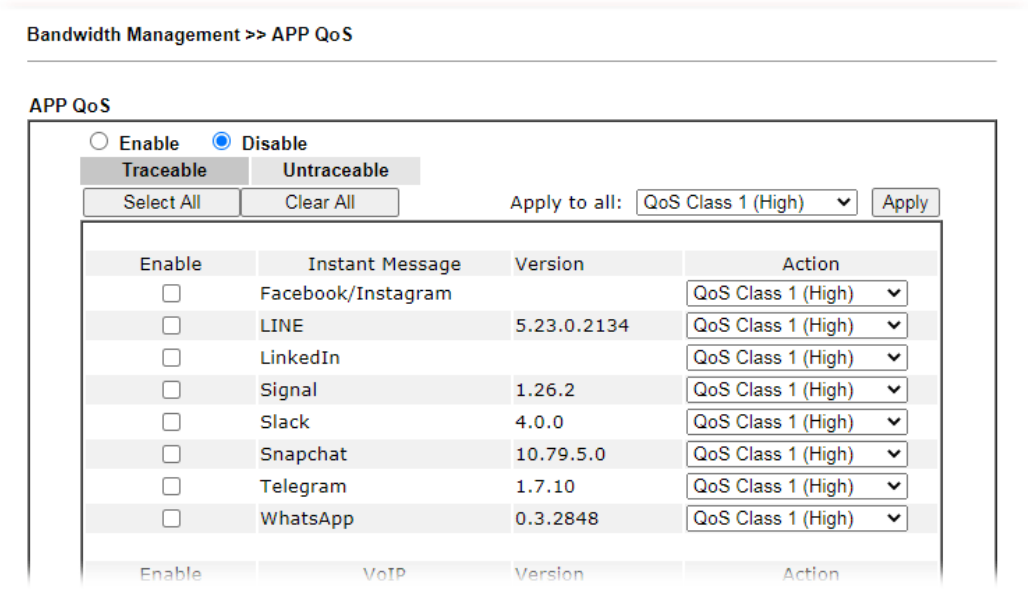
Tag Outbound Traffic

Class 1	☑ Add DSCP or Precedence Value	AF Class1 (Medium Drop)
Class 2	☑ Add DSCP or Precedence Value	AF Class2 (Low Drop)
Class 3	☑ Add DSCP or Precedence Value	AF Class3 (Medium Drop)

OK Cancel

VII-2-4 APLICACIÓN QoS

Para configurar APP QoS, desde el menú principal, seleccione**Gestión de ancho de banda**menú, luego haga clic en **Calidad de servicio de la aplicación**para abrir la página de configuración.



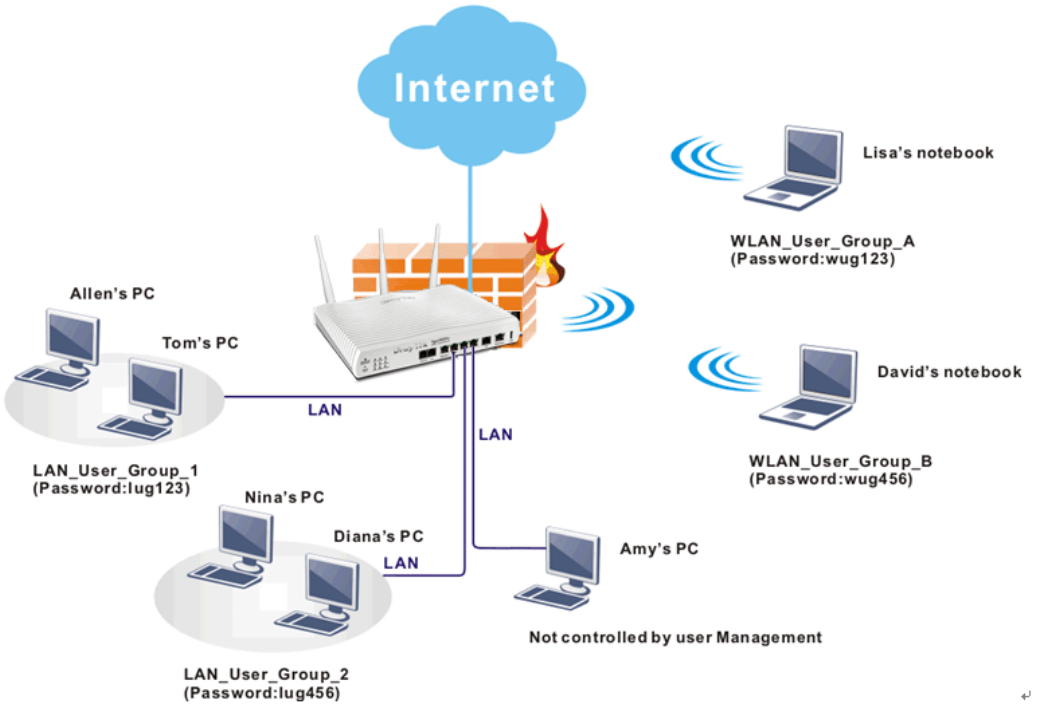
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar deshabilitar	Habilita o deshabilita la función QoS de la aplicación.
Trazable	Las aplicaciones rastreables son aquellas cuyo tráfico se puede rastrear al 100%. Todos los protocolos de esta pestaña pueden tener asignada una clase de QoS específica. **Permitir**-Seleccione para habilitar OoS para la aplicación. **Aplicar a todo**-Seleccione una clase de QoS para aplicarla a todos los protocolos. Puede anular la clase de QoS para protocolos específicos mediante el cuadro de lista desplegable Acción.
Irrastreable	Las aplicaciones imposibles de rastrear se detectan cuando intentan establecer conexiones con hosts remotos, y todo el tráfico entre los hosts remotos y la red local se colocará bajo QoS, dentro de la misma clase de QoS. Todos los protocolos de esta pestaña pueden tener asignada una clase de QoS específica. **Permitir**-Seleccione para habilitar OoS para la aplicación. **Acción**-Seleccione una clase de QoS para aplicar a todas las aplicaciones.
Seleccionar todo	Haga clic para seleccionar todas las casillas de verificación Habilitado.
Limpiar todo	Haga clic para anular la selección de todas las casillas de verificación Habilitado.

Una vez realizados los cambios, haga clic en**DE ACUERDO**para guardar los cambios, o**Cancelar**descartar.

Gestión de usuarios VII-3

La gestión de usuarios permite que el administrador de la red gestione el acceso a Internet a nivel de usuario. Una vez que un usuario ha sido autenticado por medio de un nombre de usuario y una contraseña, se le puede otorgar acceso a Internet y se pueden aplicar reglas de firewall y políticas de acceso WAN opcionales.

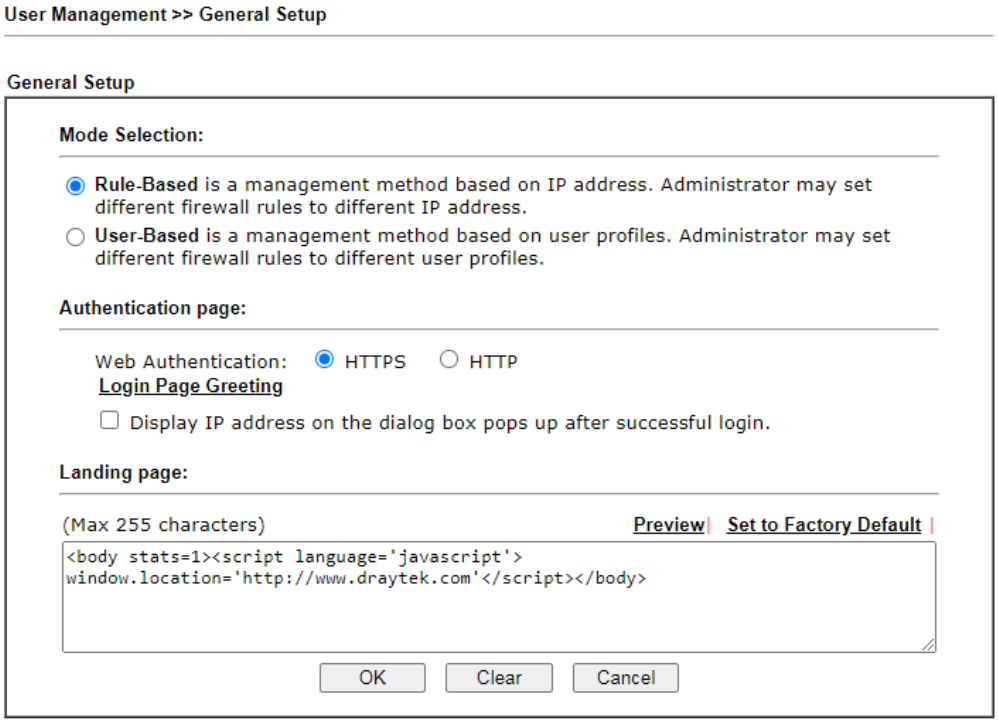


Información

En general, las reglas de filtro configuradas en el Firewall se aplican globalmente. Sin embargo, en la gestión de usuarios, las reglas de filtrado se pueden aplicar de forma selectiva a los perfiles de usuario.

VII-3-1 Configuración general

Los ajustes globales para la gestión de usuarios se pueden configurar en esta sección.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Selección de modo	El modo de gestión de usuarios. **Basado en el usuario**–El enrutador aplica las reglas de filtro configuradas en**Gestión de usuarios>>Perfil de usuario**. **Basado en reglas**–El enrutador aplica las reglas de filtro configuradas en **Cortafuegos>>Configuración general**y**Regla de filtro**.
Página de autenticación	**Autenticación web**-Protocolo web para la página de autenticación web. - HTTP: la página web no estará cifrada. - HTTPS: la página web se cifrará. **Saludo de la página de inicio de sesión** -Haga clic para ser redirigido a **Mantenimiento del sistema >> Saludo de la página de inicio de sesión**, donde puede configurar el mensaje que se muestra al usuario después de un inicio de sesión exitoso.

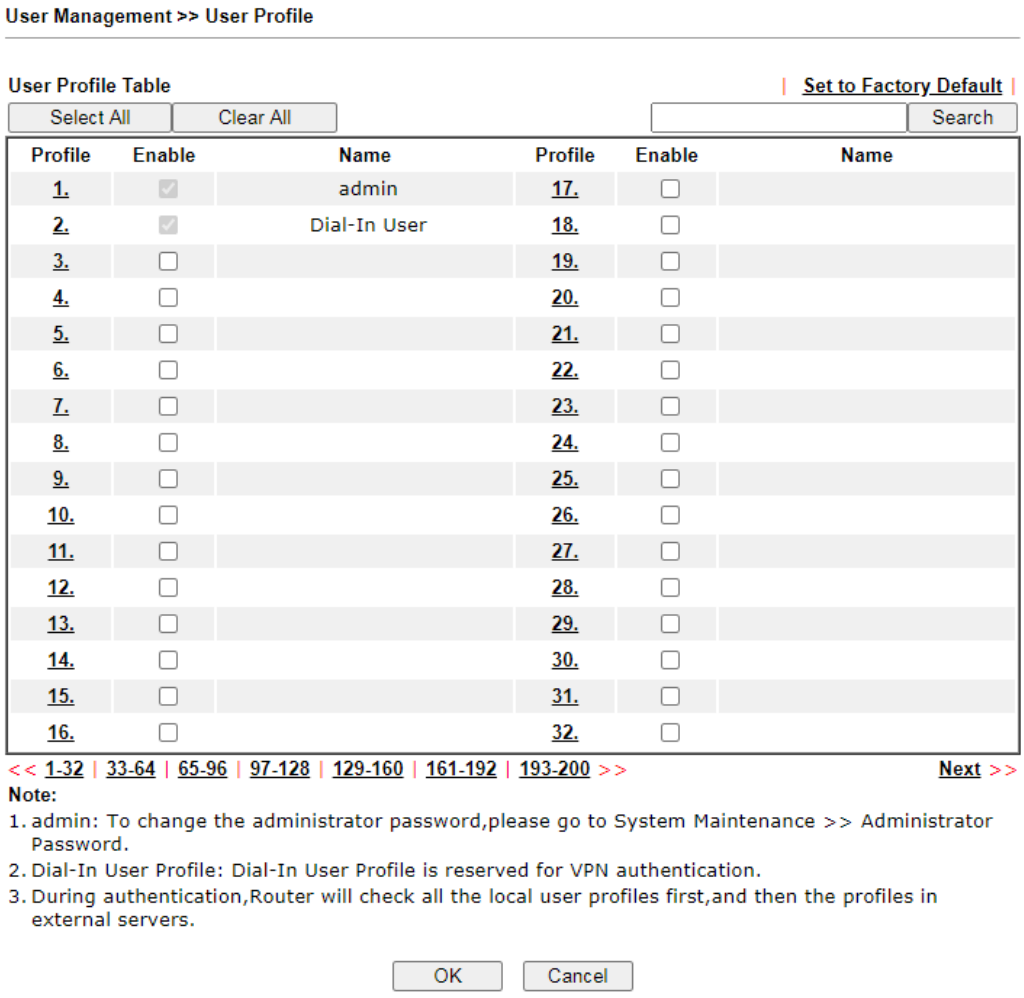
	Mostrar dirección IP en la ventana de seguimiento–Seleccione para mostrar la dirección IP del cliente en la ventana de seguimiento.
Página de destino	Código HTML que se mostrará en el saludo de la página de inicio de sesión.

Hacer clic**DE ACUERDO**para guardar los cambios,**Claro**para restaurar la configuración a los valores predeterminados de fábrica, o**Cancelar**para descartar cambios.

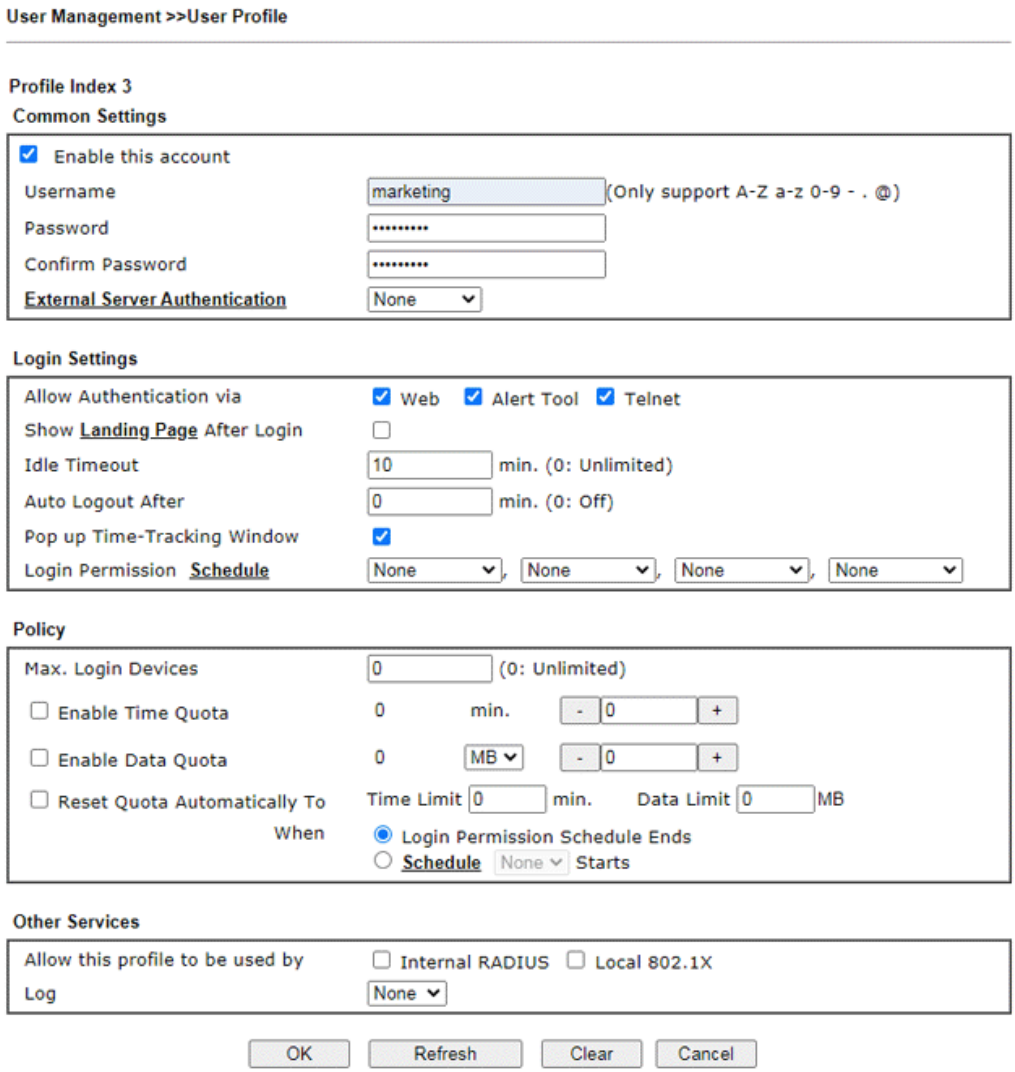
VII-3-2 Perfil de usuario

Esta página le permite crear hasta 200 perfiles de usuario para usar con Administración de usuarios.

Seleccionar**Gestión de usuarios>>Perfil de usuario**en la barra de menú, luego haga clic en un número de perfil para configurar.



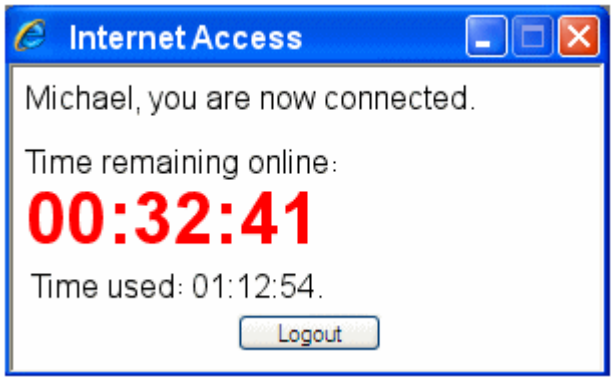
Los perfiles 1 (administrador) y 2 (usuario de acceso telefónico) son perfiles reservados. El perfil de administrador se aplica al inicio de sesión del administrador del enrutador, mientras que el perfil de usuario de acceso telefónico se aplica a todos los usuarios de acceso telefónico de VPN.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Configuraciones comunes	
Habilitar esta cuenta	Seleccione para habilitar este perfil de usuario.
Nombre de usuario	Nombre de inicio de sesión (p. ej.,*LAN_User_Group_1, WLAN_User_Group_A, WLAN_User_Group_B,*etc.) para este perfil de usuario. La longitud máxima es de 24 caracteres.
Contraseña	Contraseña (por ejemplo,*lug123, wug123, wug456,*etc.) para este perfil de usuario. La longitud máxima es de 24 caracteres. Cuando un usuario intenta acceder a Internet y la Administración de usuarios está habilitada, debe proporcionar una combinación válida de nombre de usuario y contraseña para la autenticación. El perfil con nombre de usuario y contraseña coincidentes se aplicará a la sesión.
confirmar Contraseña	Ingrese la contraseña nuevamente para confirmar.
Servicio Externo Autenticación	El enrutador autenticará a los usuarios de acceso telefónico mediante un servicio integrado (Ninguno) o externo (LDAP, Radius o TACACS+). La configuración de la contraseña se ignora cuando se utiliza un servicio de autenticación externo.
Configuración de inicio de sesión	

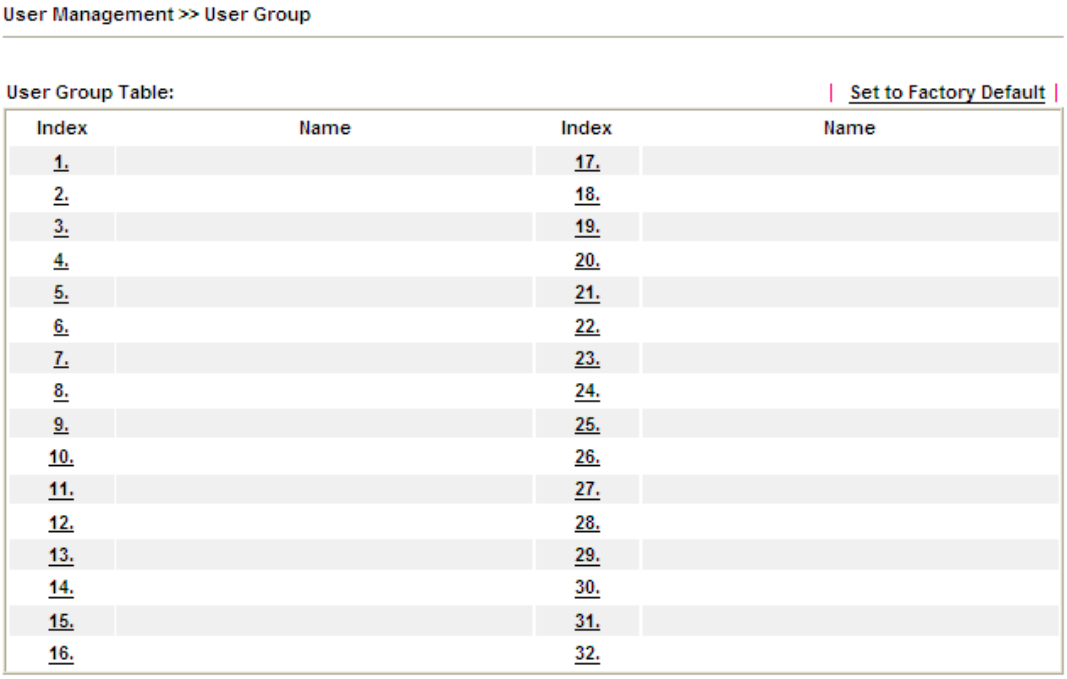
Permitir autenticación a través de	Los métodos de autenticación permitidos para este usuario. **Web**–Si se selecciona, el usuario deberá autenticarse ingresando un nombre de usuario y una contraseña cuando intente acceder a un sitio web externo por primera vez. El usuario será redirigido al sitio web externo después de una autenticación exitosa. **Herramienta de alerta**–Si se selecciona, el usuario puede ingresar el nombre de usuario y la contraseña en DrayTek Alert Tool. Se mostrará una ventana con el tiempo restante de conexión para dicho usuario. La herramienta Alter se puede descargar desde el sitio web de DrayTek. **Telnet**–Si se selecciona, el usuario puede autenticarse iniciando sesión en el enrutador mediante telnet.
Mostrar página de destino después de iniciar sesión	Cuando un usuario intenta acceder a la interfaz de usuario web de la serie de enrutadores Vigor con el nombre de usuario y la contraseña especificados en este perfil, será conducido a la página web configurada en el campo Página de destino en**Gestión de usuarios>>Configuración general**. Marque esta casilla para habilitar dicha función.
Tiempo de inactividad	Si no hay tráfico WAN hacia y desde el cliente LAN durante la cantidad de tiempo especificada (en minutos), la sesión WAN se restablece y el usuario deberá volver a autenticarse antes de que se permita nuevamente el acceso a Internet. El valor predeterminado de tiempo de espera de inactividad es de 10 minutos.
Cierre de sesión automático después	Dicha cuenta se verá obligada a cerrar sesión después de un cierto tiempo establecido aquí.
Seguimiento de tiempo emergente **Ventana**	Si está habilitado, aparecerá una ventana del navegador que muestra el tiempo restante de la sesión. Sin embargo, el sistema actualizará la hora periódicamente para mantener la conexión siempre activa. Por lo tanto, Idle Timeout no interrumpirá la conexión de red.
Calendario de permisos de inicio de sesión	Puede ingresar cuatro conjuntos de horarios para su solicitud. Todos los horarios se pueden configurar previamente en**Aplicaciones >> Horario** página web y puede utilizar el número que ha establecido en esa página web.
Política	
máx. Dispositivos de inicio de sesión	El número máximo de inicios de sesión simultáneos permitidos para este perfil. La configuración predeterminada es 0, lo que significa que no hay límite.
Habilitar cuota de tiempo	Si se selecciona, al usuario se le permite el acceso a Internet durante la cantidad de tiempo especificada después de una autenticación exitosa. El primer valor es el tiempo restante de la sesión de inicio de sesión actual, mientras que el segundo valor es el valor para incrementar o disminuir la cuota de tiempo restante haciendo clic en los botones +/-. Ambos valores están en minutos. Haga clic en +/- para aumentar/disminuir la cuota de tiempo para dicho perfil. **Nota:**Aparecerá un cuadro de diálogo que muestra el tiempo restante cuando el usuario se haya autenticado correctamente.

	 Cuando se acaba el tiempo, todas las conexiones a Internet se terminan.
Habilitar cuota de datos	Si se selecciona, el usuario puede usar la cantidad especificada de datos después de una autenticación exitosa. El primer valor es la cuota de datos restante de la sesión de inicio de sesión actual, mientras que el segundo valor es el valor para incrementar o disminuir la cuota de datos restante haciendo clic en los botones +/-. La unidad para ambos valores se puede establecer en MB (megabytes) o GB (gigabytes) mediante el cuadro desplegable MB/GB. Haga clic en +/- para aumentar/disminuir la cuota de datos para dicho perfil.
Restablecer cuota automáticamente	Seleccione para habilitar esta opción. Restablezca las cuotas de tiempo y datos a los valores predeterminados preestablecidos cuando finaliza un horario. **Límite de tiempo**–Ingrese el valor para la cuota de tiempo predeterminada. **Límite de datos**–Ingrese el valor para la cuota de datos predeterminada. **Finaliza el calendario de permisos de inicio de sesión -**Cuando finaliza el tiempo de programación, el enrutador restablecerá la cuota con valores de tiempo/datos definidos por el usuario automáticamente. **Cronograma** –Especifique un número de índice de horario para este perfil.
Otros servicios	
Permitir que este perfil sea utilizado por	Esta opción está disponible para perfiles con número de índice de 3 a 200. **RADIO interno-**Marque la casilla para habilitar la seguridad autenticada a través del servidor RADIUS interno. **802.1X local -**Marque la casilla para habilitar la seguridad autenticada a través del servidor 802.1X interno.
Registro	Syslog puede registrar las actividades del usuario. **Ninguno**– El registro está deshabilitado. **Acceso**–Se registran las actividades de inicio y cierre de sesión. **Evento**–Se registra el tráfico permitido y bloqueado. **Todo**–Se registran tanto el tipo de inicio de sesión como el de evento.

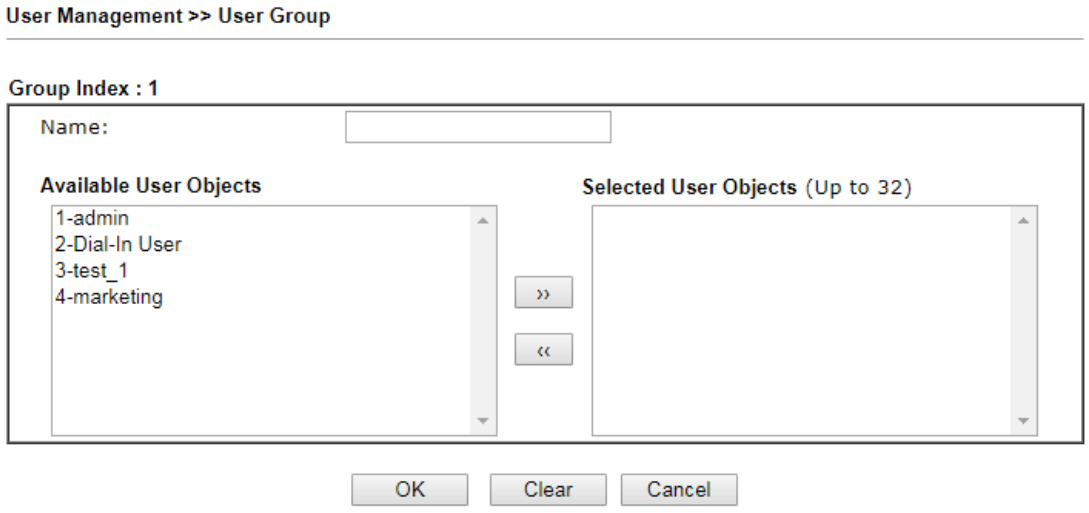
Hacer clic**DE ACUERDO**para guardar los cambios,**Claro**para restaurar la configuración a los valores predeterminados de fábrica, o **Cancelar**para descartar cambios. Hacer clic**Actualizar**para volver a cargar la página con la información de uso de datos más reciente (cuotas de datos y tiempo).

VII-3-3 Grupo de usuarios

Esta página le permite colocar varios perfiles de usuario en grupos. Estos grupos se pueden utilizar para configurar reglas de filtrado en**Cortafuegos>>Configuración general**.



Haga clic en un enlace de número de índice a su página de configuración:



Los ajustes disponibles se explican a continuación:

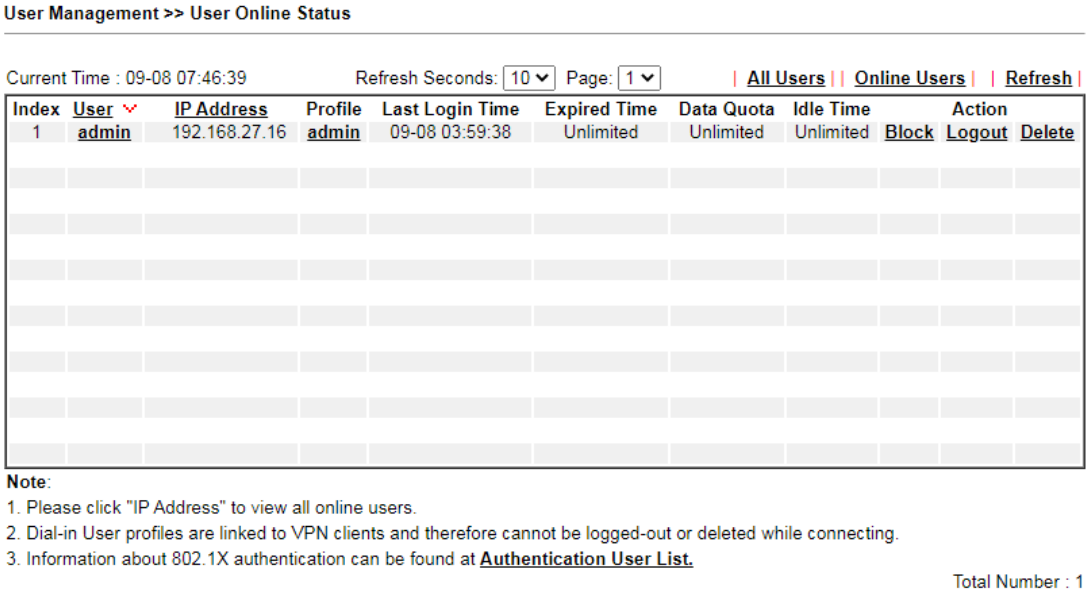
Artículo	Descripción
Nombre	Nombre que identifica a este grupo de usuarios.
Objetos de usuario disponibles	Muestra una lista de objetos de usuario que no se han colocado en el grupo actual.

>> <<	Haga clic en >> para mover los objetos de usuario seleccionados en Objetos de usuario disponibles a la izquierda a Objetos de usuario seleccionados a la derecha, agregándolos así al grupo actual. Haga clic en << para mover los objetos de usuario seleccionados en Objetos de usuario seleccionados a la derecha a Objetos de usuario disponibles a la izquierda, eliminándolos así del grupo actual.
Objetos de palabra clave seleccionados	Muestra una lista de objetos de usuario que se han colocado en el grupo actual.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para eliminar todos los objetos de usuario del grupo actual, haga clic en**Claro**.

VII-3-4 Estado en línea del usuario

Esta página muestra los usuarios que actualmente están conectados al enrutador. La lista se actualiza periódicamente para mostrar la información más actualizada.



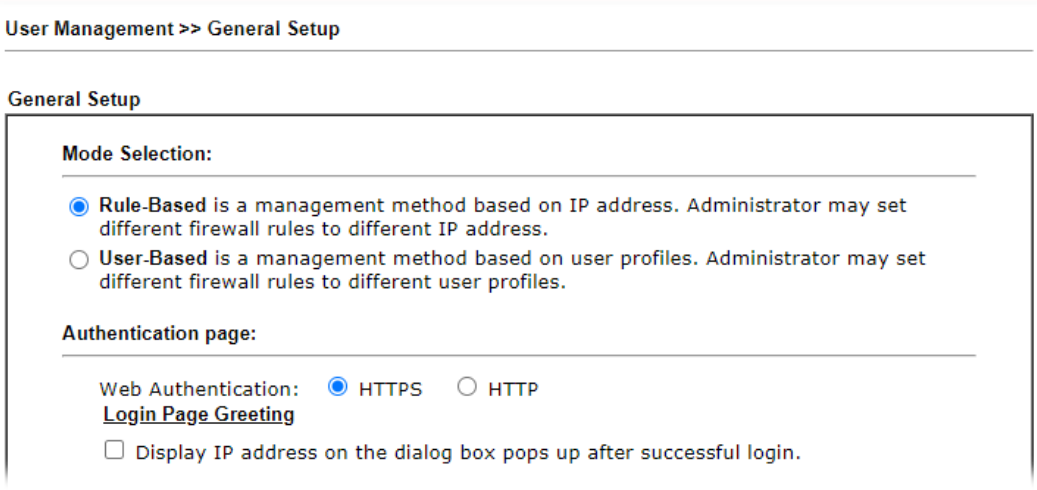
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Actualizar segundos	El intervalo de tiempo entre actualizaciones automáticas de pantalla, en segundos. Seleccione uno de 10, 15 y 30 segundos.
Actualizar	Haga clic para actualizar manualmente los datos mostrados.
Índice	Índice de la entrada del usuario.
Usuario	El nombre del usuario que está conectado. Al hacer clic en esto, aparecerá la siguiente página que permite configurar las cuotas de tiempo y datos del usuario. Para más detalles, consulte la descripción en el**Habilitar cuota de tiempo**y**Habilitar cuota de datos**artículos en el**Perfil del usuario** sección.
Dirección IP	Dirección IP LAN del dispositivo que inició el inicio de sesión.
Perfil	Nombre del perfil de usuario. Si el usuario que inició sesión es un usuario de VPN, se mostrará Usuario de acceso telefónico. De lo contrario, será lo mismo que Usuario.

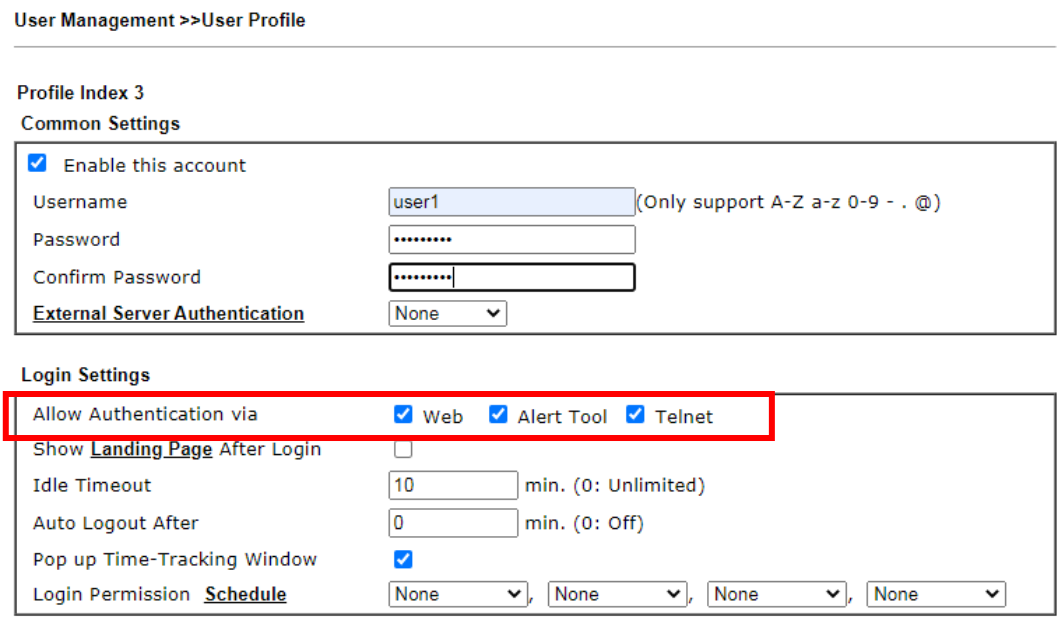
Hora del último inicio de sesión	La hora de inicio de sesión más reciente del usuario.
Tiempo expirado	El tiempo de vencimiento de la sesión de inicio de sesión actual.
Cuota de datos	Muestra la cuota para la transmisión de datos. La cuota de datos restante de esta sesión de inicio de sesión.
Tiempo de inactividad	Cantidad de tiempo que la sesión ha estado inactiva.
Acción	**Bloquear**–Evita que el usuario acceda a Internet. **Desatascar**–Reanuda el acceso a Internet de un usuario bloqueado. **Cerrar sesión**–Finaliza la sesión de inicio de sesión actual. **Borrar**–Elimina la entrada del usuario de la página Estado en línea del usuario.

A-1 Cómo autenticar clientes a través de la Administración de usuarios

Antes de utilizar la función de Gestión de usuarios, asegúrese de**Basado en el usuario**ha sido seleccionado como el**Modo**en el**Gestión de usuarios>>Configuración general**página.



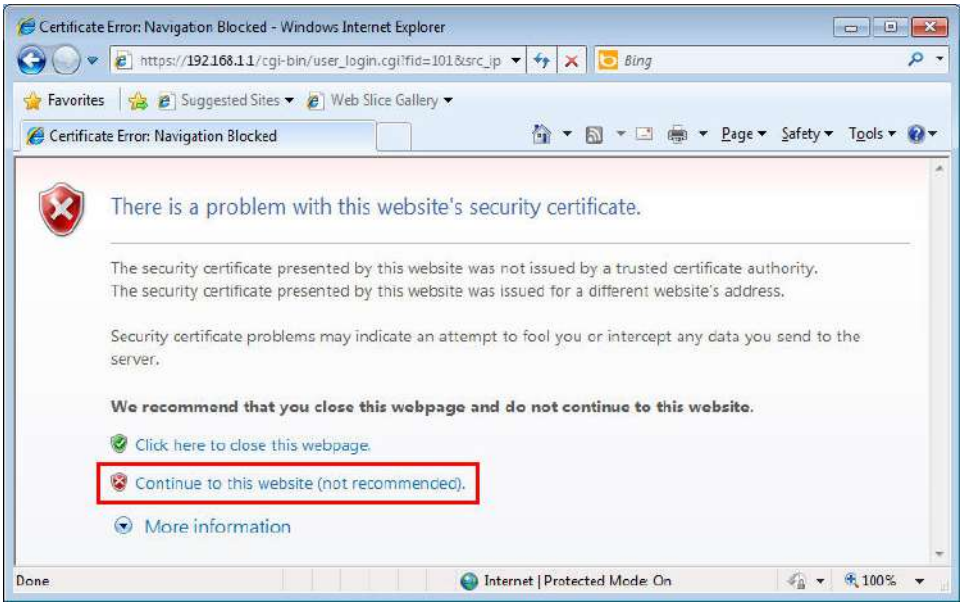
Con**Gestión de usuarios**función de autenticación, antes de que se hayan proporcionado correctamente un nombre de usuario y una contraseña válidos, un cliente en particular no podrá acceder a Internet a través del enrutador. Hay tres formas de autenticación:**Web**,**Telnet**y**Herramienta de alerta**.



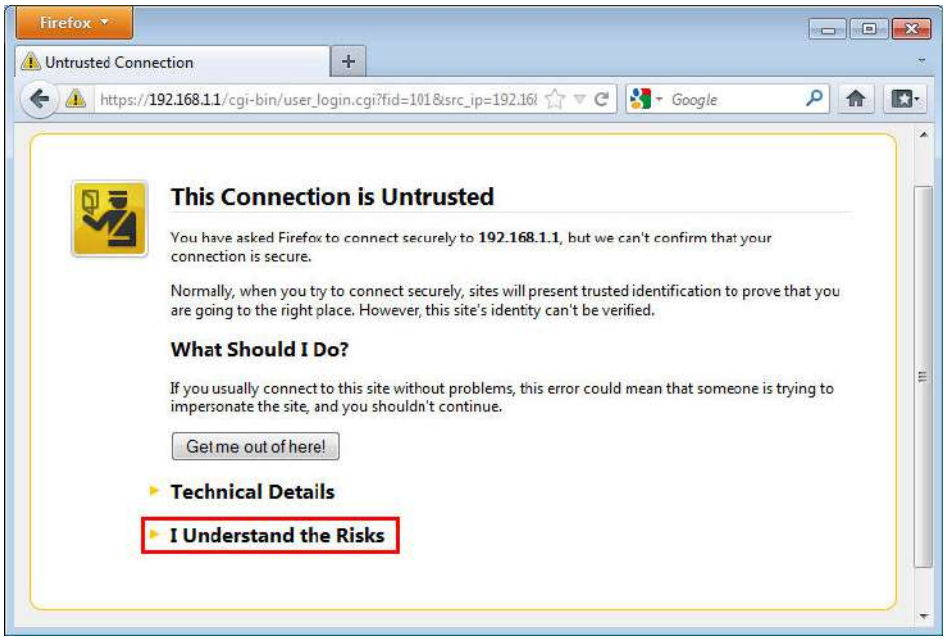
Autenticación vía Web

- Si un cliente LAN que no ha pasado la autenticación abre un sitio web externo en su navegador, primero será redirigido a la interfaz de autenticación web del enrutador. Entonces, el cliente está tratando de accederhttp://www.draytek.com y pero llevado al enrutador Vigor. Dado que se trata de una conexión SSL, algunos navegadores web mostrarán mensajes de advertencia.

    - Con Microsoft Internet Explorer, puede recibir el siguiente mensaje de advertencia. Por favor, pulse**Vaya a este sitio web (no recomendado)**.

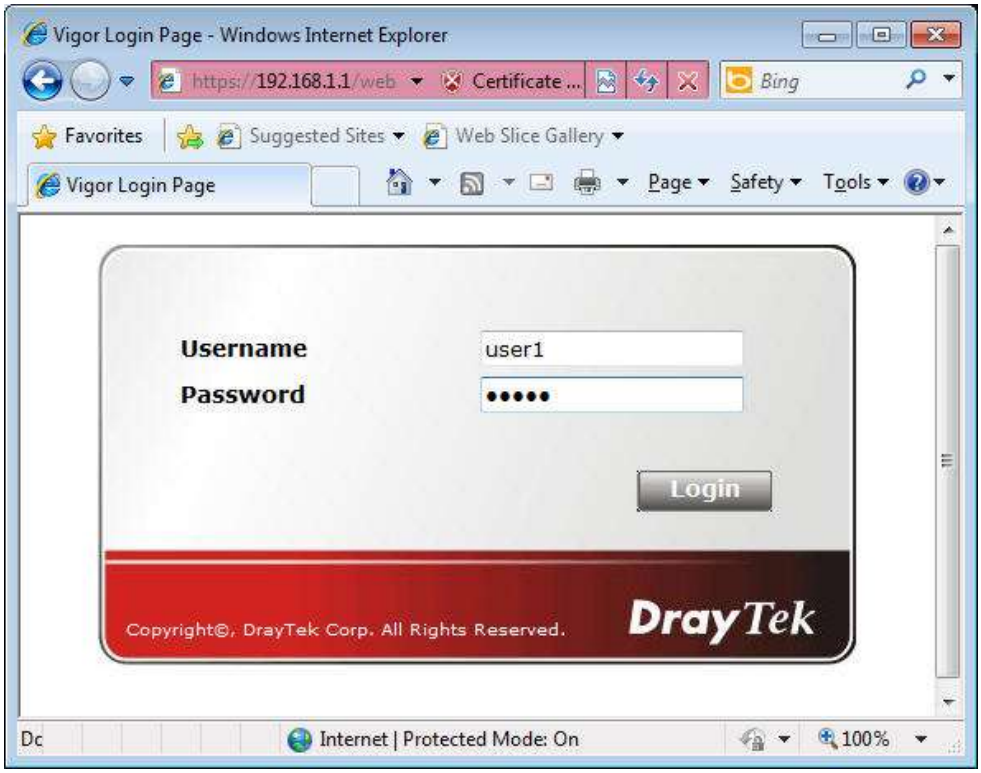


- Con Mozilla Firefox, puede recibir el siguiente mensaje de advertencia. Seleccionar **Entiendo los riesgos**.

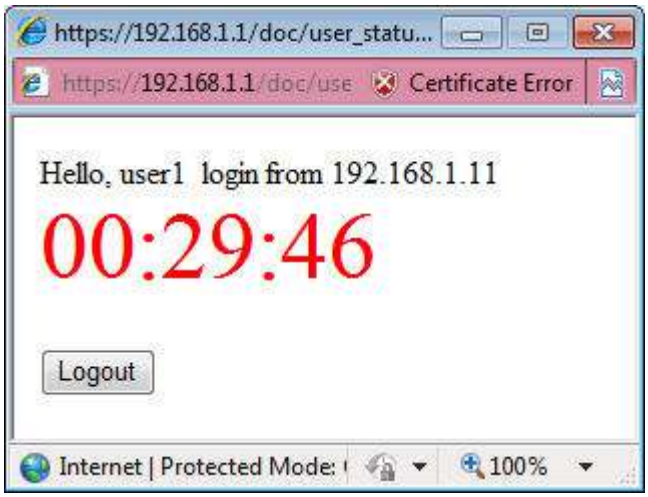


- Con el navegador Chrome, puede recibir la siguiente advertencia. Hacer clic**Procede de todas maneras**.

Después de eso, aparecerá la ventana de autenticación web. Introduzca el nombre de usuario y la contraseña de su cuenta (definida en**Gestión de usuarios**) y haga clic**Acceso**.



Si la autenticación es exitosa, el cliente será redirigido al sitio web original al que intentó acceder. En este ejemplo, es http://www.draytek.com. Además, obtendrá una ventana emergente como la siguiente. A continuación, puede acceder a Internet.

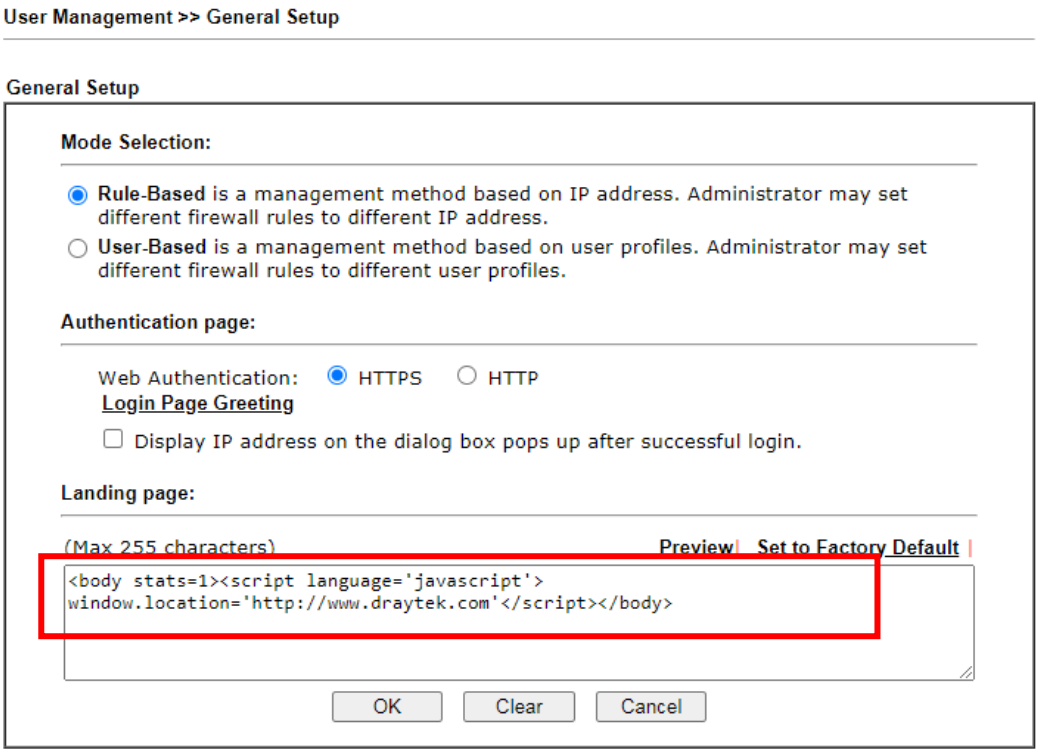


Tenga en cuenta que si bloquea el navegador web para que aparezca cualquier ventana, no verá dicha ventana.

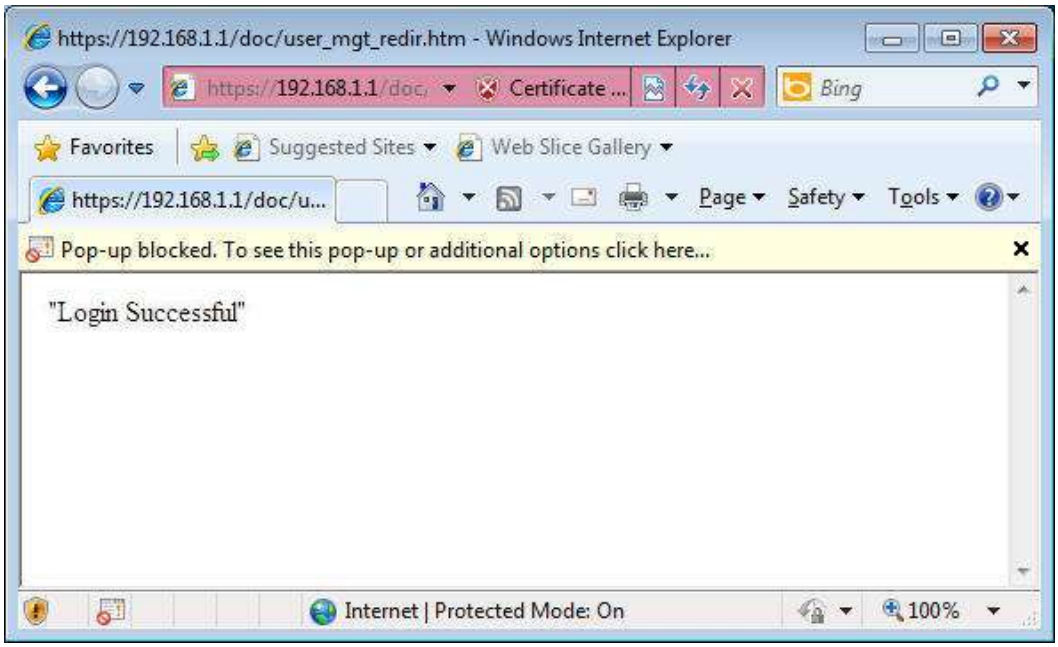
Si la autenticación falla, obtendrá el mensaje de error,**El nombre de usuario o la contraseña son incorrectos**. Inicie sesión de nuevo.

- En la descripción anterior, accede a un sitio web externo para activar la autenticación. También puede acceder directamente a la interfaz de usuario web del enrutador para la autenticación. Se admiten tanto HTTP como HTTPS, por ejemplo, http://192.168.1.1 o https://192.168.1.1. Reemplace 192.168.1.1 con la dirección IP real de su enrutador y agregue el número de puerto si se modificó el puerto de administración predeterminado.

  Si la autenticación es exitosa, obtendrá el**Mensaje de bienvenida**que se establece en el **Gestión de usuarios >> Configuración general**página.



Con la configuración predeterminada**<estadísticas del cuerpo=1><script language='javascript'> ventana.ubicación='http://www.draytek.com'</script></body>,**será redirigido a http:// www.draytek.com. Puedes cambiarlo si quieres. Por ejemplo, obtendrá el siguiente mensaje de bienvenida si ingresa**Inicio de sesión correcto**en el**Mensaje de bienvenida**mesa.



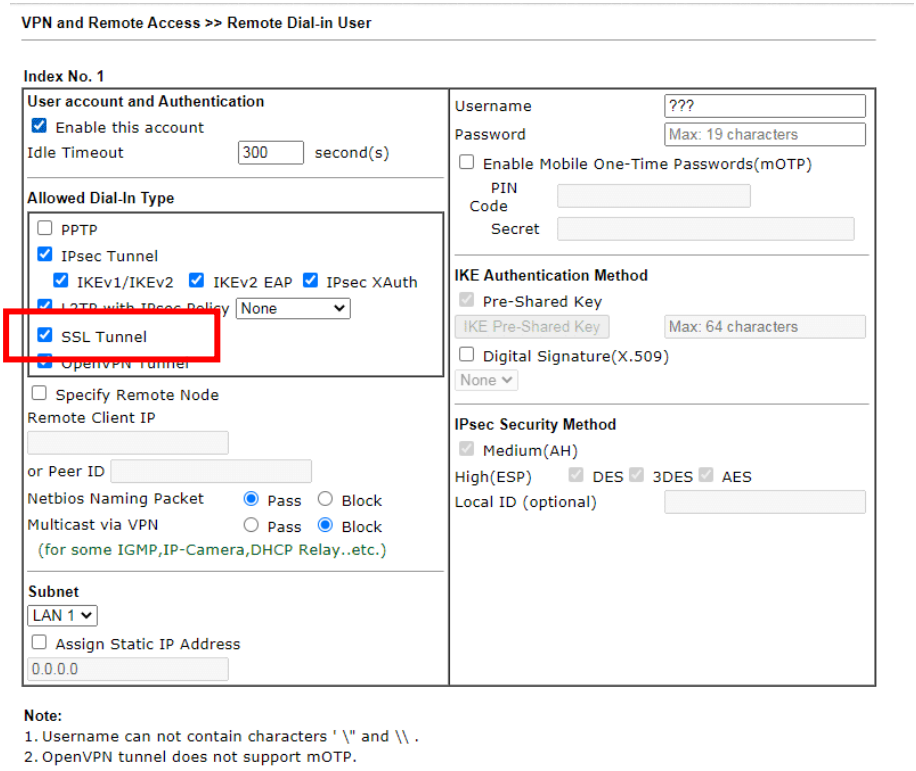
También obtendrás un**Ventana de seguimiento**si no bloquea la ventana emergente.

- No configure un perfil de usuario en**Gestión de usuarios**y un perfil de usuario de VPN Remote Dial-in con el mismo nombre de usuario. De lo contrario, puede obtener resultados inesperados. Esto se debe a que los perfiles de usuario de marcación remota de VPN se pueden extender a los perfiles de usuario en Administración de usuarios para la autenticación.

  Hay dos comportamientos diferentes cuando una cuenta de administración de usuarios y un perfil de VPN comparten el mismo nombre de usuario:

  - Si**Túnel SSL**o**Proxy web SSL**está habilitado en el perfil de VPN, el perfil de usuario en Administración de usuarios siempre será inválido para la autenticación web. Por ejemplo, si

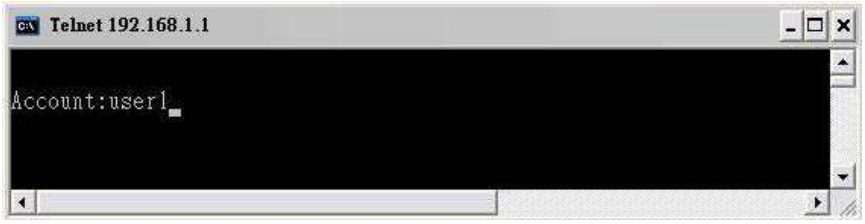
se crea un perfil de usuario en Gestión de usuarios con**chaochen/prueba**como nombre de usuario/ contraseña, mientras que un perfil de usuario de VPN Remote Dial-in con el mismo nombre de usuario “chaochen”pero una contraseña diferente "1234", siempre recibirá un mensaje de error**El nombre de usuario o la contraseña son incorrectos**cuando usas **chaochen/prueba**a través de la Web para hacer la autenticación.



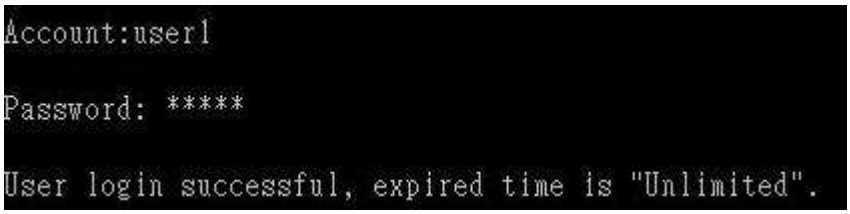
- Si**Túnel SSL**o**Proxy web SSL**está deshabilitado en el perfil de VPN, una cuenta de administración de usuarios y un perfil de VPN de marcación remota pueden usar el mismo nombre de usuario, incluso con diferentes contraseñas. Sin embargo, le recomendamos que utilice diferentes nombres de usuario para diferentes perfiles de usuario en la gestión de usuarios y perfiles de VPN.

Los clientes de LAN también pueden autenticar sus cuentas a través de telnet.

1. Telnet a la dirección IP LAN del enrutador e ingrese el nombre de la cuenta para la autenticación:



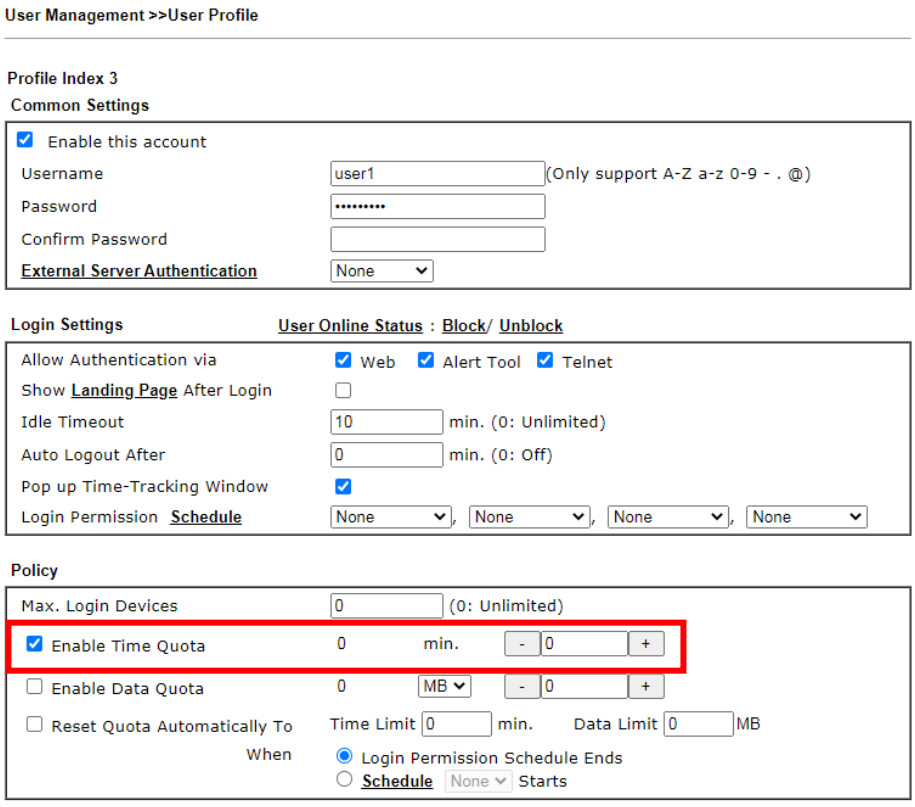
2. Ingrese la contraseña para la autenticación y presione**Ingresar**. El mensaje**Inicio de sesión de usuario exitoso**se mostrará con el tiempo vencido (si está configurado).



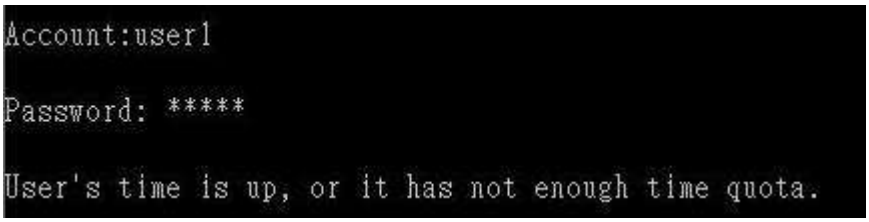
Información

Aquí el tiempo vencido es "Ilimitado" significa que la función de cuota de tiempo no está habilitada para esta cuenta. Después de iniciar sesión, esta cuenta no caducará hasta que cierre la sesión.

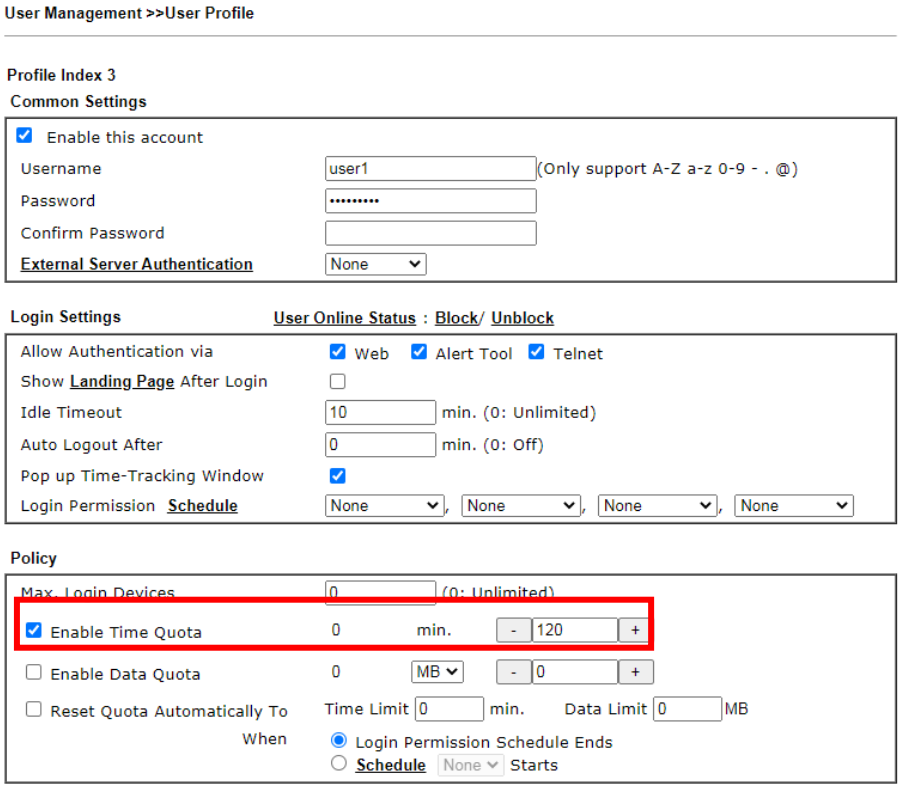
3. En la interfaz web del enrutador, la página de configuración de**Cuota de tiempo**se muestra a continuación.



4. Si la cuota de tiempo se establece en "0" minutos, recibirá el siguiente mensaje, lo que significa que esta cuenta no tiene cuota de tiempo.



Si el**Cuota de tiempo**está habilitado y el tiempo es*no*0 minuto,



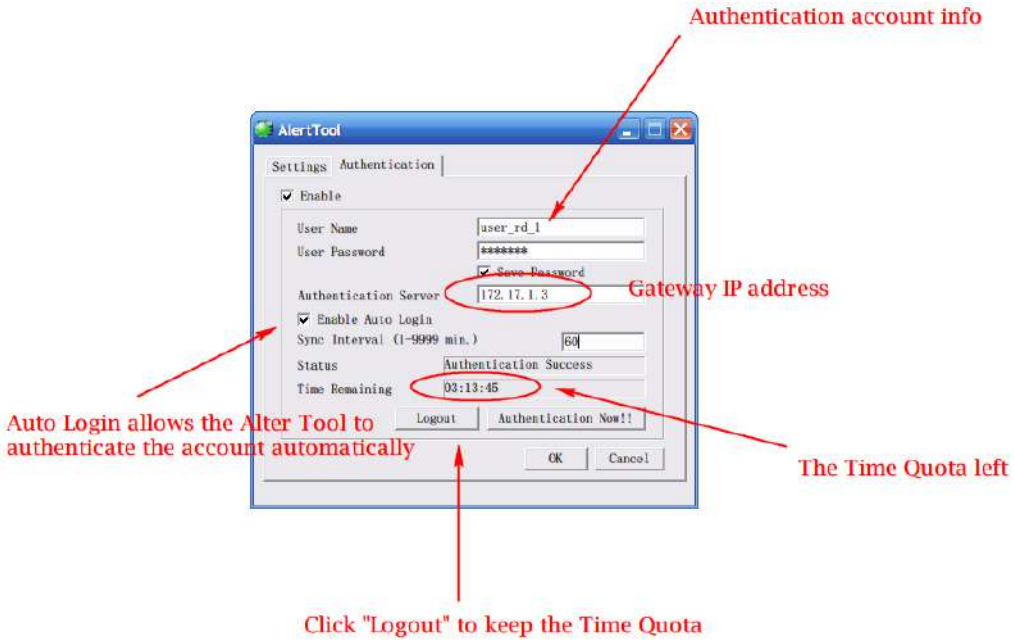
Recibirá el siguiente mensaje. El tiempo vencido se muestra después de iniciar sesión.

Después de agotar el tiempo disponible, no podrá usar más esta cuenta hasta que el administrador agregue manualmente tiempo adicional para usted.

La autenticación vía Web o Telnet es conveniente para los usuarios; sin embargo, tiene algunas limitaciones. La mayor ventaja con VigorPro Alert Notice Tool para operar la autenticación es la capacidad de hacer**ingreso automático**. Si se ha alcanzado el valor de tiempo de espera establecido en el enrutador para la cuenta de usuario, el enrutador impedirá que la computadora cliente acceda a Internet hasta que vuelva a realizar la autenticación. La autenticación a través de VigorPro Alert Notice Tool permite al usuario configurar el intervalo de reautenticación para que la utilidad envíe solicitudes de autenticación periódicamente. Esto evitará que los hosts del cliente tengan que autenticarse manualmente una y otra vez.

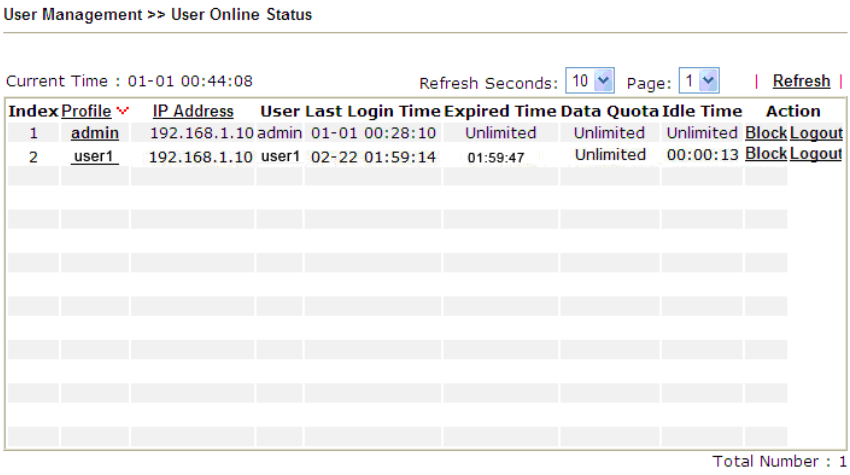
La configuración de VigorPro Alert Notice Tool es la siguiente: 1. Haga clic en

¡¡Autenticar ahora!!para iniciar la autenticación inmediatamente.



2. Puede obtener el**Herramienta de aviso de alerta VigorPro**desde el siguiente enlace: http://www.draytek.com/user/SupportDLUtility.php

Información 1	Cualquier modificación a la política de Firewall romperá las conexiones de todos los usuarios actuales. Todos tienen que autenticarse de nuevo para acceder a Internet.
Información 2	El administrador puede verificar los usuarios actuales de**Estado en línea del usuario**página.

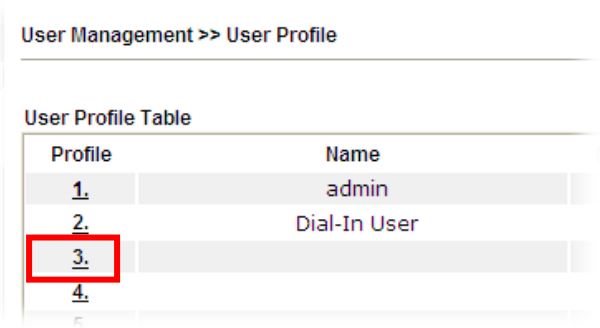


A-2 Cómo utilizar la función de página de destino

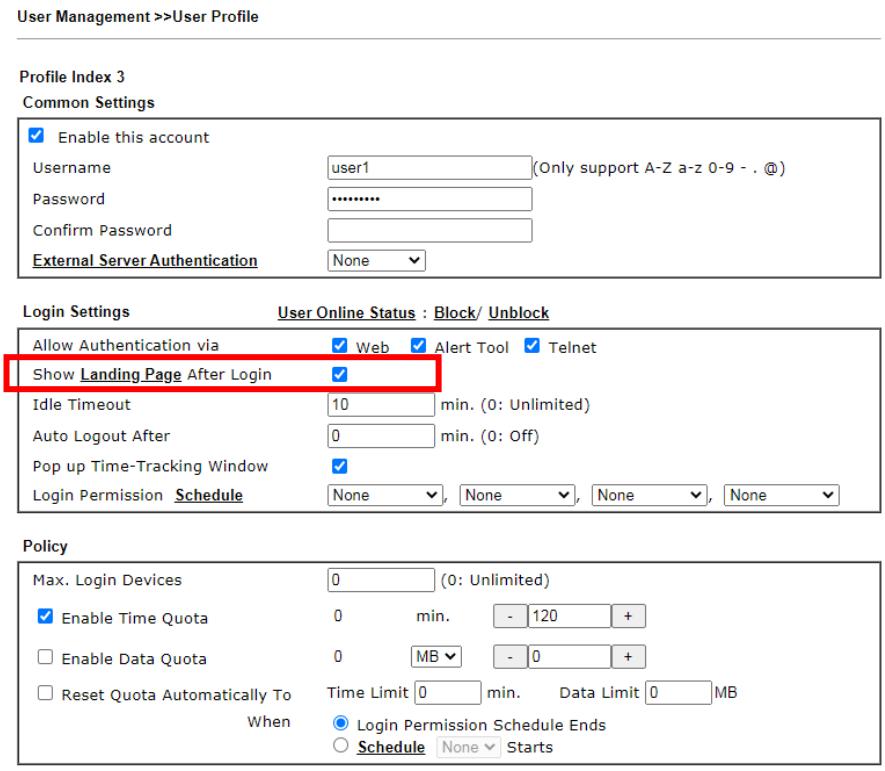
Página de destinoes una característica especial configurada bajo**Gestión de usuarios**. Puede especificar el mensaje, el contenido que se verá o especificar a qué sitio web se accederá cuando los usuarios intenten acceder a Internet pasando la autenticación. Aquí, tomamos el enrutador de la serie Vigor2927 como ejemplo.

Ejemplo 1: los usuarios pueden ver el mensaje de la página de inicio después de iniciar sesión en Internet con éxito

1. Abra la interfaz de usuario web de Vigor2927.
2. Abierto**Gestión de usuarios -> Configuración general**para obtener la siguiente página. En el campo de **Página de destino**, por favor Ingrese las palabras de "**Acceso exitoso**". Tenga en cuenta que el número máximo de caracteres que se pueden escribir aquí es 255.
3. Ahora puede habilitar el**Página de destino**función. Abierto**Gestión de usuarios -> Perfil de usuario** y haga clic en uno de los enlaces de número de índice (p. ej., número de índice 3).



4. En la página siguiente, marque la casilla de**Página de destino**y haga clic**DE ACUERDO**para guardar la configuración.

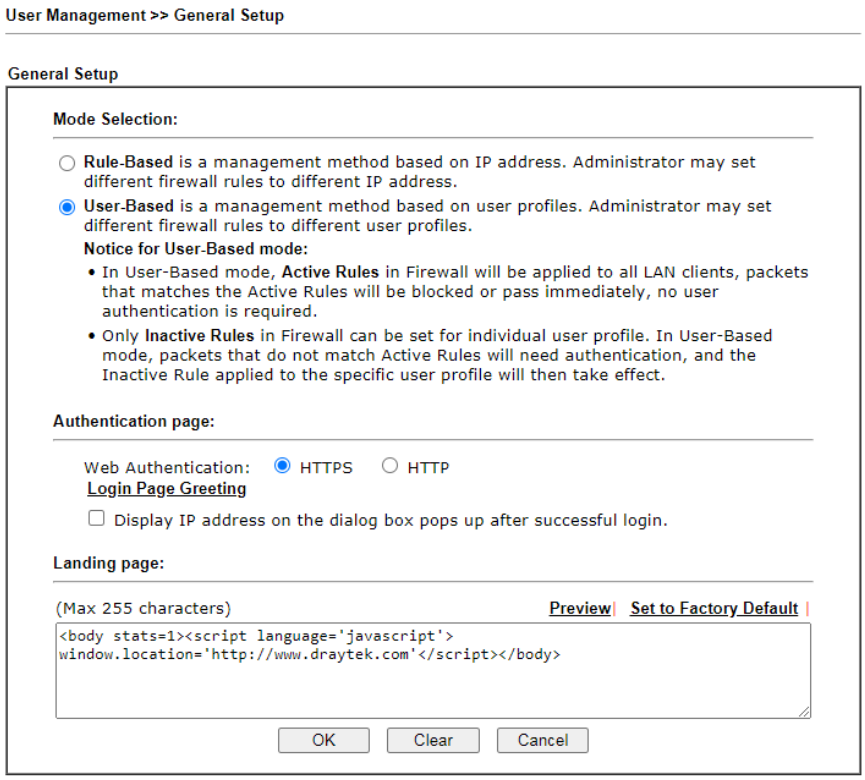


5. Abra cualquier navegador (p. ej., FireFox, Internet Explorer). Aparecerá la página de inicio de sesión y le pedirá un nombre de usuario y una contraseña. Ingrese el nombre de usuario y la contraseña correctos.

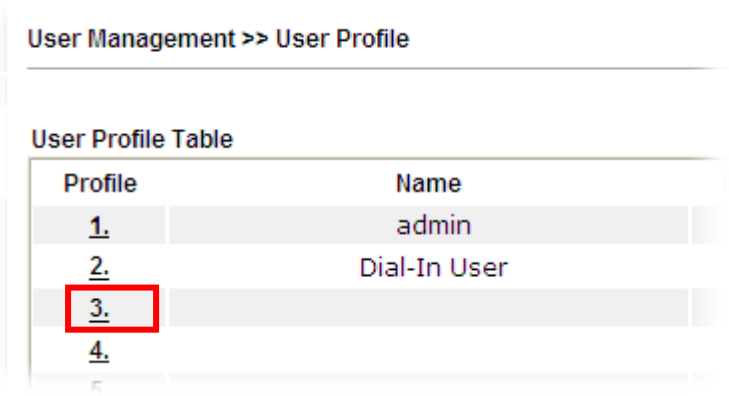
6. Haga clic en**Acceso**. Si el registro es exitoso, verá el mensaje de Inicio de sesión exitoso desde el navegador que utiliza.

Ejemplo 2: el sistema se conectará a http://www.draytek.com automáticamente después de iniciar sesión en Internet con éxito

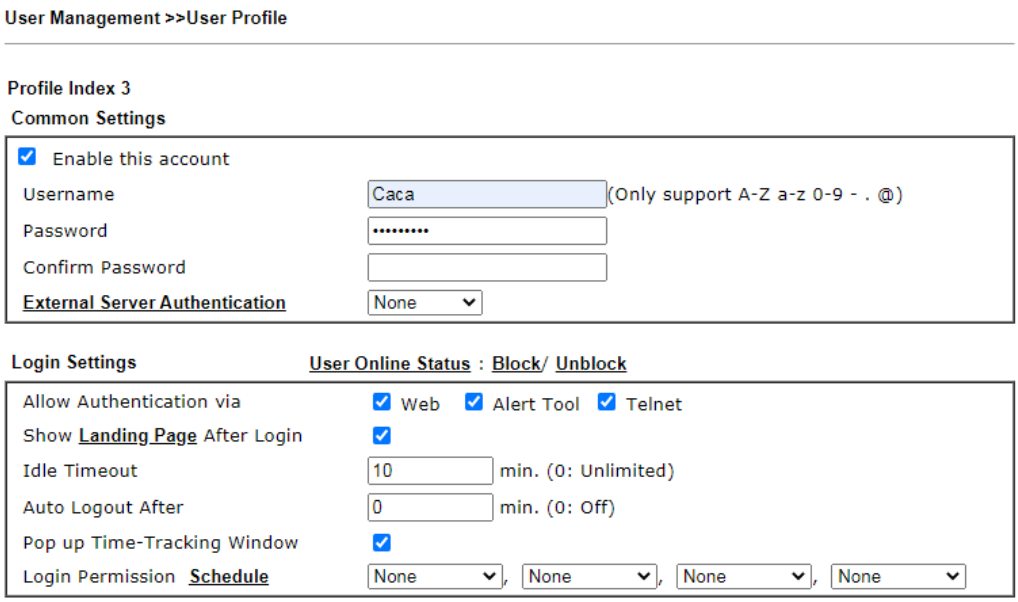
1. En el campo de**Página de destino**, por favor Ingrese las palabras de la siguiente manera: **“ <body stats=1><script language='javascript'> ventana.ubicación='http://www.draytek.com'</script></body>”**



2. A continuación, habilite la**Página de destino**función. Abierto**Gestión de usuarios -> Perfil de usuario**y haga clic en uno de los enlaces de número de índice (p. ej., número de índice 3).

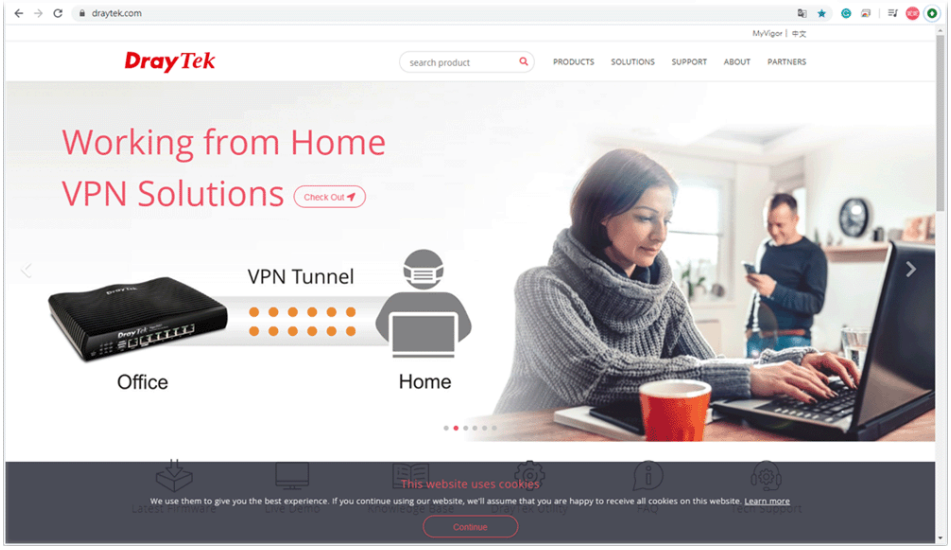


3. En la página siguiente, marque la casilla de**Página de destino**y haga clic**DE ACUERDO**para guardar la configuración.



4. Abra cualquier navegador (p. ej., FireFox, Internet Explorer). Aparecerá la página de inicio de sesión y le pedirá un nombre de usuario y una contraseña. Ingrese el nombre de usuario y la contraseña correctos.

5. Haga clic en**Acceso**. Si el registro es exitoso, será dirigido al sitio web de www.draytek.com.



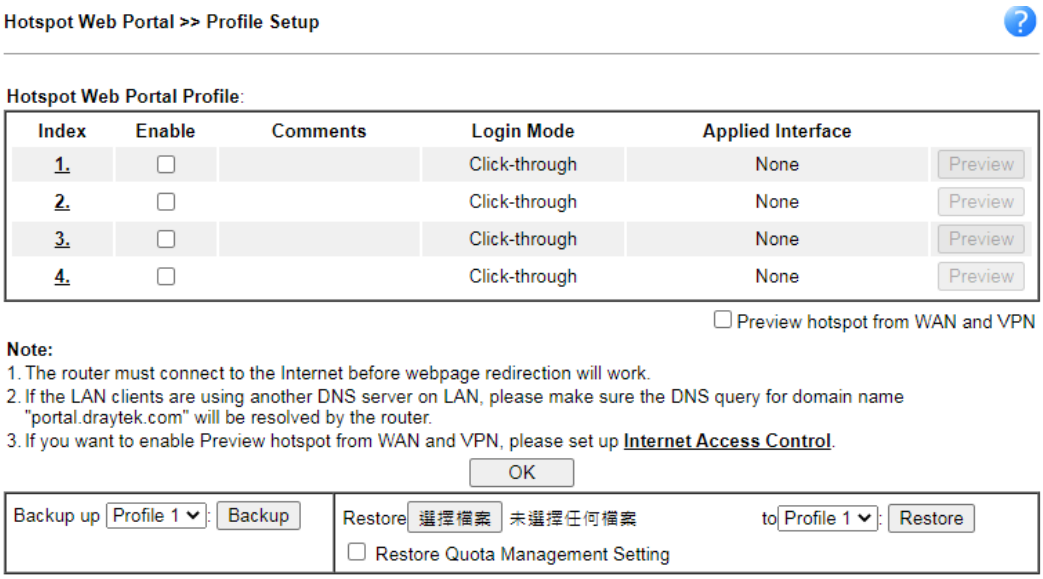
Portal web del punto de acceso VII-4

La función del portal web Hotspot le permite configurar perfiles para que los usuarios de LAN puedan ser redirigidos a direcciones URL específicas o mostrar mensajes cuando se conectan a Internet por primera vez a través del enrutador. Se puede solicitar a los usuarios que lean y acepten los términos y condiciones, o que se autentiquen, antes de obtener acceso a Internet. Otros posibles usos incluyen la publicación de anuncios y materiales promocionales, y la difusión de anuncios de servicio público.

Interfaz de usuario web

Configuración del perfil VII-4-1

Seleccionar**Configuración de perfil**para crear o modificar perfiles del Portal. Se pueden crear hasta 4 perfiles para cumplir con diferentes requisitos según las subredes de LAN, los SSID de WLAN, las direcciones IP de origen y destino, etc.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Índice	Haga clic en el enlace del número de índice para ver o actualizar la configuración del perfil.
Permitir	Marque la casilla para habilitar el perfil.
Comentarios	Muestra la descripción del perfil.

Modo de inicio de sesión	Muestra el modo de inicio de sesión utilizado por el perfil. Ver la sección *Modo de inicio de sesión*para detalles.
Interfaz aplicada	Muestra las interfaces a las que se aplica este perfil.
Avance	Haga clic en este botón para obtener una vista previa de la página del portal web Hotspot que se mostrará a los usuarios.
copia de seguridad	**Lista de perfiles**-Seleccione un perfil de origen. **Respaldo**-Haga clic para guardar el archivo de configuración según el perfil de origen seleccionado.
Restaurar ...	**Seleccionar**-Haga clic para elegir un archivo de configuración. **a**.. - Seleccione un perfil de destino. Será restaurado por el archivo de configuración seleccionado. **Restaurar**-Haga clic para realizar el trabajo de restauración. **Restaurar configuración de gestión de cuotas**-Si se selecciona, la configuración de gestión de cuotas también se restaurará en el perfil de destino.

VII-4-1-1 Método de inicio de sesión

Hay cuatro métodos de inicio de sesión para elegir para autenticar a los clientes de la red:**Saltar inicio de sesión**, **Hacer clic a través**,**Inicio de sesión en varios puntos de acceso**, y**Inicio de sesión en el servidor del portal externo**. Cada modo de inicio de sesión presentará una página web diferente a los usuarios cuando se conecten a la red.

(A) Omitir inicio de sesión, solo página de destino

Este modo no realiza ninguna autenticación. El usuario será redirigido a la página de destino. Luego, el usuario puede abandonar la página de destino para visitar otros sitios web.

(B) Clic de destino

La siguiente página se mostrará a los usuarios cuando intenten acceder a Internet por primera vez a través del enrutador. Después de hacer clic**Aceptar**en la página, los usuarios serán dirigidos a la página de destino (definida en la URL del portal cautivo) y se les otorgará acceso a Internet.

(C) Inicio de sesión en varios puntos de acceso

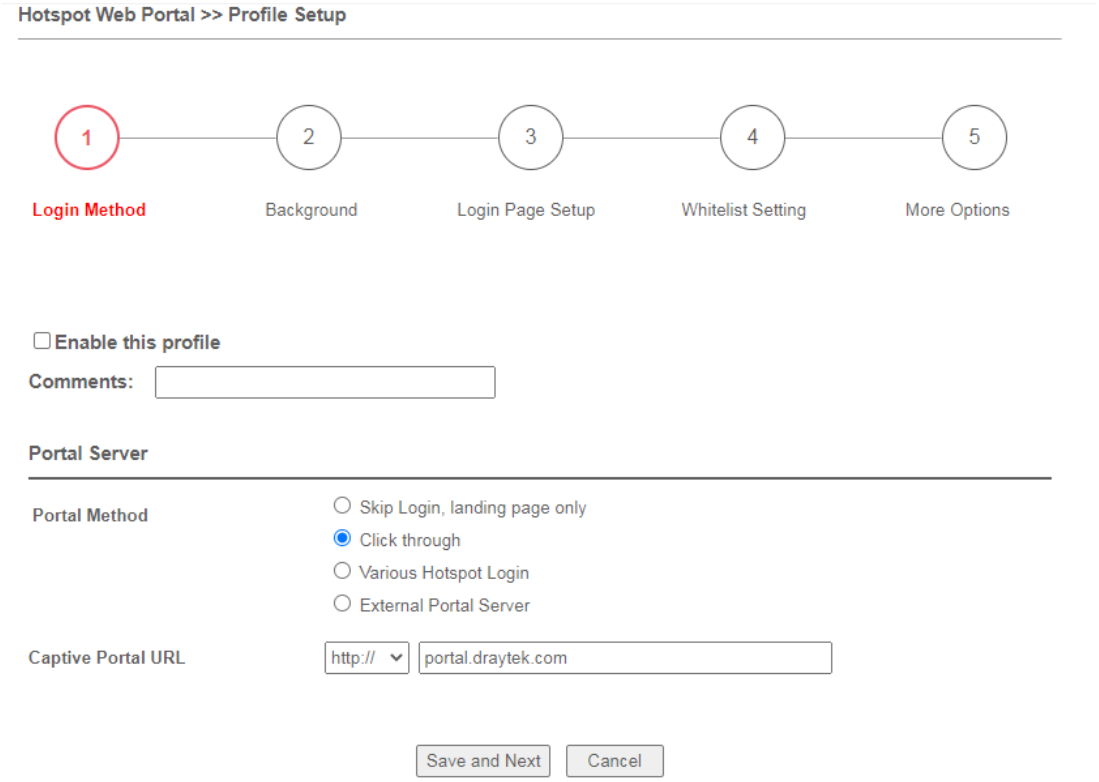
Aparecerá una página de autenticación cuando los usuarios intenten acceder a Internet por primera vez a través del enrutador. Después de autenticarse con una cuenta de Facebook, cuenta de Google, código PIN, contraseña para el servidor RADIUS, serán dirigidos a la página de inicio y se les otorgará acceso a Internet.

(D) Servidor de portal externo

El servidor RADIUS externo autenticará a los usuarios cuando intenten acceder a Internet por primera vez a través del enrutador.

VII-4-1-2 Pasos para configurar un perfil de portal web

Haga clic en el enlace de índice (p. ej., n.º 1) del perfil seleccionado para mostrar la siguiente página.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar este perfil	Marque para habilitar este perfil.
Comentarios	Introduzca una breve descripción para identificar este perfil.
Servidor de portales	
Método del portal	Hay cuatro métodos que se pueden seleccionar para el servidor de portal. Skip Login, landing page only Click through Various Hotspot Login External Portal Server
*Cuando**Omitir registro, solo página de destino**o**Hacer clic a través**se selecciona como método de portal*	
URL del portal cautivo	Introduzca la URL del portal cautivo.
*Cuando**Inicio de sesión en varios puntos de acceso**se selecciona como método de portal*	
URL del portal cautivo	Introduzca la URL del portal cautivo.
Métodos de inicio de sesión	Esta configuración está disponible cuando**Inicio de sesión en varios puntos de acceso**se selecciona como el método del portal.

	Elija el método de inicio de sesión -Seleccione uno o más métodos de inicio de sesión deseados. - Iniciar sesión con Facebook - Iniciar sesión con Google - Recibir PIN por SMS - Recibir PIN por - correo PIN con cupón - Iniciar sesión con RADIUS - Dejar información Iniciar sesión
Facebook (Inicia con Facebook**)**	Esta configuración está disponible cuando**Iniciar sesión con Facebook**está seleccionado como el método de inicio de sesión. **Identificación de la aplicación de Facebook**-Introduce un ID de aplicación de desarrollador de Facebook válido. Si aún no tiene una ID de aplicación, consulte la sección A-1*Cómo crear una ID de aplicación de Facebook para la autenticación del portal web*para obtener instrucciones sobre cómo obtener una ID de aplicación. **Secreto de la aplicación de Facebook**-Ingrese el secreto configurado para la ID de la aplicación ingresada anteriormente. Consulte la sección A-1*Cómo crear una ID de aplicación de Facebook para la autenticación del portal web*para detalles.
Google (Iniciar sesión con Google)	Esta configuración está disponible cuando**Iniciar sesión con Google**está seleccionado como el método de inicio de sesión. **Identificación de la aplicación de Google**-Introduzca un ID de aplicación de Google válido. Si aún no tiene una ID de aplicación, consulte la sección A-2*Cómo crear una ID de aplicación de Google para la autenticación del portal web*para obtener instrucciones sobre cómo obtener una ID de aplicación. **Secreto de la aplicación de Google**-Ingrese el secreto configurado para la ID de la aplicación ingresada anteriormente. Consulte la sección A-2*Cómo crear una ID de aplicación de Google para la autenticación del portal web*para detalles.
Proveedor de SMS (Recibir PIN por SMS)	Esta configuración está disponible cuando**Recibir PIN por SMS**está seleccionado como el método de inicio de sesión. **Recibir PIN a través del proveedor de SMS**-Seleccione el proveedor de SMS utilizado para enviar notificaciones de PIN. Los proveedores de SMS están configurados en**Configuración de objetos >> Objeto de servicio de SMS / correo**.
Servidor de correo (Recibir PIN a través de Correo)	Esta configuración está disponible cuando**Recibir PIN por correo**está seleccionado como el método de inicio de sesión. **Recibir PIN a través del servidor de correo**-Seleccione el servidor de correo utilizado para enviar notificaciones de PIN. Los servidores de correo están configurados en**Configuración de objetos >> Objeto de servicio de SMS / correo**.
Servidor de radio (Iniciar sesión con RADIUS)	Esta configuración está disponible cuando**Iniciar sesión con RADIUS**está seleccionado como el método de inicio de sesión. **método de autentificación**–Haga clic en el enlace para configurar el servidor RADIUS externo para autenticar a los clientes del portal web. **Autenticación RADIUS MAC**–Controlar**Permitir**para activar la autenticación de usuario por dirección MAC. **Formato de dirección MAC**–Seleccione el formato de dirección MAC que utiliza el servidor RADIUS. **Identificador RADIUS NAS**-Introduzca una identificación.
*Cuando**Servidor de portal externo**se selecciona como método de portal*	
URL de redirección	Introduzca la URL a la que se redirigirá al cliente.
Servidor de radio	**método de autentificación**-Para configurar el servidor RADIUS, haga clic en el Servidor RADIUS externo enlace y se le presentará el

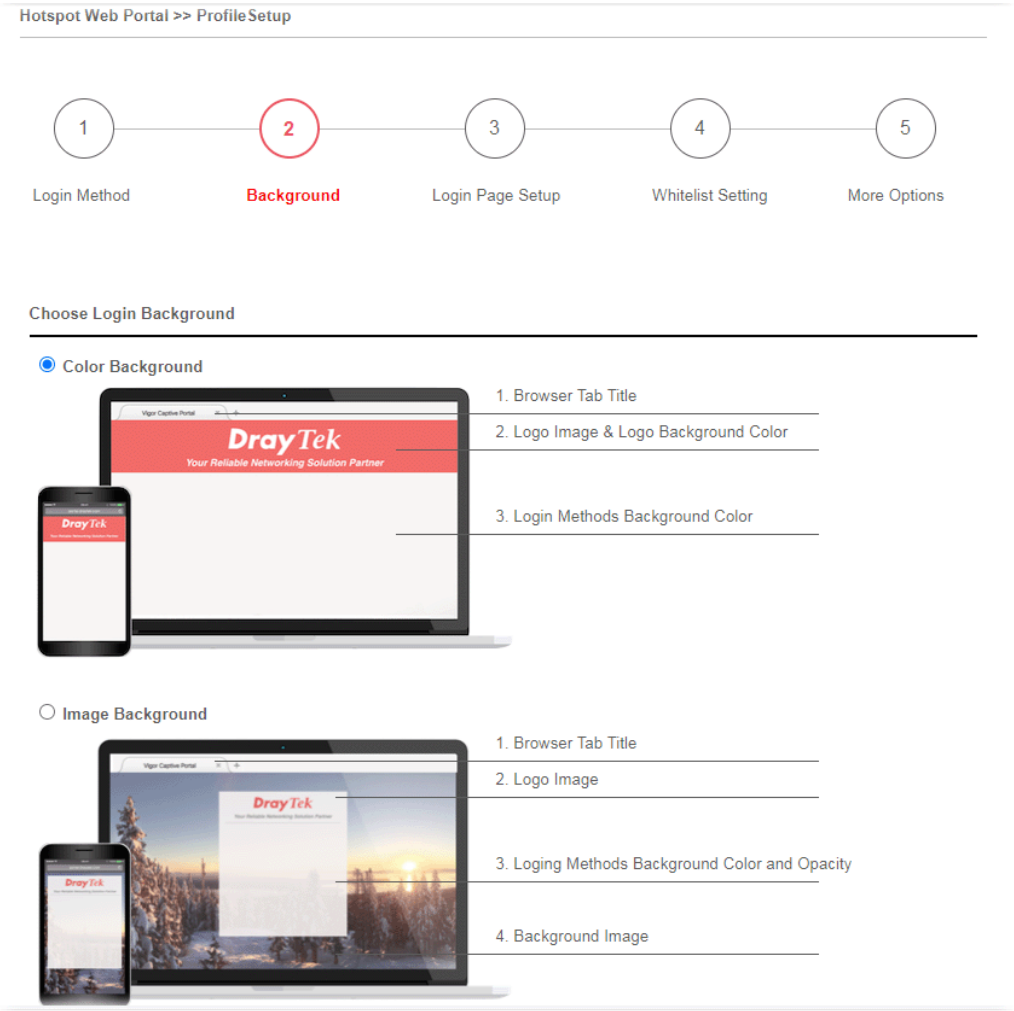
	página de configuración **Autenticación RADIUS MAC**-Si el servidor RADIUS admite la autenticación por dirección MAC, habilite**Autenticación RADIUS MAC**y seleccione el formato de dirección MAC que utiliza el servidor RADIUS. **Formato de dirección MAC**-Seleccione el formato de la dirección MAC. **Identificador RADIUS NAS**-Introduzca una identificación.
Guardar y Siguiente	Haga clic para guardar la configuración en esta página y pasar a la página siguiente.
Cancelar	Haga clic para guardar la configuración en esta página y pasar a la página siguiente.

si has elegido**Omitir inicio de sesión, solo página de destino**o**Servidor de portal externo**como el método del portal, vaya al paso 4*Lista blanca*abajo.

De lo contrario, proceda a configurar la página de inicio de sesión siguiendo los pasos 2 y 3.

2 Fondo

Si ha seleccionado un modo de inicio de sesión que requiere autenticación, seleccione un fondo para la página de inicio de sesión.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Elija iniciar sesión **Fondo**	Seleccione cualquiera**fondo de color**o**Fondo de imagen**como el esquema de fondo de la página de inicio de sesión.
Título de la pestaña del navegador	Introduzca el texto que se mostrará como título de la página web en el navegador.
Logotipo	El logotipo de DrayTek se mostrará de forma predeterminada. Sin embargo, puede ingresar texto HTML o cargar una imagen para reemplazar el logotipo predeterminado.
Fondo del logotipo **Color**	Seleccione el color de fondo del logotipo de DrayTek o seleccione**Personalizar color** e ingrese el valor RGB. Hacer clic**Avance**para obtener una vista previa del color seleccionado.
Método de inicio de sesión **Color de fondo**	Seleccione el color de fondo del panel de inicio de sesión de la lista de colores predefinidos, o seleccione**Personalizar color**e ingrese el valor RGB. Hacer clic**Avance** para obtener una vista previa del color seleccionado.
Opacidad (10 ~ 100)	Disponible cuando**Fondo de imagen**es seleccionado. Establece la opacidad de la imagen de fondo.

Imagen de fondo	Disponible cuando**Fondo de imagen**es seleccionado. Hacer clic**Navegar...**para seleccionar un archivo de imagen (formato .JPG o .PNG), luego haga clic en**Subir** para subirlo al router.
Guardar y Siguiente	Haga clic para guardar la configuración en esta página y pasar a la página siguiente.
Cancelar	Haga clic para cancelar el proceso de configuración y volver a la página de resumen del perfil.

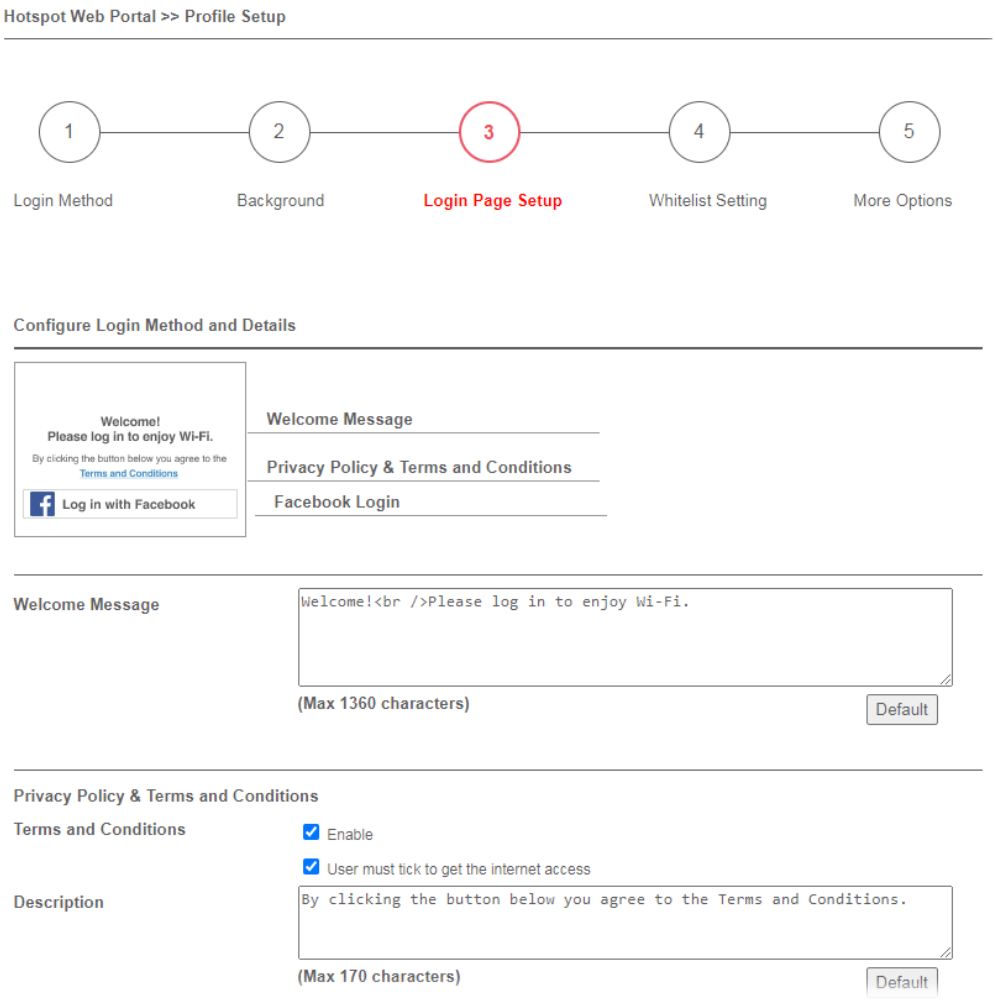
Si ha seleccionado**Omitir inicio de sesión, solo página de destino**o**Servidor de portal externo**como método de portal, continúe con el Paso 4*Configuración de lista blanca*; de lo contrario, continúe con el Paso 3*Configuración de la página de inicio de sesión.*

Configuración de la página de inicio de sesión

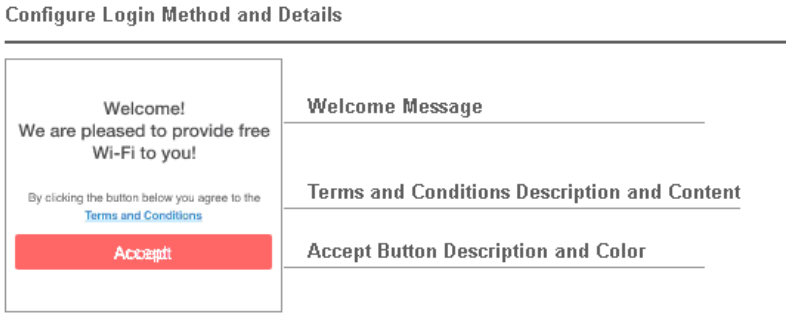
En este paso puede configurar los ajustes para la página de inicio de sesión.

Hacer clic a través

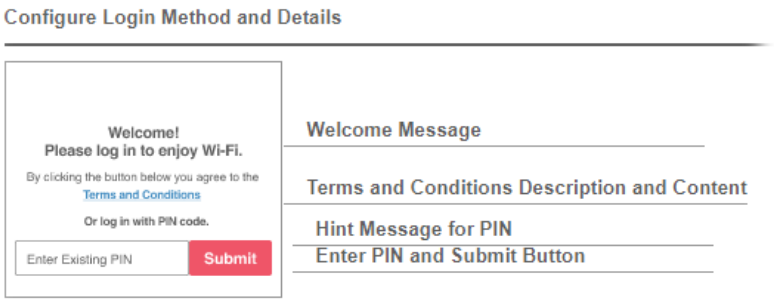
Esta sección describe la configuración de la página de inicio de sesión si ha seleccionado**Hacer clic a través**como método de inicio de sesión.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
El cuadro de diálogo de inicio de sesión se mostrará de la siguiente manera:  Sin embargo cuando**PIN con Vale**se selecciona como el método de inicio de sesión, el cuadro de diálogo de inicio de sesión será	

se muestra de la siguiente manera:

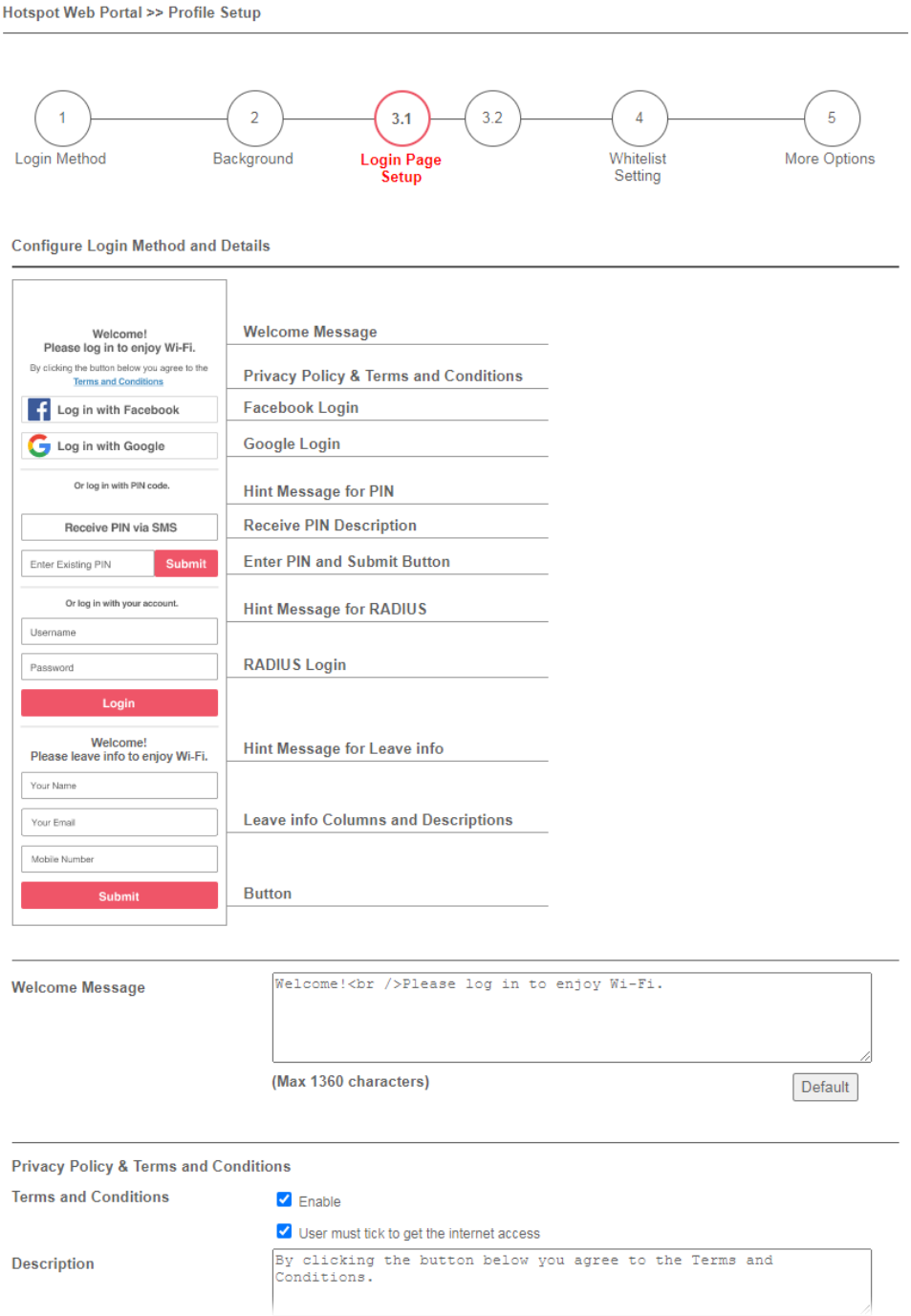


Mensaje de bienvenida	Introduzca el texto que se mostrará como mensaje de bienvenida.
Política de privacidad y términos y condiciones	
Términos y Condiciones	**Permitir**-Marque la casilla para habilitar la opción. **El usuario debe marcar para obtener el acceso a Internet**-Esta casilla de verificación está activada de forma predeterminada si**Términos y condiciones**está habilitado. **Descripción**-Introduzca el texto que se mostrará en la ventana emergente de Términos y condiciones. **Contenido -**Contiene**Contenido interno**y**Contenido externo.** Elija Contenido interno para ingresar el texto que se mostrará como el texto del hipervínculo de Términos y condiciones. O elija Contenido externo para ingresar una URL que mostrará los términos y condiciones.
Recopilación de datos para Marketing	**Permitir**-Marque la casilla para habilitar la opción. **El usuario debe marcar para obtener el acceso a Internet**-Marque la casilla para habilitar la opción. **Descripción**-Introduzca el texto para informar al usuario.
Mensaje de error cuando el usuario no marca	Introduzca el texto para notificar al usuario.
Botón Aceptar Descripción	Introduzca el texto que se mostrará en el botón de aceptar.
Aceptar color del botón	Seleccione el color del botón de aceptar de la lista de colores predefinidos, o seleccione**Personalizar color**e ingrese el valor RGB. Hacer clic **Avance**para obtener una vista previa del color seleccionado.
Guardar y Siguiente	Haga clic para guardar la configuración en esta página y pasar a la página siguiente.
Cancelar	Haga clic para cancelar el proceso de configuración y volver a la página de resumen del perfil.
Cuando**PIN con Vale**se selecciona como el método de inicio de sesión,	
Mensaje de sugerencia para el PIN	Introduzca un mensaje para recordar el código PIN.
Ingrese su PIN Descripción	Introduzca el código PIN existente.
Botón de enviar Descripción	Introduzca el texto que se mostrará en el botón Enviar.
Enviar color del botón	Seleccione el color del botón Enviar de la lista de colores predefinidos, o seleccione**Personalizar color**e ingrese el valor RGB. Hacer clic **Avance**para obtener una vista previa del color seleccionado.
Guardar y Siguiente	Haga clic para guardar la configuración en esta página y pasar a la página siguiente.

Cancelar	Haga clic para cancelar el proceso de configuración y volver a la página de resumen del perfil.

Inicio de sesión en varios puntos de acceso

Esta sección describe el paso de configuración de la página de inicio de sesión si ha seleccionado Varios Hotspot Login como método de inicio de sesión. Solo verá la configuración que sea relevante para los métodos de inicio de sesión seleccionados.

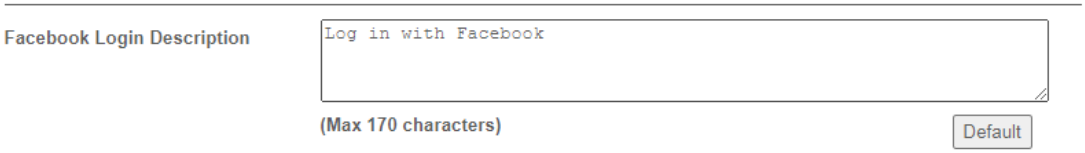


Las configuraciones que son comunes a la autenticación de Facebook, Google, PIN y RADIUS son:

Artículo	Descripción
Mensaje de bienvenida	Introduzca el texto que se mostrará como mensaje de bienvenida.
Términos y Condiciones	**Permitir**-Marque la casilla para habilitar la opción. **El usuario debe marcar para obtener el acceso a Internet**-Esta casilla de verificación es

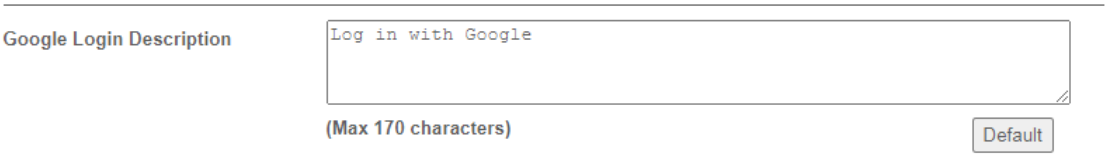
Descripción	activado por defecto si**Términos y condiciones**está habilitado. **Descripción**-Introduzca el texto que se mostrará en la ventana emergente de Términos y condiciones. **Contenido -**Contiene**Contenido interno**y**Contenido externo.** Elija Contenido interno para ingresar el texto que se mostrará como el texto del hipervínculo de Términos y condiciones. O elija Contenido externo para ingresar una URL que mostrará los términos y condiciones.
Recopilación de datos para Marketing	**Permitir**-Marque la casilla para habilitar la opción. **El usuario debe marcar para obtener el acceso a Internet**-Marque la casilla para habilitar la opción. **Descripción**-Introduzca el texto para informar al usuario.
Mensaje de error cuando el usuario no marca	Introduzca el texto para notificar al usuario.

Si ha seleccionado el inicio de sesión de Facebook, aparecerá la configuración:



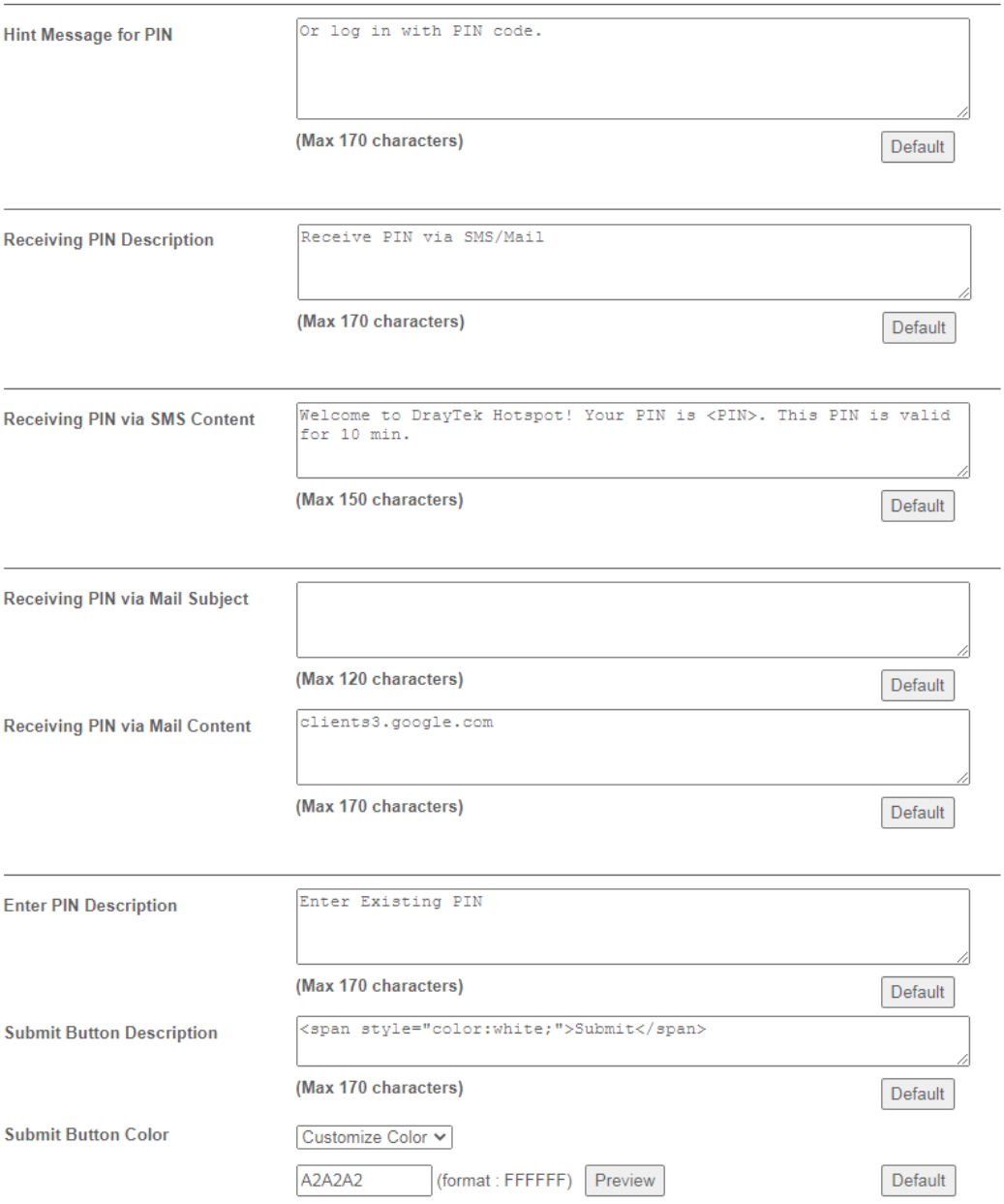
Artículo	Descripción
Inicio de sesión en Facebook Descripción	Introduzca el texto que se mostrará en el botón de inicio de sesión de Facebook.

Si ha seleccionado el inicio de sesión de Google, aparecerá la configuración:



Artículo	Descripción
Inicio de sesión de Google Descripción	Introduzca el texto que se mostrará en el botón de inicio de sesión de Google.

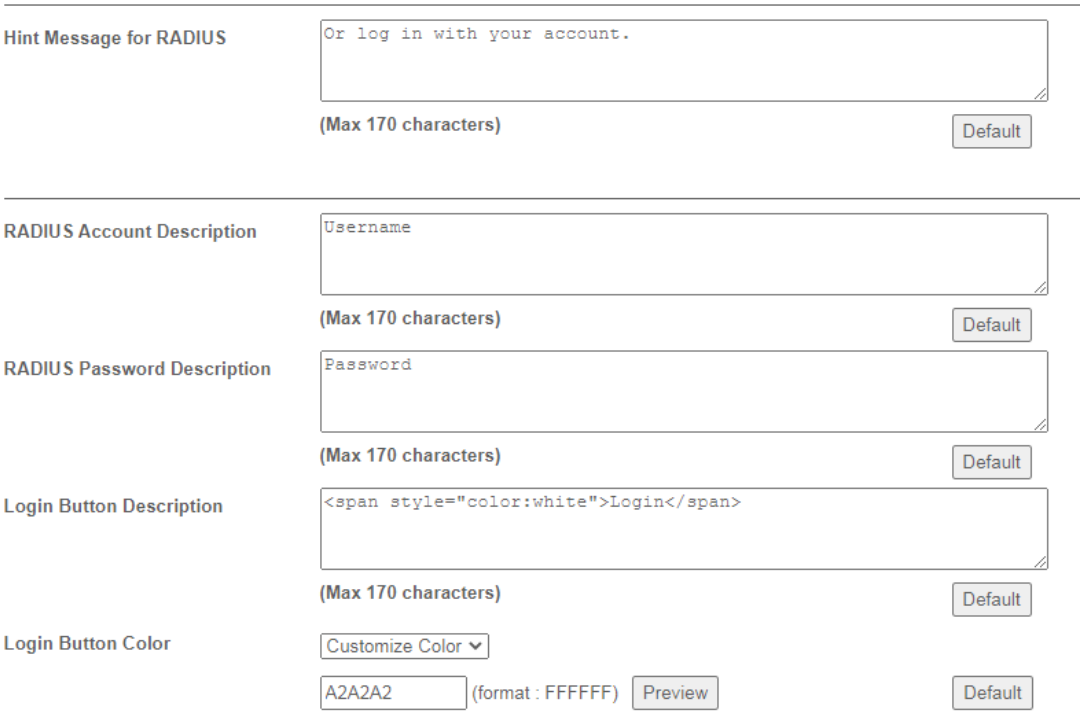
Si ha seleccionado el inicio de sesión con PIN, aparecerán estos ajustes:



Artículo	Descripción
Mensaje de sugerencia para el PIN	Ingrese el texto utilizado para sugerir a los usuarios que elijan la autenticación por SMS.
Recibiendo PIN Descripción	Ingrese el texto que se mostrará en el botón en el que el usuario hace clic para recibir un PIN por SMS.
Recibir PIN a través de Contenido SMS	Introduzca el mensaje a enviar por SMS para informar al usuario del PIN. La variable PIN se especifica mediante**<PIN>**dentro del mensaje.
Recibir PIN a través de Asunto del correo	Introduzca el asunto del correo para informar al usuario sobre el código PIN.
Recibir PIN a través de Contenido del correo	Introduzca el contenido del correo para informar al usuario sobre el código PIN.
Ingrese su PIN **Descripción**	Ingrese el mensaje que se mostrará en el cuadro de texto del PIN para solicitar al usuario que ingrese el PIN.
Botón de enviar	Ingrese el texto que se mostrará en el botón Enviar PIN

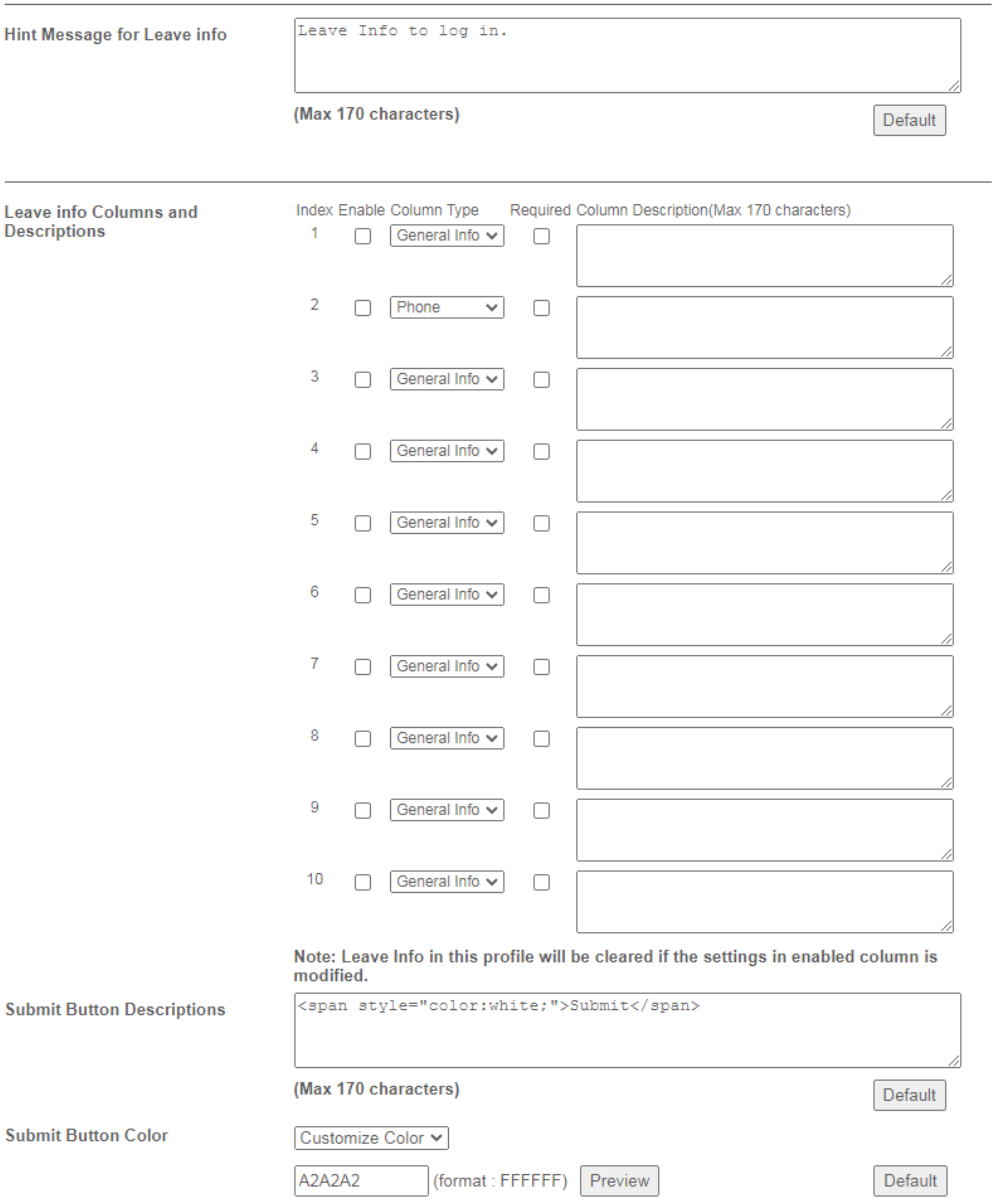
Descripción	
Enviar color del botón	Seleccione el color del botón de envío del color predefinido lista, o seleccione**Personalizar color**e ingrese el valor RGB. Hacer clic **Avance**para obtener una vista previa del color seleccionado.

Si ha seleccionado el inicio de sesión de la cuenta RADIUS, aparecerán estas configuraciones:



Artículo	Descripción
Mensaje de sugerencia para RADIO	Ingrese el texto utilizado para solicitar al usuario que inicie sesión.
Cuenta RADIUS Descripción	Ingrese el texto para solicitar al usuario que ingrese el nombre de usuario.
Contraseña de RADIO Descripción	Ingrese el texto para solicitar al usuario que ingrese la contraseña.
Botón de inicio de sesión Descripción	Introduzca el texto que se mostrará en el botón de inicio de sesión.
Color del botón de inicio de sesión	Seleccione el color del botón de inicio de sesión de la lista de colores predefinidos, o seleccione**Personalizar color**e ingrese el valor RGB. Hacer clic**Avance** para obtener una vista previa del color seleccionado.

Si ha seleccionado Dejar información de inicio de sesión, aparecerán estos ajustes:



Artículo	Descripción
Mensaje de sugerencia para dejar información	Ingrese un mensaje para pedirle al usuario que deje información personal.
Dejar columnas de información **y descripciones**	**Índice**-Hay diez entradas que se pueden modificar. **Permitir**- Marque la casilla para habilitar la configuración de entrada. **Tipo de columna**-Contiene información general, correo electrónico, teléfono y casilla de verificación. **Requerido**-Seleccione para hacer que este artículo sea el artículo requerido. El cliente no puede pasar la autenticación del servidor si no ofrece la información requerida. **Descripción de la columna**-La información se mostrará en una marca de agua para que el usuario complete la información.
Botón de enviar Descripción	Ingrese el texto que se mostrará en el botón Enviar PIN

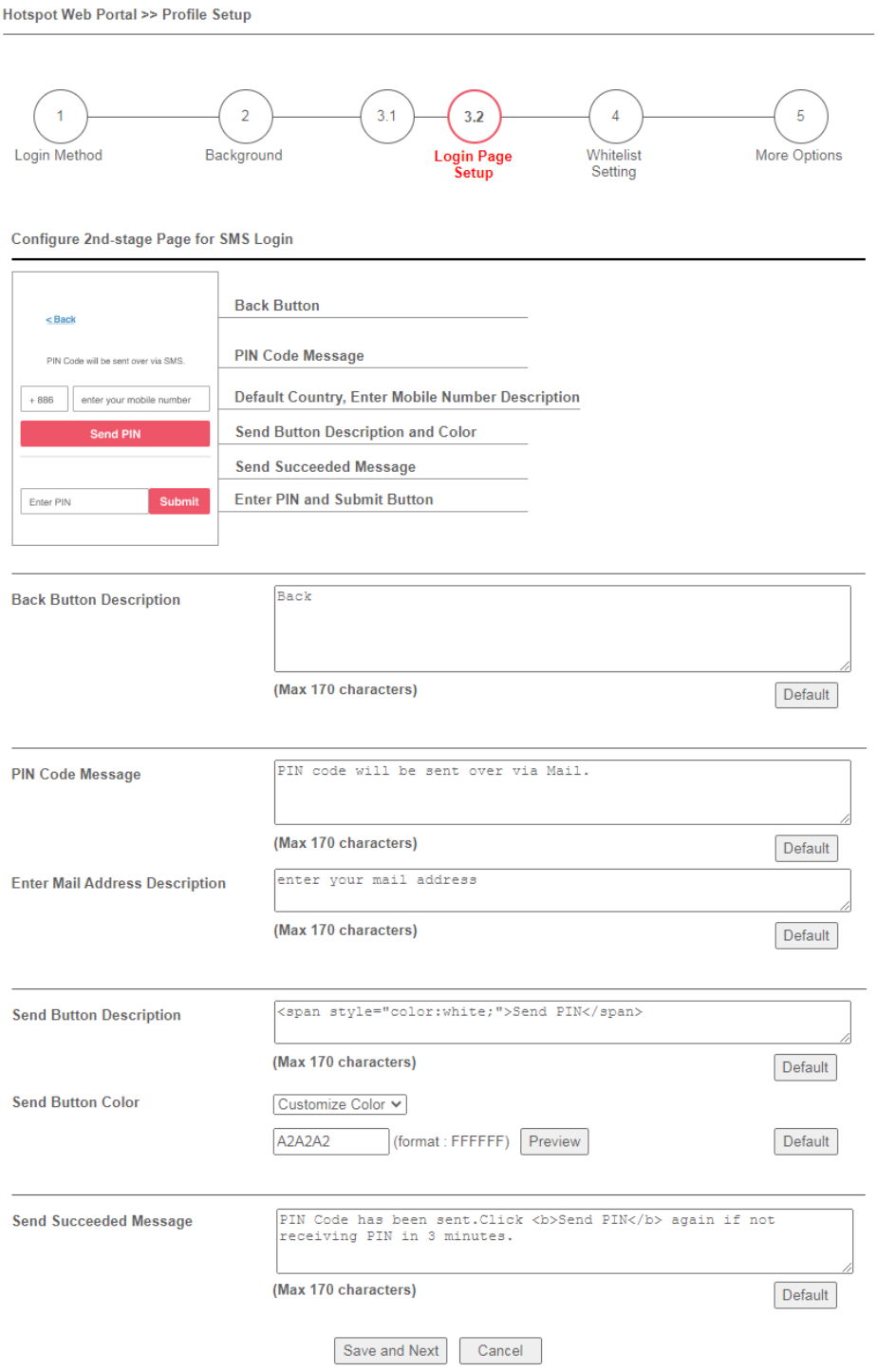
Enviar color del botón	Seleccione el color del botón Enviar de la lista de colores predefinidos, o seleccione**Personalizar color**e ingrese el valor RGB. Hacer clic **Avance**para obtener una vista previa del color seleccionado.

Y por último, siempre se muestran los botones de guardar y cancelar.

Artículo	Descripción
Guardar y Siguiente	Haga clic para guardar la configuración en esta página y pasar a la página siguiente.
Cancelar	Haga clic para cancelar el proceso de configuración y volver a la página de resumen del perfil.

Página de segunda etapa para inicio de sesión con PIN

Si ha seleccionado**PIN de inicio de sesión**como método de inicio de sesión, también deberá configurar la página que se muestra a los usuarios cuando solicitan un PIN.



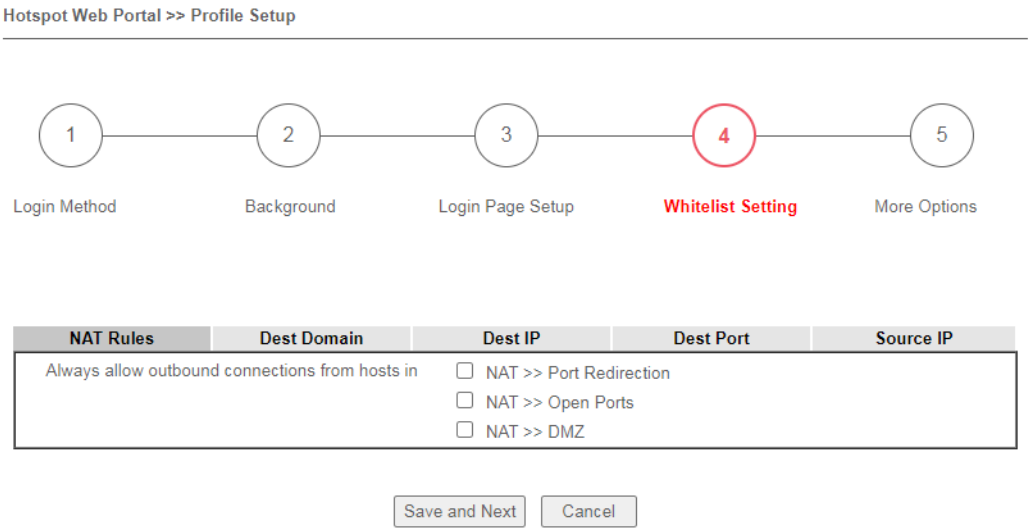
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Botón de retroceso **Descripción**	Introduzca el texto de la etiqueta del hipervínculo para volver a la página anterior.
Mensaje de código PIN	Ingrese el texto que se mostrará como el texto del cuerpo en la página.

País predeterminado **Código**	Seleccione el código de país predeterminado que se mostrará mediante el menú desplegable.
Ingresar móvil **Número Descripción**	Ingrese el mensaje que se mostrará en el cuadro de texto del número de teléfono móvil para solicitar al usuario que ingrese el número de teléfono móvil.
Botón de enviar **Descripción**	Introduzca el texto de la etiqueta del botón de envío.
Enviar color del botón	Seleccione el color del botón de envío de la lista de colores predefinidos, o seleccione **Personalizar color**e ingrese el valor RGB. Hacer clic**Avance** para obtener una vista previa del color seleccionado.
Enviar correctamente **Mensaje**	Ingrese el texto que se mostrará para notificar al usuario después de que se haya enviado el PIN.
Guardar y Siguiente	Haga clic para guardar la configuración en esta página y pasar a la página siguiente.
Cancelar	Haga clic para cancelar el proceso de configuración y volver a la página de resumen del perfil.

Configuración de lista blanca

En este paso puede configurar los ajustes de la lista blanca. Los usuarios pueden enviar y recibir tráfico que cumpla con la configuración de la lista blanca.

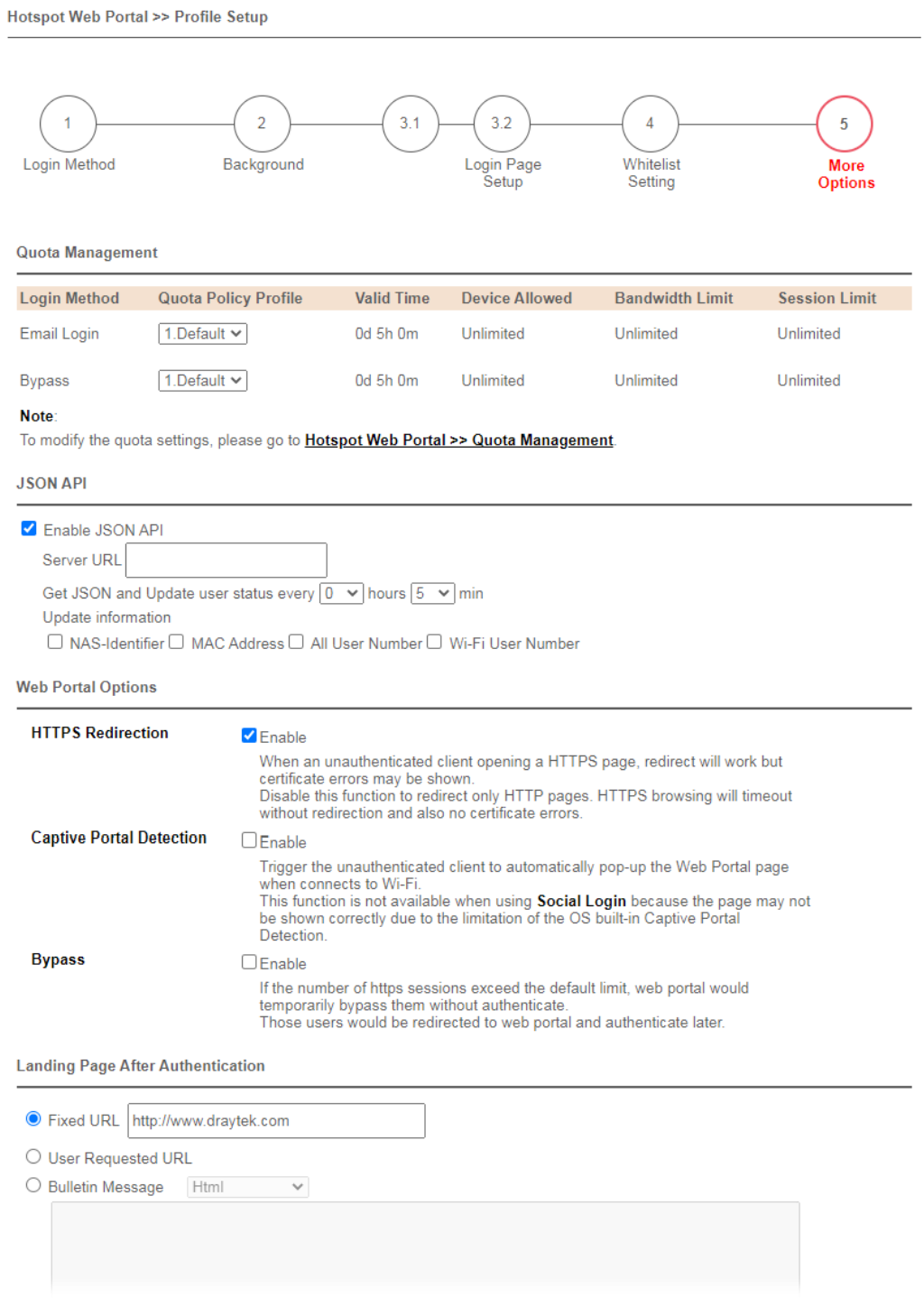


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Reglas NAT	Para evitar que la configuración del portal web entre en conflicto con las reglas NAT y provoque un comportamiento inesperado, seleccione las reglas NAT que pueden omitir el portal web. Los hosts enumerados en las reglas NAT seleccionadas siempre pueden acceder a Internet sin ser interceptados por el portal web.
Dominio de destino	Ingrese hasta 30 dominios de destino a los que se les permita acceder.
IP de destino	Ingrese hasta 30 direcciones IP de destino a las que se les permita acceder.
Puerto de destino	Ingrese hasta 30 protocolos y puertos de destino que se permiten a través del enrutador.
IP de origen	Ingrese hasta 30 direcciones IP de origen que estén permitidas a través del enrutador.
Guardar y Siguiente	Haga clic para guardar la configuración en esta página y pasar a la página siguiente.
Cancelar	Haga clic para cancelar el proceso de configuración y volver a la página de resumen del perfil.

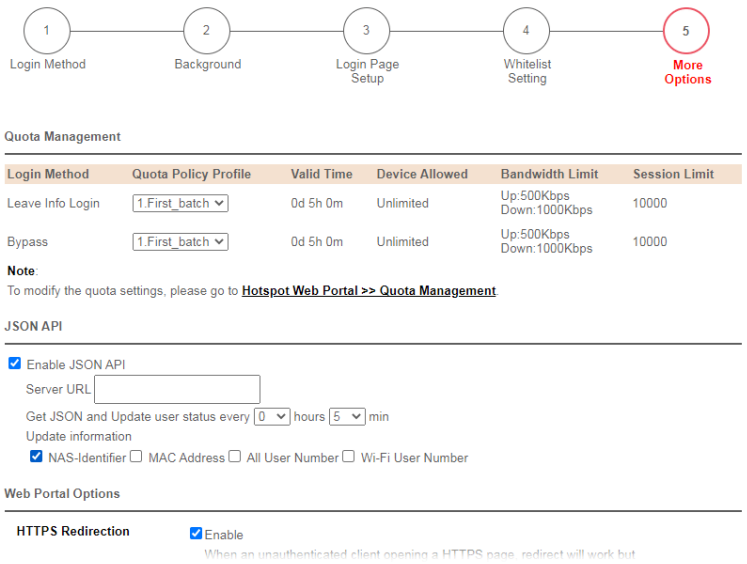
5 Mas opciones

En este paso, puede configurar opciones avanzadas para el portal web Hotspot.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Gestión de cuotas	
Perfil de la política de cuotas	Elija un perfil de política para aplicar a los clientes del portal web.

API de JSON	
Habilitar API JSON	Seleccione para habilitar el formato de API JSON. Un usuario puede modificar la configuración del punto de acceso y obtener la información del usuario sin acceder a la WUI del dispositivo Vigor. **URL del servidor**-Introduzca la dirección IP o el nombre de dominio del servidor remoto. El servidor se usará para editar la configuración del punto de acceso usando el formato API JSON. **Obtenga JSON y actualice el estado del usuario cada x horas x min**-Establezca el intervalo (hora y minuto) para que el enrutador obtenga el JSON y la información del usuario. **Actualizar información**-Seleccione los elementos que serán actualizados por el servidor remoto. 
Opciones del portal web	
Redirección HTTPS	Si se selecciona esta opción, los clientes no autenticados que accedan a sitios web HTTPS serán redirigidos a la página de inicio de sesión, pero el navegador puede alertar al usuario sobre errores de certificado. Si esta opción no está seleccionada, los intentos de acceder al sitio web HTTPS se agotarán sin redirección.
Portal cautivo Detección	Si se selecciona esta opción, la página del portal web se activa automáticamente cuando un cliente no autenticado intenta acceder a Internet. Esta función no está disponible cuando el modo de inicio de sesión está **Inicio de sesión social**, ya que es posible que la página del portal web no se muestre correctamente debido a las limitaciones de la detección de portal cautivo integrada en el sistema operativo.
Derivación	Si la cantidad de sesiones HTTPS excede el límite predeterminado, el portal web las omitirá temporalmente sin autenticación. Esos clientes serían redirigidos al portal web y se autenticarían más tarde.
Página de destino después de la autenticación	
URL fija	Especifica la página web que se mostrará después de que el usuario se haya autenticado correctamente. El usuario será redirigido a la URL especificada. Esto podría usarse para mostrar anuncios a los usuarios, como invitados que solicitan acceso inalámbrico a Internet en un hotel.
URL solicitada por el usuario	El usuario será redirigido a la URL que solicitó inicialmente.

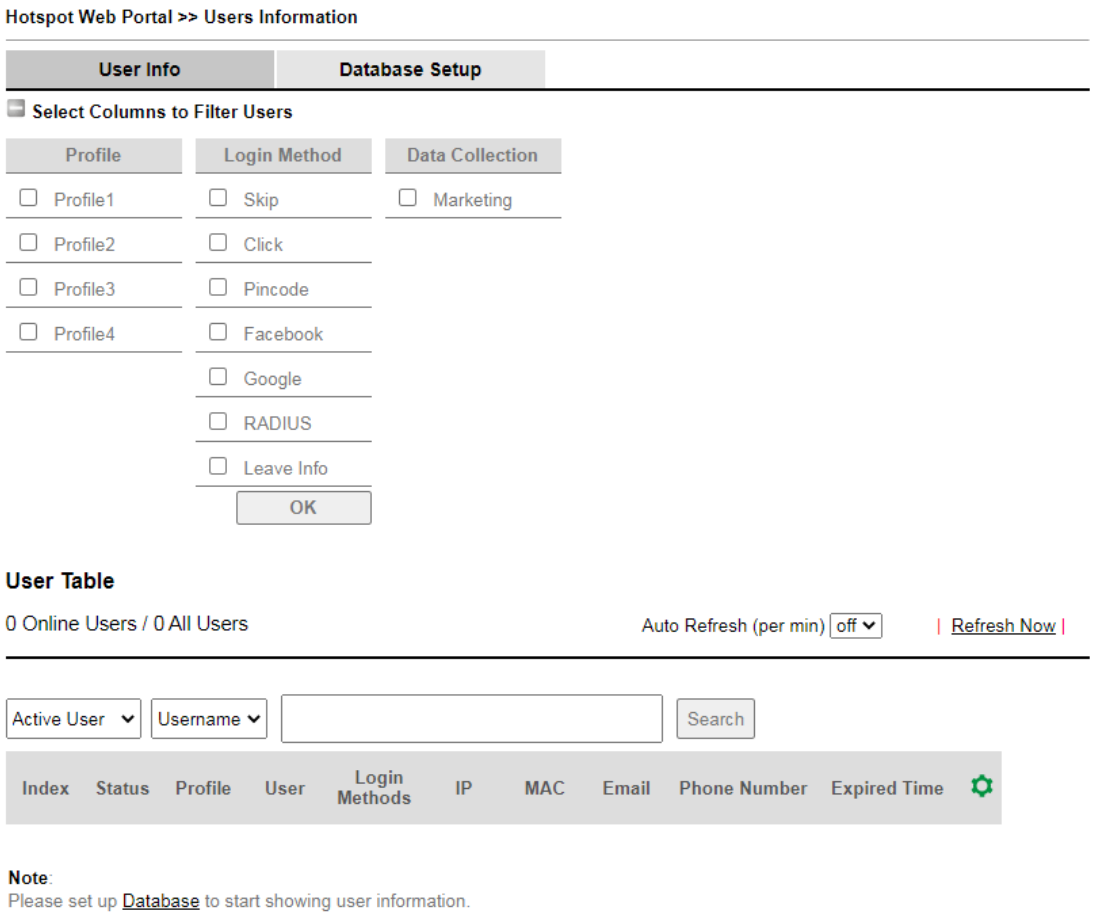
Mensaje de boletín	El mensaje aquí configurado se mostrará brevemente durante unos segundos al usuario. **Mensaje predeterminado:**Este botón está habilitado cuando**Mensaje de boletín**es seleccionado. Haga clic para cargar el texto predeterminado en el cuadro de texto del mensaje del boletín.
Interfaces aplicadas	
subred	El perfil actual del portal web Hotspot estará vigente para las subredes seleccionadas.
WiFi	El perfil actual del portal web Hotspot estará vigente para los SSID de WLAN seleccionados.
Finalizar	Haga clic para completar la configuración.
Cancelar	Haga clic para cancelar el proceso de configuración y volver a la página de resumen del perfil.

VII-4-2 Información del usuario

Esta página muestra información de los usuarios que acceden a Internet a través del portal web. Al hacer clic en el enlace de un usuario, se abrirá una nueva ventana que muestra información detallada sobre ese usuario.

VII-4-2-1 Información del usuario

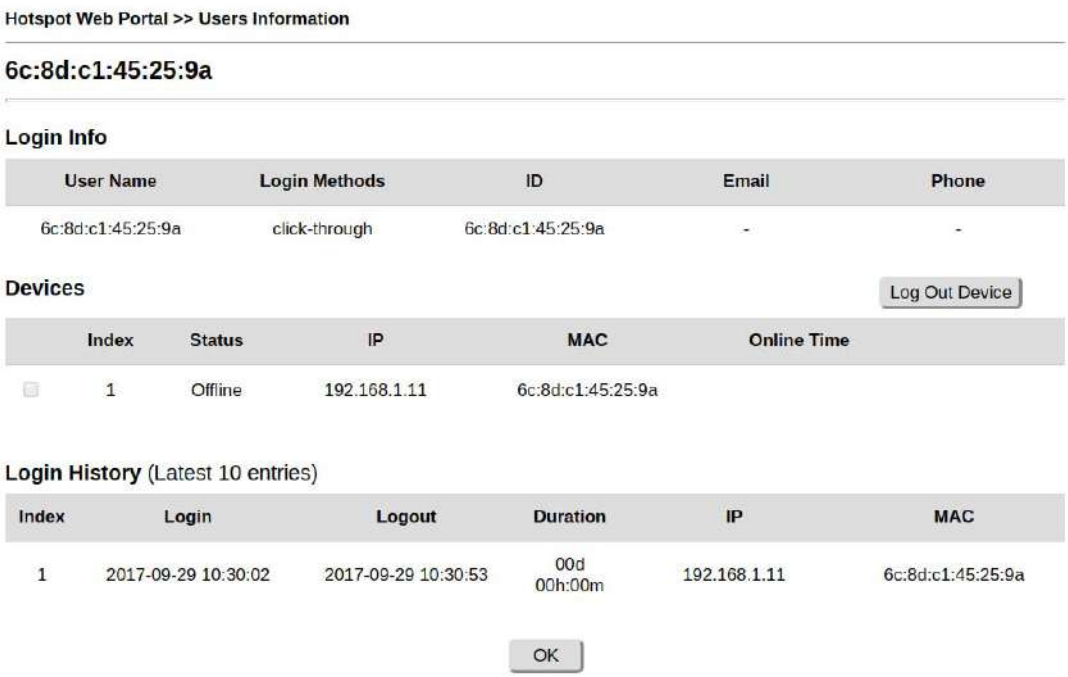
Puede optar por limitar la información de usuario que se muestra agregando filtros de perfil o de método de inicio de sesión.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Seleccionar columnas para Filtrar usuarios	Seleccione los perfiles y los métodos de inicio de sesión para filtrar los usuarios mostrados. Esto es útil cuando hay muchos usuarios y desea administrar solo un subconjunto de usuarios en función de sus perfiles y/o métodos de inicio de sesión.
Tabla de usuarios	Los detalles de los usuarios que acceden a Internet a través del portal web Hotspot se mostrarán en esta sección.

Haga clic en el enlace de la dirección MAC (o código PIN, nombre de Facebook/Google, cuenta de RADIUS) para un usuario en particular y se mostrará información detallada sobre el dispositivo seleccionado en la siguiente página.



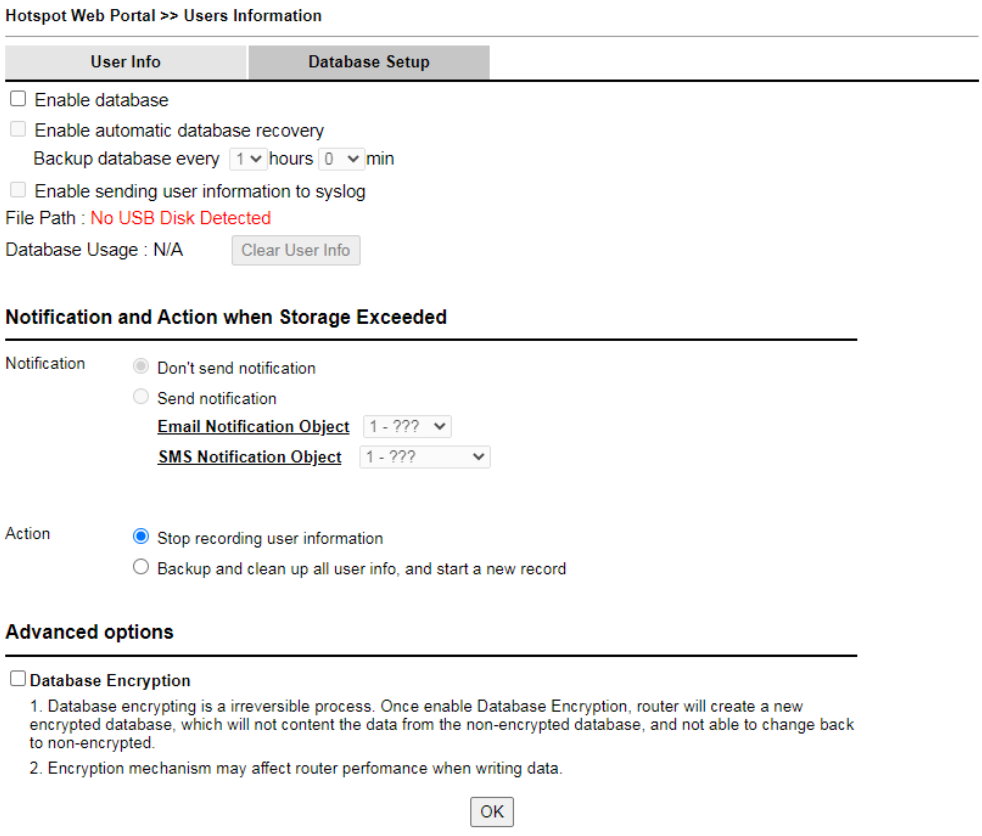
La información sobre el usuario se muestra en la sección Información de inicio de sesión.

Los dispositivos utilizados por el usuario se muestran en la sección Dispositivos. Para cerrar la sesión de un dispositivo a la fuerza, seleccione la casilla de verificación frente al dispositivo y haga clic en el botón Cerrar sesión del dispositivo.

La sección Historial de inicio de sesión muestra las 10 sesiones de inicio de sesión más recientes del usuario.

VII-4-2-2 Configuración de la base de datos

Esta página permite al usuario configurar los ajustes de la base de datos en el disco USB.



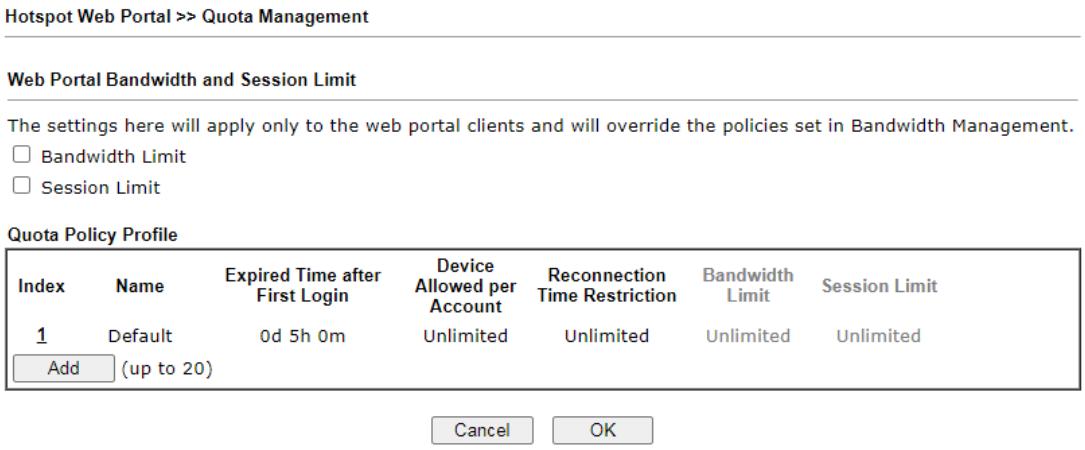
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar base de datos	Marque la casilla para registrar la información del usuario en la base de datos del enrutador. Antes de marcar esta casilla, primero inserte un disco USB con espacio de almacenamiento adecuado.
Habilitar automático recuperación de base de datos	Marque la casilla para habilitar la funcionalidad de la recuperación de la base de datos en el disco USB. **Copia de seguridad de la base de datos cada**... - Establece el intervalo para hacer una copia de seguridad de la base de datos.
Habilitar usuario remitente información a registro del sistema	Marque la casilla para enviar información de usuario a syslog.
Ruta de archivo	Si se ha insertado un disco USB en el puerto USB del enrutador Vigor, la ruta del archivo se mostrará en esta área.
Uso de la base de datos	Muestra el uso y el espacio restante en la base de datos. **Borrar información de usuario**–La información del usuario se mostrará en la página de Información del usuario. Puede eliminar la información haciendo clic en este botón.
Notificación y acción cuando se excede el almacenamiento	
Notificación	**No enviar notificación -**El sistema de enrutador Vigor no enviará ninguna notificación a ningún destinatario. **Enviar notificación**-El sistema del enrutador Vigor enviará un correo electrónico de notificación a los destinatarios especificados que seleccionaron de**Objeto de notificación de correo electrónico**y**Objeto de notificación SMS**.
Acción	**Dejar de registrar la información del usuario –**El sistema del enrutador Vigor se detendrá para registrar la información del usuario en el disco USB. **Haga una copia de seguridad y limpie toda la información del usuario, y comience un nuevo registro:**El sistema de enrutador Vigor hará una copia de seguridad de toda la información existente en el disco USB en el host y limpiará la información del disco USB. Más tarde, comenzará un nuevo registro.
Opciones avanzadas	
Cifrado de base de datos	Seleccione para que el enrutador cree una nueva base de datos cifrada. Una vez hecho esto, no podrá volver a una base de datos sin cifrar.

VII-4-3 Gestión de cuotas

El administrador del sistema puede especificar el ancho de banda y la cuota de sesiones que solo se aplica a los clientes del portal web.

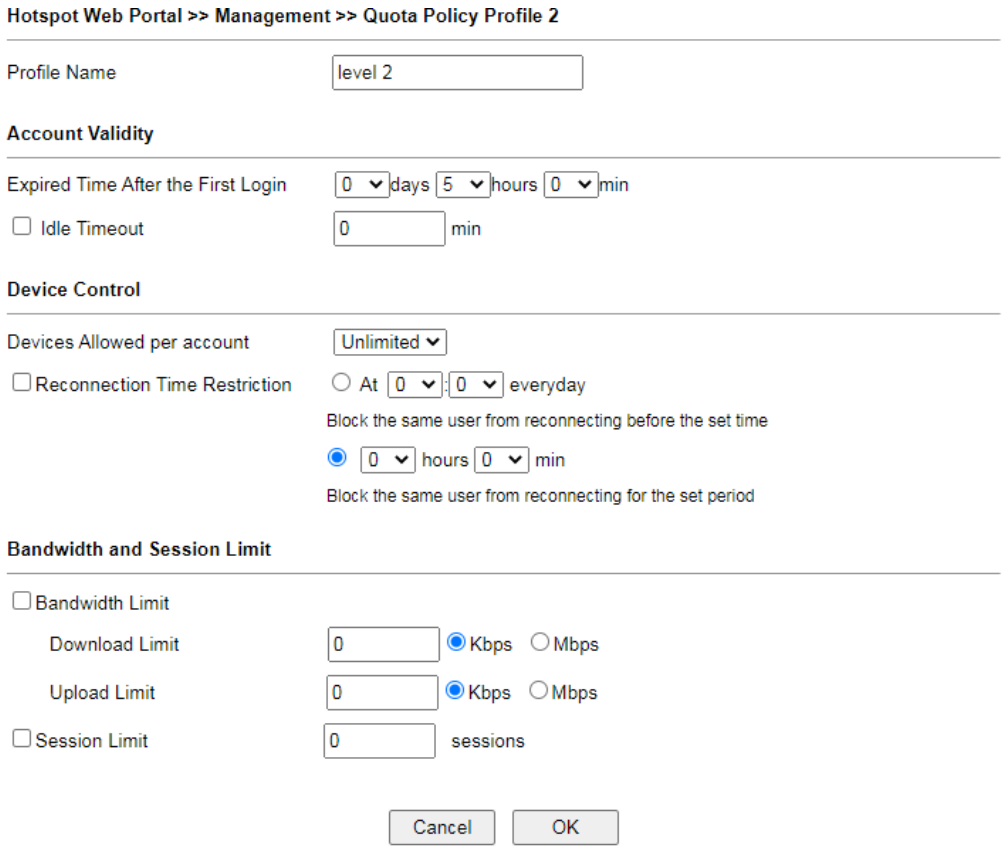
Los ajustes configurados en Gestión de cuotas anularán las políticas establecidas en**Gestión de ancho de banda>>Límite de ancho de banda**y**Gestión de ancho de banda>>Límite**.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Límite de ancho de banda	Marque la casilla para anular la política configurada en**Gestión de ancho de banda>>Límite de ancho de banda.**
Límite de sesión	Marque la casilla para anular la política configurada en**Gestión de ancho de banda>>Límite de sesión.**
Perfil de la política de cuotas	**Agregar**-Cree hasta 20 perfiles de políticas en dicha página.

Para crear un nuevo perfil de política de cuotas, haga clic en**Agregar**para abrir la página siguiente.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre de perfil	Introduzca un nombre para un nuevo perfil.
Validez de la cuenta	Establezca la duración durante la cual el inicio de sesión es válido. **Tiempo vencido después del primer inicio de sesión**–Establece los días, las horas y los minutos. Una vez que haya expirado el inicio de sesión, el enrutador Vigor bloqueará el acceso del cliente a la red/Internet. **Tiempo de inactividad**–Cuando se selecciona esta opción, el enrutador Vigor terminará la conexión de red si no hay actividad del usuario después de que haya pasado el tiempo de inactividad especificado.
Control del dispositivo	Establezca la cantidad máxima de dispositivos que se pueden conectar para cada cuenta y la restricción de tiempo para que el cliente acceda a Internet a través del portal web. **Dispositivos permitidos por cuenta**–Use la lista desplegable para seleccionar la cantidad máxima de dispositivos que se pueden conectar a la red usando la misma cuenta. **Restricción de tiempo de reconexión**–Bloquea el uso de la cuenta para conectar dispositivos a la red de una de dos maneras: - **En .... Cada día**–Después de que caduque el inicio de sesión, la cuenta no se puede usar para conectar dispositivos a la red hasta la hora del día establecida. - **Horas.. min**–Una vez que expira el inicio de sesión, la cuenta no se puede usar para conectar dispositivos a la red durante un período de tiempo determinado.
Ancho de banda y Límite de sesión	**Límite de ancho de banda**–Marque la casilla para configurar el límite de ancho de banda para el cliente del portal web.

	- **Límites de descarga/carga**–Establece las velocidades máximas de carga y descarga. **Límite de sesión**- Marque la casilla para configurar un límite máximo de sesión para los clientes del portal web.

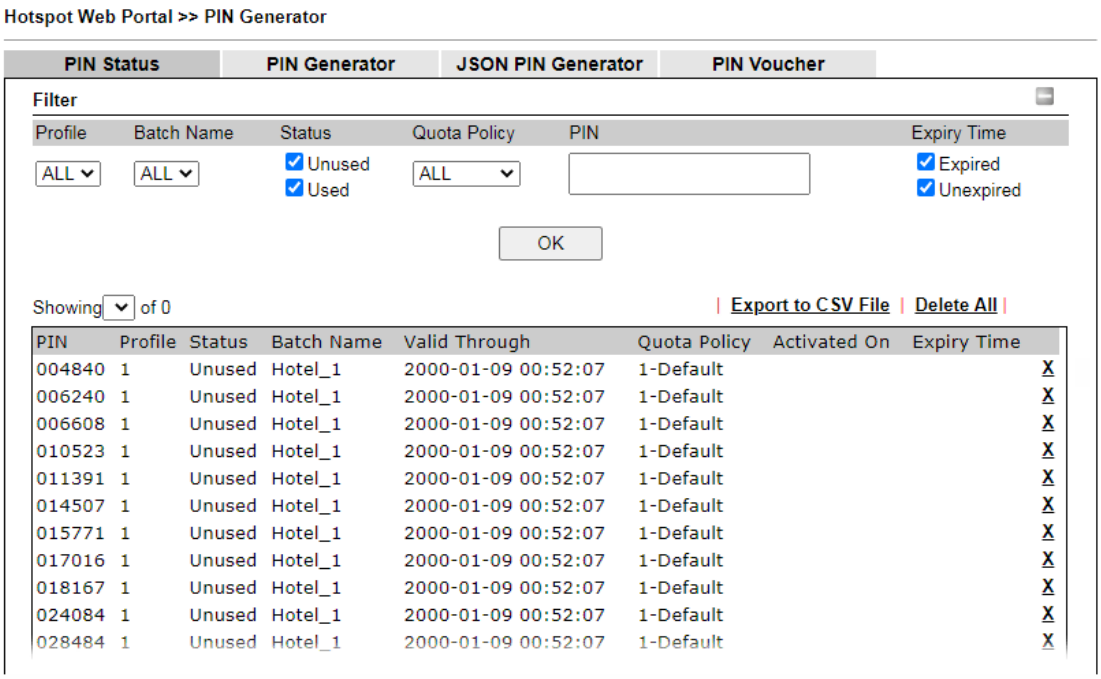
Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

Generador de PIN VII-4-4

El administrador del sistema puede generar múltiples códigos PIN para varios usos. Antes de generar códigos PIN, asegúrese de que**USB**ha sido insertado en su dispositivo Vigor.

VII-4-4-1 Estado del PIN

Esta página muestra los códigos PIN generados por PIN Generator.

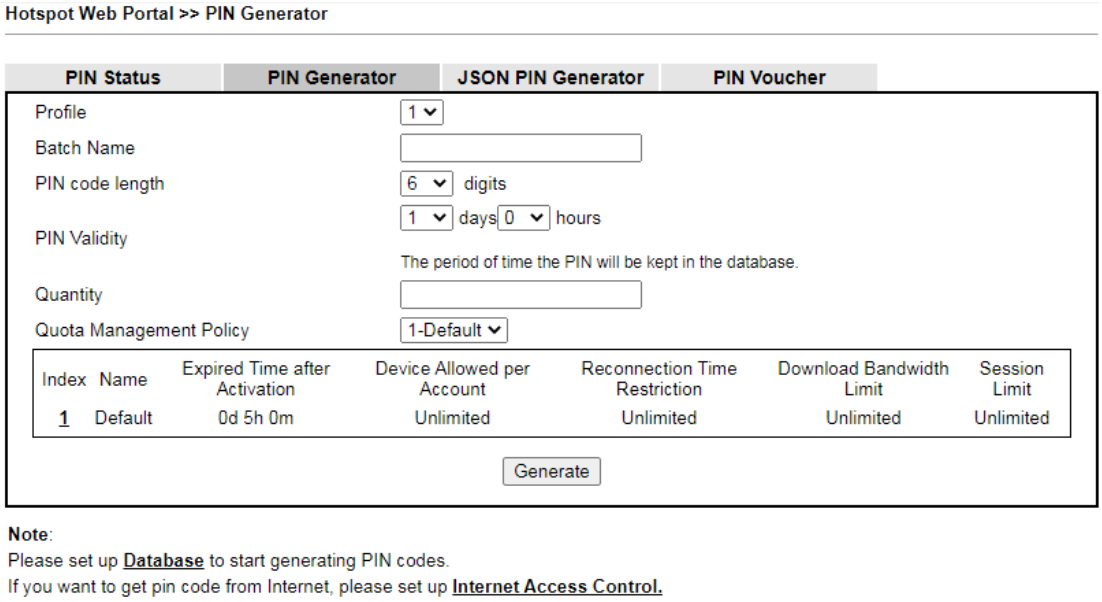


Los ajustes disponibles se explican a continuación:

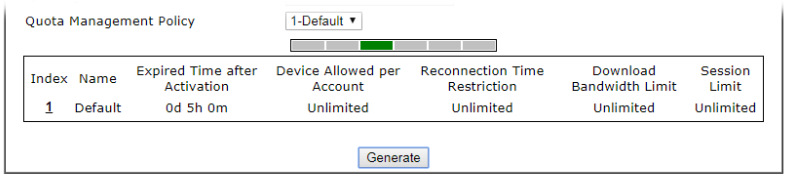
Artículo	Descripción
Perfil	Utilice el menú desplegable para elegir un número de índice (1 a 4) para el perfil del generador de PIN.
Nombre del lote	Use el menú desplegable para elegir un perfil de PIN existente o elija TODO para mostrar el estado del PIN.
Estado	**No usado**-Después de marcar la casilla, solo los códigos PIN no utilizados se mostrarán en esta página. **Usado**-Después de marcar la casilla, solo los códigos PIN utilizados se mostrarán en esta página.
Política de cuotas	Utilice el menú desplegable para elegir una política de gestión de cuotas para mostrar los códigos PIN relacionados.
ALFILER	Ingrese el código PIN para mostrar información relacionada en esta página.
Tiempo de expiración	**Venció**-Después de marcar la casilla, solo los códigos PIN caducados se mostrarán en esta página. **vigente**-Después de marcar la casilla, solo se mostrarán en esta página los códigos PIN que no hayan vencido.
DE ACUERDO	Haga clic en él para mostrar el código PIN de acuerdo con la condición de filtrado anterior.
Exportar a archivo CSV	Haga clic en él para exportar la configuración del código PIN como un archivo CSV.

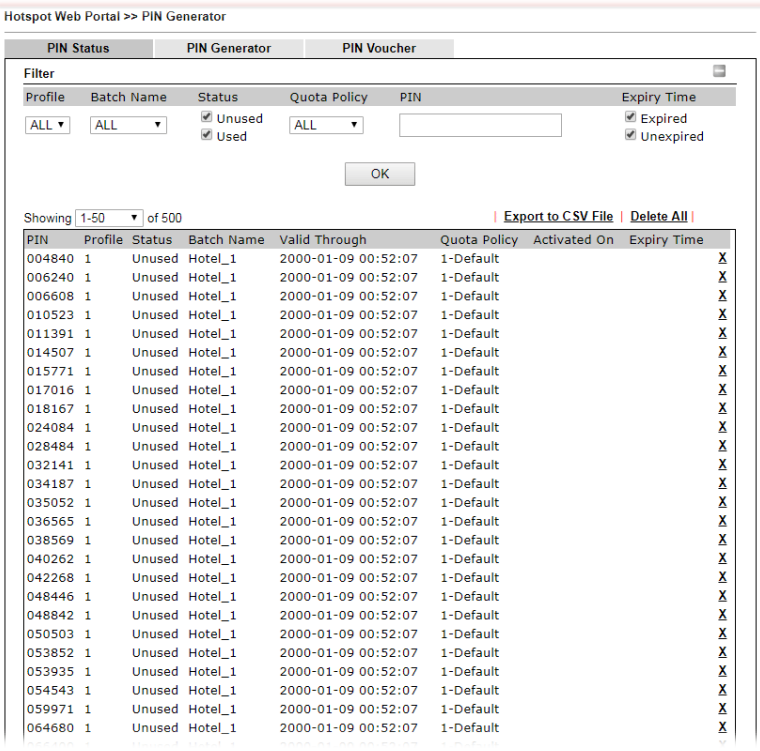
Generador de PIN VII-4-4-2

El administrador del sistema puede generar múltiples códigos PIN en respuesta a la demanda del usuario (por ejemplo, empresa).



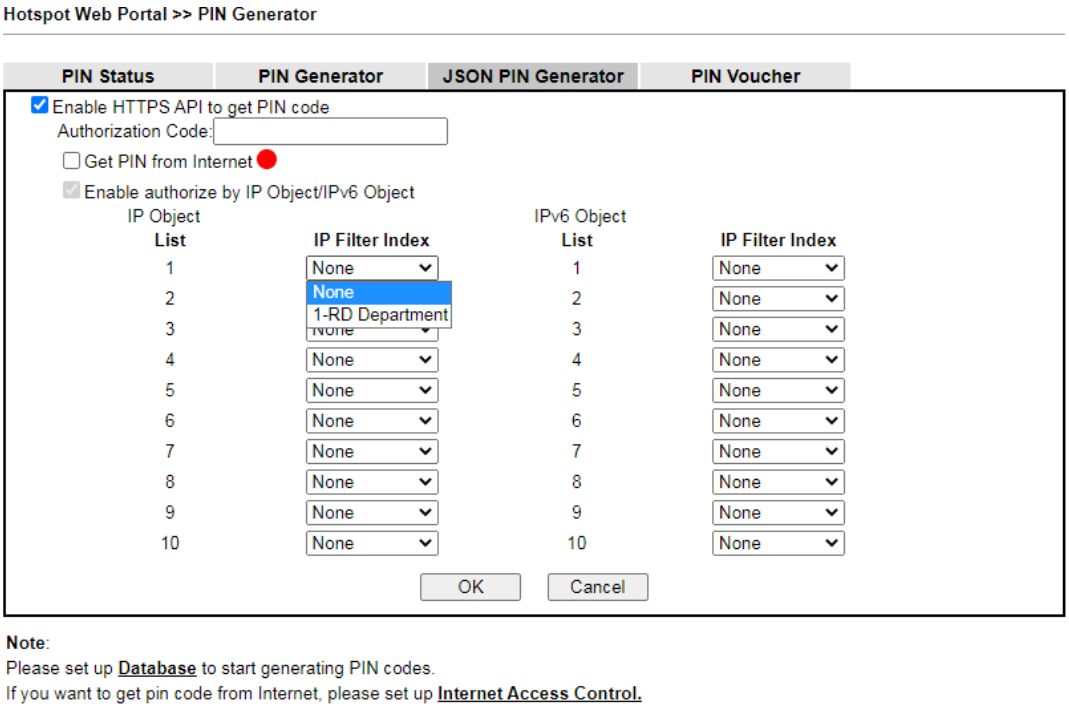
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Perfil	Utilice el menú desplegable para especificar un número de índice (del 1 al 4).
Nombre del lote	Introduzca una cadena como nombre de lote.
Longitud del código PIN	Especifique la longitud del código PIN.
Validez del PIN	Establezca el período de tiempo.
Cantidad	Establezca la cantidad del código PIN.
Gestión de cuotas **Política**	Utilice la lista desplegable para elegir el perfil de la política.
Generar	Haga clic en él para generar un código PIN como cupón. El sistema le pedirá que configure**Base de datos** antes de ejecutar la generación.  Más tarde, el código PIN disponible se mostrará en Estado del PIN.



VII-4-4-3 Generador de PIN JSON

El administrador del sistema puede generar códigos PIN JSON en respuesta a la demanda del usuario (por ejemplo, empresa).



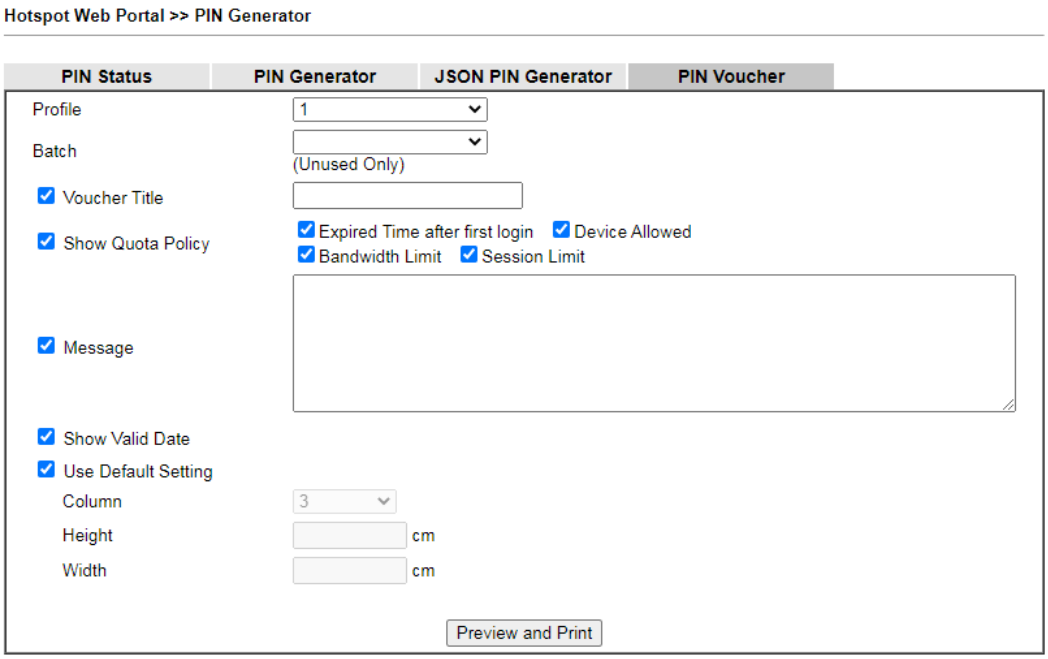
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilite la API HTTPS para obtener el código PIN	Marque la casilla para habilitar la API HTTPS.

Código de Autorización	Introduzca una cadena como autenticación de identidad.
Obtener PIN de Internet	Marque la casilla para obtener el código PIN de Internet. Antes de seleccionar, asegúrese de que la opción Servidor HTTPS esté habilitada en **Mantenimiento del Sistema>>Gestión**.
Habilitar autorización por Objeto IP/IPv6 Objeto	Marque la casilla para habilitar la autenticación basada en el objeto IP/IPv6. **Índice de filtro IP**-Utilice la lista desplegable para seleccionar el filtro IP (objeto IP/objeto IPv6).

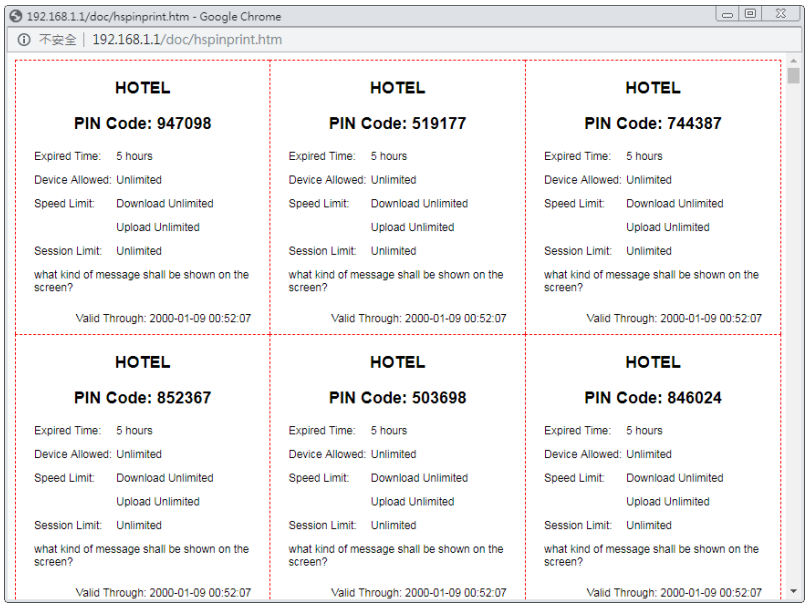
Cupón VII-4-4-4 PIN

Esta página permite imprimir la lista de códigos PIN.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Perfil	Utilice el menú desplegable para especificar un número de índice (del 1 al 4).
Lote	Utilice el menú desplegable para especificar un perfil de lote no utilizado.
Título del cupón	Ingrese una cadena como título que se mostrará en un papel impreso.
Mostrar política de cuotas	Elija los elementos que se mostrarán en la lista de códigos PIN impresa.
Mensaje	Introduzca una breve descripción que el cliente debe conocer.
Mostrar fecha válida	Marque la casilla para mostrar la fecha y hora válidas en la lista impresa.
Usar configuración predeterminada	Si está habilitado, el sistema utilizará la configuración predeterminada de tamaño de papel para imprimir la etiqueta. Si está deshabilitado, configure el tamaño del papel para imprimir los comprobantes en la impresora de etiquetas. **Columna**-Utilice la lista desplegable para especificar el valor de la columna. **Altura**-Introduzca el valor de la altura. **Ancho**-Introduzca el valor del ancho.

Vista previa e impresión	Haga clic en él para mostrar la lista de códigos PIN. Esta lista se puede imprimir si es necesario. 

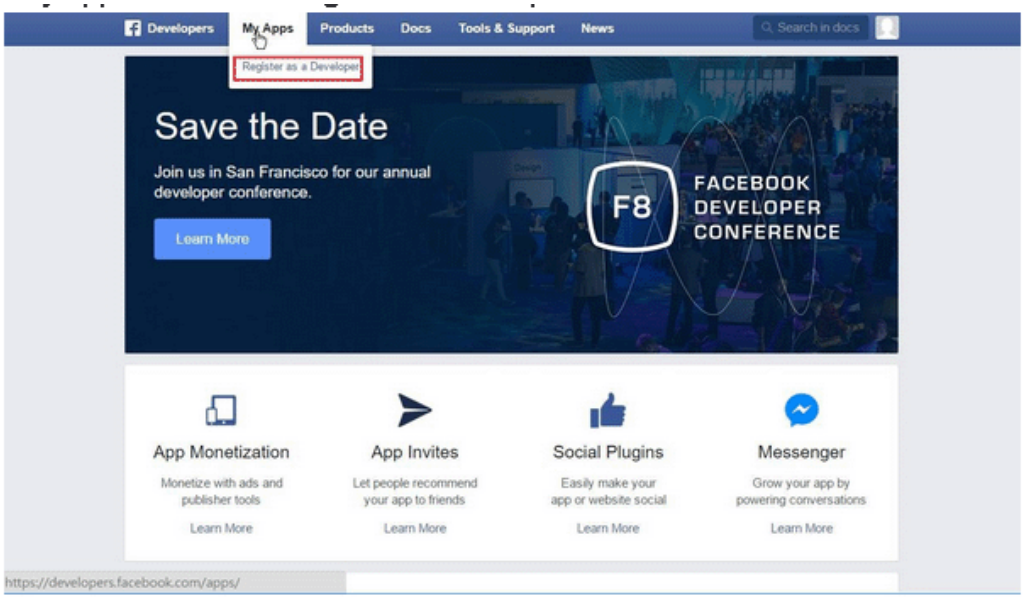
A-1 ¿Cómo crear una aplicación de Facebook para la autenticación del portal web?

La nueva característica del portal web admite el inicio de sesión social como método de autenticación y permite que el administrador de la red autentique a los clientes de LAN mediante su cuenta de Google o Facebook. Este documento presenta cómo crear la aplicación de Facebook y generar el ID de la aplicación y el secreto de la aplicación que se pueden usar en la configuración del portal web.

1. Regístrese como desarrollador de FB: vaya ahttps://developers.facebook.com/ e inicie sesión en la cuenta de FB.

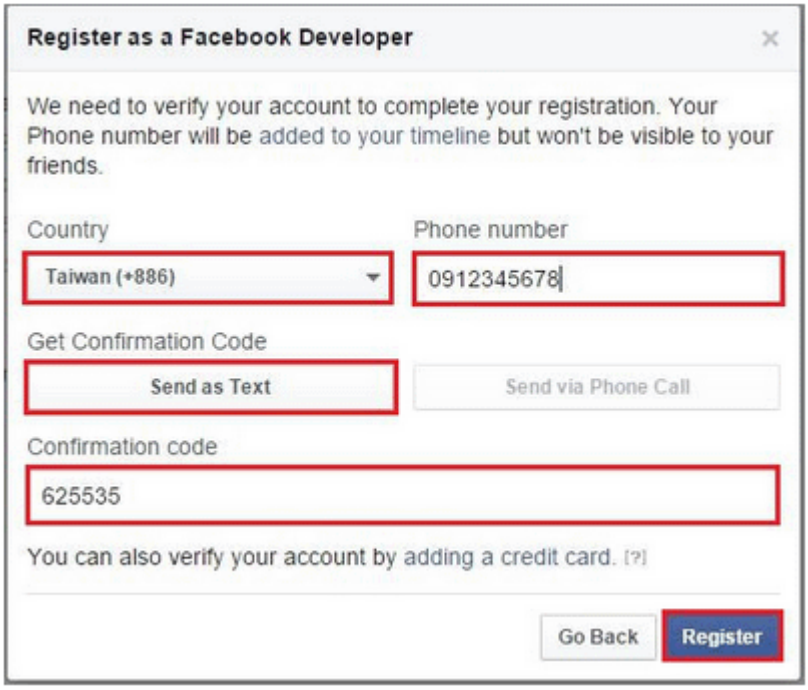
2. Registre la cuenta de Facebook como desarrollador (si la cuenta se verificó anteriormente, este paso se puede omitir).

3. Haga clic en**Mis aplicaciones**entonces escoge**Regístrate como Desarrollador.**

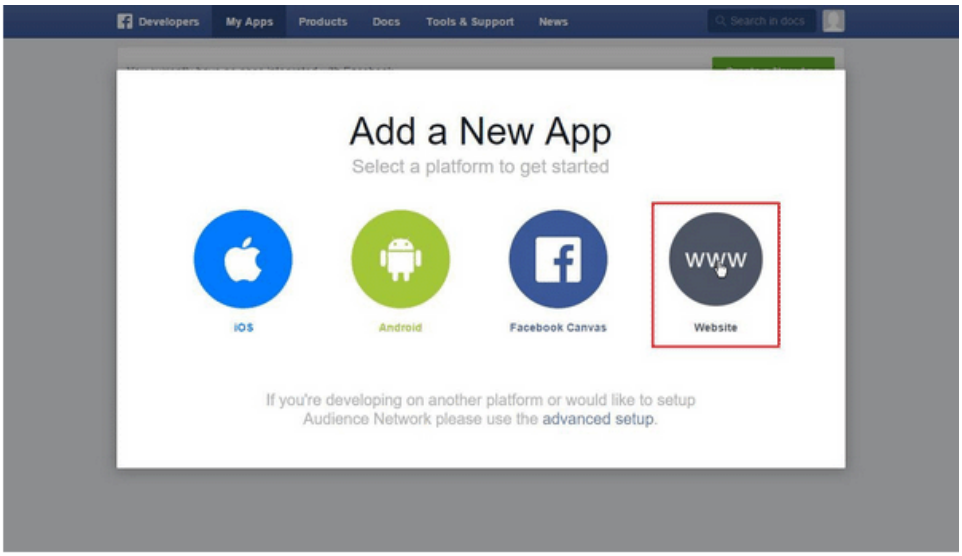


4. Cambiar a**SÍ**luego haga clic**Próximo**en la ventana emergente.

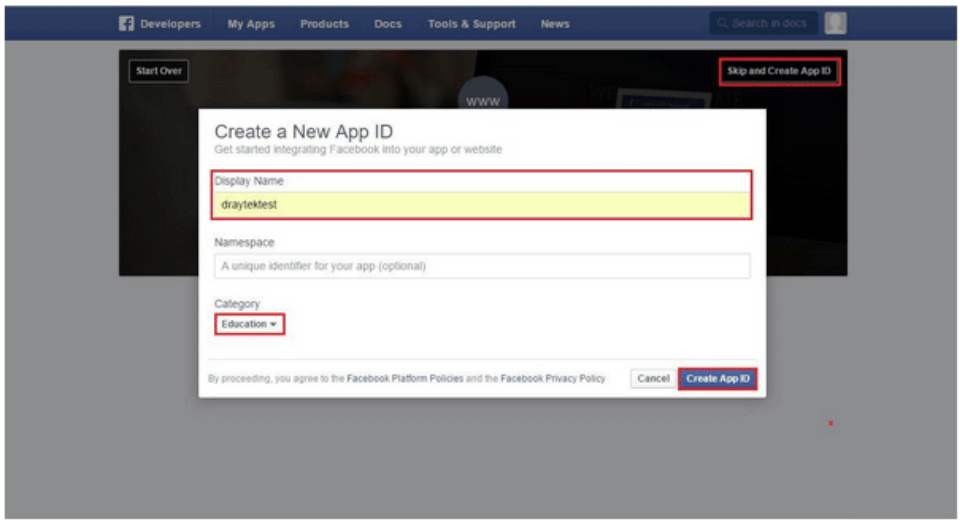
5. Elige**país**luego escribe**número de teléfono**, haga clic**Enviar como texto**en Obtener código de confirmación. Espere el mensaje del código de confirmación recibido y luego ingrese el**código de confirmación.**Hacer clic **Registro** para finalizar el proceso de registro.



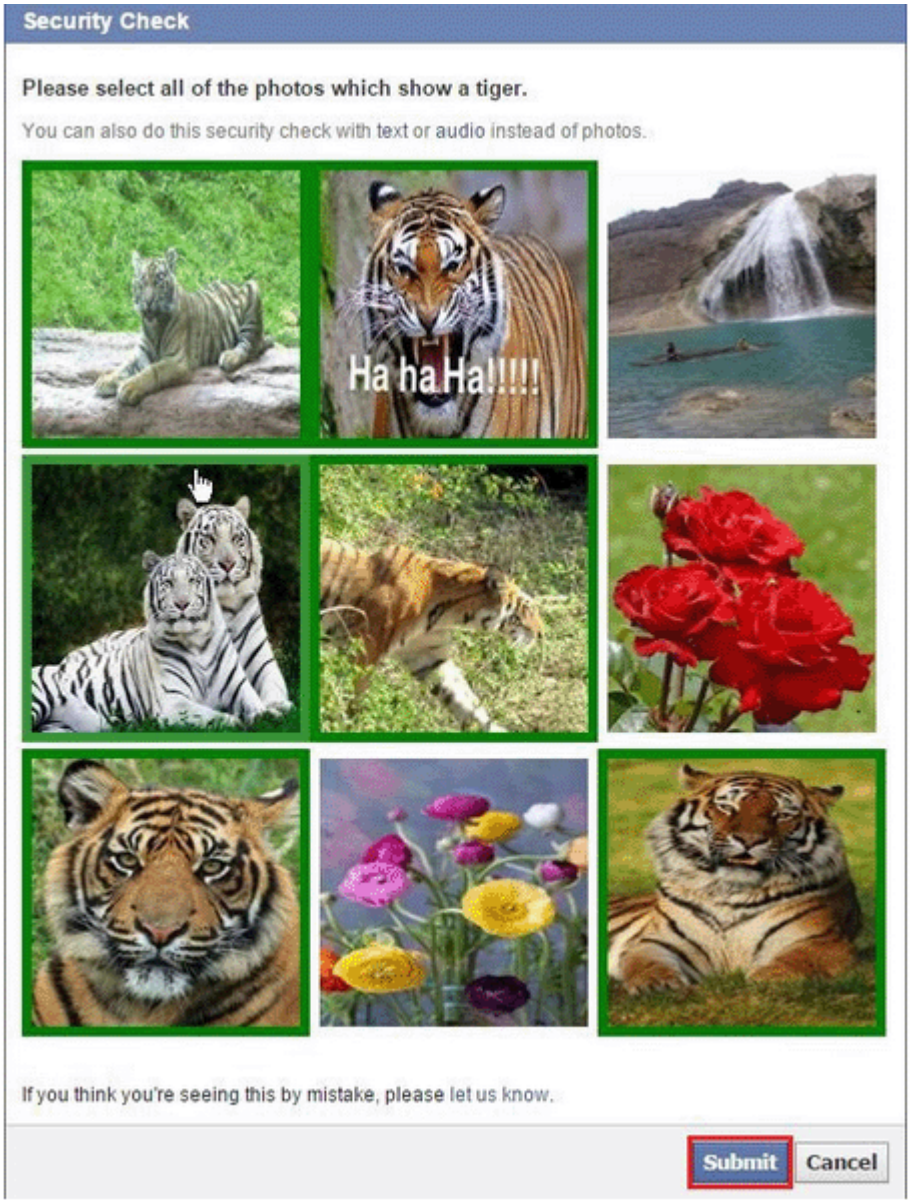
6. Agregue una nueva aplicación. Haga clic en**Mis aplicaciones > Agregar una nueva aplicación.**Elegir**Sitio web**plataforma.



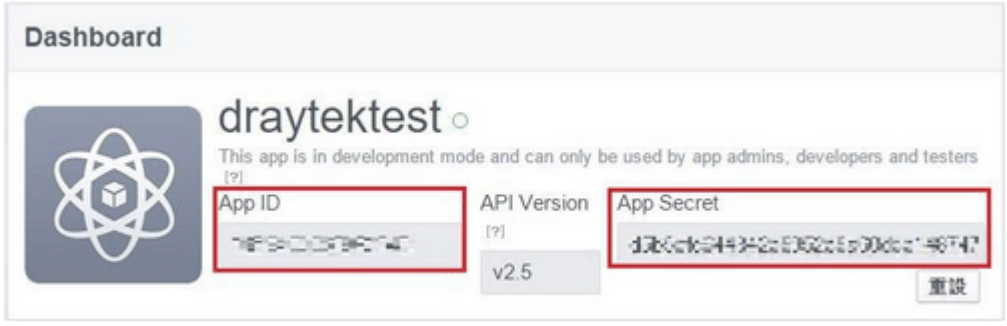
7. Haga clic en**Saltar y crear ID de aplicación**en el primer uso. Tipo**Nombre para mostrar.**Elegir**Categoría.**Hacer clic **Crear ID de aplicación.**



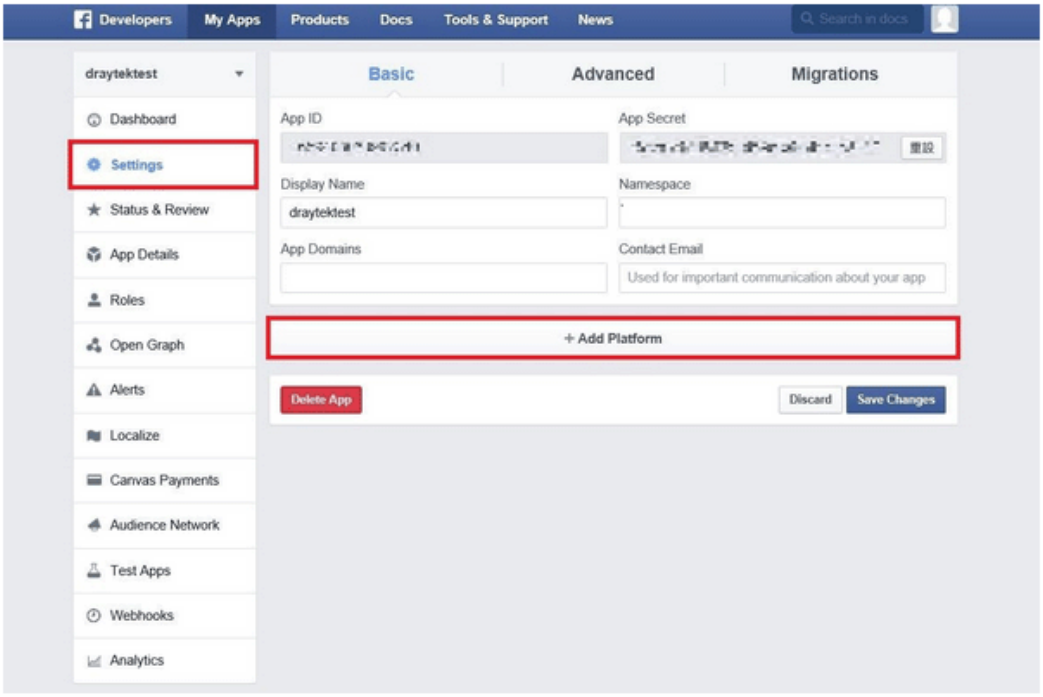
8. Aparece una ventana de verificación de seguridad, seleccione la respuesta y luego haga clic en**Entregar**para terminar el proceso.



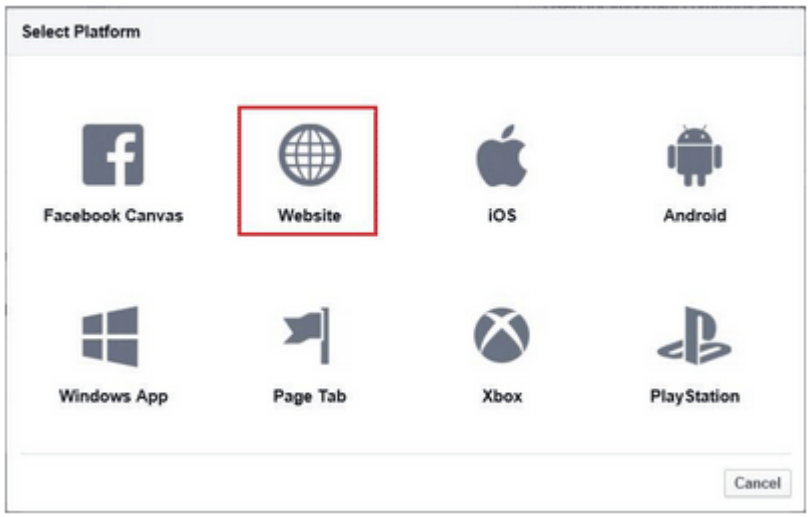
9. En el Tablero, el usuario puede obtener**identificación de la aplicación**y**App secreta**, esta información se utilizará en la configuración del portal web de Vigor Router.



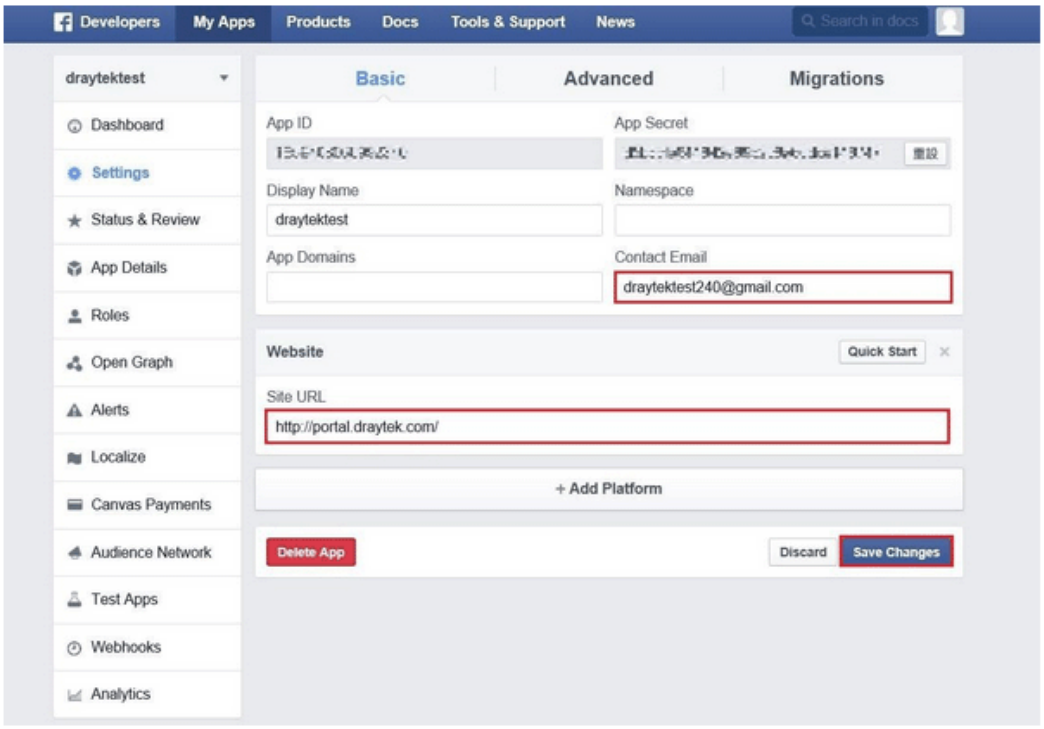
10. Agregar plataforma en Mis aplicaciones. Ir a**Ajustes**luego haga clic**Agregar plataforma.**



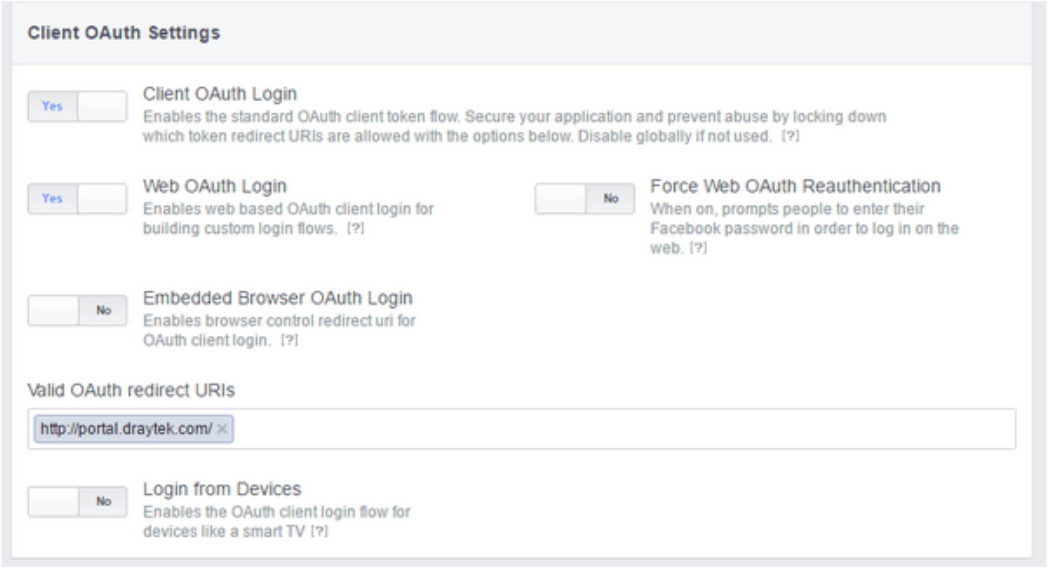
11. Elige**Sitio web**en la ventana Seleccionar plataforma.



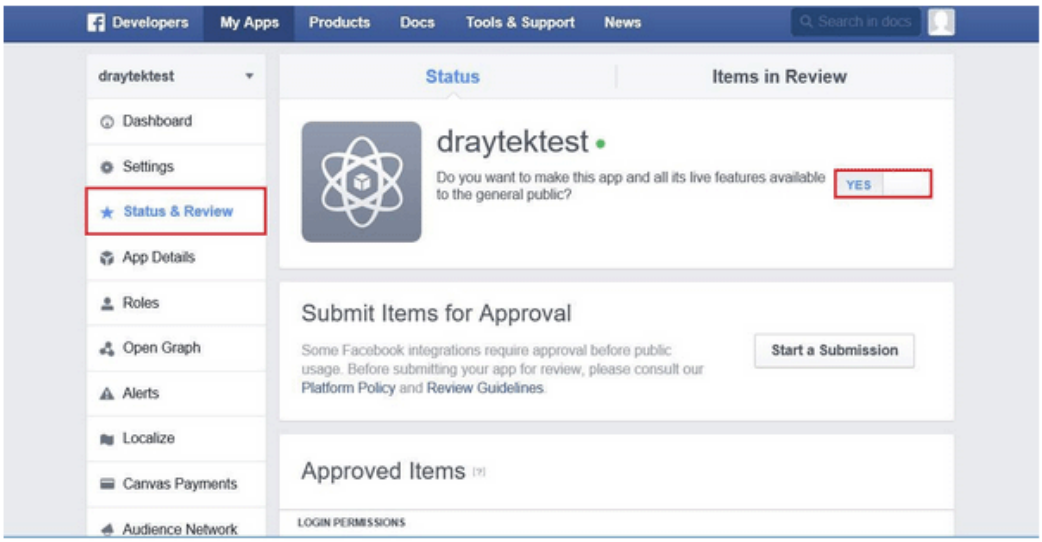
12. Introduzca el**Sitio URL**comohttp://portal.draytek.com. (*Nota*: Si cambia el puerto http en vigor, agregue el puerto http en las URL. Por ejemplo, usamos 8080 como puerto http y pondremoshttp://portal.draytek.com:8080). Introducir el**Email de contacto.**Y**C**lamer**Guardar cambios.**



13. Configure Cliente OAuth. Ir a**Ajustes**>>**Avanzado**>>**Configuración de OAuth del cliente**, ingrese "http://portal.draytek.com" en**URI de redireccionamiento de OAuth válidos**y guarde los cambios.

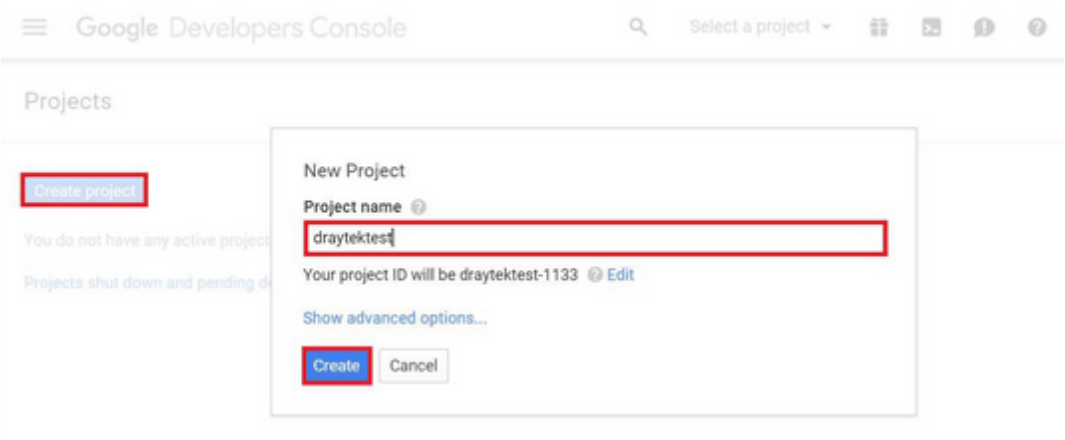


14. Ir a**Mis aplicaciones>>Estado y revisión**y cambie el estado disponible a**SÍ**para activar la APLICACIÓN.

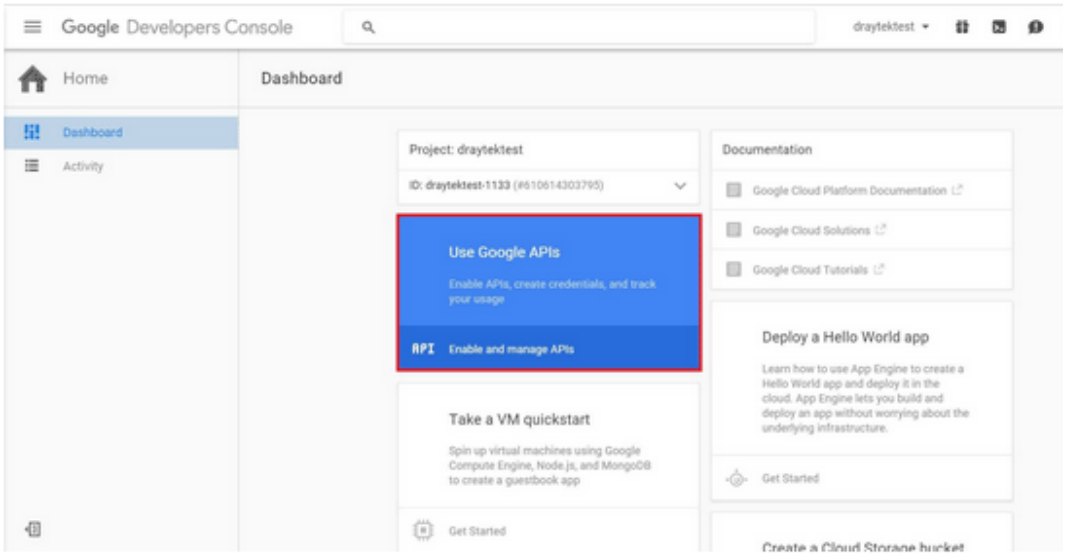

Developers
My Apps
Products
Docs
Tools & Support
News
Search in docs
draytektest
Dashboard
Settings
Status & Review
App Details
Roles
Open Graph
Alerts
Localize
Canvas Payments
Audience Network
Status
Items in Review
draytektest
Do you want to make this app and all its live features available to the general public?
YES
Submit Items for Approval
Some Facebook integrations require approval before public usage. Before submitting your app for review, please consult our Platform Policy and Review Guidelines.
Start a Submission
Approved Items
LOGIN PERMISSIONS

La nueva característica del portal web admite el inicio de sesión social como método de autenticación y permite que el administrador de la red autentique a los clientes de LAN mediante su cuenta de Google o Facebook. Este documento presenta cómo crear la aplicación de Facebook y generar el ID de la aplicación y el secreto de la aplicación que se pueden usar en la configuración del portal web.

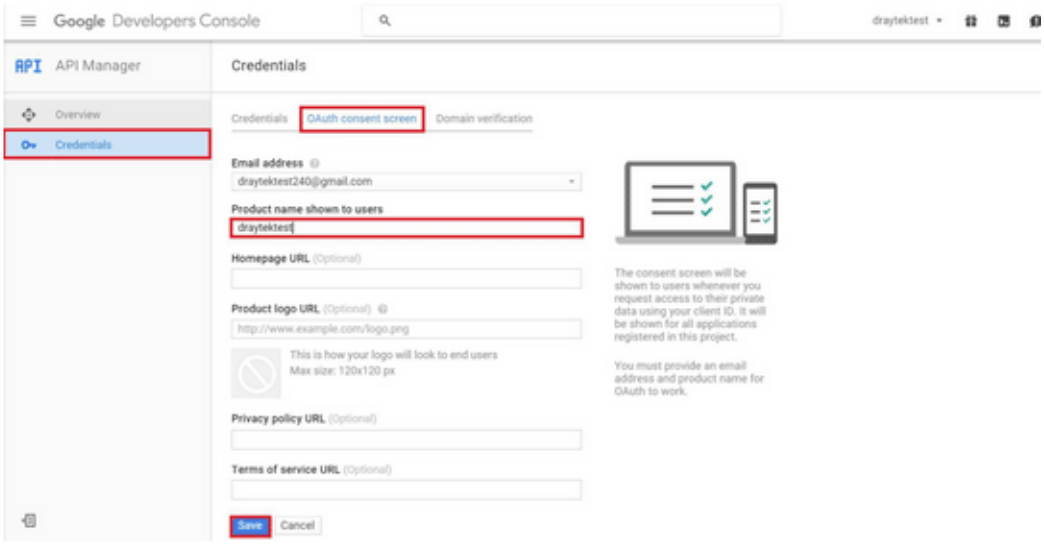
1. Crear proyecto de Desarrollador. Ir a https://code.google.com/apis/console , inicie sesión con una cuenta de Google y luego haga clic en **Crear proyecto.** Tipo **nombre del proyecto** luego haga clic **Crear.**



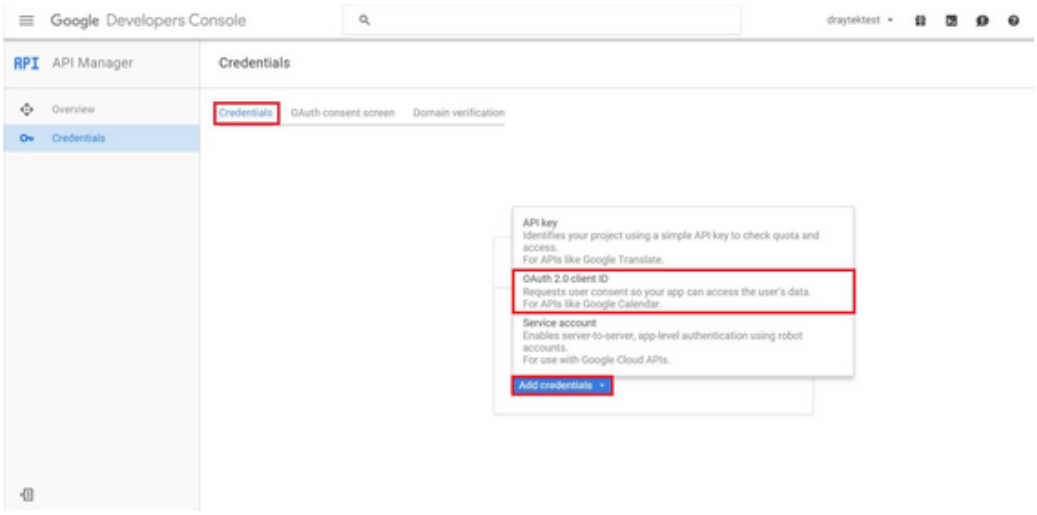
2. En Panel, elija **Usa las API de Google**.



3. Pantalla Editar consentimiento de autenticación. Ir a **Credenciales > Pantalla de consentimiento de autenticación.** Entra tu **correo electrónico** , **nombre del producto** y otro elemento opcional, luego haga clic en **Ahorrar.**



4. Crear ID de cliente. Hacer clic**Cartas credenciales**y haga clic**Agregar credenciales > ID de cliente de OAuth2.0.**

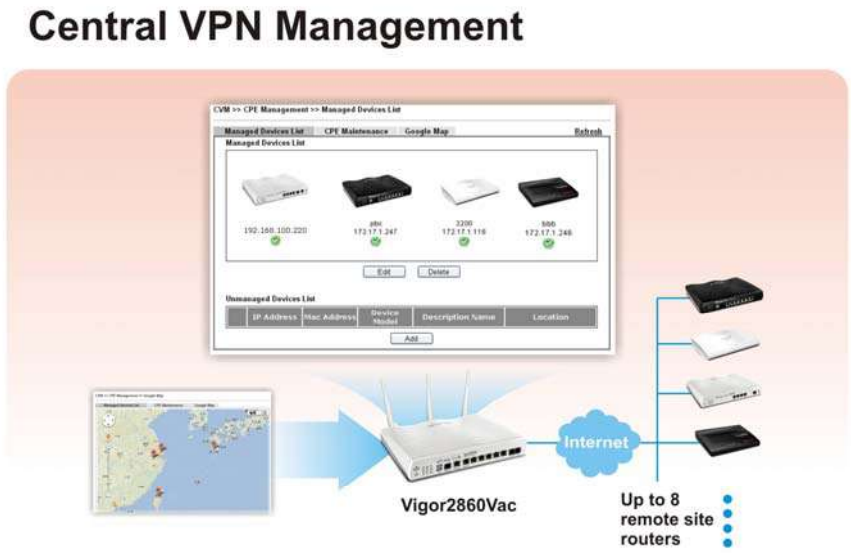


5. Elige**Aplicación web**como Tipo de aplicación, luego ingrese**nombre**. Colocar**Orígenes de JavaScript autorizados**y**URL de redirección autorizadas**como http://portal.draytek.com y haga clic en**Crear.**(*Nota*: Si cambia el puerto http en vigor, agregue el puerto http en las URL. Por ejemplo, usamos 8080 como puerto http y pondremoshttp://portal.draytek.com:8080).

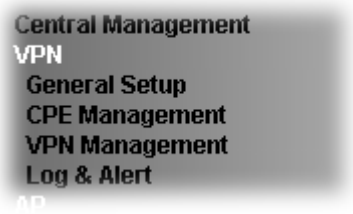
6. Obtener**Identificación del cliente**y**secreto del cliente**. Dicha información se utilizará en la página de configuración del portal web de Vigor Router.

Gestión Central VII-5 (VPN)

Vigor2927 puede construir una red privada virtual (VPN) entre sí mismo y cualquier otro CPE TR-069 mediante la función de administración central de VPN. Además, se puede tratar como un servidor (llamado servidor CVM) que puede administrar TR-069 CPE para la actualización periódica del firmware, la copia de seguridad de la configuración y la restauración de la configuración.



El menú de administración central de VPN puede administrar el CPE conectado solo a través de WAN.

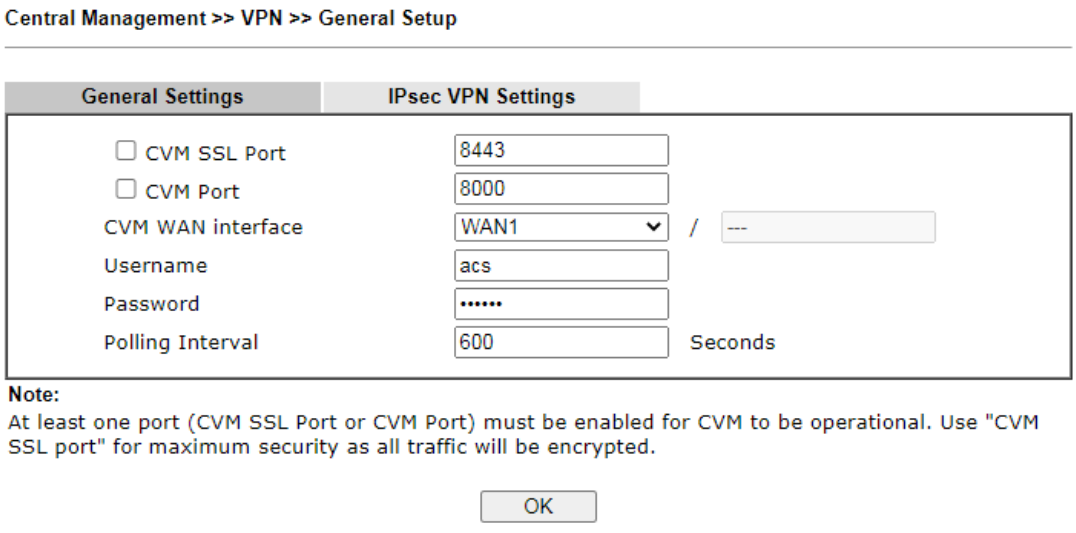


VII-5-1 Configuración general

Esta página se utiliza para configurar los ajustes que utilizarán los clientes para registrarse en dicho enrutador Vigor. Hacer clic**Configuración general**y**Configuración de IPsec VPN**para configurar los ajustes básicos del mecanismo CVM.

VII-5-1-1 Configuración general

Para habilitar la función CVM, lo primero que debe hacer es habilitar el puerto CVM o el puerto SSL CVM.



Los ajustes disponibles se explican a continuación:

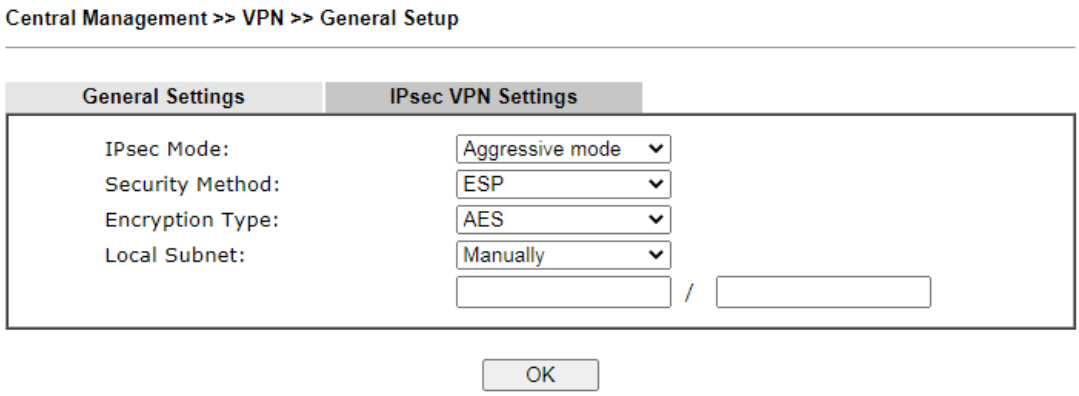
Artículo	Descripción
Puerto CVM SSL	Marque la casilla para habilitar la configuración del puerto. Introduzca el número de puerto en el cuadro.
Puerto CVM	Marque la casilla para habilitar la configuración del puerto. Introduzca el número de puerto en el cuadro.
Interfaz WAN CVM	Para el enrutador Vigor, solo se puede administrar el cliente desde la interfaz WAN, por lo tanto, debe especificar qué interfaz se utilizará para dicha función. Si elige MANUALMENTE, debe especificar la dirección IP de WAN.
Nombre de usuario	Escriba un nombre de usuario que será utilizado por cualquier CPE que intente

	conectarse al enrutador Vigor.
Contraseña	Introduzca la contraseña para el usuario.
Intervalo de votación	Ingrese el valor del tiempo (la unidad es el segundo). El rango es de 60 ~ 86400.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

Configuración de VPN de IPsec VII-5-1-2

La administración de VPN central se realiza a través de una conexión VPN IPsec.



Los ajustes disponibles se explican a continuación:

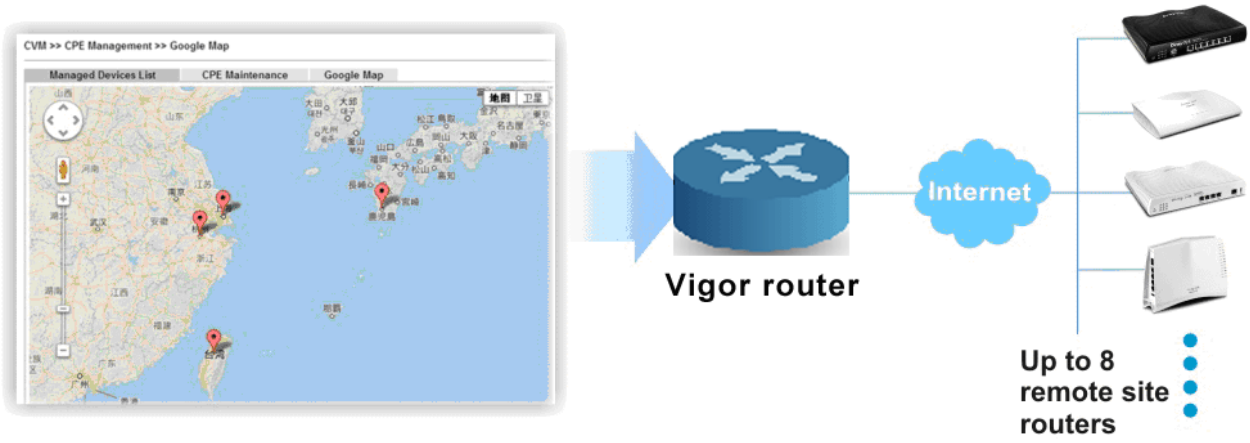
Artículo	Descripción
Modo IPsec	Elegir**Agresivo**o**Principal**como el Modo IPsec.
Método de seguridad	Elija uno de los siguientes métodos (AH o ESP) para la seguridad de la transmisión de datos. Por ejemplo, elija**Ah**para especificar el protocolo IPsec para el protocolo de encabezado de autenticación. Los datos serán autenticados pero no encriptados.
Tipo de cifrado	Elija una de las selecciones como tipo de cifrado.
Subred local	Ingrese la dirección IP y la máscara de subred del host local.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

VII-5-2 Gestión de CPE

Todos los CPE gestionados por la serie Vigor2927 se pueden ver con iconos desde esta página.

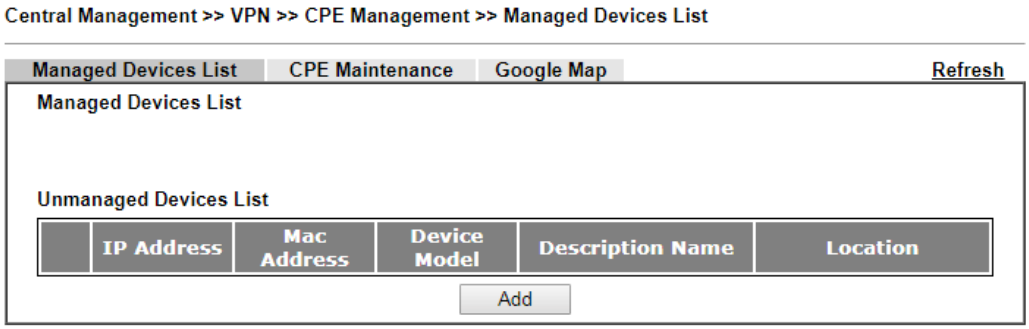
Antes de usar dicha función, asegúrese de que el puerto CVM se haya habilitado y configurado correctamente.



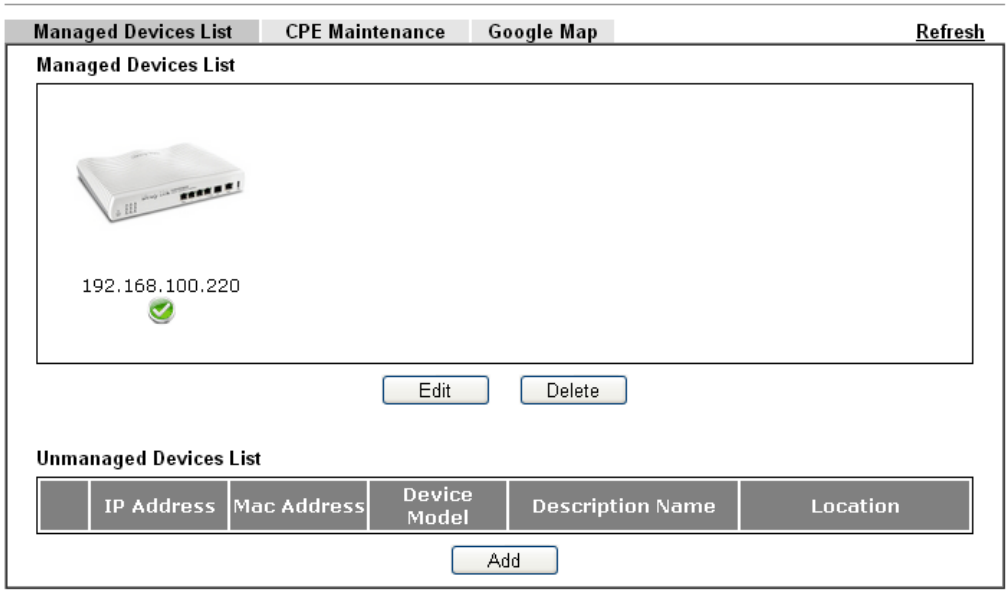
VII-5-2-1 Lista de dispositivos administrados

Esta página le permite administrar los CPE conectados a la serie Vigor2927.

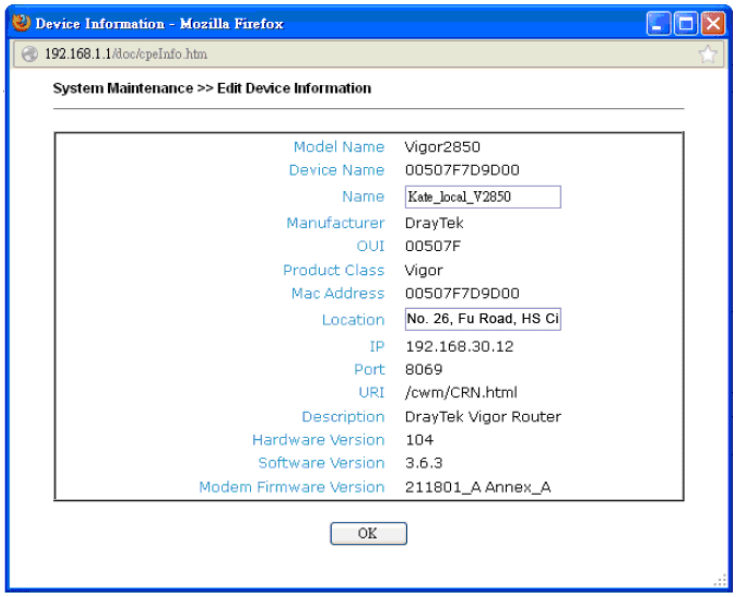
Página sin CPE conectado

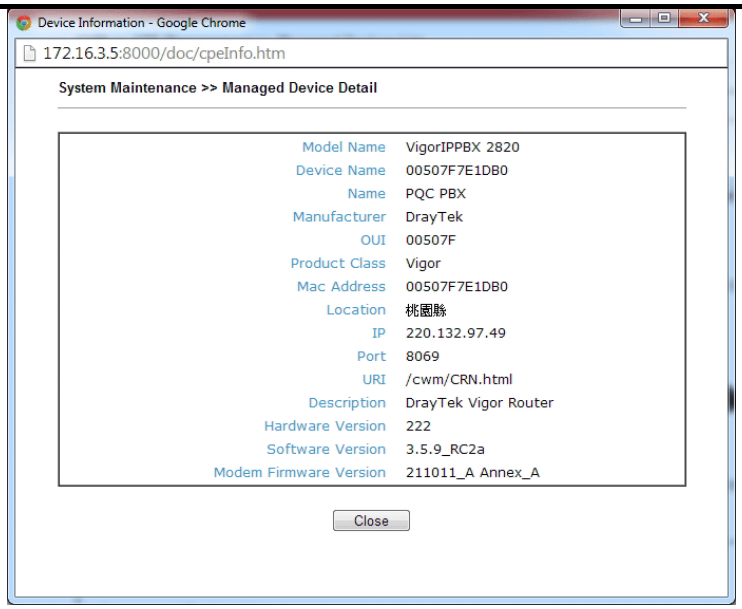


Página con CPE conectado



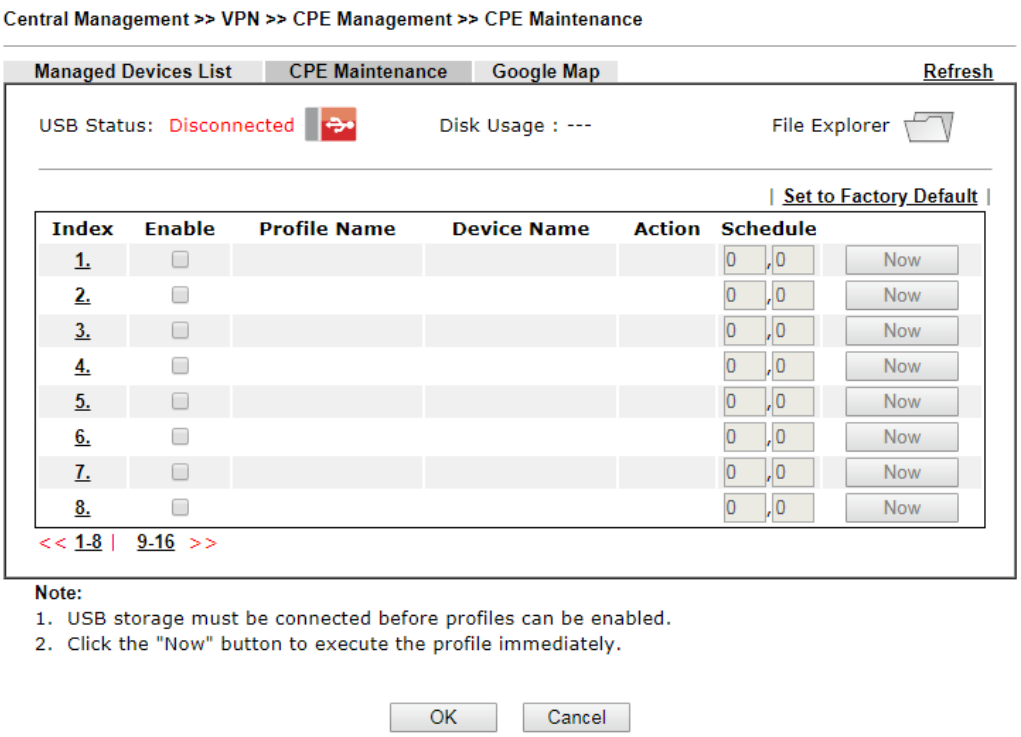
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Lista de dispositivos administrados	Esta área muestra iconos de dispositivos (hasta 8) para el CPE administrado por la serie Vigor2927. **Editar**–Para modificar el nombre y la ubicación de un CPE específico, haga clic en el que desee y haga clic en el**Editar**botón. Aparecerá una ventana emergente. Simplemente cambie el nombre y/o la ubicación manualmente.  **Borrar**–Para desconectar la gestión de cualquier CPE, haga clic en el icono de CPE que desee y haga clic en el botón Eliminar. Al hacer doble clic en el ícono de CPE, también puede aparecer la ventana Detalles del dispositivo administrado. Sin embargo, no puede modificar ningún dato en la ventana.

	
Lista de dispositivos no administrados	Cualquier dispositivo (CPE) que siga el estándar de TR-069 se puede configurar y detectar automáticamente mediante la serie Vigor2927. Solo ocho dispositivos remotos pueden ser administrados por Vigor2927 a la vez. Por lo tanto, es posible que otros dispositivos remotos detectados por la serie Vigor2927 no se muestren en dicho campo. **Agregar**–Mueva el dispositivo seleccionado de la lista de dispositivos no administrados a la lista de dispositivos administrados. **Dirección IP**–Muestra la dirección IP del dispositivo remoto. **Dirección MAC**–Muestra la dirección MAC del dispositivo remoto. **Modelo de dispositivo**–Muestra el nombre del modelo del dispositivo remoto. **Descripción Nombre**–Defina el nombre o ingrese la descripción adicional de CPE para la identificación en la administración de VPN y la administración de CPE. **Ubicación**–Ingrese la ubicación (dirección) del CPE que Google Map mostrará.
Actualizar	Haga clic en él para actualizar la página web actual.

VII-5-2-2 Mantenimiento de CPE

Esta área muestra todos los perfiles que se crean para aplicar al dispositivo administrado. Esta página puede ayudar al administrador a realizar trabajos de mantenimiento como actualización de firmware, copia de seguridad de la configuración, restauración de la configuración, etc.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Actualizar	Haga clic en él para actualizar la página actual.
Disco USB	USB Disk : - Significa un disco USB que se conecta a Vigor2927. USB Disk : - Significa que no hay disco USB conectado a Vigor2927.
Uso del disco	Disk Usage : 1084MB / 2009MB - Cuando se conecta un disco USB a Vigor2927, el uso del disco y la capacidad del disco se mostrarán en dicho campo. Disk Usage : USB Storage Disconnected - Cuando no hay Disco USB conectado a Vigor2927, dicho mensaje se mostrará en este campo.
	Haga clic en el icono para ver el contenido dentro del disco USB.
Establecer como predeterminado de fábrica	Haga clic para borrar todos los índices.
Índice	Muestra el número del perfil que puedes editar.
Permitir	Marque para habilitar el perfil.
Nombre de perfil	Muestra el nombre del perfil de mantenimiento.

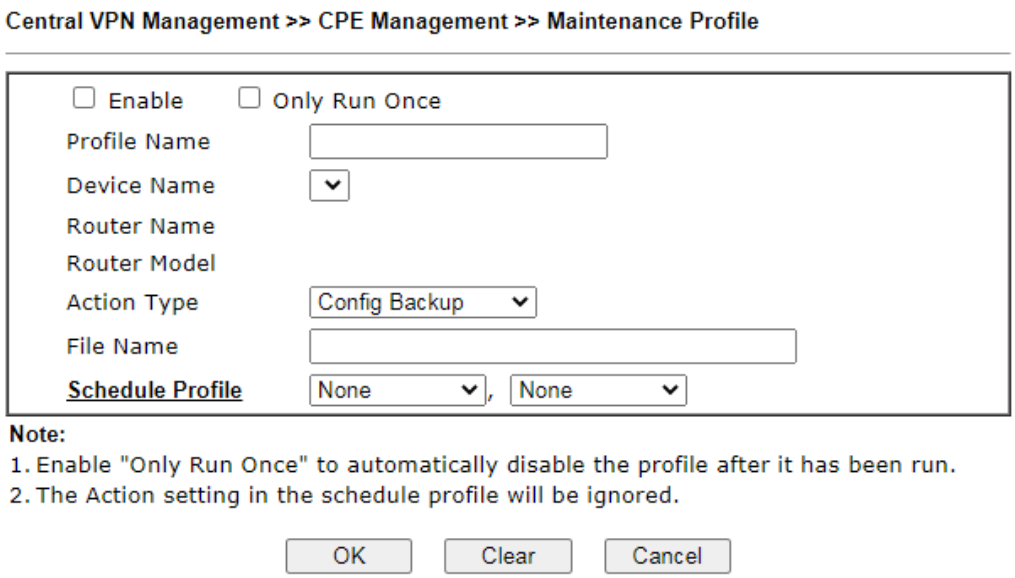
Nombre del dispositivo	Muestre el nombre del CPE administrado al que se aplicará el perfil de mantenimiento.
Acción	Muestra la acción que aceptará el CPE administrado.
Cronograma	Muestra los perfiles de horarios seleccionados para dicho perfil.
Ahora	La acción se realizará para el CPE seleccionado inmediatamente.

Cómo agregar un nuevo perfil de mantenimiento

Siga los pasos a continuación para crear un nuevo perfil de mantenimiento. 1. Haga clic en

cualquier enlace de número de índice, por ejemplo, Índice 1.

2. Aparece el cuadro de diálogo Mantenimiento.



Información	Al restaurar la configuración a un CPE, asegúrese de que el archivo de configuración que seleccionó haya sido una copia de seguridad de este CPE anteriormente. Porque la restauración desde el archivo de configuración de otro dispositivo puede causar un problema grave (p. ej., ambos dispositivos tienen un nombre de usuario/contraseña de ISP diferente. Restaurar la configuración de un CPE al otro hará que la conexión a Internet no esté en línea).

Los parámetros disponibles se enumeran a continuación:

Artículo	**Descripción**
Permitir	Márquelo para habilitar dicho perfil.
Solo ejecutar una vez	Márquelo para activar dicho perfil ejecutándose por una vez.
Nombre de perfil	Introduzca el nombre del perfil de mantenimiento.
Nombre del dispositivo	La lista desplegable mostrará todos los dispositivos CPE detectados por la serie Vigor2927. Elija el que se aplicará con dicho nuevo perfil creado.
Nombre del enrutador/ Modelo de enrutador	Muestra el nombre y el modelo del enrutador Vigor.
tipo de acción	Hay tres acciones que puede elegir para dicho perfil.

	- **Copia de seguridad de configuración**–Significa que dicho perfil se utilizará para la copia de seguridad de la configuración del CPE seleccionado. - **Restaurar configuración**–Significa que dicho perfil se utilizará para restaurar la configuración del CPE seleccionado. **Información** Al restaurar la configuración a un CPE, asegúrese de que el archivo de configuración que seleccionó haya sido una copia de seguridad de este CPE anteriormente. Porque la restauración desde el archivo de configuración de otro dispositivo puede causar un problema grave (p. ej., ambos dispositivos tienen un nombre de usuario/contraseña de ISP diferente. Restaurar la configuración de un CPE al otro hará que la conexión a Internet no esté en línea). - **Actualización de firmware**–Significa que dicho perfil se utilizará para la actualización del firmware.
Ruta de archivo	Cuando**Restaurar configuración**se selecciona como**Tipo de acción,**hacer clic **Seleccionar** para cargar un archivo de configuración desde el disco USB conectado. Posteriormente, dicho archivo se utilizará para guardar, restaurar o actualizar el firmware para CPE.
Nombre del archivo	Especifique un nombre de archivo en este campo para guardar el archivo de configuración cuando**Copia de seguridad de configuración**se selecciona como**Tipo de acción.**
Programar perfil	La serie Vigor2927 realizará la acción especificada en el CPE seleccionado según el programa configurado aquí. Especifique uno o dos perfiles de programación (representados por número) aquí.

3. Introduzca todos los ajustes y haga clic en**DE ACUERDO**.

4. Se ha creado un nuevo perfil de mantenimiento.

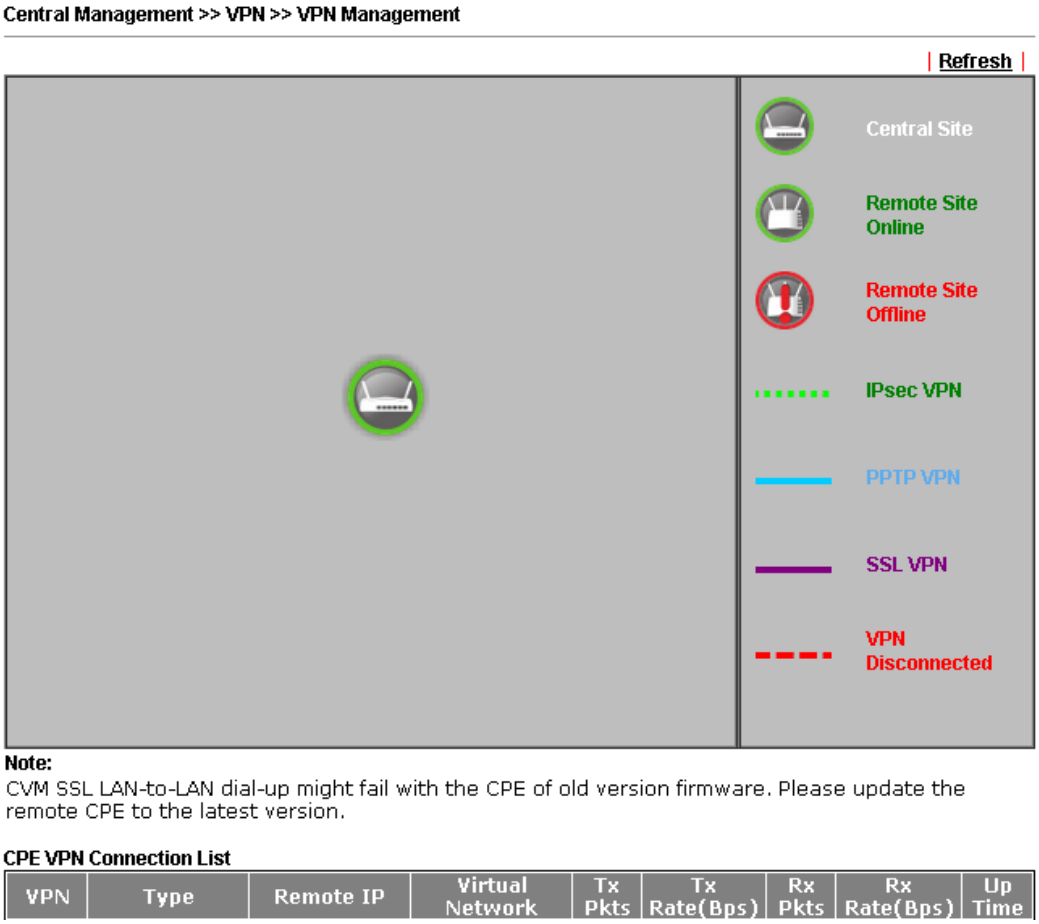
Mapa de Google VII-5-2-3

Para mostrar el**ubicación**del CPE gestionado a vista de pájaro, abierto**Gestión central de VPN>>Gestión de CPE**y haga clic en la pestaña de**Mapa de Google**.

Central Management >> VPN >> CPE Management >> Google Map

VII-5-3 Gestión de VPN

Se ofrece un método fácil y rápido para configurar los ajustes de VPN para crear una conexión VPN automáticamente entre la serie Vigor2927 (tratado como servidor VPN) y otro enrutador Vigor (tratado como dispositivo CPE, es decir, cliente VPN).



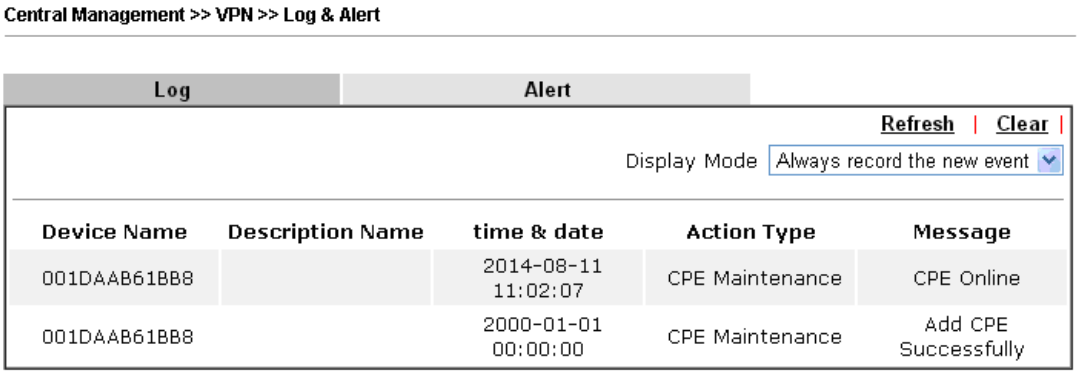
Los parámetros disponibles se enumeran a continuación:

Artículo	Descripción
Lista de conexiones VPN de CPE	
vpn	Muestra el nombre del perfil de LAN a LAN. Se genera automáticamente cuando hace clic en el botón PPTP/IPsec/Avanzado para construir la conexión VPN entre Vigor2927 y el CPE remoto.
Tipo	Muestra el tipo de acceso telefónico y el método de autenticación.
IP remota	Muestra la dirección IP del CPE remoto y la interfaz.
red virtual	Muestra la dirección IP y la máscara de subred de la serie Vigor2927.
paquetes de transmisión	Muestra el número de paquetes transmitidos.
Tasa de transmisión (bps)	Muestra el número de la tasa transmitida.
paquetes recetados	Muestra el número de paquetes recibidos.
Tasa de Rx (bps)	Muestra el número de la tarifa recibida.
tiempo activo	Muestra el tiempo de conexión de dicha VPN.

Una vez que el dispositivo es administrado (controlado) por la serie Vigor2927, se mostrará en dicha pantalla automáticamente. Si no, consulte las secciones**"¿Cómo administrar el CPE (router) a través de Vigor2927?"**para obtener información más detallada.

VII-5-4 Registro y alerta

Esta página ofrece información breve para identificar el CPE conectado a la serie Vigor2927.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Modo de visualización	Elija el modo en que desea mostrar la información relacionada en la siguiente tabla. - **Detener el registro cuando se llena -**cuando la capacidad del registro CVM esté llena, el sistema dejará de grabar. - **Grabe siempre el nuevo evento:**el sistema solo registrará los eventos más recientes.
Nombre del dispositivo	Muestra el nombre del CPE administrado.
Descripción Nombre	Muestre la breve explicación del CPE gestionado.
Hora Fecha	Muestra la hora y la fecha en que el CPE administrado escaneó mediante la serie Vigor2927.
tipo de acción	Muestre la acción que la serie Vigor2927 realizará para el CPE administrado.
Mensaje	Muestra la información de cada evento.

La página Alerta ofrece información breve para identificar el CPE conectado a la serie Vigor2927.

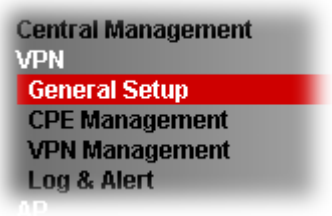
A-1 Aplicación CVM - ¿Cómo administrar el CPE (router) a través de la serie Vigor2927?

Para administrar los CPE a través de la serie Vigor2927, primero debe configurar la URL en el CPE y configurar el nombre de usuario y la contraseña para la serie Vigor2927. Para esta sección, usamos la serie Vigor2850 como ejemplo. Toda la configuración del CPE se realizará a través de la serie Vigor2850.

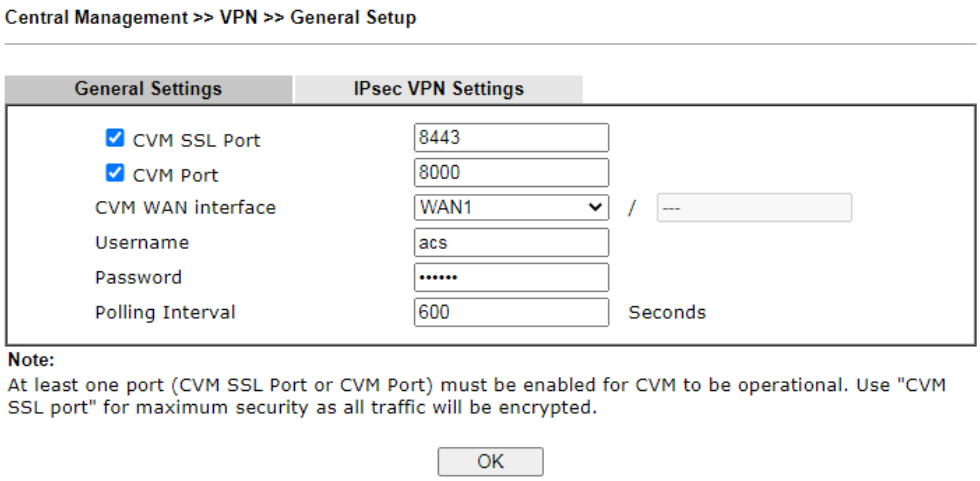
Configure los ajustes de CVM en la serie Vigor2927

1. Acceda a la interfaz de usuario web de la serie Vigor2927.

2. Abierto**Administración central >> VPN >> Configuración general.**



3. En la siguiente página, marque las casillas para Puerto CVM y Puerto SSL CVM para habilitar la configuración del puerto. Introduzca los valores para**Puerto CVM**,**Puerto CVM SSL, nombre de usuario**, y**Contraseña** respectivamente. Recuerde los valores configurados en esta página.

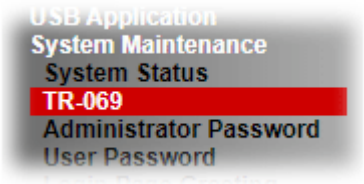


4. Haga clic en**DE ACUERDO**para guardar la configuración.

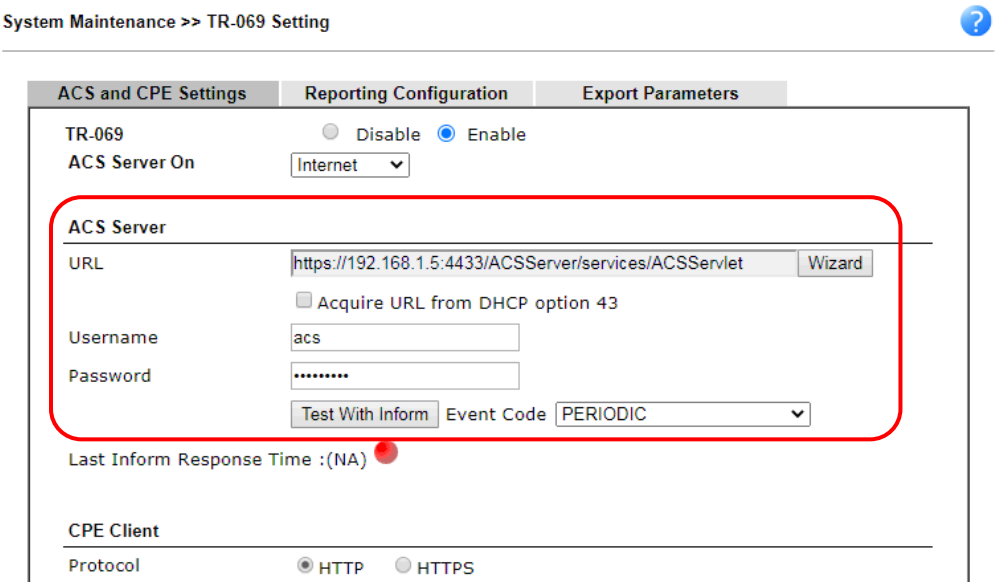
Configurar ajustes en CPE

1. Al final del CPE, acceda a la interfaz de usuario web del CPE (p. ej., la serie Vigor2865). Abra un navegador web (por ejemplo,**ES DECIR**,**Mozilla Firefox**o**netscape**) y escriba **http://192.168.1.1.**

2. Abierto**Mantenimiento del Sistema >> TR-069**.

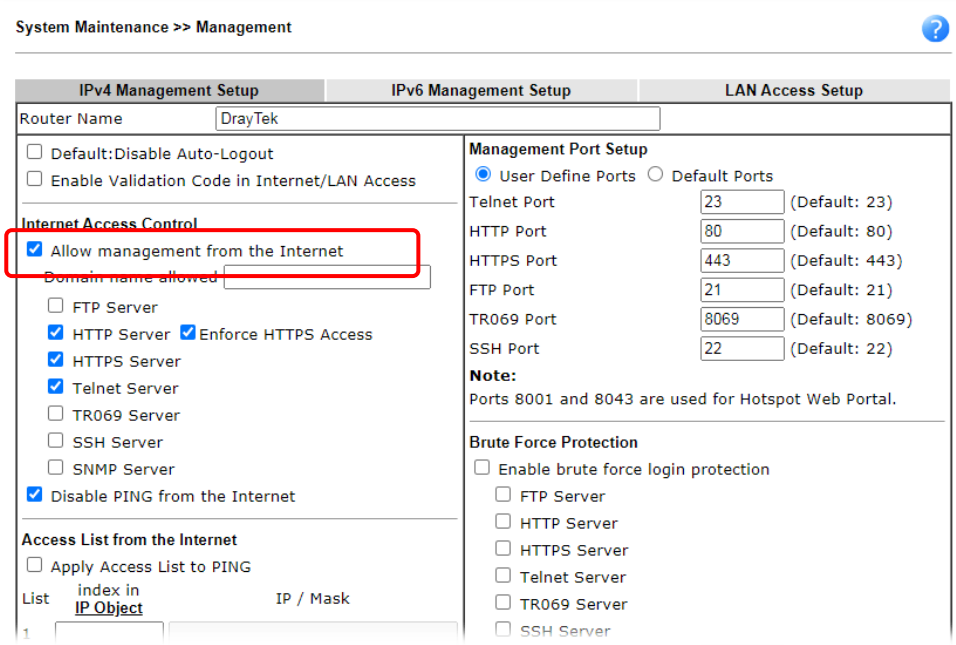


3. En el campo de**Servidor ACS**, Ingrese la URL (dirección IP con número de puerto) de la serie Vigor2927 e ingrese el mismo nombre de usuario y contraseña definidos en la página de**Administración central de VPN>>Configuración general**en la serie Vigor2927. Hacer clic**DE ACUERDO**para guardar la configuración.



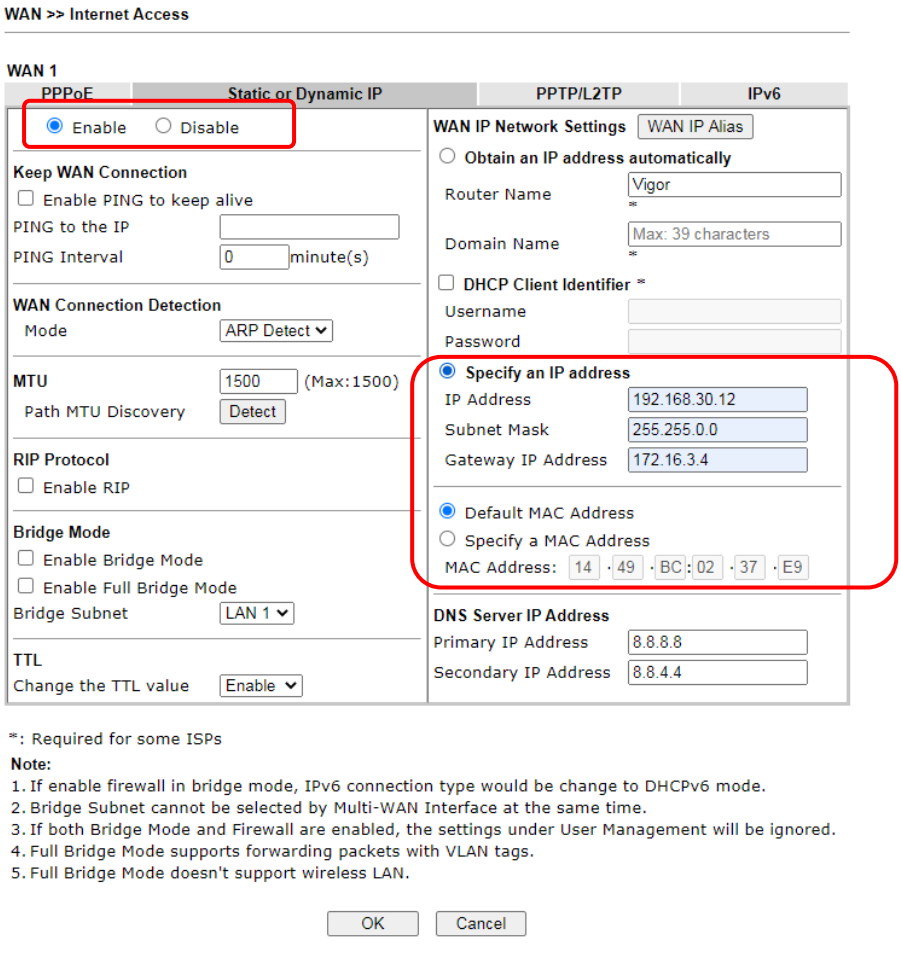
4. Abierto**Mantenimiento del sistema>>Configuración de gestión**.

5. Comprobar**Permitir la gestión desde Internet**para configurar el control de acceso a la administración y haga clic en**DE ACUERDO.**



6. Abierto**WAN>>Acceso a Internet.**Utilice la lista desplegable de**Modo de acceso**en WAN1 para seleccionar **MPoA**(RFC1483/2684). Luego, haga clic en**Página de detalles**.

7. Haga clic en**Especifique una dirección IP**. Escriba la dirección IP de WAN, la máscara de subred y la dirección IP de la puerta de enlace correctas para su CPE. Luego haga clic**DE ACUERDO**.

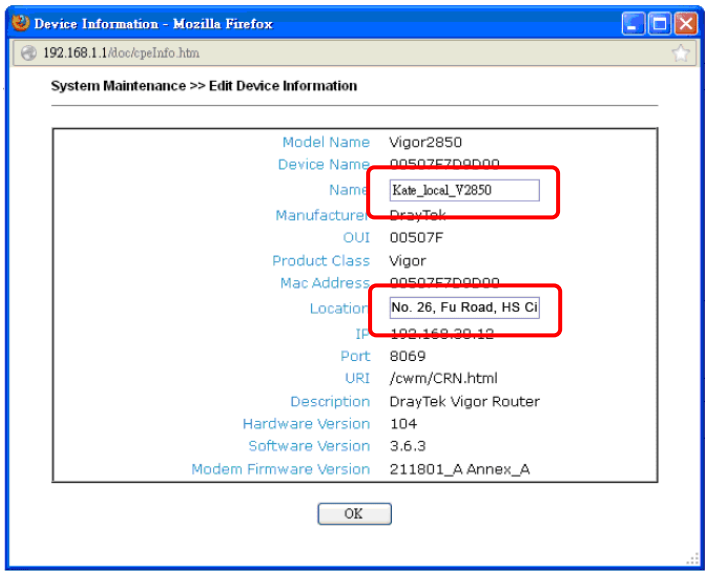


Información

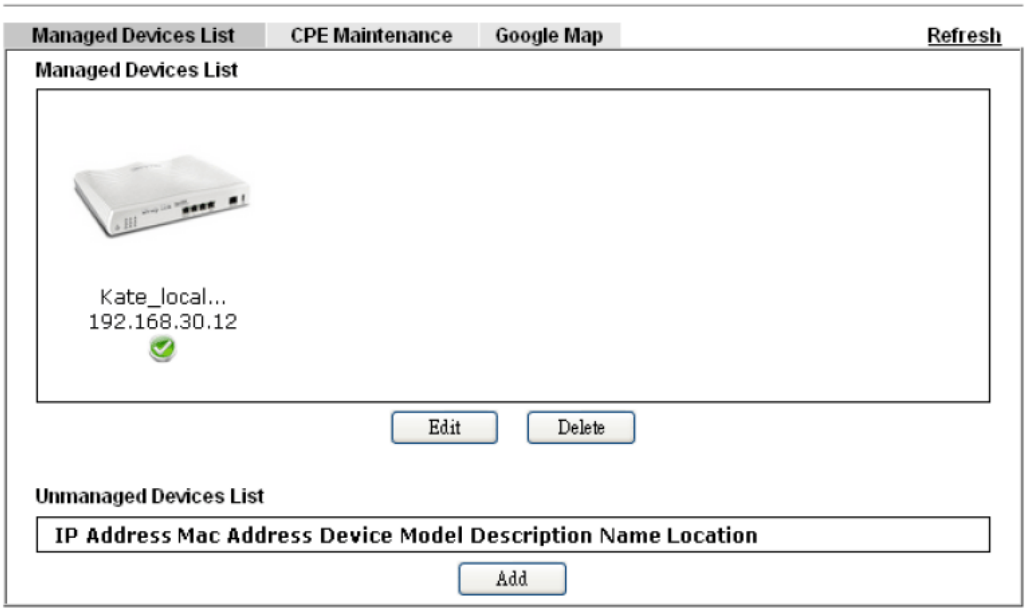
Reinicie el dispositivo CPE y vuelva a iniciar sesión en la serie Vigor2927. El CPE que se ha registrado en la serie Vigor2927 se capturará y se mostrará en la página de Administración central de VPN>>Gestión de CPE.

Consulte la página de mantenimiento de CPE

1. Vuelva a la interfaz de usuario web de la serie Vigor2927.
2. Abierto**Gestión central>>VPN>>Gestión de VPN**. Ahora se muestra un CPE en el campo de la Lista de dispositivos no administrados.
3. Elija uno (Vigor2927) de la lista de dispositivos no administrados y haga clic en**Agregar**. Aparecerá el siguiente cuadro de diálogo. Ingrese el nombre y la ubicación del enrutador respectivamente.
   Hacer clic**DE ACUERDO**para guardar la configuración.



4. El CPE seleccionado se moverá y se mostrará en la Lista de dispositivos administrados, lo que significa que está controlado/administrado por la serie Vigor2927 a partir de ahora.

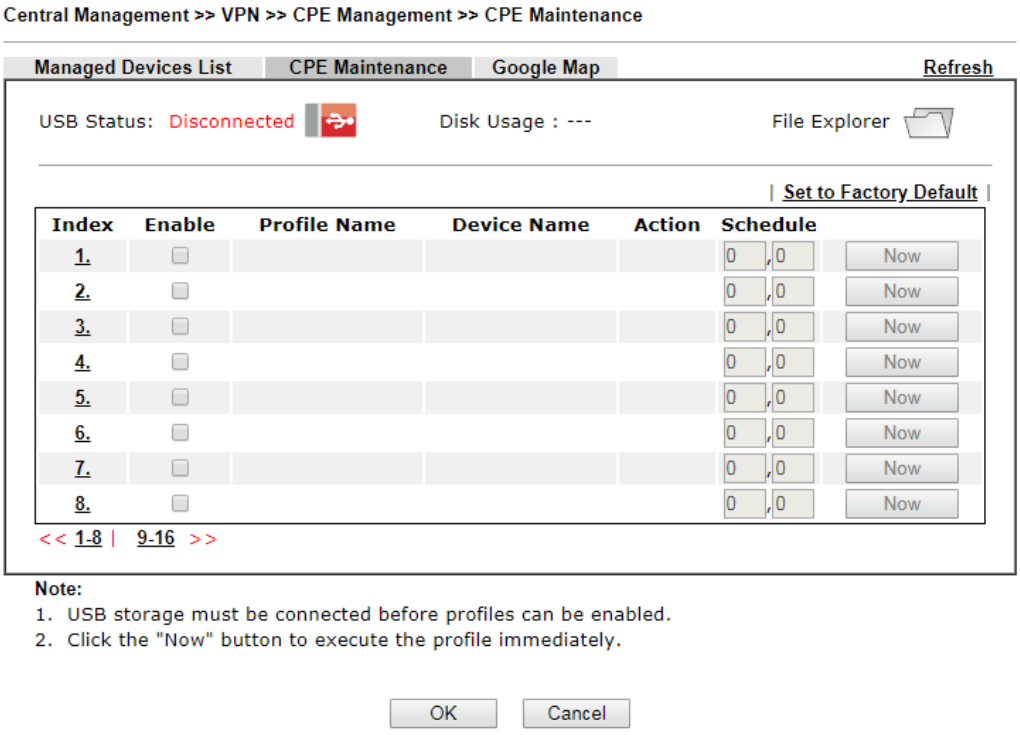


Descargue el firmware más reciente desde su sitio web de Draytek al disco de almacenamiento USB para el dispositivo (p. ej., Vigor2865) administrado por la serie Vigor2927.

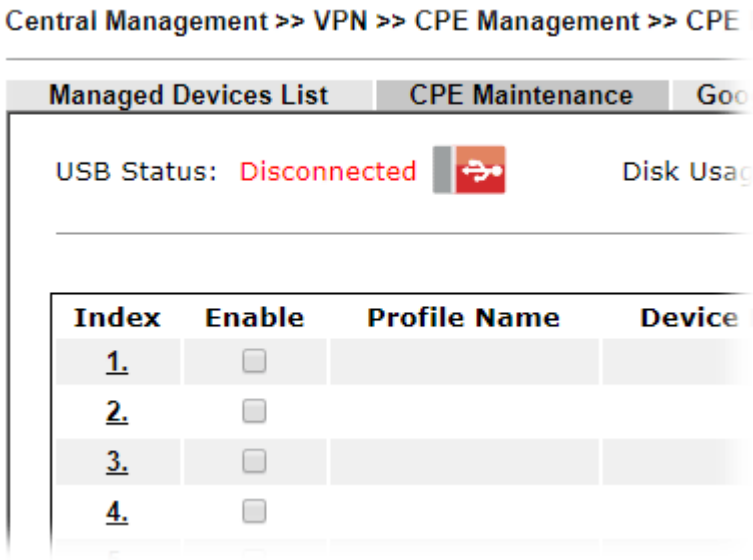
Vigor2865, como ejemplo, se elige para Vigor2927 para realizar la actualización de firmware de CPE de forma remota en este caso.

1. Conecte el disco de almacenamiento USB a la serie Vigor2927 a través de la interfaz USB. Asegúrese de que el disco USB se haya instalado correctamente; de lo contrario, la actualización del firmware no se realizará correctamente.

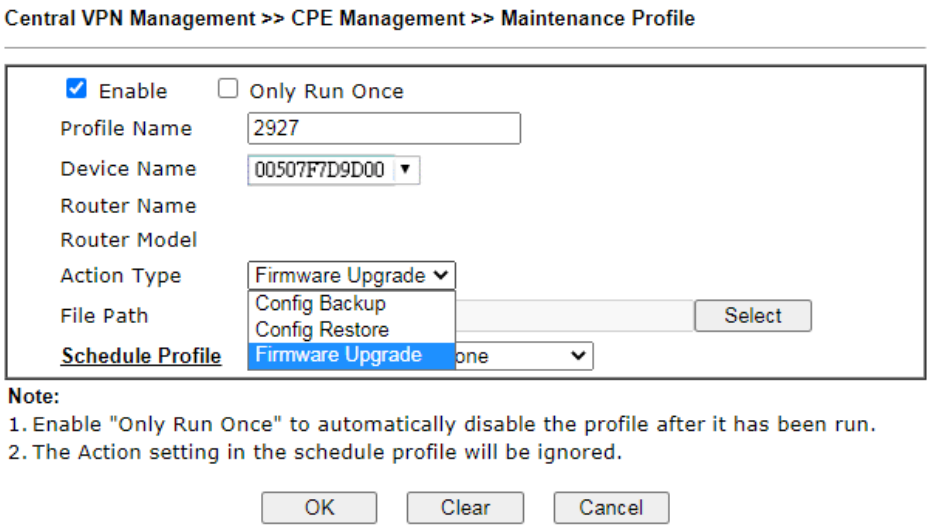
2. Acceso a la interfaz de usuario web de la serie Vigor2927. centro abierto**Gestión de VPN>>Gestión de CPE**y haga clic en el**Mantenimiento de CPE**pestaña.



3. Haga clic en cualquier enlace de número de índice, por ejemplo, Índice 1.

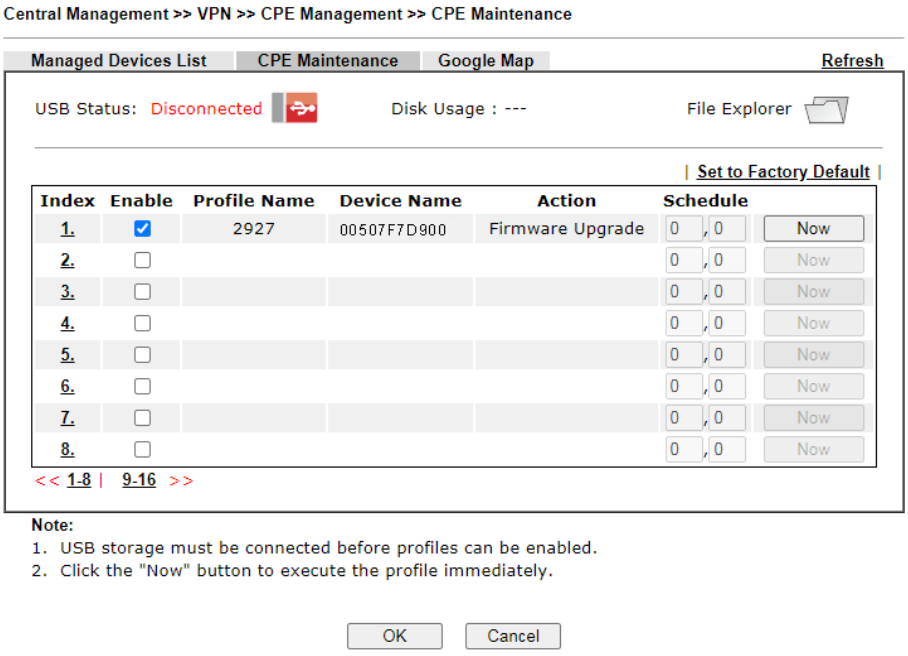


4. Aparece el cuadro de diálogo Perfil de mantenimiento.



En el campo Nombre del perfil, escriba un nombre para dicho perfil de mantenimiento; marque Habilitar; y elija el que desea realizar la actualización de firmware de la lista desplegable Nombre del dispositivo. Desde el Tipo de acción, elija Actualización de firmware. Ingrese el archivo/ruta del firmware más reciente o haga clic en Seleccionar para localizarlo. Especifique el perfil de programación. Por último, haz clic**DE ACUERDO**.

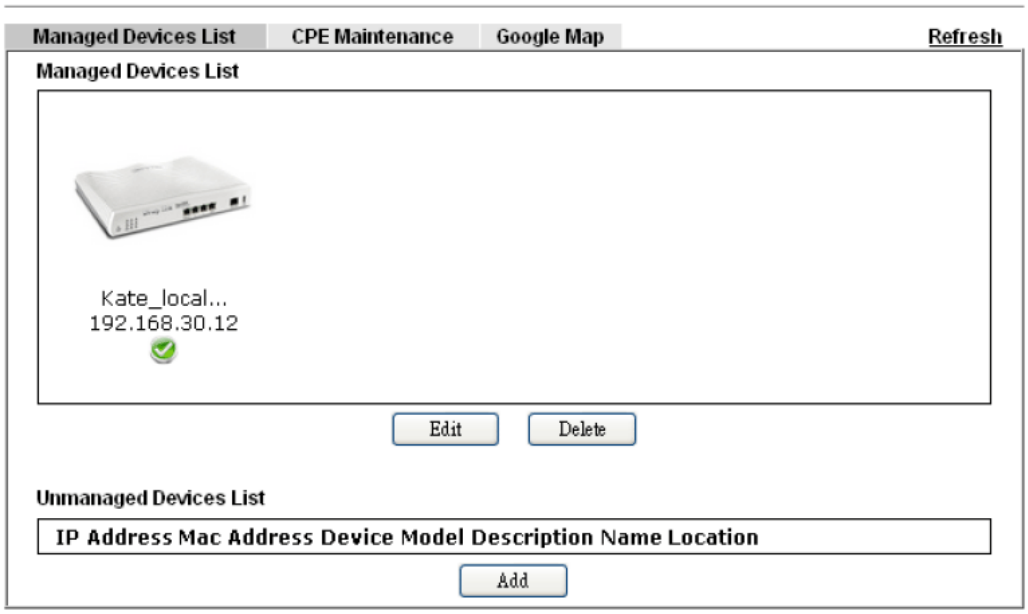
5. Ahora, se ha creado un nuevo perfil de mantenimiento.



6. Haga clic en**Ahora**para realizar la actualización de firmware inmediatamente para Vigor2927.

7. Espere varios minutos para la actualización del firmware.

8. Luego verifique la información del dispositivo para el dispositivo administrado si la actualización del firmware es exitosa o no. Hacer clic**Lista de dispositivos administrados**.



Haga clic en el icono de Vigor2865 y haga clic en**Editar**y ver la versión del software. Otra forma de verificar si la actualización del firmware se completó o no, simplemente abra**Administración central de VPN>>Registro y alerta**.

VII-6 Gestión Central (AP)

Vigor2927 puede gestionar los puntos de acceso compatibles con la gestión de puntos de acceso a través de la gestión central de puntos de acceso.

Mapa AP

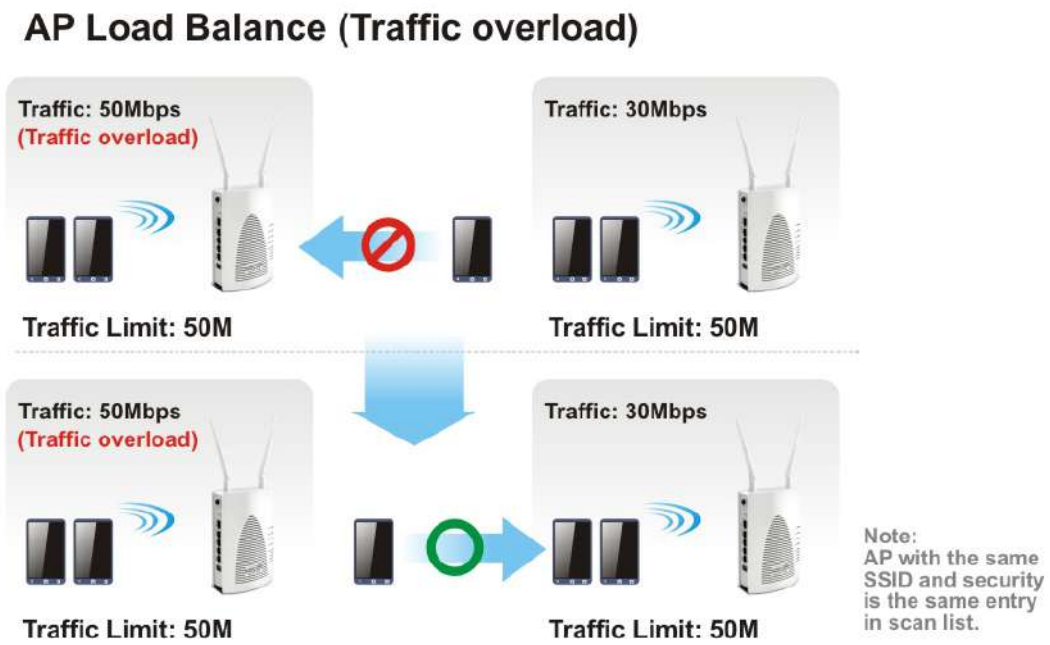
AP Map es útil para determinar la mejor ubicación para VigorAP en una habitación. Primero se debe cargar un plano de planta de una habitación. Al arrastrar y soltar el ícono de VigorAP disponible de la lista al plano de planta, la ubicación con la mejor cobertura inalámbrica se indicará claramente a través de la intensidad de la señal simulada

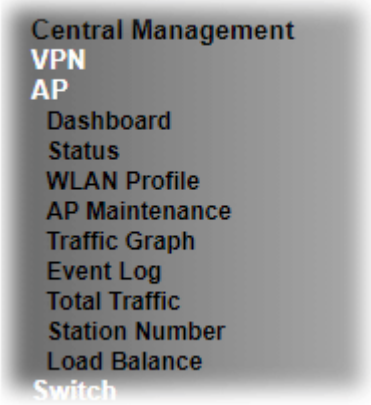
Mantenimiento AP

El enrutador Vigor puede ejecutar la copia de seguridad de la configuración, la restauración de la configuración, la actualización del firmware y el reinicio remoto para los puntos de acceso administrados por el enrutador. Es muy conveniente para el administrador procesar el mantenimiento sin acceder a la interfaz de usuario web del punto de acceso.

Balance de carga para AP

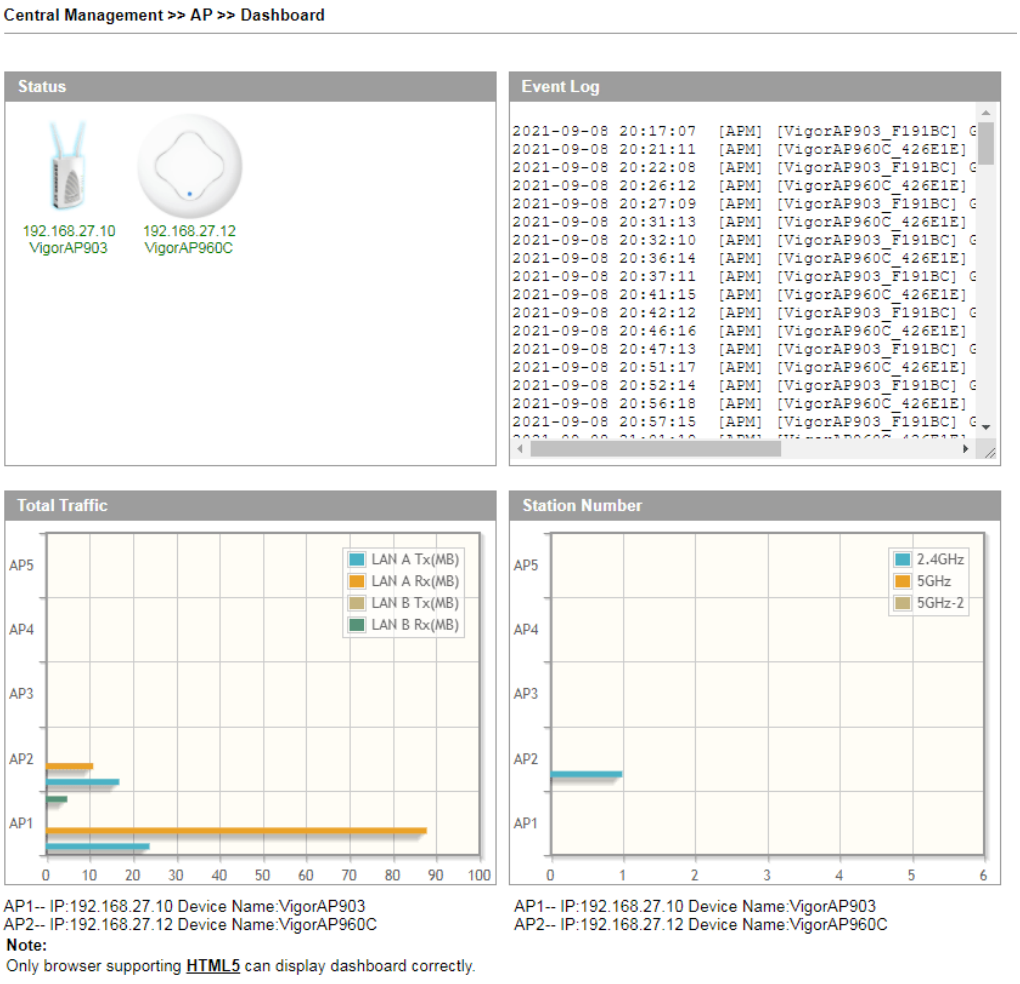
Los parámetros configurados para Load Balance pueden ayudar a distribuir el tráfico para todos los puntos de acceso registrados en el enrutador Vigor. Así, el ancho de banda no será ocupado por determinados puntos de acceso.





Tablero VII-6-1

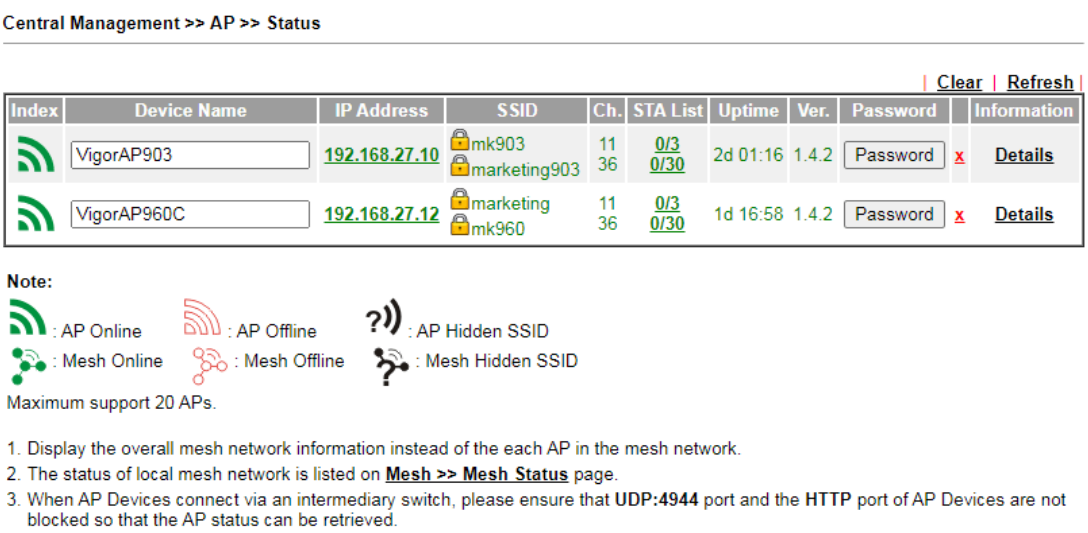
Esta página muestra la información de VigorAP sobre**Estado, registro de eventos, tráfico total**o**Número de Estación** mostrando el icono, el texto y el histograma de VigorAP. Simplemente mueva y haga clic con el cursor del mouse en **Estado, registro de eventos, tráfico total**o**Número de Estación.**Las páginas web correspondientes se abrirán inmediatamente.



Para acceder a la interfaz de usuario web de VigorAP, simplemente mueva el cursor del mouse sobre el icono de VigorAP y haga clic en él. El sistema lo guiará para acceder a la interfaz de usuario web de VigorAP.

VII-6-2 Estado

Esta página muestra el estado actual (en línea, fuera de línea o SSID oculto, dirección IP, encriptación, canal, versión, contraseña, etc.) de los puntos de acceso administrados por el enrutador Vigor. Por favor abre**Administración central de puntos de acceso>>Lista de compatibilidad de funciones**para verificar qué modelos de AP son compatibles.

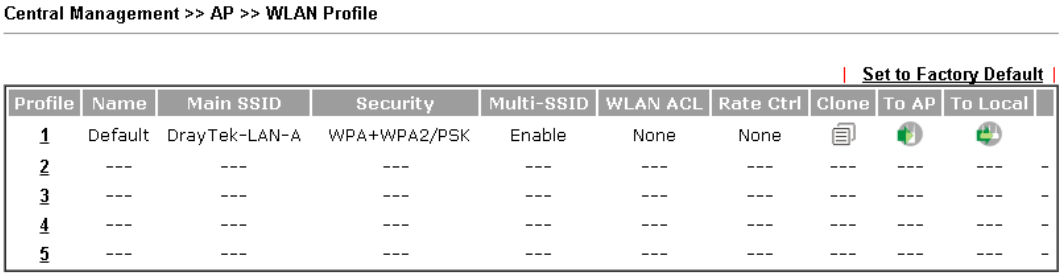


Los ajustes disponibles se explican a continuación:

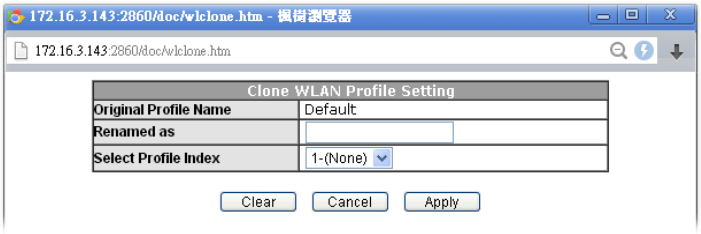
Artículo	Descripción
Índice	Haga clic en el enlace del número de índice para ver el resumen de configuración del punto de acceso.
Nombre del dispositivo	El nombre del AP administrado por el enrutador Vigor se mostrará aquí.
Dirección IP	Muestra la verdadera dirección IP del punto de acceso.
SSID	Muestra el SSID configurado para los puntos de acceso conectados a Vigor2927.
cap.	Muestra el canal utilizado por el punto de acceso.
Lista de STA	Muestra el número de clientes inalámbricos (estaciones) que se conectan al punto de acceso. Donde, 0/64 significa que hasta 64 clientes pueden conectarse al punto de acceso. Pero, ahora nadie se conecta al punto de acceso. El número que se muestra en el lado izquierdo significa 2,4 GHz; y el número que se muestra en el lado derecho significa 5GHz.
tiempo de actividad	Muestra la duración del AP encendido.
Versión	Muestra la versión de firmware utilizada por el punto de acceso.
Contraseña	Vigor2927 puede obtener información relacionada con el punto de acceso accediendo a la interfaz de usuario web del punto de acceso. Este botón se utiliza para modificar la contraseña de registro del punto de acceso conectado.
Detalles	Haga clic para abrir una ventana de información detallada relacionada con el VigorAP seleccionado.

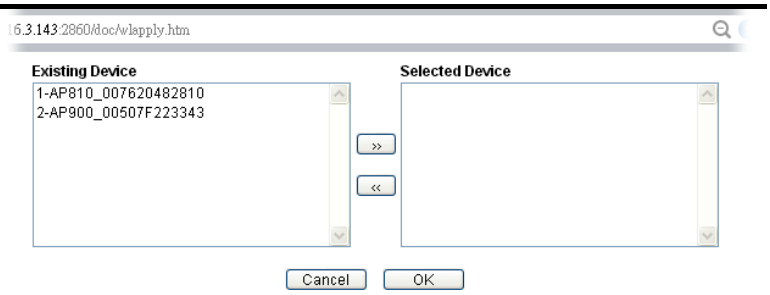
Perfil WLAN VII-6-3

El perfil WLAN se utiliza para aplicar a un punto de acceso seleccionado. Es muy conveniente para el administrador configurar la configuración del punto de acceso sin abrir la interfaz de usuario web del punto de acceso.



Haga clic en el enlace del número del perfil seleccionado para modificar el contenido del perfil. Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Perfil	Hay cinco perfiles de WLAN que se ofrecen para configurar. Simplemente haga clic en el enlace del número de índice para abrir la página de modificación.
Nombre	Mostrar el nombre del perfil. No se puede cambiar el nombre del perfil predeterminado.
SSID principal	Muestra el SSID configurado por dicho perfil inalámbrico.
Seguridad	Muestra el modo de seguridad seleccionado por dicho perfil inalámbrico.
SSID múltiple	Habilitar significa que varios SSID (más de uno) están activos. Deshabilitar significa que solo SSID1 está activo.
ACL de WLAN	Muestra el nombre de la lista de control de acceso.
Calificar Ctrl	Muestra la tasa de transmisión de carga y/o descarga.
Clon	Puede copiar configuraciones de un perfil de WLAN existente a otro perfil de WLAN. Primero, debe marcar la casilla del perfil existente como el perfil original. En segundo lugar, haga clic en**Clon**. Aparecerá el siguiente diálogo.  En tercer lugar, elija el índice de perfil para aceptar la configuración del perfil original. En cuarto lugar, escriba un nuevo nombre en el campo de **Renombrado como**. Por último, haga clic**Aplicar**para guardar la configuración en este cuadro de diálogo. El nuevo perfil se ha creado con la configuración procedente del perfil original.
A punto de acceso	Haga clic en él para aplicar el perfil inalámbrico seleccionado al punto de acceso especificado.

	 Simplemente elija el dispositivo que desee**Dispositivo existente**campo. Hacer clic**>>**para mover el dispositivo a**Dispositivo seleccionado**campo. Luego, haga clic en**DE ACUERDO**. El perfil WLAN seleccionado se aplicará al punto de acceso seleccionado inmediatamente. Más tarde, el punto de acceso se reiniciará.
a locales	El perfil WLAN configurado en esta página se especifica para VigorAP conectado al enrutador Vigor. Si es necesario, esta configuración también se puede aplicar al enrutador Vigor. Seleccione y marque uno de los perfiles inalámbricos y haga clic en este botón para aplicar la configuración a la configuración inalámbrica WI-Fi configurada para dicho enrutador Vigor.

¿Cómo editar el perfil de LAN inalámbrica?

1. Seleccione el perfil WLAN (número de índice 1 a 5) que desea editar.

2. Haga clic en el enlace del número de índice para mostrar la siguiente página.

Central Management >> AP >> WLAN Profile

WLAN Profile Edit

Device Settings	
Profile Name	Default ☐ Auto Provision
Administrator	admin
Password	•••••
2nd Subnet	◉ Enable ○ Disable
Management VLAN	☐ Enable Management VLAN: LAN-A VLAN ID 0 (0 ~ 4095) LAN-B VLAN ID 0 (0 ~ 4095)

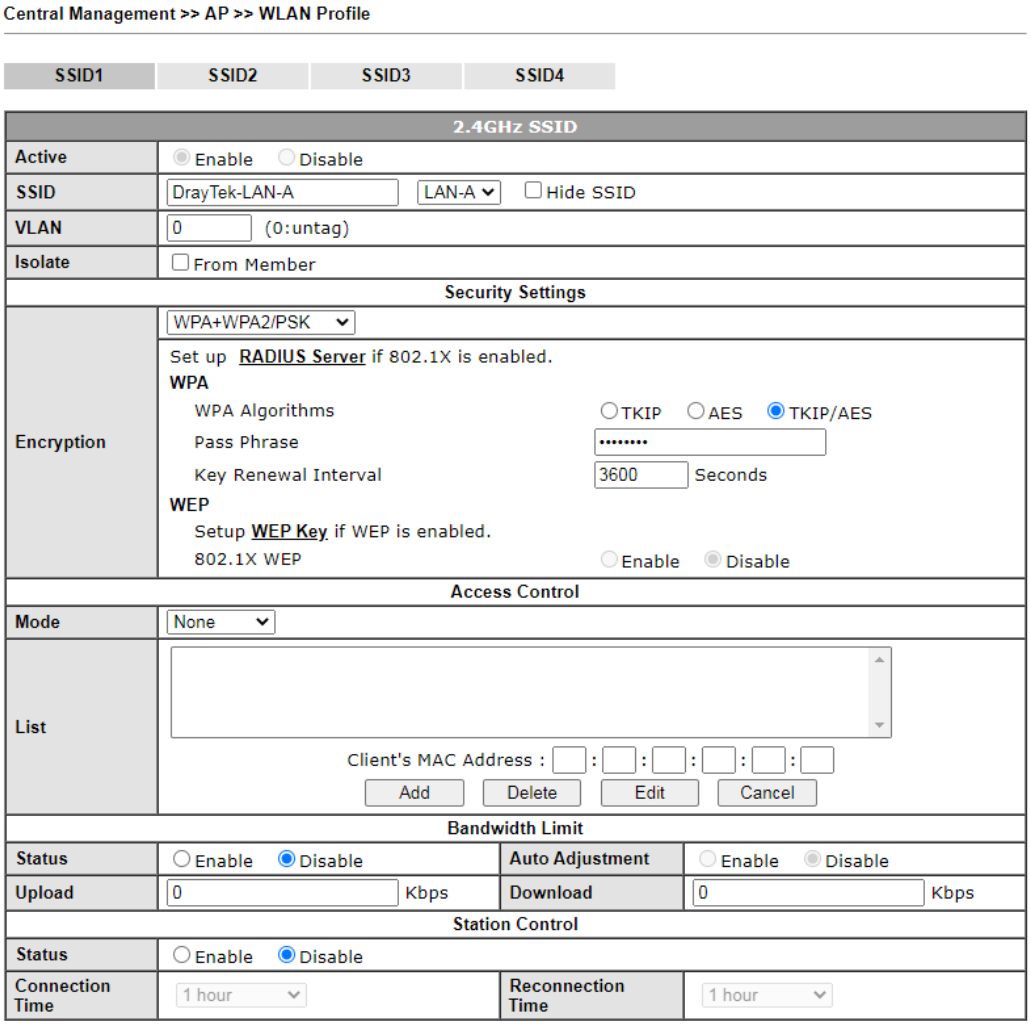
WLAN General Setting

2.4GHz	5GHz	5GHz-2
Wireless LAN	○ Enable ◉ Disable	
Limit Client	☐ Enable 64 (3 ~ 128, default: 64)	
Operation Mode	AP	
2.4G Mode	Mixed(11b+11g+11n)	
2.4G Channel	2462MHz (Channel 11)	
Airtime Fairness	☐ Enable Airtime Fairness: Triggering Client Number 2 (2 ~ 128, default: 2)	
Band Steering	☐ Enable Band Steering: Check Time for WLAN Client 5G Cap. 15 seconds (1 ~ 60, default: 15)	
Roaming	☐ Minimum Basic Rate 1 Mbps ◉ Disable RSSI Requirement ○ Strictly Minimum RSSI - 73 dbm (42 %) (default: -73) ○ Minimum RSSI - 66 dbm (60 %) (default: -66) with Adjacent AP RSSI over 5 dB (default: 5) ☐ Enable Fast Roaming(WPA2/802.1x): PMK Cache Period 10 minutes (10 ~ 600, default: 10)	
WMM	○ Enable ◉ Disable	
Tx Power	100%	
Channel Width	Auto 20/40 MHz	

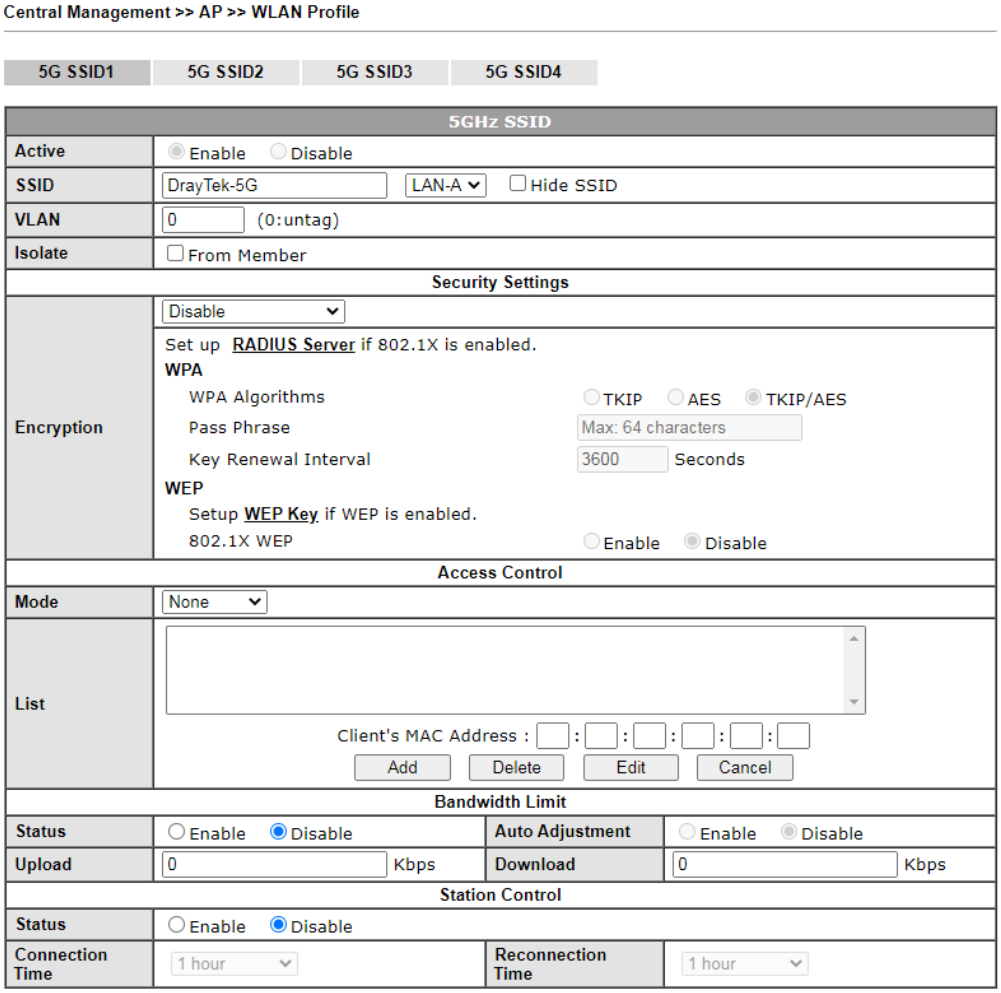
Información

La función de Aprovisionamiento automático está disponible para el perfil WLAN predeterminado.

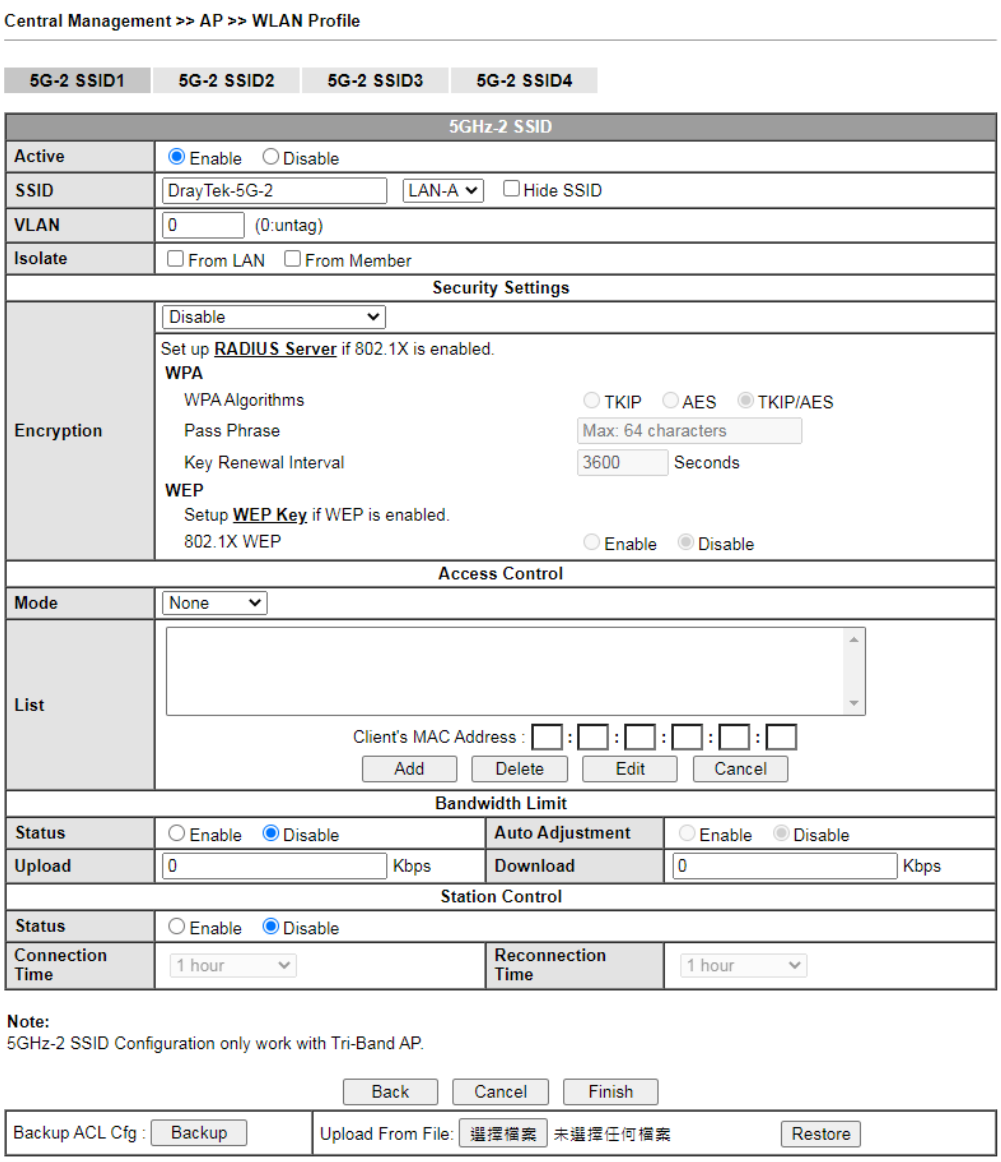
3. Después de terminar la configuración de los ajustes generales, haga clic en**Próximo**para abrir la página siguiente para la configuración de seguridad inalámbrica de 2,4 GHz.



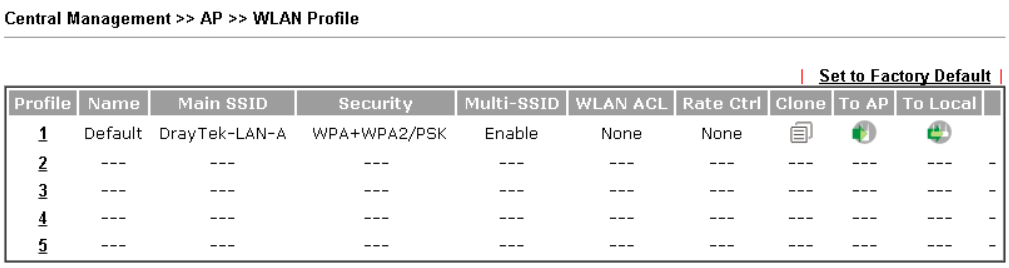
4. Después de terminar la configuración de la página web anterior, haga clic en**Próximo**para abrir la página siguiente para la configuración de seguridad inalámbrica de 5 GHz.



y configuración de seguridad inalámbrica de 5 GHz-2



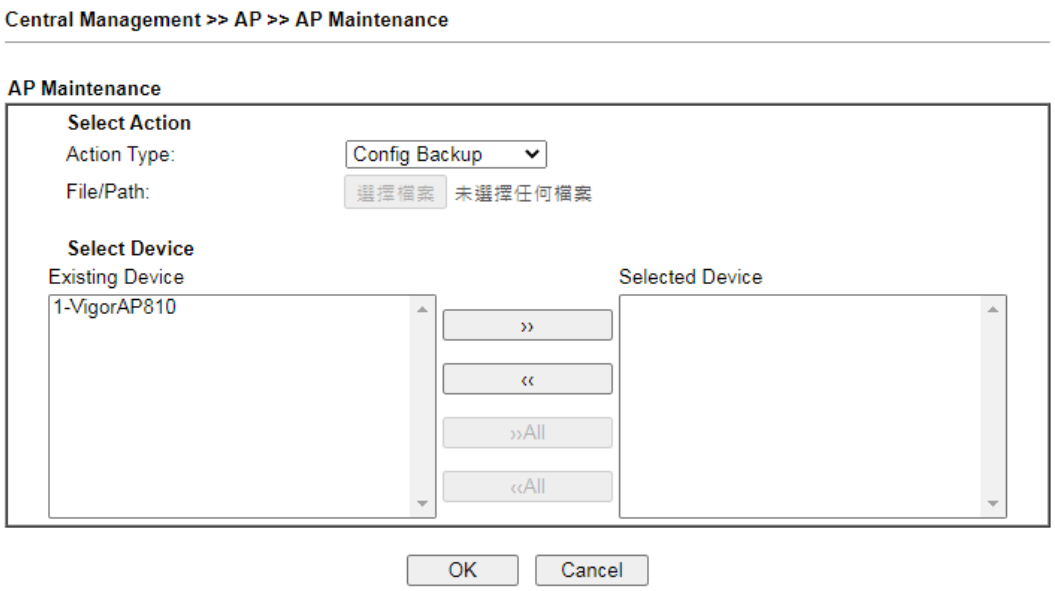
5. Cuando haya terminado la configuración de la página web anterior, haga clic en**Finalizar**para salir y volver a la primera página. El perfil WLAN modificado se mostrará en la página web.



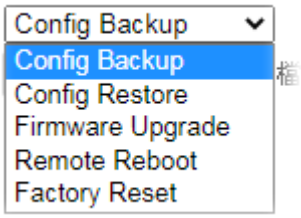
VII-6-4 Mantenimiento AP

El enrutador Vigor puede ejecutar la copia de seguridad de la configuración, la restauración de la configuración, la actualización del firmware y el reinicio remoto para los puntos de acceso administrados por el enrutador. Es muy conveniente para el administrador procesar el mantenimiento sin acceder a la interfaz de usuario web del punto de acceso.

Información	La copia de seguridad de configuración se puede realizar en un AP a la vez. Otras funciones (p. ej., restauración de configuración, actualización de firmware, reinicio remoto) se pueden realizar en más de un AP a la vez mediante el uso de Vigor2927.



Los ajustes disponibles se explican a continuación:

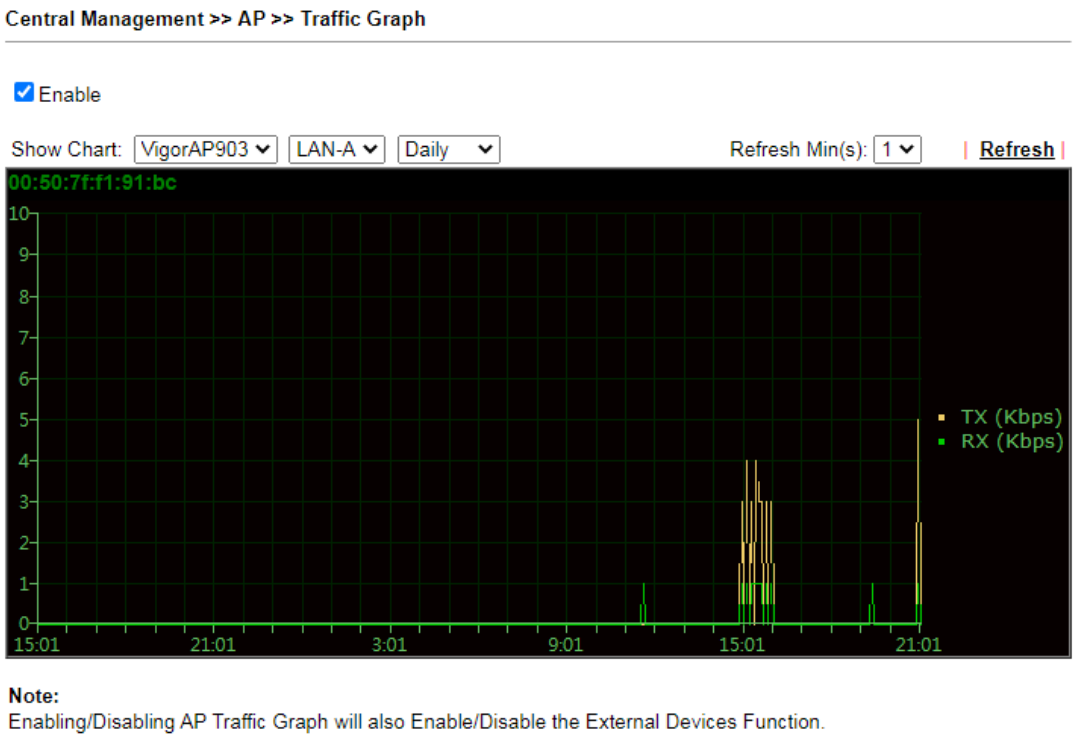
Artículo	Descripción
Acción	Hay cuatro acciones proporcionadas por el enrutador Vigor para administrar los puntos de acceso.  El enrutador Vigor puede**respaldo**la configuración del AP seleccionado, **restaurar**la configuración para el AP seleccionado, realice el **actualización de firmware**del AP seleccionado,**reiniciar**el AP seleccionado de forma remota y realizar la**restablecimiento de fábrica**para el AP seleccionado.
Ruta de archivo	Especifique el archivo y la ruta que se utilizará para realizar **Restaurar configuración**o**Actualización de firmware**.
Seleccione el dispositivo	Muestra todos los puntos de acceso disponibles administrados por el enrutador Vigor. Simplemente haga clic en << o >> para mover los dispositivos entre **Seleccione el dispositivo**y**Dispositivo seleccionado**áreas

Dispositivo seleccionado	Muestre los puntos de acceso que se aplicarán mediante dicha función después de hacer clic en Aceptar.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para realizar la acción.

VII-6-5 Gráfico de tráfico

Hacer clic**Gráfico de tráfico**para abrir la página web. Elija uno de los puntos de acceso administrados, LAN-A o LAN-B, diario o semanal para ver el gráfico de transmisión de datos. Hacer clic**Actualizar**para renovar la gráfica en cualquier momento.



El eje horizontal representa el tiempo; el eje vertical representa la tasa de transmisión (en kbps).

Información	Habilitar/deshabilitar dicha función también habilitará/deshabilitará la función Dispositivos externos.

En esta página se mostrará el registro de tiempo y eventos para todos los AP administrados por el enrutador Vigor. Es útil para la resolución de problemas si es necesario.

Central Management >> AP >> Event Log

All Event Log | Clear | Refresh |

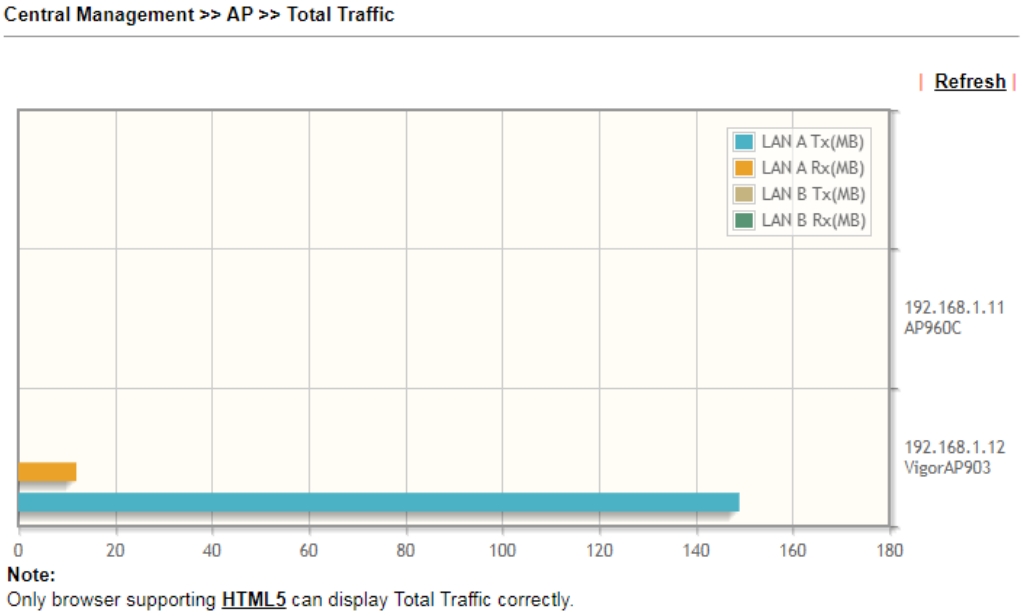
Time	APM Event Log
2000-01-12 00:34:50	[APM] [MK-AP 902_3D5490] Query Status success
2000-01-12 00:34:53	[APM] [MK-AP 902_3D5490] Apply Load Balance settings success
2000-01-12 00:35:19	[APM] [MK-AP 902_3D5490] Apply Rogue AP Detection settings success
2000-01-12 00:35:49	[APM] [MK-AP 902_3D5490] GET temper/traffic index success
2000-01-12 00:35:54	[APM] [MK-AP 902_3D5490] Query Status success
2000-01-12 00:36:10	[APM] [MK-AP 902_3D5490] GET temper/traffic data success
2000-01-12 00:36:54	[APM] [MK-AP 902_3D5490] Query Status success
2000-01-12 00:37:53	[APM] [MK-AP 902_3D5490] Query Status success
2000-01-12 00:38:53	[APM] [MK-AP 902_3D5490] Query Status success
2000-01-12 00:39:52	[APM] [MK-AP 902_3D5490] Query Status success
2000-01-12 00:40:52	[APM] [MK-AP 902_3D5490] Query Status success
2000-01-12 00:41:08	[APM] [MK-AP 902_3D5490] GET temper/traffic data success
2000-01-12 00:41:22	[APM] [MK-AP 902_3D5490] Query Status success
2000-01-12 00:42:25	[APM] [MK-AP 902_3D5490] Query Status success
2000-01-12 00:46:06	[APM] [MK-AP 902_3D5490] GET temper/traffic data success
2000-01-12 00:51:03	[APM] [MK-AP 902_3D5490] GET temper/traffic data success
2000-01-12 00:56:01	[APM] [MK-AP 902_3D5490] GET temper/traffic data success
2000-01-12 01:00:59	[APM] [MK-AP 902_3D5490] GET temper/traffic data success
2000-01-12 01:05:57	[APM] [MK-AP 902_3D5490] GET temper/traffic data success
2000-01-12 01:10:55	[APM] [MK-AP 902_3D5490] GET temper/traffic data success
2000-01-12 01:15:53	[APM] [MK-AP 902_3D5490] GET temper/traffic data success
2000-01-12 01:16:07	[APM] [MK-AP 902_3D5490] Query Status success
2000-01-12 01:18:21	[APM] [MK-AP 902_3D5490] Query Status success
2000-01-12 01:20:45	[APM] [MK-AP 902_3D5490] GET temper/traffic data success
2000-01-12 01:21:13	[APM] [MK-AP 902_3D5490] GET temper/traffic data success
2000-01-12 01:23:10	[APM] [MK-AP 902_3D5490] Apply Rogue AP Detection settings success
2000-01-12 01:25:01	[APM] [MK-AP 902_3D5490] Get Rogue AP Detection data failed
2000-01-12 01:25:22	[APM] [MK-AP 902_3D5490] Get Rogue AP Detection data failed
2000-01-12 01:25:42	[APM] [MK-AP 902_3D5490] Get Rogue AP Detection data failed
2000-01-12 01:26:03	[APM] [MK-AP 902_3D5490] Get Rogue AP Detection data failed
2000-01-12 01:26:09	[APM] [MK-AP 902_3D5490] GET temper/traffic data success
2000-01-12 01:26:23	[APM] [MK-AP 902_3D5490] Get Rogue AP Detection data failed

Note:

1. Only browser supporting **HTML5** can display Event Log correctly.
2. The APs Log can be refreshed after at least 30 seconds.

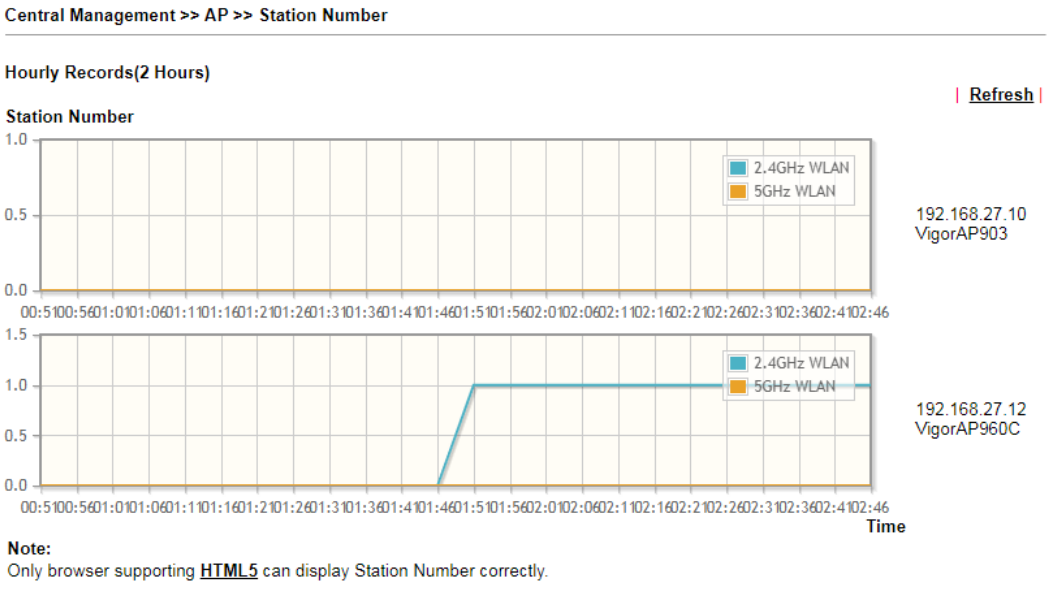
VII-6-7 Tráfico total

Dicha página mostrará el tráfico total de recepción y transmisión de datos para los VigorAP administrados por el enrutador Vigor.



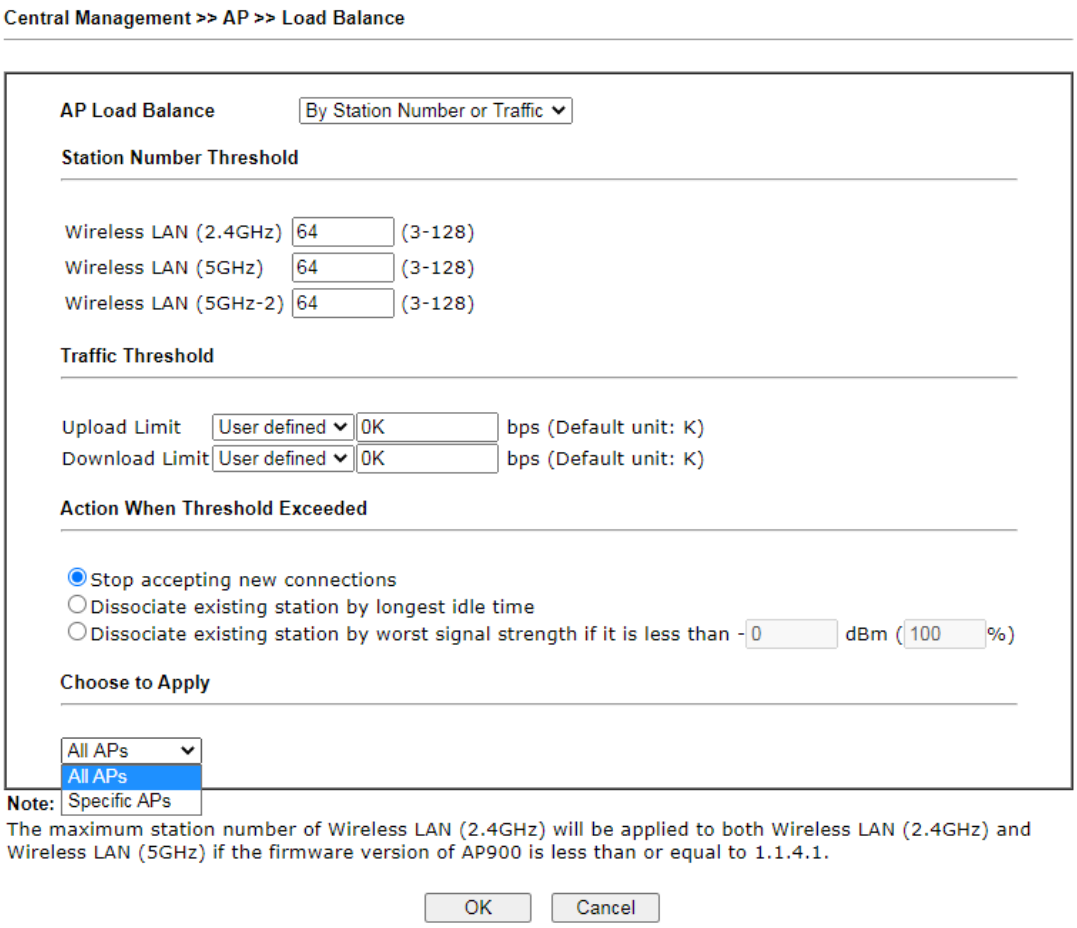
VII-6-8 Número de estación

El número total de clientes inalámbricos se mostrará en esta página, sin importar qué modo de conexión inalámbrica (2.4G WLAN o 5G WLAN) utilicen los clientes inalámbricos para acceder a Internet a través de VigorAP.



Equilibrio de carga VII-6-9

Los parámetros configurados para Load Balance pueden ayudar a distribuir el tráfico para todos los puntos de acceso registrados en el enrutador Vigor. Así, el ancho de banda no será ocupado por determinados puntos de acceso.



Los ajustes disponibles se explican a continuación:

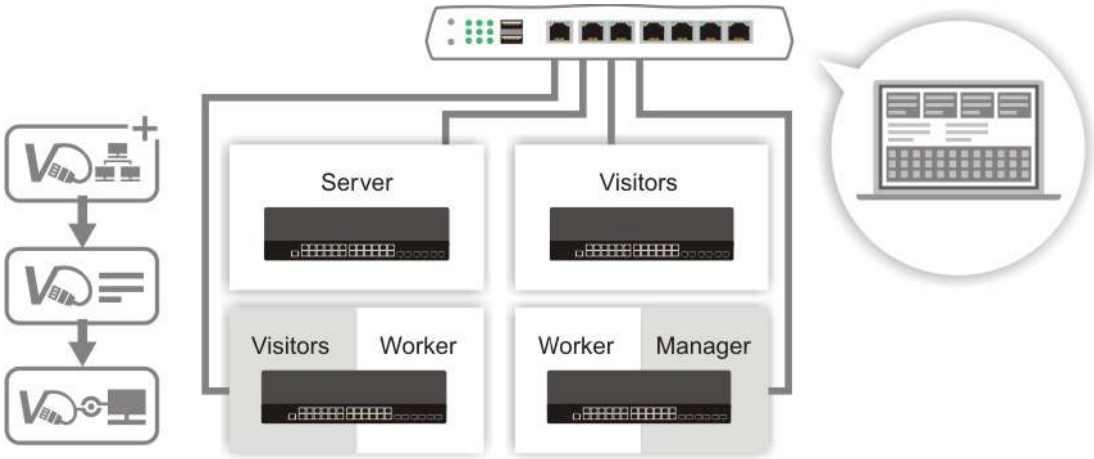
Artículo	Descripción
Equilibrio de carga AP	Se utiliza para determinar el modo de operación cuando el sistema detecta una sobrecarga entre los puntos de acceso. **Desactivar**–Deshabilite la función de equilibrio de carga AP. **Por número de estación**–La operación de balanceo de carga se ejecutará en base al número de estación configurado en esta página. Se utiliza para limitar el número permitido para la estación que se conecta al punto de acceso. El propósito es evitar que muchas estaciones se conecten al punto de acceso al mismo tiempo y causen un tráfico desequilibrado. Defina el número de estación necesario para WLAN (2,4 GHz) y WLAN (5 GHz) por separado. **Por Tráfico**–La operación de balanceo de carga se ejecutará de acuerdo a la configuración de tráfico en esta página. **Por número de estación o tráfico**-La operación de balanceo de carga se ejecutará en función del número de estación o de la configuración del tráfico.
Número de Estación Límite	Establezca el número de estaciones como umbral para activar el equilibrio de carga AP.

Umbral de tráfico	**Límite de carga**–Utilice la lista desplegable para especificar el límite de tráfico para la carga. **Límite de descarga**–Utilice la lista desplegable para especificar el límite de tráfico para la descarga.
Acción Cuándo Umbral Excedido	**Deja de aceptar nuevas conexiones –**Cuando el número de estaciones o el tráfico alcanza el umbral definido en esta página web, el enrutador Vigor detendrá cualquier nueva conexión solicitada por otro punto de acceso. **Disociar la estación existente por el tiempo de idel más largo**-Cuando el punto de acceso está sobrecargado (p. ej., alcanza el límite del número de estaciones o el límite del tráfico de la red), terminará la conexión de red de la estación del cliente que está inactiva durante mucho tiempo. **Disociar la estación existente por la peor intensidad de la señal si es inferior a**-Cuando el punto de acceso está sobrecargado (p. ej., alcanza el límite del número de estaciones o el límite del tráfico de red), terminará la conexión de red de la estación del cliente con la señal más débil.
Elija aplicar	Determine qué AP se aplicará con el equilibrio de carga. **Todos los AP**–Todos los AP se aplicarán con el equilibrio de carga. **AP específicos**–La función de balanceo de carga se aplicará al AP especificado en este campo.

Después de terminar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.

Gestión central VII-7 (conmutador)

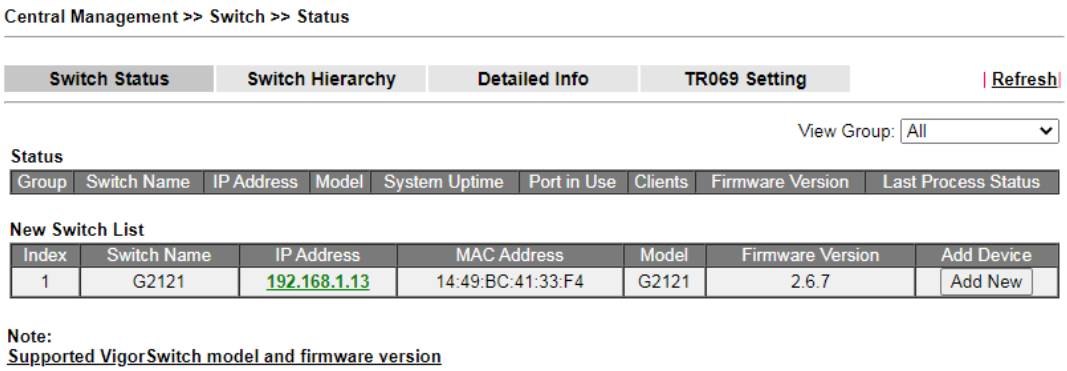
El enrutador Vigor puede administrar muchos dispositivos VigorSwitch conectados a él. A través de la configuración del perfil y del grupo, el administrador puede ejecutar una copia de seguridad del firmware/configuración, restaurar el dispositivo VigorSwitch, reiniciar el dispositivo o volver a la configuración predeterminada de fábrica de VigorSwitch al mismo tiempo.



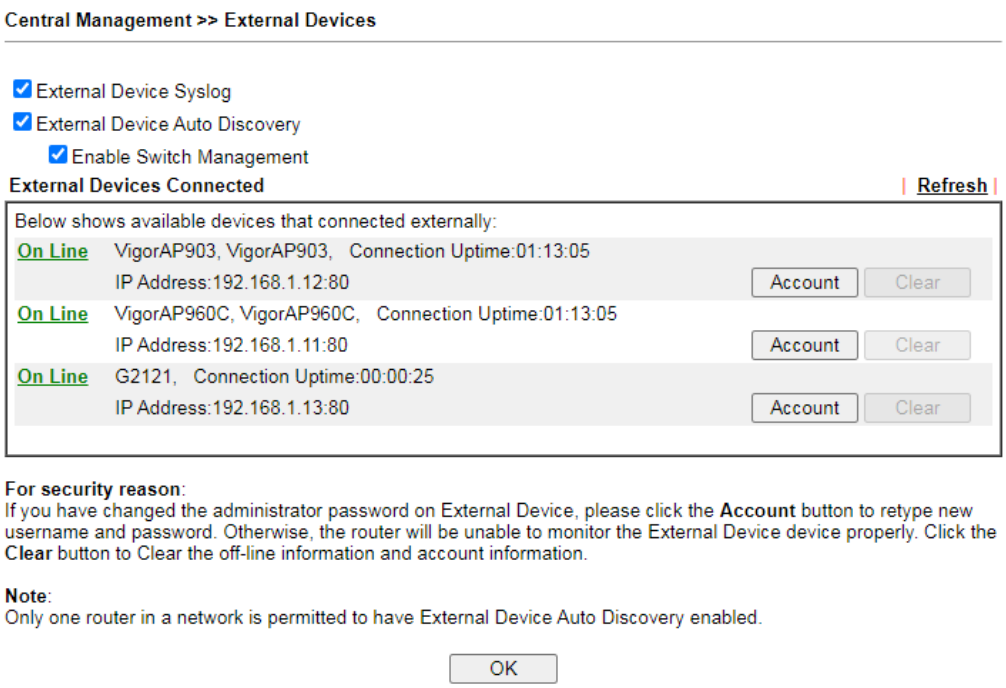
VII-7-1 Estado

VII-7-1-1 Estado del interruptor

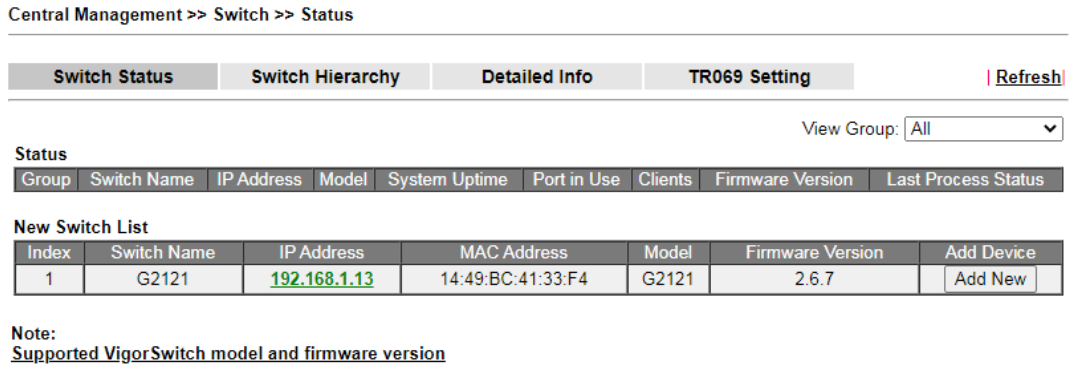
Dicha página muestra información, incluido el grupo, el nombre del conmutador, la dirección IP, el modelo, el tiempo de actividad del sistema, el puerto en uso, los clientes y la versión de firmware de VigorSwitch**conectado a**Serie Vigor2927.



Antes de comprobar el estado del interruptor, vaya a**Gestión central>>Dispositivo externo**para permitir **Detección automática de dispositivos externos**. Espere a que el sistema muestre los dispositivos disponibles.



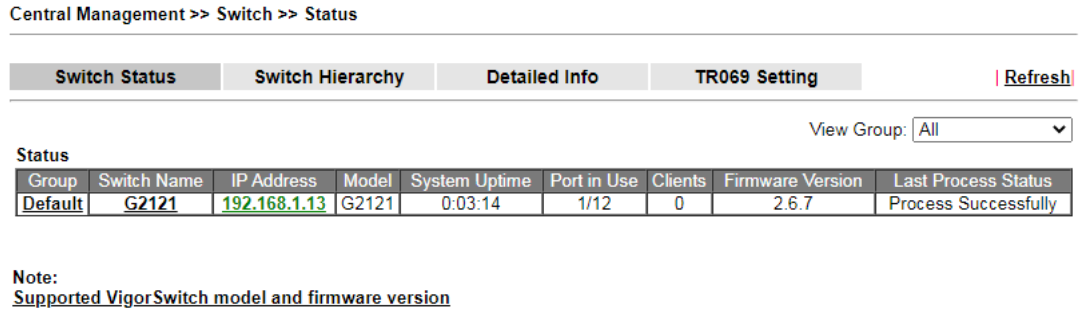
Más tarde, abre**Gestión central>>Switch>>Estado**. Los VigorSwitch disponibles para ser administrados por dicho enrutador se enumerarán en la Lista de nuevos conmutadores.



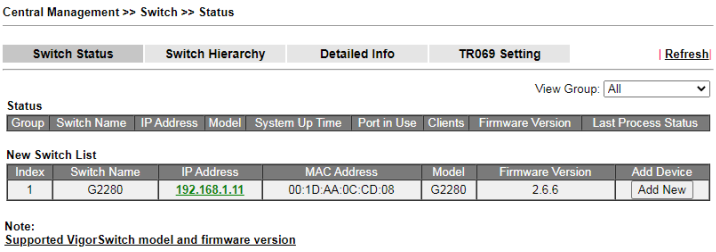
Información

VigorSwitch enumerado a continuación Estado significa que el conmutador es administrado por el enrutador Viogr; VigorSwitch enumerado a continuación New Switch List significa que Vigor2927 aún no lo administra.

Hacer clic**Agregar**para hacer que el VigorSwitch seleccionado sea administrado por el enrutador Vigor.

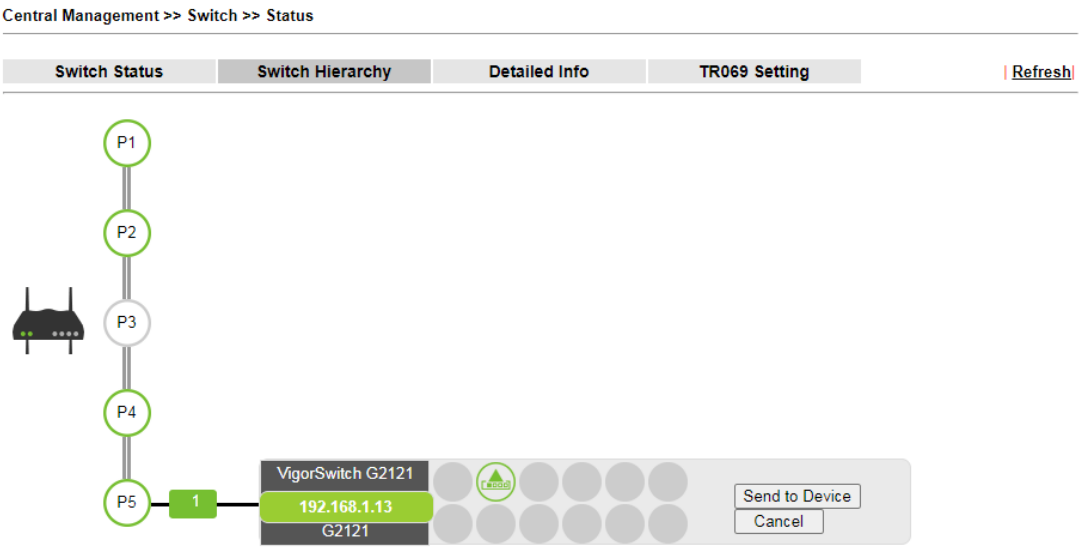


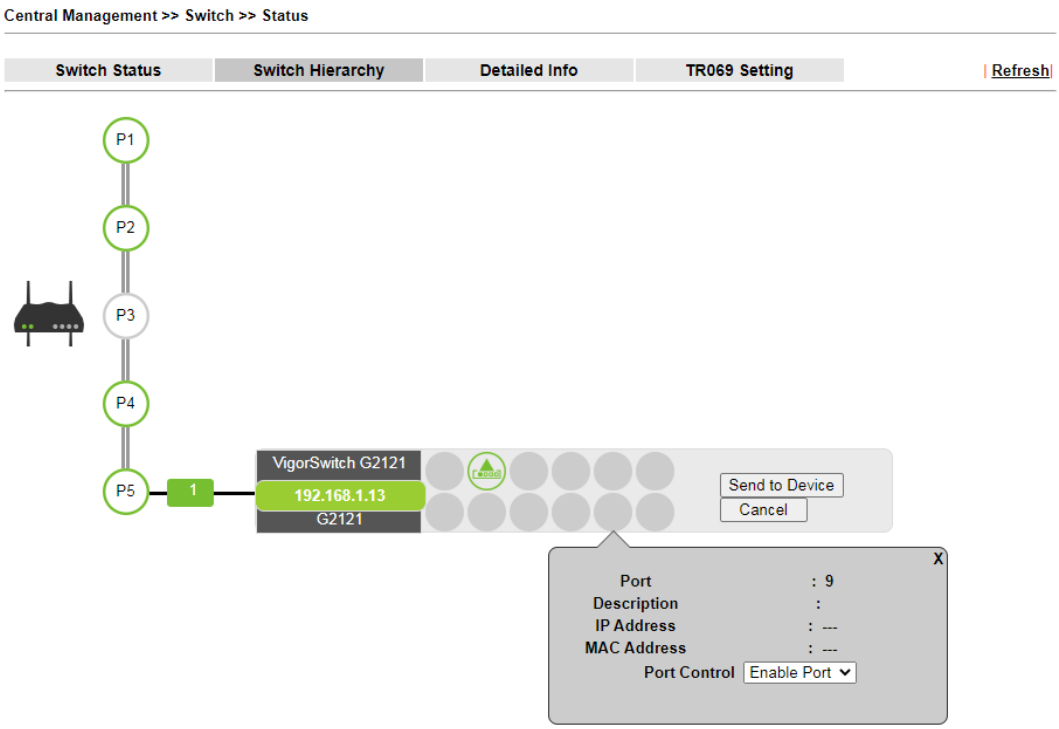
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Grupo	Muestra el enlace del nombre del grupo. Puede hacer clic en el enlace para modificar la configuración del grupo si es necesario.
Cambiar nombre	Muestra el enlace del nombre de VigorSwitch. Puede hacer clic en el enlace del nombre para acceder al perfil del conmutador.
Dirección IP	Muestra la dirección IP de VigorSwitch.
Modelo	Muestra el nombre del modelo de VigorSwitch.
Tiempo de actividad del sistema	Muestra el tiempo acumulado desde que se encendió este Vigorwitch.
Puerto en uso	Muestra cuántos dispositivos están conectados a VigorSwitch.
Clientela	Muestra el número de puertos LAN utilizados en VigorSwitch.
Versión de firmware	Muestra la versión de firmware que VigorSwitch utilizó actualmente.
Agregar	Dicho botón aparecerá solo cuando haya más de un interruptor conectado a Vigor2927. El que está en Nueva lista de interruptores se puede administrar en el grupo usado actual. Simplemente haga clic**Agregar**.  Será mejor agrupar dispositivos VigorSwitch con el mismo modelo.

Jerarquía de interruptores VII-7-1-2

Dicha página muestra la jerarquía de VigorSwitch(es) administrados bajo Vigor2927.

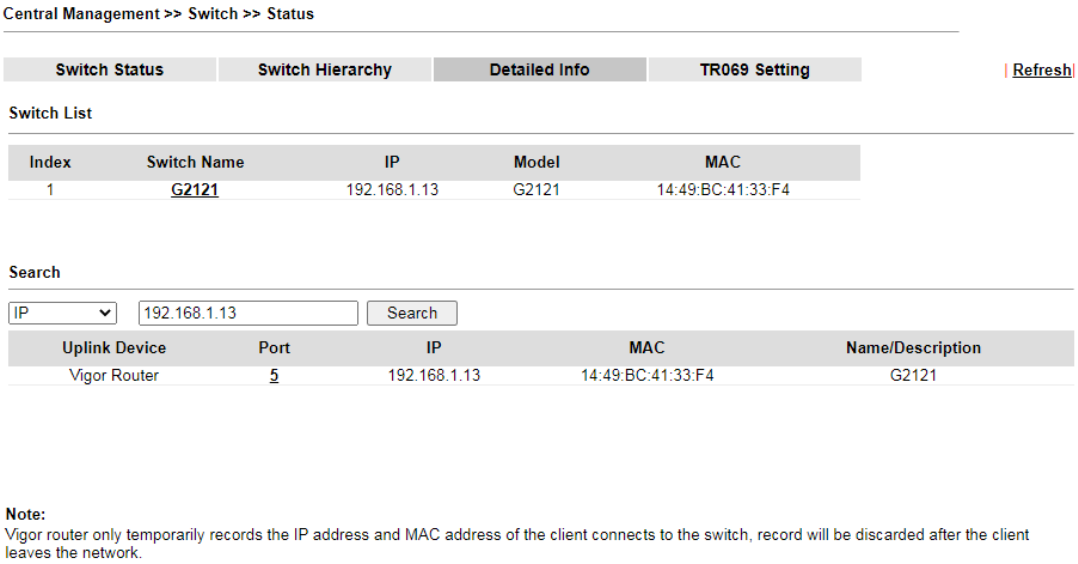




Tenga en cuenta que,**Puerto de cierre**está disponible para que el puerto LAN de VigorSwitch se conecte a un dispositivo LAN. Cuando está marcada, después de hacer clic**DE ACUERDO**, la conexión de red entre ese dispositivo y VigorSwitch terminará.

VII-7-1-3 Información detallada

Esta página muestra la jerarquía de VigorSwitch(es) administrados bajo Vigor2927.

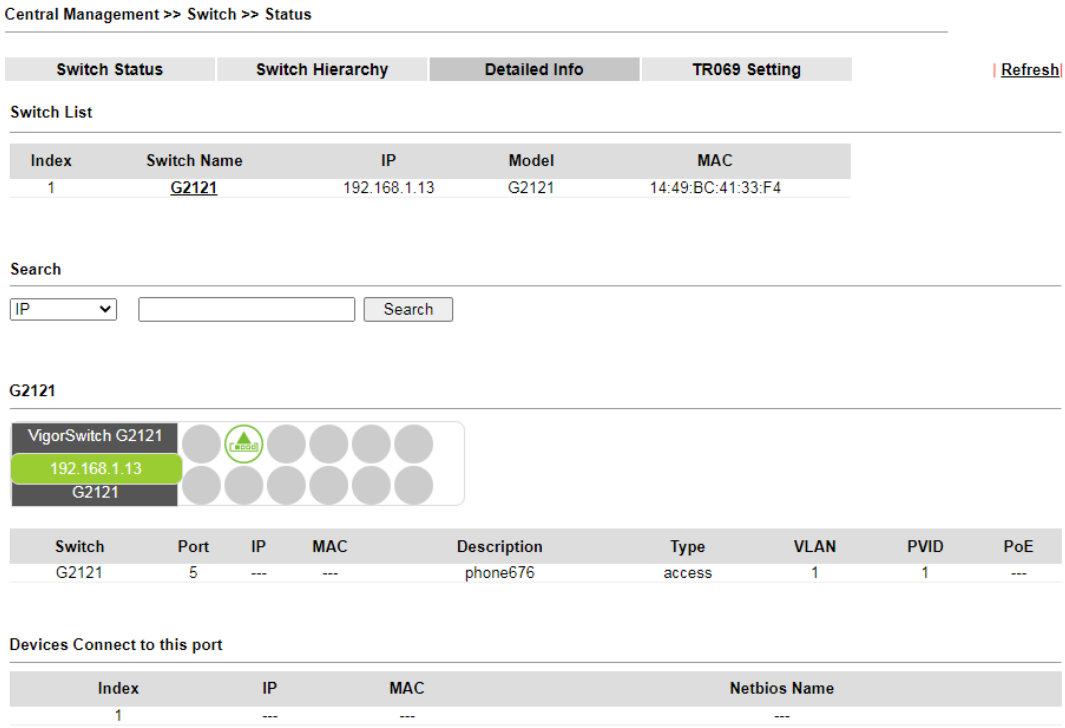


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Lista de interruptores	Muestra el número de índice, el nombre del conmutador, la dirección IP, el nombre del modelo y la dirección MAC del dispositivo VigorSwitch. **Cambiar nombre**-El enlace del nombre le permite acceder a la interfaz de usuario web del Vigor Switch.

	IP-Muestra la dirección IP del conmutador. **Modelo**-Muestra el nombre del modelo del conmutador. **MAC**-Muestra la dirección MAC del conmutador.
Buscar	**Buscar**-Después de especificar la dirección IP, la dirección MAC o el nombre del conmutador, haga clic en el botón Buscar para encontrar el dispositivo y mostrar el resultado de la búsqueda en esta página. **Dispositivo de enlace ascendente**-Muestra el nombre del servidor al que se conecta el conmutador Vigor. **Puerto**-Indica el puerto donde está conectado el conmutador al enrutador. Este enlace numérico le permite hacer clic para ver información más detallada del dispositivo buscado.

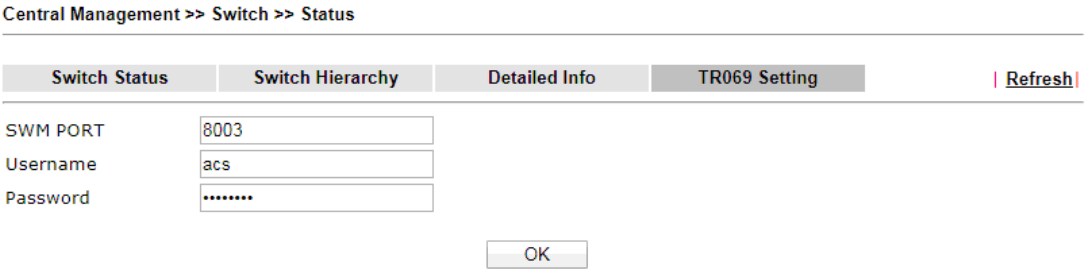
Haga clic en el vínculo del número de puerto (p. ej., 3) para abrir la siguiente página. En esta página se mostrará información detallada del nombre, número de puerto, dirección IP, dirección MAC, descripción, tipo, número de VLAN, valor PVID y capacidad PoE del conmutador.



Además, esta página mostrará la información básica (dirección IP, dirección MAC y nombre de Netbios) de "otros" dispositivos conectados a este conmutador.

Configuración VII-7-1-4 TR069

Además de HTTP/HTTPS, el enrutador Vigor puede administrar VigorSwitch con el protocolo TR-069.

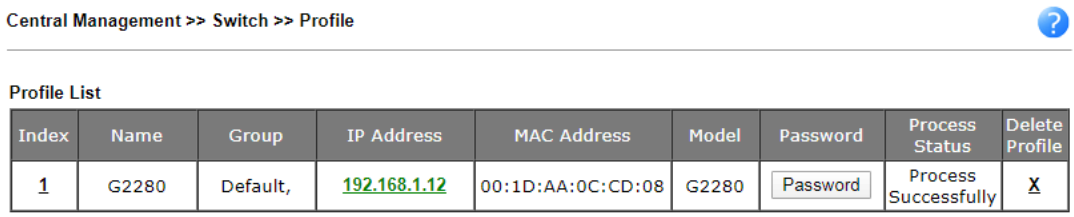


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Puerto SWM	El valor predeterminado es 8003. En caso de conflictos de puertos, cambie el número de puerto.
Nombre de usuario	Muestra el nombre de usuario que utilizará el conmutador Vigor para conectarse a este enrutador. Mantenga el valor predeterminado.
Contraseña	Muestra la contraseña que utilizará el conmutador Vigor para conectarse a este enrutador. Mantenga el valor predeterminado.

Perfil VII-7-2

Esta página mostrará información general, como nombre, grupo, dirección IP, dirección MAC, modelo y contraseña de VigorSwitch solo cuando se conecta a la serie Vigor2927. Al hacer clic en el enlace del número de índice, se mostrará una página de configuración de perfil para ese conmutador. Tenga en cuenta que cada perfil representa un VigorSwitch.

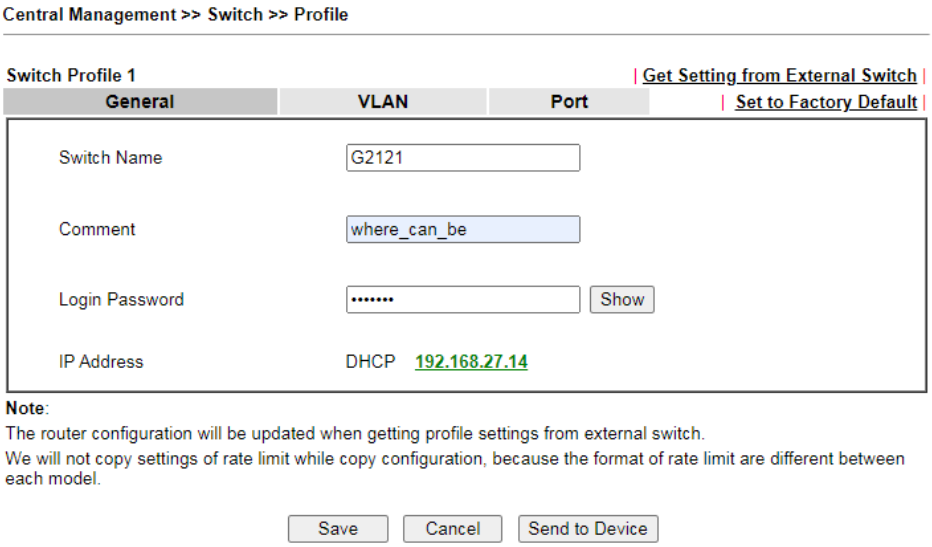


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Índice	Haga clic en el enlace del número para acceder al perfil del interruptor. Nota: Cada VigorSwitch conectado tendrá un perfil de configuración. Si hay muchos interruptores conectados a Vigor2927, se usará un número de índice diferente para representar diferentes VigorSwitch.
Nombre	Muestra el nombre definido por el usuario de VigorSwitch.
Grupo	Muestra el nombre del grupo de VigorSwitch(es).
Dirección IP	Muestra la dirección IP de VigorSwitch.
Dirección MAC	Muestra la dirección MAC de VigorSwitch.
Modelo	Muestra el nombre del modelo de VigorSwitch.
Contraseña	Haga clic en él para mostrar la información de la cuenta, incluido el nombre de usuario y la contraseña.
Borrar perfil	Haga clic en la marca de "X" para eliminar el perfil del interruptor.

Para editar el perfil del interruptor seleccionado:

1. Haga clic en el enlace del número de índice (p. ej., n.º 1) para abrir la siguiente página.

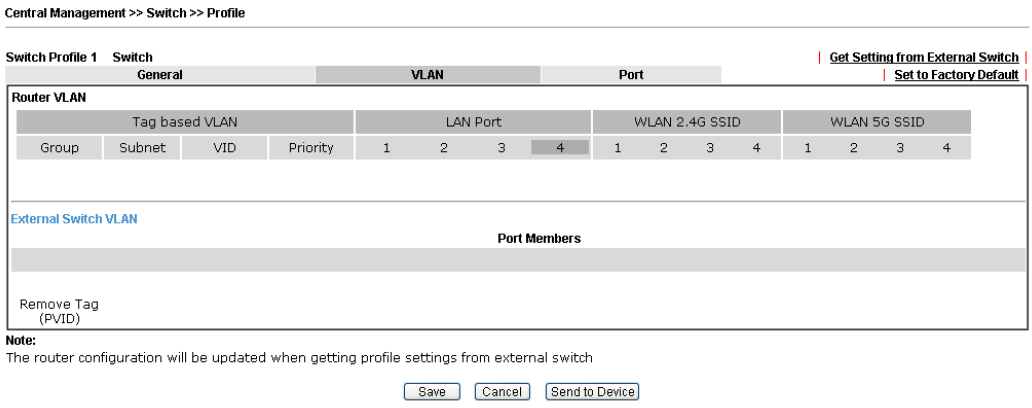


Los ajustes disponibles se explican a continuación:

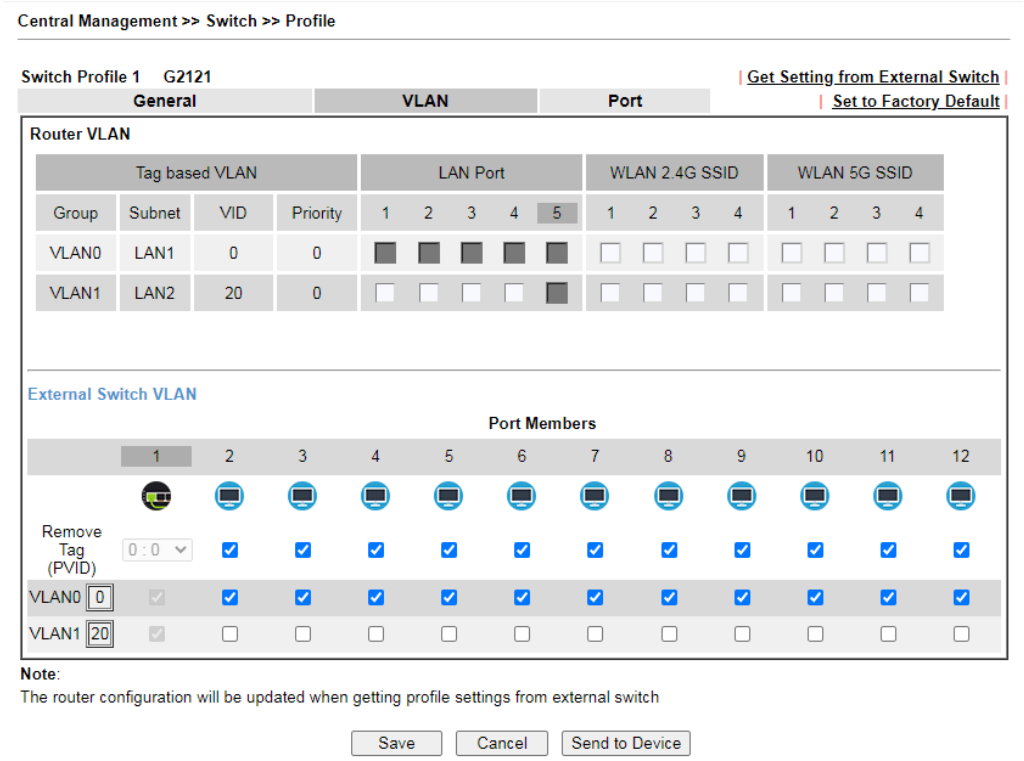
Artículo	Descripción
Cambiar nombre	Escriba un nombre para el conmutador. El propósito del nombre se utiliza para la identificación. Es útil cuando hay muchos dispositivos VigorSwitch (los mismos modos) que se conectan a los seres Vigor2927.
Comentario	Ingrese el texto en dicho campo si se requiere una explicación adicional para el cambio.
Contraseña de inicio de sesión	Muestre la contraseña de inicio de sesión original para el VigorSwitch. Sin embargo, si la contraseña de grupo (en**Gestión Central > > Cambiar>>Grupo**) está configurado con otra cadena, entonces dicho campo no puede escribir ninguna otra contraseña. Y solo se mostrará la contraseña del grupo, en su lugar.
Dirección IP	Muestra la dirección IP dinámica (del conmutador conectado) asignada por Vigor2927.
Ahorrar	Haga clic en él para guardar la configuración.
Cancelar	Haga clic en él para volver a la página web anterior sin guardar los cambios de configuración.
Enviar a dispositivo	Haga clic para transferir el cambio de configuración (por ejemplo, contraseña de inicio de sesión, nombre del interruptor, etc.) al VigorSwitch inmediatamente.

2. Después de terminar la configuración, haga clic en**VLAN**pestaña para abrir la página siguiente.

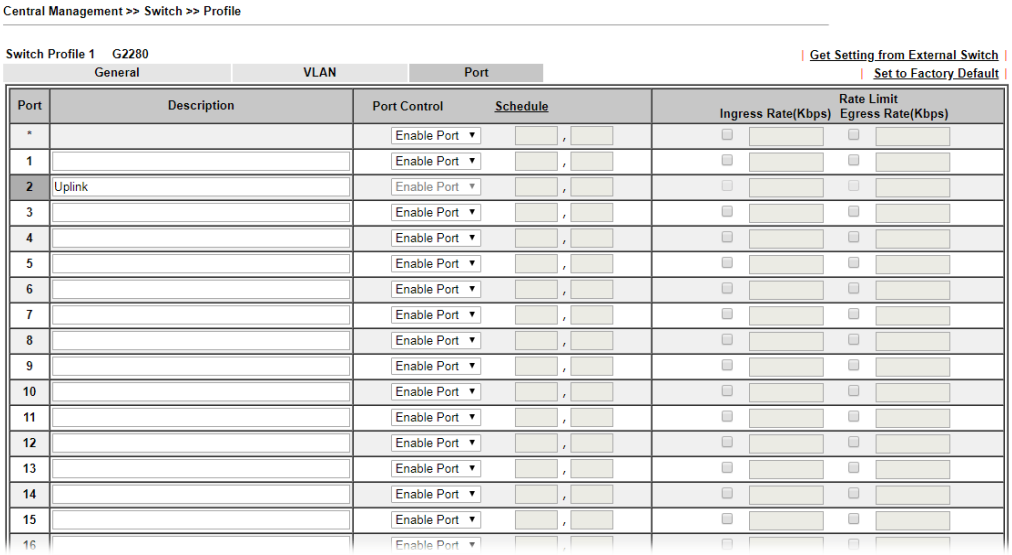
Página en blanco debido a LAN>>VLAN no configurada previamente:



Página de configuración con**LAN>>VLAN**configurado previamente:



3. Haga clic en**Ahorrar**para guardar la configuración de VLAN. Luego, haga clic en**Puerto**pestaña para acceder a la siguiente página:

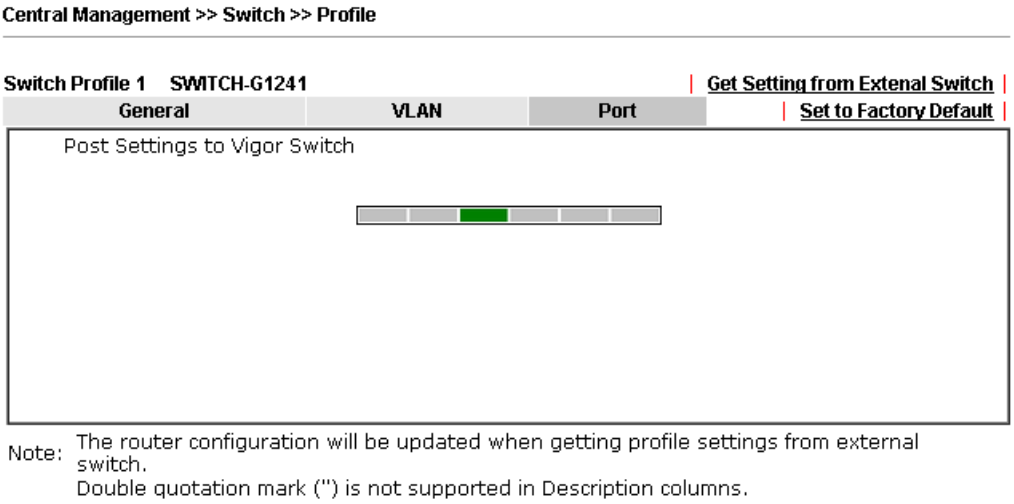


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Descripción	Si es necesario, escriba una breve descripción para explicar el dispositivo conectado a VigorSwitch a través del puerto LAN.
control portuario	**Deshabilitar puerto**–El puerto (p. ej., Puerto 2 en este caso) que se utiliza para conectar VigorSwitch y Vigor2927 no será cerrado por la serie Vigor2927. Otros puertos LAN de VigorSwitch permiten conectarse a cualquier dispositivo LAN. Cuando está marcado, después de hacer clic en Guardar, la conexión de red entre ese dispositivo y VigorSwitch se terminará.

	Cronograma–Aquí se pueden especificar dos perfiles de sechule para obligar a Vigor2927 a ejecutar una acción específica en VigorSwitch.
Límite de tarifa	Marque la casilla para escribir la tasa de entrada/tasa de salida para el VigorSwitch seleccionado. Después de hacer clic**Ahorrar**, el valor modificado en esta página se escribirá en VigorSwitch y se habilitará.

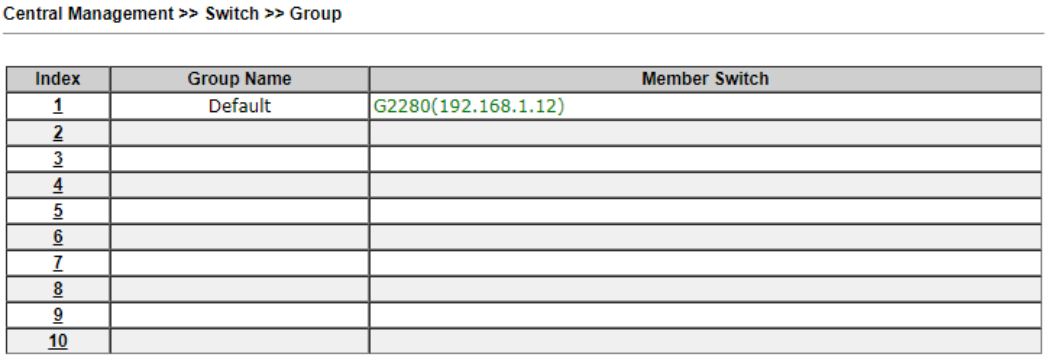
4. Haga clic en**Ahorrar**para guardar los cambios y luego haga clic en**Enviar a dispositivo**. Los ajustes se enviarán a VigorSwitch inmediatamente.



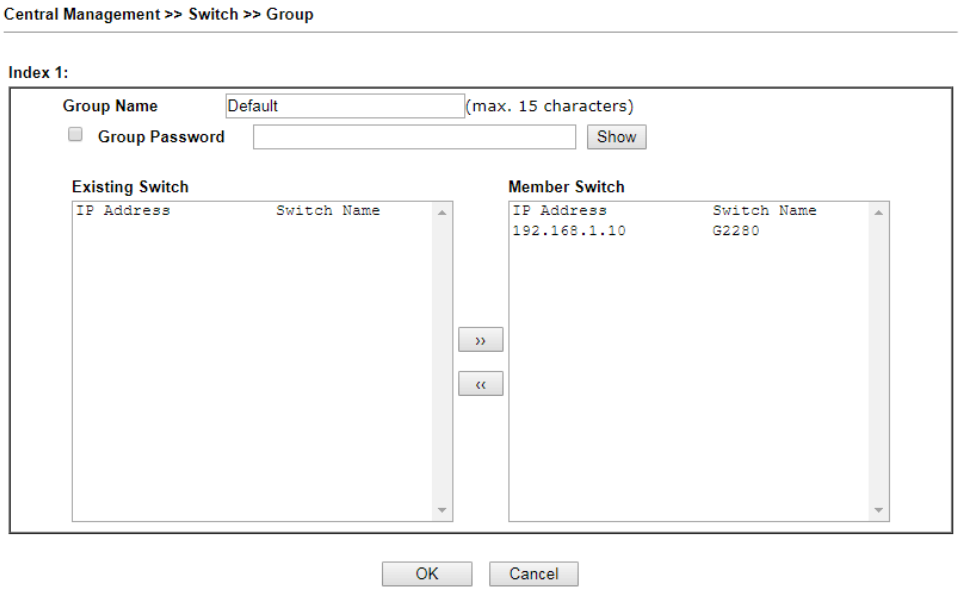
Grupo VII-7-3

Los diferentes interruptores se pueden clasificar en diferentes grupos. La contraseña específca para un grupo se puede definir y aplicar a cada conmutador de ese grupo.

A través de la configuración de contraseña común, no es necesario que el administrador del sistema recuerde varias contraseñas de inicio de sesión para acceder a diferentes dispositivos VigorSwitch.



Haga clic en cualquier enlace de número de índice para crear un nuevo grupo de interruptores.

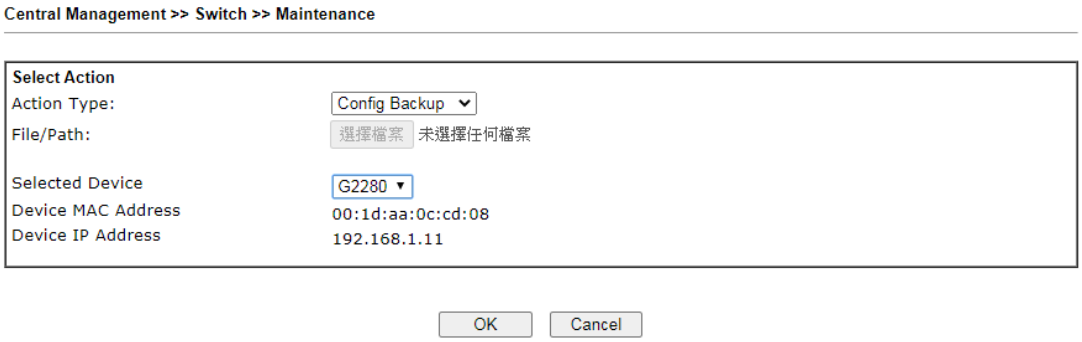


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre del grupo	Escriba un nombre como el nombre del grupo. Se pueden clasificar diferentes interruptores dentro de un grupo.
Contraseña de grupo	Escriba una contraseña que el administrador pueda usar para acceder al VigorSwitch administrado que se conecta a la serie Vigor2927. Se puede acceder a todos los interruptores del mismo grupo a través de dicha contraseña de grupo.
Interruptor existente	Muestre todos los dispositivos VigorSwitch que se conectan a Vigor2927.
Cambio de miembro	Elija los interruptores que desea agrupar y haga clic en el botón ">>" para mover los dispositivos seleccionados al campo de Member Switch. Los dispositivos bajo Cambio de miembro se agruparán bajo dicho perfil de grupo.
DE ACUERDO	Haga clic en él para guardar la configuración.
Cancelar	Haga clic en él para salir de la página de configuración sin guardar ningún cambio.

VII-7-4 Mantenimiento

Dicha función puede ejecutar la copia de seguridad de la configuración, la restauración de los dispositivos VigorSwitch seleccionados o reiniciar los dispositivos VigorSwitch de forma remota o restablecer los dispositivos VigorSwitch con la configuración predeterminada de fábrica, sin acceder a la interfaz de usuario web de VigorSwitch, respectivamente. Es conveniente que el administrador del sistema administre los dispositivos VigorSwitch.



Los ajustes disponibles se explican a continuación:

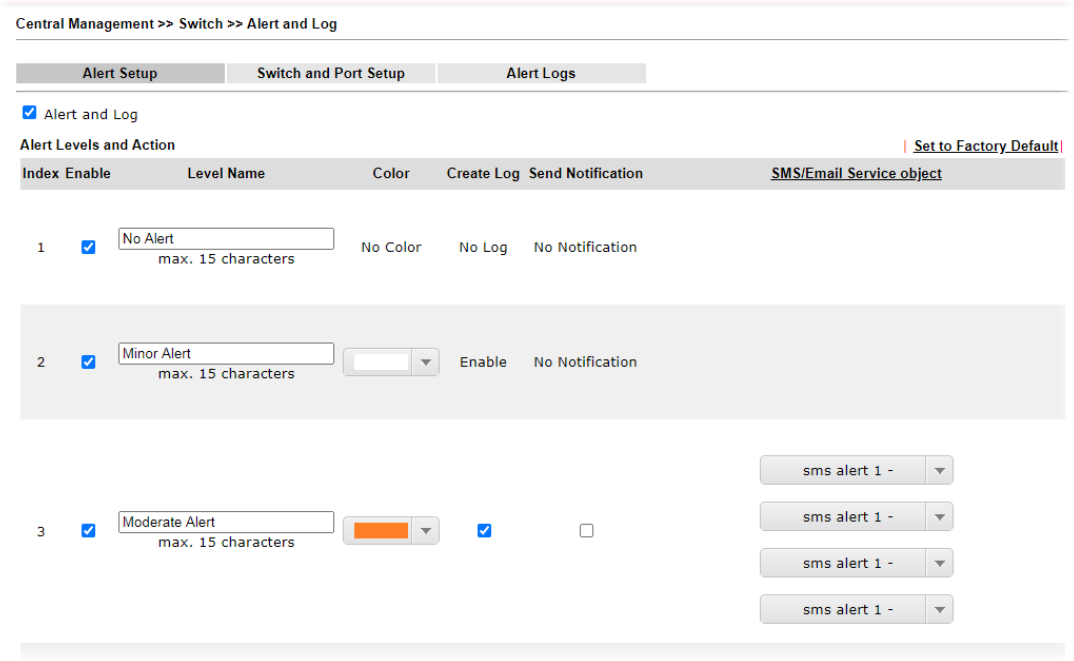
Artículo	Descripción
Seleccione la acción	**tipo de acción**–Vigor2927 ofrece cuatro acciones que incluyen copia de seguridad de configuración, restauración de configuración, reinicio remoto y restablecimiento de fábrica para realizar en VigorSwitch. **Ruta de archivo**–Haga clic en el botón para encontrar el archivo requerido.
Dispositivo seleccionado	Utilice la lista desplegable para especificar un VigorSwitch. Luego, la dirección MAC y la dirección IP relacionadas con el dispositivo se mostrarán en esta área.
DE ACUERDO	Haga clic en él para realizar inmediatamente la acción (copia de seguridad de configuración, restauración de configuración, reinicio remoto y restablecimiento de fábrica) en los dispositivos enumerados en Dispositivo seleccionado.
Cancelar	Haga clic en él para cancelar los cambios de configuración.

Alerta y registro VII-7-5

Alert and Log es útil para que el usuario comprenda rápidamente la situación anormal que ocurrió en VigorSwitch. Cuando el sistema detecta un error, la información de condición anormal se registrará en la base de datos; o el sistema enviará una alerta al dispositivo especificado (por correo electrónico o SMS) para advertir al usuario.

Configuración de alerta VII-7-5-1

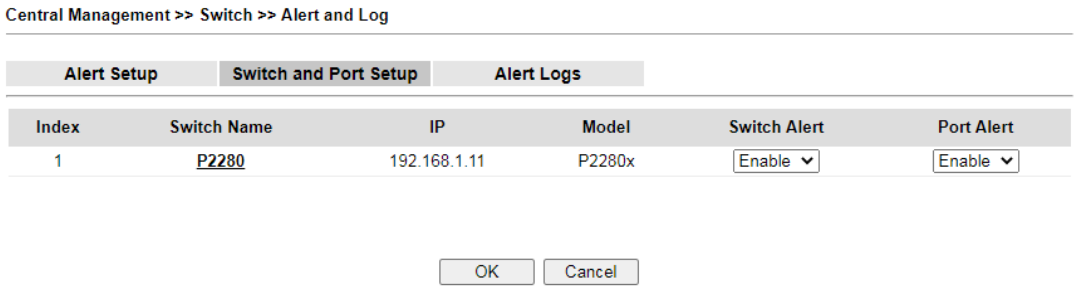
Esta página se utiliza para definir el nombre de la alerta, el nivel de alerta (en color) y determinar si registrar los datos en la base de datos o enviar un mensaje de notificación al usuario según el nivel.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Alerta y Registro	Márquelo para habilitar esta función.
Niveles de alerta y acción	**Nombre del nivel:**Defina nombres para representar la gravedad del evento de alerta. Los nombres predeterminados para el índice 1 al índice 4 se mostrarán en cada cuadro de configuración. Los índices 5 a 8 están reservados para los definidos por el usuario. **Color**–Defina el color para cada nivel de alerta. Sin embargo, el color del índice 1 es Sin color y no se puede cambiar. **Crear registro**–Marque la casilla para crear un registro de alerta. Dicho registro se verá en la página Registros de alertas. Tenga en cuenta que No Log para el índice 1; y el registro para el índice 2 está habilitado de forma predeterminada. **Enviar notificación**–Si está marcada, el sistema del enrutador Vigor enviará una notificación al número de teléfono especificado a través de SMS. **Objeto de servicio de SMS/correo electrónico:**Elija el objeto SMS que recibirá el SMS del enrutador Vigor. Se pueden seleccionar hasta 4 objetos a la vez.

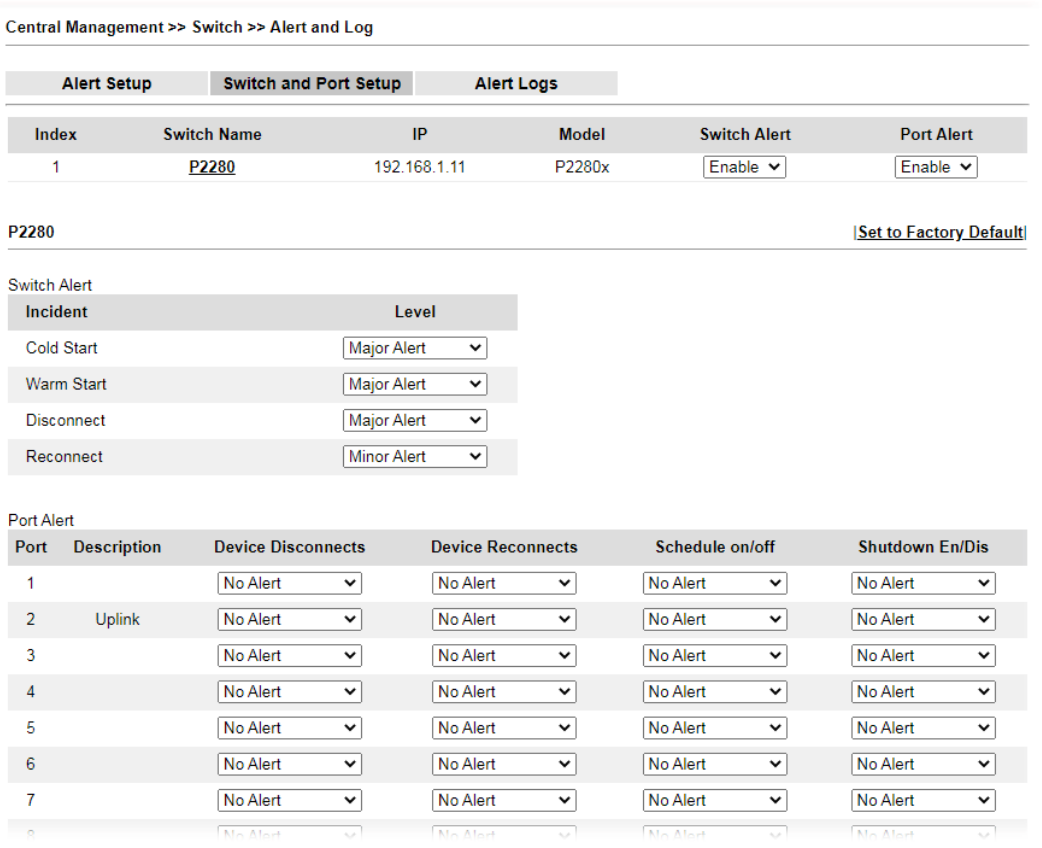
Esta página define la habilitación de la alerta de conmutador y/o alerta de puerto para cada conmutador.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Cambiar alerta	**Permitir -**Márquelo para habilitar el mecanismo de alerta para VigorSwitch.
Alerta de puerto	**Permitir -**Márquelo para habilitar el mecanismo de alerta para cada puerto de VigorSwitch.

Haga clic en el enlace Cambiar nombre (p. ej., P2280 en este caso) para obtener configuraciones detalladas.



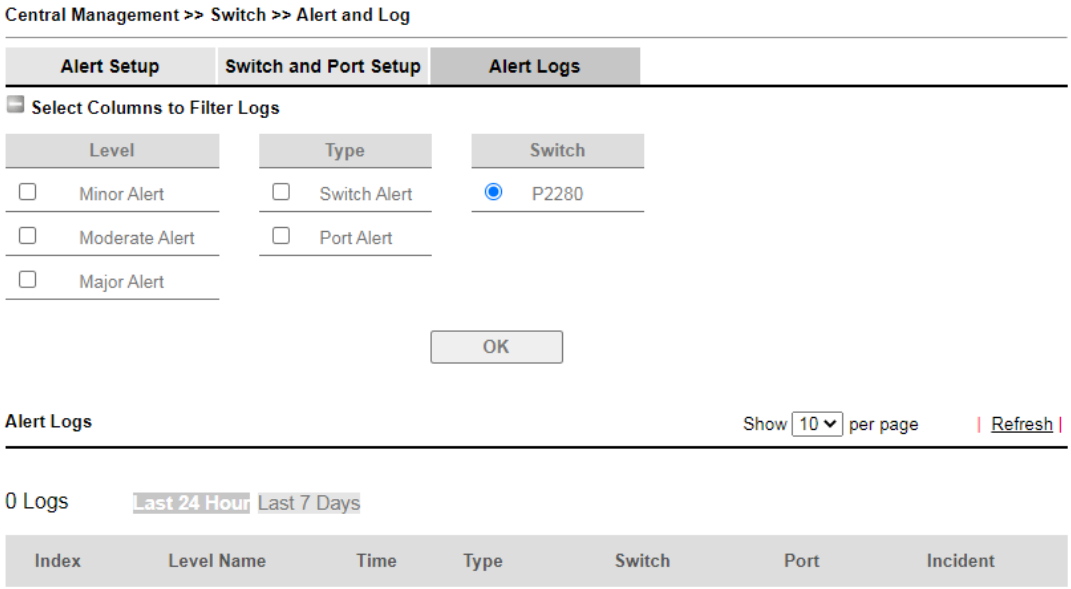
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Cambiar alerta	Cuando VigorSwitch encuentra los siguientes eventos de alerta, el mecanismo de alerta realizará las acciones correspondientes según el nivel de servicio del incidente encontrado. **Incidente -**Actualmente,**Arranque en frío, arranque en caliente, desconexión y reconexión**serán tratados como eventos de alerta. **Nivel -**Especifique el nivel de gravedad de cada incidente. A

	definido más nivel de gravedad para elegir en esta página, simplemente abra **Gestión central>>Switch>>Alerta y registro**y haga clic**Configuración de alertas**.
Alerta de puerto	**Puerto -**Los puertos Ethernet disponibles para el VigorSwitch seleccionado (p. ej., G2280 en este caso) se mostrarán en esta página. Cada puerto se puede configurar con un nivel de alerta diferente para diferentes eventos de alerta.

VII-7-5-3 Registros de alertas

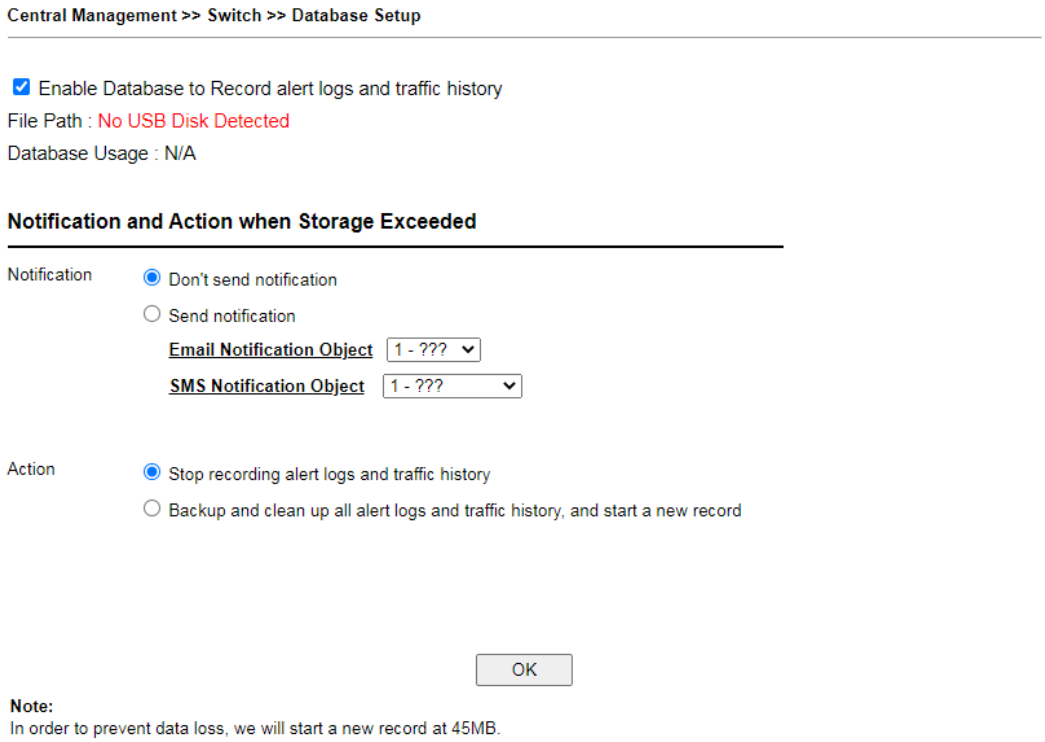
El usuario puede obtener la información filtrando la información colectiva en base a las condiciones especificadas en esta página.



Los ajustes disponibles se explican a continuación:

Artículo	**Descripción**
Seleccionar columnas para filtrar registros	**Nivel -**La alerta se puede dividir en varios niveles, Alerta Menor, Alerta Moderada y Alerta Mayor. Marque los que desea verificar en la lista de registros de alertas. **Tipo -**Compruebe el tipo (conmutador/puerto) del registro que se mostrará en la lista Registros de alerta. **Cambiar -**Los interruptores que se conectan al enrutador Vigor se mostrarán en esta área. Haz clic en el que necesites. **DE ACUERDO -**Haga clic en él para guardar la configuración. El registro relacionado con los elementos seleccionados anteriormente se mostrará en la lista de registros de alerta.
Registros de alertas	Esta área muestra registros (nombre de nivel, hora, tipo, conmutador, puerto e incidente) relacionados con VigorSwitch administrado por el enrutador Vigor.

La base de datos del conmutador se puede utilizar para registrar registros de alertas e historial de tráfico. Esta página se utiliza para determinar si es necesario que la información del usuario se registre en la base de datos del conmutador.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar la base de datos para registrar registros de alertas y tráfico historia	Marque la casilla para que la base de datos (en el disco USB) registre los registros de alerta y el historial de tráfico.
Notificación y acción cuando se excede el almacenamiento	
Notificación	**No enviar notificación**–No se enviará ninguna notificación cuando no haya capacidad de almacenamiento en USB. **Enviar notificación**–Se enviará una notificación cuando no haya capacidad de almacenamiento en USB.
Acción	**Dejar de grabar registros de alertas e historial de tráfico**–Cuando la capacidad del registro esté llena, el sistema dejará de grabar. **Haga una copia de seguridad y limpie todos los registros de alertas y el historial de tráfico, y comience un nuevo registro**-El sistema solo registrará los eventos más recientes.

Después de terminar la configuración, haga clic en**DE ACUERDO**para guardar la configuración.

Lista de soporte VII-7-7

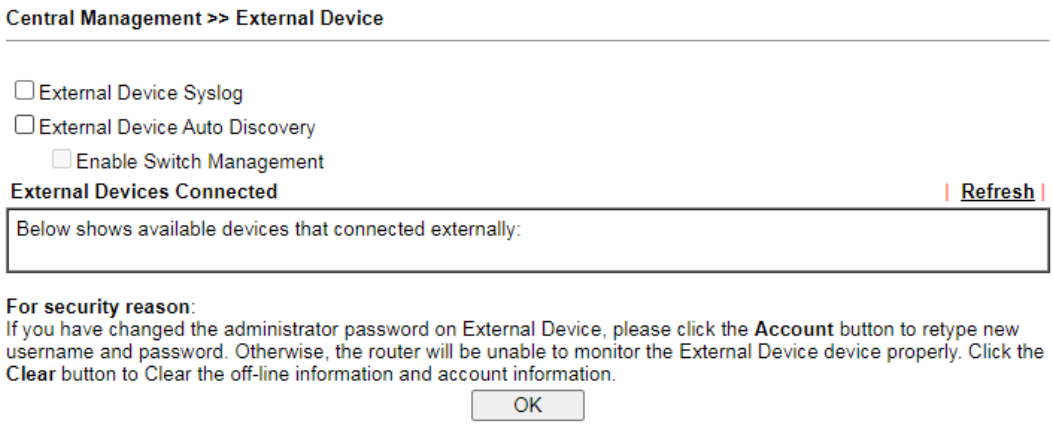
Esta página enumera todos los modelos de VigorSwitch que pueden ser administrados por Vigor2927 a través de**Gestión central>>Cambiar**.

Central Management >> Switch >> Support List

Model	Status	Firmware Version
Vigor Switch P2261	V	v3.48
Vigor Switch G2260	V	v3.48
Vigor Switch P1280	V	2.2.1
Vigor Switch G1280	V	2.2.1
Vigor Switch P2280	V	2.2.1
Vigor Switch G2280	V	2.2.1
Vigor Switch P2121	V	2.3.2
Vigor Switch G2121	V	2.4.3
Vigor Switch P1092	V	1.04.05
Vigor Switch G1080	V	1.04.05
Vigor Switch P2500	V	2.4.1
Vigor Switch G2500	V	2.4.1
Vigor Switch P2280x	V	2.4.2
Vigor Switch G2280x	V	2.4.2
Vigor Switch P1085	V	2.4.3
Vigor Switch G1085	V	2.4.3
Vigor Switch P2540x	V	2.6.0
Vigor Switch P2540xh	V	2.6.0
Vigor Switch G2540x	V	2.6.0
Vigor Switch P2100	V	2.6.4
Vigor Switch G2100	V	2.6.4
Vigor Switch PQ2200xb	V	2.6.9
Vigor Switch Q2200x	V	2.6.9
Vigor Switch FX2120	V	2.6.9
Vigor Switch P1282	V	2.6.9
Vigor Switch G1282	V	2.6.9

Gestión central VII-8 (dispositivos externos)

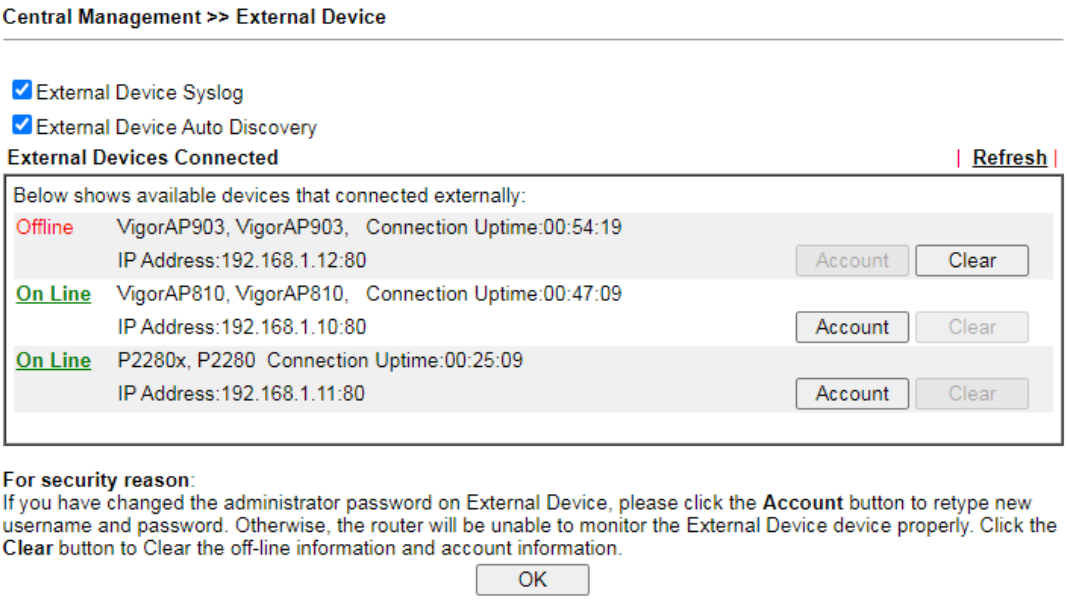
El enrutador Vigor se puede usar para conectarse con muchos tipos de dispositivos externos. Para controlar o administrar los dispositivos externos convenientemente, abra**Dispositivos externos**para hacer una configuración detallada.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Syslog del dispositivo externo	Marque esta casilla para mostrar información del dispositivo detectado en Syslog.
Dispositivo externo automático Descubrimiento	Marque esta casilla para detectar el dispositivo externo automáticamente y mostrarlo en esta página.

Desde esta página web, marque la casilla de**Detección automática de dispositivos externos**y haga clic**DE ACUERDO**. Más tarde, todos los dispositivos disponibles se mostrarán en esta página con iconos y la información correspondiente. Puede cambiar el nombre del dispositivo si es necesario o eliminar la información del dispositivo fuera de línea cuando lo desee.



Cuando haya terminado la configuración, haga clic en**DE ACUERDO**para salvarlo

Información

Esta función solo puede detectar productos DrayTek.

Título VIII Otros

Objects Settings

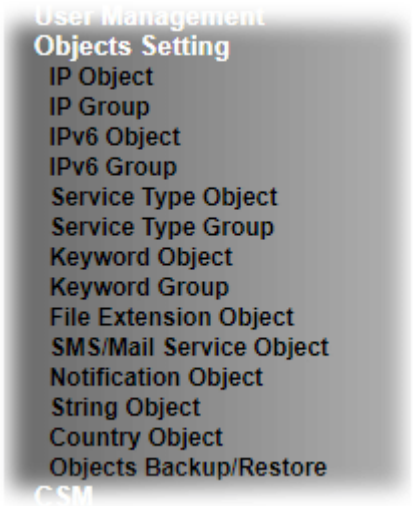
Defina objetos como dirección IP, tipo de servicio, palabra clave, extensión de archivo y otros. Estos objetos predefinidos se pueden aplicar en CSM.

USB

El dispositivo USB conectado al enrutador Vigor puede considerarse como un servidor o una interfaz WAN. A través del enrutador Vigor, los clientes en LAN pueden acceder, escribir y leer datos almacenados en el disco de almacenamiento USB con diferentes aplicaciones.

Configuración de objetos VIII-1

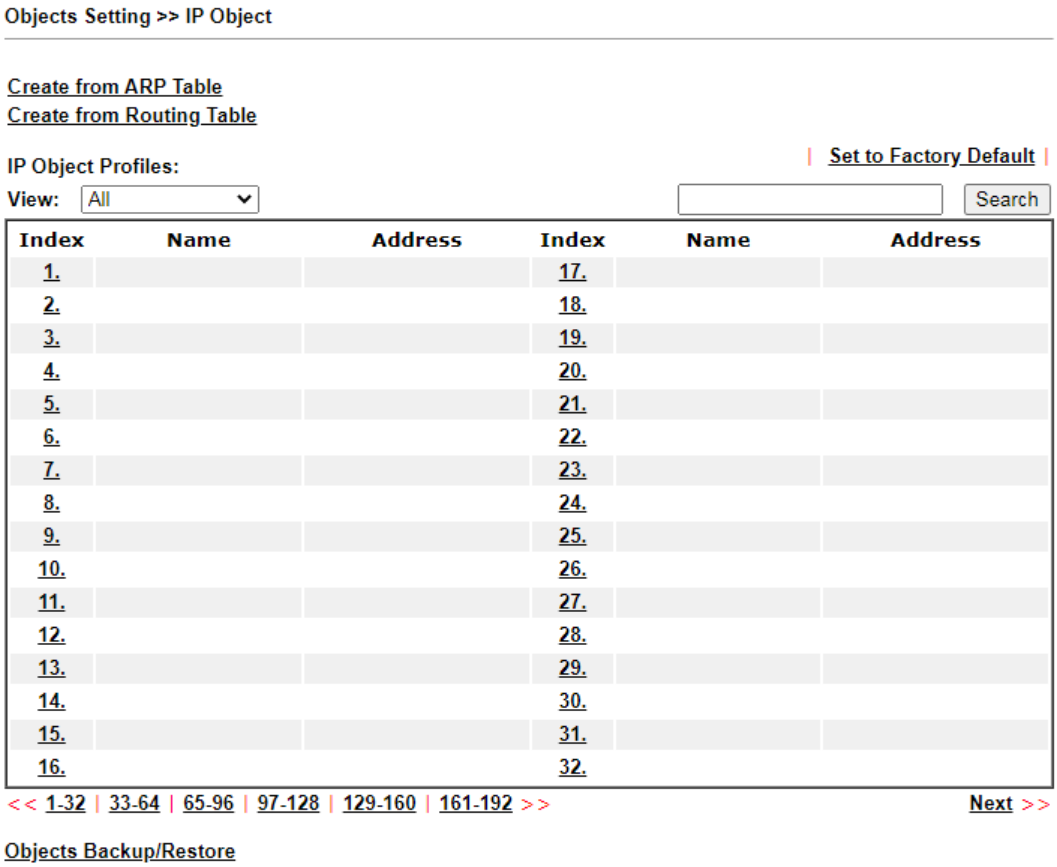
Esta sección permite la creación de objetos y grupos de objetos a partir de direcciones IP, tipos de servicio, palabras clave, extensiones de archivo, destinatarios de SMS y correo electrónico y tipos de notificación. Una vez configurados, estos objetos se pueden aplicar a las reglas de administración de contenido y firewall.



VIII-1-1 Objeto IP

Para las IP en un rango y los puertos de servicio en un rango limitado, generalmente se aplicarán al configurar los ajustes del enrutador, por lo tanto, podemos definirlos con ***objetos*** y atarlos con ***grupos*** para usar convenientemente. Posteriormente, podemos seleccionar ese objeto/grupo para aplicarlo. Por ejemplo, todas las IP de un mismo departamento se pueden definir con un objeto IP (un rango de direcciones IP).

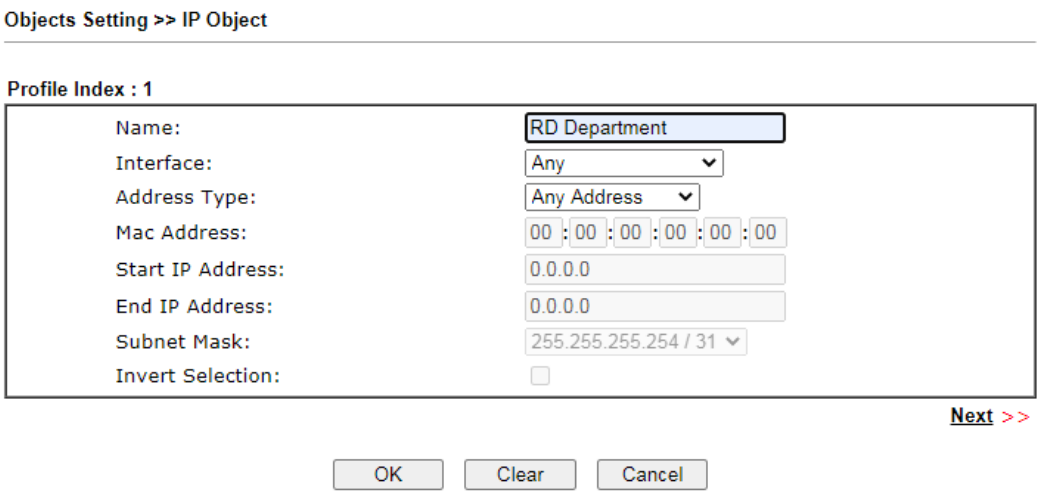
Se pueden crear hasta 192 Objetos IP.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Vista	Utilice la lista desplegable para elegir un tipo (Dirección única, Dirección de rango, Dirección de subred, Dirección Mac o todas) que el objeto IP con el tipo seleccionado se mostrará en esta página.
Establecer como predeterminado de fábrica	Borre todas las configuraciones de perfil.
Buscar	Escriba una cadena del objeto IP que desea buscar.
Índice	Número de perfil del objeto IP.
Nombre	Nombre del objeto.
DIRECCIÓN	Muestra la dirección IP configurada para el perfil de objeto.
Copia de seguridad/restauración de objetos	Haga clic en él para hacer una copia de seguridad o restaurar el objeto IP.

Para configurar un perfil, haga clic en el número de perfil en la columna Índice para abrir la página de configuración.

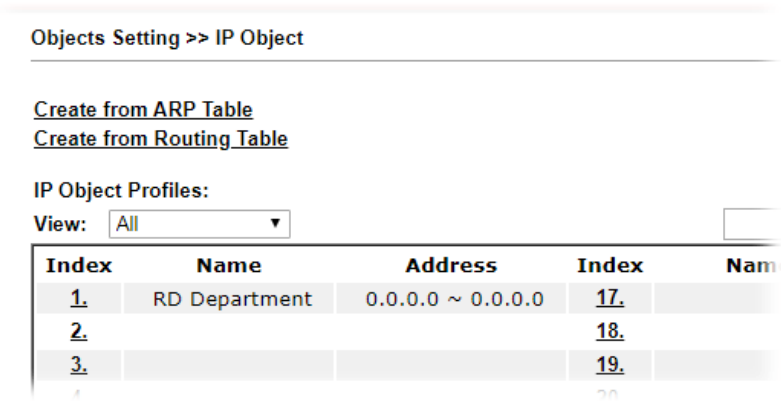


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre	Nombre que identifica a este perfil. La longitud máxima es de 15 caracteres.
Interfaz	La interfaz de red en la que se encuentran la dirección o direcciones IP. **Cualquier**–Todas las interfaces de red. **LAN/DMZ/RT/VPN**–Todas las interfaces de red excepto WAN. **PÁLIDO**–Solo interfaces WAN.
Tipo de dirección	Tipo de direcciones. **Cualquier dirección**–El objeto cubre todas las direcciones IP. **Dirección única**–El objeto cubre una dirección IP. **Dirección de rango**–El objeto cubre un rango de direcciones IP. **Dirección de subred**–El objeto cubre un rango de direcciones IP especificadas en notación de subred. **Dirección MAC**–El objeto contiene una dirección MAC.
Dirección MAC	Ingrese la dirección MAC del dispositivo de red, si el Tipo de dirección es Dirección Mac.

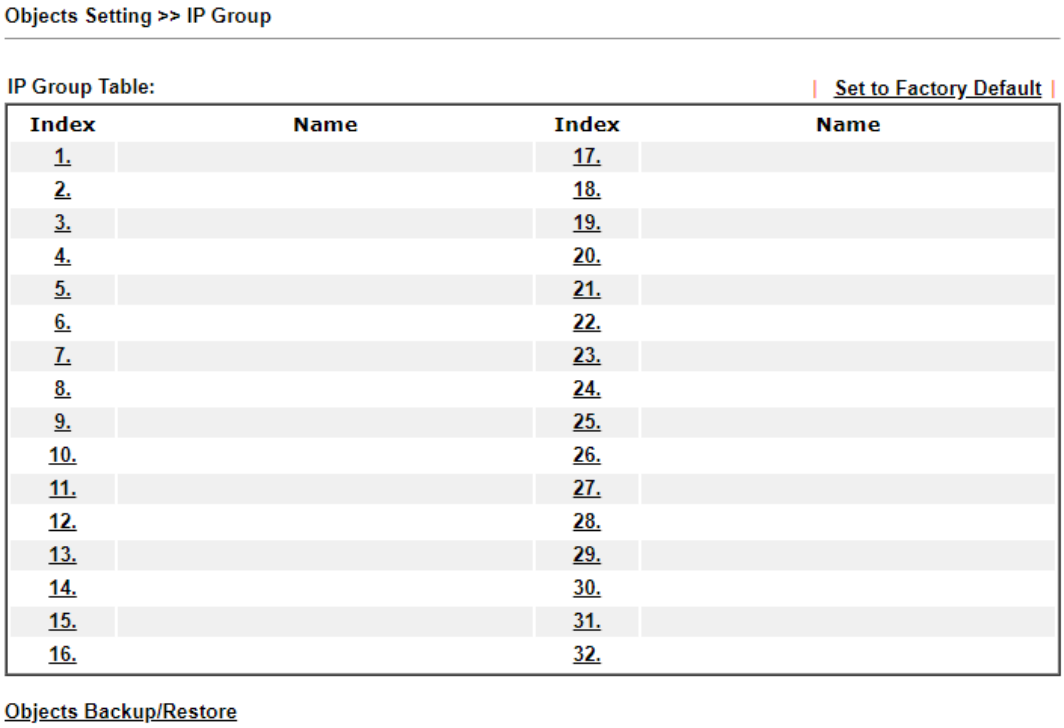
Dirección IP de inicio	Ingrese la dirección IP inicial, si el Tipo de dirección es una de Dirección única, Dirección de rango y Dirección de subred.
Dirección IP final	Ingrese la dirección IP final, si el tipo de dirección es una de dirección única, dirección de rango y dirección de subred.
Máscara de subred	Ingrese la máscara de subred, si el Tipo de dirección es Máscara de subred.
Invertir selección	Si se selecciona, se utilizarán todas las direcciones excepto las ingresadas anteriormente.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para borrar todas las configuraciones en el objeto IP actual, haga clic en**Claro**.



VIII-1-2 Grupo IP

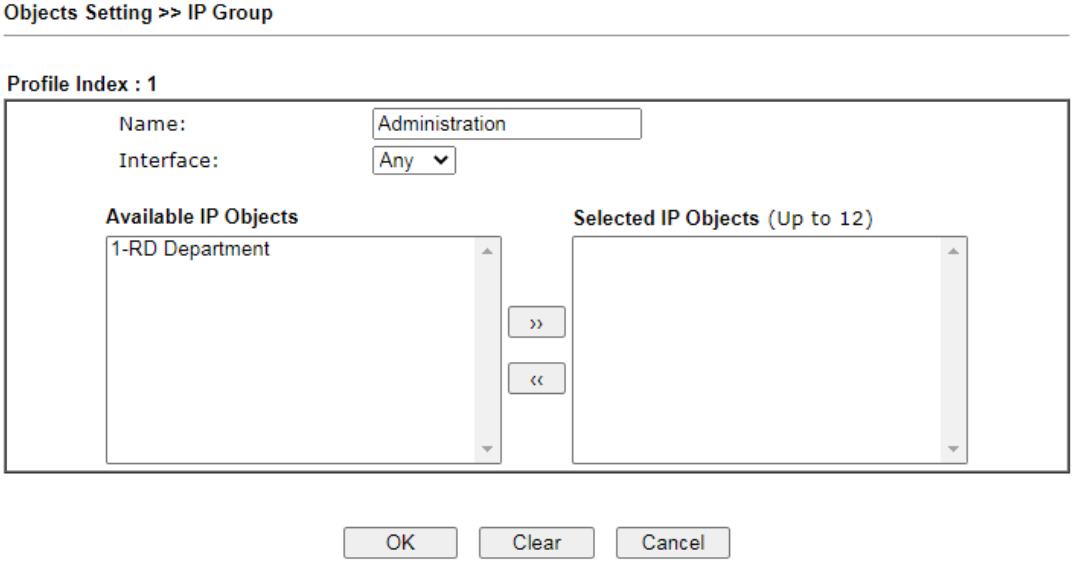
Se pueden colocar varios objetos de IP en un grupo de IP.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Establecer como predeterminado de fábrica	Borre todas las configuraciones de perfil.
Índice	Número de índice del perfil.
Nombre	Nombre que identifica al perfil.
Copia de seguridad/restauración de objetos	Haga clic en él para hacer una copia de seguridad o restaurar el objeto de grupo de IP.

Para configurar un perfil, haga clic en su índice para abrir la página de configuración.



Los ajustes disponibles se explican a continuación:

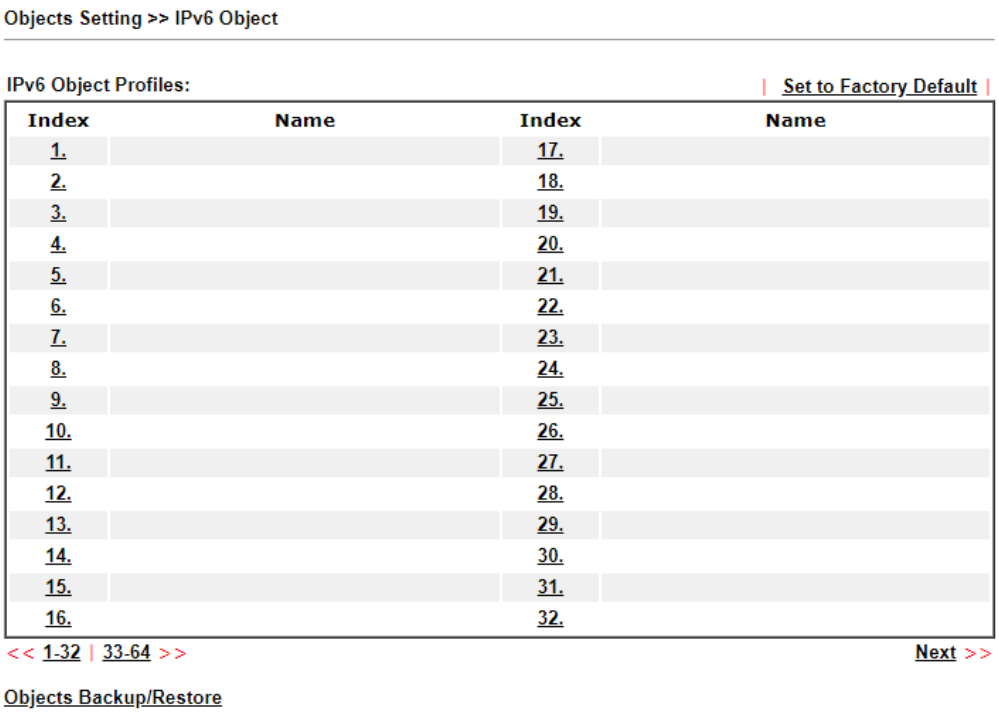
Artículo	Descripción
Nombre	Nombre que identifica a este perfil. La longitud máxima es de 15 caracteres.
Interfaz	Seleccione WAN, LAN o Cualquiera para filtrar objetos IP.
Objetos IP disponibles	Todos los objetos IP disponibles que están asociados con la interfaz seleccionada.
Objetos IP seleccionados	Objetos de IP que se han agregado a este perfil.

Para agregar un objeto de IP al grupo de IP, selecciónelo en Objetos de IP disponibles y, a continuación, haga clic en el botón **>>** botón. Para eliminar un objeto de IP del grupo de IP, selecciónelo en Objetos de IP seleccionados y, a continuación, haga clic en el botón**<<**botón.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para borrar todas las configuraciones en el grupo IP actual, haga clic en**Claro**.

VIII-1-3 Objeto IPv6

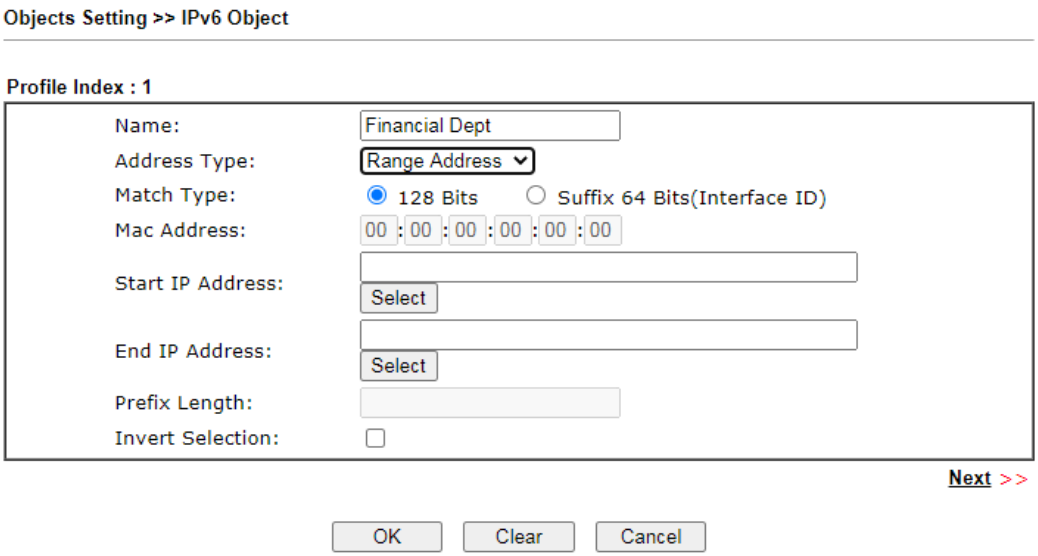
Se pueden crear hasta 64 objetos IPv6.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Establecer como predeterminado de fábrica	Borre todas las configuraciones de perfil.
Índice	Número de índice del perfil.
Nombre	Nombre que identifica al perfil.
Copia de seguridad/restauración de objetos	Haga clic en él para hacer una copia de seguridad o restaurar el objeto IPv6.

Para configurar un perfil, haga clic en el número de perfil en la columna Índice para abrir la página de configuración.



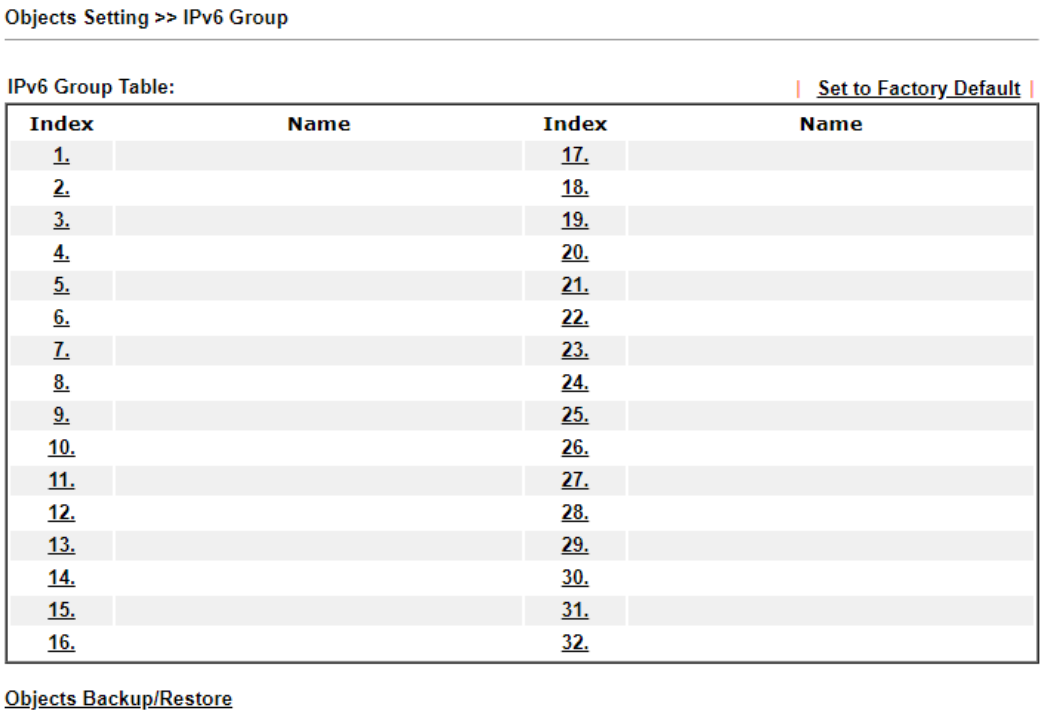
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre	Nombre que identifica a este perfil. La longitud máxima es de 15 caracteres.
Tipo de dirección	Tipo de direcciones. **Cualquier dirección**-El objeto cubre todas las direcciones IPv6. **Dirección única**-El objeto cubre una dirección IPv6. **Dirección de rango**-El objeto cubre un rango de direcciones IPv6. **Dirección de subred**-El objeto cubre un rango de direcciones IPv6 especificadas en notación de subred. **Dirección MAC**-El objeto contiene una dirección MAC.
Tipo de concordancia	Especifique el tipo de coincidencia (128 bits o sufijo de 64 bits) para la dirección IPv6.
Dirección MAC	Ingrese la dirección MAC del dispositivo de red, si el Tipo de dirección es Dirección Mac.
Dirección IP de inicio	Ingrese la dirección IP inicial, si el Tipo de dirección es una de Dirección única, Dirección de rango y Dirección de subred.
Dirección IP final	Ingrese la dirección IP final, si el tipo de dirección es una de dirección única, dirección de rango y dirección de subred.
Longitud del prefijo	Ingrese la longitud del prefijo IPv6, si el Tipo de dirección es Dirección de subred.
Invertir selección	Si se selecciona, se utilizarán todas las direcciones excepto las ingresadas anteriormente.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para borrar todas las configuraciones en el objeto IPv6, haga clic en**Claro**.

VIII-1-4 Grupo IPv6

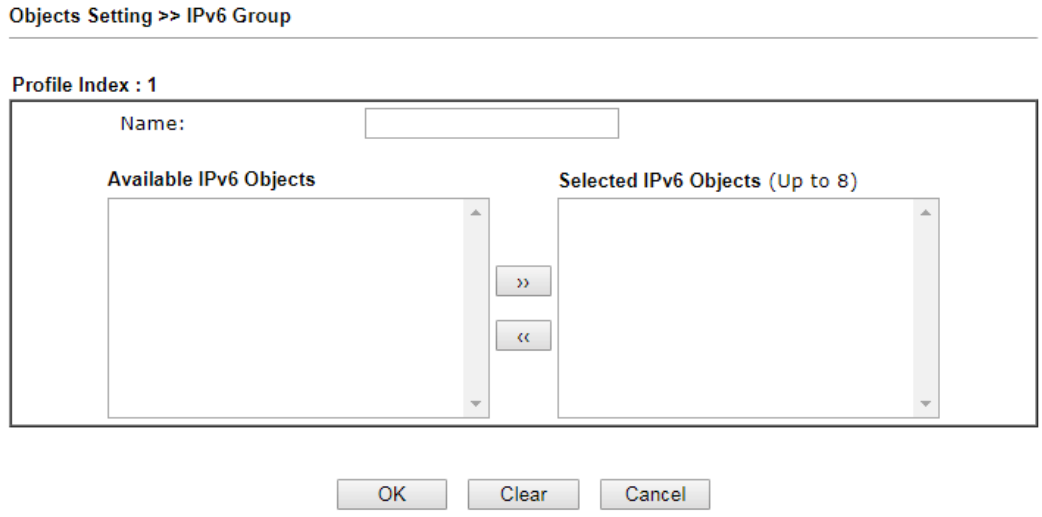
Múltiple**Objetos IPv6**se puede colocar en un**Grupo IPv6**.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Establecer como predeterminado de fábrica	Borre todas las configuraciones de perfil.
Índice	Número de índice del perfil.
Nombre	Nombre que identifica al perfil.
Copia de seguridad/restauración de objetos	Haga clic en él para hacer una copia de seguridad o restaurar el grupo IPv6.

Para configurar un perfil, haga clic en el número de perfil en la columna Índice para abrir la página de configuración.



Los ajustes disponibles se explican a continuación:

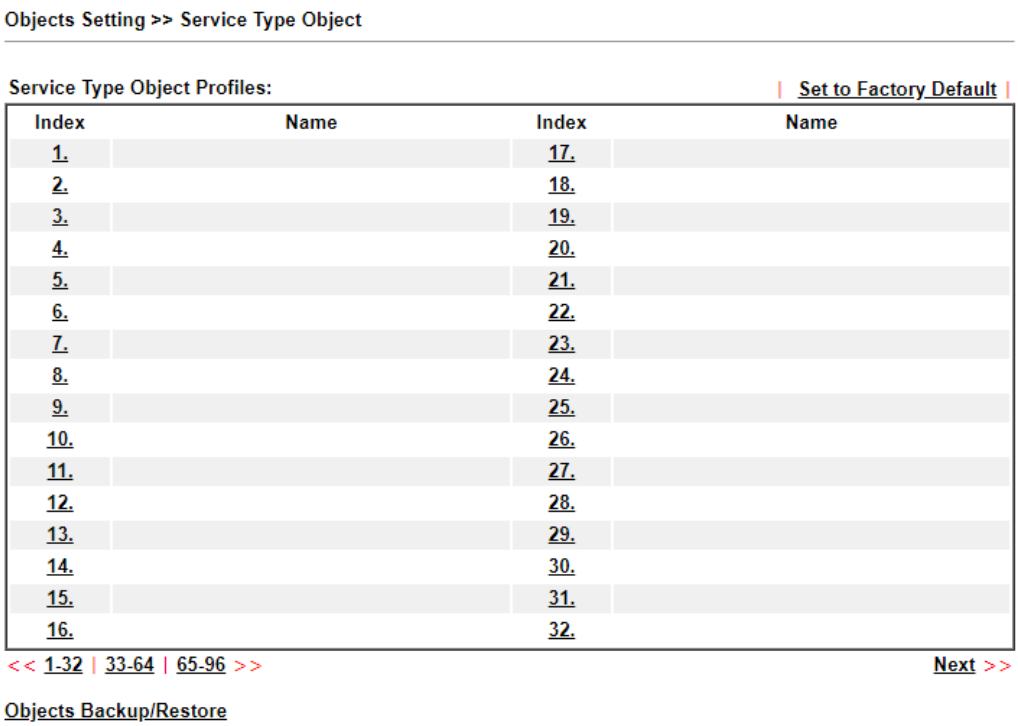
Artículo	Descripción
Nombre	Nombre que identifica a este perfil. La longitud máxima es de 15 caracteres.
Objetos IPv6 disponibles	Todos los objetos IP disponibles que están asociados con la interfaz seleccionada.
Objetos IPv6 seleccionados	Objetos IPv6 que se han agregado a este perfil.

Para agregar un objeto IPv6 al grupo IPv6, selecciónelo en Objetos IPv6 disponibles y luego haga clic en el botón > > botón. Para eliminar un objeto IPv6 del grupo IPv6, selecciónelo en Objetos IPv6 seleccionados y luego haga clic en el botón <<.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para borrar todas las configuraciones en el grupo IPv6 actual, haga clic en**Claro**.

VIII-1-5 Objeto de tipo de servicio

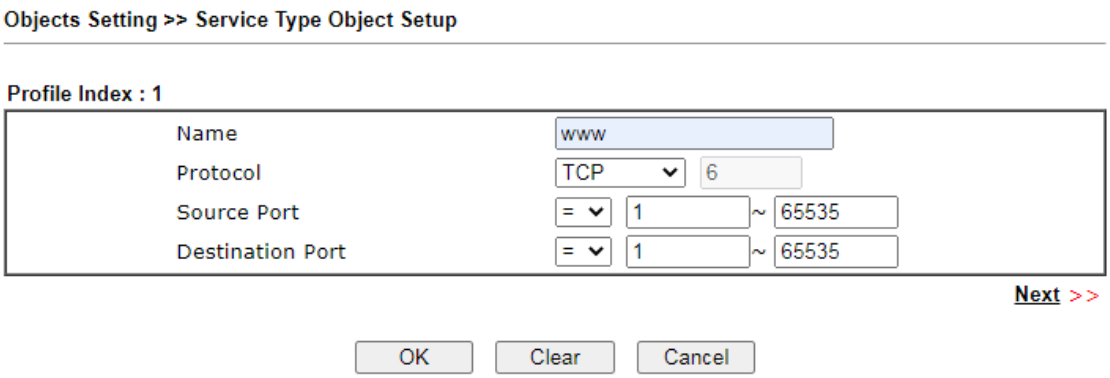
Se pueden crear hasta 96 objetos de tipo de servicio.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Establecer como predeterminado de fábrica	Borre todas las configuraciones de perfil.
Índice	Número de índice del perfil.
Nombre	Nombre que identifica al perfil.
Copia de seguridad/restauración de objetos	Haga clic en él para hacer una copia de seguridad o restaurar el objeto de tipo de servicio.

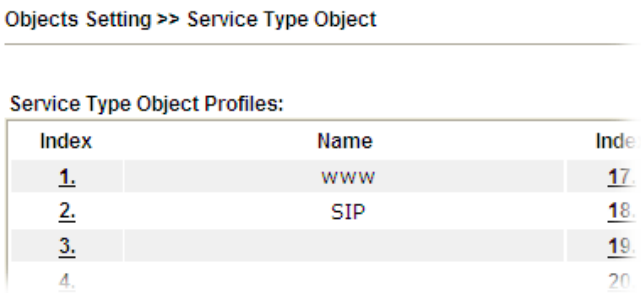
Para configurar un perfil, haga clic en el número de perfil en la columna Índice para abrir la página de configuración.



Los ajustes disponibles se explican a continuación:

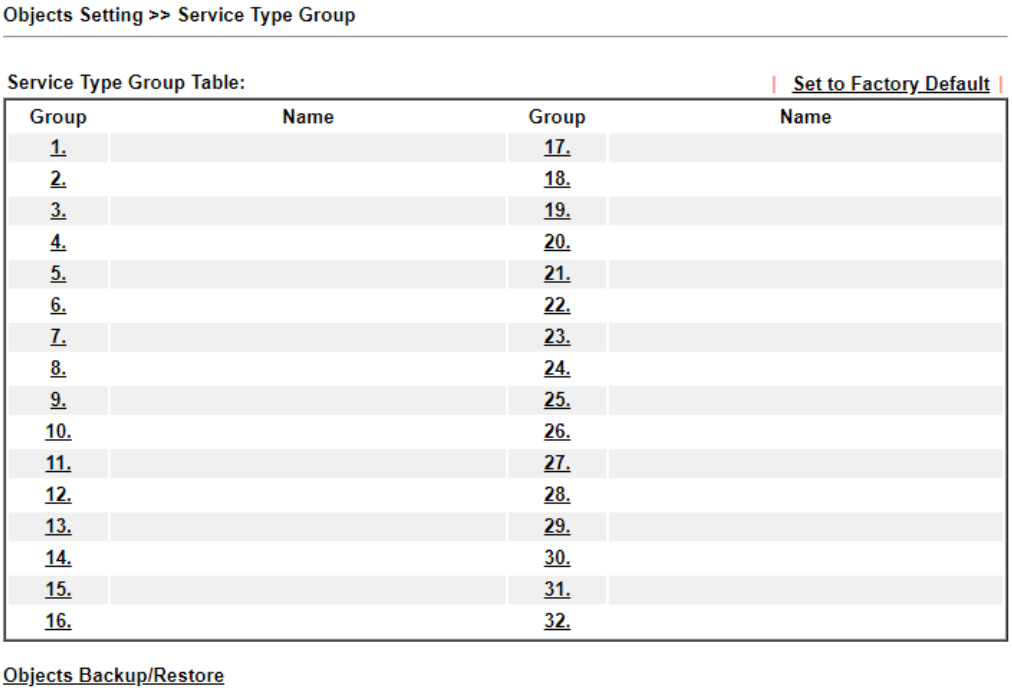
Artículo	Descripción
Nombre	Nombre que identifica a este perfil. La longitud máxima es de 15 caracteres.
Protocolo	Protocolo(s) a los que se aplica este perfil. **Cualquier**– Todos los protocolos. **ICMP**–Protocolo de mensajes de control de Internet **IGMP**–Protocolo de gestión de grupos de Internet **TCP**– Protocolo de Control de Transmisión **UDP**–Protocolo de datagramas de usuario **TCP/UDP**–Protocolo de control de transmisión y protocolo de datagramas de usuario **Otro**–Otros protocolos no enumerados anteriormente. Introduzca el número de protocolo en el cuadro de texto.
Puerto de origen/destino	Cuando el protocolo seleccionado incluye TCP o UDP, se pueden especificar los puertos de origen y destino. = – cualquier puerto que se encuentre dentro del rango especificado. !=: cualquier puerto que se encuentre fuera del rango especificado. – todos los números de puerto que son mayores que el valor especificado. <–todos los números de puerto que son más pequeños que el valor especificado.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para borrar todas las configuraciones en el objeto de tipo de servicio actual, haga clic en**Claro**.



VIII-1-6 Grupo de tipo de servicio

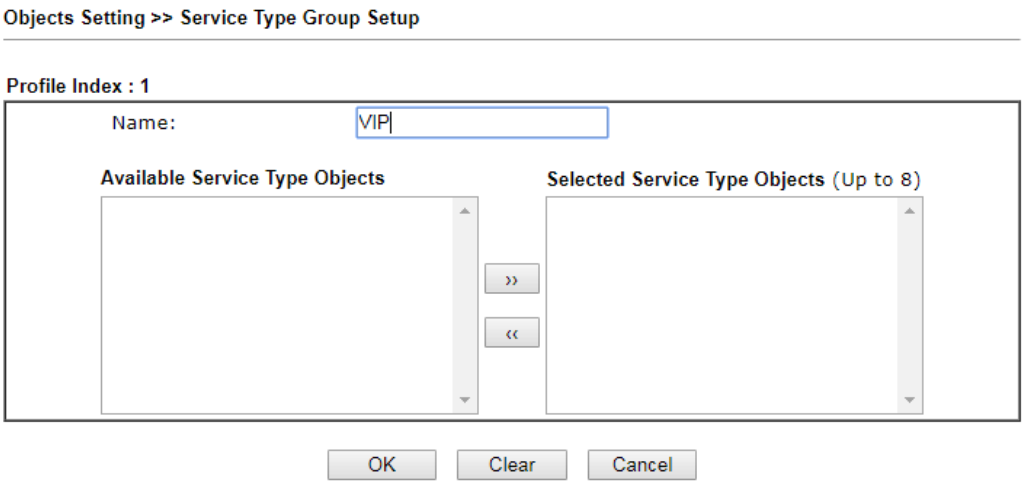
Múltiple**Objetos de tipo de servicio**se puede colocar en un**Grupo de tipo de servicio**.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Establecer como predeterminado de fábrica	Borre todas las configuraciones de perfil.
Índice	Número de índice del perfil.
Nombre	Nombre que identifica al perfil.
Copia de seguridad/restauración de objetos	Haga clic en él para hacer una copia de seguridad o restaurar el objeto de grupo de tipo de servicio.

Para configurar un perfil, haga clic en el número de perfil en la columna Índice para abrir la página de configuración.



Los ajustes disponibles se explican a continuación:

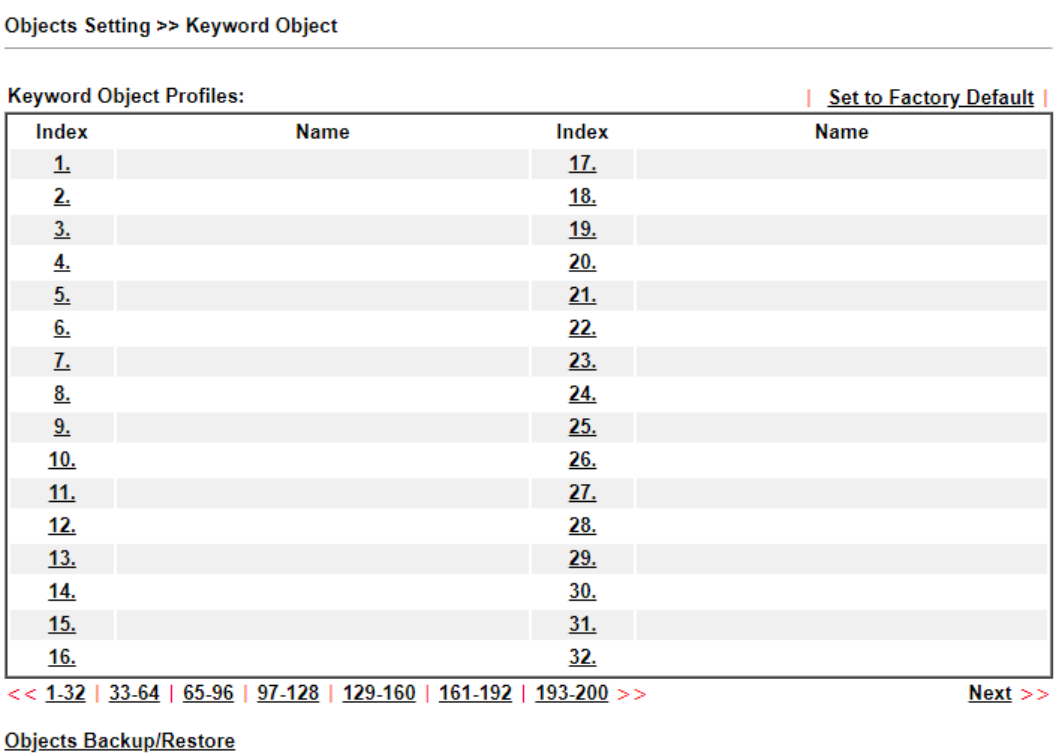
Artículo	Descripción
Nombre	Nombre que identifica a este perfil. La longitud máxima es de 15 caracteres.
Tipo de servicio disponible Objetos	Todos los objetos de tipo de servicio disponibles.
Tipo de servicio seleccionado Objetos	Objetos de tipo de servicio que se han agregado a este perfil.

Para agregar un objeto de tipo de servicio al grupo de tipo de servicio, selecciónelo en**Objetos de tipo de servicio disponibles**, luego haga clic en el**>>**botón. Para eliminar un objeto de tipo de servicio del grupo de tipo de servicio, selecciónelo en**Objetos de tipo de servicio seleccionados**, luego haga clic en el**<<**botón.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para borrar todas las configuraciones en el grupo de tipo de servicio actual, haga clic en**Claro**.

VIII-1-7 Objeto de palabra clave

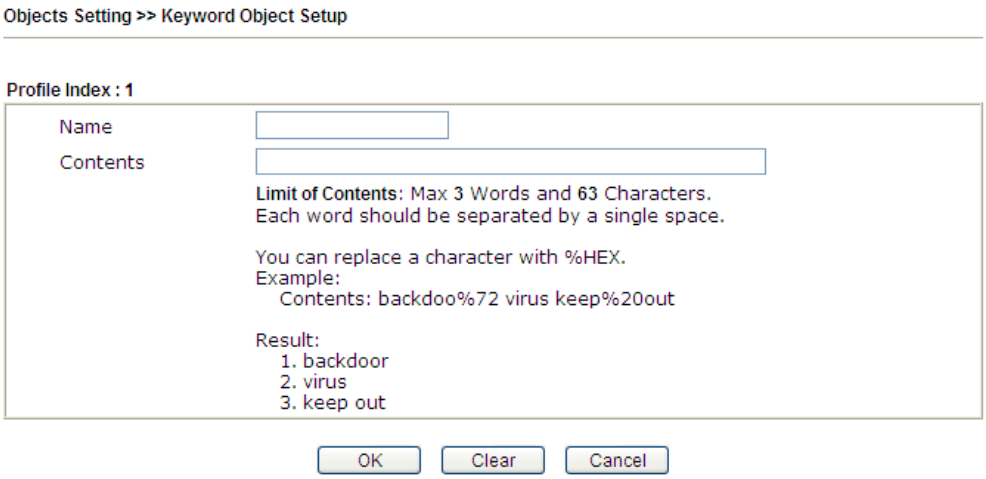
Se pueden crear 200 perfiles de objetos de palabras clave para usar como listas negras o listas blancas en**CSM >>Perfil de filtro de contenido de URL**y**Perfil de filtro de contenido web**.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Establecer como predeterminado de fábrica	Borre todas las configuraciones de perfil.
Índice	Número de índice del perfil.
Nombre	Nombre que identifica al perfil.
Copia de seguridad/restauración de objetos	Haga clic en él para hacer una copia de seguridad o restaurar el objeto de palabra clave.

Para configurar un perfil, haga clic en su índice para abrir la página de configuración.



Los ajustes disponibles se explican a continuación:

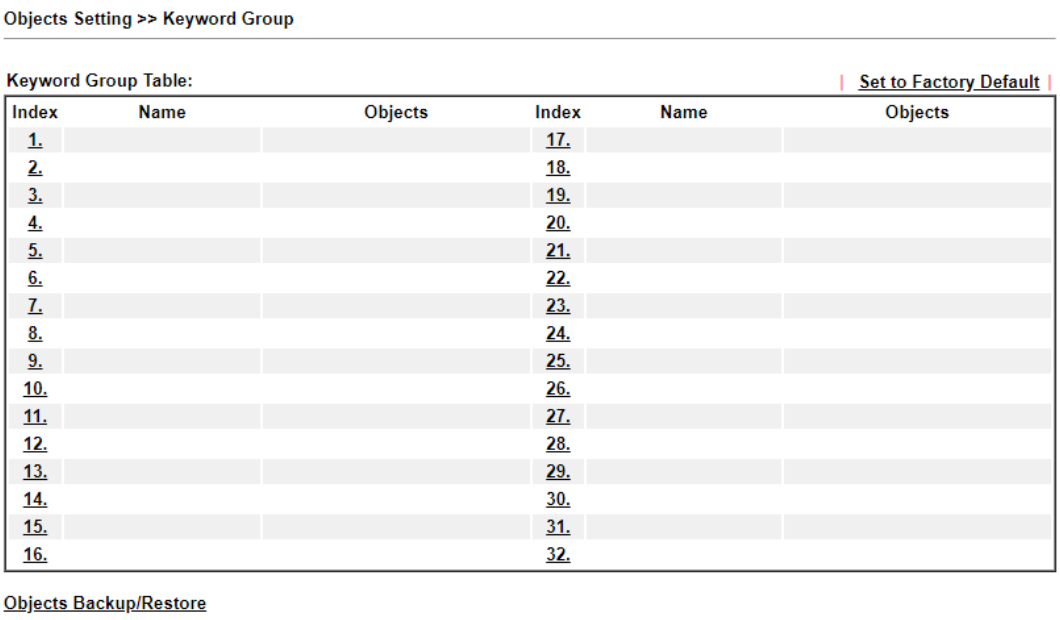
Artículo	Descripción
Nombre	Nombre que identifica a este perfil. La longitud máxima es de 15 caracteres.
Contenido	Palabras clave a combinar. Se pueden ingresar hasta 3 frases clave, separadas por espacios, para una longitud total de 63 caracteres. Para frases clave que contienen espacios, reemplace los espacios con la secuencia %20. Por ejemplo, la frase "mantener fuera" debe ingresarse como "mantener% 20 fuera".

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para borrar todas las configuraciones en el objeto de palabra clave actual, haga clic en**Claro**.

VIII-1-8 Grupo de palabras clave

Se pueden colocar varios objetos de palabras clave en un grupo de palabras clave.

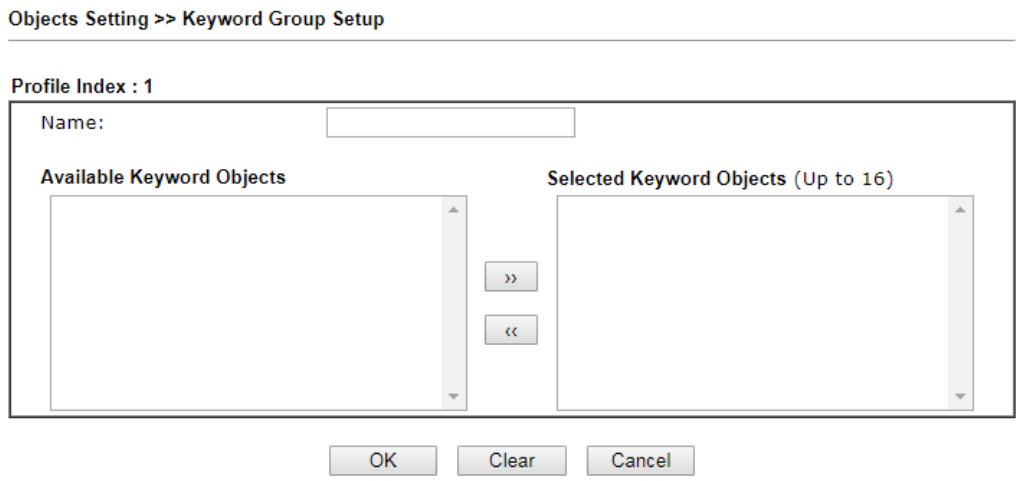
Los grupos de palabras clave se pueden elegir como listas negras o listas blancas en**CSM >>URL/perfil de filtro de contenido web**.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Establecer como predeterminado de fábrica	Borre todas las configuraciones de perfil.
Índice	Número de índice del perfil.
Nombre	Nombre que identifica al perfil.
Objetos	Muestre los objetos de palabra clave en este grupo.
Copia de seguridad/restauración de objetos	Haga clic en él para hacer una copia de seguridad o restaurar el grupo de palabras clave.

Para configurar un perfil, haga clic en su índice para abrir la página de configuración.



Los ajustes disponibles se explican a continuación:

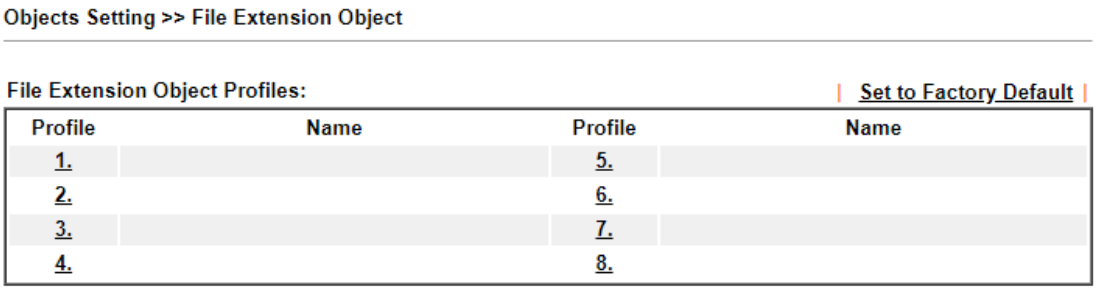
Artículo	Descripción
Nombre	Nombre que identifica a este perfil. La longitud máxima es de 15 caracteres.
Objetos de palabra clave disponibles	Todos los objetos de palabra clave que no se han agregado a este perfil.
Objetos de palabra clave seleccionados	Objetos de palabra clave que se han agregado a este perfil.

Para agregar un objeto de tipo de servicio al grupo de tipo de servicio, selecciónelo en**Objetos de tipo de servicio disponibles**, luego haga clic en el**>>**botón. Para eliminar un objeto de tipo de servicio del grupo de tipo de servicio, selecciónelo en**Objetos de tipo de servicio seleccionados**, luego haga clic en el**<<**botón.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para borrar todas las configuraciones en el grupo de palabras clave actual, haga clic en**Claro**.

Objeto de extensión de archivo VIII-1-9

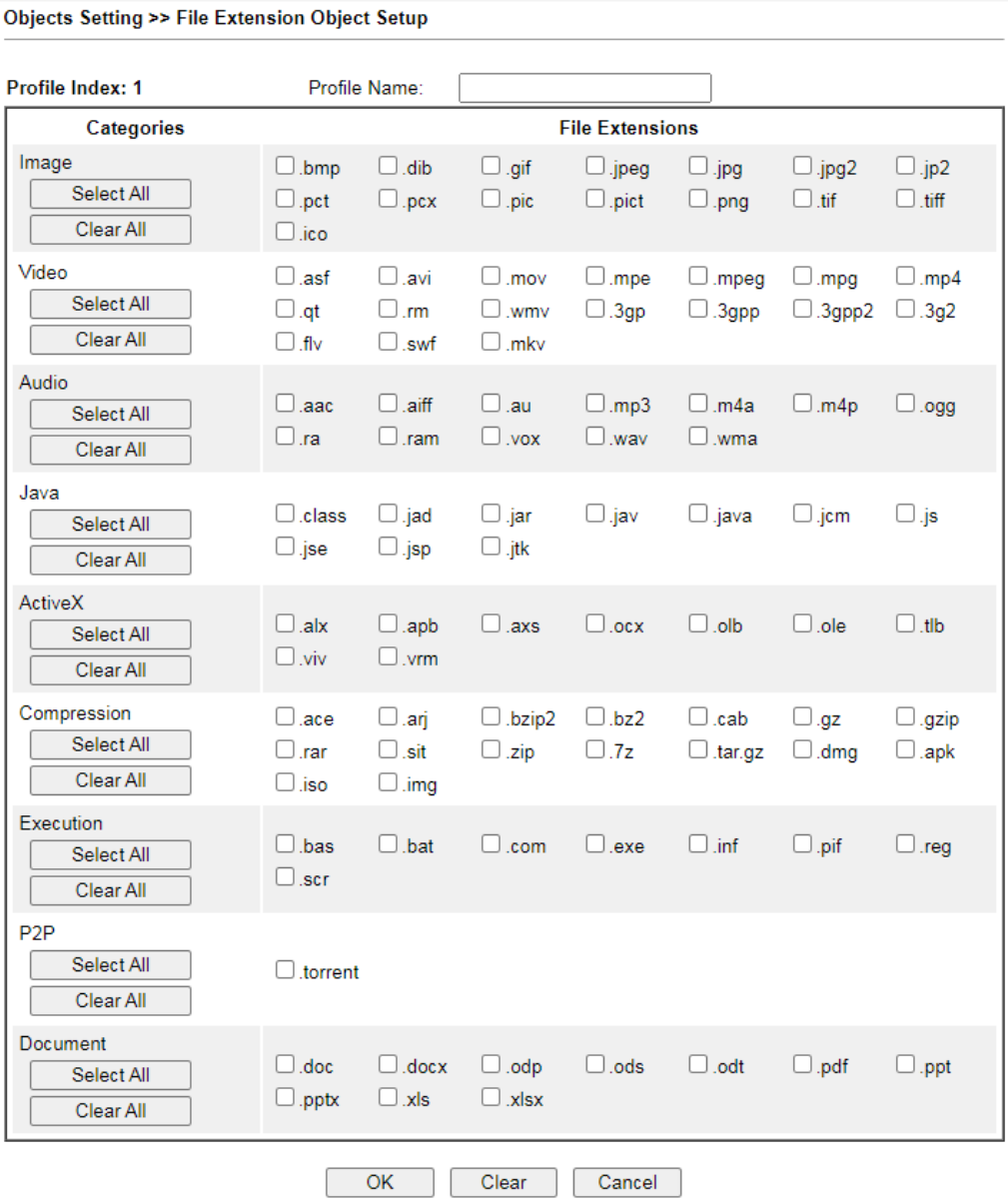
Se pueden configurar hasta 8 objetos de extensión de archivo para usar con**CSM>>Filtro de contenido de URL**.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Establecer como predeterminado de fábrica	Borre todas las configuraciones de perfil.
Índice	Número de índice del perfil.
Nombre	Nombre que identifica al perfil.
Copia de seguridad/restauración de objetos	Haga clic en él para hacer una copia de seguridad o restaurar el objeto de extensión de archivo.

Para configurar un perfil, haga clic en su índice para abrir la página de configuración.



Los ajustes disponibles se explican a continuación:

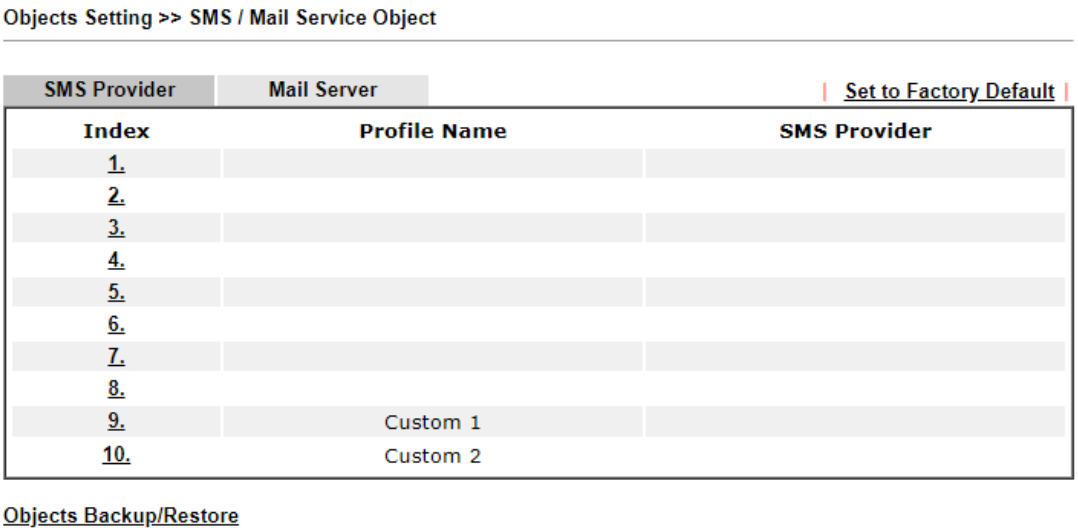
Artículo	Descripción
Nombre de perfil	Nombre que identifica a este perfil. La longitud máxima es de 7 caracteres.
Seleccionar todo	Selecciona todas las extensiones de archivo para la categoría.
Limpiar todo	Anula la selección de todas las extensiones de archivo para la categoría.

Seleccione las extensiones de archivo que desea incluir en el perfil. Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para borrar todas las configuraciones en el objeto de extensión de archivo actual, haga clic en**Claro**.

VIII-1-10 Objeto de servicio de SMS/correo

Objeto de servicio de SMS

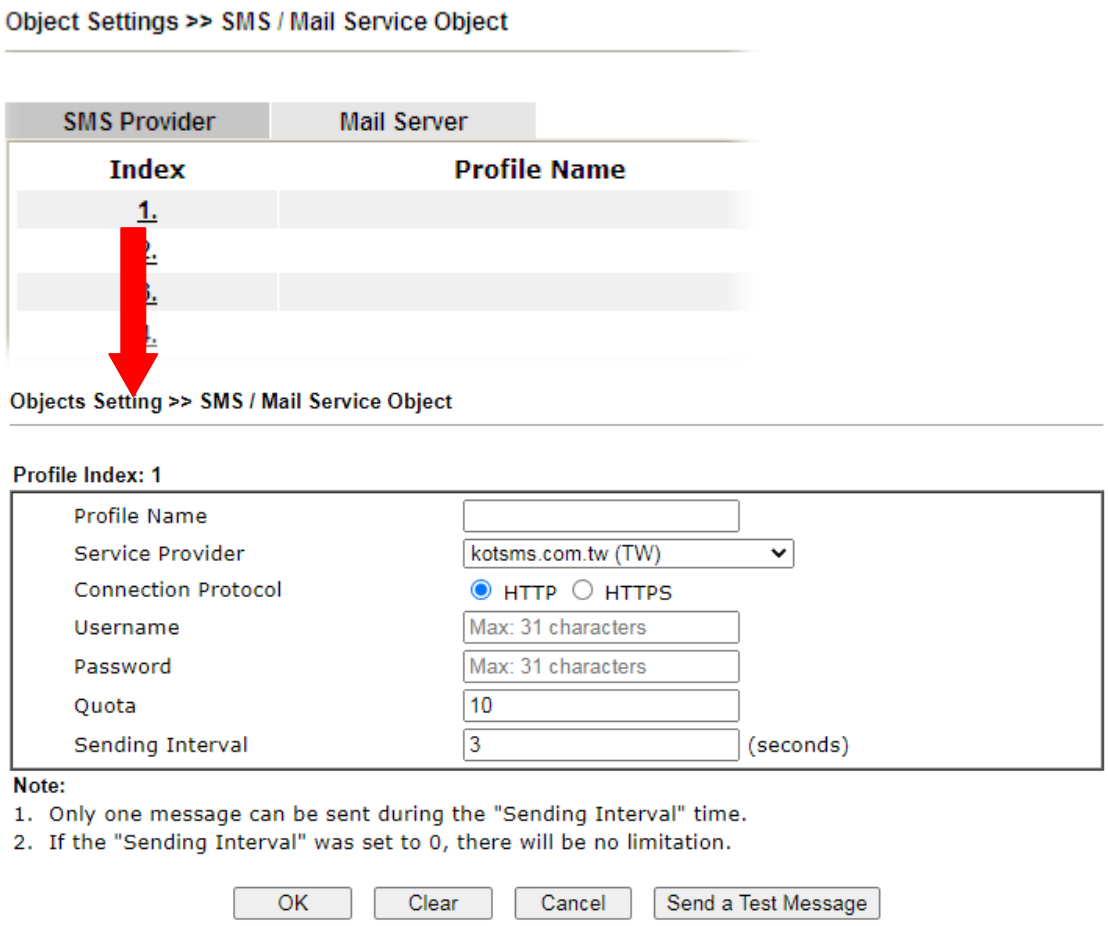
Se pueden configurar hasta 10 objetos de servicio SMS para usar con**Aplicación>>Servicio de Alerta SMS**.



Cada elemento se explica de la siguiente manera:

Artículo	Descripción
Establecer como predeterminado de fábrica	Borre todas las configuraciones de perfil.
Índice	Número de índice del perfil.
Nombre de perfil	Nombre que identifica al perfil.
Proveedor de SMS	El proveedor de SMS seleccionado para el perfil.
Copia de seguridad/restauración de objetos	Haga clic en él para hacer una copia de seguridad o restaurar el objeto de servicio.

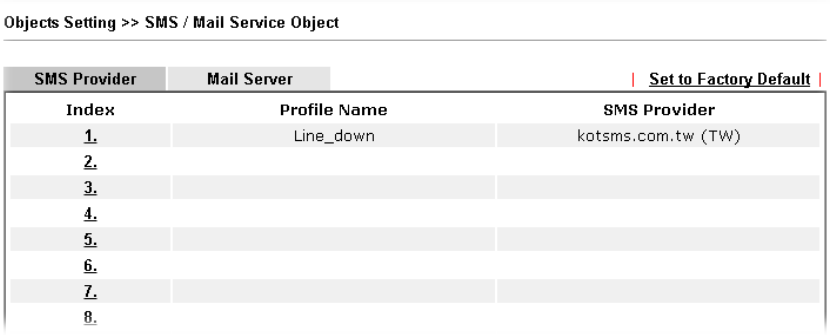
Para configurar un perfil, haga clic en el**Proveedor de SMS**y luego haga clic en su índice para que aparezca la página de configuración.



Los ajustes disponibles se explican a continuación:

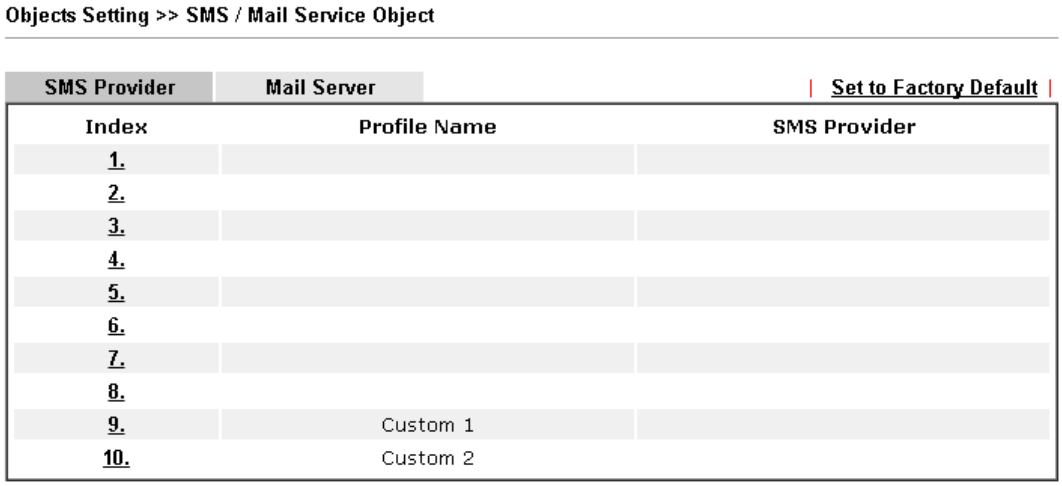
Artículo	Descripción
Nombre de perfil	Nombre que identifica a este perfil. La longitud máxima es de 31 caracteres.
Proveedor de servicio	Seleccione un proveedor de servicios de la lista desplegable.
Protocolo de conexión	Especifique HTTP o HTTPS.
Nombre de usuario	Nombre de usuario utilizado para iniciar sesión en el servicio. La longitud máxima es de 31 caracteres.
Contraseña	Contraseña utilizada para iniciar sesión en el servicio. La longitud máxima es de 31 caracteres.
Cuota	Número restante de mensajes de texto que se pueden enviar. El valor de la cuota se reduce en 1 cada vez que el enrutador envía un mensaje SMS. Cuando la cuota llegue a 0, no se enviará ningún SMS hasta que se restablezca a más de 0.
Intervalo de envío	Cantidad mínima de tiempo, en segundos, para esperar entre el envío de mensajes SMS.
Enviar un mensaje de prueba	Haga clic para enviar un correo electrónico de prueba de acuerdo con la configuración anterior.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para borrar todas las configuraciones en el objeto de servicio SMS, haga clic en**Claro**.

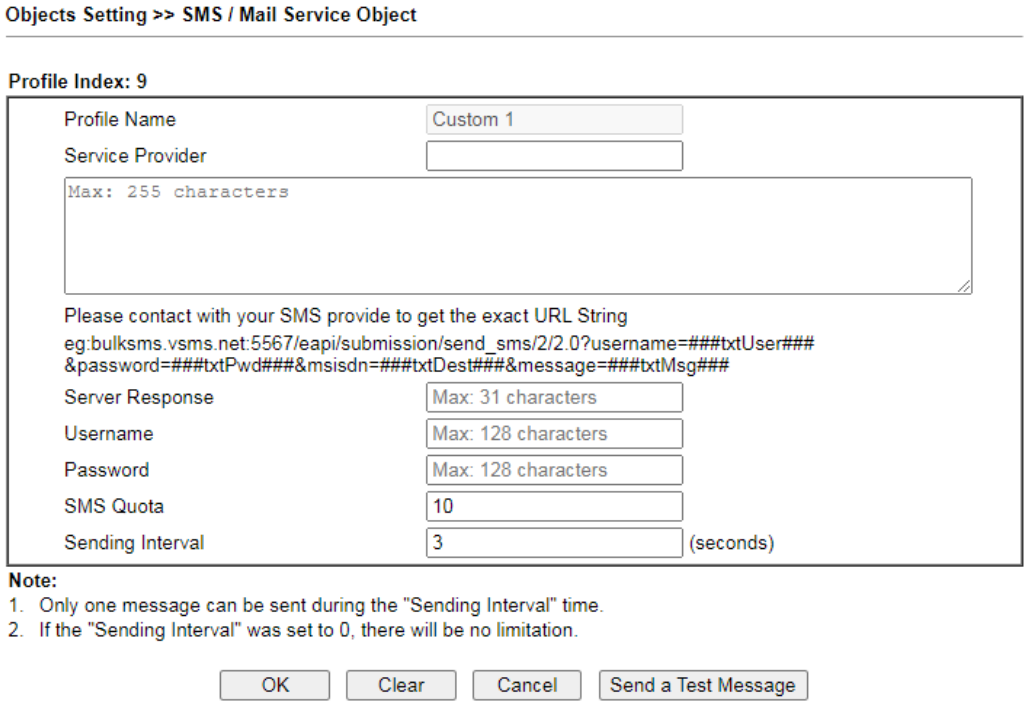


Servicio de SMS personalizado

El enrutador ofrece una extensa lista de proveedores de servicios de SMS predeterminados para su conveniencia. Sin embargo, si su proveedor de servicios no se encuentra entre la lista de proveedores de servicios admitidos, simplemente use los índices 9 y 10 para crear un perfil de servicio de SMS personalizado.



Para configurar un perfil personalizado, haga clic en la pestaña Proveedor de SMS y luego haga clic en uno de los 2 índices (9 y 10) para abrir la página de configuración.



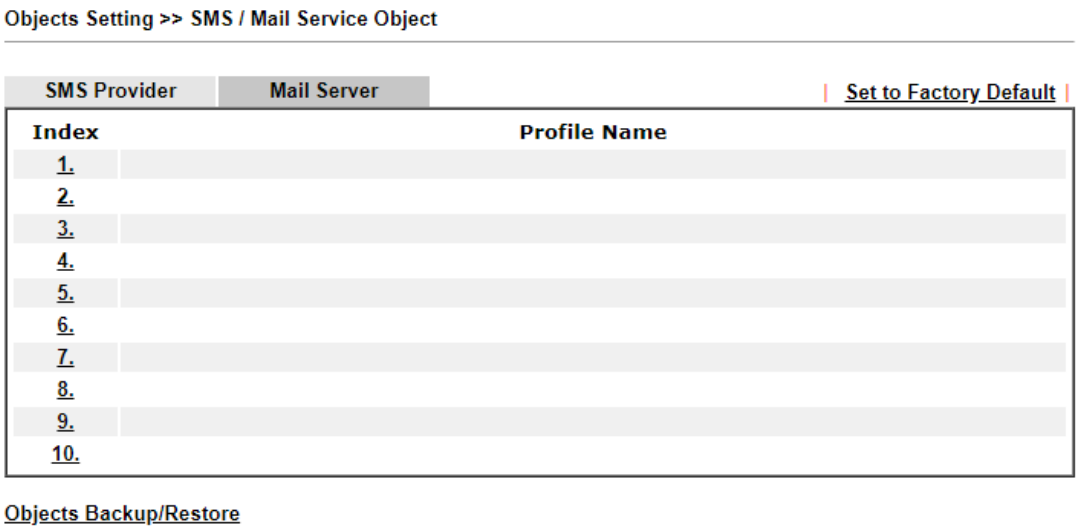
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre de perfil	Nombre de perfil de solo visualización, que es Personalizado 1 para el Índice 9 y Personalizado 2 para el Índice 10.
Proveedor de servicio	Introduzca un identificador para el proveedor de servicios. La longitud máxima es de 23 caracteres.
Cuadro de entrada	Introduzca la URL del servicio de SMS. La longitud máxima es de 255 caracteres. Comuníquese con el proveedor de servicios para obtener la URL adecuada que debe usar.
Respuesta del servidor	Ingrese el texto API definido por el proveedor de SMS. Permite que el enrutador Vigor reconozca que el servidor SMS ha recibido la solicitud proveniente del servidor SMS.
Nombre de usuario	Nombre de usuario utilizado para iniciar sesión en el servicio. La longitud máxima es de 31 caracteres.
Contraseña	Contraseña utilizada para iniciar sesión en el servicio. La longitud máxima es de 31 caracteres.
Cuota	Número restante de mensajes de texto que se pueden enviar. El valor de la cuota se reduce en 1 cada vez que el enrutador envía un mensaje SMS. Cuando la cuota llegue a 0, no se enviará ningún SMS hasta que se restablezca a más de 0.
Intervalo de envío	Cantidad mínima de tiempo, en segundos, para esperar entre el envío de mensajes SMS.

Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para borrar todas las configuraciones en el objeto de servicio SMS, haga clic en**Claro**.

Objeto de servicio de correo

Hasta 10**Objetos de servicio de correo**se puede configurar para su uso con Aplicación>>Servicio de alerta de correo.

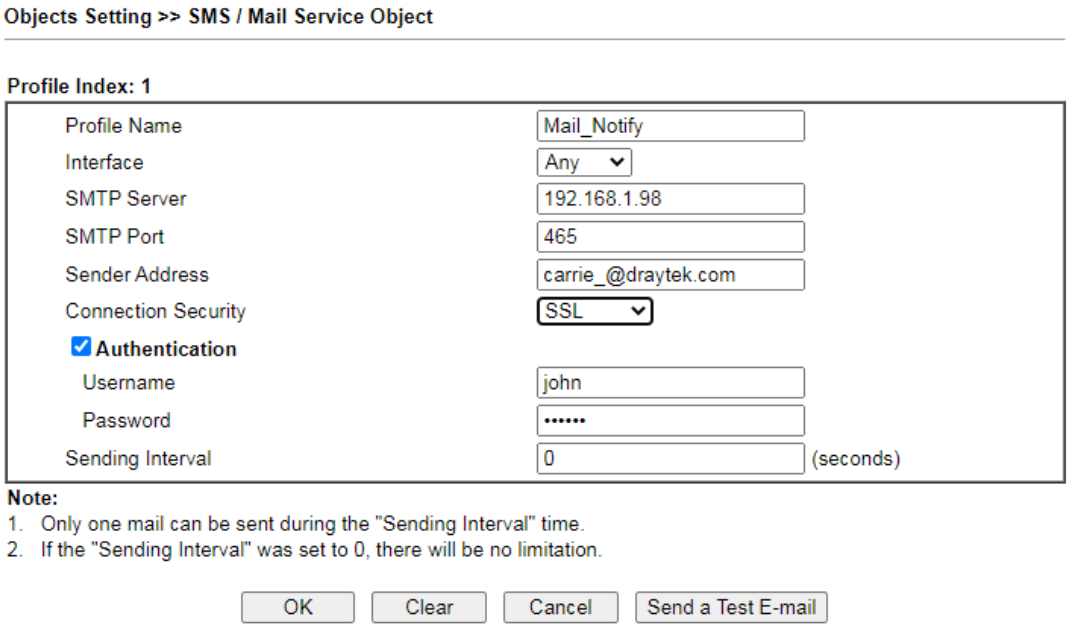


Cada elemento se explica de la siguiente manera:

Artículo	Descripción
Establecer como predeterminado de fábrica	Borre todas las configuraciones de perfil.
Índice	Número de índice del perfil.

Nombre de perfil	Nombre que identifica al perfil.
Copia de seguridad/restauración de objetos	Haga clic en él para hacer una copia de seguridad o restaurar el objeto de servicio.

Para configurar un perfil, haga clic en la pestaña Servidor de correo y luego haga clic en su índice para abrir la página de configuración.



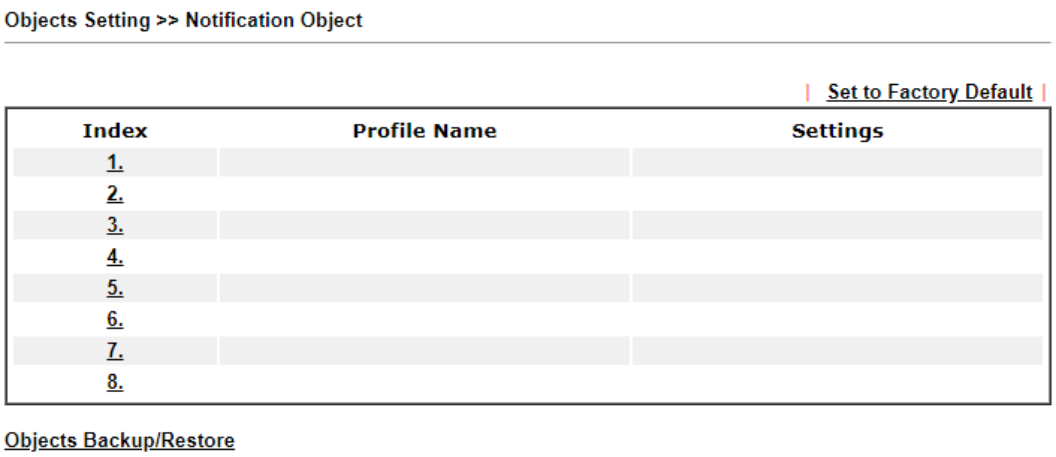
Los ajustes disponibles se explican a continuación:

Artículo	**Descripción**
Nombre de perfil	Nombre que identifica a este perfil. La longitud máxima es de 31 caracteres.
Interfaz	Seleccione una interfaz para el paso del correo.
Servidor SMTP	Dirección IP del servidor SMTP.
Puerto SMTP	Número de puerto del servidor SMTP.
Dirección del remitente	Dirección de correo electrónico del remitente.
Seguridad de conexión	Utilice Plaintext, StartTLS o SSL para comunicarse con el servidor SMTP.
Autenticación	Seleccione para enviar el nombre de usuario y la contraseña al servidor SMTP para la autenticación. **Nombre de usuario**–Nombre de usuario para la autenticación. La longitud máxima es de 31 caracteres. **Contraseña**–Contraseña para autenticación. La longitud máxima es de 31 caracteres.
Intervalo de envío	Cantidad mínima de tiempo, en segundos, para esperar entre el envío de mensajes de correo electrónico.
Enviar un correo electrónico de prueba	Haga clic para enviar un correo electrónico de prueba de acuerdo con la configuración anterior.

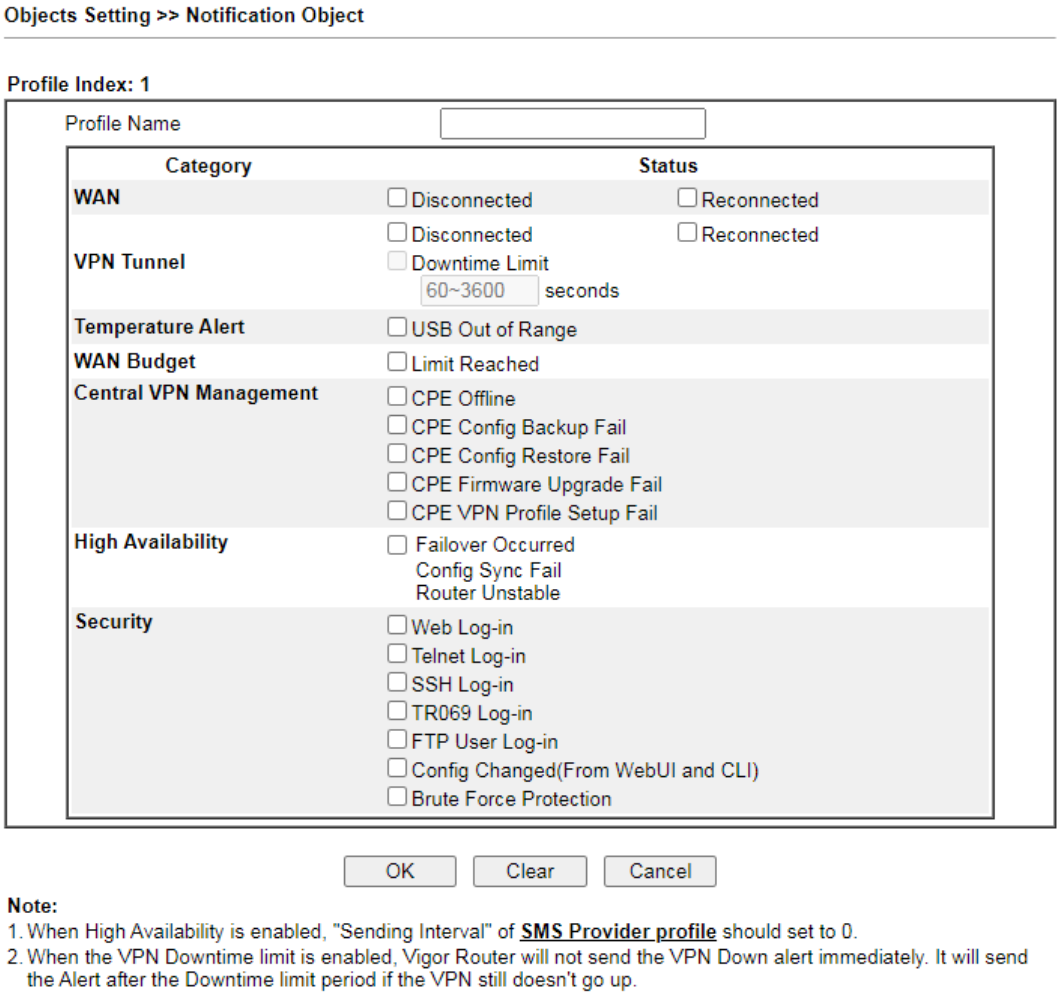
Para guardar los cambios en la página, haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para borrar todas las configuraciones en el objeto de servicio de correo, haga clic en**Claro**.

VIII-1-11 Objeto de notificación

Se pueden configurar hasta 8 objetos de notificación para su uso en**Aplicación>>Servicio de Alerta SMS**y **Aplicación>>Servicio de Alerta por Correo**.



Para configurar un perfil, haga clic en su índice para abrir la página de configuración.



Los ajustes disponibles se explican a continuación:

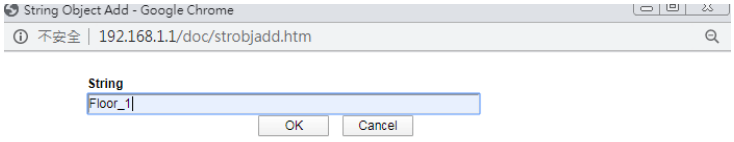
Artículo	Descripción
Nombre de perfil	Nombre que identifica a este perfil. La longitud máxima es de 31 caracteres.
Categoría	Áreas a monitorear.
Estado	Seleccione los estados a monitorear. Por ejemplo, la casilla de verificación de**Error de actualización de firmware de CPE** bajo la categoría de**Gestión central de VPN**está chequeado. Una vez que dicho perfil esté habilitado, el sistema de enrutador Vigor enviará una notificación al destinatario a través de SMS.

Para guardar los cambios en la página, haga clic en Aceptar. Para descartar los cambios, haga clic en Cancelar. Para borrar todas las configuraciones en el objeto de notificación, haga clic en Borrar.

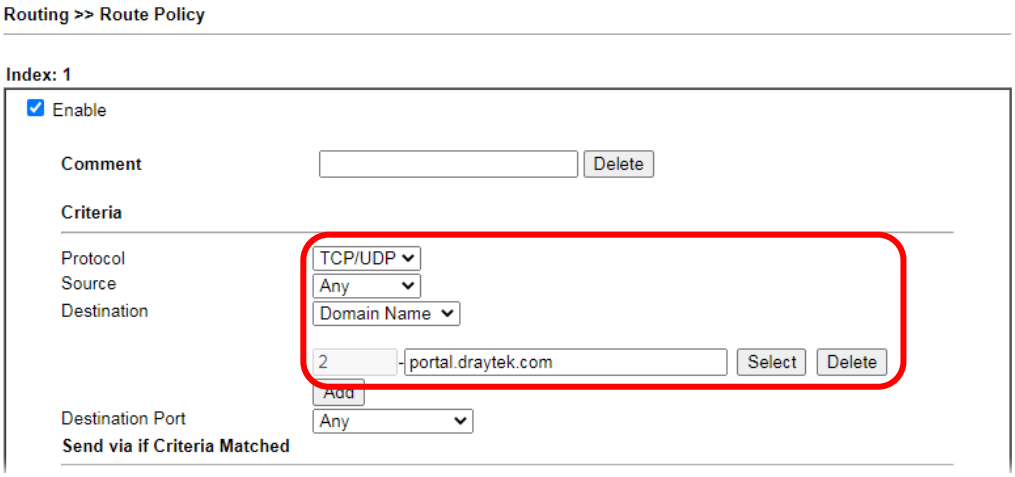
Objeto de cadena VIII-1-12

Esta página le permite establecer perfiles de cadena que se aplicarán en la política de ruta (selección de nombre de dominio para el destino), etc.

Los ajustes disponibles se explican a continuación:

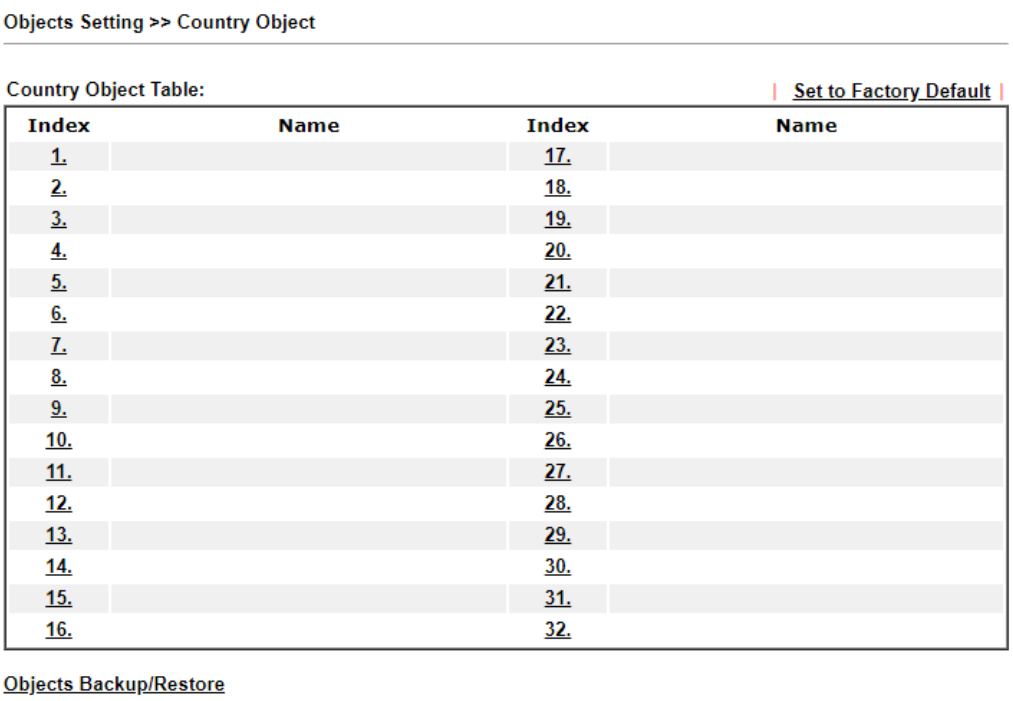
Artículo	Descripción
Agregar	Haga clic en él para abrir la página siguiente para agregar un nuevo objeto de cadena. 
Establecer como predeterminado de fábrica	Haga clic en él para borrar todas las configuraciones en esta página.
Índice	Muestra el enlace numérico del perfil de cadena.
Cadena	Muestra la cadena definida.
Claro	Elija la cadena que desea eliminar. Luego haga clic en esta casilla de verificación para eliminar la cadena seleccionada.

A continuación se muestra un ejemplo para aplicar un objeto de cadena (en la política de ruta):



VIII-1-13 Objeto País

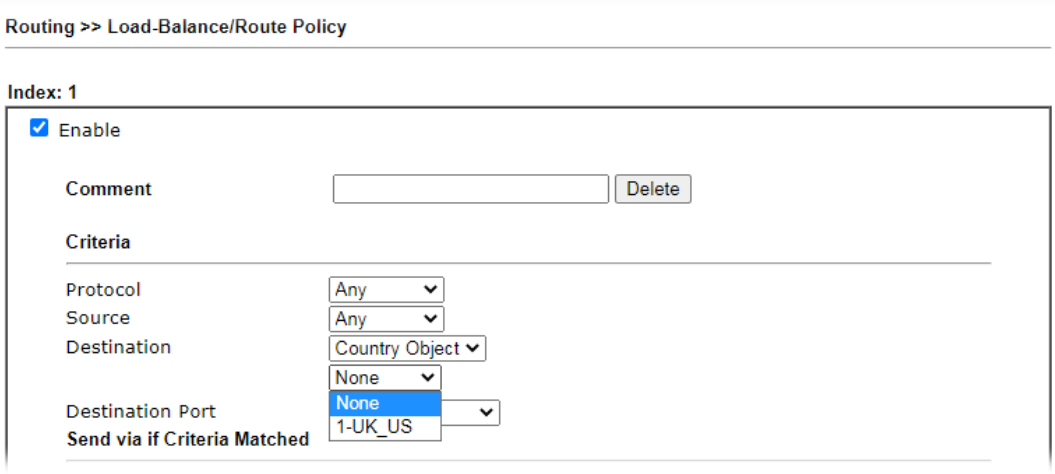
El perfil de objeto de país puede determinar qué país/países serán bloqueados por el cortafuegos del enrutador Vigor.



Información

Este producto incluye datos GeoLite2 creados por MaxMind, disponibles en https://www.maxmind.com.

El objeto de país, al agrupar las direcciones IP de varios países, se puede aplicar mediante otras funciones, como el destino de la política del enrutador (consulte la siguiente figura como ejemplo).



Para configurar un nuevo perfil, siga los pasos que se detallan a continuación:

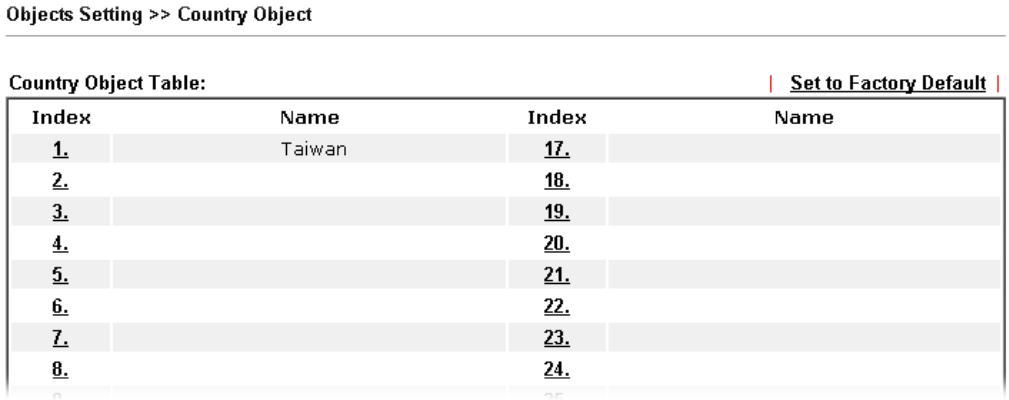
1. Abierto**Configuración de objeto>>Objeto de país**y haga clic en el número (p. ej., #1) en la columna Índice para ver los detalles de la configuración.

2. La página de configuración se mostrará de la siguiente manera:

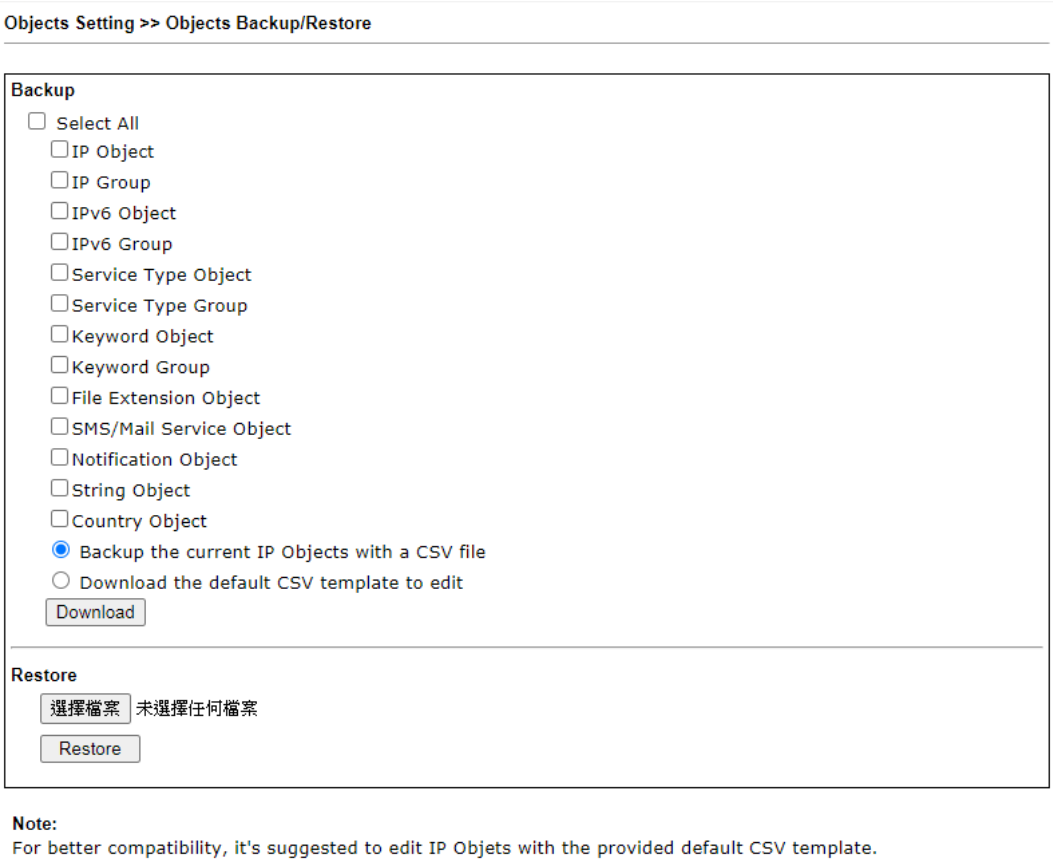
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre	Escriba un nombre para dicho perfil. La longitud máxima del nombre que puede establecer es de 15 caracteres.
País disponible / País seleccionado	Seleccione cualquier país de País disponible. Haga clic en >> para mover el país seleccionado y colocarlo en País seleccionado. Tenga en cuenta que un perfil de país puede contener de 1 a 16 países.

3. Después de finalizar todas las configuraciones aquí, haga clic en**DE ACUERDO**para guardar la configuración.



La configuración de los objetos se puede respaldar como un archivo. El archivo de respaldo se puede importar al dispositivo para restaurar la configuración en el futuro si es necesario.



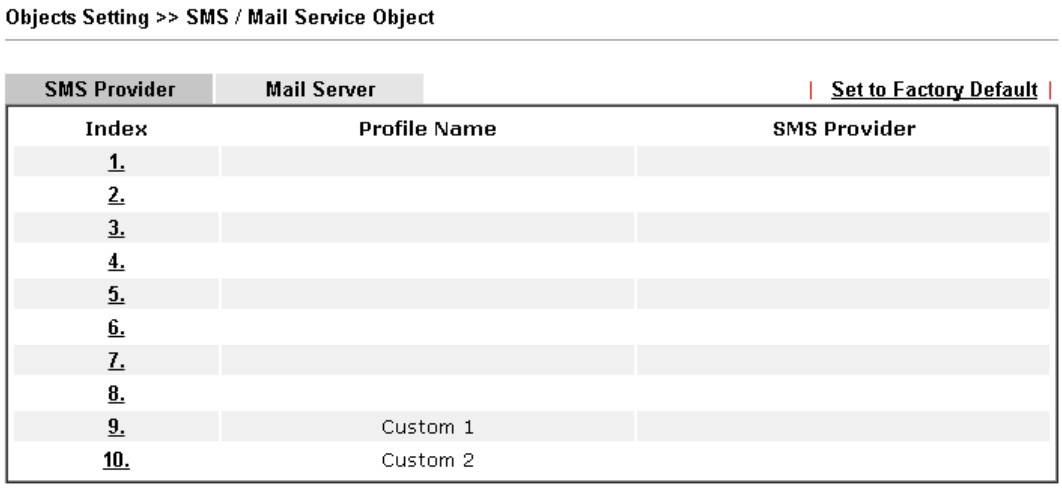
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Respaldo	Por lo general, los objetos se pueden crear uno por uno a través de la página web en**Configuración de objetos**. Sin embargo, para un usuario que quiere ahorrar más tiempo en la creación masiva de varios objetos, el enrutador Vigor ofrece un método rápido para modificar los objetos con un solo archivo, un archivo CSV. Todos los objetos (o la plantilla) se pueden exportar como un archivo haciendo clic en Descargar. Luego, el usuario puede abrir el archivo CSV a través de Microsoft Excel y modificar todos los objetos IP al mismo tiempo. **Copia de seguridad de los objetos IP actuales con un archivo CSV**–Haga clic en él para hacer una copia de seguridad de los objetos IP actuales como un archivo CSV. Dicho archivo se puede restaurar para uso futuro. **Descargue la plantilla CSV predeterminada para editar**–Después de hacer clic en él, presione Descargar para almacenar la plantilla CSV predeterminada (una tabla sin datos de entrada) en su disco duro. **Descargar**–Descargue el archivo CSV del enrutador Vigor y guárdelo en su disco duro.
Restaurar	**Seleccionar**–Haga clic en él para especificar un archivo CSV predefinido. **Restaurar**–Importe el archivo CSV seleccionado al enrutador Vigor.

A-1 Cómo enviar una notificación a un número de teléfono específico a través del servicio de SMS en desconexión de WAN

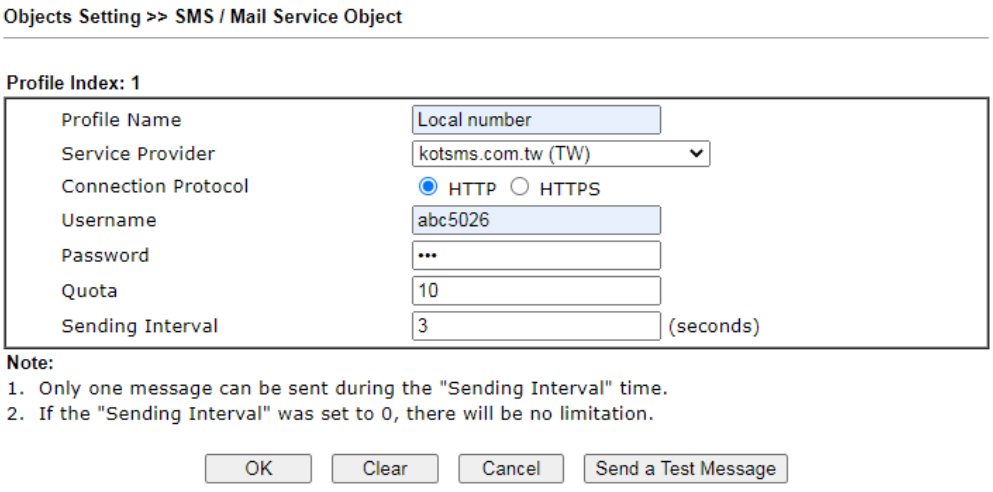
Siga los pasos que se enumeran a continuación:

1. Inicie sesión en la interfaz de usuario web del enrutador Vigor.
2. Configure primero los objetos relacionales. Abierto**Configuración de objetos>>Objeto de servidor de correo/SMS**para obtener la siguiente página.

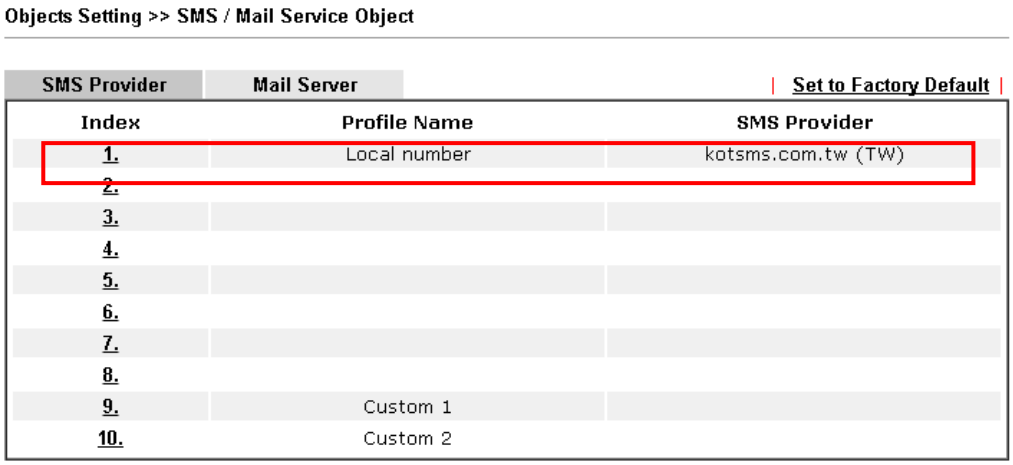


Los índices 1 a 8 le permiten elegir el proveedor de servicios de SMS integrado. Si el proveedor de servicios de SMS no está en la lista, puede configurar el Índice 9 y el Índice 10 para agregar el nuevo proveedor de servicios al enrutador Vigor.

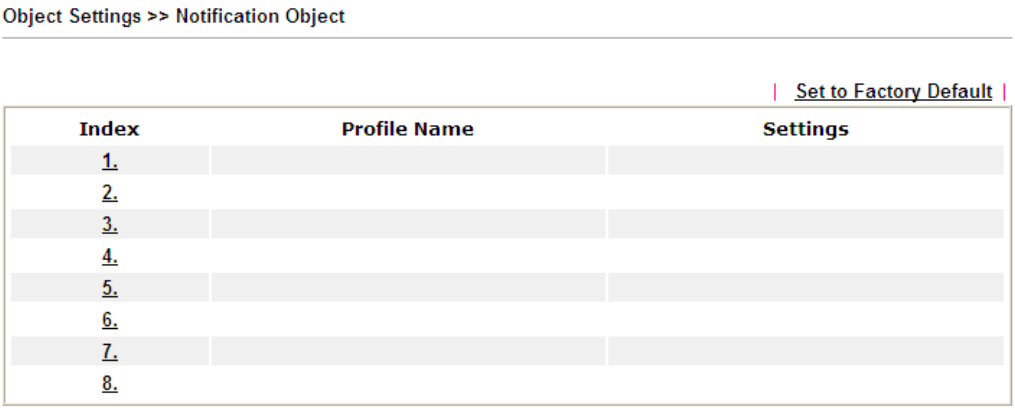
3. Elija cualquier número de índice (p. ej., índice 1 en este caso) para configurar la configuración del proveedor de SMS. En la página siguiente, ingrese el nombre de usuario y la contraseña y establezca la cuota que el enrutador puede enviar el mensaje.



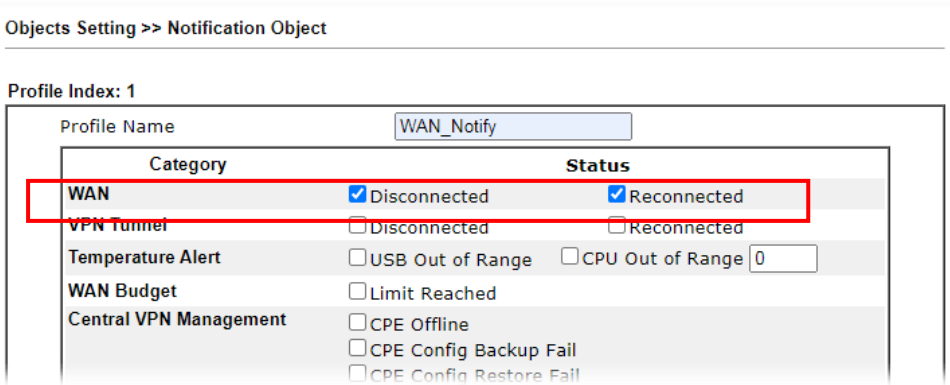
4. Después de terminar la configuración, haga clic en**DE ACUERDO**para volver a la página anterior. Ahora ha terminado la configuración del perfil del proveedor de SMS.



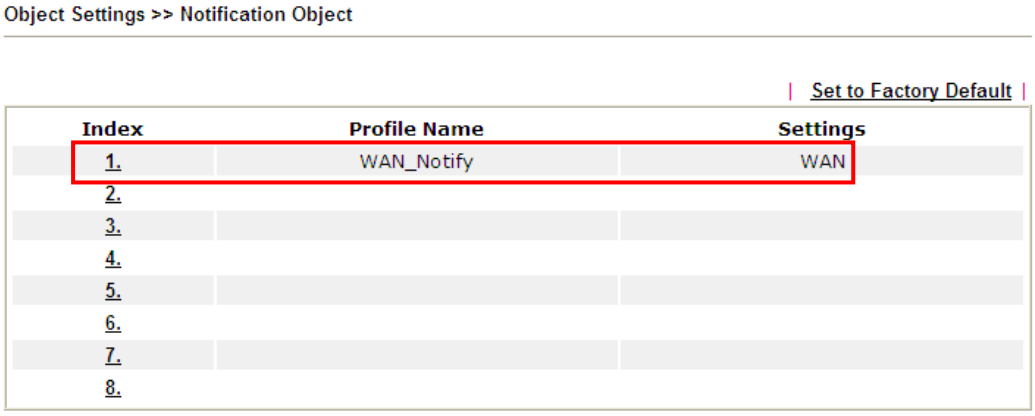
5. Abierto**Configuración de objetos>>Objeto de notificación**para configurar las condiciones de evento de la notificación.



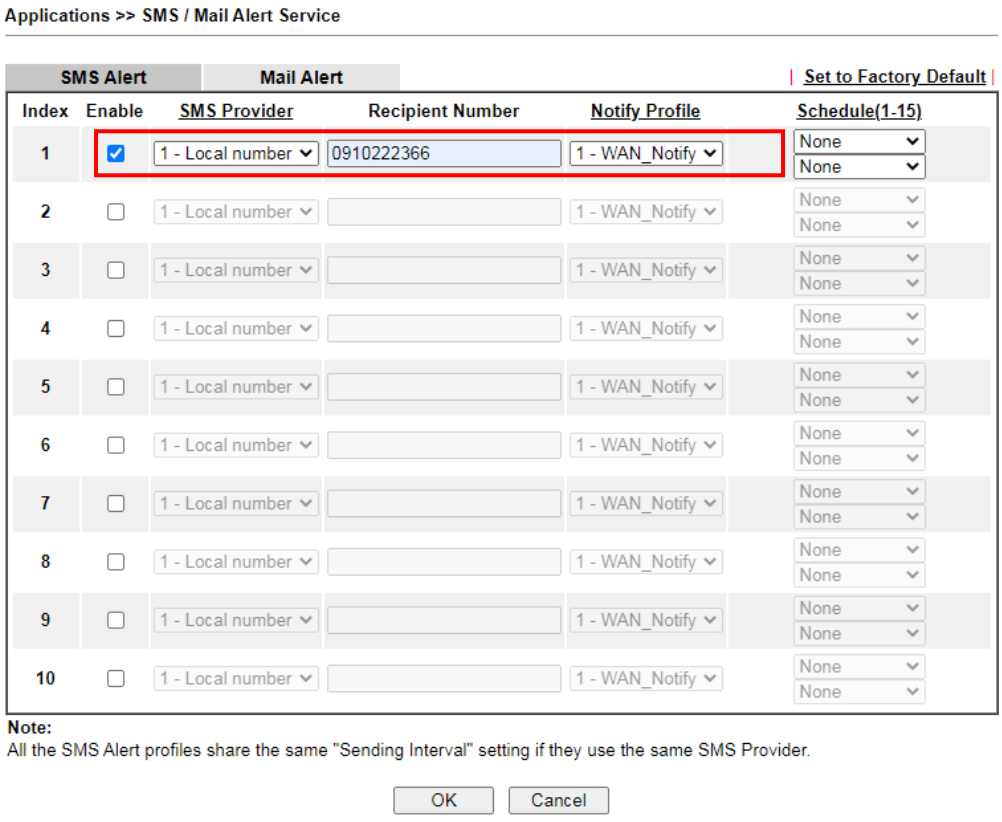
6. Elija cualquier número de índice (p. ej., Índice 1 en este caso) para configurar las condiciones para enviar el SMS. En la página siguiente, Ingrese el nombre del perfil y verifique la Cajas desconectadas y reconectadas para que la WAN funcione en conjunto con el tema de este documento.



7. Después de terminar la configuración, haga clic en**DE ACUERDO**para volver a la página anterior. Ha finalizado la configuración de la configuración del perfil del objeto de notificación.



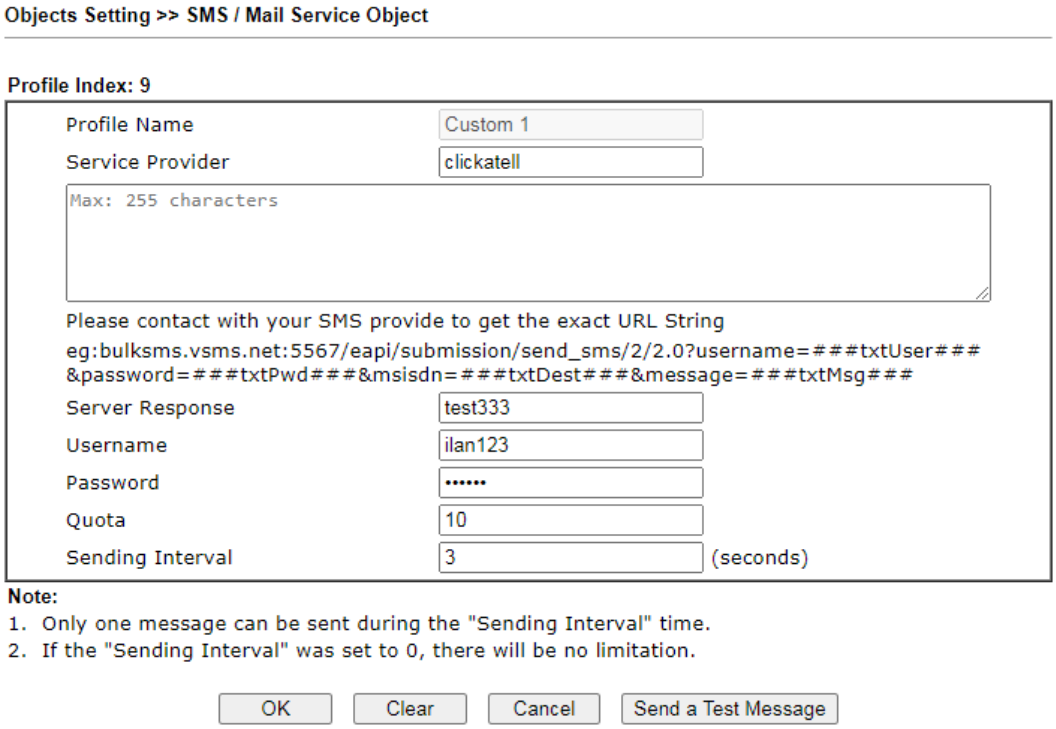
8. Ahora, abre**Aplicación >> Servicio de Alerta SMS / Mail**. Utilice la lista desplegable para elegir el proveedor de SMS y el perfil de notificación (especifique la hora de envío de SMS). Luego, ingrese el número de teléfono en el campo de Número de destinatario (el que recibirá el SMS).



9. Haga clic en**DE ACUERDO**para guardar la configuración. Más tarde, si una de las conexiones WAN falla en su enrutador, el sistema enviará un SMS al número de teléfono especificado. Si el enrutador solo tiene una interfaz WAN, el sistema enviará un SMS al número de teléfono mientras vuelve a conectar la interfaz WAN con éxito.

Observación: cómo personalizar el proveedor de SMS

Elija uno de los números de índice (9 o 10) que le permite personalizar el proveedor de SMS. En la página web, ingrese la cadena URL del proveedor de SMS e ingrese el nombre de usuario y la contraseña. Después de hacer clic**DE ACUERDO**, el nuevo proveedor de SMS agregado se agregará y estará disponible para que lo especifique para enviar SMS.



VIII-2 Aplicación USB

Los dispositivos USB conectados al enrutador Vigor pueden funcionar como servidores de almacenamiento, interfaces WAN, impresoras de red o termómetros.

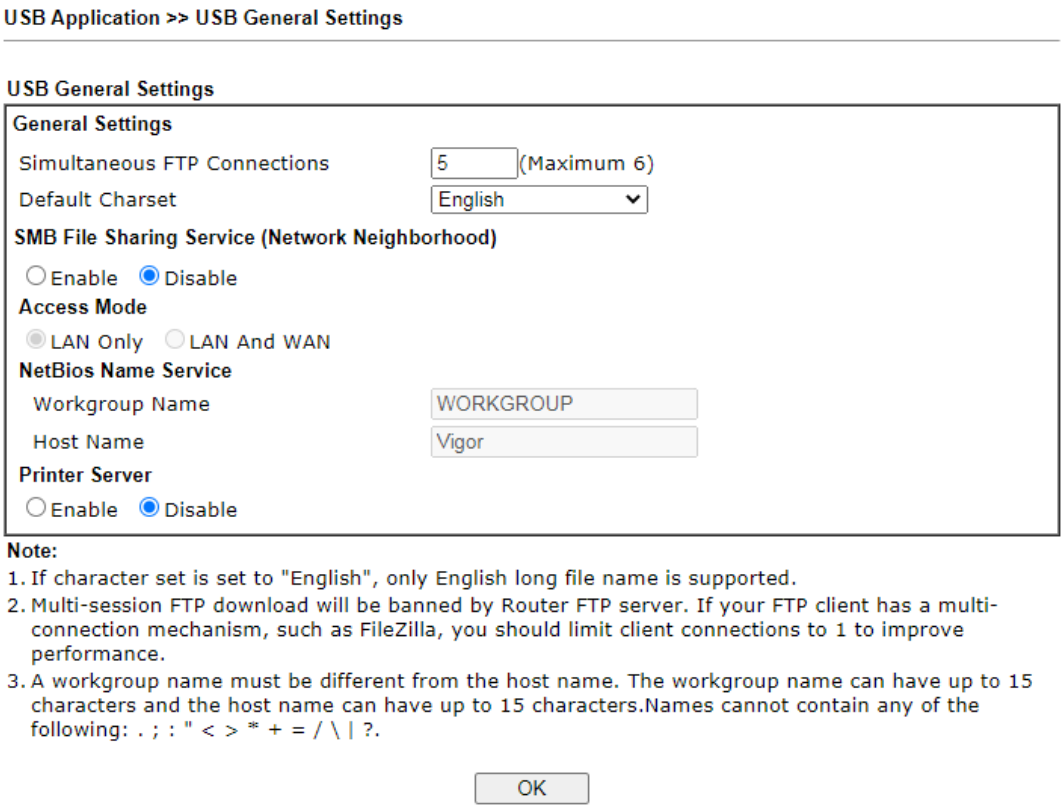
Después de establecer la configuración en la aplicación USB, se puede acceder a un dispositivo de almacenamiento USB mediante el protocolo FTP o SMB desde clientes LAN con la dirección IP del enrutador Vigor y el nombre de usuario y la contraseña ingresados en**Aplicación USB>>Gestión de usuarios USB**.

Información

Los módems USB que son compatibles con el enrutador se enumeran en**Aplicación USB>>Lista de soporte de módem**. Para la conexión de red a través de un módem USB, consulte**WAN>>Acceso a Internet**y**WAN>>Configuración general**para obtener información detallada.

VIII-2-1 Configuración general de USB

Esta página le permite configurar la función de uso compartido de archivos del enrutador Vigor, donde los dispositivos de almacenamiento masivo USB, como memorias USB y discos duros, pueden ser accesibles para los clientes LAN. Actualmente, solo los sistemas de archivos FAT16 y FAT32 son compatibles con el enrutador Vigor, así que verifique que la unidad USB contenga estos sistemas de archivos. Se recomienda FAT32 debido a su compatibilidad con nombres de archivo largos, de la que carece FAT16.



Los ajustes disponibles se explican a continuación:

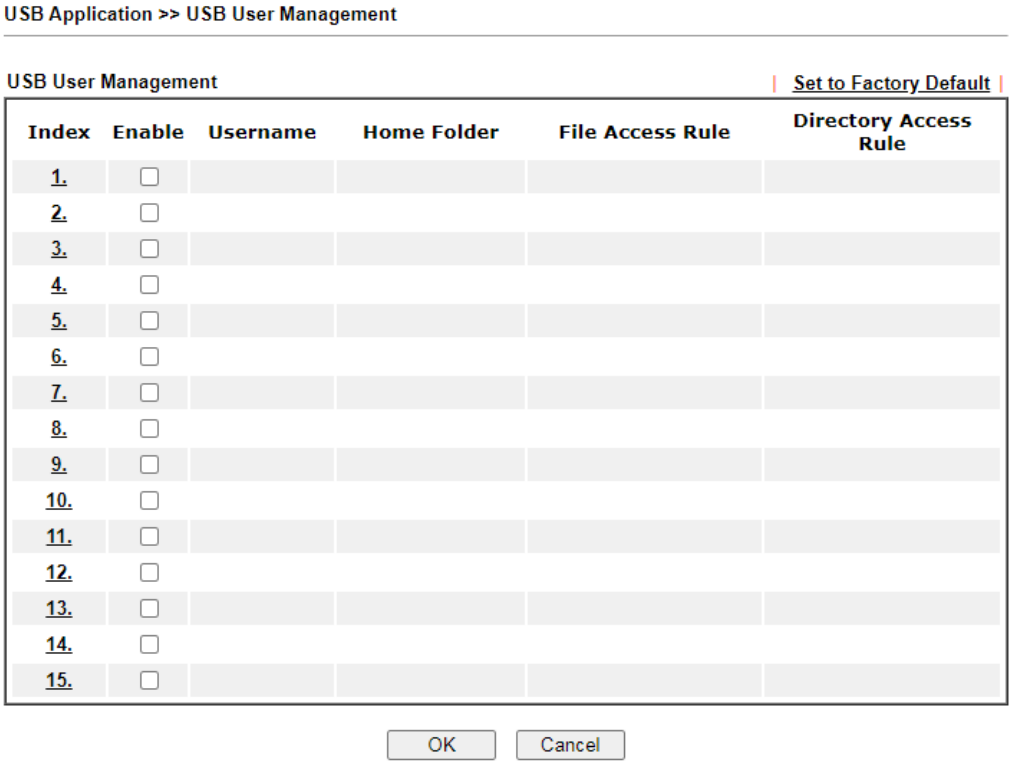
Artículo	Descripción
Configuración general	**Conexiones FTP simultáneas -**Ingrese el número máximo de sesiones FTP simultáneas permitidas. El router permite hasta 6 sesiones simultáneas. **Juego de caracteres predeterminado -**Seleccione el conjunto de caracteres para los nombres de archivos y directorios. Actualmente, el enrutador Vigor admite cuatro

	juegos de caracteres El juego de caracteres predeterminado es inglés.
Servicio de intercambio de archivos SMB	Hacer clic**Permitir**para habilitar el servicio SMB (uso compartido de archivos).
Modo de acceso	**Solo LAN**–Solo los usuarios de la LAN pueden conectarse y acceder al disco USB compartido. **LAN y WAN**-Tanto los usuarios de LAN como los de WAN pueden acceder al servidor SMB del enrutador.
Servicio de nombres NetBios	Para el servicio de uso compartido de archivos SMB, debe especificar un nombre de grupo de trabajo y un nombre de host. Los dos nombres no pueden ser idénticos, y tampoco pueden contener ninguno de los siguientes caracteres: ; : " < > * + = \ | ? **Nombre del grupo de trabajo:**Introduzca el nombre del grupo de trabajo. La longitud máxima permitida es de 15 caracteres. **Nombre del anfitrión:**Ingrese el nombre de host NetBIOS para el enrutador. La longitud máxima permitida es de 23 caracteres.
Servidor de impresora	**Permitir**–Seleccione para permitir que el enrutador Vigor actúe como un servidor de impresión para las impresoras conectadas al USB.

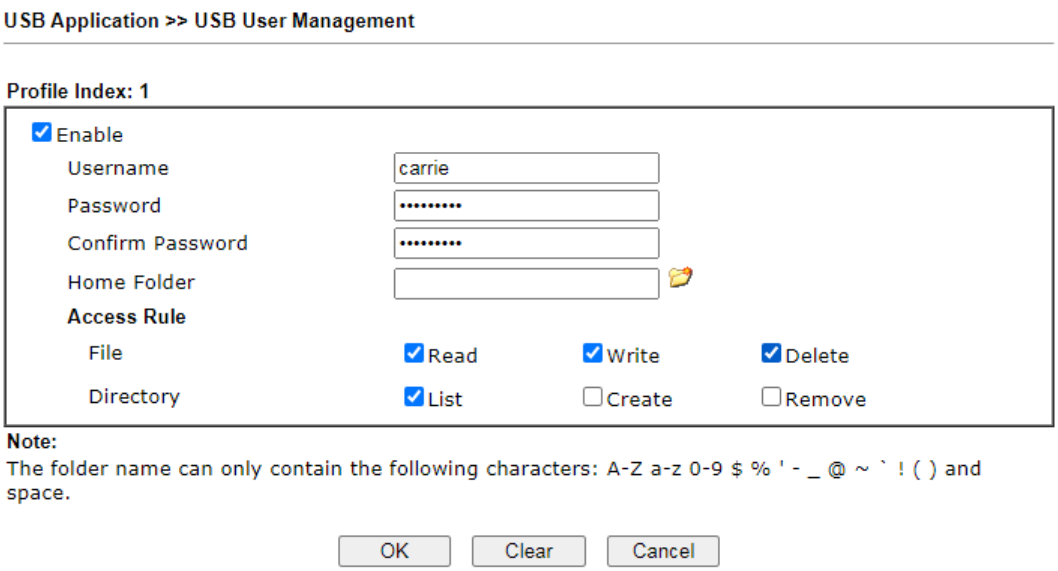
Seleccionar**DE ACUERDO**para guardar los cambios en la página.

VIII-2-2 Gestión de usuarios USB

Esta página le permite configurar perfiles para usuarios de FTP/SMB. Cualquier usuario que desee acceder al disco de almacenamiento USB debe autenticarse utilizando un nombre de usuario y una contraseña que se hayan configurado en esta página. Conecte un dispositivo de almacenamiento USB antes de agregar o modificar la configuración en esta página; de lo contrario, aparecerá un mensaje de error solicitándole que lo haga antes de permitirle continuar.

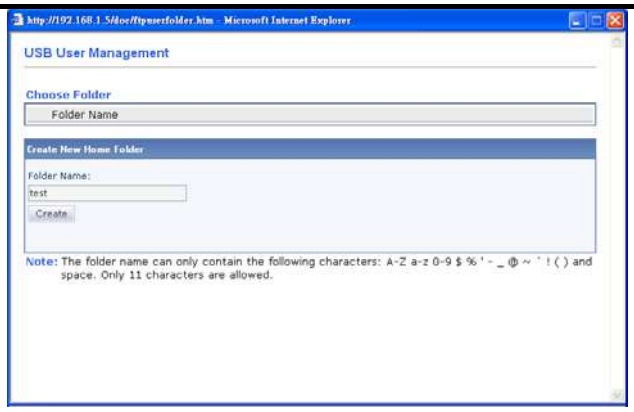


Haga clic en el número de índice para acceder a la página de configuración.



Los ajustes disponibles se explican a continuación:

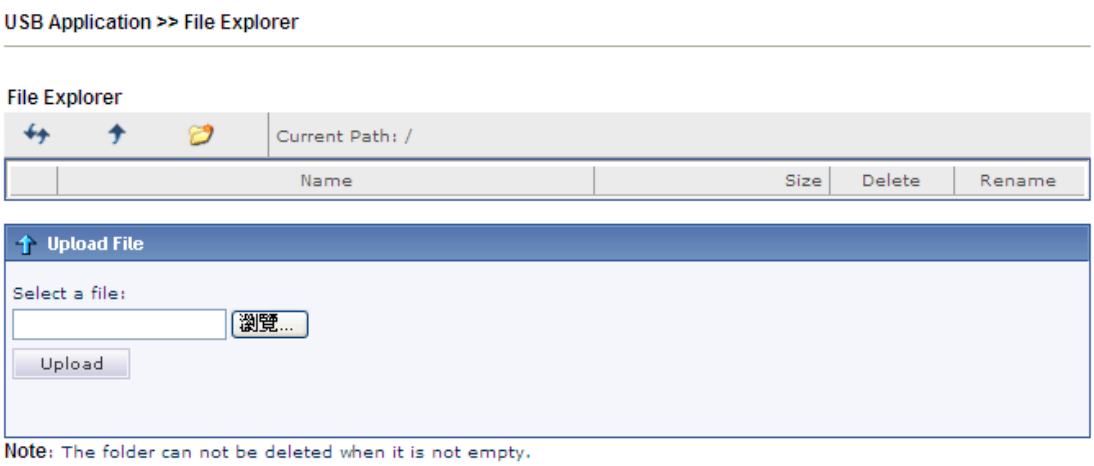
Artículo	Descripción
Permitir	Marque para activar este perfil (cuenta) para servicio FTP y/o servicio SMB. Posteriormente, el usuario puede utilizar el nombre de usuario especificado en esta página para iniciar sesión en el servidor FTP.
Nombre de usuario	Introduzca el nombre de usuario para este perfil de usuario. La longitud máxima permitida del nombre de usuario es de 11 caracteres. **Nota:**No se admite el acceso de usuarios anónimos. **Nota:**"Admin" no se puede utilizar como nombre de usuario, ya que está reservado para el acceso a páginas web en el enrutador Vigor y para la actualización del firmware FTP. **Nota:**Asegúrese de que el cliente FTP no utilice el modo FTP pasivo, ya que no es compatible con el enrutador Vigor.
Contraseña	Introduzca la contraseña para este perfil de usuario. La longitud máxima permitida del nombre de usuario es de 11 caracteres.
confirmar Contraseña	Introduzca la contraseña de nuevo para confirmar.
Carpeta de inicio	Ingrese la carpeta que será la carpeta raíz para las sesiones FTP y SMB establecidas con las credenciales de este perfil de usuario. Solo las carpetas y los archivos dentro de esta carpeta raíz seleccionada son accesibles para el usuario. Además, si el usuario escribe "/" aquí, puede acceder a todas las carpetas y archivos del disco en el disco de almacenamiento USB. Para navegar por la lista de carpetas disponibles para seleccionar, o para crear una nueva carpeta, haga clic en el icono.

	 **Nota**: Si el dispositivo de almacenamiento USB está protegido contra escritura, no se pueden crear nuevas carpetas. Solo se pueden seleccionar las carpetas existentes. **Nota**: Solo las carpetas directamente debajo de la raíz se pueden seleccionar como carpeta de inicio.
regla de acceso	Determina la autoridad para dicho perfil. Cualquier usuario que use dicho perfil para acceder al disco de almacenamiento USB debe seguir la regla especificada aquí. **Archivo**–Verifique los elementos (Leer, Escribir y Eliminar) para dicho perfil. **Directorio**–Verifique los elementos (Lista, Crear y Eliminar) para dicho perfil.

Para guardar los cambios en esta página, asegúrese de que un dispositivo de almacenamiento USB esté conectado y haga clic en**DE ACUERDO**. Para descartar los cambios, haga clic en**Cancelar**. Para borrar todas las configuraciones en el objeto IP actual, haga clic en**Claro**.

VIII-2-3 Explorador de archivos

File Explorer ofrece una manera fácil para que los usuarios vean y administren el contenido del disco de almacenamiento USB conectado en el enrutador Vigor.



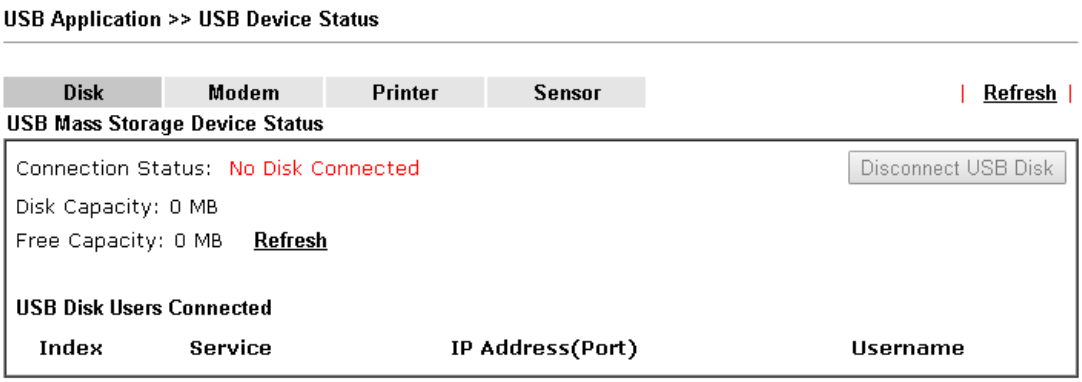
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Actualizar	Haga clic en este icono para actualizar la lista de archivos y carpetas.

Atrás	Haga clic en este icono para volver a la carpeta principal.
Crear	Haga clic en este icono para agregar una nueva carpeta.
Trayectoria de corriente	Muestra la carpeta actual.
Subir	Para cargar un archivo en el dispositivo de almacenamiento USB, haga clic en el **Navegar...**para abrir el cuadro de diálogo de selección de archivos. Seleccione el archivo que desea cargar y haga clic en el botón**Subir** botón para iniciar el proceso de carga.

VIII-2-4 Estado del dispositivo USB

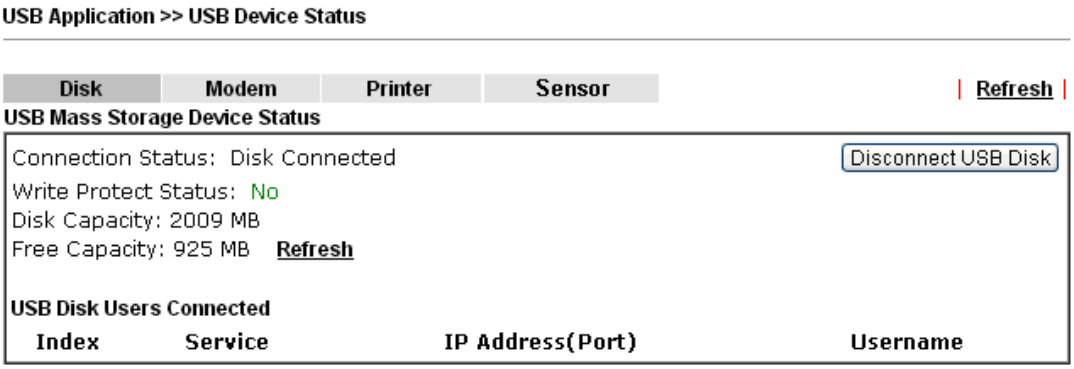
Esta página permite monitorear el estado de los dispositivos USB (disco, módem, impresora y sensor) conectados al enrutador Vigor. Para mantener la integridad de los datos de un disco USB conectado al enrutador, siempre haga clic en**Desconectar disco USB**antes de desconectar el disco del enrutador.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Estado de conexión	Muestra si un disco USB está conectado o no. Si no hay un dispositivo USB conectado al enrutador Vigor, se mostrará "No Disk Connected".
Capacidad de disco	Muestra la capacidad total del disco de almacenamiento USB.
Capacidad Libre	Muestra el espacio libre en el disco de almacenamiento USB. Hacer clic**Actualizar** en cualquier momento para obtener la capacidad libre más actualizada.
Usuarios de discos USB conectados	Muestra los clientes que están conectados al servidor SMB/FTP. **Índice**–El índice de perfil utilizado por el cliente LAN para establecer la conexión. **Servicio**–Muestra si la conexión está usando FTP o SMB. **Dirección IP**–Muestra la dirección IP del cliente. **Nombre de usuario**–Muestra el nombre de usuario utilizado para establecer la conexión.
Desconectar disco USB	Antes de desconectar el dispositivo de almacenamiento USB del enrutador, asegúrese de hacer clic primero para asegurarse de que todos los datos se hayan escrito en el disco y todos los archivos abiertos estén cerrados.

Después de conectar un dispositivo de almacenamiento USB, el**Estado de conexión**se actualizará en unos segundos.



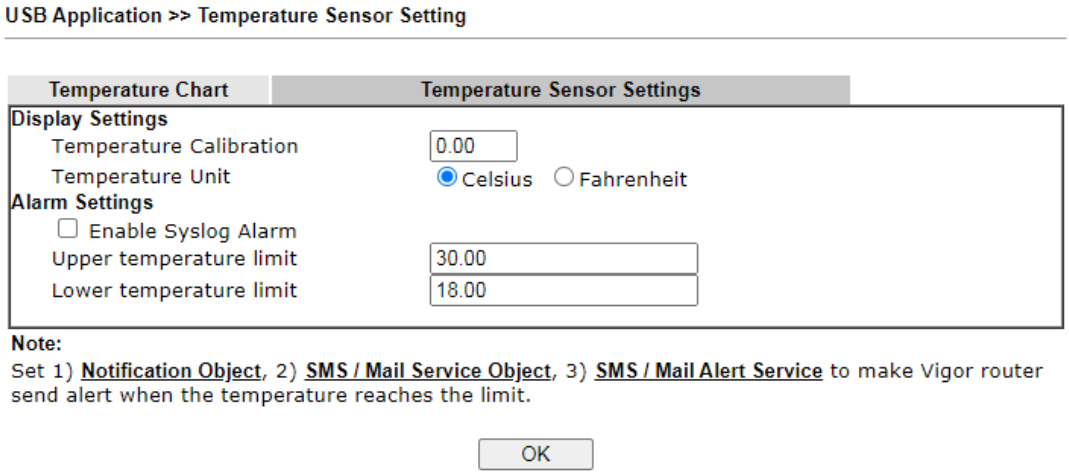
Sensor de temperatura VIII-2-5

Un termómetro USB ya está disponible. Complementa las instalaciones de su enrutador DrayTek instalado, lo que lo ayudará a monitorear el servidor o el entorno de la sala de comunicaciones de datos y le notificará si la sala de servidores o la sala de comunicaciones de datos se está sobrecalentando.

Durante el verano en particular, es importante asegurarse de que su servidor o equipo de comunicación de datos no se sobrecaliente debido a fallas en el sistema de enfriamiento.

La inclusión de un termómetro USB en los enrutadores Vigor compatibles monitoreará continuamente la temperatura de su entorno. Cuando se alcanza un umbral predeterminado, se le avisará por correo electrónico o SMS para que pueda tomar las medidas adecuadas.

Para obtener una lista de termómetros USB compatibles, visite nuestro sitio web en https://www.draytek.com/en/products/usb-thermometer/ o comuníquese con su socio DrayTek local.

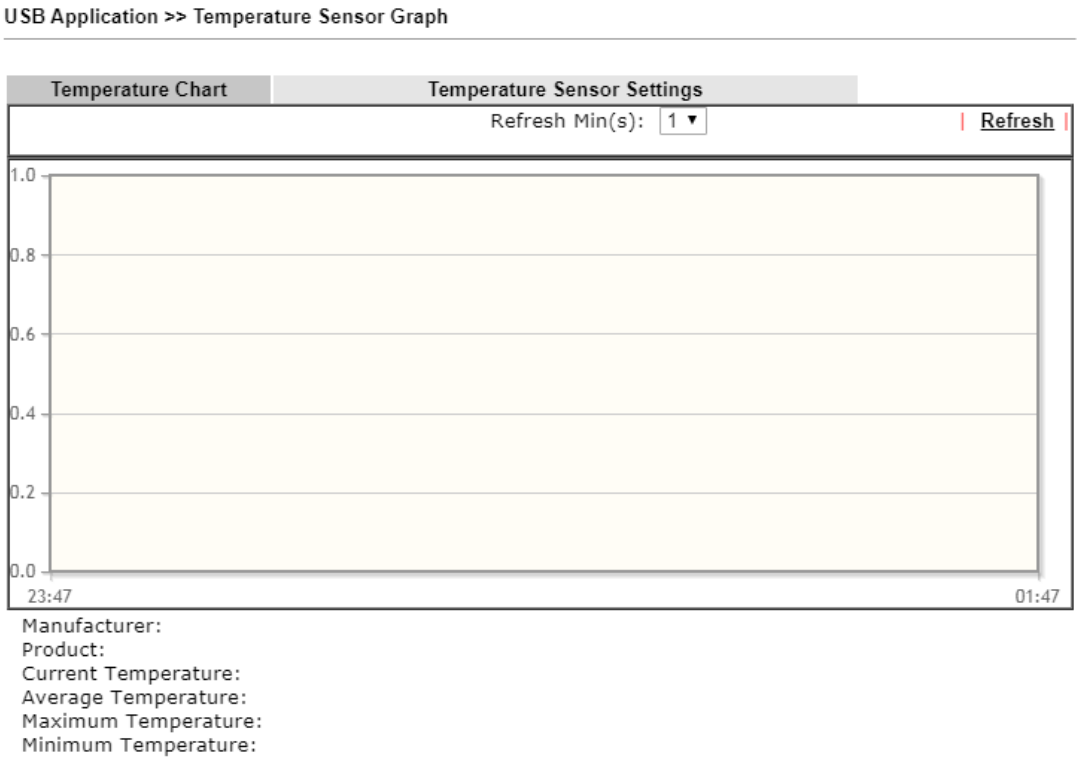


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Configuración de pantalla	**Calibración de temperatura**-Introduzca la diferencia entre la temperatura real y la temperatura que indica el termómetro. **Unidad de temperatura -**Seleccione la escala de temperatura a utilizar.
Configuración de alarma	**Habilitar alarma de Syslog**-Seleccione para habilitar el registro de la temperatura en Syslog. **Límite de temperatura superior/Límite de temperatura inferior**- Introduzca los límites de temperatura superior e inferior. Si la temperatura cae fuera de este rango, se enviará una alerta.

Gráfico de temperatura

A continuación se muestra un ejemplo de gráfico de temperatura:



VIII-2-6 Lista de soporte de módem

Esta página enumera las marcas y modelos de módems USB compatibles con el enrutador Vigor.

Esta lista está sujeta a cambios entre diferentes versiones de firmware a medida que se agrega soporte para nuevos módems.

USB Application >> Modem Support List

The following compatibility test lists 3.5G/LTE modems **supported by Vigor router under certain environment or countries.** If the LTE modem you have is on the list but cannot work properly, please write an e-mail to support@draytek.com or consult your dealer for further information.

Brand	Model	LTE	Access Mode	Status
4G system	XSPlug P3		PPP	Y
Aiko	Aiko 76E		PPP	Y
Alcatel	Alcatel L100V	✓	DHCP	Y
	Alcatel L800	✓	DHCP	Y
	Alcatel W100	✓	DHCP	Y
	Alcatel W800	✓	DHCP	Y
	Alcatel X500		PPP	Y
	Alcatel Y855	✓	DHCP	Y
Alfa	ALFA Flyppp		PPP	Y
Amoi	Amoi H01		PPP	Y
BandRich	Bandluxe C321		PPP	Y
	Bandluxe C330		PPP	Y
	Bandluxe C331		PPP	Y
	Bandluxe C502		PPP	Y
BigPond	BigPond Next G Wireless		PPP	Y
	Broadband USB Mobile Card		PPP	Y
D-Link	D_LINK DWM156		DHCP	M
	Huawei E150		PPP	Y
	Huawei E153		PPP	Y
	Huawei E172		PPP	Y
	Huawei E176c		PPP	M
	Huawei E270		PPP	Y

VIII-2-7 Lista de soporte de clientes SMB

Esta página muestra una lista de clientes SMB en varias plataformas y sus niveles de compatibilidad con el enrutador Vigor según lo determinado por nuestras pruebas internas. Esta lista está sujeta a cambios a medida que se agregue o mejore la compatibilidad con clientes SMB.

USB Application >> SMB Client Support List

The following compatibility test lists suggested SMB clients supported by Vigor router.

Platform	Application	Status
Microsoft® Windows® XP	Built in	I
Microsoft® Windows Vista™	Built in	Y
Microsoft® Windows® 7	Built in	Y
Microsoft® Windows® 8	Built in	M
Microsoft® Windows® 10	Built in	Y
OS X® 10.7.5	Built in	Y
OS X® 10.10	Built in	Y
Ubuntu 14.04	Built in	Y
Android™	AndSMB	Y
Android™	ES File Explorer	Y
Android™	File Expert	Y
Android™	File Manager	Y
Android™	Solid Explorer	Y
Android™	SharesFinder	Y
iOS	eXPlayer	Y
iOS	nPlayer	Y

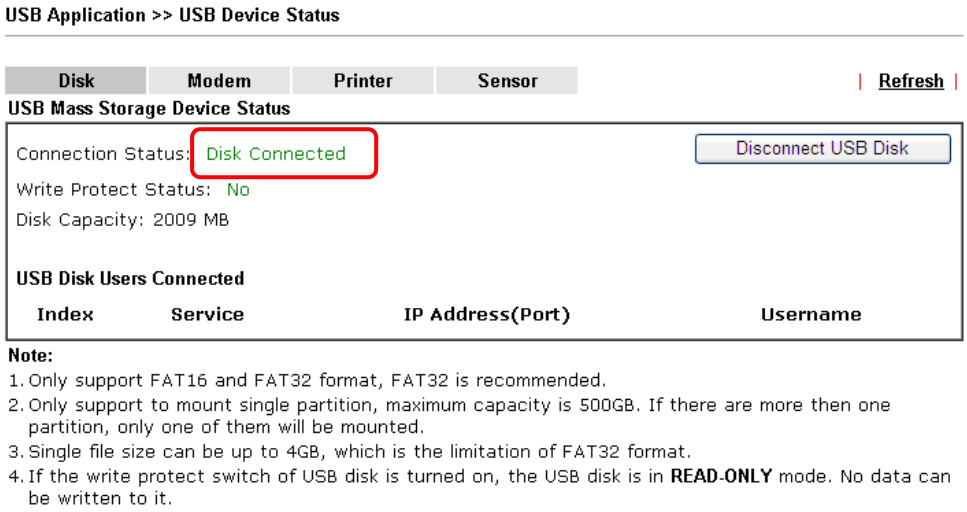
Y: Tested and is supported.
I: Supported but has some issue.
M: Has not been tested but might be supported.

A-1 ¿Cómo puedo obtener los archivos del dispositivo de almacenamiento USB que se conecta al enrutador Vigor?

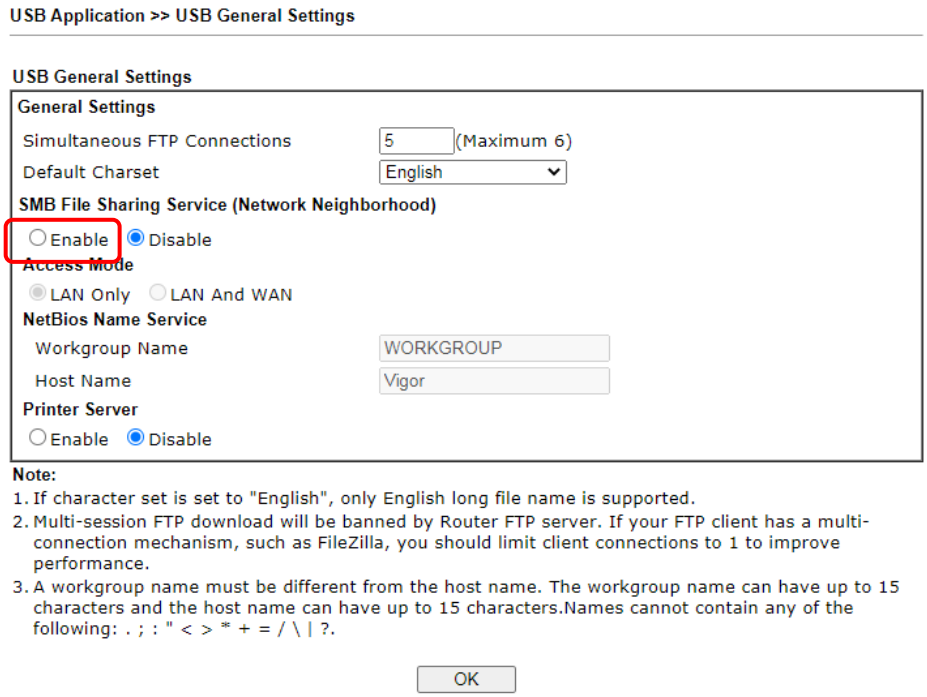
Los archivos en el dispositivo de almacenamiento USB se pueden revisar abriendo**Aplicación USB>>Explorador de archivos.**Si es necesario que elimine, copie archivos en el dispositivo o escriba, pegue archivos en el dispositivo, debe hacerlo a través del servidor SMB o servidor FTP.

El servicio SMB se basa en el servicio FTP USB original. Primero deberá configurar USB FTP. Nos gustaría dar breves instrucciones sobre la configuración USB FTP aquí.

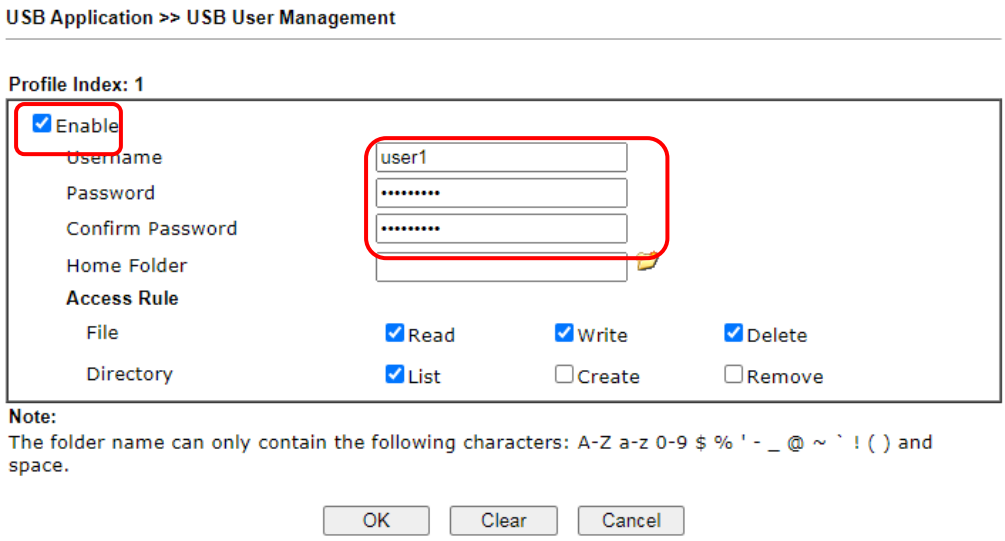
1. Conecte el dispositivo USB al puerto USB del enrutador. Cerciorarse**disco conectado**aparece en el**Estado de conexión**como la figura que se muestra a continuación:



2. Luego, abre**Aplicación USB >> Configuración general de USB**para habilitar el servicio SMB.

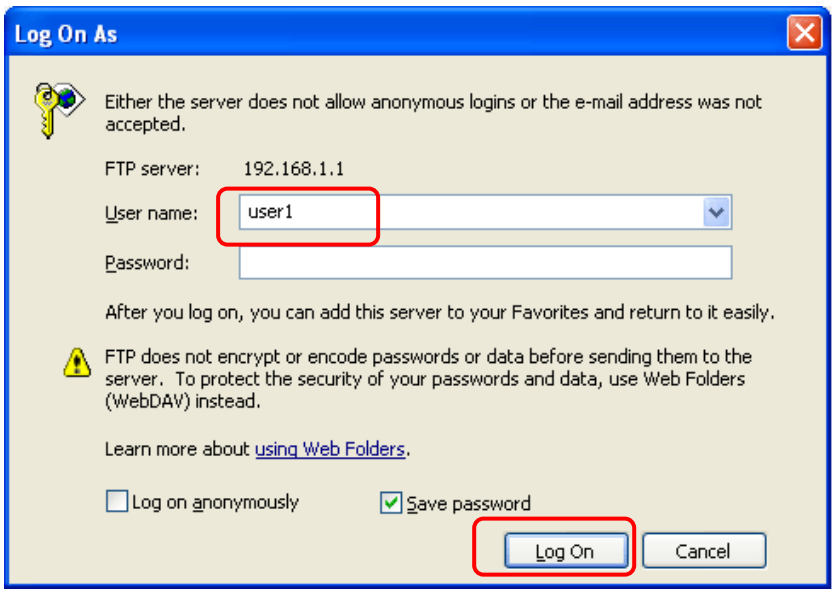


3. Configure una cuenta de usuario para el servicio FTP utilizando**Aplicación USB >>Gestión de usuarios USB.** Hacer clic**Permitir**para habilitar la cuenta de usuario FTP/SMB. En el siguiente ejemplo, configuramos una nueva cuenta con el nombre de usuario "usuario1" y le otorgamos permisos de "Lectura", "Escritura", "Eliminación" y "Lista".

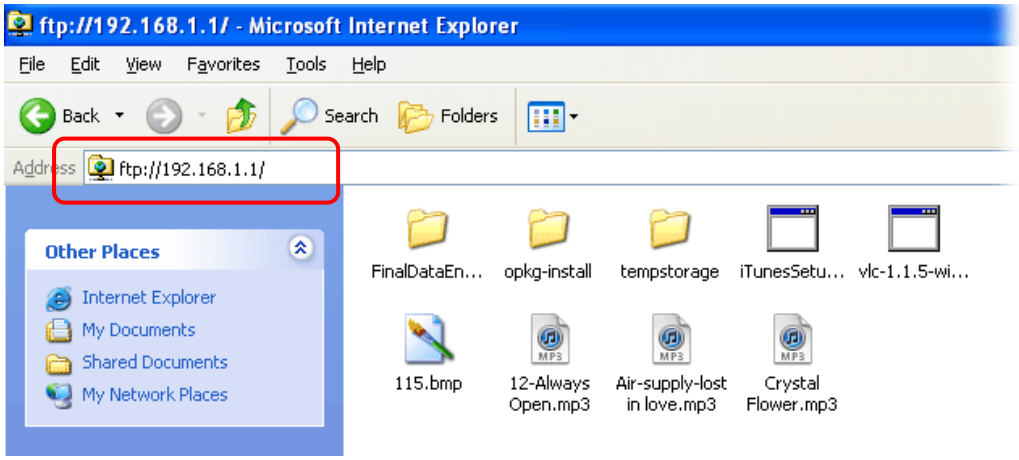


4. Haga clic en**DE ACUERDO**para guardar la configuración.

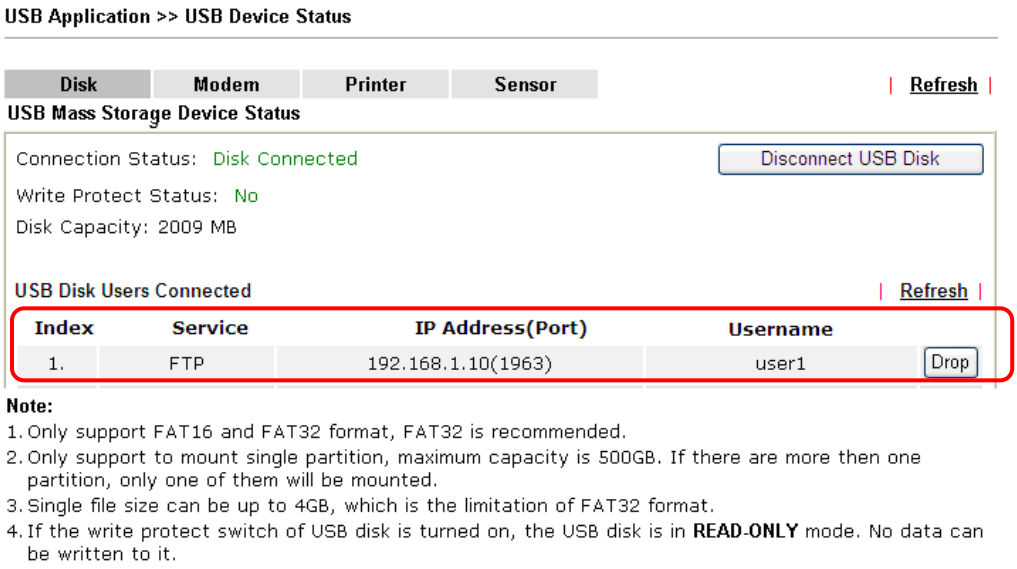
5. Para verificar que el servicio FTP se está ejecutando correctamente, abra una ventana del navegador e ingrese ftp://192.168.1.1 como destino. Reemplace 192.168.1.1 con la dirección IP real del enrutador. Cuando se le solicite ingresar las credenciales de inicio de sesión, ingrese el nombre de usuario "usuario1" para iniciar sesión.



6. Cuando aparezca la siguiente pantalla, se ha conectado con éxito al servidor FTP y ha verificado que funciona correctamente.



7. Si marca**Aplicación USB >> Estado del disco USB**en el navegador, verá la sesión FTP iniciada por el usuario1.



Note:

1. Only support FAT16 and FAT32 format, FAT32 is recommended.
2. Only support to mount single partition, maximum capacity is 500GB. If there are more then one partition, only one of them will be mounted.
3. Single file size can be up to 4GB, which is the limitation of FAT32 format.
4. If the write protect switch of USB disk is turned on, the USB disk is in **READ-ONLY** mode. No data can be written to it.

Ahora, los usuarios en LAN de Vigor2927 pueden acceder al dispositivo de almacenamiento USB ingresando ftp://192.168.1.1 en cualquier navegador. Pueden agregar o eliminar archivos/directorios, según la regla de acceso para la configuración de la cuenta FTP en**Aplicación USB >>Gestión de usuarios USB.**

Esta página se deja en blanco.

Parte IX Solución de problemas

Troubleshooting

Esta parte lo guiará para resolver situaciones anormales si no puede acceder a Internet después de instalar el enrutador y finalizar la configuración web.

Diagnóstico IX-1

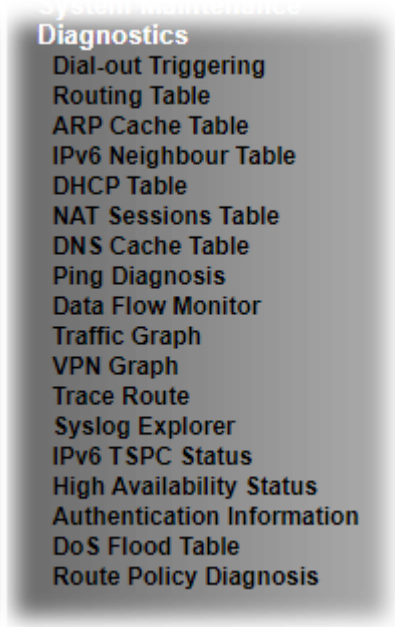
Esta sección lo guiará para resolver situaciones anormales si no puede acceder a Internet después de instalar el enrutador y finalizar la configuración web. Siga las secciones a continuación para verificar el estado de su instalación básica etapa por etapa.

- Comprobando si el estado del hardware es correcto o no.
- Comprobando si la configuración de la conexión de red en su computadora está bien o no. Hacer
- ping al enrutador desde su computadora.
- Comprobando si la configuración del ISP está bien o no. Volver a la
- configuración predeterminada de fábrica si es necesario.

Si se completaron todas las etapas anteriores y el enrutador aún no puede funcionar normalmente, es el momento de que se comunique con su distribuidor o con el soporte técnico de DrayTek para obtener ayuda avanzada.

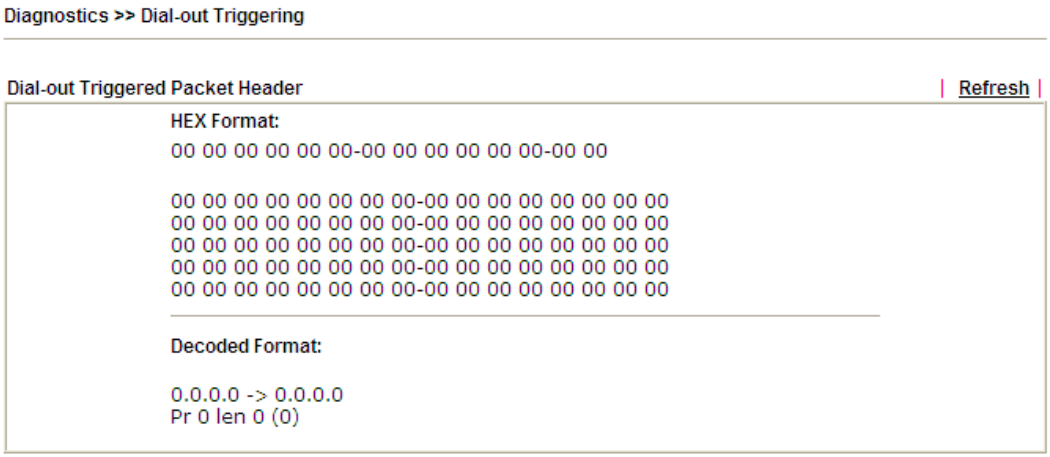
Interfaz de usuario web

Primero, eche un vistazo a los elementos del menú en Diagnósticos. Las herramientas de diagnóstico proporcionan una forma útil de**vista**o**diagnosticar**el estado de su enrutador Vigor.



Activación de marcación de salida IX-1-1

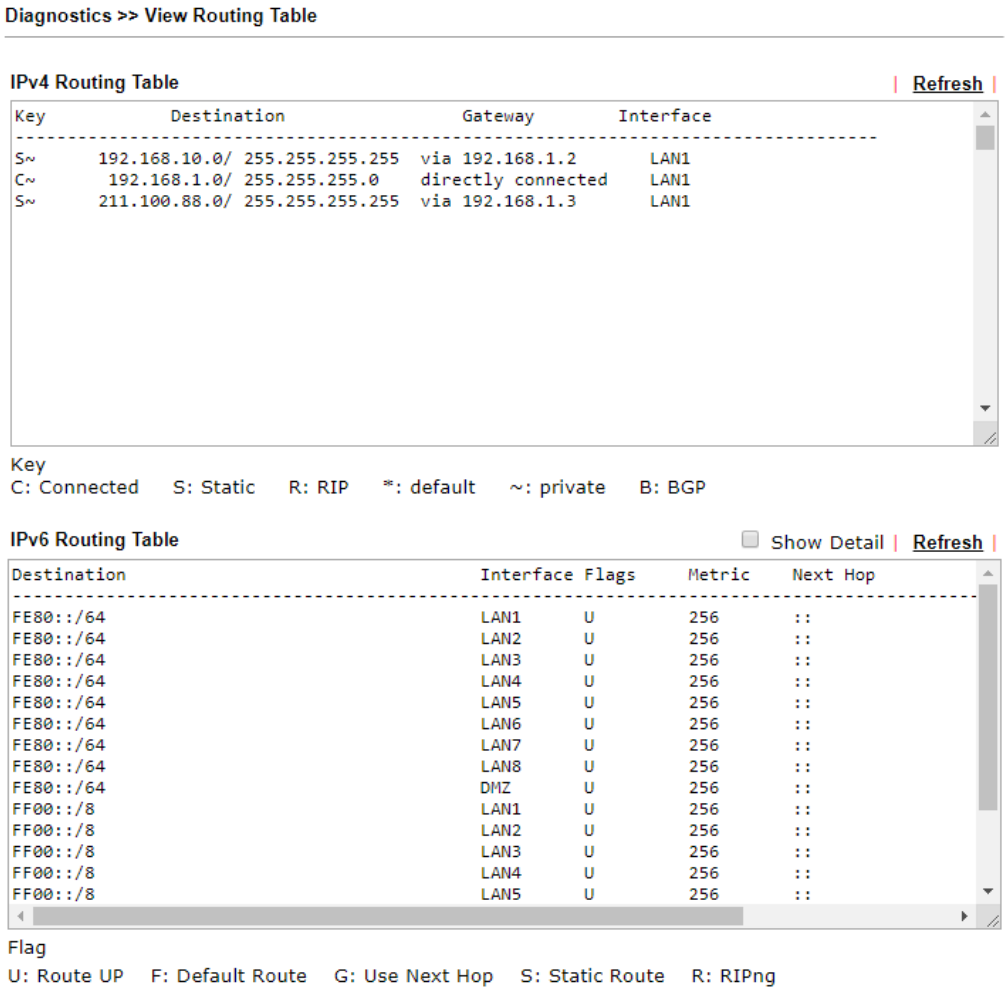
Hacer clic**Diagnóstico**y haga clic**Activación de marcación de salida**para abrir la página web. La conexión a Internet (p. ej., PPPoE) se activa mediante el envío de un paquete desde la dirección IP de origen.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Formato decodificado	Muestra la dirección IP de origen (local), la dirección IP de destino (remota), el protocolo y la longitud del paquete.
Actualizar	Haz clic para recargar la página.

Hacer clic**Diagnóstico**y haga clic**Tabla de ruteo**para abrir la página web.

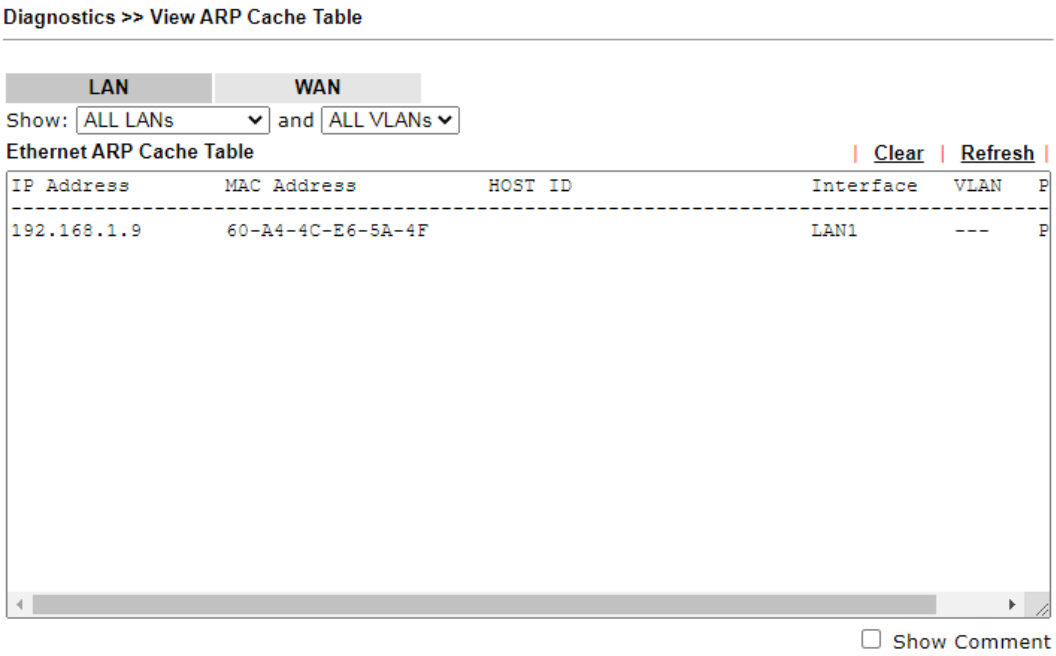


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Actualizar	Haz clic para recargar la página.

IX-1-3 Tabla de caché ARP

Hacer clic**Diagnóstico**y haga clic**Tabla de caché ARP**para ver el contenido de la memoria caché ARP (Protocolo de resolución de direcciones) que se encuentra en el enrutador. La tabla muestra una asignación entre una dirección de hardware Ethernet (Dirección MAC) y una dirección IP.



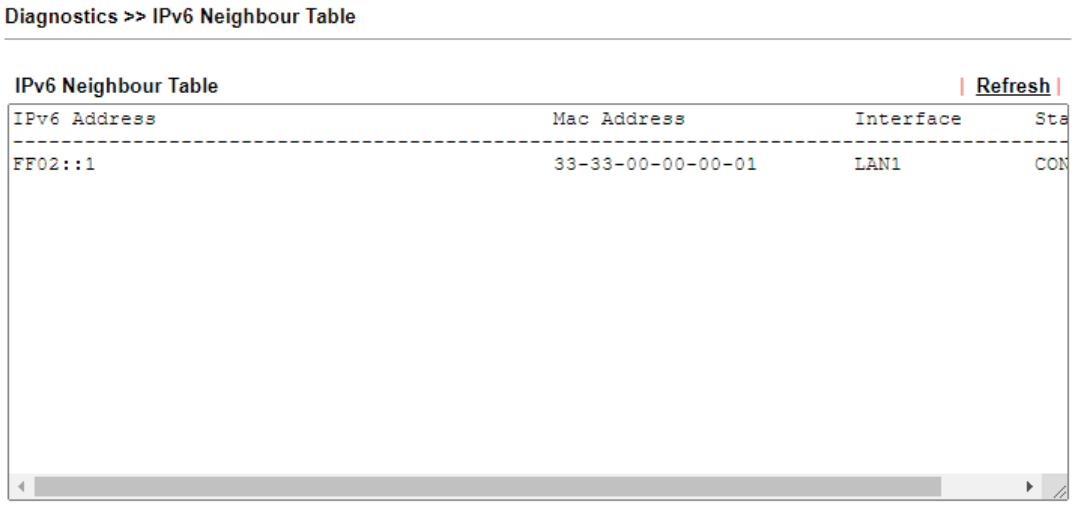
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Espectáculo	Especifique LAN y VLAN para mostrar información relacionada. De forma predeterminada, esta página mostrará toda la información sobre LAN y VLAN.
Actualizar	Haz clic para recargar la página.

IX-1-4 Tabla de vecinos IPv6

La tabla muestra una asignación entre una dirección de hardware Ethernet (Dirección MAC) y una dirección IPv6. Esta información es útil para diagnosticar problemas de red, como conflictos de direcciones IP, etc.

Hacer clic**Diagnóstico**y haga clic**Tabla de vecinos IPv6**para abrir la página web.



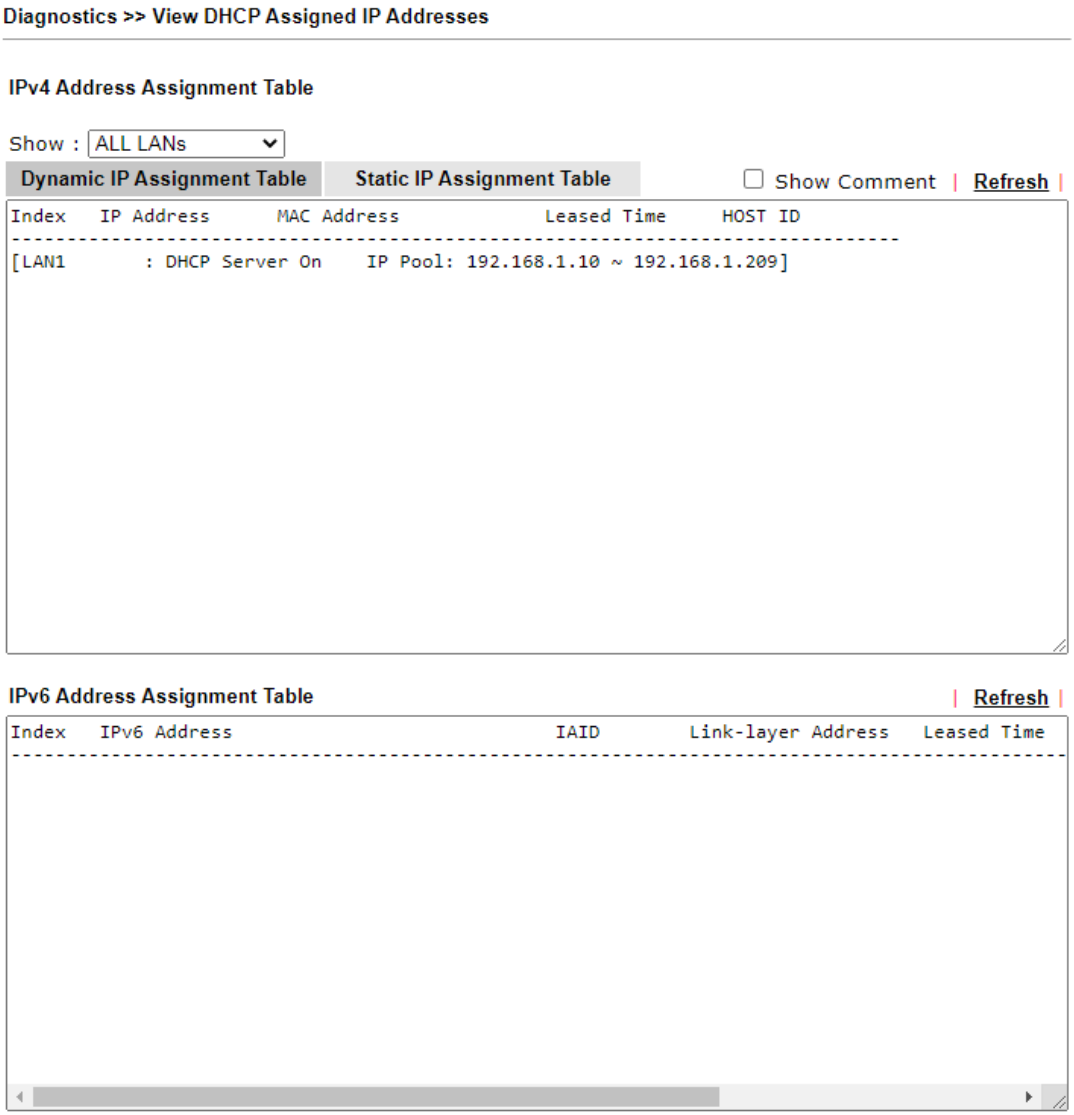
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Actualizar	Haz clic para recargar la página.

IX-1-5 Tabla DHCP

La instalación proporciona información sobre las asignaciones de direcciones IP. Esta información es útil para diagnosticar problemas de red, como conflictos de direcciones IP, etc.

Hacer clic**Diagnóstico**y haga clic**Tabla DHCP**para abrir la página web.

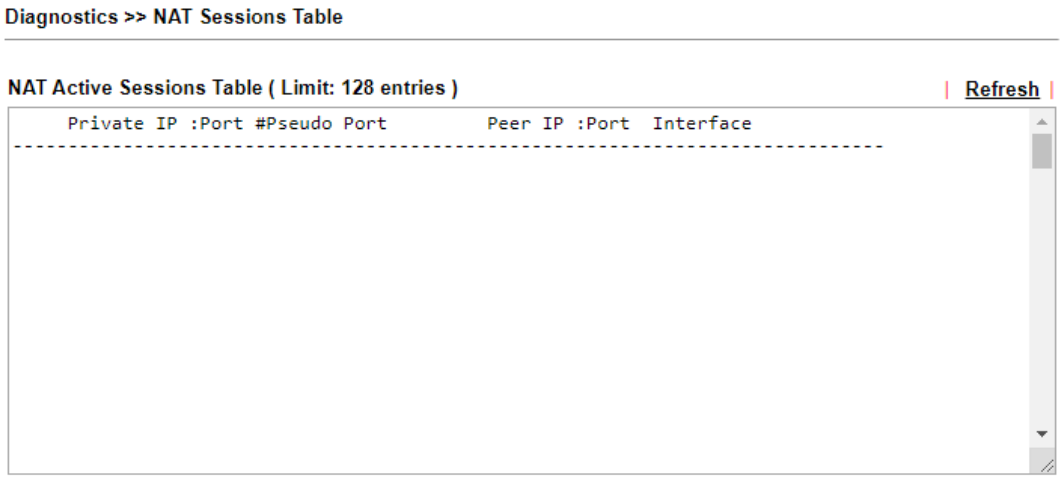


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Índice	Muestra el número de elemento de conexión.
Dirección IP	Muestra la dirección IP asignada por este enrutador para la PC especificada.
Dirección MAC	Muestra la dirección MAC para la PC especificada a la que DHCP le asignó la dirección IP.
tiempo arrendado	Muestra el tiempo arrendado de la PC especificada.
ID DE ANFITRIÓN	Muestra el nombre de ID de host de la PC especificada.
Actualizar	Haz clic para recargar la página.

IX-1-6 Tabla de sesiones NAT

Hacer clic**Diagnóstico**y haga clic**Tabla de sesiones NAT**para abrir la página de lista.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
IP privada: Puerto	Indica la dirección IP de origen y el puerto de la PC local.
# Pseudo Puerto	Indica el puerto temporal del router utilizado para NAT.
IP del mismo nivel:Puerto	Indica la dirección IP de destino y el puerto del host remoto.
Interfaz	Muestra el número que representa para diferentes interfaces.
Actualizar	Haz clic para recargar la página.

IX-1-7 Tabla de caché de DNS

Hacer clic**Diagnóstico**y haga clic**Tabla de caché de DNS**para abrir la página web.

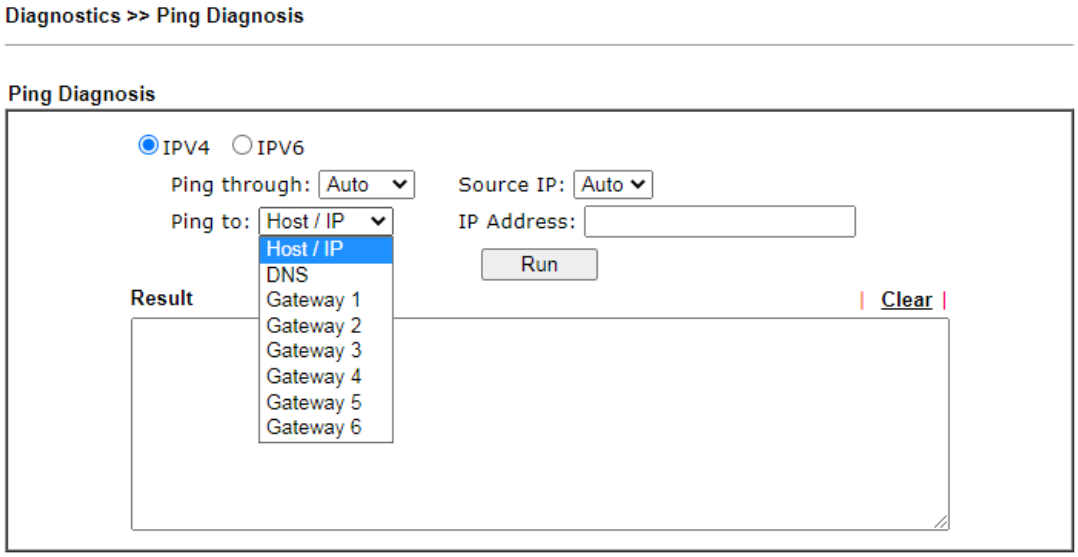
El registro del nombre de dominio y la dirección IP de mapeo para responder a la consulta de DNS desde la LAN se almacenarán temporalmente en el caché del enrutador Vigor y se mostrarán en**Diagnóstico >> Tabla de caché de DNS**.

Los ajustes disponibles se explican a continuación:

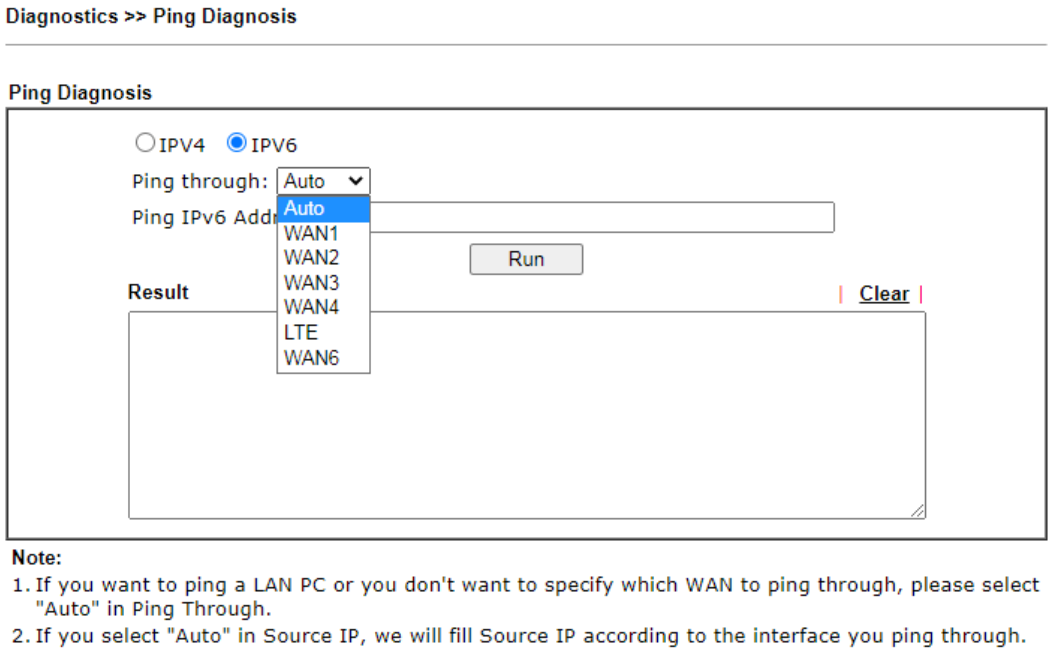
Artículo	Descripción
Claro	Haga clic en este enlace para eliminar el resultado de la ventana.
Actualizar	Haz clic para recargar la página.
Cuando el TTL de una entrada es mayor que....	Marque la casilla Ingrese el valor de TTL (tiempo de vida) para cada entrada. Hacer clic**DE ACUERDO**para habilitar dicha función. Significa que cuando el valor TTL de cada consulta de DNS alcanza el umbral del valor especificado aquí, el registro correspondiente se eliminará de la memoria caché del enrutador automáticamente.

IX-1-8 Diagnóstico de ping

Hacer clic**Diagnóstico**y haga clic**Diagnóstico de ping**para abrir la página web.



o



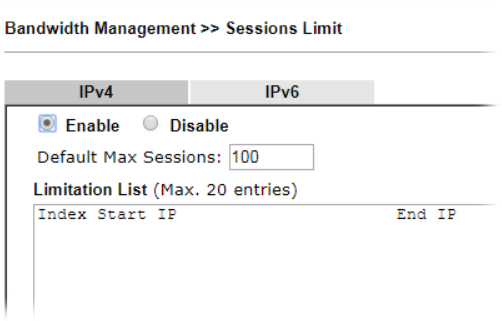
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
IPV4 /IPV6	Elija la interfaz para dicha función.
Hacer ping a través	Utilice la lista desplegable para elegir la interfaz WAN/LTE por la que desea hacer ping o elija**Auto**a ser determinado por el enrutador automáticamente.

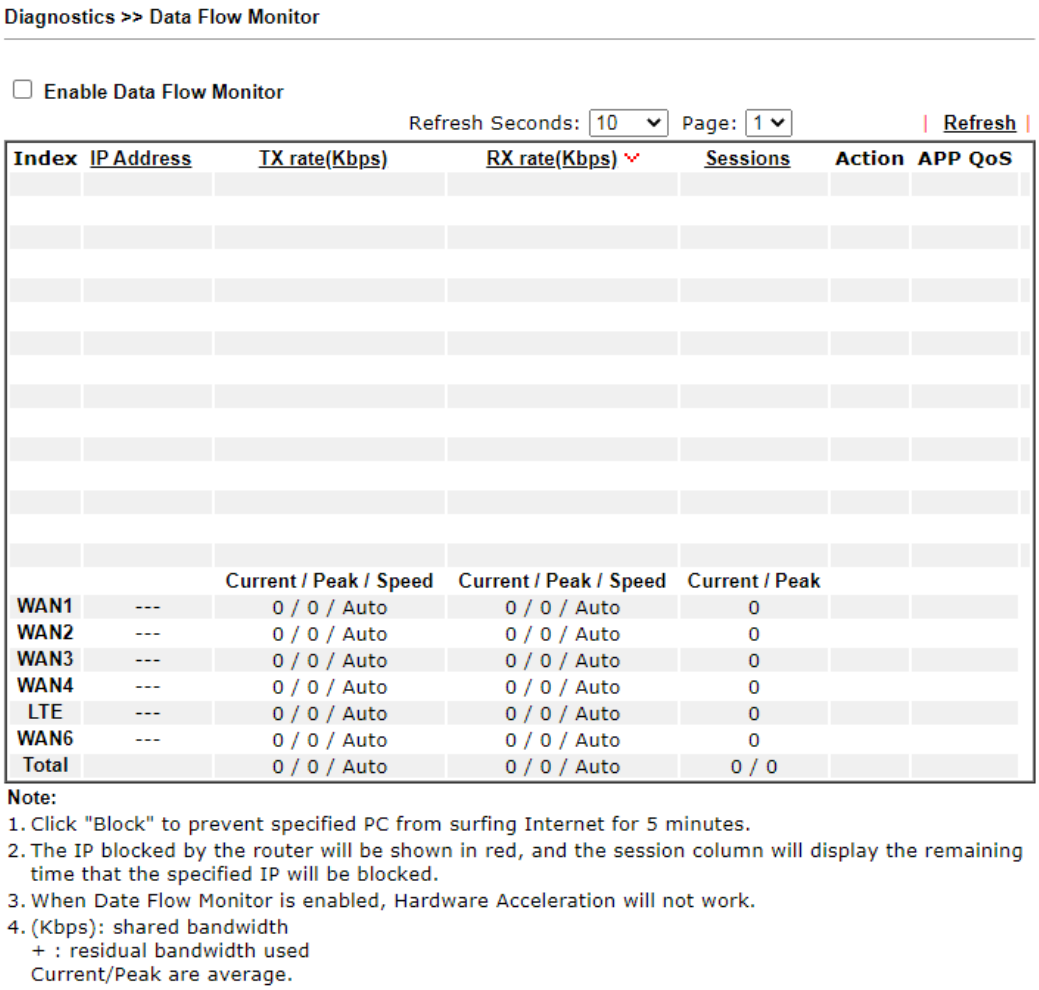
hacer ping a	Utilice la lista desplegable para elegir el destino al que desea hacer ping.
Dirección IP	Ingrese la dirección IP del Host/IP al que desea hacer ping.
Hacer ping a la dirección IPv6	Ingrese la dirección IPv6 a la que desea hacer ping.
Correr	Haga clic en este botón para iniciar el trabajo de ping. El resultado se mostrará en la pantalla.
Claro	Haga clic en este enlace para eliminar el resultado de la ventana.

Monitor de flujo de datos IX-1-9

Esta página muestra el procedimiento de ejecución de la dirección IP monitoreada y actualiza los datos en un intervalo de varios segundos. La dirección IP que se muestra aquí está configurada en Administración de ancho de banda. Debe habilitar el límite de ancho de banda de IP y el límite de sesión de IP antes de invocar Data Flow Monitor. De lo contrario, aparecerá un cuadro de diálogo de notificación para recordarle que lo habilite.



Hacer clic**Diagnóstico**y haga clic**Monitoreo de flujo de datos**para abrir la página web. Puedes hacer clic**Dirección IP**, **tasa de transmisión**,**tasa de RX**o**Sesión**enlace para organizar la visualización de datos.



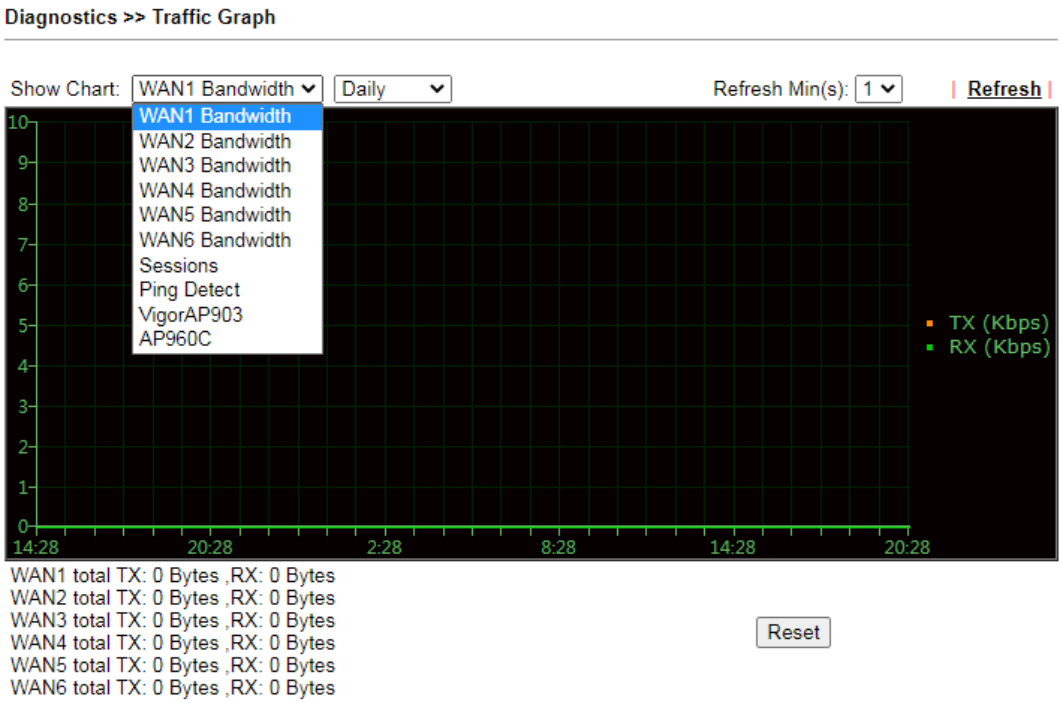
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar el monitor de flujo de datos	Marque esta casilla para habilitar esta función.
Actualizar segundos	Utilice la lista desplegable para elegir el intervalo de tiempo de actualización del flujo de datos que realizará el sistema automáticamente.
Actualizar	Haga clic en este enlace para actualizar esta página manualmente.
Índice	Muestra el número del flujo de datos.
Dirección IP	Muestra la dirección IP del dispositivo monitoreado.
Tasa de transmisión (kbps)	Muestra la velocidad de transmisión del dispositivo monitoreado.
Tasa de RX (kbps)	Muestra la velocidad de recepción del dispositivo monitoreado.
Sesiones	Muestre el número de sesión que especificó en la página web Limitar sesión.
Acción	**Bloquear**-puede evitar que la PC específica acceda a Internet en 5 minutos. **Desatascar**–El dispositivo con la dirección IP se bloqueará durante cinco minutos. El tiempo restante se mostrará en la columna de la sesión. Haga clic en él para cancelar el bloqueo de la dirección IP.
Calidad de servicio de la aplicación	Utilice la lista desplegable para cambiar la prioridad en la transmisión de datos para la dirección IP especificada (host).

Corriente/Pico/Velocidad	**Actual**significa la tasa de transmisión actual y la tasa de recepción para la interfaz WAN. **Cima**significa el valor pico más alto detectado por el enrutador en la transmisión de datos. **Velocidad**significa la velocidad de línea especificada en **WAN>>Configuración general**. Si no especifica ninguna tarifa en esa página, aquí se mostrará **Auto**en cambio.

IX-1-10 Gráfico de tráfico

Hacer clic**Diagnóstico**y haga clic**Gráfico de tráfico**para abrir la página web. Elija WAN1/WAN2/WAN3/WAN4/WAN5/WAN6 Ancho de banda, Sesiones, Ping Detect, diario o semanal para ver diferentes gráficos de tráfico. Hacer clic **Reiniciar**para poner a cero los datos acumulados de RX/TX (recibidos y transmitidos) de WAN. Hacer clic**Actualizar** para renovar la gráfica en cualquier momento.

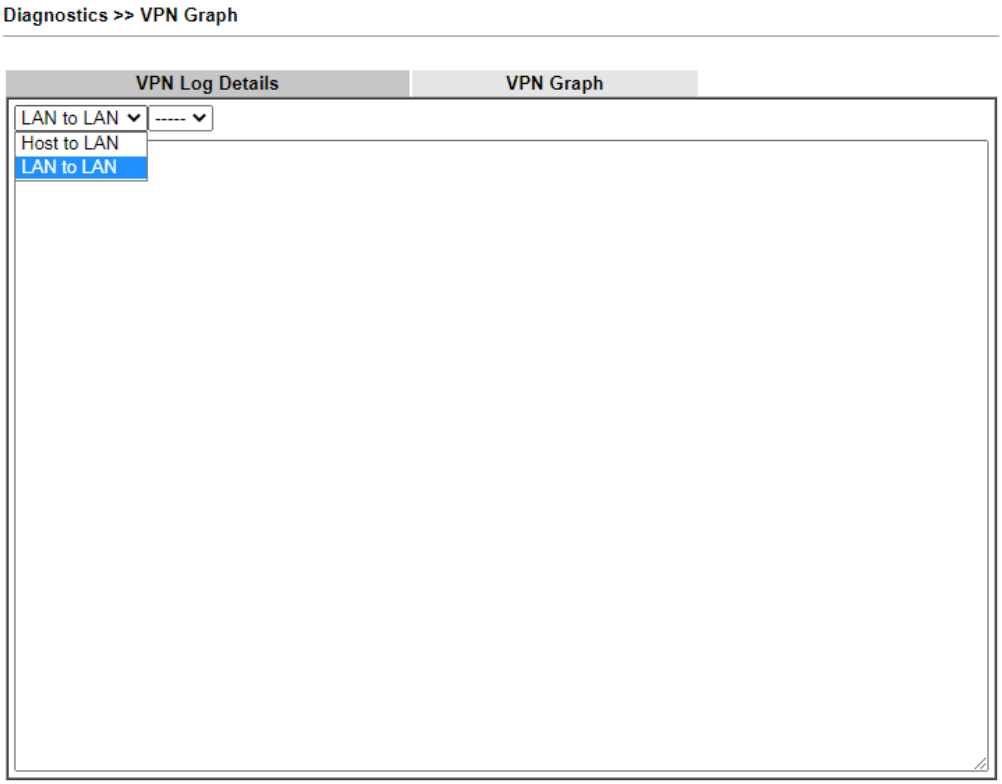


El eje horizontal representa el tiempo. Sin embargo, el eje vertical tiene diferentes significados. Para el gráfico de ancho de banda WAN1/WAN2/WAN3/WAN4/WAN5/WAN6, los números que se muestran en el eje vertical representan los números de los paquetes transmitidos y recibidos en el pasado.

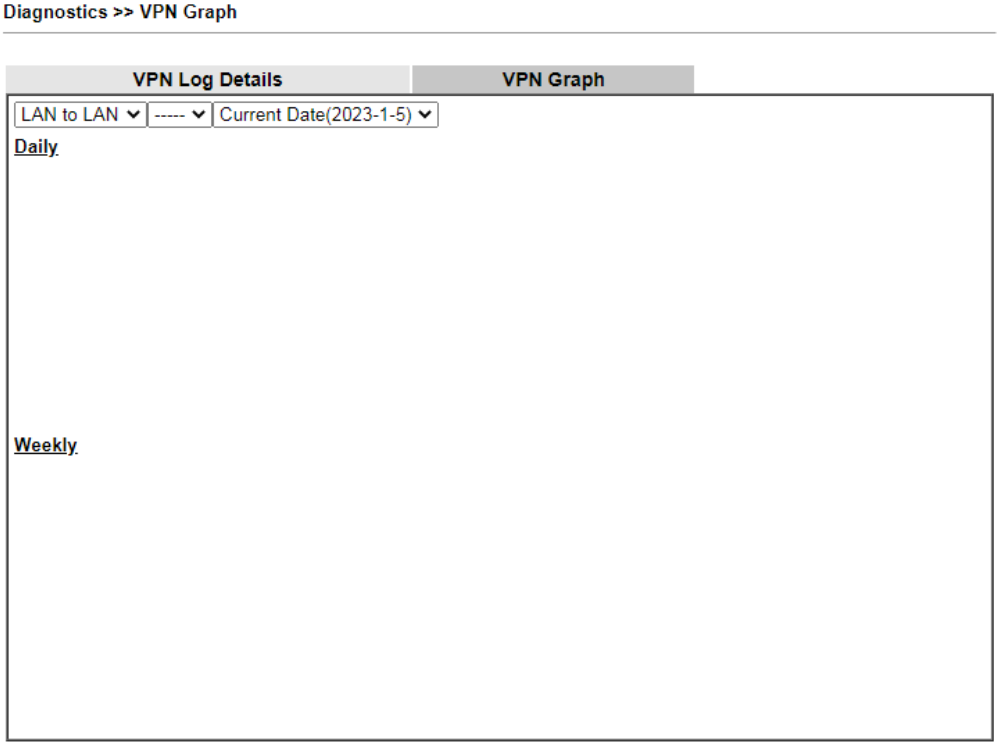
Para el gráfico de sesiones, los números que se muestran en el eje vertical representan los números de las sesiones NAT durante el pasado.

Gráfico VPN IX-1-11

Hacer clic**Diagnóstico**y haga clic**Gráfico VPN**para abrir la página web.

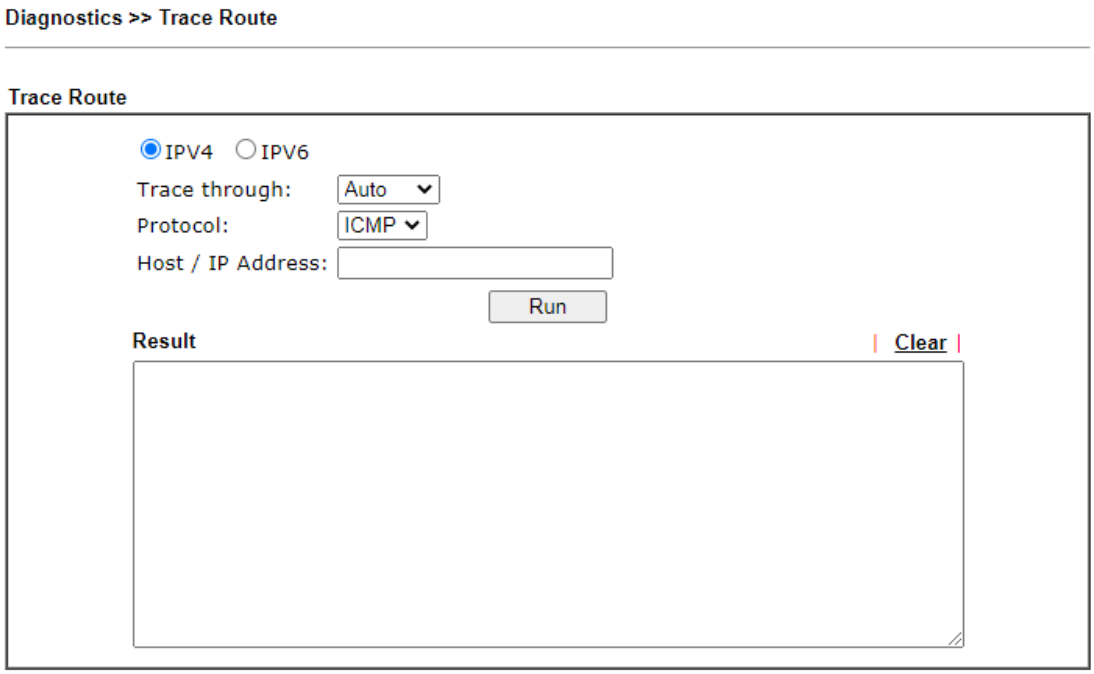


y

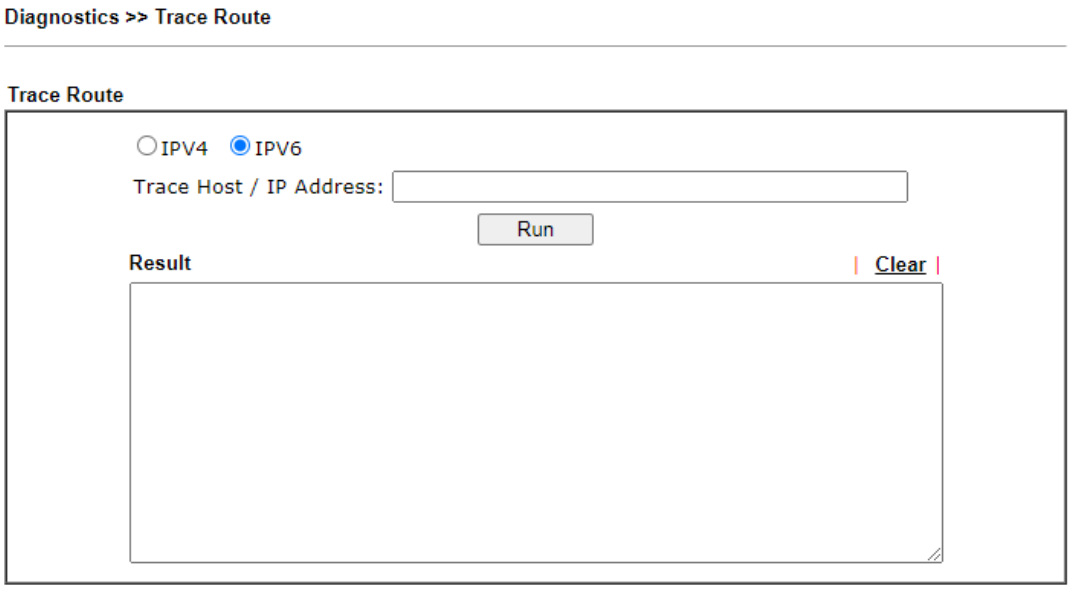


IX-1-12 Trazar ruta

Hacer clic**Diagnóstico**y haga clic**Trazar ruta**para abrir la página web. Esta página le permite rastrear las rutas desde el enrutador hasta el host. Simplemente ingrese la dirección IP del host en el cuadro y haga clic en **Correr**. El resultado del seguimiento de la ruta se mostrará en la pantalla.



o



Los ajustes disponibles se explican a continuación:

Artículo	**Descripción**
IPv4 / IPv6	Haga clic en uno de ellos para mostrar la información correspondiente.
Rastrear a través	Use la lista desplegable para elegir la interfaz a través de la cual desea hacer ping.

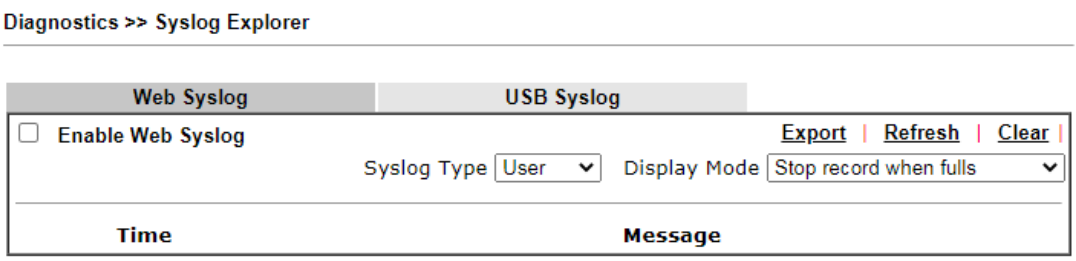
Protocolo	Utilice la lista desplegable para elegir el protocolo por el que desea hacer ping.
Servidor/Dirección IP	Indica la dirección IP del host.
Rastrear host/dirección IP	Indica la dirección IPv6 del host.
Correr	Haga clic en este botón para iniciar el trabajo de rastreo de rutas.
Claro	Haga clic en este enlace para eliminar el resultado de la ventana.

IX-1-13 Explorador de Syslog

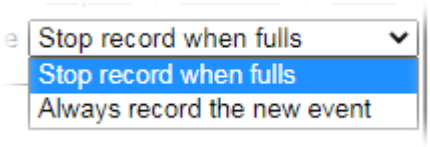
Dicha página proporciona syslog en tiempo real y muestra la información en la pantalla.

Para Web Syslog

Esta página muestra la hora y el mensaje para la configuración de Usuario/Firewall/llamada/WAN/VPN. Puedes comprobar**Habilitar Syslog Web,**especifique el tipo de Syslog y elija el modo de visualización que desee. Posteriormente, el evento de Syslog con el tipo especificado se mostrará para su referencia.

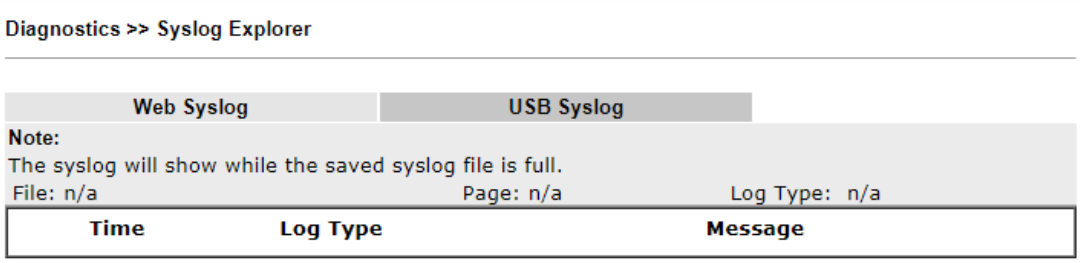


Los ajustes disponibles se explican a continuación:

Artículo	**Descripción**
Habilitar registro del sistema web	Marque esta casilla para habilitar la función de Web Syslog.
Tipo de registro del sistema	Utilice la lista desplegable para especificar un tipo de Syslog que se mostrará.
Exportar	Haga clic en este enlace para guardar los datos como un archivo.
Actualizar	Haga clic en este enlace para actualizar esta página manualmente.
Claro	Haga clic en este enlace para borrar la información de esta página.
Modo de visualización	Hay dos modos para que usted elija.  **Detener el registro cuando se llena -**Cuando la capacidad de syslog esté llena, el sistema dejará de grabar. **Grabe siempre el nuevo evento:**el sistema solo registrará los eventos más recientes.
Tiempo	Muestra la hora en que ocurrió el evento.
Mensaje	Muestra la información de cada evento.

Para registro de sistema USB

Esta página muestra el syslog registrado en el disco de almacenamiento USB.



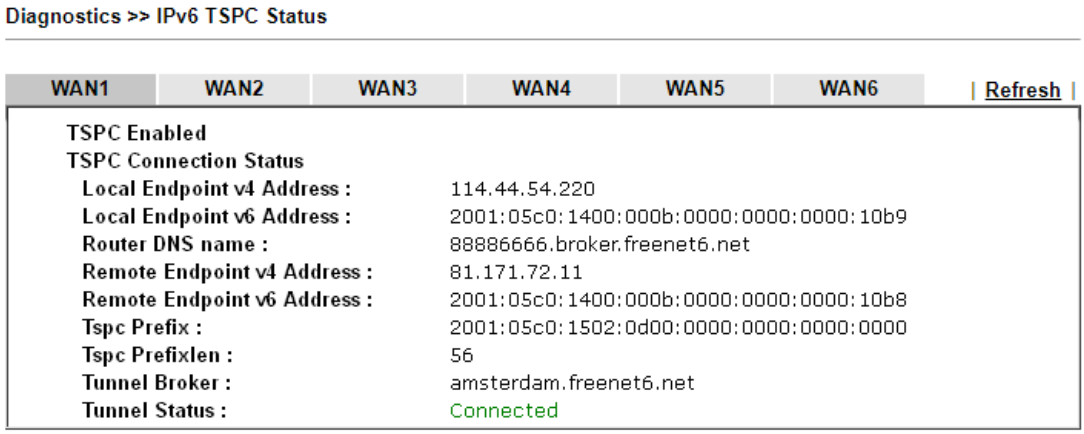
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Tiempo	Muestra la hora en que ocurrió el evento.
Tipo de registro	Mostrar el tipo de registro.
Mensaje	Muestra la información de cada evento.

IX-1-14 Estado de TSPC de IPv6

La página web de estado de IPv6 TSPC podría ayudarlo a diagnosticar el estado de conexión de TSPC.

Si TSPC se configuró correctamente, el enrutador mostrará la siguiente página cuando el usuario se conecte al agente de túnel con éxito.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Actualizar	Haga clic en este enlace para actualizar esta página manualmente.

IX-1-15 Estado de alta disponibilidad

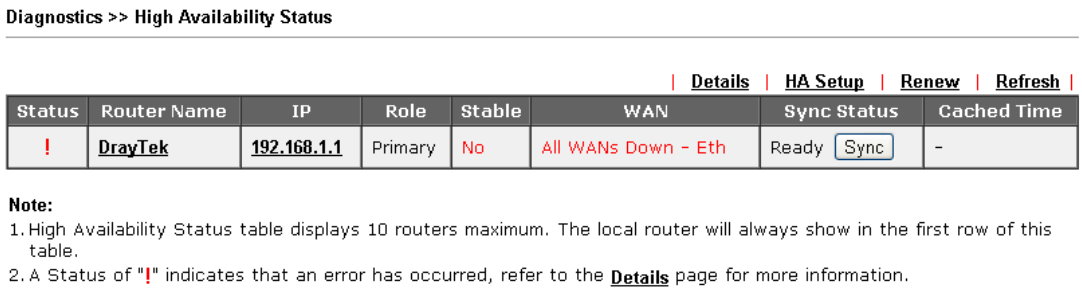
Todos los enrutadores bajo el mismo grupo DARP (Protocolo de resolución de direcciones DrayTek) se pueden ver en dicha página. Sin embargo, solo se mostrará información parcial del estado del enrutador.

Los enrutadores Vigor con las siguientes condiciones serán tratados como el mismo grupo DARP:

- alta disponibilidad habilitada

- el mismo método de redundancia
- el mismo ID de grupo
- la misma clave de autenticación
- la misma interfaz de gestión

Abierto**Diagnósticos>>Estado de alta disponibilidad**.



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Detalles/Atrás	**Detalles -**Haga clic en él para mostrar el estado detallado de la configuración de alta disponibilidad para el enrutador seleccionado. **Atrás**–Volver a la pagina anterior.
Configuración de alta disponibilidad	Haga clic para abrir**Aplicaciones>>Alta disponibilidad**para modificar la configuración.
Renovar	Haga clic para obtener el estado más reciente de otro enrutador (excepto el enrutador principal).
Actualizar	Haga clic en él para obtener el estado más reciente del enrutador principal.
Estado	**"!"**significa que ha ocurrido un error. Referirse a**Detallado** información y modificar la configuración de alta disponibilidad si es necesario.
Nombre del enrutador	Muestra el nombre del dispositivo.
IP	Muestra la dirección IPv4 de dicho enrutador.
Role	"Abajo" significa que la función de HA está deshabilitada. "Principal" significa que dicho enrutador representa el enrutador principal en HA. "Secundario" significa que dicho enrutador representa el enrutador secundario en HA.
Estable	"No" significa que aún no se ha determinado el enrutador principal. DARP está negociando. "SÍ" significa que se determina el enrutador principal.
PÁLIDO	"Al menos una UP" significa que al menos una interfaz WAN se conecta a Internet. "Todas las WAN inactivas" significa que ninguna interfaz WAN se conecta a Internet.
Estado de sincronización	"No listo" significa que la sincronización de la configuración no se puede ejecutar, o la sincronización de la configuración está deshabilitada, o la inicialización de la sincronización se ejecuta pero falla. "Listo" significa que la sincronización de la configuración está lista para ejecutarse. "Progresando" significa que la sincronización de la configuración está funcionando.

	“Error” significa que la sincronización de la configuración se ejecutó y falló; o nombre de modelo incorrecto. "Igual" significa que la configuración correspondiente es igual al enrutador principal.
Tiempo en caché	Muestra el período de tiempo desde la última vez que se obtuvo el estado más reciente de otro enrutador (excepto el enrutador principal).

Haga clic en el enlace de**Nombre del enrutador**,**IP**o**Detalles**, la siguiente página se mostrará en la pantalla.

Diagnostics >> High Availability Status >> Details

[Local Router] | Back | HA Setup | Renew | Refresh |

DrayTek			192.168.1.1(FE80::D567:1F16:1B69:8B7C)	
Role	**Stable**	**WAN**	**Sync Status**	**Cached Time**
Primary	No !	All WANs Down - Eth !	Ready Sync	-

Config Sync Status	Not Ready	**DHCPv6 Sync Status**	Ready
MAC	00:1d:aa:00:00:00	**HTTPs Port**	443
Model	Vigor2865ac	**Firmware Version**	4.0.4_RC2_STD
Enable High Availability	Off !	**Redundancy Method**	Active-Standby
Group ID	1	**Priority ID**	10
Authentication Key	draytek	**Management Interface**	LAN1
Update DDNS	Off	**Protocol**	IPv4
Virtual IPv4	Off !		
Virtual IPv6	On	LAN1	FE80::200:5EFF:FE00:101
		LAN2	FE80::200:5EFF:FE00:101
		LAN3	FE80::200:5EFF:FE00:101
		LAN4	FE80::200:5EFF:FE00:101
		LAN5	FE80::200:5EFF:FE00:101
		LAN6	FE80::200:5EFF:FE00:101
		LAN7	FE80::200:5EFF:FE00:101
		LAN8	FE80::200:5EFF:FE00:101
		DMZ	FE80::200:5EFF:FE00:101
Enable Config Sync	Off	**Config Sync Interval**	0 Day 0 Hour 15 Minute
Last Config Sync By	00:00:00:00:00:00		

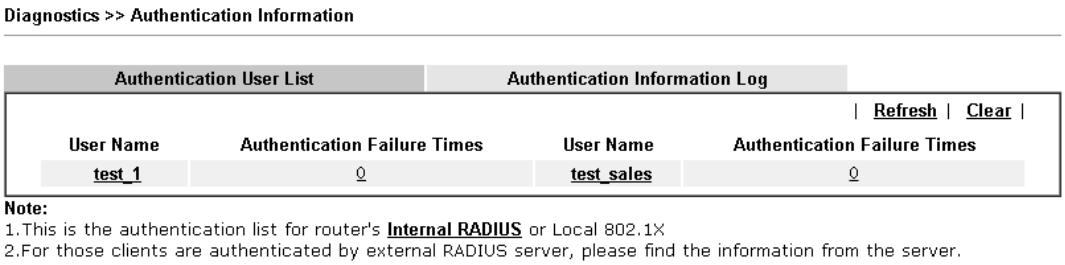
Note:
Displays up to 10 routers. Each router can show up to 9 Virtual IPs.

IX-1-16 Información de autenticación

Lista de usuarios de autenticación

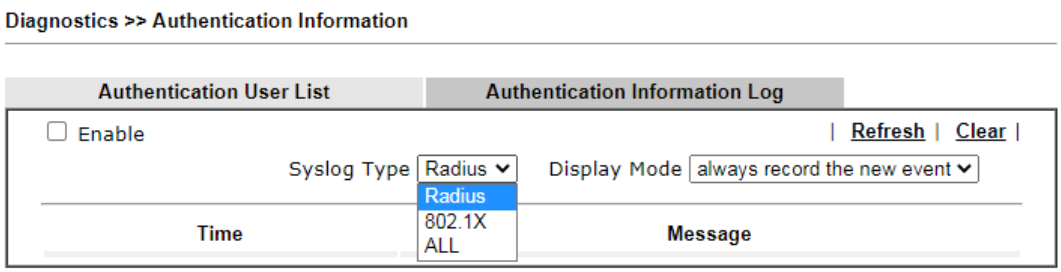
Dicha página muestra los trabajos de autenticación realizados por RADIUS interno o Local 802.1X.

Cuando el cursor del mouse se mueve al enlace del nombre debajo de Nombre de usuario, el mensaje de conexión (incluida la información de error de autenticación) sobre RADIUS interno o el servicio local 802.1X se mostrará en un cuadro de diálogo emergente.



Registro de información de autenticación

Esta página mostrará la información completa del registro de autenticación.



Los ajustes disponibles se explican a continuación:

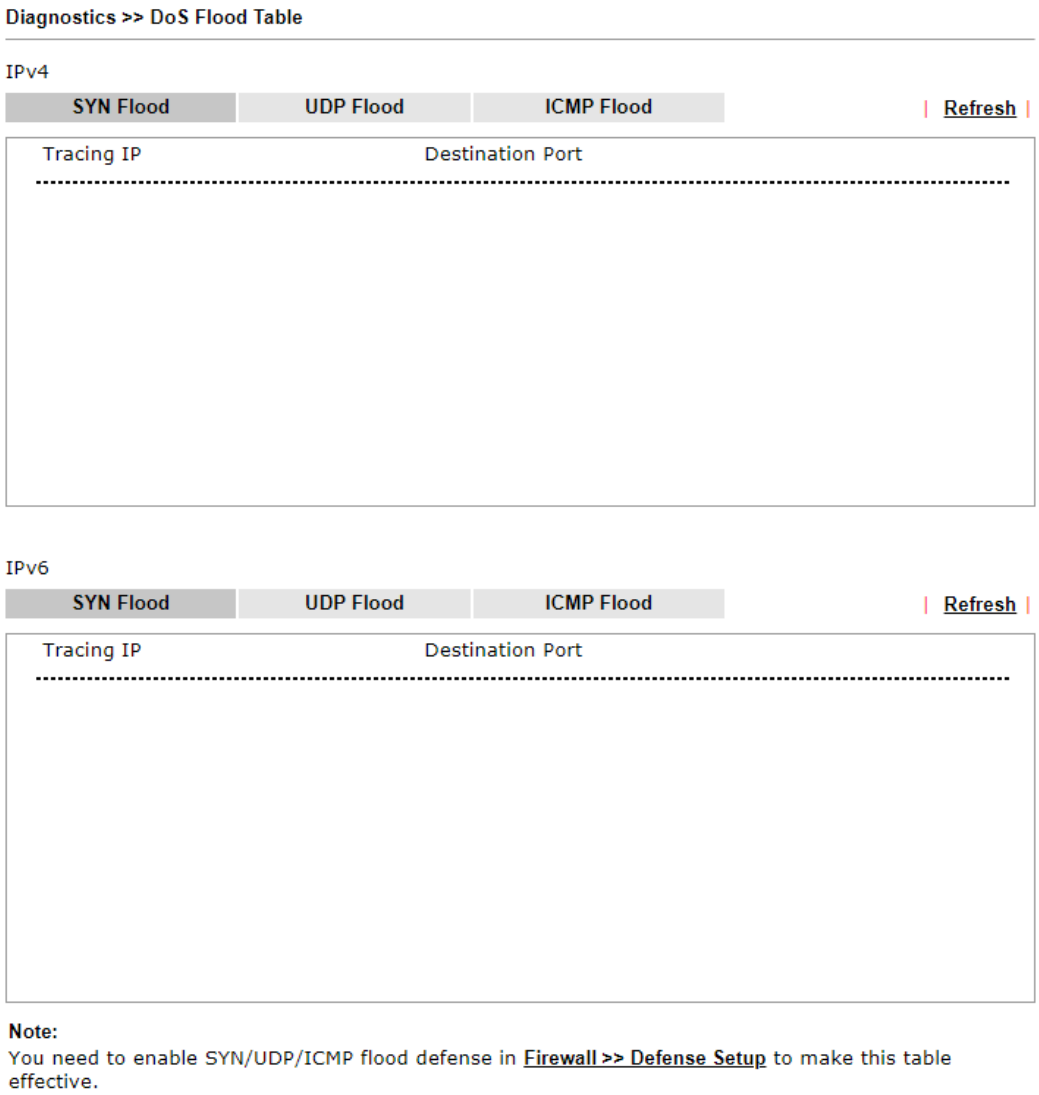
Artículo	Descripción
Permitir	Marque la casilla para habilitar dicha función.
Actualizar	Haga clic en él para actualizar la página actual.
Claro	Haga clic en él para eliminar todos los registros.
Tipo de registro del sistema	Especifique RADIUS, 802.1X o Todo para mostrar el registro de información de autenticación relacionada.
Modo de visualización	Elija el modo en que desea mostrar la información relacionada en la siguiente tabla. - **Detener el registro cuando se llena -**Cuando la capacidad del registro CVM esté llena, el sistema dejará de grabar. - **Grabe siempre el nuevo evento:**el sistema solo registrará los eventos más recientes.
Tiempo	Muestra la hora en que el usuario se autenticó mediante la serie Vigor2927.
Mensaje	Muestra la información de autenticación realizada por la serie Vigor2927.

IX-1-17 Tabla de inundaciones DoS

Esta página puede mostrar el contenido de la conexión IP detectada por el mecanismo DoS Flooding Defense. Es útil y conveniente para los ingenieros de redes (p. ej., ingenieros de MIS) inspeccionar el entorno de la red para averiguar si hay alguna conexión anormal.

La información de la IP rastreada y el puerto de destino utilizado para los ataques SYN Flood, UDP Flood y ICMP Flood se detectarán y mostrarán respectivamente en diferentes páginas.

Además, la dirección IP detectada y sospechosa de atacar el sistema de red se puede bloquear en breve haciendo clic en el**Bloquear**botón que se muestra en las páginas de SYN Flood, UDP Flood y ICMP Flood.

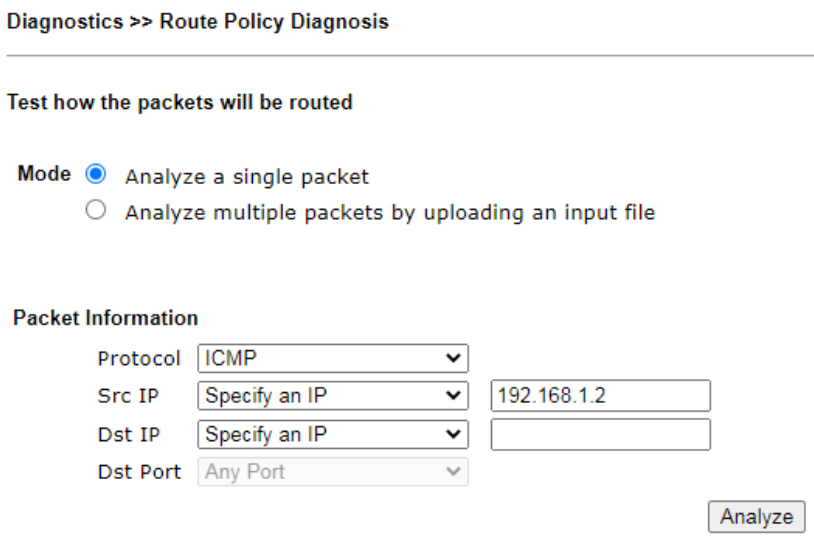


Información

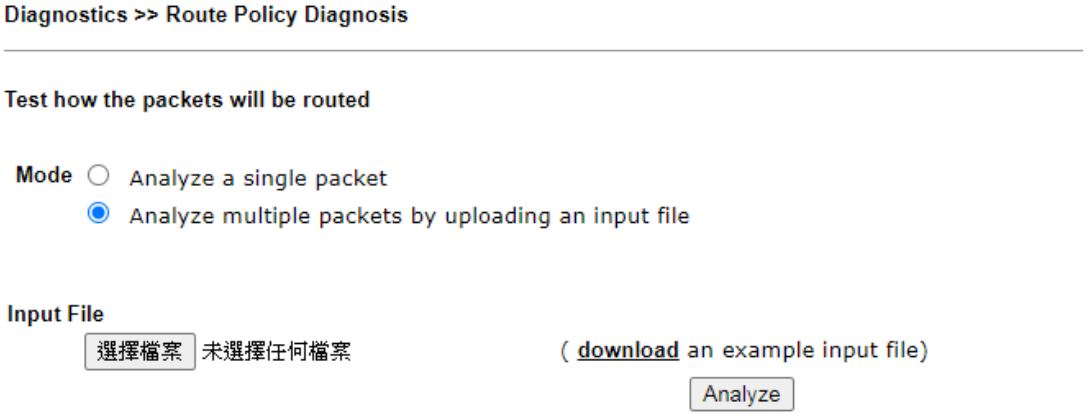
El icono - (⊗) - significa que algo anda mal (p. ej., atacar el sistema) con esa dirección IP.

IX-1-18 Diagnóstico de Política de Ruta

Con el análisis realizado por dicha página, se puede rastrear la posible ruta (ruta estática, tabla de enrutamiento o ruta de política) de los paquetes enviados fuera del enrutador.

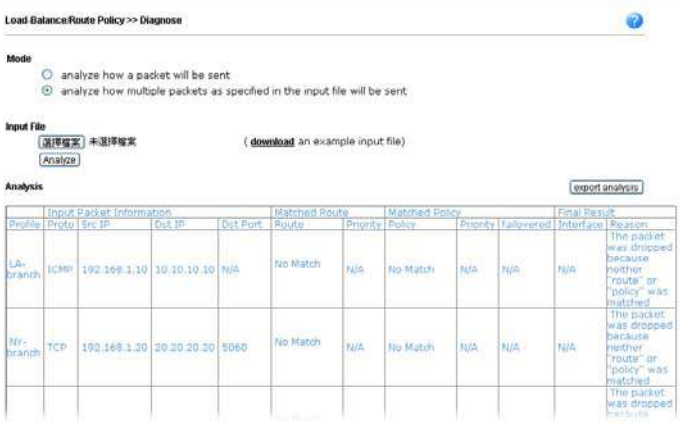


o



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Modo	**Analizar un solo paquete**–Elija dicho modo para hacer que el enrutador Vigor analice cómo se enviará un solo paquete mediante una política de ruta. **Analiza múltiples paquetes**... - Elija dicho modo para hacer que el enrutador Vigor analice cómo una política de ruta enviará múltiples paquetes en un archivo específico.
Información del paquete	Especifique la naturaleza de los paquetes que analizará el enrutador Vigor. **ICMP/UDP/TCP/ANY**-Especificar un protocolo para el diagnóstico. **IP de origen**–Escriba una dirección IP como IP de origen.

	DST IP–Escriba una dirección IP como IP de destino. **puerto de horario de verano**–Utilice la lista desplegable para especificar el puerto de destino. **Analizar**–Haga clic en él para realizar el trabajo de análisis. El resultado analizado se mostrará en la página..
Fichero de entrada	Está disponible cuando se selecciona Analizar varios paquetes... como **Modo.** **Seleccionar**–Haga clic en el enlace de descarga para obtener un archivo de ejemplo en blanco. Luego, haga clic en dicho botón para seleccionar ese archivo ".csv" en blanco para guardar el resultado del análisis. **Analizar**–Haga clic en él para realizar el trabajo de análisis. El resultado analizado se mostrará en la página. Si es necesario, haga clic en **análisis de exportación** para exportar el resultado como un archivo.  Tenga en cuenta que el análisis se basó en la configuración actual de "política de ruta/equilibrio de carga", no garantizamos que sea 100 % igual al caso real.

IX-2 Comprobación de si el estado del hardware es correcto o no

Siga los pasos a continuación para verificar el estado del hardware.

1. Compruebe la línea de alimentación y las conexiones del cable WLAN/LAN. Referirse a "**Instalación de hardware I-2"**para detalles.
2. Encienda el enrutador. Asegúrate que**LED DE ACTO**parpadea una vez por segundo y el correspondiente **LED de LAN**es brillante.

3. Si no, significa que hay algún problema con el estado del hardware. Simplemente de vuelta a **"Instalación de hardware I-2"**para ejecutar de nuevo la instalación del hardware. Y luego, inténtalo de nuevo.

IX-3 Comprobación de si la configuración de la conexión de red en su computadora es correcta o no

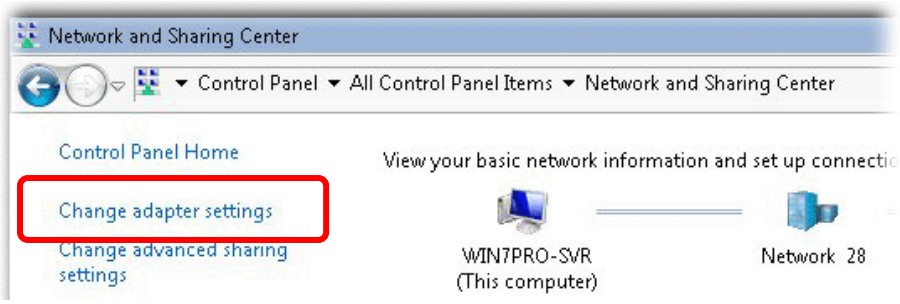
A veces, la falla del enlace ocurre debido a una configuración de conexión de red incorrecta. Después de probar la sección anterior, si el enlace sigue fallando, siga los pasos que se enumeran a continuación para asegurarse de que la configuración de la conexión de red sea correcta.

Para ventanas

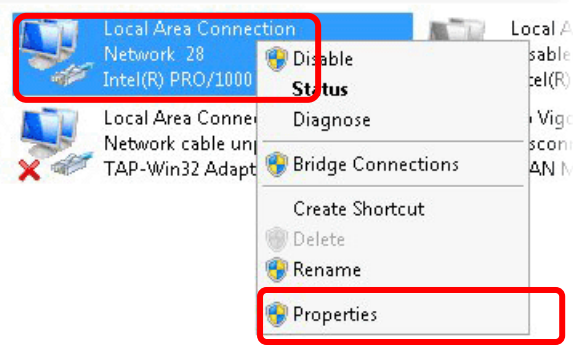
Información	El ejemplo se basa en Windows 7. En cuanto a los ejemplos para otros sistemas operativos, consulte los pasos similares o busque notas de soporte en www.DrayTek.com.

1. Abierto**Todos los programas>>Primeros pasos>>Panel de control.**Hacer clic**Redes y recursos compartidos.**

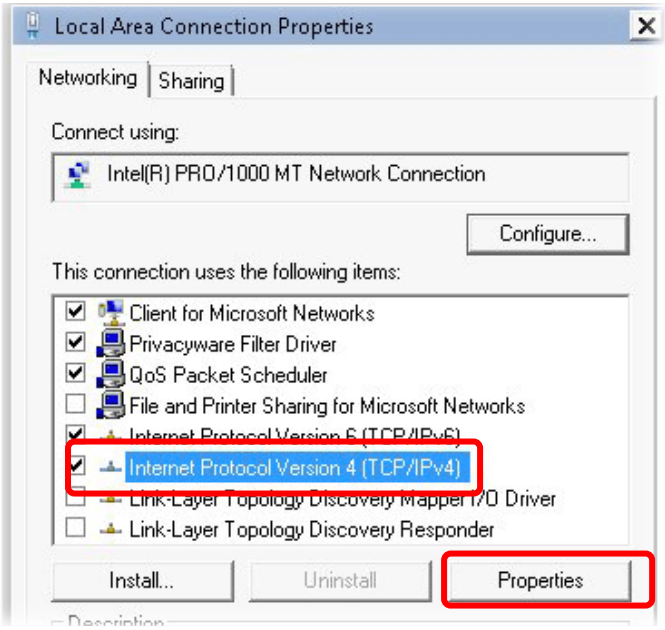
2. En la siguiente ventana, haga clic en**Cambiar la configuración del adaptador**.



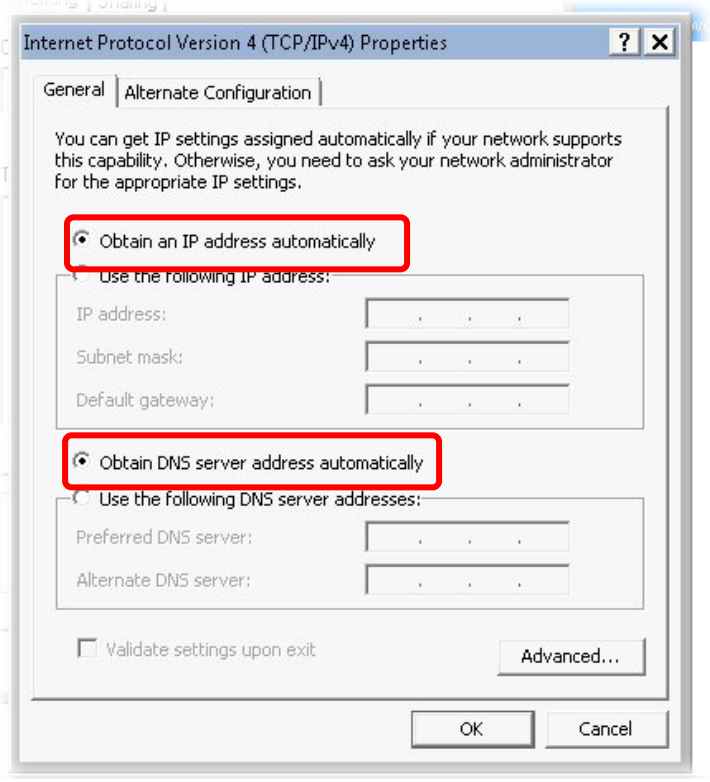
3. Se mostrarán iconos de conexión de red en la ventana. Haga clic derecho en**Conexión de área local**y haga clic en**Propiedades**.



4. Seleccione**Protocolo de Internet versión 4 (TCP/IP)**y luego haga clic**Propiedades**.



5. Seleccione**Obten una direccion IP automaticamente**y**Obtener la dirección del servidor DNS automáticamente**. Finalmente, haga clic en**DE ACUERDO**.

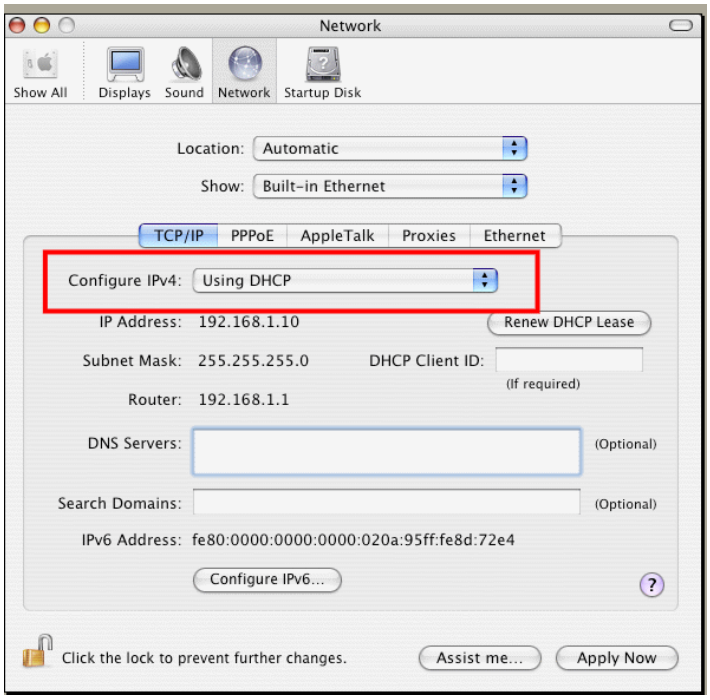


Para sistema operativo Mac

1. Haga doble clic en el sistema operativo Mac utilizado actualmente en el escritorio.

2. Abra el**Solicitud**carpeta y entrar**Red**.

3. En el**Red**pantalla, seleccione**Uso de DHCP**de la lista desplegable de Configurar IPv4.



IX-4 Hacer ping al enrutador desde su computadora

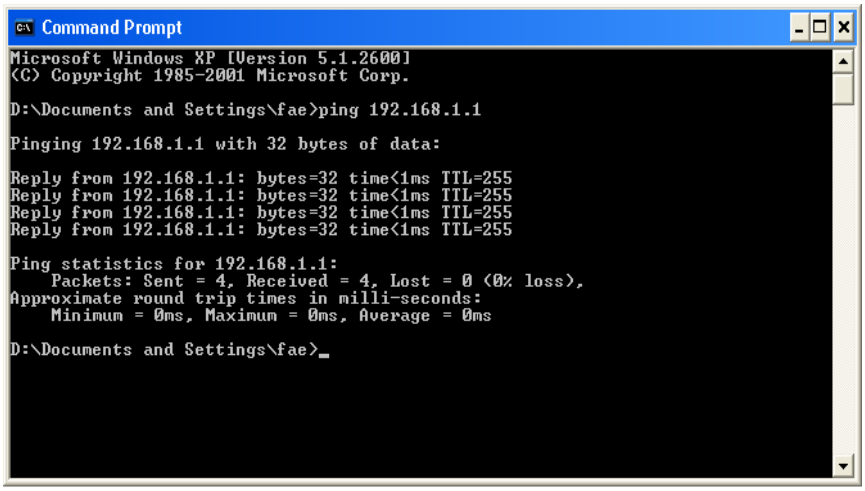
La dirección IP de puerta de enlace predeterminada del enrutador es 192.168.1.1. Por alguna razón, es posible que deba usar el comando "ping" para verificar el estado del enlace del enrutador.**Lo más importante es que la computadora recibirá una respuesta de 192.168.1.1.**De lo contrario, verifique la dirección IP de su computadora. Le sugerimos que configure la conexión de red como**obtener IP automáticamente**. (Por favor refiérase a la sección anterior IX-3)

Siga los pasos a continuación para hacer ping al enrutador correctamente.

Para ventanas

1. Abra el**Dominio**Ventana de solicitud (de**Menú Inicio > Ejecutar**).

2. Tipo**cmd**(para Windows 7/8/10/11). Aparecerá el cuadro de diálogo de comandos de DOS.



3. Escriba ping 192.168.1.1 y presione [Enter]. Si el enlace está bien, la línea de**“Responde desde 192.168.1.1:bytes=32 tiempo<1ms TTL=255”**aparecerá.

4. Si la línea no aparece, verifique la configuración de la dirección IP de su computadora.

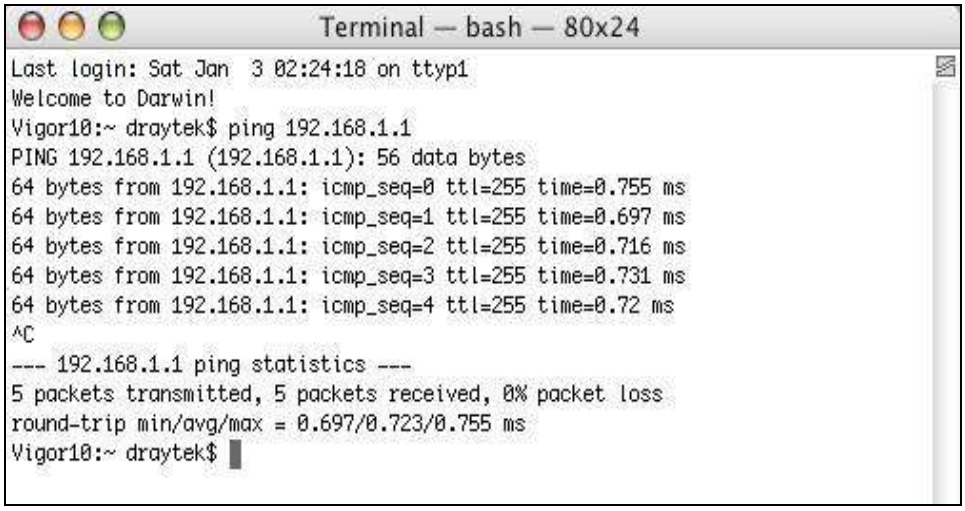
Para Mac OS (Terminal)

1. Haga doble clic en el MacO utilizado actualmente en el escritorio.

2. Abra el**Solicitud**carpeta y entrar**Utilidades**.

3. Doble clic**Terminal**. Aparecerá la ventana Terminal.

4. Tipo**ping 192.168.1.1**y presione [Entrar]. Si el enlace está bien, la línea de**“64 bytes de 192.168.1.1: icmp_seq=0 ttl=255 tiempo=xxxx ms**" aparecerá.


Terminal — bash — 80x24
Last login: Sat Jan 3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$

IX-5 Comprobación de si la configuración del ISP está bien o no

Si la conexión WAN no puede estar activa, verifique si los LED (de acuerdo con las explicaciones de los LED enumeradas en la sección I-1-1, Indicadores y conectores) son correctos o no. Si los LED están apagados, por favor:

-Cambiar el**Tipo físico**de**Autonegociación**a otros valores (por ejemplo, dúplex completo de 100M).

-A continuación, cambie el tipo físico de módem (p. ej., DSL/FTTX(GPON)/Cable módem) ofrecido por el ISP con el mismo valor configurado en el enrutador Vigor. Compruebe si los LED del enrutador Vigor están encendidos o no.

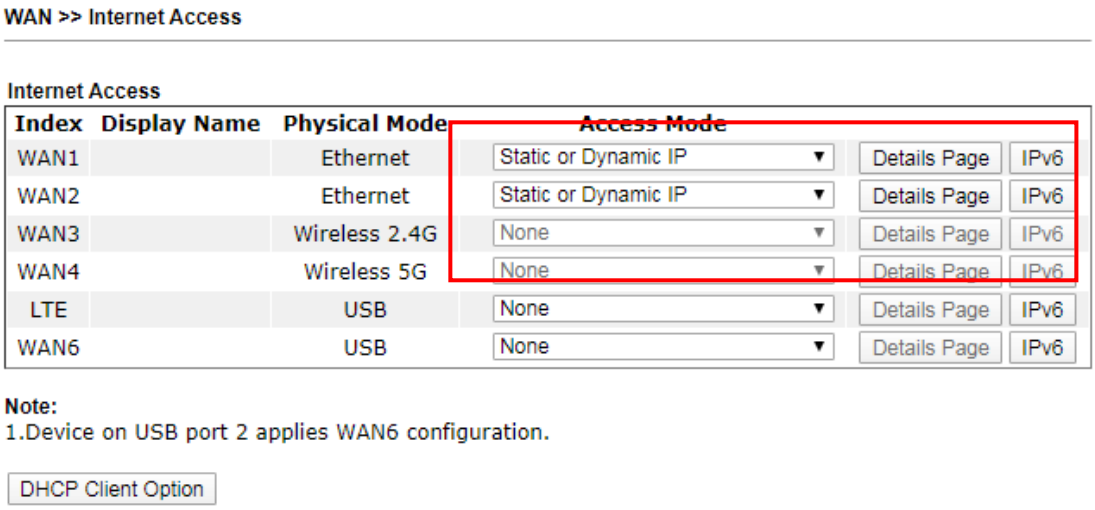
-De lo contrario, instale un conmutador adicional para conectar tanto el enrutador Vigor como el módem ofrecido por el ISP. Luego, verifique si los LED en el enrutador Vigor están encendidos o no.

-Si el problema de los LED no se puede resolver con las medidas anteriores, póngase en contacto con el distribuidor más cercano o envíe un correo electrónico a DrayTek FAE para obtener asistencia técnica.

-Compruebe si los ajustes que ofrece el ISP están bien configurados o no.

Cuando los LED están encendidos y correctos, pero la conexión WAN aún no puede estar activa, por favor:

-Abierto**WAN >> Acceso a Internet**y luego verifique si la configuración del ISP está configurada correctamente. Hacer clic**Página de detalles**de WAN1~WAN6 para revisar las configuraciones que configuró previamente.



IX-6 Problemas para la conexión de red 3G/4G

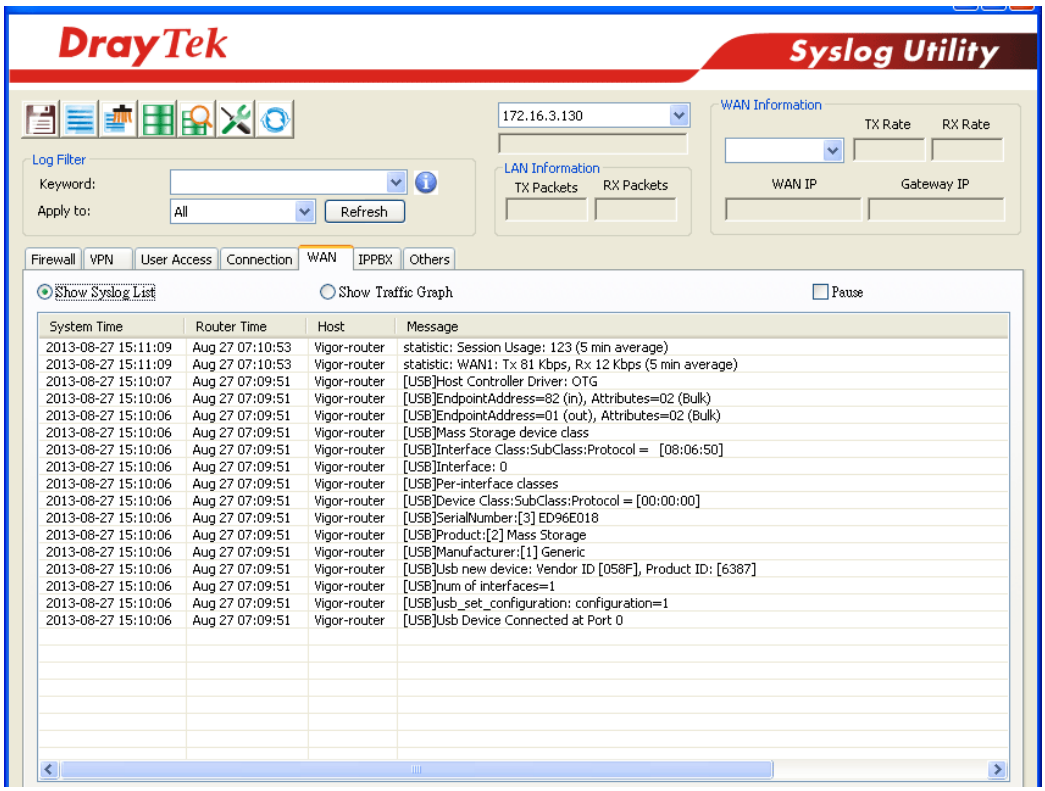
Cuando tenga problemas para usar la transmisión de red 3G/4G, verifique lo siguiente:

Compruebe si las luces LED USB están encendidas o apagadas

Debe esperar unos 15 segundos después de insertar el módem USB 3G/4G en su Vigor2927. Más tarde, el LED USB se encenderá, lo que significa que la instalación del módem USB se realizó correctamente. Si el LED USB no se enciende, retire y vuelva a insertar el módem. Si aún falla, reinicie Vigor2927.

El LED USB se enciende pero la conexión de red no funciona

Verifique que el código PIN de la tarjeta SIM esté deshabilitado o no. Utilice la utilidad del módem USB 3G/4G para desactivar el código PIN y vuelva a intentarlo. Si aún falla, podría ser el problema de cumplimiento del sistema. Abra DrayTek Syslog Tool para capturar la información de conexión (registro WAN) y envíe la página (similar al siguiente gráfico) al centro de servicio de DrayTek.



La velocidad de transmisión no es lo suficientemente rápida

Conecte su computadora portátil con un módem USB 3G/4G para probar la velocidad de conexión y verificar si el problema es causado por Vigor2927. Además, consulte el manual del módem USB 3G/4G para ver el estado del LED y asegurarse de que el módem se conecte a Internet a través del modo HSDPA. Si desea utilizar el módem en interiores, colóquelo cerca de la ventana para obtener una mejor recepción de la señal.

IX-7 Volver a la configuración predeterminada de fábrica si es necesario

A veces, una conexión incorrecta se puede mejorar volviendo a la configuración predeterminada. Intente restablecer el enrutador por software o hardware. Esta función está disponible en**Modo de administrador**solo.

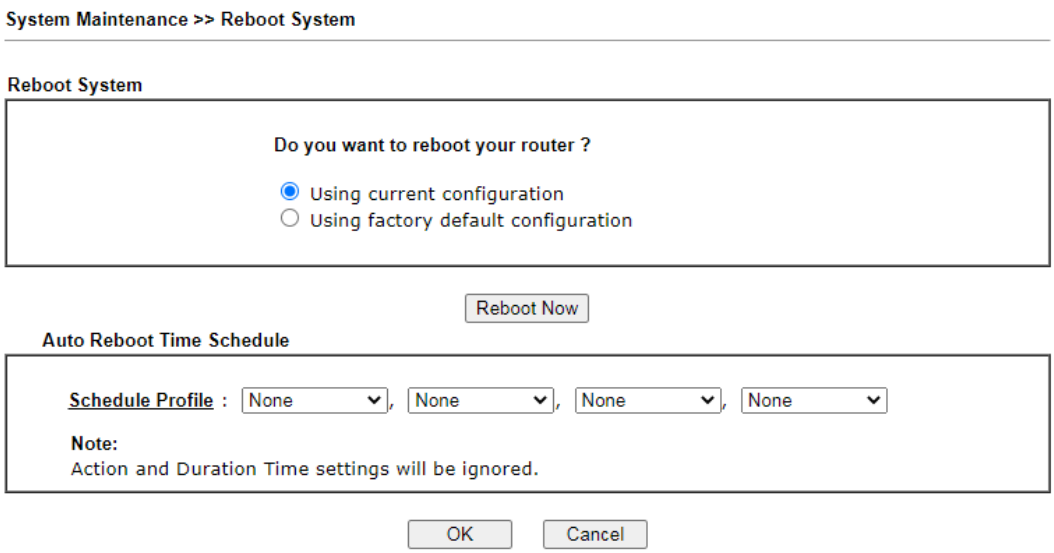
Información

Después de presionar la configuración predeterminada de fábrica, perderá todas las configuraciones que hizo antes. Asegúrese de haber registrado todos los ajustes útiles antes de presionar. La contraseña por defecto de fábrica es nula.

Restablecimiento de software

Puede restablecer el enrutador a los valores predeterminados de fábrica a través de la página web. Esta función está disponible en**Modo de administrador**solo.

Ir a**Mantenimiento del sistema**y elige**Reiniciar el sistema**en la página web. La siguiente pantalla aparecerá. Elegir **Uso de la configuración predeterminada de fábrica**y haga clic**Reinicie ahora**. Después de unos segundos, el enrutador devolverá todas las configuraciones a las configuraciones de fábrica.



Restablecimiento de hardware

Mientras el enrutador está funcionando (LED ACT parpadeando), presione el**Restablecimiento de fábrica**y manténgalo presionado durante más de 5 segundos. cuando ves el**ACTO**El LED parpadea rápidamente, suelte el botón. Luego, el enrutador se reiniciará con la configuración predeterminada.

Después de restaurar la configuración predeterminada de fábrica, puede volver a configurar los ajustes del enrutador para que se ajusten a su solicitud personal.

IX-8 Contacto con DrayTek

Si el enrutador sigue sin funcionar correctamente después de muchos intentos, comuníquese con su distribuidor para obtener más ayuda de inmediato. Si tiene alguna pregunta, no dude en enviar un correo electrónico a support@DrayTek.com.

Comandos Telnet de la Parte X

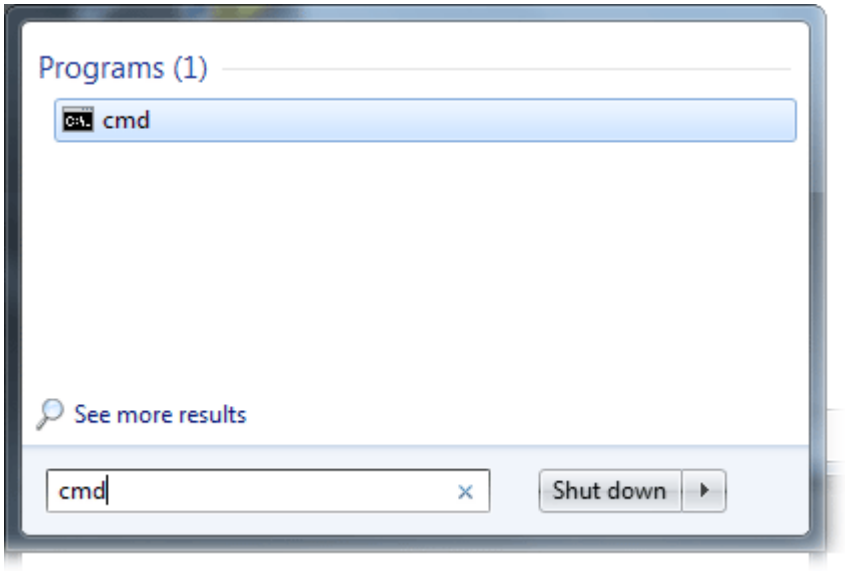
Accediendo a Telnet de Vigor2927

Este capítulo también brinda una descripción general para acceder a telnet y describe las versiones de firmware para los enrutadores que se explican en este manual.

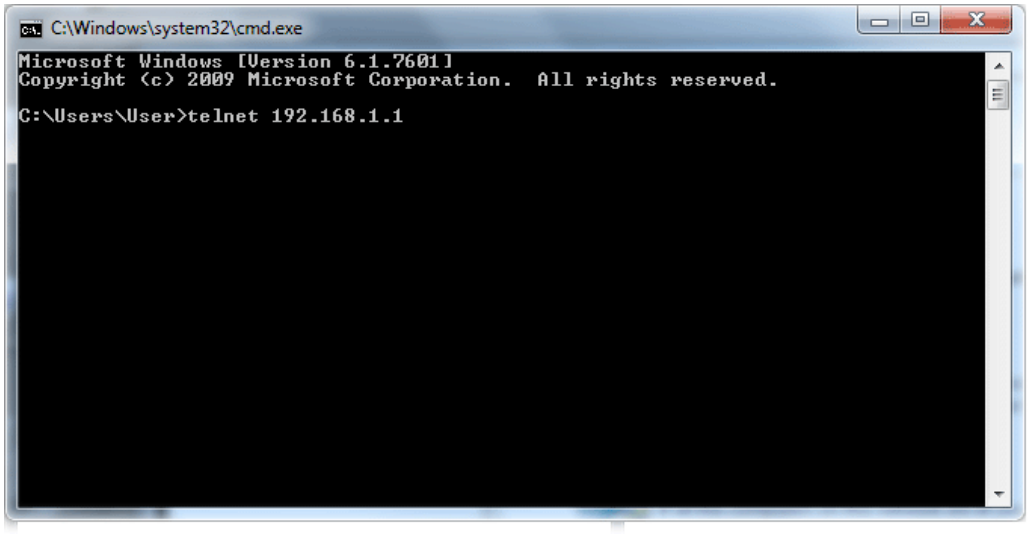
Información

Para usuarios de Windows 7, asegúrese de que las características de Windows del cliente Telnet se hayan activado en**Panel de control>>Programas**.

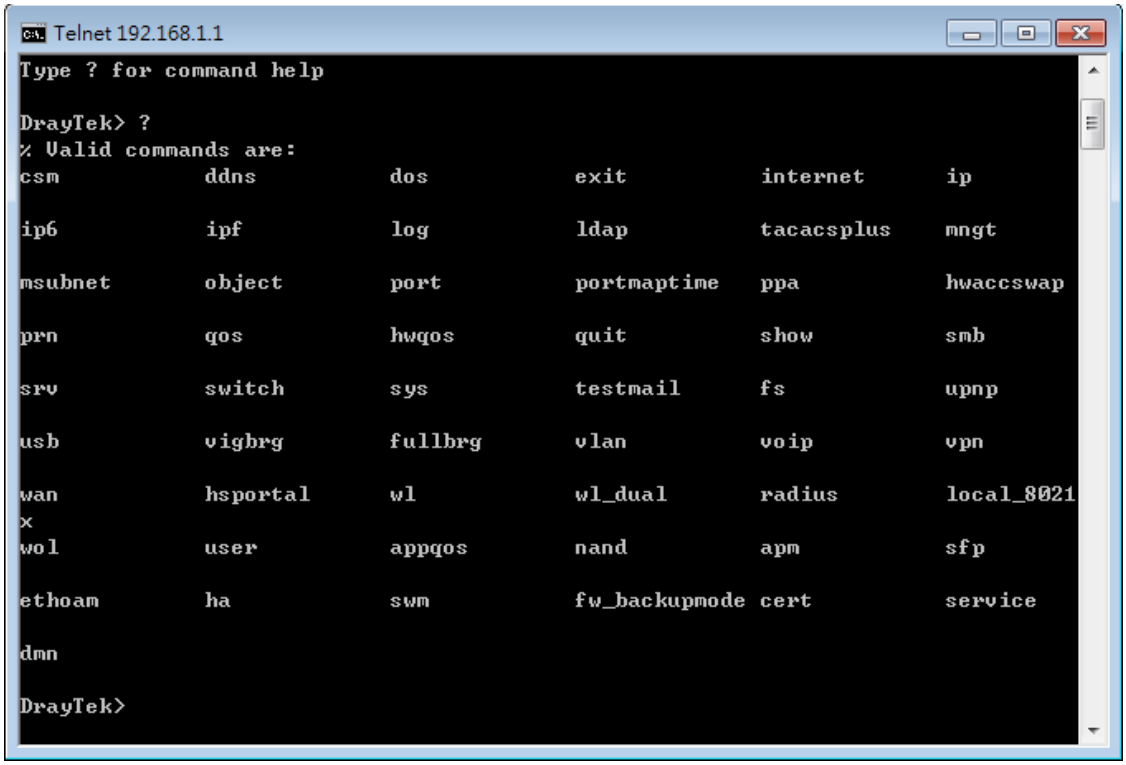
Tipo**cmd**y presione Entrar. La terminal Telnet estará abierta más tarde.



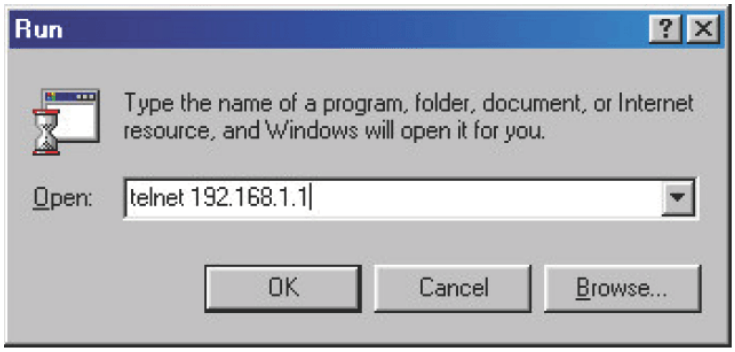
En la siguiente ventana, escriba**Telnet 192.168.1.1**como se muestra a continuación y presione Entrar. Tenga en cuenta que la dirección IP del ejemplo es la dirección predeterminada del enrutador. Si ha cambiado el valor predeterminado, ingrese la dirección IP actual del enrutador.



Luego, ingrese admin/admin para Cuenta/Contraseña. Luego, ingrese**?**. Verá una lista de comandos válidos/comunes según el enrutador que utilice.



Para los usuarios que utilizan un sistema Windows anterior (por ejemplo, 2000/XP), simplemente haga clic en**Inicio >> Ejecutar**y tipo **Telnet 192.168.1.1**en el cuadro Abrir como se muestra a continuación. A continuación, escriba admin/admin para Cuenta/Contraseña. Y, tipo**?**para obtener una lista de comandos válidos/comunes.



Comando Telnet: csm appe prof

Los comandos de CSM le permiten configurar el perfil de CSM para definir perfiles de política para diferentes políticas de aplicaciones de mensajería instantánea (IM)/P2P (punto a punto).

"csm appe prof" se utiliza para configurar el nombre del perfil de cumplimiento de la aplicación. Dicho perfil se aplicará en**Regla predeterminada**de**Cortafuegos>>Configuración general**para filtrar

Sintaxis

csm appe prof-i*ÍNDICE [-v | -n NOMBRE|establecerpredeterminado]*

Sintaxis Descripción

Parámetro	Descripción
ÍNDICE	Significa especificar el número de índice del perfil CSM, del 1 al 32.
-v	Significa ver la configuración del perfil CSM.
- norte	Significa establecer un nombre para el perfil CSM.
NOMBRE	Significa especificar un nombre para el perfil CSM, menos de 15 caracteres.
establecer predeterminado	Restablecer a la configuración predeterminada.

Ejemplo

> csm appe prof -i 1 -n juegos
Se configuró el nombre del Perfil 1 de APPE.

Comando Telnet: conjunto de aplicaciones csm

Se utiliza para configurar ajustes de grupo para IM/P2P/Protocolo y otros en el perfil de cumplimiento de aplicaciones.

Sintaxis

conjunto de aplicaciones csm*-i ÍNDICE -v GRUPO*

conjunto de aplicaciones csm*-i ÍNDICE -e AP_IDX*

conjunto de aplicaciones csm*-i ÍNDICE -d AP_IDX*

conjunto de aplicaciones csm*-i ÍNDICE -p AP_IDX*

conjunto de aplicaciones csm*-i ÍNDICE -q AP_IDX*

Sintaxis Descripción

Parámetro	Descripción
ÍNDICE	Especifique el número de índice del perfil CSM, del 1 al 32.
- v GRUPO	Ver la configuración de MI/P2P/Protocolo y Otros del perfil CSM. GRUPO - Especifique la categoría de la aplicación. Las opciones disponibles son: IM, P2P, Protocolo y Otros.
- y AP_IDX	Habilite para bloquear una aplicación específica. AP_IDX: especifique el número de índice de la aplicación.
-d AP_IDX	Deshabilitar para bloquear una aplicación específica. AP_IDX: especifique el número de índice de la aplicación.
-p AP_IDX	Habilite la ruta de la política para la acción de una aplicación específica.

	AP_IDX: especifique el número de índice de la aplicación.
-qAP_IDX	Deshabilite la ruta de la política para la acción de una aplicación específica. AP_IDX: especifique el número de índice de la aplicación.
AP_IDX	Cada aplicación tiene un número de índice independiente para la identificación en el comando CLI. Especifique aquí el número de índice de la solicitud. Si no tiene idea del número inex, haga lo siguiente (Tome IM como ejemplo): Escriba “csm appe set –I 1 –v IM”, el sistema enumerará todos los números de índice de las aplicaciones categorizadas en IM.

Ejemplo

```
> conjunto de aplicaciones csm -i 1 -p 1
¡El índice de APP no es compatible con Policy Route!
>
```

Comando Telnet: csm appe show

Se utiliza para mostrar información de grupo (IM/P2P/Protocolo y otros) Perfil de aplicación de la aplicación.

Sintaxis

programa de aplicación csm*[-a|-i|-p|-t|-m]*

Sintaxis Descripción

Parámetro	**Descripción**
- a	Ver el estado de configuración de Todos los grupos.
- i	Ver el estado de configuración del grupo IM.
- pag	Ver el estado de configuración del grupo P2P.
- t	Ver el estado de configuración del grupo de protocolos.
- m	Ver el estado de configuración del grupo Otros.

Ejemplo

```
> csm appe show -t Índice de
  tipos                                  Nombre          Versión
-------------------------------------------------------------------------------
Protocolo                 43                  BGP               4
        Protocolo         44                  DNS
        Protocolo         45                  FTP
        Protocolo         46                  GIT
        Protocolo         47                H.323
        Protocolo         48                 HTTP             1.1
        Protocolo         49       IBM Informix®
        Protocolo         50              ibmdb2
        Protocolo         51                 ICMP
        Protocolo         52  IMAP/INICIOTLS IMAP              4.1
        Protocolo         53                  IRC           2.4.0
        Protocolo         54       SQL de Microsoft
        Protocolo         55                 MQTT
```

```
Protocolo      56        mysql
Protocolo      57        NNTP
Protocolo      58        NNTPS
Protocolo      59        NTP
Protocolo      60        Oráculo           11g
Protocolo      61        INICIO POP3/POP3
Protocolo      62        postgresql

Protocolo      63        RÁPIDO            Q025
- - - MÁS --- ['q': Salir, 'Entrar': Líneas nuevas, 'Barra espaciadora': Página siguiente]
```

Comando Telnet: configuración de la aplicación csm

Se utiliza para mostrar el estado de configuración (habilitado o deshabilitado) para IM/P2P/Protocolo/Otras aplicaciones.

Sintaxis

csm appe config -v*ÍNDICE [-i|-p|-t|-m]*

Sintaxis Descripción

Parámetro	Descripción
ÍNDICE	Especifique el número de índice del perfil CSM, del 1 al 32.
- i	Ver el estado de configuración del grupo IM.
- pag	Ver el estado de configuración del grupo P2P.
- t	Ver el estado de configuración del grupo de protocolos.
- m	Ver el estado de configuración del grupo Otros.

Ejemplo

```
> csm appe config -v 1 -m Grupo
            Tipo      Índice        Nombre          Permitir
---------------------------------------------------------------------------
OTROS    tunelización   74   Llamarada de la nube   Desactivar
OTROS    tunelización   75   DNSCrypt               Desactivar
OTROS    tunelización   76   DynaPass               Desactivar
OTROS    tunelización   77   puerta libre           Desactivar
OTROS    tunelización   78   Escudo hotspot         Desactivar
OTROS    tunelización   79   Túnel HTTP             Desactivar
OTROS    tunelización   80   Proxy HTTP             Desactivar
OTROS    tunelización   81   iniciar sesión hamachi Desactivar
OTROS    tunelización   82   EM Teredo              Desactivar
OTROS    tunelización   83   DNS abierto            Desactivar
OTROS    tunelización   84   OpenVPN                Desactivar
OTROS    tunelización   85   PGPNet                 Desactivar
OTROS    tunelización   86   Túnel de ping          Desactivar
OTROS    tunelización   87   Túnel Real             Desactivar
OTROS    tunelización   88   Cielo de fuego         Desactivar
OTROS    tunelización   89   CALCETINES4/CALCETINES5 Desactivar
OTROS    tunelización   90   SoftEther VPN          Desactivar
OTROS    tunelización   91   TinyVPN                Desactivar
OTROS    tunelización   92   Colina                 Desactivar
OTROS    tunelización   93   UltraVPN               Desactivar
OTROS    tunelización   94   VNN                    Desactivar
```

```
      OTROS          tunelización          95          Wujie/UltraSurf          Desactivar
- - - MÁS ---          ['q': Salir, 'Entrar': Líneas nuevas, 'Barra espaciadora': Página siguiente] --
>
```

Comando Telnet: interfaz de aplicación csm

Se utiliza para configurar la interfaz de descarga de firmas APPE.

Sintaxis

interfaz de la aplicación csm*<AUTOMÁTICO/WAN#>*

Sintaxis Descripción

Parámetro	Descripción
AUTO	El enrutador Vigor especifica la interfaz WAN automáticamente.
PÁLIDO	Especifique la interfaz WAN para la descarga de firmas.

Ejemplo

```
> interfaz de la aplicación csm wan1
La interfaz de descarga está configurada como "WAN1" ahora.
> interfaz de aplicación csm automática
La interfaz de descarga está configurada como "seleccionada automáticamente" ahora.
```

Comando Telnet: csm appe email

Se utiliza para configurar el correo electrónico de notificación para la firma APPE en función de los ajustes configurados en **Mantenimiento del sistema>>SysLog/Configuración de alerta de correo (**en el que, la caja de**Firma APPE**está marcado debajo **Activar alerta de correo electrónico**).

Sintaxis

correo electrónico de la aplicación csm*<-e|-d|-s>*

Sintaxis Descripción

Parámetro	Descripción
- mi	Habilite el mecanismo de notificación por correo electrónico.
- d	Deshabilitar el mecanismo de correo electrónico de notificación.
- s	Envíe un correo electrónico de ejemplo.

Ejemplo

```
> csm appe email -e Habilitar el
correo electrónico de APPE.
```

Comando Telnet: csm ucf

Se utiliza para configurar los ajustes del perfil de filtro de control de URL.

Sintaxis

espectáculo csm ucf

csm ucf establecer por defecto

msj csm ucf*GMS*

csm ucf objeto*ÍNDICE <-n NOMBRE_DE_PERFIL | -l [P/B/A] | uac | wf >* **csm ucf objeto***ÍNDICE -n NOMBRE_PERFIL* **csm ucf objeto***ÍNDICE -p VALOR* **csm ucf objeto***ÍNDICE -l P/B/A* **csm ucf objeto***ÍNDICE uac* **csm ucf objeto***ÍNDICE wf*

Sintaxis Descripción

Parámetro	Descripción
espectáculo	Significa mostrar todos los perfiles.
establecer predeterminado	Significa volver a la configuración predeterminada para todo el perfil.
mensaje mensaje	Significa configurar el mensaje de administración. MSG significa el contenido (menos de 255 caracteres) del mensaje en sí.
objeto	Significa especificar el objeto para el perfil.
ÍNDICE	Significa especificar el número de índice del perfil CSM, del 1 al 8.
- norte	Significa establecer el nombre del perfil.
NOMBRE DE PERFIL	Significa especificar el nombre del perfil (menos de 16 caracteres)
- pag	Establezca la prioridad (definida por el número especificado en VALOR) para el perfil.
VALOR	Los números del 0 al 3 representan diferentes condiciones. 0: Significa Paquete: Aprobado. 1: Significa Paquete: Bloque. 2: Significa O bien: Control de acceso URL primero. 3: Significa Cualquiera: Característica web primero.
- yo	Significa el tipo de registro del perfil. Ellos son: P: Pasar, B: bloque, R: Todo,
GMS	Significa especificar el Mensaje de Administración, menos de 255 caracteres
uac	Significa configurar la parte de control de acceso URL.
wf	Significa configurar la parte de la característica web.

Ejemplo

```
> csm ucf obj 1 -n juego -l B Índice de perfil: 1
Nombre de perfil:[juego]
> espectáculo csm ucf
Tabla de perfil de filtro de contenido de URL:
Perfil     Nombre          Perfil     Nombre
------------------------------  ------------------------------
[1]        [juego          ]    [5]        [               ]
[2]        [               ]    [6]        [               ]
[3]        [               ]    [7]        [               ]
[4]        [               ]    [8]        [               ]
------------------------------  ------------------------------
```

Mensaje de administración (máx. 255 caracteres):
- -
<body>
<p>La página web solicitada ha sido bloqueada por URL Content Filt

er.<p>Póngase en contacto con el administrador del sistema para obtener más información.
</cuerpo>

Comando Telnet: csm ucf obj ÍNDICE uac

Significa configurar los ajustes relacionados con el control de acceso URL (uac).

Sintaxis

csm ucf objeto*ÍNDICE uac -v* **csm**
ucf objeto*ÍNDICE uac -e* **csm ucf**
objeto*ÍNDICE uac -d* **csm ucf**
objeto*ÍNDICE uac -a P|B* **csm ucf**
objeto*ÍNDICE uac -i E|D*
csm ucf objeto*ÍNDICE uac -o KEY_WORD_Object_Index*
csm ucf objeto*ÍNDICE uac -g KEY_WORD_Group_Index*

Sintaxis Descripción

Parámetro	Descripción
ÍNDICE	Significa especificar el número de índice del perfil CSM, del 1 al 8.
-v	Significa ver la configuración del protocolo del perfil CSM.
- mi	Significa habilitar la función de control de acceso URL.
- d	Significa deshabilitar la función de control de acceso URL.
- a	Configure la acción de aplicación específica, P o B. B: bloque. El acceso a la web cumple con el control de acceso de URL se bloqueará. Pa: paso. El acceso a la web cumple con la URL Control de acceso se pasará.
- i	Evita el acceso a la web desde cualquier dirección IP. E: Habilitar la función. Se bloqueará el acceso a Internet desde cualquier dirección IP. D: Deshabilitar la función.
- o	Establezca el objeto de palabra clave.
KEY_WORD_Object_Index	Especifique el número de índice del perfil de objeto.
- g	Establezca el grupo de palabras clave.
KEY_WORD_Group_Index	Especifique el número de índice del perfil de grupo.

Ejemplo

> csm ucf obj 1 uac -i E Registro:
[bloque]
Selección de prioridad: [Cualquiera: Control de acceso de URL primero]
Control de acceso URL

```
[ ]Habilitar acción de control de acceso a URL:[pasar]
[v] Impedir el acceso a la web desde la dirección IP.
   No Obj NO. Nombre del objeto
 ----------------------------------------------

   No Grupo NO.       Nombre del grupo
 ----------------------------------------------

> csm ucf obj 1 uac -a B Registro:
[bloque]
Selección de prioridad: [Cualquiera: Control de acceso de URL primero]
Control de acceso URL

[ ]Habilitar acción de control de acceso a URL:[bloquear]
[v] Impedir el acceso a la web desde la dirección IP.
   No Obj NO. Nombre del objeto
 ----------------------------------------------

   No Grupo NO.       Nombre del grupo
 ----------------------------------------------
>
```

Comando Telnet: csm ucf obj ÍNDICE wf

Significa configurar los ajustes relacionados con la característica web (wf).

Sintaxis

csm ucf objeto*ÍNDICE wf -v* **csm**
ucf objeto*ÍNDICE wf -e* **csm ucf**
objeto*ÍNDICE wf -d* **csm ucf**
objeto*ÍNDICE wf -a P|B*
csm ucf objeto*ÍNDICE wf -s WEB_FEATURE*
csm ucf objeto*ÍNDICE wf -u WEB_FEATURE*
csm ucf objeto*ÍNDICE wf -f Índice_objeto_extensión_archivo*

Sintaxis Descripción

Parámetro	Descripción
ÍNDICE	Significa especificar el número de índice del perfil CSM, del 1 al 8.
-v	Significa ver la configuración del protocolo del perfil CSM.
- mi	Significa habilitar la restricción de la función web.
- d	Significa deshabilitar la restricción de la función web.
- un P|B	Configure la acción de la función web, P o B. B: bloque. Se bloqueará el acceso web a la función web. Pa: paso. Se aprobará el acceso a la web que cumpla con la característica de la web.
- s CARACTERÍSTICA_WEB	Significa habilitar la configuración de la característica web. Las características disponibles para la configuración son: c: galleta p: representante tu: subir
- u WEB_FEATURE	Significa cancelar la configuración de la función web.

- f	Significa establecer el número de índice del objeto de extensión de archivo.
File_Extension_Object_inde x	Ingrese el número de índice (1 a 8) para el objeto de extensión de archivo.

Ejemplo

```
> csm ucf obj 1 wf -sc
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Característica web
[ ]Habilitar acción de función de restricción web:[aprobar]

Índice de objeto de extensión de archivo: [0] Nombre de perfil: []

[V] Cookie [ ] Proxy [ ] Subir
```

Comando Telnet: csm wcf

Significa configurar los ajustes relacionados con el filtro de control web (wcf).

Sintaxis

csm espectáculo wcf

mira csm wcf

caché csm wcf

csm wcf servidor WCF_SERVER

csm wcf msg MSG

csm wcf establecer por defecto

csm wcf objeto*ÍNDICE -v* **csm**

wcf objeto*ÍNDICE -a P|B*

csm wcf objeto*ÍNDICE -n NOMBRE_PERFIL*

csm wcf objeto*ÍNDICE -l P|B|A*

csm wcf objeto*ÍNDICE -o KEY_WORD Índice de objetos* **csm**

wcf objeto*ÍNDICE -g PALABRA_CLAVE Índice de grupo* **csm**

wcf objeto*ÍNDICE -w E|D|P|B*

csm wcf objeto*ÍNDICE -s CATEGORÍA|GRUPO_WEB* **csm**

wcf objeto*ÍNDICE -u CATEGORÍA|GRUPO_WEB*

Sintaxis Descripción

Parámetro	Descripción
espectáculo	Significa mostrar los perfiles de filtro de contenido web.
Mirar	Significa mostrar la información de licencia de WCF.
Cache	Significa establecer el nivel de caché para el perfil.
Servidor WCF_SERVER	Significa configurar el servidor de filtro de contenido web.
mensaje msj	Significa configurar el mensaje de administración. MSG significa el contenido (menos de 255 caracteres) del mensaje en sí.
establecer predeterminado	Significa volver a la configuración predeterminada para todo el perfil.
objeto	Significa especificar el perfil del objeto.
ÍNDICE	Significa especificar el número de índice del perfil de filtro de contenido web, del 1 al 8.
-v	Significa ver el perfil de filtro de contenido web.

- un P|B	Configure la acción del perfil de filtro de contenido web, P o B. B: bloque. Se bloqueará el acceso web a la función web. Pa: paso. Se aprobará el acceso a la web que cumpla con la característica de la web.
- norte	Significa establecer el nombre del perfil.
NOMBRE DE PERFIL	Significa especificar el nombre del perfil (menos de 16 caracteres)
- l P|B|A	Significa el tipo de registro del perfil. Ellos son: P: Pasar, B: bloque, R: Todos
- o	Establezca el objeto de palabra clave.
KEY_WORD_Object_Index	Especifique el número de índice del perfil de objeto.
- g	Establezca el grupo de palabras clave.
KEY_WORD_Group_Index	Especifique el número de índice del perfil de grupo.
- w	Significa establecer la acción para la lista blanca y negra. E: Habilitar, D: Deshabilitar, Pa: pase, B:Bloque
- s	Significa elegir los artículos en CATEGORÍA o WEB_GROUP.
- tu	Significa descartar elementos en CATEGORÍA o WEB_GROUP.
WEB_GROUP	Child_Protection, Ocio, Negocios, Chatear, Computadora Internet, Otro
CATEGORÍA	Incluye: "Publicidad y ventanas emergentes", "Alcohol y tabaco", "Anonimizadores", "Artes", "Negocios", "Transporte", "Chat", "Foros y grupos de noticias", "Compromiso", "Informática y tecnología", "Delito y actividad", "Citas y anuncios personales", "Sitios inactivos", "Educación", "Entretenimiento", "Finanzas", "Apuestas", "Juegos", "Gobierno", "Odio e intolerancia", "Salud y Medicina", "Drogas ilegales", "Búsqueda de empleo", "Transmisión de medios y descargas", "Noticias", "Organizaciones sin fines de lucro y ONG", "Desnudez", "Sitios personales", "Phishing y fraude", "Política" , "Pornografía y sexo explícito", "Bienes raíces", "Religión", "Restaurantes y cenas", "Motores de búsqueda y portales", "Compras", "Redes sociales", "Sitios de spam", "Deportes", "Malware", "Traductores", "Viajes", "Violencia", "Armas", "Correo electrónico basado en web", "General", "Ocio y recreación", "Botnets", "Cultos", "Moda y belleza", "Tarjetas de felicitación", "Hackeo ", "Software ilegal", "Compartir imágenes", "Seguridad de la información", "Mensajería instantánea", "Errores de red", "Dominios estacionados", "Peer-to-Peer", "Dirección IP privada", "Hacer trampa en la escuela" , "Educación sexual", "Insípido", "Imágenes de abuso infantil", "Sitios sin categoría"

Ejemplo

```
> csm wcf obj 1 -n test_wcf Índice de
perfil: 1
Nombre de perfil:[test_wcf]
[]Lista blanca/negra
Acción:[bloquear]
   No Obj NO.          Nombre del objeto
 ---------------------------------------------- No
   Grp NO. Nombre del grupo
 ----------------------------------------------
Acción:[bloquear]

Registro: [bloquear]

--------------------------------------------------------------------------------
Seguridad
   [ ]Anonimizadores                    [ ]Comprometida                    [ ]Fi
estafa y fraude
```

```
   [ ]Sitios de spam                    [ ] Malware                    [ ]Bot
redes
   [ ]Errores de red                    [ ]Dominios aparcados
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Control de padres
   [v]Alcohol y tabaco                  [v]chatear                     [v]cri
terminal y actividad
   [v]Odio e intolerancia               [v] Drogas ilegales            [v] Desnudo
idad
   [v]Pornografía y sexo explícito pons [v]Violencia                   [v]Wea

   [v]Cultos                            [v]Hacer trampa en la escuela  [v]Sexo
 Educación
   [v]Insípido                          [v]Imágenes de abuso infantil
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Productividad
   [ ]Publicidad y pop-ups y            [ ]Informática y tecnología    [ ]Dato
   personales
   [ ]Descargar sitios                  [ ]Finanzas                    [ ] Juego
costoso
   [ ]Juegos                            [ ]Búsqueda de trabajo         [ ]Str
Medios de comunicación y descargas
   [ ]Compras                           [ ]Redes sociales              [ ]Esp
rts
   [ ]Hackear                           [ ]Software ilegal             [ ] Soy
compartir
   [ ]Mensajería instantánea            [ ]De igual a igual
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Uso general
   [ ]Artes                             [ ]Negocio                     [ ] Tra
deporte
   [ ]Entretenimiento en foros y        [ ]Educación                   [ ]Ent
grupos de noticias
   [ ]Gobierno                          [ ]Salud y Medicina            [ ]Nuevo
s
   [ ]Entidades sin fines de lucro y    [ ]Sitios personales           [ ]pol
ONGs y Derecho
   [ ]Bienes raíces                     [ ]Religión                    [ ] Res.
Restaurantes y Restaurantes
   [ ] Motores de Búsqueda y Portales   [ ]Traductores                 [ ] Tra
   vel
   [ ]Correo electrónico basado en web  [ ]General                     [ ] Ley
seguro y recreación
   [ ] Moda y Belleza                   [ ]Tarjetas de felicitación   [ ] Información
ormación Seguridad
   [ ] Dirección IP privada             [ ]Sitios sin categorizar
>
```

Comando Telnet: csm dnsf

Significa configurar los ajustes relacionados con el filtro DNS.

Sintaxis

habilitar csm dnsf*ENCENDIDO*|

APAGADO **registro del sistema csm**

dnsf*N*|*P*|*B*|*A* **csm dnsf wcf <**

ÍNDICE> **csm dnsf ucf <***ÍNDICE*>

csm dnsf tiempo de caché*<CACHE_TIME>*

bloqueo csm dnsf*mostrar/encender/apagar*

csm dnsf perfil_mostrar

csm dnsf perfil_editar*ÍNDICE*

csm dnsf perfil_editar*ÍNDICE -n <NOMBRE_DE_PERFIL>*

csm dnsf perfil_editar*ÍNDICE -I <P|B|A>*

csm dnsf perfil_editar*ÍNDICE -w <PERFIL_WCF>*
csm dnsf perfil_editar*ÍNDICE -u <PERFIL_UCF>*
csm dnsf perfil_editar*ÍNDICE -c <HORA_CACHE>*
csm dnsf profile_setdefault
csm dnsf local_bw <*e/d/p/b/a/g/o/s/c>*

Sintaxis Descripción

Parámetro	Descripción
permitir	Habilite o deshabilite el filtro DNS. ENCENDIDO: habilitar. APAGADO: deshabilitar.
registro del sistema	Determinar el contenido de los registros que se transmiten a Syslog. Pa: paso. Los registros de los paquetes que pasan por el filtro DNS se enviarán a Syslog. B: bloque. Los registros de los paquetes bloqueados por el filtro DNS se enviarán a Syslog. R: Todo. Los registros de los paquetes que atraviesan o bloquean el filtro DNS se enviarán a Syslog. N: Ninguno. No se enviará ningún registro a Syslog.
wcf <ÍNDICE>	Especifique un perfil WCF (1 a 8) como base del filtrado de DNS. Escriba un número para indicar el número de índice del perfil de WCF (1 es el primer perfil, 2 es el segundo perfil, etc.).
ucf <ÍNDICE>	Especifique un perfil UCF (1 a 8) como base del filtrado de DNS. Escriba un número para indicar el número de índice del perfil UCF (1 es el primer perfil, 2 es el segundo perfil, etc.).
tiempo de caché <CACHE_TIME>	CACHE_TIME: significa establecer el tiempo de vida de la memoria caché (los valores disponibles son de 1 a 24; 1 es una hora, 2 es dos horas, etc.) para el filtro DNS. APAGADO no es caché; AUTO está usando TTL de pkt.
bloqueo <valor>	DNS envía una página de bloqueo para el puerto de redirección. Cuando una página web está bloqueada por el filtro DNS, el sistema del enrutador enviará una página de mensaje para describir que no se permite visitar la página. ENCENDIDO: Habilite la función de mostrar la página de mensajes. APAGADO: deshabilite la función de mostrar la página de mensajes. MOSTRAR: Mostrar la función de mostrar la página de mensajes está activada o desactivada.
perfil_mostrar	Muestre la tabla del perfil de filtro DNS.
perfil_editar	Modifique el contenido del perfil de filtro DNS.
- n <NOMBRE_DE_PERFIL>	PROFILE_NAME: Ingrese el nombre del perfil de filtro DNS que desea modificar.
- yo <P/B/A>	Especifique el tipo de registro del perfil. Pa: paso. B: bloque. R: Todo.
- w <PERFIL_WCF>	WCF_PROFILE: ingrese el número de índice del perfil WCF.
- u <PERFIL_UCF>	UCF_PROFILE: Introduzca el número de índice del perfil UCF.
- c <TIEMPO_CACHE>	- c significa establecer el tiempo de caché para el filtro DNS. CACHE_TIME: significa establecer el tiempo de vida de la memoria caché (los valores disponibles son de 1 a 24; 1 es una hora, 2 es dos horas, etc.) para el filtro DNS.
profile_setdefault	Restablecimiento a la configuración predeterminada de fábrica.
bw_local <e/d/p/b/s/c>	Establezca la lista negra/blanca de la configuración local del filtro DNS. e: Habilite la función de lista blanca/negra.

	d: Deshabilitar la función de lista blanca/negra. p: Establezca la acción como "Pasar". b: Establezca la acción como "Bloquear". s: Muestra el ajuste de configuración. c: borre la configuración y restablezca la configuración predeterminada de fábrica.
local_bw a <tipo de índice> <START_IP><END/MASK_IP>	Configure el tipo de dirección para la lista blanca/negra del filtro DNS. escriba el índice: Ingrese 0/1/2/3/4. En el cual, 0=máscara, 1=único, 2=cualquiera, 3=rango, 4=grupo y objetos <START_IP>: Introduzca una dirección IP como punto de partida. <END/MASK_IP>: Introduzca una dirección IP como punto final.
local_bw g <elemento número><índice de grupo>	Seleccione el índice de grupo para la lista blanca/negra del filtro DNS. item_number: 1 o 2 (grupo 1 o grupo 2) índice_grupo: 1 a 192
local_bw o <elemento número><índice de grupo>	Seleccione el índice de objetos para la lista blanca/negra del filtro DNS. item_number: 1 o 2 (objeto 1 u objeto 2) índice_objeto: 1 a 32

Ejemplo

```
> csm dnsf local_bw e 1 Habilite el bloqueo
y la lista blanca.
> csm dnsf wcf 1 servicio dns
configurado!!!
> ¡¡¡csm dnsf cachetime auto use
TTL desde pkt!!!
> csm dnsf local_bw a 0 192.168.1.20 255.255.255.0
Tipo de dirección: 0:máscara, 1:simple, 2:cualquiera, 3:rango, 4:objeto y grupo Establezca
el tipo de dirección [MÁSCARA]
> csm dnsf profile_edit 1 -n testformarket Perfil Índice: 1

Nombre de perfil:[testformarket]

Registro: [bloquear]

Índice de perfil WCF: 0

Índice de perfil UCF: 0
```

Comando Telnet: habilitar ddns

Habilitar/deshabilitar el servicio DDNS.

Sintaxis

habilitar ddns*<0/1>*

Sintaxis Descripción

Parámetro	Descripción
Habilitar <0/1>	Habilite o deshabilite el servicio DDNS. 1: habilitar. 0: deshabilitar.

Ejemplo

```
> habilitar ddns 1
  Habilitar la configuración de DNS dinámico
>
```

Comando Telnet: conjunto de ddns

Este comando permite a los usuarios configurar la cuenta DNS de Dynamica.

Sintaxis

conjunto de ddns*opción <valor>*

Sintaxis Descripción

Parámetro	Descripción
- yo <valor>	Significa el número de índice de la cuenta de DNS dinámico. <valor>=1~6
- E <valor>	Significa habilitar/deshabilitar la cuenta de DNS dinámico. <valor>=0~1 0: Deshabilitar 1: Habilitar
- W <valor>	Significa especificar la interfaz WAN. <valor>=1~6 1: WAN1 Primero 2: solo WAN1 3: WAN2 primero 4: solo WAN2 5: WAN3 primero 6: solo WAN3 ejemplo: Para configurar la interfaz WAN: WAN1 Primero
- L <valor>	Significa escribir Nombre de inicio de sesión. [valor]: límite de hasta 64 caracteres
- P <valor>	Significa escribir Contraseña. [valor]: límite de hasta 24 caracteres
- C <valor>	Significa habilitar/deshabilitar comodines. <valor>=0~1 0: Deshabilitar 1: Habilitar
- B <valor>	Significa habilitar/deshabilitar Backup MX. <valor>=0~1 0: Deshabilitar 1: Habilitar
- M <valor>	Significa escribir Mail Extender. [valor]: límite de hasta 60 caracteres
- R <valor>	Significa escribir Determinar IP de WAN real. <valor>=0~1 0: IP de la WAN, 1: IP de Internet
- S <valor>	Significa especificar el proveedor de servicios. Si el usuario desea establecer una página definida por el usuario, el valor debe seleccionar 1. <valor>= 1~19 1: definido por el usuario 2:3322 DDNS (www.3322.org) 3: ChangeIP.com (www.changeip.com) 4:ddns.com.cn (www.ddns.com.cn) 5: DtDNS (www.dtdns.com) 6: dyn.com (www.dyn.com) 7: DynAccess (www.dynaccess.com) 8: dynami.co.za (www.dynami.co.za) 9: freedns.afraid.org (freedns.afraid.org)

	10: NO-IP.COM Gratis (www.no-ip.com) 11: opendns.com (www.opendns.com) 12: OVH (www.ovh.com) 13: Strato (www.strato.eu) 14: TwoDNS (www.twodns.de) 15: TZO (www.tzo.com) 16: ubddns.org (ubddns.org) 17: Viettel DDNS (vddns.vn) 18: vigorddns.com (www.vigorddns.com) 19: ZoneEdit DDNS (dynamic.zoneedit.com)
T <valor>	Significa escribir Tipo de servicio. <valor>= 1~3 1: dinámico 2: personalizado 3: estática
- D <Nombre de host> <Nombre de subdominio>	Significa escribir Nombre de Dominio. es decir: Configuración del índice de cuenta 1 Nombre de dominio para el tipo de servicio dinámico > > ddns conjunto -i 1 -T 1 -D "anfitrión ddns.com.cn" es decir: índice de cuenta 2 que configura el nombre de dominio para el tipo de servicio personalizado > > conjunto ddns -i 2 -T 2 -D "nombre de dominio" es decir: Configuración del índice de cuenta 3 Nombre de dominio para el tipo de servicio estático > > ddns conjunto -i 3 -T 3 -D "nombre de dominio"
- H <valor>	Significa escribir Host de proveedor definido por el usuario. <valor>= límite de hasta 64 caracteres
- Un <valor>	Significa escribir API de servicio definido por el usuario. <valor>= límite de hasta 256 caracteres
- un <valor>	Significa escribir Tipo de autenticación definido por el usuario. <valor>=0~1 0: básico 1: dirección URL
- N <valor>	Significa escribir Tipo de conexión definido por el usuario. <valor>=0~1 0: http 1: HTTPS
- O <valor>	Significa escribir Respuesta del servidor definida por el usuario. <valor>: límite de hasta 32 caracteres

Ejemplo

```
> ddns set -i 1 -S 6 -T 1 -D "nombre de host dnsalias.net" -L usuario1 -P pwd1
> Guardar Aceptar
```

Comando Telnet: registro ddns

Muestra el registro de DDNS.

Ejemplo

```
> registro ddns
>
```

Comando Telnet: tiempo ddns

Establece y muestra la hora de DDNS.

Sintaxis

ddns tiempo*<actualizar en minutos>*

Sintaxis Descripción

Parámetro	Descripción
Actualización en minutos	Ingrese el valor como hora de DDNS. El rango es de 1 a 14400.

Ejemplo

```
> tiempo ddns
tiempo ddns <actualización en
minutos> Válido: 1 ~ 1440
% Ahora: 1440
> ddns tiempo 1000
tiempo ddns <actualización en
minutos> Válido: 1 ~ 1440
% Ahora: 1000
```

Comando Telnet: ddns forceupdate

Este comando actualizará DDNS automáticamente.

Ejemplo

```
> actualización forzada de ddns
  Ahora actualizando DDNS...
  Verifique el resultado usando el comando "ddns log"
```

Comando Telnet: ddns setdefault

Este comando devolverá DDS con la configuración predeterminada de fábrica.

Ejemplo

```
> ddns establecido por defecto
> Establecer como predeterminado de fábrica.
```

Comando Telnet: mostrar ddns

Este comando permite a los usuarios verificar el contenido de la cuenta DDNS seleccionada.

Sintaxis

mostrar ddns -i*<valor>*

Sintaxis Descripción

Parámetro	Descripción
- yo <valor>	Muestre el contenido de la cuenta DDNS seleccionada ingresando el número de índice de la cuenta. <valor>=1~6

Ejemplo

```
> ddns show -i 1
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
 Índice: 1
 [ ] Habilitar cuenta de DNS dinámico
 Interfaz WAN: WAN1 primero
 Proveedor de servicios: dyn.com (www.dyn.com) Tipo
 de servicio: Dinámico
 Nombre de dominio: [].[]
 Nombre de inicio de sesión:
 [ ] Comodines
 [ ] MX de copia de seguridad
 Extensor de correo:
 Determinar IP WAN real: IP WAN

>
```

Comando Telnet: dos

Este comando permite a los usuarios configurar los ajustes para el sistema de defensa DoS.

Sintaxis

dos-*V | D | A*

dos-*s ATTACK_F [UMBRAL][TIEMPO ESPERA]]*

dos-*un | e [ATAQUE_F][ATAQUE_0] | d [ATAQUE_F][ATAQUE_0]]* **dos**-*o*

<TIPO_REGISTRO>|p <TIPO_REGISTRO> |l <TIPO_REGISTRO>

dos-*P <agregar4/eliminar4> <tipo> <valor> |<agregar6/eliminar6> <tipo> <valor> | <mostrar> | quitar4 todo |quitar6 todo>*

dos-*B <agregar4/eliminar4> <tipo> <valor> |<agregar6/eliminar6> <tipo> <valor> | <mostrar> | quitar4 todo |quitar6 todo>*

dos-*<0/1>*

dos-*p<0/1>*

dos-*yo <1/2/3>*

dos-*f <0/1/mostrar>* **dos**-*yo*

<1/2/3/4/mostrar>

Sintaxis Descripción

Parámetro	Descripción
-V	Significa ver la configuración del sistema de defensa DoS.
- D	Significa desactivar el sistema de defensa DoS.
- A	Significa activar el sistema de defensa DoS.
- s	Significa habilitar la función de defensa para un ataque específico y establecer sus parámetros.
ATAQUE_F	Significa especificar el nombre de los ataques de inundación o escaneo de puertos, por ejemplo, synflood, udpflood, icmpflood o postscan.
LÍMITE	Significa la tasa de paquetes (paquetes/segundo) a la que se detectará un ataque de inundación. Establezca un valor mayor que 20.
SE ACABÓ EL TIEMPO	Significa el tiempo (segundos) que se bloqueará un ataque de inundación. Establezca un valor mayor que 5.

- a	Significa habilitar la función de defensa para todos los ataques enumerados en ATTACK_0.
- mi	Significa habilitar la función de defensa para un(os) ataque(s) específico(s).
ATAQUE_0	Significa especificar un nombre de los siguientes ataques: ip_option, tcp_flag, land, teardrop, smurf, pingofdeath, traceroute, icmp_frag, syn_frag, unknow_proto, fraggle.
- d	Significa deshabilitar la función de defensa para un(os) ataque(s) específico(s).
- P <agregar4/eliminar4> <tipo> <valor> |<agregar6/eliminar6> <tipo> <valor> | <mostrar> | quitar4 todo |quitar6 todo>	Agregue o elimine la dirección IPv4/IPv6 en la lista blanca de IP de paso. add4/remove4: agregue/elimine una dirección IPv4/IPv6 a/de la lista blanca. add6/remove6: Agregar/eliminar una dirección IPv6 a/de la lista blanca. Tipo: dos tipos, -i y -c. Donde, "-i" significa la dirección IPv4 y "-c" significa el objeto de país. Valor: Ingrese la dirección IP para -i; introduzca el número de índice del perfil de objeto de país. Mostrar: muestra la lista blanca.
- B <agregar4/eliminar4> <tipo> <valor> |<agregar6/eliminar6> <tipo> <valor> | <mostrar> | quitar4 todo |quitar6 todo>	Agregue o elimine la dirección IPv4/IPv6 en la lista negra de bloqueo de IP. add4/remove4: Agregar/eliminar una dirección IPv4/IPv6 a/de la lista negra. add6/remove6: Agregar/eliminar una dirección IPv6 a/de la lista negra. Tipo: dos tipos, -i y -c. Donde, "-i" significa la dirección IPv4 y "-c" significa el objeto de país. Valor: Ingrese la dirección IP para -i; introduzca el número de índice del perfil de objeto de país. Mostrar: Muestra la lista negra.
dos -o <TIPO_REGISTRO>	Habilitar/deshabilitar registro de defensa dos. <TIPO_REGISTRO>: Ingrese 0 o 1. 0: Deshabilitar 1: Habilitar
dos -p <TIPO_REGISTRO>	Habilitar/deshabilitar el registro de defensa contra la suplantación de identidad. <TIPO_REGISTRO>: Ingrese 0 o 1. 0: Deshabilitar 1: Habilitar
dos -l <TIPO_REGISTRO>	Habilitar/deshabilitar el registro de la lista blanca/negra de defensa dos. <TIPO_REGISTRO>: Ingrese 0 a 3. 0: Ninguno 1: lista blanca 2: Lista negra 3: Todos
dos -f <0/1/mostrar>	Establezca la prioridad de la lista blanca/lista negra. [0/1/mostrar]: 0:Lista blanca; 1: lista negra
dos -i <1/2/3/4/mostrar>	Establezca el intervalo de tiempo para enviar el registro de lista blanca/ lista negra. [1/2/3/4/espectáculo]: 1:30; 2:60; 3:180; 4:300 segundos

Ejemplo

```
> dos –A
El sistema Dos Defense está activado
> dos –s synflood 50 10
Synflood está habilitado! Umbral=50 <pke/seg> tiempo de espera=10 <pke/seg>
> dos -P add4 -i 192.168.5.89 Agregar IP en
Passing IP List con éxito.
> dos -P mostrar
Lista blanca de IP de aprobación de DoS:
    Tipo        IPv4            Tipo    IPv6
 1. PI          192.168.5.89    IP      ::
 2. PI          0.0.0.0         IP      ::
 3. PI          0.0.0.0         IP      ::
 4. PI          0.0.0.0         IP      ::
```

5. PI	0.0.0.0	IP	::
6. PI	0.0.0.0	IP	::
7. PI	0.0.0.0	IP	::
8. PI	0.0.0.0	IP	::
9. PI	0.0.0.0	IP	::
10. PI	0.0.0.0	IP	::
11. PI	0.0.0.0	IP	::
12. PI	0.0.0.0	IP	::
13. PI	0.0.0.0	IP	::
14. PI	0.0.0.0	IP	::
15. PI	0.0.0.0	IP	::
16. PI	0.0.0.0	IP	::

Comando Telnet: salir

Escriba este comando y saldrá de la ventana de telnet.

Comando Telnet: Internet

Este comando le permite configurar ajustes detallados para la conexión WAN.

Sintaxis

Internet*-W n -M n [-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
- Wn	Significa seleccionar la interfaz WAN para la configuración. n: 1 a x. El valor predeterminado es WAN1.
- hombre	M significa configurar el modo de acceso a Internet (obligatorio) y n significa diferentes modos. n=0: fuera de línea n=1: PPPoE n=2: IP dinámica n=3: IP estática n=4: PPTP con IP dinámica, n=5: PPTP con IP estática, n=6: L2TP con IP dinámica n=7: L2TP con IP estática n=A: Módem USB 3G/4G (modo PPP), n=B: Módem USB 3G/4G (modo DHCP)
<comando><parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede ingresar varios comandos en una línea.
- S <nombre del proveedor de servicios de Internet>	Significa establecer el nombre del ISP (máx. 23 caracteres).
- P <activar/desactivar>	Significa habilitar el servicio PPPoE.
- tu <nombre de usuario>	Significa configurar el nombre de usuario (máx. 49 caracteres) para acceder a Internet.
- p <contraseña>	Significa establecer una contraseña (máx. 49 caracteres) para acceder a Internet.
- un	Significa establecer el tipo de autenticación PPP y n significa diferentes tipos (representados por 0-1). n=0: PAP/CHAP (esta es la configuración predeterminada) n=1: solo PAP
- tn	Significa establecer la duración de la conexión y n significa diferentes condiciones. n=-1: siempre activo

	n=1 ~ 999: Tiempo de inactividad para fuera de línea (predeterminado 180 segundos)
- yo <dirección IP>	Esto significa que*servidor PPPoE*asignará una dirección IP especificada aquí para CPE (cliente PPPoE). Si escribe 0.0.0.0 como <dirección IP>, el ISP le asignará la dirección IP adecuada. Sin embargo, si escribe una dirección IP aquí, el enrutador la usará como una IP fija.
- w <dirección IP>	Significa asignar una dirección IP WAN para dicha conexión. Escriba una dirección IP aquí para el puerto WAN.
- n <máscara de red>	Significa asignar una máscara de red para la conexión WAN. Debe escribir 255.255.255.xxx (x se puede modificar) como máscara de red para el puerto WAN.
- g <puerta de enlace>	Significa asignar IP de puerta de enlace para dicha conexión WAN.
- s <ip del servidor>	Significa configurar la IP del servidor PPTP/L2TP.
- Un <idx>	Establezca el modo Siempre encendido y <idx> como WAN de respaldo #
- B <modo>	Establecer en el modo de copia de seguridad. <modo> 0: cuando se desconecta cualquier WAN; 1: cuando todas las WAN se desconectan.
-V	Significa ver el perfil de Acceso a Internet.
- C <código pin del sim>	Configure (modo PPP) el código PIN de la tarjeta SIM (máx. 15 caracteres).
- O <cadena inicial>	Establecer (modo PPP) Cadena inicial de módem (máx. 47 caracteres).
- T <cadena inicial2>	Establecer (modo PPP) Modem Initial String2 (máx. 47 caracteres)
- D <cadena de marcación>	Establezca (modo PPP) Cadena de marcación del módem (máx. 31 caracteres).
- v <nombre del servicio>	Establecer (modo PPP) Nombre del servicio (máx. 23 caracteres).
- m <nombre de usuario ppp>	Establecer (modo PPP) Nombre de usuario PPP (máx. 63 caracteres).
- o <contraseña ppp>	Configure (modo PPP) la contraseña PPP (máx. 62 caracteres).
- es	Establezca (modo PPP) el tipo de autenticación PPP. n= 0: PAP/CHAP (predeterminado), 1: Solo PAP
- qn	(Modo PPP) Índice (1-15) en Configuración de programación-Uno
- xn	(Modo PPP) Índice (1-15) en Configuración de programa-Dos
- sí	(Modo PPP) Índice (1-15) en Configuración de programa-Tres
- zn	(Modo PPP) Índice (1-15) en Configuración de programación-Cuatro
- Q <modo>	Configure (modo PPP o modo DHCP) el modo de detección de conexión WAN. <modo> 0: Detección ARP; 1: detección de ping
- Yo <ping ip>	Establezca (modo PPP o modo DHCP) IP de ping de detección de conexión WAN. <ip de ping>= ppp.qqq.rrr.sss: IP de ping de detección de conexión WAN
- Ln	Establezca (modo PPP) el valor TTL de detección de conexión WAN (1-255).
- R norte	Establecer (modo PPP) Segundos de intervalo de eco de detección de conexión WAN. n= 3 a 60.
- E <código pin del sim>	Configure (modo DHCP) el código PIN de la tarjeta SIM (máx. 19 caracteres).
- G <modo>	Configure (modo DHCP) Modo de red. <modo> 0: 4G/3G/2G; 1: solo 4G; 2: solo 3G; 3: solo 2G
- N <nombre de apn>	Establecer (modo DHCP) Nombre APN (máx. 47 caracteres)
- tu <n>	Configure la MTU para el modo DHCP. n= 1000 a 1440.

Ejemplo

```
> internet -M 1 -S tcom -u nombre de usuario -p contraseña -a 0 -t -1 -i 0.0.0.0 WAN1 Modo de
  Internet configurado en PPPoE/PPPoA
  Nombre de ISP de WAN1 establecido en tcom Nombre de
  usuario de WAN1 establecido en nombre de usuario
  Contraseña de WAN1 establecida correctamente
  Tipo de autenticación PPP de WAN1 establecido en PAP/CHAP Tiempo de
  espera inactivo de WAN1 establecido en siempre activo
  IP de puerta de enlace WAN1 establecida en 0.0.0.0
> internet -V
Modo de Internet WAN1: PPPoE
Nombre ISP: tcom
Nombre de usuario: nombre de usuario
Autenticación: PAP/CHAP Tiempo
de espera inactivo: -1
IP WAN: IP dinámica
>
```

Comando Telnet: ip pubsubnet

Este comando permite a los usuarios habilitar o deshabilitar la subred de enrutamiento IP para su enrutador.

Sintaxis

pubsubred ip*<Habilitar/Deshabilitar>*

Sintaxis Descripción

Parámetro	Descripción
Permitir	Habilite la función.
Desactivar	Deshabilitar la función.

Ejemplo

```
> ip pubsubnet habilitar
subred pública habilitada!
>
```

Comando Telnet: ip pubaddr

Este comando permite configurar el**Subred enrutada por IP**para el enrutador.

Sintaxis

IP pubaddr*?*

IP pubaddr*<dirección IP de subred pública>*

Sintaxis Descripción

Parámetro	Descripción
?	Muestre una dirección IP que permita a los usuarios configurarla como la dirección IP de la subred pública.
dirección IP de subred pública	Especifique una dirección IP. El sistema establecerá la que especificó como la dirección IP de la subred pública.

Ejemplo

```
> ip pubaddr?
% ip addr <dirección IP de subred pública> %
Ahora: 192.168.0.1

> dirección IP pub 192.168.2.5
% Establecer dirección IP de subred pública hecho !!!
```

Comando Telnet: ip pubmask

Este comando permite a los usuarios configurar la máscara para la subred enrutada por IP de su enrutador.

Sintaxis

máscara de pub ip*?*

máscara de pub ip*<máscara de subred pública>*

Sintaxis Descripción

Parámetro	Descripción
?	Muestre una dirección IP que permita a los usuarios configurarla como máscara de subred pública.
dirección IP de subred pública	Especifique una máscara de subred. El sistema configurará la que especificó como la máscara de subred pública.

Ejemplo

```
> ip pubmask?
% ip pubmask <máscara de subred pública>
% Ahora: 255.255.255.0

> ip pubmask 255.255.0.0
% Establecer máscara de subred pública hecho !!!
```

Comando Telnet: ip lanalias

Este comando se utiliza para configurar el alias de IP de WAN.

Sintaxis

ip lanalias*<idx> <opción>*

Sintaxis Descripción

Parámetro	Descripción
<idx>	Significa el número de índice del perfil. Idx: 1 a 5
<opción>	Los comandos disponibles con parámetros se enumeran a continuación.
- mi <0/1>	Significa habilitar/deshabilitar la función de alias de IP. 0: deshabilitar 1: habilitar
- una <dirección IP>	Significa configurar la dirección IP auxiliar.
- wn	Significa agregar una dirección para la interfaz WAN seleccionada. N=0, ninguno N=1, significa WAN1

	N=2, significa WAN2 . . .
-r	Significa eliminar la dirección de la interfaz WAN seleccionada.

Ejemplo

```
> ip lanalias 1 -r
> ip lanalias 1 -a 192.168.1.2
> ip lanalias
Uso:
%% ip lanalias [idx] [Opción]
   idx :índice de perfil de 1 a 5 Opción:

   - mi 1                  :1:activar, 0:desactivar
   - una 192.168.1.2: dirección IP como alias
   - w 1                   :Número WAN o 0
   -r                     (Ninguno) :eliminar este perfil

Tabla de direcciones de alias IP de LAN:
N.º de índice             Dirección IP de estado            Preferir salida
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 1
                          Deshabilitar 192.168.1.2                   n / A
     2                    Deshabilitar 0.0.0.0            n / A
     3                    Deshabilitar 0.0.0.0            n / A
     4                    Deshabilitar 0.0.0.0            n / A
     5                    Deshabilitar 0.0.0.0            n / A
```

Comando Telnet: dirección IP

Este comando permite a los usuarios establecer/agregar una IP de LAN específica a su enrutador.

Sintaxis

dirección IP<*dirección IP*>

Sintaxis Descripción

Parámetro	Descripción
dirección IP	Significa la dirección IP de LAN.

Ejemplo

```
> ip addr 192.168.50.1 %
Establecer dirección IP OK !!!
```

Información

Cuando se cambia la dirección IP de LAN, la dirección IP de inicio del servidor DHCP sigue siendo la misma. Para que la asignación de IP del servidor DHCP sea consistente con esta nueva dirección IP (deben estar en el mismo segmento de red), la dirección IP de la PC debe estar fijada con la misma dirección IP LAN (segmento de red) establecida por este comando para acceder a la web interfaz de usuario del enrutador. Más tarde, modifique las direcciones de inicio para el DHCP

	servidor.

Comando Telnet: ip nmask

Este comando permite a los usuarios establecer/agregar una máscara de red específica para su enrutador.

Sintaxis

máscara ip<*máscara de red IP*>

Sintaxis Descripción

Parámetro	Descripción
máscara de red IP	Significa la máscara de red de LAN IP.

Ejemplo

```
> ip nmask 255.255.0.0 %
Establecer máscara de red IP OK !!!
```

Comando Telnet: ip arp

ARP muestra la condición coincidente para la dirección IP y MAC.

Sintaxis

ip arp añadir <*Dirección IP> <Dirección MAC> <LAN o WAN>*

ip arp del*<Dirección IP> <LAN o WAN>* **ip arp al ras**

estado de ip arp

ip arp aceptar*<0/1/2/3/4/5/estado>* **ip arp setCacheLife***<tiempo>*

En el cual,**añadir**permite a los usuarios agregar una nueva dirección IP en la tabla ARP;**arp del**permite a los usuarios eliminar una dirección IP;**al ras**permite a los usuarios borrar el caché de arp;**estado de arp**permite a los usuarios revisar el estado actual de la tabla arp;**aceptar**permite aceptar o rechazar la dirección MAC de origen/destino; arp**establecerCacheLife**permite a los usuarios configurar la duración en la que los cachés ARP se pueden almacenar en el sistema. Si**ip arp setCacheLife**está configurado con "60", significa que tiene un caché ARP en 0 segundos. Sesenta segundos más tarde sin recibir ningún mensaje ARP, el sistema pensará que dicha memoria caché ARP ha caducado. El sistema emitirá algunas solicitudes ARP para ver si este caché sigue siendo válido.

Sintaxis Descripción

Parámetro	Descripción
dirección IP	Significa la dirección IP de LAN.
Dirección MAC	Significa la dirección MAC de su enrutador.
LAN o WAN	Indica la dirección de la función arp.
0/1/2/3/4/5/estado	0: deshabilitar para aceptar la dirección mac de origen ilegal 1: habilitar para aceptar la dirección mac de origen ilegal 2: deshabilitar para aceptar la dirección mac de destino ilegal 3: habilitar para aceptar la dirección mac de destino ilegal 4: Rechazar VRRP mac en la tabla arp 5: Acepte VRRP mac en el estado de la tabla arp: muestre el estado de configuración.

Tiempo	Los ajustes disponibles serán 10, 20, 30,....2550 segundos.

Ejemplo

```
> estado de aceptación de ip arp
Aceptar fuente ilegal mac arp: deshabilitar

Aceptar dest mac arp ilegal: deshabilitar

Aceptar VRRP mac en la tabla arp: deshabilitar
> estado de ip arp
[Tabla ARP]
 Dirección IP del índice    Dirección MAC        ID DE ANFITRIÓN    Interfaz   VLAN   Puerto
   1 192.168.1.10 60-A4-4C-E6-5A-4F A1000381                        LAN1       - - -   P1
   2    192.168.1.12      00-1D-AA-7C-F5-A4                         LAN1       - - -   P3
   3    192.168.1.13      14-49-BC-43-E5-79                         LAN1       - - -   P2
   4    192.168.1.100     14-49-BC-0A-8A-B8                         LAN1       - - -   P5
>
```

Comando Telnet: ip dhcpc

Este comando está disponible para WAN DHCP.

Sintaxis

ip dhcpc*opción*
ip dhcpc*opción -h|l* **ip dhcpc***opción -d <idx>*
ip dhcpc*opción -e<1 o 0> -w <número wan> -c <número de opción> -v <valor de opción>* **ip dhcpc***opción -e <1 o 0> -w <número wan> -c <número de opción> -x "<valor de opción>"* **ip dhcpc***opción -e <1 o 0> -w <número wan> -c <número de opción> -a <valor de opción>* **ip dhcpc** *opción -u <idx número>* **ip dhcpc***liberar <número wan>* **ip dhcpc***renovar <número wan>* **ip dhcpc***estado*

Sintaxis Descripción

Parámetro	Descripción
opción	Es una configuración opcional para el servidor DHCP. - h: uso de la pantalla - l: enumera todas las opciones de DHCP configuradas a medida - d: eliminar la opción de cliente dhcp personalizado por número de índice - e: activar/desactivar función de opción, 1:activar, 0:desactivar - w: establece el número de WAN (p. ej., 1=WAN1) - c: establecer número de opción: 0~255 - v: establece el valor de la opción por cadena - x: establece el valor de la opción por byte sin procesar (hexadecimal) - u: actualización por número de índice - r: elimina todas las opciones personalizadas del Cliente DHCP

liberar	Significa liberar la dirección IP WAN actual.
renovar	Significa renovar la dirección IP WAN y obtener otra nueva.
estado	Muestra el estado actual del cliente DHCP.

Ejemplo

```
> estado ip dhcpc
==========
WAN1:

Estado del cliente DHCP: ¡Ninguno cliente DHCP activo!

==========
WAN2:

Estado del cliente DHCP: ¡Ninguno cliente DHCP activo!

==========
WAN3:

Estado del cliente DHCP: ¡Ninguno cliente DHCP activo!

==========
WAN4:

Estado del cliente DHCP: ¡Ninguno cliente DHCP activo!

==========
WAN5:

Estado del cliente DHCP: ¡Ninguno cliente DHCP activo!

==========
WAN6:

Estado del cliente DHCP: ¡Ninguno cliente DHCP activo! . . .
```

Comando Telnet: ip ping

Este comando permite a los usuarios hacer ping a la dirección IP de WAN1/WAN2/PVC3/PVC4/PVC5 para verificar si la conexión WAN está bien o no.

Sintaxis

ip-ping *<Dirección IP> <AUTO/WAN1/WAN2/WAN5/WAN6> <Dirección IP de origen>*

Sintaxis Descripción

Parámetro	Descripción
dirección IP	Significa la dirección IP WAN.
AUTOMÁTICO/WAN1/WAN2/WAN5/WAN6>	Significa el puerto WAN/PVC por el que pasa la dirección IP anterior.
Dirección IP origen	Significa la dirección IP de origen.

Ejemplo

```
> IP ping 172.16.3.229 WAN1

Hacer ping a 172.16.3.229 con 64 bytes de datos: Recibir
respuesta de 172.16.3.229, tiempo=0ms Recibir respuesta
de 172.16.3.229, tiempo=0ms Recibir respuesta de
172.16.3.229, tiempo=0ms
```

Paquetes: Enviados = 5, Recibidos = 5, Perdidos = 0 <0% de pérdida>

Comando Telnet: ip tracert

Este comando permite a los usuarios rastrear las rutas desde el enrutador hasta el host.

Sintaxis

seguimiento de ip <*Host/dirección IP> <WAN1/WAN2/WAN3/WAN4/WAN5/WAN6> <Udp/Icmp>*

Sintaxis Descripción

Parámetro	Descripción
dirección IP	Significa la dirección IP de destino.
WAN1/WAN2/WAN3/WAN4/ WAN5/WAN6	Significa el puerto WAN por el que pasa la dirección IP anterior.
UDP/Icmp	Significa UDP o ICMP.

Ejemplo

```
> ip tracert 22.128.2.62 WAN1 Traceroute a
22.128.2.62, 30 saltos máx. 1
      172.16.3.7        10ms
2     172.16.1.2        10ms
3     Pide tiempo fuera.
4     168.95.90.66 50ms
5     211.22.38.134 50ms
6     220.128.2.62 50ms
Seguimiento completo
```

Comando Telnet: ip telnet

Este comando permite a los usuarios acceder al dispositivo especificado por telnet.

Sintaxis

IP telnet <*Dirección IP><Puerto>*

Sintaxis Descripción

Parámetro	Descripción
dirección IP	Introduzca la dirección IP de WAN o LAN del dispositivo remoto.
Puerto	Escriba un número de puerto (por ejemplo, 23). Configuraciones disponibles: 0 ~65535.

Ejemplo

```
> ip telnet 172.17.3.252 23
>
```

Comando Telnet: ip rip

Este comando permite a los usuarios configurar el RIP (protocolo de información de enrutamiento) de IP.

Sintaxis

rasgar ip <*0/1/2***>**

Sintaxis Descripción

Parámetro	Descripción
0/1/2	0 significa deshabilitar; 1 significa primera subred y 2 significa segunda subred.

Ejemplo

```
> IP rasgar 1
%% Establecer RIP 1ra subred.
```

Comando Telnet: ip wanrip

Este comando permite a los usuarios configurar el RIP (protocolo de información de enrutamiento) de la IP WAN.

Sintaxis

ip wanrip*<si no> -e <0/1>*

Sintaxis Descripción

Parámetro	Descripción
si no	Significa la interfaz de conexión. 1: WAN1,2: WAN2, 3: PVC3,4: PVC4,5: PVC5 **Nota**: PVC3 ~PVC5 son WAN virtuales.
- mi	Significa deshabilitar o habilitar la configuración RIP para la interfaz WAN especificada. 1: habilite la función de configuración RIP de WAN IP. 0: Deshabilitar la función.

Ejemplo

```
> ip wanrip?
  Válido ex:ip wanrip <si no> -e <0/1> <si no> 1:
  WAN1,2: WAN2
            3: PVC3,4: PVC4,5: PVC5
  - e <0/1> 0: deshabilitar, 1: habilitar
  Estado actual:
  WAN[1] Protocolo Rip deshabilitar
  WAN[2] Protocolo Rip deshabilitar
  WAN[3] Protocolo Rip deshabilitar
  WAN[4] Protocolo Rip deshabilitar
  WAN[5] Protocolo Rip deshabilitar
  WAN[6] Protocolo Rip habilitar
  WAN[7] Protocolo Rip habilitar WAN
  [8] Rip Protocol habilitar WAN[9] Rip
  Protocol habilitar WAN[10] Rip
  Protocol habilitar WAN[11] Rip
  Protocol habilitar WAN[12] Rip
  Protocol habilitar WAN[13] Rip
  Protocol habilitar WAN[14] Rip
  Protocol habilitar WAN[ 15] Activar
  protocolo Rip WAN[16] Activar
  protocolo Rip
> ip wanrip 5 -e 1
> ip wanrip?
  Válido ex:ip wanrip <si no> -e <0/1> <si no> 1:
  WAN1,2: WAN2
            3: PVC3,4: PVC4,5: PVC5
```

```
 - e <0/1> 0: deshabilitar, 1: habilitar
 Estado actual:
 WAN[1] Rip Protocol deshabilitar
 WAN[2] Rip Protocol deshabilitar
 WAN[3] Rip Protocol deshabilitar
 WAN[4] Rip Protocol deshabilitar
 WAN[5] Rip Protocol deshabilitar
. . .
```

Comando Telnet: ruta ip

Este comando permite a los usuarios establecer una ruta estática.

Sintaxis

ruta ip*agregue <dst><netmask><gateway><ifno><rtype>*
ruta ip*del <dst><máscara de red><rtipo>* **ruta ip***estado*

ruta ip*cnc*
ruta ip*predeterminado <wan1/wan2/off/?>*
ruta ip*limpiar <1/0>*

Sintaxis Descripción

Parámetro	Descripción
agregar	Significa agregar una dirección IP como ruta estática.
del	Significa eliminar la dirección IP especificada.
estado	Significa el estado actual de la ruta estática.
horario de verano	Significa la dirección IP del destino.
máscara de red	Significa la máscara de red de la dirección IP especificada.
puerta	Significa la puerta de enlace del enrutador conectado.
si no	Significa la interfaz de conexión. 3=WAN1 5=WAN3,6=WAN4,7=WAN5 Sin embargo, WAN3, WAN4, WAN5 son WAN basadas en enrutadores
tipor	Significa el tipo de ruta. predeterminado: ruta predeterminada; estática: ruta estática.
cnc	Significa rango de IP actual para CNC Network.
por defecto	Establezca WAN1/WAN2/off como ruta predeterminada actual.
limpio	Limpie todas las configuraciones de ruta. 1: Habilitar la función. 0: Deshabilitar la función.

Ejemplo

```
> ruta IP agregar 172.16.2.0 255.255.255.0 172.16.2.4 3 estática
> estado de ruta ip

Códigos: C - conectado, S - estático, R - RIP, * - predeterminado, ~ - privado C~
                192.168.1.0/          255.255.255.0 está conectado directamente, LAN1
S               172.16.2.0/          255.255.255.0 a través de 172.16.2.4, WAN1
```

Comando Telnet: ip igmp_proxy

Este comando permite a los usuarios habilitar/deshabilitar el servidor proxy igmp.

Sintaxis

ip igmp_proxy*colocar*

ip igmp_proxy*reiniciar*

ip igmp_proxy*pálido*

ip igmp_proxy*consulta*

ip igmp_proxy*ppp <0/1>* **ip**

igmp_proxy*estado*

ip igmp_proxy*versión <v2/v3/automático/mostrar>* **ip**

igmp_proxy*registro del sistema <0/1>*

Sintaxis Descripción

Parámetro	Descripción
colocar	Significa habilitar el servidor proxy.
reiniciar	Significa desactivar el servidor proxy.
pálido	Significa especificar la interfaz WAN para el servicio IGMP.
consulta	Significa establecer el intervalo de consulta general de IGMP. El valor predeterminado es 125000 ms.
ppp <0/1>	0: no es necesario configurar IGMP con encabezado PPP. 1 – Establecer IGMP con cabecera PPP.
estado	Significa mostrar el estado actual del servidor proxy.
versión <v2/v3/automático/mostrar>	Significa configurar la versión IGMP fija en v2 o v3.
registro del sistema <0/1>	Significa configurar IGMP syslog. 0: deshabilitar 1: habilitar

Ejemplo

```
> ip igmp_proxy consulta 130000
  Este comando es para configurar el intervalo de consulta general de IGMP. El
  valor predeterminado es 125000 ms.
  La configuración actual es: 130000 ms
>
```

Comando Telnet: ip igmp_snoop

Este comando permite a los usuarios habilitar o deshabilitar la función de indagación de IGMP.

Sintaxis

ip igmp_snoop habilitar

ip igmp_snoop deshabilitar

estado de ip igmp_snoop

IP igmp_snoop hw_acc*<encendido/apagado/estado>* **ip**

igmp_snoop txquery*<activar/desactivar> <v2/v3>* **ip**

igmp_snoop clave*<encendido/apagado>* **ip igmp_snoop**

separada*<encendido/apagado>* **ip igmp_snoop lista de**

aceptación*<tipo><índice>*

Sintaxis Descripción

Parámetro	Descripción
permitir	Significa habilitar la función igmp snoop
desactivar	Significa deshabilitar la función igmp snoop.
estado	Significa mostrar la configuración actual de igmp.
hw_acc <encendido/apagado/estado>	Significa habilitar/deshabilitar la aceleración de hardware de multidifusión. Encendido: habilita la función. Apagado: deshabilita la función.
txquery <activar/desactivar> <v2/v3>	Significa enviar IGMP QUERY a LAN periódicamente. Activado: habilitar Apagado: deshabilitar v2: versión v2 v3: versión v3
chkleave <activar/desactivar>	Significa verificar el estado de la licencia. Activado: habilita la función de verificación de salida del snoop IGMP. Desactivado: abandonará SALIR si todavía hay clientes en el mismo grupo.
separar <activar/desactivar>	Significa configurar paquetes IGMP separados por NAT/Bridge. Encendido: Los paquetes se separarán. Apagado: los paquetes no serán separados por NAT/Bridge.
lista de aceptación <tipo><índice>	Tipo: Ingrese 0 (deshabilitar), 1 (objeto de ip) o 2 (grupo de ip). Índice: Ingrese 0 a 192 (para objeto ip); ingrese 0 a 32 (para el grupo ip).

Ejemplo

```
> habilitar ip igmp_snoop
%% ip igmp snooping [habilitar|deshabilitar|estado], IGMP Snooping está habilitado.
> ip igmp_snoop deshabilitar
%% ip igmp snooping [habilitar|deshabilitar|estado], IGMP Snooping está deshabilitado.
```

Comando Telnet: ip igmp_fl

Este comando permite a los usuarios habilitar o deshabilitar la función IGMP Fast Leave.

Sintaxis

ip igmp_fl habilitar

ip igmp_fl deshabilitar

estado de ip igmp_fl

Sintaxis Descripción

Parámetro	Descripción
permitir	Significa habilitar la función IGMP Fast Leave
desactivar	Significa deshabilitar la función IGMP Fast Leave.
estado	Significa mostrar la configuración actual de IGMP Fast Leave.

Ejemplo

```
> ip igmp_fl habilitado?
  Si desea utilizar la salida rápida de IGMP, "DEBE" habilitar la indagación de IGMP.
```

```
> habilitar ip igmp_snoop
% ip igmp snooping [habilitar|deshabilitar|estado], IGMP Snooping está habilitado.
>
```

Comando Telnet: sesión ip

Este comando permite a los usuarios establecer el número máximo de límite de sesión para la IP especificada; configure el mensaje para exceder el límite de sesión y configure cuántos segundos funciona el bloque de sesión IP.

Sintaxis

sesión de ip*en*

sesión de ip*apagado*

sesión de ip*<número> predeterminado*

sesión de ip*defaultp2p <num>* **sesión**

de ip*estado*

sesión de ip*espectáculo*

sesión de ip*temporizador <número>*

sesión de ip*<bloquear/desbloquear> <IP>*

sesión de ip*<agregar/eliminar> <IP1-IP2> <núm> <p2pnúm>*

Sintaxis Descripción

Parámetro	Descripción
en	Significa activar el límite de sesión para cada IP.
apagado	Significa desactivar el límite de sesión para cada IP.
<número> predeterminado	Significa establecer el número predeterminado de límite de número de sesión.
Defautlp2p <num>	Significa establecer el número predeterminado de límite de número de sesión para p2p.
estado	Significa mostrar la configuración actual.
espectáculo	Significa mostrar todas las configuraciones de límite de sesión en el rango de IP.
temporizador <número>	Significa establecer cuándo funciona el bloque de sesión de IP. La unidad es segunda.
<bloquear/desbloquear> <IP>	Significa bloquear/desbloquear la dirección IP especificada. Bloqueo: La IP no puede acceder a Internet a través del enrutador. Desbloquear: la IP especificada puede acceder a Internet a través del enrutador.
<agregar/eliminar> <IP1-IP2> <núm> <p2pnúm>	Significa agregar/eliminar los límites de sesión en un rango de IP. <IP1-IP2>: establece el rango de direcciones IP especificadas para este comando. <num>: establece el número de límites de sesión, por ejemplo, 100. <p2pnum>: establece el número de límites de sesión, por ejemplo, 50 para P2P.

Ejemplo

```
> sesión ip por defecto 100
> sesión IP agregar 192.168.1.5-192.168.1.100 100 50
> sesión ip en
> estado de la sesión ip

  Rango de IP:
    192.168.1.5 - 192.168.1.100 : 100

  El límite de sesión de ip actual está activado
```

El número de sesión predeterminado actual es 100

Comando Telnet: ancho de banda ip

Este comando permite a los usuarios establecer el número de límite de ancho de banda máximo para la IP especificada.

Sintaxis

ancho de banda ip*en*

ancho de banda ip*apagado*

ancho de banda ip*predeterminado <tasa_tx><tasa_rx>*

ancho de banda ip*estado*

ancho de banda ip*enrutamiento <activar/desactivar>*

ancho de banda ip*programar <s1> <s2> <s3> <s4>* **ancho**

de banda ip*espectáculo*

ancho de banda ip*<agregar/eliminar><IP1-IP2><tx><rx><compartido>*

Sintaxis Descripción

Parámetro	Descripción
en	Significa activar el límite de ancho de banda IP.
apagado	Significa desactivar el límite de ancho de banda IP.
predeterminado [tasa_tx][tasa_rx]	Significa establecer la tasa predeterminada de tx y rx del límite de ancho de banda. El rango es de 0 a 65535 Kbps.
estado	Significa mostrar la configuración actual.
enrutamiento <activar/desactivar>	Significa aplicar a la subred enrutada IP. En: aplicar a Desactivado: no se aplica a
programar <s1> <s2> <s3> <s4>	Significa configurar el perfil de horario (1 a 4). S1 ~ S4: se pueden configurar hasta cuatro perfiles. Perfiles de horarios disponibles del 0 al 16.
espectáculo	Significa mostrar todas las configuraciones de límites de ancho de banda dentro del rango de IP.
agregar	Significa agregar el ancho de banda dentro del rango de IP.
del	Significa eliminar el ancho de banda dentro del rango de IP.
IP1-IP2	Significa el rango de direcciones IP especificadas para este comando.
tx	Significa establecer la velocidad de transmisión para el límite de ancho de banda.
receta	Significa establecer la tasa de recepción para el límite de ancho de banda.
compartido	Significa que el ancho de banda se compartirá para el rango de IP.

Ejemplo

```
> ancho de banda ip por defecto 200 800
> ancho de banda IP agregar 192.168.1.50-192.168.1.100 10 60
> estado del ancho de banda ip

  Rango de IP:
    192.168.1.50 - 192.168.1.100 : Tx:10K Rx:60K

  El límite de ancho de banda IP actual está desactivado
```

El ajuste automático está desactivado

Comando Telnet: ip dataflowmonitor.

Este comando permite a los usuarios configurar el monitor de flujo de datos.

Sintaxis

monitor de flujo de datos ip*en*

monitor de flujo de datos ip*apagado*

monitor de flujo de datos ip*estado*

Sintaxis Descripción

Parámetro	Descripción
en	Significa habilitar la función Monitor de flujo de datos.
apagado	Significa deshabilitar la función Monitor de flujo de datos.
espectáculo	Significa mostrar el estado actual de la función Monitor de flujo de datos.

Ejemplo

```
> estado de ip dataflowmonitor Monitor
de flujo de datos: desactivado
```

Comando Telnet: ip bindmac

Este comando permite a los usuarios configurar el enlace IP-MAC para el host LAN.

Sintaxis

ip bind mac*en*

ip bind mac*apagado*

ip bind mac*estricto*

ip bind mac*estricto_off*

ip bind mac*subred <todo/establecer LAN_Index/desestablecer LAN_Index/borrar/mostrar>* **ip**

bind mac*agregar <IP><MAC><comentario>* **ip bind mac***del <IP/todos>* **ip bind mac***espectáculo*

Sintaxis Descripción

Parámetro	Descripción
en	Significa activar la política IP bandmac. Incluso la IP no está en la tabla de políticas, aún puede acceder a la red.
apagado	Significa desactivar toda la política de bindmac.
estricto	Significa que solo las direcciones IP en la tabla de políticas IP bindmac pueden acceder a la red.
estricto_off	Significa desactivar la política IP bindmac.
subred <todo/conjunto LAN_Index/desestablecido LAN_Index/borrar/mostrar>	Significa configurar la subred LAN para vincular el modo estricto.
espectáculo	Significa mostrar la dirección IP y la dirección MAC del par vinculado.

agregar	Significa agregar una ip bindmac.
del	Significa eliminar una ip bindmac.
IP	Significa Ingresar la dirección IP para enlazar con la dirección MAC especificada.
MAC	Significa Ingresar la dirección MAC para enlazar con la dirección IP especificada.
Comentario	Significa escribir palabras como una breve descripción.
Todo	Significa eliminar todas las configuraciones de IP bindmac.

Ejemplo

```
> ip bindmac agregar 192.168.1.46 00:50:7f:22:33:55 solo para prueba
> mostrar ip bindmac
La función ip bind mac está DESACTIVADA La función ip
bind mac está ESTRICTAMENTE DESACTIVADA Mostrar
todas las entradas de IP Bind MAC.
IP: 192.168.1.46 enlace MAC: 00-50-7f-22-33-55 ID DE HOST:
   Comentario: solo
```

Comando Telnet: ip bgp

Border Gateway Protocol (BGP) es un protocolo estandarizado diseñado para intercambiar información de enrutamiento y accesibilidad entre sistemas autónomos (AS) en Internet.

Sintaxis

modo ip bgp *<0/1>*

ip bgp como *<0~4294967295>*

retención de ip bgp *<10~65535>*

reintentar ip bgp *<3~255 >* **ip**

bgp id *<xxxx>* **mostrar ip bgp**

vecino ip bgp *<idx>* **modo** *<0/1>* **vecino ip**
bgp *<idx>* **nombre** *<longitud máxima>*
vecino ip bgp *<idx>* **ip** *<xxxx>*
vecino ip bgp *<idx>* **como** *<1~4294967295>*
vecino ip bgp *<idx>* **peso** *<0~7>* **vecino ip bgp**
<idx> **anteponer** *<0~7>* **vecino ip bgp** *<idx>*
md5 *<0/1>* **vecino ip bgp** *<idx>* **llave** *<longitud*
máxima> **vecino ip bgp** *<idx>* **mostrar ip bgp**
vecino mostrar todo

ip bgp estática *<sidx> <ip> <máscara de red>* **ip**

bgp estática *<sidx>* **eliminar ip bgp muestra**

estática

Sintaxis Descripción

Parámetro	Descripción
modo <0/1>	Habilite o deshabilite el GMP. 0: deshabilitar 1: habilitar

como <0~4294967295>	Configure el número AS para el enrutador local. <0~4294967295>
espera <10~65535>	Establezca el intervalo de tiempo (en segundos) para determinar que el par está inactivo cuando el enrutador no puede recibir ningún mensaje de actividad del par dentro del tiempo. <10~65535>: el valor predeterminado es 180 seg.
reintentar <3~255>	Configure el tiempo de reintento de la conexión BGP. <3~255>: el valor predeterminado es 120 segundos
identificación <xxxx>	Seleccione una IP de subred local habilitada como ID de enrutador. <xxxx>: Introduzca una dirección IP.
espectáculo	Muestra todas las configuraciones de BGP.
vecino <idx> modo <0/1>	Habilite o deshabilite el perfil de vecino. <idx>: 1 a 8. Número de índice del perfil vecino. 0: deshabilitar 1: habilitar
vecino <idx> nombre <max len>	Establezca un nombre para el perfil de vecino. <idx>: 1 a 8. Número de índice del perfil vecino. <max len>: Ingrese un nombre (no más de 20 caracteres).
vecino <idx> ip <xxxx>	Establezca la dirección IP para el perfil de vecino especificado. <idx>: 1 a 8. Número de índice del perfil vecino. <xxxx>: Introduzca una dirección IP (p. ej., 192.168.1.33).
vecino <idx> como <1~4294967295>	Establezca un número de AS para el perfil de vecino especificado. <idx>: 1 a 8. Número de índice del perfil. <1~4294967295>: Introduzca un número.
vecino <idx> peso <0~7>	Establezca el valor de ponderación para el perfil de vecino especificado. <idx>: 1 a 8. Número de índice del perfil vecino. <0~7>: más alto es mejor.
vecino <idx> anteponer <0~7>	Establezca el valor antepuesto para el perfil de vecino especificado. <idx>: 1 a 8. Número de índice del perfil vecino. <0~7>: más bajo es mejor.
vecino <idx> md5 <0/1>	Habilite o deshabilite la autenticación MD5 para el perfil vecino. <idx>: 1 a 8. Número de índice del perfil. 0: Deshabilitar. 1: Habilitar.
vecino <idx> clave <long máx>	Configure la clave utilizada para la autenticación MD5. <idx>: 1 a 8. Número de índice del perfil vecino. <max len>: Ingrese un nombre (no más de 20 caracteres).
vecino <idx> mostrar	Muestra la configuración de BGP para el perfil de vecino especificado. <idx>: 1 a 8. Número de índice del perfil.
vecino mostrar todo ocultar todo	Muestra la configuración de BGP de los perfiles vecinos.
estático <sidx> <ip> <máscara de red>	Configure la dirección IP y la máscara de subred para el perfil de red estática especificado. <sidx>: 1 a 16. Número de índice del perfil de red estático. <ip>: Introduzca una dirección IP. <máscara de red>: Introduzca una máscara de red.
<sidx> estático eliminar	Eliminar/borrar la configuración del perfil de red estática seleccionado. <sidx>: 1 a 16. Número de índice del perfil.
espectáculo estático	Muestra la configuración de BGP de los perfiles de red estáticos.

Ejemplo

```
> ip bgp id 255.255.255.0
```

```
Establecer ID de enrutador BGP: 255.255.255.0
> ip bgp mostrar
BGP está habilitado
Número del sistema autónomo local: 33333
Tiempo de espera: 180
Tiempo de reintento de conexión: 20
ID de enrutador: 255.255.255.0

Vecino BGP:
Modo Idx como nombre de número          Dirección IP          Estado          anteponer peso
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 1
      es     0                    Vacío          Ninguno          0     0
2     Dis    0                    Vacío          Ninguno          0     0
3     Dis    0                    Vacío          Ninguno          0     0
4     Dis    0                    Vacío          Ninguno          0     0
5     Dis    0                    Vacío          Ninguno          0     0
6     Dis    0                    Vacío          Ninguno          0     0
7     Dis    0                    Vacío          Ninguno          0     0
8     Dis    0                    Vacío          Ninguno          0     0

Redes estáticas BGP:
Índice: 8, dirección IP: 192.168.2.56, máscara: 255.255.255.254
```

Comando Telnet: ip maxnatuser

Este comando se utiliza para establecer el número máximo de usuarios de NAT.

Sintaxis

ip maxnatuser*número de usuario*

Sintaxis Descripción

Parámetro	Descripción
Número de usuario	Un número especificado aquí significa el total de usuarios de NAT que admite el enrutador Vigor. 0 – Significa sin limitación.

Ejemplo

```
> ip maxnatuser 100 % Max
usuario NAT = 100
```

Comando Telnet: ip policy_rt

Este comando se utiliza para configurar el perfil de ruta de la política IP.

Sintaxis

ip política_rt*[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
<comando><parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede ingresar varios comandos en una línea.
Configuración generalpara ruta de política	
- yo <valor>	Especifique un número de índice para configurar el perfil de ruta de la política. Valor: 1 a 60. "-1" significa obtener un índice de póliza gratis automáticamente.
- mi <0/1>	0: deshabilitar el perfil de ruta de política seleccionado. 1: habilitar el perfil de ruta de política seleccionado.

- o <valor>	Determinar el funcionamiento de la ruta de la política. Valor: add: crea un nuevo perfil de ruta de política. del: eliminar un perfil de ruta de política existente. editar: modificar un perfil de ruta de política existente. flush: restablece la ruta de la política a la configuración predeterminada.
- 1 <cualquiera/rango>	Especifique el modo IP de origen. Rango: Indique un rango de direcciones IP. Cualquiera: significa que cualquier dirección IP se tratará como dirección IP de origen.
- 2 <cualquier/rango_ip/subred_ip/dominio>	Especifique el modo IP de destino. Cualquiera: no es necesario especificar una dirección IP, ya que ninguna dirección IP se tratará como dirección IP de destino. ip_range: Indica un rango de direcciones IP. ip_subnet: Indica la subred IP. dominio: Indica el nombre de dominio.
- 3 <cualquiera/rango>	Especifique el modo de puerto de destino. Rango: Indique un rango de número de puerto. Cualquiera: significa que cualquier número de puerto se puede utilizar como puerto de destino.
- G <predeterminado/específico>	Especifique el modo de puerta de enlace.
- L <predeterminado/específico>	Especifique el modo de puerta de enlace de conmutación por error.
- s <valor>	Indique la IP de origen de inicio. Valor: El formato de tipo será “xxx.xxx.xxx.xxx”. (por ejemplo, 192.168.1.0)
- S <valor>	Indique la IP de origen final. Valor: El formato de tipo será “xxx.xxx.xxx.xxx”. (p. ej., 192.168.1.100)
- d <valor>	Indique la IP de destino de inicio. Valor: El formato de tipo será “xxx.xxx.xxx.xxx”. (por ejemplo, 192.168.2.0)
- D <valor>	Indique la dirección IP de destino. Valor: El formato de tipo será “xxx.xxx.xxx.xxx”. (p. ej., 192.168.2.100)
- p<valor>	Indique el inicio del puerto de destino. Valor: escriba un número (1 ~ 65535) como inicio del puerto (p. ej., 1000).
- P <valor>	Indique el extremo del puerto de destino. Valor: Escriba un número (1 ~ 65535) como extremo del puerto (por ejemplo, 2000).
- y <valor>	Indique la prioridad del perfil de ruta de política. Valor: Escriba un número (0 ~ 250). El valor predeterminado es “150”.
- Yo <valor>	Indique la interfaz especificada para el perfil de ruta de política. Valor: las interfaces disponibles incluyen, LAN1~LAN16, IP_Routed_Subnet, DMZ_Subnet, VOIP_WAN, WAN1~WAN6, VPN_PROFILE_1~VPN_PROFILE_64,WAN_1_IP_ALIAS_1~ WAN_4_IP_ALIAS_32
- g <valor>	Indique la dirección IP de la puerta de enlace. Valor: El formato de tipo será “xxx.xxx.xxx.xxx”. (por ejemplo, 192.168.3.1)
- l <valor>	Indique la dirección IP de conmutación por error. Valor: El formato de tipo será “xxx.xxx.xxx.xxx”. (por ejemplo, 192.168.4.1)
- t <valor>	Significa "protocolo". Valor: las configuraciones disponibles incluyen "TCP", "UDP", "TCP/UDP", "ICMP" y "Cualquiera".
- norte <0/1>	Indica la función de “Forzar NAT”. 0: Deshabilitar la función. 1: Habilitar la función.

- F <valor>	Significa "habilitar la conmutación por error por MOS". valor: 0 o 1
- M <valor>	Significa "Valor del MOS de conmutación por error". valor: 2.0 ~ 4.0
- un <0/1>	Indica habilitar la función de failover. 0: Deshabilitar la función. 1: Habilitar la función.
- f <valor>	Significa especificar la interfaz para la conmutación por error. Valor: las interfaces disponibles incluyen, NO_FAILOVER, Predeterminado_WAN, Política1~Política50, LAN1~LAN16, IP_Routed_Subnet, DMZ_Subnet, WAN1~WAN6, VPN_PROFILE_1~VPN_PROFILE_64, WAN_1_IP_ALIAS_1 ~ WAN_4_IP_ALIAS_32
- b <valor>	Significa "conmutación por recuperación". Valor: las configuraciones disponibles incluyen, 0: deshabilitar la función de "conmutación por recuperación". 1: Habilite la función de "recuperación".
-v	Ver la configuración de conmutación por recuperación actual.
Diagnosticarpara ruta de política	
- s <valor>	Significa “IP de origen”. Valor: las configuraciones disponibles incluyen: Cualquiera: indica que cualquier dirección IP se puede utilizar como dirección IP de origen. “xxx.xxx.xxx.xxx”: el formato de tipo (p. ej., 192.168.1.0).
- d <valor>	Significa “IP de destino”. Valor: las configuraciones disponibles incluyen: Cualquiera: indica que cualquier dirección IP se puede utilizar como dirección IP de destino. “xxx.xxx.xxx.xxx”: especifique una dirección IP.
- p <valor>	Significa “puerto de destino”. Valor: Especifique un número o escriba Cualquiera (indicando cualquier número).
- t <valor>	Significa "protocolo". Valor: las configuraciones disponibles incluyen "ICMP", "TCP", "UDP" y "Cualquiera".

Ejemplo

```
> ip policy_rt diagnostic -s 192.168.1.100 -d cualquier -p cualquier -t ICMP

    ----------------------------------------------------
        Coincidencia Ruta (Prioritaria)
    ----------------------------------------------------
    * Sin coincidencia

    ----------------------------------------------------
        Coincidencia Política (Prioritaria)
    ----------------------------------------------------
    * Política_1 (200)

    * Conclusión: el paquete se descartó porque la interfaz de envío del
estera
la política ched "política 1" estaba inactiva y no había una configuración de conmutación por error
> ip policy_rt -i -1 -o add -1 range -s 192.168.1.10 -S 192.168.1.20 -2 ip_range –d 202.211.100.10
-D 202.211.100.20 -g 202.211.100.1 -I WAN2
```

Comando Telnet: ip landNSRes

Este comando se utiliza para establecer perfiles DNS de LAN. Con esta función, el usuario puede configurar algunos servicios (como ftp, www o base de datos) con un nombre de dominio al que es fácil acceder.

Sintaxis

ip landnresres*[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
- una <Dirección IP>	Se utiliza para configurar la asignación de direcciones IP (dirección IPv4/IPv6 o varias direcciones de subred). Dirección IP: escriba la dirección IP (p. ej., 192.168.1.56).
- c <CNOMBRE>	Se utiliza para establecer CNAME. CNAME: ingresa una cadena.
- d <número de índice de asignación de direcciones>	Significa eliminar el número de índice con la asignación de direcciones configurada. número de índice de asignación de direcciones: escriba el número de índice que representa el perfil de asignación de direcciones.
- mi <0/1>	Significa habilitar o deshabilitar la función de LAN DNS o Perfil de reenvío de DNS. 0: deshabilitar 1: habilitar
- i <número de índice de configuración de perfil>	Significa crear un perfil LAN DNS con un nombre de dominio específico. número de índice de configuración de perfil: escriba el número de índice que representa el perfil con el nombre de dominio configurado.
- yo	Significa listar información detallada de la configuración del perfil..
- n<nombre de dominio>	Significa especificar un nombre de dominio para acceder.
- p<nombre de perfil>	Significa establecer el nombre del perfil LAN DNS.
-r	Significa borrar el perfil de nombre de dominio especificado y la configuración de asignación de direcciones.
-R	Significa establecer la configuración predeterminada de fábrica.
-s<0/1>	Significa determinar todos los paquetes de subred o solo los paquetes con la misma subred serán respondidos para el perfil de asignación de direcciones. 0: responde a todos los paquetes de subred. 1: responde solo el mismo paquete de subred.
-z	Significa actualizar la configuración de LAN DNS a la caché de DNS.

Ejemplo

```
> ip lanDNSRes -i 1 -n ftp.drayTek.com
% Configure el nombre de dominio de Set1:ftp.drayTek.com
> ip lanDNSRes -i 1 -a 172.16.2.10 -s 1 % Configurar la
IP de Set1:172.16.2.10
% Configurar Idx de Set1: 1 ReplyOnlySameSubnet: Sí
> ip lanDNSRes -i 1 -a 172.16.3.10 -s 1 % Configurar la
IP de Set1:172.16.3.10
% Configurar Idx de Set1: 2 ReplyOnlySameSubnet: Sí
> ip lanDNSRes -i 1 -a 172.16.4.10 -s 1 % Configurar la
IP de Set1:172.16.4.10
% Configurar Idx de Set1: 3 ReplyOnlySameSubnet: Sí
>
```

Comando Telnet: ip dnsforward

Este comando se utiliza para configurar el perfil DNS de LAN para el reenvío de DNS condicional.

Sintaxis

ip dnsreenviar*[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede ingresar varios comandos en una línea.
- una <Dirección IP/Nombre de Dominio>	Establezca la dirección IP o el nombre de dominio del servidor DNS reenviado. <Dirección IP/Nombre de dominio>: Introduzca una dirección IP o el nombre de dominio.
- d <número de índice de asignación del servidor DNS>	Elimine el perfil DNS de LAN seleccionado. <Número de índice de asignación de servidor DNS>: Ingrese el número de índice.
- mi <0/1>	0: deshabilitar esta función. 1: habilitar esta función.
- i <número de índice de configuración de perfil>	Escriba el número de índice del perfil. <número de índice de configuración de perfil>: Ingrese el número de índice.
- yo	Enumere el contenido del perfil LAN DNS (incluido el nombre de dominio, la dirección IP y el mensaje).
- n <nombre de dominio>	Establecer nombre de dominio.
- p <nombre de perfil>	Establecer nombre de perfil para LAN DNS.
-r	Restablece la configuración para el perfil seleccionado.
-R	Establecido en la configuración predeterminada de fábrica.

Ejemplo

```
> ip dnsforward -i 1 -n ftp.drayTek.com % Configure el
nombre de dominio de Set1:ftp.drayTek.com
> ip dnsforward -i 1 -a 172.16.1.1 % Configurar
la IP de Set1: 172.16.1.1
> ip dnsforward -i 1 -l % Idx: 1

% Estado: Deshabilitar
% Perfil: prueba
% Nombre de dominio: ftp.drayTek.com
% IP del servidor DNS: 172.16.1.1
>
```

Comando Telnet: ip spoofdef

Este comando se utiliza para habilitar/deshabilitar la defensa contra la suplantación de IP.

Sintaxis

suplantación de identidad IP*<WAN/LAN><0/1>*

Sintaxis Descripción

Parámetro	Descripción
<WAN/LAN>	Significa bloquear el paquete IP de WAN/LAN con IP de origen inconsistente

	DIRECCIÓN.
<0/1>	0: Deshabilitar la función. 1: Habilitar la función.

Ejemplo

```
> ip spoofdef WAN 1
Configuración guardada:
>
```

Comando Telnet: dirección ip6

Este comando permite a los usuarios configurar la dirección IPv6 para su enrutador.

Sintaxis

dirección ip6 -s*<prefijo> <longitud-prefijo> <LAN1/..LAN8/DMZ/ WAN1/..WAN4/USB1/USB2/VPN1/..VPN64>*

dirección ip6 -d*<prefijo> <prefijo-longitud><LAN1/..LAN8/DMZ/ WAN1/..WAN4/USB1/USB2/VPN1/..VPN64>*

dirección ip6 -a*<LAN1/..LAN8/DMZ/ WAN1/..WAN4/USB1/USB2/VPN1/..VPN64> -u*

dirección ip6 -v*<LAN1/..LAN8/DMZ/ WAN1/..WAN4/USB1/USB2>*

dirección ip6 -t*<prefijo-viejo><longitud-prefijo-viejo><prefijo-nuevo> <longitud-prefijo-nuevo> <LAN1/..LAN8/DMZ/ WAN1/..WAN4/USB1/USB2>*

dirección ip6 -o*<1/2>*

dirección ip6 -o 3*<prefijo> <prefijo-longitud> <WAN1/WAN2/USB1/USB2>*

dirección ip6 -l*<prefijo> <prefijo-longitud> <LAN1/..LAN8/DMZ>*

dirección ip6 <-*p/-b> <prefijo> <prefijo-longitud> <WAN1/..WAN4/USB1/USB2>*

dirección ip6 -x*<LAN1/..LAN8/DMZ>* **dirección ip6 -c***<LAN1/..LAN8/DMZ>* **dirección ip6 -e***<tipo> < LAN1/..LAN8/DMZ>*

Sintaxis Descripción

Parámetro	Descripción
- s <prefijo> <prefijo-longitud> < LAN1/..LAN8/DMZ/ WAN1/..WAN4/USB1/USB2/VPN1/..VPN64>	Significa agregar una dirección ipv6 estática. <prefijo>: Significa ingresar el número de prefijo de la dirección IPv6. <prefix-length>: Significa ingresar un valor fijo como la longitud del prefijo. <LAN1/..LAN8/DMZ/ WAN1/..WAN4/USB1/USB2/VPN1/..VPN64>: Significa especificar la interfaz LAN/WAN/USB/VPN para dicha dirección.
- d <prefijo> <prefijo-longitud> <LAN1/..LAN8/DMZ/ WAN1/..WAN4/USB1/USB2/VPN1/..VPN64>	Significa eliminar una dirección ipv6. <prefijo>: Significa ingresar el número de prefijo de la dirección IPv6. <prefix-length>: Significa ingresar un valor fijo como la longitud del prefijo. <LAN1/..LAN8/DMZ/ WAN1/..WAN4/USB1/USB2/VPN1/..VPN64>: Significa especificar la interfaz LAN/WAN/USB/VPN para dicha dirección.
- a < LAN1/..LAN8/DMZ/ WAN1/..WAN4/USB1/USB2/VPN1/..VPN64> -u	Significa mostrar el estado de la(s) dirección(es) actual(es). <LAN1/..LAN8/DMZ/ WAN1/.. WAN4/USB1/USB2/VPN1/..VPN64>: Significa especificar la interfaz LAN/WAN/USB/VPN. <-u>: Significa mostrar solo la dirección de unidifusión.
- v <LAN1/..LAN8/ WAN1/..WAN4/USB1/USB2>	Significa mostrar el estado de la lista de prefijos.

- t <prefijo-antiguo><longitud-del-prefijo-antiguo><prefijo-nuevo> <nueva-longitud-prefijo> <LAN1/..LAN8 /WAN1/..WAN4/USB1/USB2>	Significa actualizar la tabla de direcciones IPv6 estáticas de WAN. <prefijo-antiguo>: Significa ingresar el número de prefijo de la dirección IPv6. <old prefix-length>: Significa ingresar un valor fijo como la longitud del prefijo. <nuevo-prefijo>: Significa ingresar el número de prefijo de la dirección IPv6. <nueva-longitud-prefijo>: Significa ingresar un valor fijo como la longitud del prefijo. <LAN1/..LAN8/WAN1/..WAN4/USB1/USB2 >: Significa especificar la interfaz LAN/WAN/USB para dicha dirección.
- o <1/2>	<1>: Significa mostrar la lista de prefijos antiguos. <2>: Significa enviar la opción de prefijo antiguo por RA.
- o <3> <prefijo> <prefijo-longitud> <WAN1/..WAN4/USB1/USB2>	<3>: Significa establecer un prefijo antiguo. <prefijo>: Significa ingresar el número de prefijo de la dirección IPv6. <prefix-length>: Significa ingresar un valor fijo como la longitud del prefijo. <WAN1/..WAN4/USB1/USB2 >: Significa especificar una interfaz WAN/ USB para dicha dirección.
- l <prefijo> <prefijo-longitud> <LAN1/..LAN8/DMZ>	Significa agregar una ULA. <prefijo>: Significa ingresar el número de prefijo de la dirección IPv6. <prefix-length>: Significa ingresar un valor fijo como la longitud del prefijo. <LAN1/..LAN8/DMZ>: Significa especificar una interfaz LAN para dicha dirección.
- p/-b <prefijo> <prefijo-longitud> <WAN1/..WAN4/USB1/USB2>	Significa agregar/eliminar un prefijo a/de la lista de prefijos. p: agrega un prefijo a una lista de prefijos. b: Eliminar un prefijo de una lista de prefijos. <prefijo>: Significa ingresar el número de prefijo de la dirección IPv6. <prefix-length>: Significa ingresar un valor fijo como la longitud del prefijo. <WAN1/..WAN4/USB1/USB2 >: Significa especificar una interfaz WAN/ USB para dicha dirección.
- x <LAN1/..LAN8/DMZ>	Significa generar una ULA automáticamente. <LAN1/..LAN8/ DMZ>: Significa especificar una interfaz LAN.
- c <LAN1/..LAN8/DMZ>	Significa eliminar un ULA. <LAN1/..LAN8/DMZ>: Significa especificar una interfaz LAN.
- e <tipo> <LAN1/..LAN8/DMZ>	Significa establecer el tipo de ULA. <tipo>: 0, deshabilitar; 1, estático; 2, auto <LAN1/..LAN8/DMZ>: Significa especificar una interfaz LAN.

Ejemplo

```
> dirección ip6 -a
LAN
Dirección de unidifusión:
  FE80::250:7FFF:FE00:0/64 (Enlace)
Dirección de multidifusión:
  FF02::2
  FF02::1:FF00:0
  FF02::1
. . .
. . .
```

Comando Telnet: ip6 dhcp req_opt

Este comando se utiliza para configurar los ajustes de solicitud de opciones para el cliente DHCPv6.

Sintaxis

ip6 dhcp*req_opt<LAN1|..LAN8|DMZ|WAN1|..WAN4|USB1|USB2> <comando> <parámetro>| ...*

Sintaxis Descripción

Parámetro	Descripción
req_opt	Significa solicitud de opción.
LAN1|..LAN8|DMZ|WAN1|.. WAN4|USB1|USB2	Significa especificar la interfaz LAN o WAN para dicha dirección.
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede ingresar varios comandos en una línea.
- a	Significa mostrar el estado actual de DHCPv6.
- s	Significa preguntar al SIP.
- S	Significa preguntar el nombre SIP.
- d	Significa preguntar la configuración de DNS.
- D	Significa preguntar el nombre DNS.
- norte	Significa preguntar a NTP.
- i	Significa preguntar NIS.
- I	Significa preguntar el nombre NIS.
- pag	Significa preguntar NISP.
- PAG	Significa preguntar el nombre de NISP.
- b	Significa preguntarle a BCMCS.
- B	Significa preguntar el nombre de BCMCS.
-r	Significa pedir tiempo de actualización.
Parámetro	1: se mostrará el parámetro relacionado con la solicitud. 0: no se mostrará el parámetro relacionado con la solicitud.

Ejemplo

```
> ip6 dhcp req_opt WAN2 -S 1
> ip6 dhcp req_opt WAN2 -r 1
> ip6 dhcp req_opt WAN2 -a
% La interfaz WAN2 está configurada para solicitar las siguientes opciones de DHCPv6: %
        nombre del sorbo
>
```

Comando Telnet: cliente ip6 dhcp

Este comando le permite usar el protocolo DHCPv6 para obtener la dirección IPv6 del servidor.

Sintaxis

ip6 dhcp*cliente <WAN1|...|WAN4|USB1|USB2> [-<comando> <parámetro>| ...*

Sintaxis Descripción

Parámetro	Descripción

cliente	Significa la configuración del cliente dhcp.
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]* significa que puede escribir varios comandos en una línea.
- a	Significa mostrar el estado actual de DHCPv6.
- p <IAID>	Significa solicitar ID de asociación de identidad para delegación de prefijo.
- n <DIAID>	Significa solicitar una identificación de asociación de identidad para una dirección no temporal.
- t <tiempo>	Significa establecer el intervalo de solicitud. <tiempo>: 0 ~ 7 segundos (el valor predeterminado es 0).
- c <parámetro>	Significa enviar una confirmación rápida al servidor. 1: Habilitar 0: Deshabilitar
- i <parámetro>	Significa enviar una solicitud de información al servidor. 1: Habilitar 0: Deshabilitar
- e <parámetro>	Significa habilitar o deshabilitar el cliente DHCPv6. 1: Habilitar 0: Deshabilitar
- m <parámetro>	Significa habilitar/deshabilitar el DUID del servidor establecido por la capa de enlace y el tiempo. 1: Habilitar 0: Deshabilitar
- d	Significa mostrar el DUID del cliente.
- Un <parámetro>	Significa establecer el protocolo de autenticación. 0: no definir 2: protocolo retrasado
- R <parámetro>	Significa establecer el valor del reino (máximo: 31 caracteres) en el protocolo retrasado. <parámetro>: Introduzca una cadena.
- S <parámetro>	Significa establecer un secreto compartido (máx.: 31 caracteres) en protocolo retrasado. <parámetro>: Introduzca una cadena.
- K <parámetro>	Significa establecer la ID de clave (1~65535) en el protocolo retrasado. <parámetro>: Introduzca un número.

Ejemplo

```
> ip6 dhcp cliente WAN2 -d Cliente DUID =
000300011449bc0a6241
>
```

Comando Telnet: servidor ip6 dhcp

Este comando le permite configurar el servidor DHCPv6.

Sintaxis

ip6 dhcp*servidor [-<comando> <parámetro>| ...]*

Sintaxis Descripción

Parámetro	Descripción

servidor	Significa la configuración del servidor dhcp.
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede ingresar varios comandos en una línea.
- a	Significa mostrar el estado actual de DHCPv6.
- b	Significa mostrar la tabla de asignación de IP DHCPv6 actual.
- n <nombre>	Significa establecer un nombre de grupo.
- c <parámetro>	Significa enviar una confirmación rápida al servidor. 1: Habilitar 0: Deshabilitar
- e <parámetro>	Significa habilitar o deshabilitar el servidor DHCPv6. 1: Habilitar 0: Deshabilitar
- t <tiempo>	Significa establecer preferencias de por vida.
- y <tiempo>	Significa establecer una vida útil válida.
- tu <tiempo>	Significa configurar el tiempo T1.
- o <tiempo>	Significa configurar el tiempo T2.
- yo <pool_min_addr>	Significa establecer la dirección IPv6 de inicio del grupo de direcciones.
- x <pool_max_addr>	Significa establecer la dirección IPv6 final del grupo de direcciones.
-R	Significa enviar un paquete de reconfiguración al cliente.
-r<0/1>	Significa deshabilitar (0) o habilitar (1) el rango automático.
- N <0/1>	Significa deshabilitar (0) o habilitar (1) la asignación aleatoria de direcciones.
- d <dirección>	Significa establecer la primera dirección DNS IPv6. <dirección> : Ingrese una dirección IPv6.
- D <dirección>	Significa configurar la segunda dirección DNS IPv6. <dirección> : Ingrese una dirección IPv6.
- m<1/0>	Significa habilitar (1) o deshabilitar (0) el DUID del servidor establecido por Link Layer y Time.
- q <nombre>	Significa configurar la lista de búsqueda de dominio DNS. <nombre>: Introduzca un nombre.
-z<0/1>	Significa deshabilitar (0) o habilitar (1) el DHCP PD.
pdadd <suffix> <prefix_len> <cliente linklocal><cliente DUID>	Significa agregar un nodo PD.
pddel <índice PD>	Significa eliminar el nodo PD. <Índice PD>: Introduzca un número.
- Un <parámetro>	Significa establecer el protocolo de autenticación. <parámetro>: Introduzca 0, 2 o 3. 0: no definir 2: protocolo retrasado 3: Clave de reconfiguración
- M <parámetro>	Significa establecer el valor del reino (máximo: 31 caracteres) en el protocolo retrasado. <parámetro>: Introduzca una cadena.
- S <parámetro>	Significa establecer un secreto compartido (máx.: 31 caracteres) en protocolo retrasado. <parámetro>: Introduzca una cadena.

- K <parámetro>	Significa establecer la ID de clave (1~65535) en el protocolo retrasado. <parámetro>: Introduzca un número.

Ejemplo

```
> servidor ip6 dhcp LAN1 pdadd 11:22:33 64 fe80::e202:1bff:fe65:4084
000100011d2ce39a00e06f25c839
%          ¡Añadir a la lista de PD éxito!
%% Estado de PD: inválido, sin prefijo disponible.
>
```

Comando Telnet: internet ip6

Este comando le permite configurar los ajustes para acceder a Internet.

Sintaxis

internet ip6*-W n -M n [-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]* significa que puede escribir varios comandos en una línea.
- Wn	**W**medios para configurar la interfaz WAN y**norte**significa diferentes selecciones. El valor predeterminado es WAN1. n=1: WAN1 n=2: WAN2 n=3: WAN3 . . n=X: WANx
- hombre	M significa configurar el modo de acceso a Internet (obligatorio) y n significa diferentes modos (representados por 0 – 5) n= 0: Desconectado, n=1: PPA, n=2: TSPC, n=3: UICAA, n=4: DHCPv6, n=5: estático n=6: 6in4-estático n=7: 6º
- min	Significa configurar la MTU de IPv6. N = cualquier valor (0 significa "sin especificar").
6º	
- C<n>	Significa configurar el sexto modo de conexión. n=0: automático n=1: estático
- s <servidor>	Significa establecer la 6.ª retransmisión de borde IPv4. <servidor>: Introduzca una cadena.
- m<n>	Significa establecer la sexta longitud de la máscara de dirección IPv4. <n>: Introduzca un número.
- p <prefijo>	Significa establecer el prefijo IPv6 para la sexta conexión.

	<prefijo>: Introduzca un número de prefijo de dirección IPv6.
- yo <n>	Significa establecer la longitud del prefijo para la sexta conexión. <n>: Significa ingresar un valor fijo como la longitud del prefijo.
6 en 4	
- s <servidor>	Significa configurar la dirección IPv4 del punto final remoto 6in4.
- I <Dirección IPv6>	Significa configurar la dirección IPv6 para la conexión 6in4.
-P<n>	Significa establecer la longitud del prefijo WAN IPv6 para la conexión 6in4.
- p <prefijo>	Significa configurar el prefijo de enrutamiento LAN 6in4.
- yo <n>	Significa establecer la longitud del prefijo enrutado LAN 6in4.
- T<n>	Significa configurar 6in4 Tunnel TTL.
TSPC/AICCU	
- tu <nombre de usuario>	Significa establecer el nombre de usuario (máx. 63 caracteres). <nombre de usuario>: Introduzca una cadena.
- P <contraseña>	Significa establecer una contraseña (máx. 63 caracteres). <contraseña>: Introduzca una contraseña.
- s <servidor>	Significa configurar la IP del servidor de túnel. <servidor>: Ingrese una dirección IPv4 o URL (máx. 63 caracteres)
AICCU	
- p <prefijo>	Significa configurar el prefijo de subred (AICCU). <prefijo>: Introduzca un número de prefijo de dirección IPv6.
- yo <n>	Significa establecer la longitud del prefijo de subred (AICCU). <n>: Introduzca un número.
- o <1/0>	Significa configurar AICCU siempre encendido. 1: en 0: apagado
- f	Significa establecer la identificación del túnel AICCU.
Estático	
- w <dirección>	Significa configurar la puerta de enlace predeterminada. <dirección>: Introduzca una dirección IPv6.
Otros	
- d <servidor>	Significa configurar la primera IP del servidor DNS. <servidor>: Introduzca una dirección IPv6.
- D <servidor>	Significa configurar la segunda IP del servidor DNS. <servidor>: Introduzca una dirección IPv6.
- t <dhcp/ra/ninguno>	Significa configurar el modo de prueba de WAN PPP ipv6 para DHCP o RA. <dhcp/ra/none>: Ingrese dhcp, ra o ninguno.
-V	Significa ver el perfil de acceso a Internet IPv6.
- k	Significa marcar el Túnel en la WAN.
-j	Significa colocar el Túnel en la WAN.
- rn	Significa establecer el tiempo de espera RA de la máquina de estado de prefijo.
-cn	Significa establecer el tiempo de espera del cliente DHCPv6 de la máquina de estado del prefijo.
-q <0/1/2>	Significa establecer el modo de detección de WAN. 0:NS Detección 1: detección de ping 2: siempre encendido
- z <valor>	Significa configurar Ping Detect TTL (0-255). <valor>: Introduzca 0~255.
- x <nombre de host/dirección IPv6>	Significa configurar Ping Detect Host (nombre de host o dirección IPv6). <nombre de host/dirección ipv6>: ingrese un nombre de host o una dirección IPv6.
- yo <valor>	Significa establecer el intervalo de conexión ipv6. <valor>: ingrese un número (1500-60000 (unidad: 10 ms)).
-b <0/1>	Significa habilitar DNSv6 basado en DHCPv6. 1 = activado 0 = apagado
- D <0/1>	Significa Habilitar RIPng. 1 = activado 0 = apagado

Ejemplo

```
> ip6 internet -W 2 -M 2 -u 88886666 -p draytek123456 –s amsterdam.freenet6.net Esta
  configuración tendrá efecto después de reiniciar.
  Utilice el comando "sys reboot" para reiniciar el enrutador.
> reinicio del sistema
```

Comando Telnet: ip6 relincho

Este comando le permite mostrar la tabla de vecinos de IPv6.

Sintaxis

relincho ip6*-s <dirección_inet6> <dirección_eth> <LAN1/..LAN8/DMZ/WAN1/..WAN4/USB1/USB2>*
relincho ip6*-d <dirección_inet6> <LAN1/..LAN8/DMZ/WAN1/..WAN4/USB1/USB2>* **relincho ip6***-a <dirección_inet6> <-N LAN1/..LAN8/DMZ/WAN1/..WAN4/USB1/USB2>*

Sintaxis Descripción

Parámetro	Descripción
- s <dirección_inet6> <dirección_eth> <LAN1/..LAN8/DMZ/WAN1/ WAN4/USB1/USB2>	Significa agregar un vecino. <inet6_addr>: ingrese una dirección IPv6. <eth_addr>: Introduzca una dirección de submáscara. <LAN1/..LAN8/DMZ/WAN1/..WAN4/USB1/USB2>: especifique una interfaz para el vecino.
- d <dirección_inet6> <LAN1/..LAN8/DMZ/WAN1/. . WAN4/USB1/USB2>	Significa eliminar a un vecino. <inet6_addr>: ingrese una dirección IPv6. < LAN1/..LAN8/DMZ/WAN1/..WAN4/USB1/USB2>: Especifique una interfaz para el vecino.
- a <dirección_inet6> <-N LAN1/..LAN8/DMZ/WAN1/. WAN4/USB1/USB2>	Significa mostrar el estado del vecino. <inet6_addr>: ingrese una dirección IPv6. <LAN1/..LAN8/DMZ/WAN1/..WAN4/USB1/USB2>: especifique una interfaz para el vecino.

Ejemplo

```
> ip6 neigh -s 2001:2222:3333::1111 00:50:7F:11:ac:22:WAN2 % Vecino
2001:2222:3333::1111 agregado exitosamente!
> ip6 relincho -a

DIRECCIÓN I/F                                   MAC               ESTADO
-------------------------------------------------------------------------------
LAN1 ::                                                           NINGUNO
  LAN1 2001:2222:3333::1111 LAN1                                  FALLIDO
  FE80::D161:4B76:3314:9E59                     14-49-bc-0a-8a-b8 DURO
  LAN1 FF02::1                                  33-33-00-00-00-01  CONECTADO
NINGUNO
>
```

Comando Telnet: ip6 pneigh

Este comando le permite agregar un vecino proxy.

Sintaxis

precio ip6*-s <dirección_inet6> <LAN1/..LAN8/DMZ/WAN1/..WAN4/USB1/USB2>*
precio ip6*-d <dirección_inet6><LAN1/..LAN8/DMZ/WAN1/..WAN4/USB1/USB2>*
precio ip6*-a <dirección_inet6> <-N LAN1/..LAN8/DMZ/WAN1/..WAN4/USB1/USB2>*

Sintaxis Descripción

Parámetro	Descripción

- s <dirección_inet6> <LAN1/..LAN8/DMZ/WAN 1/..WAN4/USB1/USB2>	Significa agregar un vecino proxy. <inet6_addr>: ingrese una dirección IPv6. <LAN1/..LAN8/DMZ/WAN1/..WAN4/USB1/USB2>: especifique una interfaz para el vecino proxy.
- d <dirección_inet6> <LAN1/..LAN8/DMZ/WAN 1/..WAN4/USB1/USB2>	Significa eliminar un vecino proxy. <inet6_addr>: ingrese una dirección IPv6. <LAN1/..LAN8/DMZ/WAN1/..WAN4/USB1/USB2>: especifique una interfaz para el vecino proxy.
- a <dirección_inet6> <-N LAN1/..LAN8/DMZ/WAN1 /..WAN4/USB1/USB2>	Significa mostrar el estado del vecino proxy. <inet6_addr>: ingrese una dirección IPv6. <LAN1/..LAN8/DMZ/WAN1/..WAN4/USB1/USB2>: especifique una interfaz para el vecino proxy.

Ejemplo

```
> ip6 relincho -s FE80::250:7FFF:FE12:300 LAN1 %
        ¡Vecino FE80::250:7FFF:FE12:300 agregado con éxito!
```

Comando Telnet: ruta ip6

Este comando le permite la política de ruta IPv6.

Sintaxis

ruta ip6*-s <prefijo> <prefijo-longitud> <puerta de enlace> <LAN1/..LAN8/DMZ/WAN1/..WAN4/ USB1/USB2/VPN1/..VPN64> <-D>*

ruta ip6 -*d <prefijo> <prefijo-longitud>*

ruta ip6 -*a <LAN1/..LAN8/DMZ/WAN1/..WAN4/USB1/USB2/VPN1/..VPN64>*

ruta ip6 -*yo*

Sintaxis Descripción

Parámetro	**Descripción**
- s <prefijo> <prefijo-longitud> <puerta de enlace> <LAN1/..LAN8/DMZ/WAN1/WAN4/ USB1/USB2/VPN1/..VPN64> <-D>	Significa agregar una ruta. <prefijo>: Significa ingresar el número de prefijo de la dirección IPv6. <longitud del prefijo>: Significa ingresar un valor fijo como la longitud del prefijo. <puerta de enlace>: Significa ingresar a la puerta de enlace del enrutador. <LAN1/..LAN8/DMZ/WAN1/..WAN4/ USB1/USB2/VPN1/..VPN64>**:** Significa especificar la interfaz LAN o WAN o VPN para dicha dirección. <-D>: Significa que dicha ruta se tratará como la ruta predeterminada.
-d <prefijo> <prefijo-longitud>	Significa borrar una ruta. <prefijo>: Significa ingresar el número de prefijo de la dirección IPv6. <longitud del prefijo>: Significa ingresar un valor fijo como la longitud del prefijo.
-a <LAN1/..LAN8/DMZ/WAN1/.. WAN4/USB1/USB2/VPN1/..VP N64>	Significa mostrar el estado de la ruta. <LAN1/..LAN8/DMZ/ WAN1/..WAN4/USB1/USB2/VPN1/..VPN64>**:** Significa especificar la interfaz LAN o WAN o VPN para dicha dirección.
- yo	Significa borrar la tabla de enrutamiento.

Ejemplo

```
> ruta ip6 -s FE80::250:7FFF:FE12:500 16 FE80::250:7FFF:FE12:100 LAN1 %
        ¡Ruta FE80::250:7FFF:FE12:500/16 agregada con éxito!
> ruta ip6 -a LAN1

PREFIJO/PREFIX-LEN                          I/F BANDERA MÉTRICA NEXT-HOP
```

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- ::0.0.0.1/128                                LAN1      0 U ::
  FE80::/128                                   LAN1      0 U ::
  FE80::1649:BCFF:FE0A:6240/128                LAN1      0 U ::
  FE80::/64                                    LAN1   256U ::
  FE80::/16                                    LAN1 1024 UGS FE80::250:7FFF:FE12:100 LAN1 256
  FF00::/8                                     U ::
>
```

Comando Telnet: ip6 ping

Este comando le permite anclar una dirección IPv6 o un host.

Sintaxis

silbido de bala ip6*<Dirección IPv6/Host> <LAN1/..LAN8/DMZ/WAN1/..WAN4/USB1/USB2> <recuento de envíos> <tamaño_de_datos>*

Sintaxis Descripción

Parámetro	Descripción
Dirección IPV6/Host	Significa especificar la dirección IPv6 o el host para hacer ping.
LAN1/..LAN8/DMZ/WAN1/.. WAN4/USB1/USB2	Significa especificar una interfaz para dicha dirección.
tamaño de datos	Va de 1 a 1452.

Ejemplo

```
> ip6 ping 2001:4860:4860::8888 WAN2

Haciendo ping 2001:4860:4860::8888 con 64 bytes de datos:

Recibir respuesta desde 2001:4860:4860::8888, tiempo=330ms
Recibir respuesta desde 2001:4860:4860::8888, tiempo=330ms
Recibir respuesta desde 2001:4860:4860::8888, tiempo=330ms
Recibir respuesta desde 2001: 4860:4860::8888, tiempo=330ms
Recibir respuesta de 2001:4860:4860::8888, tiempo=330ms

Paquetes: Enviados = 5, Recibidos = 5, Perdidos = 0 <% de pérdida>
>
```

Comando Telnet: tracert ip6

Este comando le permite rastrear las rutas desde el enrutador hasta el host.

Sintaxis

seguimiento ip6 <*Dirección IPV6/Host><LAN1/..LAN8/DMZ/WAN1/..WAN4/USB1/USB2>*

Sintaxis Descripción

Parámetro	Descripción
<Dirección IPV6/Host>	Significa especificar la dirección IPv6 o el host para hacer ping.
<LAN1/..LAN8/DMZ/WAN1/ WAN4/USB1/USB2>	Significa especificar una interfaz para dicha dirección.

Ejemplo

```
> ip6 tracert 2001:4860:4860::8888
traceroute a 2001:4860:4860::8888, 30 saltos como máximo a través del protocolo ICMP
   1 2001:5C0:1400:B::10B8 2              340ms
   2001:4DE0:1000:A22::1 3                330ms
   2001:4DE0:A::1                        330ms
   4 2001:4DE0:1000:34::1                340ms
   5 2001:7F8:1: :A501:5169:1 330ms 6
   2001:4860::1:0:4B3                    350ms
   7 2001:4860::8:0:2DAF                 330ms
   8 2001:4860::2:0:66mi                 340ms
   9 Solicitud agotada. 10                  *
 2001:4860:4860::8888                    350ms
Seguimiento completo.
>
```

Comando Telnet: ip6 tspc

Este comando le permite mostrar el estado de TSPC.

Sintaxis

ip6 tpc*<si no>*

Sintaxis Descripción

Parámetro	Descripción
si no	Significa la interfaz de conexión. Ifno=1 (significa WAN1) Info=2 (significa WAN2)

Ejemplo

```
> ip6 tspc 2
Dirección del extremo local v4: 111.243.177.223
Dirección del extremo local v6: 2001:05c0:1400:000b:0000:0000:0000:10b9 Nombre DNS
del enrutador: 8886666.broker.freenet6.net
Dirección de punto final remoto v4: 81.171.72.11
Dirección del extremo remoto v6: 2001:05c0:1400:000b:0000:0000:0000:10b8 Tspc Prefixlen:
56
Corredor de túneles: Amsterdam.freenet.net

Estado: Conectado

>
```

Comando Telnet: ip6 radvd

Este comando le permite habilitar o deshabilitar el servidor RADVD.

Sintaxis

ip6*<LAN1/..LAN8/DMZ> <-<comando> <parámetro>/ ... >*

Sintaxis Descripción

Parámetro	Descripción
<<comando>	Los comandos disponibles con parámetros se enumeran a continuación.

<parámetro>/...>	*<...>*significa que puede ingresar varios comandos en una línea.
-s<0/1>	Significa habilitar o deshabilitar la vida útil predeterminada del servidor RADVD. 1: habilite el servidor RADVD. 0: deshabilitar el servidor RADVD.
- D <0/1/2>	Significa configurar RDNSS Deshabilitar/Habilitar/Implementar (0/1/2) cuando la WAN está activa.
- d <tiempo de vida>	Significa establecer la vida útil predeterminada de RA.
- yo <lifetme>	Significa establecer el tiempo de intervalo mínimo de RA (seg).
- Yo <lifetme>	Significa establecer el tiempo de intervalo RA MAX (seg).
- h <límite de salto>	Significa establecer el límite de salto RA.
- m <mtu/auto>	Significa configurar RA MTU, 1280-1500. mtu: auto - selección automática de MTU desde WAN,
- e <tiempo>	Significa establecer un tiempo alcanzable.
- un <tiempo/infinito>	Significa configurar el temporizador de retransmisión/infinito.
- pag <0/1/2>	Significa establecer la preferencia predeterminada de radvd Baja/Media/Alta. 0- bajo 1-medio 2-alto
-v	Significa ver la configuración de radvd.
-V	Significa ver la configuración en RA.
- L <tiempo/infinito>	Significa establecer un prefijo de por vida válido.
- P <tiempo/infinito>	Significa establecer el tiempo de vida preferido del prefijo.
- r <número>	Significa configurar la prueba RA para el artículo. <núm>: 0, 121, 124 0: predeterminado, 121: logotipo 121, 124: logotipo 124..
-R	Significa recargar Config y enviar RA para subredes.
- tu	Significa ver MTU en todas las interfaces.

Ejemplo

```
> ip6 radvd LAN1 -s 1 % [LAN1]
configuración ! % Habilitar LAN1
radvd OK!
> ip6 radvd LAN1 -d 1800 %
[LAN1] configuración !
% Establecer tiempo de vida predeterminado ok: 1800 !
> Configuración ip6 radvd
LAN1 -V % [LAN1] ! %
        Vida útil predeterminada: 0 segundos Tiempo
%       de intervalo mínimo: 200 segundos Tiempo de
%       intervalo máximo: 600 segundos Límite de
%       salto                   : 64
%       MTU                     : 0
%       tiempo alcanzable       : 0
%       Tiempo de retransmisión : 0
%       Preferencia             : Medio
>
```

Comando Telnet: gestión ip6

Este comando le permite administrar la configuración de la lista de acceso.

Sintaxis

lista de gestión ip6

lista de gestión ip6*agregar <Índice> <Índice de objetos IPv6>|eliminar <índice>|vaciar* **estado de gestión ip6**

gestión ip6*<internet/ http/telnet/ping/https/ssh/enforce_https> <activar/desactivar>*

Sintaxis Descripción

Parámetro	Descripción
lista	Significa mostrar la información de configuración de la lista de acceso.
add <Índice> <Índice de objetos IPv6> |remove <Nº>|descarga>	Significa agregar una dirección IPv6 que se puede utilizar para ejecutar la gestión a través de Internet. <Índice>: 1 a 10. Se pueden configurar diez perfiles para la lista de acceso IPv6. <Índice de objetos IPv6>: Significa el número de índice del objeto IP (1 a 64) o el objeto de palabra clave (1 a 64). eliminar <Índice>: significa eliminar (eliminar) el objeto de IP/ palabra clave especificado.
enjuagar	Significa borrar la tabla de acceso IPv6.
estado	Significa mostrar el estado de la gestión remota de IPv6.
Internet/ http/telnet/ping/https/ssh/ enforce_https	Estos protocolos se utilizan para acceder a Internet.
encendido apagado	Significa habilitar (encender) o deshabilitar (apagar) el acceso a Internet a través de http/telnet/ping.

Ejemplo

```
> Lista de administración de ip6 Agregar 1 62 %%
Establezca Aceptar.
>
```

Comando Telnet: ip6 en línea

Este comando le permite comprobar el estado en línea de IPv6 LAN/WAN.

Sintaxis

ip6*en línea <WAN1/..WAN4/USB1/USB2>*

Sintaxis Descripción

Parámetro	Descripción
<WAN1/..WAN4/USB1/USB2>	Significa la interfaz de conexión.

Ejemplo

```
> ip6 en línea WAN1 % Estado en
  línea de WAN1 : % IPv6 WAN1
  deshabilitado % Puerta de enlace
  predeterminada : :: % Interfaz :
  ABAJO % Tiempo de actividad :
  00:00:00
  % Servidor DNS IPv6: :: Estático %
  Servidor DNS IPv6: :: Estático %
  Servidor DNS IPv6: :: Estático
```

```
% paquetes Tx = 0, bytes Tx = 0, paquetes Rx = 0, bytes Rx = 0 % MTU en línea:
1280, configuración MTU: 0
```

Comando Telnet: ip6 aiccu

Este comando le permite establecer la configuración de IPv6 para la interfaz WAN con el tipo de conexión de AICCU.

Sintaxis

ip6 aiccu -i*<si no>***-r**
ip6 aiccu -i*<si no>***-s**

Sintaxis Descripción

Parámetro	Descripción
<Si no>	Significa la interfaz de conexión. 1=WAN1 2=WAN2
-r	Significa eliminar (eliminar) el número de índice especificado con la configuración de IPv6.
- s	Significa mostrar el estado de la interfaz.

Ejemplo

```
> ip6 aiccu -i 1 -s Estado:
Inactivo
>
```

Comando Telnet: ip6 ntp

Este comando le permite establecer la configuración de IPv6 para el servidor NTP (Network Time Protocols).

Sintaxis

ip6 ntp–h
ip6 ntp–v
ip6 ntp–p<0/1>

Sintaxis Descripción

Parámetro	Descripción
– h	Se utiliza para mostrar el uso de dicho comando.
-v	Se utiliza para mostrar el estado de NTP.
- pag <0/1>	Se utiliza para especificar el servidor NTP para IPv6. 0 – Automático 1 – Primera consulta al servidor NTP IPv6.

Ejemplo

```
> ip6 ntp -p 1
% Establecer prioridad NTP: IPv6 primero
```

Comando Telnet: ip6 lan

Este comando le permite establecer la configuración de IPv6 para la interfaz LAN.

Sintaxis

ip6 lan-ln<-*<l:w:d:D:m:o:s> <parámetro> / ... >*

Sintaxis Descripción

Parámetro	Descripción
– h	Se utiliza para mostrar el uso de dicho comando.
- yo <n>	Significa seleccionar la interfaz LAN que se configurará. n= 1: LAN1 n= 2: LAN2, ... x: LANx. El valor predeterminado es LAN1
- w<n>	Significa seleccionar la interfaz WAN para que sea la interfaz principal. n= 0: Ninguno, n=1: WAN1, n=2: WAN2, ... x: WANx.
- d <servidor>	Significa configurar la primera IP del servidor DNS. <servidor>: Introduzca la dirección IPv6.
- D <servidor>	Significa configurar la segunda IP del servidor DNS. <servidor>: Introduzca la dirección IPv6.
- m<n>	Significa configurar la administración de LAN ipv6. n=0: APAGADO n=1:SLAAC. El valor predeterminado es SLAAC n=2:DHCPv6
-o<n>	Significa habilitar el indicador Otra opción (O-bit). (O-bit es redundante cuando la administración es DHCPv6) n=0: Deshabilitar n=1: Habilitar.
- mi <n>	Significa agregar una extensión WAN. n: 1: WAN1, 2: WAN2, ... x: WANx.
- E <n>	Significa eliminar una extensión WAN. n: 1: WAN1 ,2: WAN2, ... x: WANx.
- b <mapa>	Significa configurar el mapa de bits (decimal) para la extensión WAN. <mapa>: 0: WAN1; 1: WAN2, ... n: WAN(n+1).
- f<n>	Significa deshabilitar IPv6. n=1: deshabilitar IPv6, n=0: habilitar IPv6.
-R <n>	Significa habilitar/deshabilitar RIPng. n=1: Habilitar RIPng, n=0: deshabilitar RIPng.
-s <n>	Significa mostrar la configuración de LAN IPv6. n=0:mostrar todo. El valor predeterminado es mostrar todo. n=1 a 8: LAN1 a LAN8. n=17: DMZ.

Ejemplo

```
> ip6 lan -l 1 -w 1 -d 2001:4860:4860::8888 -o 1 -f 0 -s 2 % ¡Establecer LAN1!


%      ¡Establecer WAN1 principal!

%   Establecer el primer servidor DNS 2001:4860:4860::8888

%      Establecer otra opción ¡Habilitar!

%      [LAN1] compatible con ipv6!

 Esta configuración tendrá efecto después de reiniciar. Utilice el
 comando "sys reboot" para reiniciar el enrutador.

% Ajuste [LAN2]:
%  WAN principal       : WAN1
%  Gestión             : SLAAC
%  Otra opción         : Desactivar
%  Extensión WAN       : Ninguno
%  ID de subred        : 2
%  IP estática(0)      : ::/0
%                      [si no: 0, habilitar: 0]
%  IP estática(1)      : ::/0
%                      [si no: 0, habilitar: 0]
%  IP estática(2)      : ::/0
```

```
%                    [si no: 0, habilitar: 0]
%  IP estática(3)      : ::/0
%                    [ifno: 0, habilitar: 0]:
%  DNS1              2001:4860:4860::8888
%  DNS2              : 2001:4860:4860::8844
%  Tipo ULA           : APAGADO
%  RIPng             : Permitir
>
```

Comando Telnet: sesión ip6

Este comando le permite establecer el límite de sesiones para la dirección IPv6.

Sintaxis

sesión ip6 *en*

sesión ip6 *apagado*

sesión ip6 *<número>*

predeterminado **sesión ip6** *estado*

sesión ip6 *espectáculo*

sesión ip6 *agregar <IP1-IP2> <numero>*

sesión ip6 *del <IP1-IP2> <núm>*

Sintaxis Descripción

Parámetro	Descripción
en	Significa activar el límite de sesión para cada IP.
apagado	Significa desactivar el límite de sesión para cada IP.
<número> predeterminado	Significa establecer el número predeterminado de límite de número de sesión. <núm>: Introduzca un número.
estado	Significa mostrar la configuración actual.
espectáculo	Significa mostrar todas las configuraciones de límite de sesión de rango de IP.
añadir <IP1-IP2><número>	<añadir>:Significa agregar el límite de sesión para un rango de IPv6. <IP1-IP2>: Especifique un rango para las direcciones IPv6. <núm>: Introduzca un número.
del<IP1-IP2><num>	<del>:Significa eliminar el límite de sesión para un rango de IPv6. <IP1-IP2>: Especifique un rango para las direcciones IPv6. <núm>: Introduzca un número.

Ejemplo

```
> sesión ip6 en
> sesión ip6 añadir 2100:ABCD::2-2100:ABCD::10 100
> estado de sesión ip6

   Rango de IPv6:
      2100:ABCD::2 - 2100:ABCD::10 : 100

   El límite de sesión IP6 actual está activado

   El número de sesión predeterminado actual es 100
```

Comando Telnet: ancho de banda ip6

Este comando le permite establecer la configuración de IPv6 para el control del ancho de banda.

Sintaxis

ancho de banda ip6 *en*

ancho de banda ip6 *apagado*

ancho de banda ip6 *predeterminado <tasa_tx> <tasa_rx>*

ancho de banda ip6 *estado*

ancho de banda ip6 *espectáculo*

ancho de banda ip6*agregar <IP1-IP2> <tx><rx><compartido>*

ancho de banda ip6*del <IP1-IP2> <tx><rx><compartido>*

Sintaxis Descripción

Parámetro	Descripción
en	Significa activar el límite de ancho de banda para cada IP.
apagado	Significa desactivar el límite de ancho de banda para cada IP.
predeterminado <tasa_tx> <tasa_rx>	Significa establecer la transmisión predeterminada (tx), la tasa de recepción (rx) del límite de ancho de banda (0-30000 Kbps/Mbps). <tx_rate>: Introduzca un número. <rx_rate>: Introduzca un número.
estado	Significa mostrar la configuración actual.
espectáculo	Significa mostrar todas las configuraciones de límite de ancho de banda del rango de IP.
añadir <IP1-IP2> <tx><rx><compartido>	<add>: Significa agregar el límite de ancho de banda para un rango de IPv6. <IP1-IP2>: especifique un rango para las direcciones IPv6. <tx><rx>: Significa el límite de ancho de banda para la tasa de transmisión y recepción. <compartido>: Significa que el ancho de banda será compartido para el rango de IPv6.
del <IP1-IP2> <tx><rx><compartido>	<del>: Significa eliminar el límite de ancho de banda para un rango de IPv6 por primera IP (IP1) o 'del todo'. <IP1-IP2>: especifique un rango para las direcciones IPv6. <tx><rx>: Significa el límite de ancho de banda para la tasa de transmisión y recepción. <compartido>: Significa que el ancho de banda será compartido para el rango de IPv6.

Ejemplo

```
> ancho de banda ip6 activado
> ancho de banda ip6 añadir 2001:ABCD::2-2001:ABCD::10 512 5M compartido
> estado del ancho de banda ip6

   Rango de IPv6:
      2001:ABCD::2 - 2001:ABCD::10 : Tx:512K Rx:5M compartido

   El límite de ancho de banda ip6 actual está activado

   La tasa de ancho de banda ip6 predeterminada actual es Tx: 2000K Rx: 8000K bps
> ancho de banda ip6 del 2001:ABCD::2
>
```

Comando Telnet: vista ipf

Usuarios de IPF para ver la versión del filtro de IP, para ver/establecer el indicador de registro, para ver las reglas de filtro de IP en ejecución.

Sintaxis

vista ipf*[-VdhrtzZ]*

Sintaxis Descripción

Parámetro	Descripción
-V	Significa mostrar la versión de este filtro IP.
- d	Significa mostrar las reglas de filtrado de datos en ejecución.
- h	Significa mostrar el número de aciertos de las reglas de filtrado.
-r	Significa mostrar las reglas de filtrado de llamadas y datos en ejecución.
- t	Significa mostrar toda la información a la vez.
-z	Significa borrar las estadísticas de una regla de filtro.
-Z	Significa borrar las estadísticas brutas del filtro IP.

Ejemplo

```
> vista ipf -V
ipf: Filtro IP: v3.3.1 (1852) Kernel: Filtro
IP: v3.3.1 En ejecución: sí

Indicadores de registro: 0x6055af1c = bloque, nomatch
Predeterminado: pasa todo, Registro: disponible
```

Comando Telnet: conjunto ipf

Este comando se utiliza para establecer la regla general, el conjunto de filtros y la regla de filtro para el cortafuegos.

Sintaxis

conjunto ipf <*Opciones***>**

conjunto ipf<*SET_NO***><***Opciones***>**

conjunto ipf<*CONJUNTO_NO***>*regla*<***RULE_NO***><***Opciones***>**

Sintaxis Descripción

Parámetro	Descripción
conjunto ipf<Opciones>	Significa establecer la configuración general del cortafuegos y la regla predeterminada.
ipf establecer <SET_NO><Opciones>	Significa configurar el conjunto de filtros de firewall, incluidos los comentarios y el siguiente conjunto de filtros.
ipf set <SET_NO> regla <RULE_NO> <Opciones>	Significa establecer la regla de firewall en el conjunto de filtros. Para obtener información detallada, consulte Comando Telnet: regla ipf.
Acerca del conjunto ipf<Opciones>	
-V	Significa visualizar la configuración del conjunto general.
- re <p1>	Significa configurar el filtro de datos. <p1>: especifique el número de índice (1 a 12) del perfil establecido. Para deshabilitar la configuración, ingrese "0".
- pag <p1><p2>	Significa configurar acciones para paquetes que no coinciden con ninguna regla y si registra syslog. <p1>: escriba "0" para permitir que pasen los paquetes que no coincidan con ninguna regla; Escriba "1" para bloquear los paquetes que no coincidan con ninguna regla. <p2>: "0" significa que el registro relacionado con la coincidencia de reglas no se registrará en Syslog; "1" significa que el registro relacionado con la coincidencia de reglas se registrará en Syslog. Por ejemplo, para configurar el pase para el paquete que no coincide con ninguna regla y habilitar syslog,***-pag 0 1***.
- R <v4/v6> <Habilitar/Deshabilitar>	Significa aceptar paquetes de enrutamiento de WAN. <v4/v6>: IPv4 o IPv6.

	<Habilitar/Deshabilitar>: Ingrese 0 (habilitar) o 1 (deshabilitar). Establezca Aceptar paquete de enrutamiento de WAN por IPv4, ingrese***-R v4 0***.
- L <p1>	Significa habilitar o deshabilitar la función de firewall de seguridad estricta. <p1>: ingrese 1 (habilitar) o 0 (deshabilitar).
- C <p1>	Significa configurar la página de códigos. <p1>: Introduzca un número de página de códigos (0 a 20). Por ejemplo, ipf establece -C 20. 0. Ninguno 1. ANSI(1250)-Europa Central 2. ANSI(1251)-cirílico 3. ANSI(1252)-Latin I 4. ANSI(1253)-griego 5. ANSI(1254)-turco 6. ANSI(1255)-hebreo 7. ANSI(1256)-Árabe 8. ANSI(1257)-Báltico 9. ANSI(1258)-Vietnam 10. OEM(437)-Estados Unidos 11. OEM(850)-latín multilingüe I 12 OEM (860)-portugués 13 OEM(861)-islandés 14 OEM (863)-francés canadiense 15 OEM (865)-nórdico 16. ANSI/OEM(874)-Tailandés 17 ANSI/OEM(932)-cambio japonés-JIS 18. ANSI/OEM(936)-chino simplificado GBK 19. ANSI/OEM(949)-coreano 20. ANSI/OEM(950)-chino tradicional Big5
-M <p1><p2>	Significa configurar APP Enforcement y Syslog. <p1>: Introduzca un número (0 a 32). Donde, 0 significa ninguno; 1 a 32 mens el número de índice del perfil. <p2>: "0" significa que el registro relacionado con el cumplimiento de aplicaciones no se registrará en Syslog; "1" significa que el registro relacionado con el cumplimiento de la aplicación se registrará en Syslog.
- Arriba <p1><p2>	Significa configurar el filtro de contenido de URL para los paquetes que no coinciden con ninguna regla. <p1>: Introduzca un número (0 a 8). Donde, 0 significa ninguno; 1 a 8 mens el número de índice del perfil. <p2>: "0" significa que el registro relacionado con el filtro de contenido de URL no se registrará en Syslog; "1" significa que el registro relacionado con el filtro de contenido de URL se registrará en Syslog.
- W <p1><p2>	Significa configurar el filtro de contenido web para paquetes que no coincidan con ninguna regla. <p1>: Introduzca un número (0 a 8). Donde, 0 significa ninguno; 1 a 8 mens el número de índice del perfil. <p2>: "0" significa que el registro relacionado con Web Content Filter no se registrará en Syslog; "1" significa que el registro relacionado con Web Content Filter se grabará en Syslog.
- D <p1><p2>	Significa configurar el filtro DNS para paquetes que no coincidan con ninguna regla. <p1>: Introduzca un número (0 a 8). Donde, 0 significa ninguno; 1 a 8 mens el número de índice del perfil. <p2>: "0" significa que el registro relacionado con el filtro DNS no se registrará en Syslog; "1" significa que el registro relacionado con el filtro DNS se registrará en Syslog.

- un <p1>	Significa configurar los ajustes avanzados.
- f <p1>	Significa aceptar grandes paquetes UDP o ICMP fragmentados entrantes. <p1>: ingrese 1 (habilitar) o 0 (deshabilitar).
- t <p1>	Significa habilitar o deshabilitar el Modo transparente. <p1>: ingrese 1 (habilitar) o 0 (deshabilitar).
- E <p1><p2>	Significa establecer el recuento máximo para la limitación de la sesión. <p1>: Introduzca un número (0 a 50000) <p2>: "0" significa que el registro relacionado con el control de sesión no se registrará en Syslog; "1" significa que el registro relacionado con el control de la sesión se grabará en Syslog.
- P <p1><p2>	Significa establecer la clase QoS. <p1>: Introduzca un número (0 a 4). 0: Ninguno 1: Clase 1 2: Clase 2 3: Clase 3 4: Clase predeterminada <p2>: "0" significa que el registro relacionado con la clase de QoS no se registrará en Syslog; "1" significa que el registro relacionado con la clase de QoS se registrará en Syslog.
- Y <p1><p2>	Significa configurar la gestión de usuarios. <p1>: Introduzca un número (-1 a 2). - 1: Ninguno 0: Todo 1: objeto de usuario 2: grupo de usuarios <p2>: 1 a 200 (si p1 se configura con 1, objeto de usuario) o 1 a 32 (si p1 se configura con 2, grupo de usuarios)
- y <p1>	Significa que el registro relacionado con la gestión de usuarios se registrará o no en Syslog. <p1>: ingrese 1 (habilitar) o 0 (deshabilitar).
-w <p1>	Significa establecer el tamaño de la ventana del protocolo TCP. <p1>: Introduzca un valor (0 a 65535).
- Un <p1>	Significa habilitar o deshabilitar la función de captura de paquetes. <p1>: ingrese 1 (habilitar) o 0 (deshabilitar).
Acerca de ipf set <SET_NO><Opciones>	
- m <Comentarios>	Significa establecer un comentario para un conjunto de filtros. <Comentarios>: Introduzca una descripción para el conjunto de filtros.
-v	Significa ver el comentario y el siguiente conjunto de filtros.
- n <NEXT_SET_NO>	Significa especificar el siguiente conjunto de filtros del conjunto de filtros actual. <NEXT_SET_NO>: Introduzca un número (1 a 12). Por ejemplo, ipf establece 1 -n 2.

Ejemplo

```
> ipf set -R "v4 1"
Configuración guardada.
> ipf set -R "v6 1"
Configuración guardada.
> conjunto ipf -v
Filtro de datos: Habilitar (Conjunto de filtros de inicio = 1)
```

```
Marca de registro      : Desactivar

Acciones para paquetes que no coinciden con ninguna regla:
   Pasar o Bloquear         : Aprobar
   Página de código         : ANSI(1252)-Latín I
   Límite máximo de sesiones: 60000
   sesiones actuales        : 0
   IP de vinculación de Mac : No estricto
   Clase QOS                : Ninguno
   Captura de paquetes      : Desactivar
   Cumplimiento de la aplicación : Ninguno
   Filtro de contenido URL: Ninguno
   Filtro de contenido WEB: Ninguno
   Filtro DNS               : Ninguno
   Política de equilibrio de carga: selección automática
   ---------------------------------------------------------------------- Página
   de código                : ANSI(1252)-Latín I
   Tamaño de ventana        : 65535
   Hora de término de la sesión : 60
   Banner DrayTek           : Permitir
   ----------------------------------------------------------------------
   Aceptar grandes paquetes entrantes UDP o ICMP fragmentados: habilitar el modo
   transparente                                          : Desactivar
   ---------------------------------------------------------------------- Bloquear
   paquete de enrutamiento desde WAN:
      [iv] IPv4
      [iv] IPv6
   ----------------------------------------------------------------------
   [v] Activar cortafuegos de seguridad estricta l
>
```

Comando Telnet: regla ipf

Este comando se utiliza para establecer la regla de filtrado para el cortafuegos.

Sintaxis

regla ipf*señor*[-<comando> <parámetro> | ***...***

regla ipf sr -v

Sintaxis Descripción

Parámetro	Descripción
s	Significa el conjunto de filtros. s: Ingrese un valor (1 a 12).
r	Significa Regla de filtro r: Introduzca un valor (1~7).
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]* significa que puede escribir varios comandos en una línea.
- mi <0/1>	Significa habilitar o deshabilitar la configuración de la regla. 0: deshabilitar 1: habilitar
-v	Se utiliza para mostrar la configuración actual de la regla de filtro.
- D <valor>	Significa establecer la dirección del flujo de paquetes. Es para**Filtro de datos** solo.

	0: LAN/DMZ/RT/VPN -> WAN 1: WAN -> LAN/DMZ/RT/VPN 2: LAN/DMZ/RT/VPN -> LAN/DMZ/RT/VPN
- Yo "<e/d><para1, para2,...>"	Significa configurar la interfaz de entrada. e: Habilitar la función. d: Deshabilitar la función. Para1, para2,...: Los valores disponibles incluyen todos, LAN1, LAN2,...LAN8, RT, VPN, WAN1, WAN2,...WAN9 Ejemplo: > regla ipf 3 1 -e 1 -I "e LAN1"
- O "<e/d><párrafo 1, párrafo 2,...>"	Significa configurar la interfaz de salida. e: Habilitar la función. d: Deshabilitar la función. Para1, para2,...: Los valores disponibles incluyen todos, LAN1, LAN2,...LAN8, RT, VPN, WAN1, WAN2,...WAN9 Ejemplo: > regla ipf 3 1 -e 1 -O "e LAN2"
- s "o|o6|g|g6|c <campo> <obj>"	Significa especificar el objeto de IP de origen, el grupo de IP. o: Indica “objeto IPv4”. o6: Indica objeto IPv6". g: Indica "grupo IPv4". g6: Indica "grupo IPv6". c: Indica objeto país. campo: Indica la cantidad de objetos/grupos que se pueden configurar para esta regla a la vez. - Se permiten 2 perfiles de objeto para IPv4 - Se permiten 2 perfiles de grupo para el grupo IPv4 - Se permiten 3 perfiles de objeto para IPv6 - Se permite 1 perfil de grupo para el grupo IPv6 obj : indica el número de índice del objeto o el número de índice del grupo. - Rango para IPv4, de 1 a 192, 0 significa ninguno. - Rango para grupo IPv4, de 1 a 32, 0 significa ninguno. - Rango para IPv6, de 1 a 64, 0 significa ninguno. - Rango para grupo IPv6, de 1 a 32, 0 significa ninguno. - Rangos por objeto país, de 1 a 32. Por ejemplo, -s "o 1 2" significa que los perfiles de objeto IPv4 1 y 2 se configuran como IP de origen. Ejemplo: > regla ipf 3 1 -e 1 -s "o 1 2"
- d "o|o6|g|g6|c <campo> <obj>"	Significa especificar objeto de IP de destino, grupo de IP. o: Indica “objeto IPv4”. o6: Indica objeto IPv6". g: Indica "grupo IPv4". g6: Indica "grupo IPv6". c: Indica objeto país. campo: Indica la cantidad de objetos/grupos que se pueden configurar para esta regla a la vez. - Se permiten 2 perfiles de objeto para IPv4 - Se permiten 2 perfiles de grupo para el grupo IPv4 - Se permiten 3 perfiles de objeto para IPv6 - Se permite 1 perfil de grupo para el grupo IPv6 obj : indica el número de índice del objeto o el número de índice del grupo. - Rango para IPv4, de 1 a 192, 0 significa ninguno. - Rango para grupo IPv4, de 1 a 32, 0 significa ninguno. - Rango para IPv6, de 1 a 64, 0 significa ninguno. - Rango para grupo IPv6, de 1 a 32, 0 significa ninguno.

	- Rango por objeto país, de 1 a 32. Por ejemplo, -s "o 1 2" significa que los perfiles de objeto IPv4 1 y 2 se establecen como IP de destino. Ejemplo: > regla ipf 3 1 -e 1 -d "o 2 2"
– d "tu<Tipo de dirección> <Dirección IP inicial> <Dirección IP final> | <Máscara de dirección>"	significa configurar**destino**Dirección IP, incluido el tipo de dirección, la dirección IP inicial, la dirección IP final y la máscara de dirección. u: Significa "definido por el usuario". *Tipo de dirección*:Escriba el número (que representa un tipo de dirección diferente). 0: Dirección de subred 1: Dirección única 2: Cualquier dirección 3: Ejemplo de dirección de rango: Establecer dirección de subred => -d "u 0 192.168.1.10 255.255.255.0" Establecer dirección única => -d "u 1 192.168.1.10 " Establecer cualquier dirección => -d "u 2 " Establecer dirección de rango => -d "u 3 192.168.1.10 192.168.1.15"
- So|g <obj>	Significa especificar el objeto Tipo de servicio. o : indica perfil “objeto”. g: indica perfil de “grupo”. <obj> : indica el número de índice del objeto o el número de índice del grupo. Los ajustes disponibles van de 1 a 96. Por ejemplo, -S "o 1" significa el primer perfil de objeto de tipo de servicio.
- S "u <protocolo> <valor_puerto_origen> <destino_puerto_vale>"	Significa configurar ajustes avanzados para el tipo de servicio, como el protocolo y el rango de puertos. u: significa "definido por el usuario". <protocolo>: Significa TCP(6),UDP(17), TCP/UDP(255), Cualquiera(0), ICMP(1), ICMPv6(58), Otro(otro) <valor_puerto_origen> : 1: Puerto OP, el rango es 0-3. 0:= =, 1:!=, 2:>, 3:< 3: Rango de puertos del número de puerto de inicio, el rango es 1-65535. 5: rango de puertos del número de puerto final, el rango es 1-65535. <valor_puerto_destino>: 2: Puerto OP, el rango es 0-3, 0:==, 1:!=, 2:>, 3:< 4 : Rango de puertos del número de puerto de inicio, el rango es 1-65535. 6: rango de puertos del número de puerto final, el rango es 1-65535.
- f <valor>	Significa establecer el tipo de fragmento. 0: No me importa. 1 : Sin fragmentar. 2: Fragmentado. 3: Demasiado corto
- F "<Parámetro 0> <Parámetro 1>"	Significa la acción de filtro que puede especificar. <parámetro 0>: Ingrese el número para establecer la acción de filtrado. 0 : Pase inmediatamente. 1: Bloquear inmediatamente. 2: Pase si no hay más coincidencias. 3: Bloquear si no hay más coincidencias. <Param 1>: Permite que el registro se grabe en Syslog. 0 : Deshabilitar registro. 1 : Habilitar registro.

- m "<Parámetro 0> <Parámetro 1>"	Significa establecer el tipo de IP de enlace MAC y el Syslog. <param 0>: Introduzca el número para elegir el tipo. 0 : No estricto. 1: estricto. <Param 1>: Permite que el registro se grabe en Syslog. 0 : Deshabilitar registro. 1 : Habilitar registro.
- Y <Parámetro 0> <Parámetro 1>	Significa configurar la gestión de usuarios. <param 0>: Introduzca el número para elegir el tipo. - 1 : Ninguno. 0 : Todo. 1: Objeto de usuario 2: grupo de usuarios <Param 1>: Deje que el registro se registre en Syslog si <param 0> está configurado con Ninguno/TODO. 0 : Deshabilitar. 1 : Habilitar. Ingrese el número de objeto de usuario (1 a 200) / número de grupo (1 a 32) si el <parámetro 0> está configurado con Objeto de usuario.
- y <valor>	Significa que el registro relacionado con la gestión de usuarios se registrará o no en Syslog. <valor>: ingrese 1 (habilitar) o 0 (deshabilitar)
- L <Parámetro 0> <Parámetro 1>	Significa establecer el recuento máximo para la limitación de la sesión. <param 0>: Introduzca el número (0 a 60000) para elegir el tipo. <Param 1>: Permite que el registro se grabe en Syslog. 0 : Deshabilitar. 1 : Habilitar.
- q <Parámetro 0> <Parámetro 1>	Significa establecer la clasificación para QoS. <Parámetro 0>: 1– Clase 1, 2 – Clase 2, 3 – Clase 3, 4 – Otro <Param 1>: Permite que el registro se grabe en Syslog. 0 : Deshabilitar. 1 : Habilitar.
- Un "<Parámetro 0>"	Significa habilitar o deshabilitar la función de captura de paquetes. <Param 0>: Ingrese 0 o 1. 0 : Deshabilitar. 1 : Habilitar.
- l <Parámetro 0> <Parámetro 1>	Significa política de equilibrio de carga. Esta función se usa solo para "depurar". <Param 0>: Introduzca 0, 1, 2 o 3. 0:Selección automática, 1: WAN 1. 2: WAN 2. 3: WAN 3. <Param 1>: Ingrese 0 o 1. 0: Deshabilitar registro. 1:Habilitar registro.
- un "<parámetro 0> <parámetro 1>"	Significa especificar qué perfil de cumplimiento de aplicaciones se aplicará.

	<Param 0>: Los ajustes disponibles van de 0 a 32. “0” significa que no se aplicará ningún perfil. <Param 1>: permite que el registro se registre en Syslog. 0 : Deshabilitar. 1 : Habilitar.
- u <Parámetro 0> <Parámetro 1>	Significa especificar qué perfil de filtro de contenido de URL se aplicará. <Param 0>: Los ajustes disponibles van de 0 a 8. “0” significa que no se aplicará ningún perfil. <Param 1>: permite que el registro se registre en Syslog. 0 : Deshabilitar. 1 : Habilitar.
- w "<Parámetro 0> <Parámetro 1>"	Significa especificar qué perfil de filtro de contenido web se aplicará. <Param 0>: Los ajustes disponibles van de 0 a 8. “0” significa que no se aplicará ningún perfil. <Param 1>: permite que el registro se registre en Syslog. 0 : Deshabilitar. 1 : Habilitar.
- n "<Parámetro 0> <Parámetro 1>"	Significa especificar qué perfil de filtro DNS se aplicará. <Param 0>: Los ajustes disponibles van de 0 a 8. “0” significa que no se aplicará ningún perfil. <Param 1>: permite que el registro se registre en Syslog. 0 : Deshabilitar. 1 : Habilitar.
- N <valor>	Significa establecer el siguiente conjunto de filtros. <valor>: Los ajustes disponibles van de 0 a 12. “0” significa que no se aplicará ningún perfil. 0 : Ninguno 1 : Juego #1; 2: Conjunto #2, y así sucesivamente.
-c<0~20>	Significa configurar la página de códigos. Un número diferente representa una página de códigos diferente. 0. Ninguno 1. ANSI(1250)-Europa Central 2. ANSI(1251)-cirílico 3. ANSI(1252)-Latin I 4. ANSI(1253)-griego 5. ANSI(1254)-turco 6. ANSI(1255)-hebreo 7. ANSI(1256)-Árabe 8. ANSI(1257)-Báltico 9. ANSI(1258)-Vietnam 10. OEM(437)-Estados Unidos 11. OEM(850)-latín multilingüe I 12 OEM (860)-portugués 13 OEM(861)-islandés 14 OEM (863)-francés canadiense 15 OEM (865)-nórdico 16. ANSI/OEM(874)-Tailandés 17 ANSI/OEM(932)-cambio japonés-JIS 18. ANSI/OEM(936)-chino simplificado GBK 19. ANSI/OEM(949)-coreano 20. ANSI/OEM(950)-chino tradicional Big5
- C "<Tamaño de Windows>	Significa establecer el tamaño de la ventana y el tiempo de espera de la sesión (minuto).

<Tiempo de espera_de_sesión>"	<Tamaño de Windows>: la configuración disponible oscila entre 1 y 65535. <Session_Timeout>: aproveche al máximo los recursos de la red.
- b <valor>	Significa habilitar o deshabilitar DrayTek Banner. <valor>: 0 : Deshabilitar; 1 : Habilitar.
- t "i <Parámetro 0> <Parámetro 1>"	Significa establecer el perfil de programación. En total, se pueden especificar cuatro conjuntos de perfiles de programación. <param 0>: Ingrese el número de índice (1 a 4) para cada conjunto. <parámetro 1>: Ingrese el número de índice (0 a 15) del perfil de programación para cada conjunto. 0 significa ninguno. Por ejemplo, -t "i 1 3" significa que el perfil de programación n.º 3 está configurado para el conjunto n.º 1. Ejemplo: > regla ipf 3 1 -e 1 -t "i 1 3"
- t "c <valor>"	Significa habilitar o deshabilitar la función de borrar sesiones cuando el horario está activado. <valor>: 0 : Deshabilitar; 1 : Habilitar.
- M <Tus comentarios>	Significa establecer comentarios para la regla del filtro. <Tus comentarios>: Ingresa una breve descripción.
- U "<arriba/abajo>"	Significa subir o bajar el orden de una regla de filtro en el conjunto de filtros. arriba: Indica mover la regla de filtrado hacia arriba. down: Indica mover la regla de filtrado hacia abajo.

Ejemplo

```
> regla ipf 2 1 -v Conjunto
de filtros 2 Regla 1:

Estado: Deshabilitar
Comentarios: <null>
Índice (1-15) en Configuración de programación: <null>, <null>, <null>, <null>

Borrar sesiones cuando el horario está activado: deshabilitar

Dirección          : LAN/DMZ/RT/VPN -> WAN
Interfaz Src: LAN1, LAN2, LAN3, LAN4, LAN5, LAN6, LAN7, LAN8, DMZ, enrutado, VPN


Interfaz Dst: WAN1, WAN2, WAN3, WAN4, WAN5, WAN6, WAN7, WAN8, WAN9 IP de origen:
cualquiera
IP de destino: Cualquiera
Tipo de servicio    : Cualquier
Fragmentos          : no me importa

Pasar o Bloquear                : Pasar inmediatamente
Rama a otro conjunto de filtros: Ninguno
Límite máximo de sesiones       : 60000
Sesiones actuales               : 0
IP de vinculación de Mac        : No estricto
Clase QoS                       : Ninguno
Captura de paquetes             : Desactivar
Cumplimiento de la aplicación   : Ninguno
Filtro de contenido de URL      : Ninguno
Filtro de contenido WEB         : Ninguno
Filtro DNS                      : Ninguno
Política de equilibrio de carga : Selección automática
```

```
Registro                              : Desactivar
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - Página
de código                             : ANSI(1252)-Latín I
Tamaño de ventana                     : 65535
Hora de término de la sesión          : 60
Banner DrayTek                        : Permitir
  - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
  Control estricto de seguridad
    [ ] Cumplimiento de la aplicación
>
```

Comando Telnet: pista de flujo ipf

Este comando se utiliza para establecer y ver sesiones de seguimiento de flujo.

Sintaxis

conjunto de pista de flujo ipf *<-r/-e>*

vista de pista de flujo ipf *<-f/-b>*

Sintaxis Descripción

Parámetro	Descripción
-r	Significa actualizar la pista de flujo.
- mi	Significa habilitar o deshabilitar el flowtrack.
- f	Significa mostrar el estado de las sesiones de flowtrack. Si no especifica ninguna dirección IP, se mostrará todo el estado de la sesión de flowtrack.
- b	Significa mostrar el estado de todas las sesiones de IPv6.

Ejemplo

```
> ipf flowtrack set -r Actualizar el
estado de flujo ok
> vista de seguimiento de flujo ipf -f
Comience a mostrar el estado de las sesiones de flowtrack:

ORIGEN>>      192.168.1.11:59939 ->             8.8.8.8: 53, si no = 0
RESPONDER >>          8.8.8.8: 53 ->            192.168.1.11:59939, si no = 3
          proto=17, edad=93023180(3920), bandera=203
          ORIGEN>> 192.168.1.11:15073 ->        8.8.8.8:     53 ,si no=0
RESPONDER >>          8.8.8.8: 53 ->            192.168.1.11:15073, si no = 3
          proto=17, edad=93025100(2000), bandera=203
          ORIGEN>> 192.168.1.11: 7247 ->        8.8.8.8:     53 ,si no=0
RESPONDER >>          8.8.8.8: 53 ->            192.168.1.11: 7247, si no = 3
          proto=17, age=93020100(7000), flag=203 End para
mostrar el estado de las sesiones de flowtrack
> ipf flowtrack set -e Flujo
actual_habilitar=0
> ipf flowtrack set -e Curretn
flow_enable=1
>
```

Comando Telnet: Registro

Este comando permite a los usuarios ver el registro de la interfaz WAN, como el registro de llamadas, el registro de filtro de IP, el búfer de registro de vaciado, etc.

Sintaxis

registro*[-cfhiptwx?] [-F a | do | f | w]*

Sintaxis Descripción

Parámetro	Descripción
- C	Significa mostrar el último registro de llamadas.
- f	Significa mostrar el registro del filtro IP.
-F	Significa mostrar el búfer de registro de descarga. a: vaciar todos los registros c: vaciar el registro de llamadas f: vaciar el registro de filtro de IP w: vaciar el registro de WAN
- h	Significa mostrar esta ayuda de uso.
- pag	Significa mostrar el registro de PPP/MP.
- t	Significa mostrar todos los registros guardados en el búfer de registro.
- w	Significa mostrar el registro WAN.
- X	Significa mostrar el volcado hexadecimal del cuerpo del paquete.

Ejemplo

```
> registro -w
25:36:25.580 ---->DHCP (WAN-5) Largo = 548XID = 0x7880fdd4
        IP del cliente          = 0.0.0.0
        Tu dirección Ip         = 0.0.0.0
        IP del siguiente servidor = 0.0.0.0 IP del
        agente de retransmisión = 0.0.0.0
25:36:33.580 ---->DHCP (WAN-5) Largo = 548XID = 0x7880fdd4
        IP del cliente          = 0.0.0.0
        Tu dirección Ip         = 0.0.0.0
        IP del siguiente servidor = 0.0.0.0 IP del
        agente de retransmisión = 0.0.0.0
25:36:41.580 ---->DHCP (WAN-5) Largo = 548XID = 0x7880fdd4
        IP del cliente          = 0.0.0.0
        Tu dirección Ip         = 0.0.0.0
        IP del siguiente servidor = 0.0.0.0 IP del
        agente de retransmisión = 0.0.0.0
25:36:49.580 ---->DHCP (WAN-5) Largo = 548XID = 0x7880fdd4
        IP del cliente          = 0.0.0.0
        Tu dirección Ip         = 0.0.0.0
        IP del siguiente servidor = 0.0.0.0 IP del
        agente de retransmisión = 0.0.0.0
25:36:57.580 ---->DHCP (WAN-5) Longitud = 548XID = 0x7880fdd4
        IP del cliente          = 0.0.0.0
        Tu dirección Ip         = 0.0.0.0
- - - MÁS ---          ['q': Salir, 'Entrar': Líneas nuevas, 'Barra espaciadora': Página siguiente] ---
```

Comando Telnet: usuario ldap

Este comando se utiliza para configurar el perfil LDAP.

Sintaxis

usuario ldap*<ÍNDICE><OPCIÓN>*

Sintaxis Descripción

Parámetro	Descripción
ÍNDICE	Especifique el número de índice (1 a 8) del perfil LDAP.
OPCIÓN	
- n VALOR	Nombre del perfil de configuración.
- b VALOR	Nombre distinguido de la base de configuración.
- un valor	Configurar filtro adicional.
- g VALOR	Nombre distinguido del grupo de configuración.
- c VALOR	Configurar el identificador de nombre común.
-v	Ver información detallada del perfil LDAP.

Ejemplo

```
> ldap usuario 1 -n LD_user_test1 ¡El
nombre del perfil ha sido actualizado!
> usuario ldap 1 -v
Índice de perfil: 1
Nombre de perfil: LD_user_test1
Identificador de nombre común:
Nombre distinguido base: Filtro
adicional:
Nombre distinguido del grupo:
>
```

Comando Telnet: conjunto ldap

Este comando se utiliza para establecer la configuración general (p. ej., dirección IP, número de puerto) para el servidor LDAP.

Sintaxis

conjunto ldap*<Opciones><Valor>*

Sintaxis Descripción

Parámetro	Descripción
habilitar <0-1>	Activa o desactiva la función LDAP. 0 : Deshabilitar la función. 1 : Habilitar la función.
escriba <0-2>	Establezca el tipo de enlace como Simple (0), Anónimo (1) y Regular (2).
SSL <0-1>	Habilite o deshabilite la función LDAP a través del túnel SSL. 0 : Deshabilitar la función. 1 : Habilitar la función.
IP <VALOR>	Configure la dirección IP para el servidor LDAP.
puerto <VALOR>	Establezca el número de puerto para el servidor LDAP.

dn <VALOR>	Establecer el valor de DN regular
PCD <VALOR>	Establezca el valor de contraseña regular.

Ejemplo

```
> ldap set enable 1 ¡LDAP
habilitado!
> ldap habilitado.
> conjunto ldap ssl 1
¡Se ha habilitado LDAP con SSL!
> ldap set IP 192.168.100.155 Se ha
configurado la IP del servidor LDAP.
> ldap establecer puerto 389
El puerto del servidor LDAP se ha configurado.
> ldap set dn dc=example,dc=com LDAP
Regular DN ha sido configurado.
> conjunto ldap PWD 123456
Se ha configurado la contraseña normal de LDAP.
```

Comando Telnet: vista ldap

Este comando se utiliza para comprobar el estado actual de la configuración de los ajustes de LDAP.

Sintaxis

vista ldap

Ejemplo

```
> vista ldap?
Activar LDAP: Desactivado.
Tipo de enlace LDAP:Simple
LDAP con SSL: Deshabilitado
DN normal de LDAP:
Contraseña normal de LDAP:
IP del servidor LDAP:
Puerto del servidor LDAP: 389
>
```

Comando Telnet: conjunto tacacsplus

Este comando permite a los usuarios configurar los ajustes generales para el servidor TACACS+.

Sintaxis

tacacsplus conjunto*<Opciones><Valor>*

Sintaxis Descripción

Parámetro	Descripción
habilitar <0/1>	Deshabilitar (0)/habilitar (1) el servidor TACACS+.
IP <VALOR>	Configure la dirección IP del servidor TACACS+.
puerto <VALOR>	Configure el número de puerto del servidor TACACS+.
secreto_compartido <VALOR>	Establezca el valor del secreto compartido del servidor TACACS+.

Ejemplo

```
> tacacsplus set enable 1
¡TACACS+ habilitado!
  Esta configuración tendrá efecto después de reiniciar. Utilice el
  comando "sys reboot" para reiniciar el enrutador.

> tacacsplus set IP 192.168.1.59 Se ha
configurado la IP del servidor TACACS+.
  Esta configuración tendrá efecto después de reiniciar. Utilice el
  comando "sys reboot" para reiniciar el enrutador.
> vista tacacsplus
TACACS+ Activar: Activar.
IP del servidor TACACS+: 192.168.1.59
Puerto del servidor TACACS+: 49
TACACS+ Tipo:ASCII
Secreto compartido de TACACS+:
>
```

Comando Telnet: vista tacacsplus

Este comando permite a los usuarios verificar la configuración general del servidor TACACS+

Sintaxis

tacacsplus vista

Ejemplo

```
> vista tacacsplus
TACACS+ Activar: Activar.
IP del servidor TACACS+: 192.168.1.59
Puerto del servidor TACACS+: 49
TACACS+ Tipo:ASCII
Secreto compartido de TACACS+:
```

Comando Telnet: mngt ftpport

Este comando permite a los usuarios configurar el puerto FTP para la administración.

Sintaxis

soporte de administración *<Puerto FTP>*

Sintaxis Descripción

Parámetro	Descripción
puerto ftp	Significa Ingresar el número para el puerto FTP. La configuración predeterminada es 21.

Ejemplo

```
> gestión ftpport 21

% Establezca el puerto del servidor FTP en 21 hecho.
```

Comando Telnet: mngt httpport

Este comando permite a los usuarios configurar el puerto HTTP para la administración.

Sintaxis

gestión de puerto http*<Puerto HTTP>*

Sintaxis Descripción

Parámetro	Descripción
puerto HTTP	Significa ingresar el número para el puerto HTTP. La configuración predeterminada es 80.

Ejemplo

```
> gestionar httpport 80
% Establezca el puerto del servidor web en 80 hecho.
```

Comando Telnet: mngt httpsport

Este comando permite a los usuarios configurar el puerto HTTPS para la administración.

Sintaxis

gestión httpsport*<Puerto HTTPS>*

Sintaxis Descripción

Parámetro	Descripción
puerto HTTPS	Significa Ingresar el número para el puerto HTTPS. La configuración predeterminada es 443.

Ejemplo

```
> gestión httpssport 443
% Establezca el puerto del servidor web en 443 hecho.
```

Comando Telnet: mngt sslvpnport

Este comando permite a los usuarios configurar el puerto SSL VPN para la administración.

Sintaxis

administración sslvpnport <*Puerto VPN SSL>*

Sintaxis Descripción

Parámetro	Descripción
Puerto VPN SSL	Significa escribir el número para el puerto SSL VPN. La configuración predeterminada es 443.

Ejemplo

```
> administración sslvpnport 1010
% Establezca el puerto SSL VPN en 1010 hecho.
```

Comando Telnet: mngt telnetport

Este comando permite a los usuarios configurar el puerto telnet para la administración.

Sintaxis

administración de telnetport*<puerto telnet>*

Sintaxis Descripción

Parámetro	Descripción
puerto telnet	Significa Ingresar el número para el puerto telnet. La configuración predeterminada es 23.

Ejemplo

```
> gestión telnetport 23
% Establezca el puerto del servidor Telnet en 23 hecho.
```

Comando Telnet: mngt sshport

Este comando permite a los usuarios configurar el puerto SSH para la administración.

Sintaxis

puerto de gestión *<puerto ssh>*

Sintaxis Descripción

Parámetro	Descripción
puerto ssh	Significa Ingresar el número para el puerto SSH. La configuración predeterminada es 22.

Ejemplo

```
> gestión puerto 23
% Establezca el puerto ssh en 23 hecho.
```

Comando Telnet: mngt noping

Este comando se usa para pasar o bloquear Ping desde la LAN PC a Internet.

Sintaxis

gestión no *en*

gestión no *apagado*

gestión no *ver registro*

gestión no *borrar registro*

Sintaxis Descripción

Parámetro	Descripción
en	Todos los paquetes PING se reenviarán desde la PC LAN a Internet.
apagado	Todos los paquetes PING serán bloqueados desde LAN PC a Internet.
ver registro	Significa mostrar un registro de la acción de ping, incluida la MAC de origen y la IP de origen.
borrar registro	Significa borrar el registro de la acción de ping.

Ejemplo

```
> mngt nopeando
¡Ninguna salida de paquete de ping está DESACTIVADA!
```

Comando Telnet: gusano de defensa mngt

Este comando puede bloquear el puerto especificado para pasar a través del enrutador.

Sintaxis

Gusano de defensa *en*

Gusano de defensa *apagado*

Gusano de defensa *<añadir puerto>*

Gusano de defensa *<del puerto>*

Gusano de defensa *<ver registro>*

Gusano de defensa *<borrar registro>*

Sintaxis Descripción

Parámetro	Descripción
en	Significa activar la función de defensa contra el paquete de gusanos.
apagado	Significa desactivar la función de defensa contra el paquete de gusanos.
añadir puerto	Significa agregar un nuevo puerto TCP para el bloque.
del puerto	Significa eliminar un puerto TCP para bloquear.
ver registro	Significa mostrar un registro del paquete de gusanos de defensa, incluidas la MAC de origen y la IP de origen.
borrar registro	Significa eliminar el registro del paquete del gusano de defensa.

Ejemplo

```
> mngt defenseworm agregar 21
Agregar puerto TCP 21
Bloquear lista de puertos TCP: 135, 137, 138, 139, 445, 21
> mngt defenseworm del 21
Borrar puerto TCP 21
Bloquear lista de puertos TCP: 135, 137, 138, 139, 445
```

Comando Telnet: mngt rmtcfg

Este comando puede permitir que los administradores del sistema inicien sesión desde Internet. Por defecto, no está permitido.

Sintaxis

administración rmtcfg *<estado>*

administración rmtcfg *<habilitar>*

administración rmtcfg *<deshabilitar>*

administración rmtcfg *<http/https/ftp/telnet/ssh/tr069/snmp/enforce_https> <activar/desactivar>*

Sintaxis Descripción

Parámetro	Descripción
estado	Significa mostrar la configuración actual para su referencia.
permitir	Significa permitir que los administradores del sistema inicien sesión desde Internet.
desactivar	Significa negar a los administradores del sistema el inicio de sesión desde Internet.
http/https/ftp/telnet/ssh/tr069/snmp/enforce_https	Significa especificar uno de los servidores/protocolos para habilitar o deshabilitar.
encendido apagado	encendido: habilita la función.

	off: desactiva la función.

Ejemplo

```
> mngt rmtcfg ftp en
Habilitar falla del servidor
La función de configuración remota ha sido deshabilitada,
habilítela ingresando mngt rmtcfg enable

> mngt rmtcfg habilitar
%% La función de configuración remota se ha habilitado.
>  mngt rmtcfg ftp activado
Se ha habilitado el %% servidor FTP.
```

Comando Telnet: mngt lanaccess

Este comando permite a los usuarios administrar el acceso al enrutador Vigor a través del puerto LAN.

Sintaxis

lanaccess*-e <0/1> –s <valor> –i <valor>*

lanaccess*–I* **lanaccess***–mi*

lanaccess*–F*
lanaccess*–d*
lanaccess*–v*
lanaccess*–h*

Sintaxis Descripción

Parámetro	Descripción
- mi <0/1>	Significa habilitar/deshabilitar la función. 0-deshabilitar la función. 1-habilitar la función.
- s <valor>	Significa especificar el servicio ofrecido. Los valores disponibles incluyen: FTP, HTTP, HTTPS, ENFORCE_HTTPS, TELNET, SSH, Ninguno, Todos
- yo <valor>	Significa la interfaz a la que se le permite acceder. Los valores disponibles incluyen: LAN2~LAN16, DMZ, subred enrutada por IP, ninguna, todas **Nota**: LAN1 siempre está permitida para acceder al enrutador.
- Yo <valor>	Significa el índice de objetos de IP al que se permite acceder. Los valores disponibles incluyen: 1 a 192.
-E<0/1>	Significa habilitar la función de IP específica permitida para acceder. 0-deshabilitar la función. 1-habilitar la función.
- f	Significa vaciar todos los ajustes.
- d	Significa restaurar la configuración predeterminada de fábrica.
-v	Significa ver la configuración actual.
- h	Significa obtener el uso de dicho comando.

Ejemplo

```
> administración lanaccess -e 1
> administración lanaccess -s FTP, TELNET
> administración lanaccess -i LAN3
> administración lanaccess -v
Configuración de control de acceso LAN actual:
* Habilitar: Sí
   -FTP: Sí
   -HTTP: Sí
   -HTTPS: Sí
   - TELNET: Sí
   -SSH: Sí
   - TR069: Sí
   - Hacer cumplir HTTPS: No
  Subred:
      - LAN 1: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - LAN 2: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - LAN 3: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - LAN 4: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - LAN 5: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - LAN 6: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - LAN 7: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - LAN 8: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - LAN 9: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - LAN 10: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - LAN 11: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - LAN 12: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - LAN 13: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - LAN 14: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - LAN 15: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - LAN 16: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - DMZ: habilitado
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
   - Subred enrutada por IP: habilitada
      - La IP específica (tipo: objeto IP) (índice: 0) está deshabilitada
>
```

Comando Telnet: mngt echoicmp

Este comando permite a los usuarios rechazar o aceptar paquetes PING de Internet.

Sintaxis

gestión ecoicmp *<habilitar>*

gestión ecoicmp *<deshabilitar>*

Sintaxis Descripción

Parámetro	Descripción
permitir	Significa aceptar el paquete echo ICMP.
desactivar	Significa descartar el paquete echo ICMP.

Ejemplo

```
> mngt echoicmp enable %% Paquete
Echo ICMP habilitado.
```

Comando Telnet: lista de acceso mngt

Este comando le permite especificar que el administrador del sistema puede iniciar sesión desde un host o red específicos. Se permite un máximo de diez IP/máscaras de subred.

Sintaxis

lista de acceso de administración *lista*

lista de acceso de administración *agregar <Índice><Índice de objetos IP>* **lista de acceso de administración** *eliminar <Índice>* **lista de acceso de administración** *enjuagar*

Sintaxis Descripción

Parámetro	Descripción
lista	Puede mostrar la configuración actual para su referencia.
agregar	Significa agregar una nueva entrada.
<Índice><Índice de objetos IP>	Significa especificar el objeto IP. Configuraciones disponibles: <índice>: ingrese el número de índice del perfil de la lista de acceso. <Índice de objetos de IP>: ingrese el número de índice del objeto de IP.
No.	Se permite asignar un máximo de 10 objetos IP.
índice	Significa el número de índice (1 a 192) de los objetos IP preconfigurados.
eliminar	Significa eliminar el elemento seleccionado.
enjuagar	Significa eliminar todas las configuraciones en la lista de acceso.

Ejemplo

```
> mngt accesslist agregar 1 1 %%
Establezca Aceptar.
> lista de lista de acceso mngt
%% Lista de acceso:
```

```
  [Índice]          [Índice de objetos IP]          [IP/CIDR o StartIP ~ EndIP]
================================================== ====================
  1                 1                               Por favor, configure el índice = 1 para el objeto IP

>
```

Comando Telnet: mgt wanlogin

Este comando le permite habilitar o deshabilitar la función de inicio de sesión WAN.

Sintaxis

iniciar sesión*permitir*

iniciar sesión*desactivar*

Ejemplo

```
> mngt wanlogin enable %%
wanlogin habilitado.
>
```

Comando Telnet: mngt snmp

Este comando le permite configurar SNMP para la administración.

Sintaxis

administración snmp*[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede ingresar varios comandos en una línea.
- mi <1/2>	1: Habilite la función SNMP. 2: deshabilite la función SNMP.
- un <1/2>	1: Habilitar la función SNMPV1. 2: Deshabilitar la función SNMPV1.
- b <1/2>	1: Habilitar la función SNMPV2C. 2: Deshabilitar la función SNMPV2C.
-c<1/2>	1: Habilitar la función SNMPV3. 2: Deshabilitar la función SNMPV3.
- g <Nombre de la comunidad>	Significa establecer el nombre para obtener comunidad escribiendo un carácter adecuado. (máx. 23 caracteres)
- s <Nombre de la comunidad>	Significa establecer comunidad escribiendo un nombre propio. (máx. 23 caracteres)
- m <dirección IP>	Significa configurar un host como administrador para ejecutar la función SNMP. Escriba la dirección IPv4 para especificar cierto host. Permite configurar 3 IPs, separadas por ",".
- t <Nombre de la comunidad>	Significa establecer una comunidad trampa escribiendo un nombre propio. (máx. 23 caracteres)
- n <dirección IP>	Significa configurar el host de notificación. Permite configurar 2 IPs, separadas por ",".
- T <segundos>	Significa establecer el tiempo de espera de trampa <0~999>.

- o <nombre de usuario>	Significa configurar una cuenta de usuario (máximo 23 caracteres) para la gestión de usuarios.
- pag <0/1/2>	Significa establecer el algoritmo de autenticación. 0: sin autorización 1: MD5_AUTH 2: SHA_AUTH
- q <contraseña>	Significa establecer la contraseña (máximo 23 caracteres) para la autenticación.
-r <0,3/4/6>	Significa establecer el algoritmo de privacidad 0, 3: No_PRIV 4: DES_PRIV 6: AES_PRIV
- tu <contraseña>	Significa establecer la contraseña (máximo 23 caracteres) para la privacidad.
-V	Significa enumerar la configuración de SNMP.

Ejemplo

```
> gestión snmp -e 1 -g draytek -s DK -m
192.168.1.20,192.168.5.192/26,10.20.3.40/24 -t trapcom -n
192.168.1.20,10.20.3.40 -T 88
¡¡¡Agente SNMP encienda!!! Obtener
  Community configurado en draytek Establecer
  Community configurado en DK
  Manager Host IP configurada en 192.168.1.20,192.168.5.192/26,10.20.3.40/24 Trap
  Community configurada en trapcom
  La IP del host de notificaciones se establece en 192.168.1.20, 10.20.3.40. El tiempo de
  espera de captura se establece en 88 segundos.
>
```

Comando Telnet: mngt bfp

Este comando le permite configurar la protección de fuerza bruta (BFP) para la administración del sistema.

Sintaxis

gestión bfp*[<comando><parámetro>|...]*

Sintaxis Descripción

Parámetro	Descripción
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]* significa que puede escribir varios comandos en una línea.
- mi 0/1	Activar/desactivar la función BFP. 0 – Deshabilitar 1 – Habilitar
- s <servicio>	Significa habilitar diferentes servicios. servicio: los tipos disponibles son FTP, HTTP, HTTPS, TELNET, TR069, SSH, VPN, Ninguno y Todos.
- l <fracaso>	Significa establecer tiempos de reintento de falla de inicio de sesión. falla: el número disponible es del 1 al 255.
- p <penalización>	Significa establecer tiempo de penalización para BFP. La unidad es seg.
- tu <IP>	Significa desbloquear una dirección IP en la lista.
-v	Significa ver la configuración actual.

Ejemplo

```
> administración bfp -e 1
> gestión bfp -s FTP
> administración bfp -l 10
> administración bfp -v
Configuración actual de protección de fuerza bruta:
* Habilitar: sí
* Servicio:
  -FTP:              Sí
  -HTTP:             No
  - HTTPS:           No
  -TELNET:           No
  -TR069:            No
  -SSH:              No
* Máximo de errores de inicio de sesión: 10
* Período de penalización: 0
```

Comando Telnet: mngt cert_import

Este comando le permite importar un certificado al enrutador Vigor.

Sintaxis

administración cert_import local_cert *<*

URL><contraseña> **gestión cert_import trust_ca** *<URL>*

Sintaxis Descripción

Parámetro	Descripción
local_cert url <URL> <contraseña>	URL: ingrese una URL (http://....) para descargar el certificado. El archivo está encriptado con el formato de archivo "xxxx.p12". Contraseña: ingrese la contraseña para descifrar el certificado .p12.
trust_ca <URL>	URL: ingrese una URL (http://....) para descargar el certificado. El archivo está encriptado con el formato de archivo "xxxx.p12".

Comando Telnet: mngt telnettimeout

Este comando le permite configurar el tiempo de espera para la conexión telnet.

Sintaxis

gestión telnettimeout *<valor>*

Sintaxis Descripción

Parámetro	Descripción
<valor>	Rango de 60 a 300. El valor predeterminado es 300 (segundos).

Ejemplo

```
> mngt telnettimeout 100 %
Telnet timeout : 100s

>
```

Comando Telnet: mngt sshtimeout

Este comando le permite configurar el tiempo de espera para la conexión SSH.

Sintaxis

gestión sshtimeout*<valor>*

Sintaxis Descripción

Parámetro	Descripción
<valor>	Rango de 60 a 300. El valor predeterminado es 180 (segundos).

Ejemplo

```
> mngt sshtimeout 200 % SSH
tiempo de espera: 200 s
>
```

Comando Telnet: mngt ip6_IIDs

Este comando le permite configurar la ID de la interfaz IPv6.

Sintaxis

administración de ip6-IID*-e <valor>>*

administración de ip6_IID*-r <interfaz>*

administración de ip6_IID*-s*

Sintaxis Descripción

Parámetro	Descripción
- e <valor>	Se utiliza para determinar la forma de generar la identificación de la interfaz IPv6. val = 0 : Usar IID EUI-64 como id de interfaz val = 1 : Usar IID aleatorios como id de interfaz
- r <interfaz>	Se utiliza para volver a generar los IID aleatorios de la interfaz especificada. interfaz = LAN1/LAN2/.../WAN1/WAN2/USB1/USB2...
- s	Muestra los IID aleatorios para cada interfaz.

Ejemplo

```
> gestión ip6_IIDs -e 1
% Configuración exitosa, el cambio tendrá efecto después de reiniciar el enrutador.
> gestión ip6_IIDs -r LAN1
% Configuración exitosa, el cambio tendrá efecto después de reiniciar el enrutador.
> administración ip6_IIDs -s
% IID de LAN = 9a5d:06c3:c972:f3ad % IID de
WAN1 = 7651:92cc:6f8b:42c8 % IID de WAN2
= 79e5:56cd:be43:384a % IID de WAN3 =
0193:56a8:5c6e:01e7 % IID de WAN4 = 47bf:
a971:857d:5a07 % LTE
        IID = e4bf:d21d:f59f:888d IID =
% USB    4c55:260c:e5f5:57b7
>
```

Comando Telnet: conmutador msubnet

Este comando se utiliza para configurar varias subredes.

Sintaxis

conmutador msubnet *<2/3/4/5/6/7/8/dmz><Activar/Desactivar>*

Sintaxis Descripción

Parámetro	Descripción
2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7 8=LAN8 dmz=DMZ
Encendido apagado	Activado significa activar la subred para la interfaz LAN especificada. Apagado significa apagar la subred.

Ejemplo

```
> conmutador msubnet 2 en
% LAN2          ¡Subred activada!

  Esta configuración tendrá efecto después de reiniciar. Utilice el
  comando "sys reboot" para reiniciar el enrutador.
```

Comando Telnet: msubnet addr

Este comando se utiliza para configurar la dirección IP para la interfaz LAN especificada.

Sintaxis

dirección de subred m *<2/3/4/5/6/7/8/dmz><dirección IP>*

Sintaxis Descripción

Parámetro	Descripción
2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7 8=LAN8 dmz=DMZ
dirección IP	Ingrese la dirección IP privada para la interfaz LAN especificada.

Ejemplo

```
> msubnet addr 2 192.168.5.1
```

```
% Establecer la dirección IP de la subred LAN2 hecho !!!

 Esta configuración tendrá efecto después de reiniciar. Utilice el
 comando "sys reboot" para reiniciar el enrutador.
```

Comando Telnet: msubnet nmask

Este comando se utiliza para configurar la dirección de máscara de red para la interfaz LAN especificada.

Sintaxis

msubnet nmask *<2/3/4/5/6/7/8/dmz><dirección IP>*

Sintaxis Descripción

Parámetro	Descripción
2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7 8=LAN8 dmz=DMZ
dirección IP	Ingrese la dirección de la máscara de subred para la interfaz LAN especificada.

Ejemplo

```
> msubnet nmask 2 255.255.0.0 % Establecer
máscara de subred LAN2 hecho !!!

 Esta configuración tendrá efecto después de reiniciar. Utilice el
 comando "sys reboot" para reiniciar el enrutador.
```

Comando Telnet: estado de msubnet

Este comando se utiliza para mostrar el estado actual de la subred.

Sintaxis

estado de la subred*<2/3/4/5/6/7/8/dmz>*

Sintaxis Descripción

Parámetro	Descripción
2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7 8=LAN8

	dmz=DMZ

Ejemplo

```
> estado msubnet 2 %
LAN2              Desactivado: 0.0.0.0/0.0.0.0, IP de inicio de PPP: 0.0.0.60
% servidor DHCP: Desactivado
% Puerta de enlace Dhcp: 0.0.0.0, IP de inicio: 0.0.0.10, Recuento de grupos: 50
```

Comando Telnet: msubnet dhcps

Este comando le permite habilitar o deshabilitar el servidor DHCP para la subred.

Sintaxis

msubnet dhcps <*2/3/4/5/6/7/8/dmz><Activar/Desactivar>*

Sintaxis Descripción

Parámetro	Descripción
2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7 8=LAN8 dmz=DMZ
Encendido apagado	Encendido significa habilitar el servidor DHCP para la interfaz LAN especificada. Apagado significa deshabilitar el servidor DHCP.

Ejemplo

```
> msubnet dhcps 3 de descuento
% LAN3              ¡Servidor DHCP de subred deshabilitado!

  Esta configuración tendrá efecto después de reiniciar. Utilice el
  comando "sys reboot" para reiniciar el enrutador.
```

Comando Telnet: msubnet nat

Este comando se usa para configurar la subred para NAT o uso de enrutamiento.

Sintaxis

msubnet nat <*2/3/4/5/6/7/8/dmz><Activar/Desactivar>*

Sintaxis Descripción

Parámetro	Descripción
2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7

	8=LAN8 dmz=DMZ
Encendido apagado	Activado: significa que la subred se configurará para el uso de NAT. Apagado- Significa que la subred se configurará para el uso de enrutamiento.

Ejemplo

```
> msubnet nat 2 apagado
¡% Subred LAN2 es para uso de enrutamiento!
¡% Subred LAN2 es para uso de enrutamiento!
%Nota: si tiene varias conexiones WAN, recuerde configurar una política de equilibrio de carga para que los paquetes de esta subred se reenvíen a la interfaz WAN correcta.


 Esta configuración tendrá efecto después de reiniciar. Utilice el
 comando "sys reboot" para reiniciar el enrutador.
```

Comando Telnet: puerta de enlace msubnet

Este comando se utiliza para configurar una dirección IP como la puerta de enlace utilizada para la subred.

Sintaxis

puerta de enlace msubnet*<2/3/4/5/6/7/8/dmz><IP de puerta de enlace>*

Sintaxis Descripción

Parámetro	Descripción
2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7 8=LAN8 dmz=DMZ
IP de acceso	Especifique una dirección IP como la IP de la puerta de enlace.

Ejemplo

```
> msubnet gateway 2 192.168.1.13 % Establecer
LAN2 Dhcp Gateway IP hecho !!!

 Esta configuración tendrá efecto después de reiniciar. Utilice el
 comando "sys reboot" para reiniciar el enrutador.
```

Comando Telnet: msubnet ipcnt

Este comando se utiliza para definir el número total permitido para cada interfaz LAN.

Sintaxis

msubnet ipcnt*<2/3/4/5/6/7/8/dmz> <Recuentos de IP>*

Sintaxis Descripción

Parámetro	Descripción
2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 2=LAN2

	3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7 8=LAN8 dmz=DMZ
recuentos de IP	Especifique un número total de direcciones IP permitidas para cada interfaz LAN. El rango disponible es de 0 a 220.

Ejemplo

```
> msubnet ipcnt 2 15
  Esta configuración tendrá efecto después de reiniciar. Utilice el
  comando "sys reboot" para reiniciar el enrutador.
```

Comando Telnet: charla msubnet

Este comando se utiliza para establecer una ruta entre dos interfaces LAN.

Sintaxis

charla msubnet*<1/2/3/4/5/6/7/8/dmz> <1/2/3/4/5/6/7/8/dmz> <Activar/Desactivar>*

Sintaxis Descripción

Parámetro	Descripción
1/2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 1=LAN1 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7 8=LAN8 dmz=DMZ
Encendido apagado	On – Significa habilitar la función. Apagado-Significa desactivar la función.

Ejemplo

```
> msubnet hablar 1 2 en
% Habilitar enrutamiento entre LAN1              y LAN2              !

  Esta configuración tendrá efecto después de reiniciar. Utilice el
  comando "sys reboot" para reiniciar el enrutador.
> msubnet hablar?
% conversación subred m <1/2/3/4/5/6/7/8/dmz> <1/2/3/4/5/6/7/8/dmz> <Activar/Desactivar>
% donde 1:LAN1, 2:LAN2, 3:LAN3, 4:LAN4, 5:LAN5, 6:LAN6, 7:LAN7, 8:LAN8, dmz:DMZ Puerto

% Ahora:
%              LAN1   LAN2   LAN3   LAN4   LAN5   LAN6   LAN7   LAN8   Puerto DMZ
% LAN1          V
% LAN2          V      V
```

```
% LAN3                                  V
% LAN4                                      V
% LAN5                                          V
% LAN6                                              V
% LAN7                                                  V
% LAN8                                                      V
% puerto DMZ                                                    V

>
```

Comando Telnet: msubnet starttip

Este comando se usa para configurar una dirección IP inicial para DCHP.

Sintaxis

consejo de inicio de msubnet*<2/3/4/5/6/7/8/dmz><IP de puerta de enlace>*

Sintaxis Descripción

Parámetro	Descripción
2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7 8=LAN8 dmz=DMZ
IP de acceso	Escriba una dirección IP como dirección IP inicial para una subred.

Ejemplo

```
> msubnet starttip 2 192.168.2.90 %Set
LAN2 Dhcp Start IP done !!!

  Esta configuración tendrá efecto después de reiniciar. Utilice el
  comando "sys reboot" para reiniciar el enrutador.
> punta de inicio msubnet?
% msubnet starttip <2/3/4/5/6/7/8/dmz> <IP de puerta de enlace>
% Ahora: LAN2 192.168.2.90; LAN3 192.168.3.10; LAN4 192.168.4.10; LAN5 192.168.5.10; LAN6
192.168.6.10; LAN7 192.168.7.10; LAN8 192.168.8.10
>
```

Comando Telnet: msubnet pppip

Este comando se utiliza para configurar una dirección IP inicial para la conexión PPP.

Sintaxis

msubnet pppip*<2/3/4/5/6/7/8/dmz><IP de inicio>*

Sintaxis Descripción

Parámetro	Descripción
2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 2=LAN2

	3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7 8=LAN8 dmz=DMZ
IP de inicio	Escriba una dirección IP como la dirección IP inicial para la conexión PPP.

Ejemplo

```
> msubnetppip 2 192.168.2.250
% Establecer LAN2 PPP (IPCP) Iniciar IP hecho !!!

  Esta configuración tendrá efecto después de reiniciar. Utilice el
  comando "sys reboot" para reiniciar el enrutador.

> msubnet pppip?
% msubnet pppip <2/3/4/5/6/7/8/dmz> <IP de inicio>
% Ahora: LAN2 192.168.2.250; LAN3 192.168.3.200; LAN4 192.168.4.200; LAN5 192.168.5.200; LAN6
192.168.6.200; LAN7 192.168.7.200; LAN8 192.168.8.200
```

Comando Telnet: tipo de nodo msubnet

Este comando se utiliza para especificar el tipo de nodo que requiere la opción DHCP.

Sintaxis

tipo de nodo msubnet*<2/3/4/5/6/7/8/dmz><contar>*

Sintaxis Descripción

Parámetro	Descripción
2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7 8=LAN8 dmz=DMZ
contar	Elija el siguiente número para especificar un tipo de nodo diferente. 1= nodo B 2= nodo P 4= nodo M 8= nodo H 0= No especificar ningún tipo de nodo.

Ejemplo

```
> tipo de nodo msubnet?
% tipo de nodo de subred m <2/3/4/5/6/7/8/dmz> <recuento>
% Ahora: LAN2 0; LAN3 0; LAN4 0; LAN5 0; LAN6 0; LAN7 0; LAN8 0
```

```
% de recuento: 1. Nodo B 2. Nodo P 4. Nodo M 8. Nodo H

> tipo de nodo msubnet 2 1
% Establecer tipo de nodo Dhcp LAN2 hecho !!!

> tipo de nodo msubnet?
% tipo de nodo de subred m <2/3/4/5/6/7/8/dmz> <recuento>
% Ahora: LAN2 1; LAN3 0; LAN4 0; LAN5 0; LAN6 0; LAN7 0; LAN8 0

% de recuento: 1. Nodo B 2. Nodo P 4. Nodo M 8. Nodo H
```

Comando Telnet: msubnet primWINS

Este comando se usa para configurar el servidor WINS primario.

Sintaxis

msubnet primWINS*<2/3/4/5/6/7/8/dmz><IP de GANA>*

Sintaxis Descripción

Parámetro	Descripción
2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7 8=LAN8 dmz=DMZ
GANA IP	Ingrese la dirección IP como IP WINS.

Ejemplo

```
> msubnetprimWINS?
% msubnet primWINS <2/3/4/5/6/7/8/dmz> <IP de WINS>
% Ahora: LAN2 0.0.0.0; LAN3 0.0.0.0; LAN4 0.0.0.0; LAN5 0.0.0.0; LAN6 0.0.0.0; LAN

7 0.0.0.0; LAN8 0.0.0.0

> msubred primWINS 2 192.168.3.5
% Establecer LAN2 Dhcp Primario WINS IP hecho !!!

> msubnetprimWINS?
% msubnet primWINS <2/3/4/5/6/7/8/dmz> <IP de WINS>
% Ahora: LAN2 192.168.3.5; LAN3 0.0.0.0; LAN4 0.0.0.0; LAN5 0.0.0.0; LAN6 0.0.0.0; LAN7 0.0.0.0;
LAN8 0.0.0.0
```

Comando Telnet: msubnet secWINS

Este comando se utiliza para configurar el servidor WINS secundario.

Sintaxis

msubnet secWINS*<2/3/4/5/6/7/8/dmz> <IP de GANA>*

Sintaxis Descripción

Parámetro	Descripción
2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7 8=LAN8 dmz=DMZ
GANA IP	Ingrese la dirección IP como IP WINS.

Ejemplo

```
> msubnet secWINS?
% msubnet secWINS <2/3/4/5/6/7/8/dmz> <IP de WINS>
% Ahora: LAN2 0.0.0.0; LAN3 0.0.0.0; LAN4 0.0.0.0; LAN5 0.0.0.0; LAN6 0.0.0.0; LAN

7 0.0.0.0; LAN8 0.0.0.0
> msubnet secWINS 2 192.168.3.89
% Establecer LAN2 Dhcp Secundaria WINS IP hecho !!!

> msubnet secWINS?
% msubnet secWINS <2/3/4/5/6/7/8/dmz> <IP de WINS>
% Ahora: LAN2 192.168.3.89; LAN3 0.0.0.0; LAN4 0.0.0.0; LAN5 0.0.0.0; LAN6 0.0.0.0; LAN7 0.0.0.0;
LAN8 0.0.0.0
```

Comando Telnet: msubnet tftp

Este comando se usa para configurar el servidor TFTP para múltiples subredes.

Sintaxis

msubnet tftp*<2/3/4/5/6/7/8/dmz> <nombre del servidor TFTP>*

Sintaxis Descripción

Parámetro	Descripción
2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7 8=LAN8 dmz=DMZ
nombre del servidor TFTP	Escriba un nombre para indicar el servidor TFTP.

Ejemplo

```
> msubnet tftp?
% msubnet tftp <2/3/4/5/6/7/8/dmz> <nombre del servidor TFTP>
```

```
% Ahora: LAN2
                LAN3
                LAN4
                LAN5
                LAN6
                LAN7
                LAN8
> msubnet tftp 2 publicar
% Establecer el nombre del servidor LAN2 TFTP hecho !!!

> msubnet tftp?
% msubnet tftp <2/3/4/5/6/7/8/dmz> <nombre del servidor TFTP> %
Ahora: LAN2 publicar
                LAN3
                LAN4
                LAN5
                LAN6
                LAN7
                LAN8
```

Comando Telnet: msubnet mtu

Este comando le permite configurar el valor de MTU para la subred enrutada LAN/DMZ/IP.

Sintaxis

mtu msubnet *<interfaz><valor>*

Sintaxis Descripción

Parámetro	Descripción
interfaz	Las configuraciones disponibles incluyen LAN1~LAN6, IP_Routed_Subnet y DMZ.
valor	1000 ~ 1500 (Bytes), predeterminado: 1500 (Bytes)

Ejemplo

```
> msubred mtu LAN1 1492
> msubnet mtu?
Uso:

  > msubnet mtu <interfaz> <valor>

  <interfaz>: LAN1~LAN6, IP_Routed_Subnet, DMZ <valor>: 1000 ~ 1508
  (Bytes), predeterminado: 1500 (Bytes)

  ej.: >msubnet mtu LAN1 1492

Configuraciones actuales:

   MTU LAN1:          1500 (bytes)
   MTU LAN2:          1500 (bytes)
   MTU LAN3:          1500 (bytes)
   MTU LAN4:          1500 (bytes)
   MTU LAN5:          1500 (bytes)
```

```
    MTU LAN6:              1500 (bytes)
    MTU LAN7:              1500 (bytes)
    MTU LAN8:              1500 (bytes)
    MTU de DMZ:            1500 (bytes)
    MTU de subred enrutada por IP: 1500 (bytes)
>
```

Comando Telnet: tiempo de arrendamiento de msubnet

Este comando se usa para establecer el tiempo de concesión para múltiples subredes.

Sintaxis

tiempo de concesión de msubnet*<1/2/3/4/5/6/7/8/dmz> <Tiempo de arrendamiento seg.>*

Sintaxis Descripción

Parámetro	Descripción
1/2/3/4/5/6/7/8/dmz	Significa interfaz LAN. 1=LAN1 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6 7=LAN7 8=LAN8 dmz=DMZ
Tiempo de arrendamiento seg.	Ingrese un valor (rango: 10 a 259200).

Ejemplo

```
> tiempo de arrendamiento de msubnet?
% msubnet leasetime <1/2/3/4/5/6/7/8/dmz> <Tiempo de concesión (seg.)>
% Ahora:LAN1 86400; LAN2 259200; LAN3 259200; LAN4 259200; LAN5 259200; LAN6 25920 0; LAN7
259200; LAN8 259200; Puerto DMZ 259200
> msubnet leasetime 8 300 % Establecer
tiempo de concesión de LAN8: 300
>
```

Comando Telnet: objeto ip obj

Este comando se utiliza para crear un perfil de objeto IP.

Sintaxis

objeto ip obj setdefault objeto ip
obj*ÍNDICE -v* **objeto ip obj***ÍNDICE -n*
NOMBRE **objeto ip obj***ÍNDICE -i*
INTERFAZ **objeto ip obj***ÍNDICE -s*
INVERTIR

objeto ip objI*NDEX -a TIPO <START_IP><END/MASK_IP>*

Sintaxis Descripción

Parámetro	Descripción
establecer predeterminado	Significa volver a la configuración predeterminada para todos los perfiles.
ÍNDICE	Significa el número de índice del perfil de objeto especificado.
-v	Significa ver la información del perfil del objeto especificado. Ejemplo:*objeto ip obj 1 -v*
- n NOMBRE	Significa definir un nombre para el objeto IP. NOMBRE: escriba un nombre con menos de 15 caracteres. Ejemplo:*objeto ip obj 9 -n bruce*
- yo INTERFAZ	Significa definir una interfaz para el objeto IP. INTERFACE=0, significa cualquier INTERFAZ=1, significa LAN INTERFAZ=3, significa WAN Ejemplo:*objeto ip obj 8 -i 0*
- s INVERTIR	Significa establecer la selección inversa para el perfil del objeto. INVERT=0, significa deshabilitar la función. INVERT=1, significa habilitar la función. Ejemplo:*objeto ip obj 3 -s 1*
- un tipo	Significa establecer el tipo de dirección y la IP para el perfil del objeto IP. TIPO=0, significa Máscara TIPO=1, significa Soltero TIPO=2, significa Cualquiera TIPO=3, significa Rango TIPO=4, significa MAC Ejemplo:*objeto ip obj 3 -a 2*
<START_IP>	Cuando el TIPO se establece en 2, debe escribir una dirección IP como punto de partida y otra dirección IP como punto final. Escriba una dirección IP.
<END/MASK_IP>	Escriba una dirección IP (diferente con START_IP) como la dirección IP final.

Ejemplo

```
> objeto ip obj 1 -n marketing OK.

> objeto ip obj 1 -a 1 192.168.1.45 OK.

> objeto ip obj 1 -v IP
  Objeto Perfil 1 Nombre :
  [marketing]
  Interfaz: [cualquiera]
  Tipo de dirección: [única]
  Dirección IP inicial:[192.168.1.45]
  Dirección IP final/máscara:[0.0.0.0]
  Dirección MAC:[00:00:00:00:00:00] Invertir
  selección:[0]
```

Comando Telnet: objeto ip grp

Este comando se utiliza para integrar varios objetos de IP en un perfil de grupo de IP.

Sintaxis

objeto ip grpestablecer predeterminado

objeto ip grp*ÍNDICE -v*

objeto ip grp*ÍNDICE -n NOMBRE* **objeto**
ip grp*ÍNDICE -i INTERFAZ* **objeto ip grp**
ÍNDICE -a IP_OBJ_ÍNDICE

Sintaxis Descripción

Parámetro	Descripción
establecer predeterminado	Significa volver a la configuración predeterminada para todos los perfiles.
ÍNDICE	Significa el número de índice del perfil de grupo especificado.
-v	Significa ver la información del perfil de grupo especificado. Ejemplo:*objeto ip grp 1 -v*
- n NOMBRE	Significa definir un nombre para el grupo de IP. NOMBRE: escriba un nombre con menos de 15 caracteres. Ejemplo:*objeto ip grp 8 -n bruce*
- yo INTERFAZ	Significa definir una interfaz para el grupo de IP. INTERFACE=0, significa cualquier INTERFAZ=1, significa LAN INTERFAZ=2, significa WAN Ejemplo:*objeto ip grp 3 -i 0*
- una IP_OBJ_INDEX	Significa especificar perfiles de objeto IP para el perfil de grupo. Ejemplo:*:objeto ip grp 3 -a 1 2 3 4 5* Los perfiles de objeto IP con número de índice 1,2,3,4 y 5 se agruparán bajo dicho perfil.

Ejemplo

```
> object ip grp 2 -n Primer perfil de
  grupo IP 2
  Nombre primero]
  Interfaz: [cualquiera]
  Índice de objeto IP incluido: [0:][0]

  [1:][0]
  [2:][0]
  [3:][0]
  [4:][0]
  [5:][0]
  [6:][0]
  [7:][0]
  [8:][0]
  [9:][0]
  [10:][0]
  [11:][0]

> object ip grp 2 -i 1 IP Group
Profile 2 Name :[First]

  Interfaz: [Lan]
  Índice de objeto IP incluido: [0:][0]

  [1:][0]
  [2:][0]
  [3:][0]
```

```
[4:][0]
[5:][0]
[6:][0]
[7:][0]
[8:][0]
[9:][0]
[10:][0]
[11:][0]

¡Establecer bien!
```

Comando Telnet: objeto ipv6 obj

Este comando se utiliza para crear un perfil de objeto IP.

Sintaxis

objeto ip obj setdefault objeto ip
obj*ÍNDICE -v* **objeto ip obj***ÍNDICE -n*
NOMBRE **objeto ip obj***ÍNDICE -i*
INTERFAZ **objeto ip obj***ÍNDICE -s*
INVERTIR
objeto ip objI*NDEX -a TIPO <START_IP><END_IP>/<Longitud del prefijo>*

Sintaxis Descripción

Parámetro	Descripción
establecer predeterminado	Significa volver a la configuración predeterminada para todos los perfiles.
ÍNDICE	Significa el número de índice del perfil de objeto especificado.
-v	Significa ver la información del perfil del objeto especificado. Ejemplo:*objeto ip obj 1 -v*
- n NOMBRE	Significa definir un nombre para el objeto IPv6. NOMBRE: escriba un nombre con menos de 15 caracteres. Ejemplo:*objeto ip obj 9 -n bruce*
- yo INTERFAZ	Significa definir una interfaz para el objeto IP. INTERFACE=0, significa cualquier INTERFAZ=1, significa LAN INTERFAZ=3, significa WAN Ejemplo:*objeto ip obj 8 -i 0*
- s INVERTIR	Significa establecer la selección inversa para el perfil del objeto. INVERT=0, significa deshabilitar la función. INVERT=1, significa habilitar la función. Ejemplo:*objeto ip obj 3 -s 1*
- mi [0/1]	Significa establecer el tipo de coincidencia del perfil de objeto IPv6. 0: significa 128 Bits 1: significa ID de interfaz de sufijo de 64 bits.
- un tipo	Significa establecer el tipo de dirección y la IP para el perfil de objeto IPv6. TIPO=0, significa Máscara TIPO=1, significa Soltero TIPO=2, significa Cualquiera TIPO=3, significa Rango TIPO=4, significa MAC Ejemplo:*objeto ip obj 3 -a 2*

<START_IP><END_IP>	Cuando el TIPO se configura con 0, 1,3, debe escribir una dirección IP como punto de partida y otra dirección IP como punto final. Escriba la(s) dirección(es) IP según la selección de TIPO.
<Longitud del prefijo>	Cuando el TIPO se configura con 0, 1 o 3, debe ingresar un número como longitud de prefijo para la dirección IPv6.

Ejemplo

```
> obj ipv6 obj 3 -a 3 2607:f0d0:1002:51::4 2607:f0d0:1002:51::4 Configuración
guardada.
> obj ipv6 obj 3 -v IPv6
Objeto Perfil 3 Nombre :[]

 Tipo de dirección: [rango]
 Dirección IPv6 inicial:[2607:F0D0:1002:51::4] Dirección
 IPv6 final:[2607:F0D0:1002:51::4] Longitud del prefijo:[0]

 Dirección MAC:[00:00:00:00:00:00] Invertir
 selección:[0]
  Tipo de coincidencia:[0]
```

Comando Telnet: objeto ipv6 grp

Este comando se utiliza para integrar varios objetos de IP en un perfil de grupo de IP.

Sintaxis

objeto ip grpestablecer predeterminado

objeto ip grp*ÍNDICE -v* **objeto ip grp***ÍNDICE -n*

NOMBRE **objeto ip grp***ÍNDICE -a*

IP_OBJ_ÍNDICE

Sintaxis Descripción

Parámetro	Descripción
establecer predeterminado	Significa volver a la configuración predeterminada para todos los perfiles.
ÍNDICE	Significa el número de índice del perfil de grupo especificado.
-v	Significa ver la información del perfil de grupo especificado. Ejemplo:*objeto ip grp 1 -v*
- n NOMBRE	Significa definir un nombre para el grupo de IP. NOMBRE: escriba un nombre con menos de 15 caracteres. Ejemplo:*objeto ip grp 8 -n bruce*
- una IP_OBJ_INDEX	Significa especificar perfiles de objeto IP para el perfil de grupo. Ejemplo:*:objeto ip grp 3 -a 1 2 3 4 5* Los perfiles de objeto IP con número de índice 1,2,3,4 y 5 se agruparán bajo dicho perfil.

Ejemplo

```
> objeto ipv6 grp 1 -n marketingtest Perfil de
 grupo IP 1
 Nombre :[prueba de marketing]
 Índice de objeto IP incluido: [0:][0]

 [1:][0]
```

```
 [2:][0]
 [3:][0]
 [4:][0]
 [5:][0]
 [6:][0]
 [7:][0]

> objeto ipv6 grp 1 -a 1 2 3 4 5 Perfil de
grupo IPv6 1
Nombre :[prueba de marketing]
Índice de objeto IP incluido: [0:][1]

[1:][2]
[2:][3]
[3:][4]
[4:][5]
[5:][0]
[6:][0]
[7:][0]
```

Comando Telnet: país del objeto

Este comando se utiliza para crear un perfil de objeto de país.

Sintaxis

conjunto de países objeto*ÍNDICE -v* **conjunto de países objeto***ÍNDICE -n NOMBRE* **conjunto de países objeto***ÍNDICE -a PAÍS_ÍNDICE* **país del objeto activar país del objeto establecer lista de países del objeto por defecto**

Sintaxis Descripción

Parámetro	Descripción
ÍNDICE	Significa el número de índice del perfil de objeto de país especificado (1 a 32).
- n NOMBRE	Significa definir un nombre para el perfil de objeto de país.
PAÍS_INDEX	Significa el número de código de un país. Para obtener la información detallada del número de código, utilice la "lista de países objeto" para obtener el que necesita.
activar	Significa activar el perfil de objeto de país.
establecer predeterminado	Significa volver a la configuración predeterminada para todos los perfiles.
lista	Muestra una lista de países con número de código. Por ejemplo, "222" significa "Taiwán"; "241" significa "Estados Unidos".

Ejemplo

```
> objeto conjunto de países 1 -n Mejor
país objeto Perfil 1 Nombre :[Mejor]

 Índice de países incluidos:

¡Establecer bien!
> objeto conjunto de países 1 -a 222
```

Objeto de país Perfil 1 Nombre :
[Mejor]
Índice de países incluidos: [0:]
[222] Taiwán

¡Establecer bien!

Comando Telnet: objeto servicio obj

Este comando se utiliza para crear un perfil de objeto de servicio.

Sintaxis

objetos**obj servicio establecer objeto**
predeterminado obj servicio*ÍNDICE -v* **objeto**
servicio obj*ÍNDICE -n NOMBRE* **objeto servicio**
obj*ÍNDICE -p PROTOCOLO*
objeto servicio obj*ÍNDICE -s CHK <START_P><END_P>*
objeto servicio obj*ÍNDICE -d CHK <START_P><END_P>*

Sintaxis Descripción

Parámetro	Descripción
establecer predeterminado	Significa volver a la configuración predeterminada para todos los perfiles.
ÍNDICE	Significa el número de índice del perfil de objeto de servicio especificado.
-v	Significa ver la información del perfil del objeto de servicio especificado. Ejemplo:*objeto servicio obj 1 -v*
- n NOMBRE	Significa definir un nombre para el objeto IP. NOMBRE: escriba un nombre con menos de 15 caracteres. Ejemplo:*objeto servicio obj 9 -n bruce*
- y PROTOCOLO	Significa definir un PROTOCOLO para el perfil del objeto de servicio. PROTOCOLO =0, significa cualquier PROTOCOLO =1, significa PROTOCOLO ICMP =2, significa PROTOCOLO IGMP =6, significa PROTOCOLO TCP =17, significa PROTOCOLO UDP =58, significa PROTOCOLO ICMPv6 =255, significa TCP/UDP Otros valores significan otros protocolos. Ejemplo:*objeto servicio obj 8 -i 0*
CHK	Significa la acción de verificación para la configuración del puerto. 0=igual**(=)**, cuando los valores del puerto inicial y final son los mismos, indica un puerto; cuando los valores del puerto inicial y del puerto final son diferentes, indica un rango para el puerto y disponible para este tipo de servicio. 1=no igual**(!=)**, cuando los valores de puerto inicial y puerto final son los mismos, indica todos los puertos excepto el puerto definido aquí; cuando los valores del puerto inicial y del puerto final son diferentes, indica que todos los puertos excepto el rango definido aquí están disponibles para este tipo de servicio. 2=más grande**(>)**, el número de puerto mayor que este valor está disponible. 3=menos**(<)**, el número de puerto menor que este valor está disponible para este perfil.

- s CHK <START_P><END_P>	Significa establecer la comprobación del puerto de origen y configurar el rango de puertos (1~65565) para TCP/UDP. START_P: ingrese un número de puerto para indicar el puerto de origen inicial. END_P: ingrese un número de puerto para indicar el puerto de origen final. Ejemplo:*objeto servicio obj 3 -s 0 100 200*
- d CHK <START_P><END_P>	Significa establecer la verificación del puerto de destino y configurar el rango de puertos (1~65565) para TCP/UDP. START_P: ingrese un número de puerto para indicar el puerto de destino inicial. END_P: ingrese un número de puerto para indicar el puerto de destino final. Ejemplo:*objeto servicio obj 3 -d 1 100 200*

Ejemplo

```
> objeto servicio obj 1 -n límite
> objeto servicio obj 1 -p 255
> objeto servicio obj 1 -s 1 120 240
> objeto servicio obj 1 -d 1 200 220
> objeto servicio obj 1 -v Objeto
  de servicio Perfil 1 Nombre:
  [límite]
  Protocolo:[255]
  Acción de verificación de puerto de origen:[!=]
  Rango de puerto de origen:[120~240] Acción de
  verificación de puerto de destino:[!=] Rango de
  puerto de destino:[200~220]
```

Comando Telnet: servicio de objetos grp

Este comando se utiliza para integrar varios objetos de servicio en un perfil de grupo de servicios.

Sintaxis

objeto servicio grp setdefault objeto servicio grp
ÍNDICE -v **grupo de servicios de objetos***ÍNDICE -n*
NOMBRE **grupo de servicios de objetos***ÍNDICE -a*
SER_OBJ_INDEX

Sintaxis Descripción

Parámetro	Descripción
establecer predeterminado	Significa volver a la configuración predeterminada para todos los perfiles.
ÍNDICE	Significa el número de índice del perfil de grupo especificado.
-v	Significa ver la información del perfil de grupo especificado. Ejemplo:*objeto servicio grp 1 -v*
- n NOMBRE	Significa definir un nombre para el grupo de servicios. NOMBRE: escriba un nombre con menos de 15 caracteres. Ejemplo:*objeto servicio grp 8 -n bruce*
- un SER_OBJ_INDEX	Significa especificar perfiles de objeto de servicio para el perfil de grupo. Ejemplo:*:objeto servicio grp 3 -a 1 2 3 4 5* Los perfiles de objeto de servicio con número de índice 1,2,3,4 y 5 se agruparán bajo dicho perfil.

Ejemplo

```
> objeto servicio grp 1 -n Grope_1 Servicio
  Grupo Perfil 1
  Nombre :[Grope_1]
  Índice de objeto de servicio incluido: [0:]
  [0]
  [1:][0]
  [2:][0]
  [3:][0]
  [4:][0]
  [5:][0]
  [6:][0]
  [7:][0]

> objeto servicio grp 1 -a 1 2 Servicio
  Grupo Perfil 1
  Nombre :[Grope_1]
  Índice de objeto de servicio incluido: [0:]
  [1]
  [1:][2]
  [2:][0]
  [3:][0]
  [4:][0]
  [5:][0]
  [6:][0]
  [7:][0]
```

Comando Telnet: objeto kw

Este comando se utiliza para crear un perfil de palabra clave.

Sintaxis

objeto kw obj establecer objeto
predeterminado kw obj mostrar PÁGINA
objeto kw obj*ÍNDICE -v* **objeto kw obj**
ÍNDICE -n NOMBRE **objeto kw obj***ÍNDICE -a*
CONTENIDO

objeto kw obj*ÍNDICE -c*

objeto kw obj*ÍNDICE -t*

Sintaxis Descripción

Parámetro	Descripción
establecer predeterminado	Significa volver a la configuración predeterminada para todos los perfiles.
Mostrar PÁGINA	Significa mostrar el contenido del perfil especificado. PÁGINA: Introduzca el número de página.
espectáculo	Significa mostrar los contenidos para todos los perfiles.
ÍNDICE	Significa el número de índice del perfil de palabra clave especificado.
-V	Significa ver la información del perfil de palabra clave especificado.
- n NOMBRE	Significa definir un nombre para el perfil de palabra clave. NOMBRE: escriba un nombre con menos de 15 caracteres.
- un CONTENIDO	Significa establecer los contenidos para el perfil de palabra clave. Ejemplo:*objeto kw obj 40 -una prueba*

- C	Significa borrar el contenido del perfil del objeto de palabra clave.
- t<0/1>	Significa establecer el tipo de objeto de palabra clave. <0>: normales <1> : nombre de dominio

Ejemplo

```
> objeto kw obj 1 -n hijos Perfil 1

 Nombre    :[niños]
 Tipo      :[Normal]
 Contenido:[]
> objeto kw obj 1 -a Perfil de juego 1

 Nombre    :[niños]
 Tipo      :[Normal]
 Contenido: [apuestas]

> objeto kw obj 1 -v Perfil 1

 Nombre    :[niños]
 Tipo      :[Normal]
  Contenido: [apuestas]
```

Comando Telnet: objeto fe

Este comando se utiliza para crear un perfil de objeto de extensión de archivo.

Sintaxis

Mostrar objeto fe

objeto fe establecido por defecto

objeto fe obj*ÍNDICE -v* **objeto fe**

obj*ÍNDICE -n NOMBRE*

objeto fe obj*ÍNDICE -e CATEGORÍA|EXTENSIÓN_ARCHIVO*

objeto fe obj*ÍNDICE -d CATEGORÍA|EXTENSIÓN_ARCHIVO*

Sintaxis Descripción

Parámetro	Descripción
espectáculo	Significa mostrar los contenidos para todos los perfiles.
establecer predeterminado	Significa volver a la configuración predeterminada para todos los perfiles.
ÍNDICE	Significa el número de índice (de 1 a 8) del perfil de objeto de extensión de archivo especificado.
-v	Significa ver la información del perfil de objeto de extensión de archivo especificado.
- n NOMBRE	Significa definir un nombre para el perfil del objeto de extensión de archivo. NOMBRE: escriba un nombre con menos de 15 caracteres.
- mi	Significa habilitar la CATEGORÍA específica o FILE_EXTENSION.
- d	Significa deshabilitar la CATEGORÍA específica o FILE_EXTENSION
CATEGORÍA|EXTENSIÓN_ARCHIVO	CATEGORÍA: Imagen, Video, Audio, Java, ActiveX, Compresión, Ejecución

	Ejemplo:*objeto fe obj 1 -e Imagen* EXTENSIÓN DE ARCHIVO: ".bmp", ".dib", ".gif", ".jpeg", ".jpg", ".jpg2", ".jp2", ".pct", ".pcx", ".pic", ".pict", ".png", ".tif", ".tiff", ".asf", ".avi", ".mov", ".mpe", ".mpeg", ".mpg", ".mp4", ".qt", ".rm", ".wmv", ".3gp", ".3gpp", ".3gpp2", ".3g2", ".aac", ".aiff", ".au", ".mp3", ".m4a", ".m4p", ".ogg", ".ra", ".ram", ".vox", ".wav", ".wma", ".class", ".jad", ".jar", ".jav", ".java", ".jcm", ".js", ".jse", ".jsp", ".jtk", ".alx", ".apb", ".axs", ".ocx", ".olb", ".ole", ".tlb", ". viv", ".vrm", ".ace", ".arj", ".bzip2", ".bz2", ".cab", ".gz", ".gzip", ".rar", ". sentarse", ".zip", ".bas", ".bat", ".com",murciélago", ".com",murciélago", ".com", ".exe", ".inf", ".pif", ".reg", ".scr", "torrent", ".doc", ".docx", ".odp", ".ods", " .odt", ".pdf", ".ppt", ".pptx", ".xls", ".xlsx Ejemplo:*objeto fe obj 1 -e .bmp*

Ejemplo

```
> objeto fe obj 1 -n música
> objeto fe obj 1 -e Audio
> objeto fe obj 1 -v Índice
de perfil: 1
Nombre de perfil: [música]

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Categoría de imagen:
 [ ].bmp      [ ].dib      [ ].gif      [ ].jpeg      [ ].jpg      [ ].jpg2      [ ].jp2 [ ].pct
 [ ].pcx      [ ].Foto     [ ].imagen   [ ].png       [ ].tif      [ ].tiff      [ ].ico
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Categoría de vídeo:
 [ ].asf      [ ].avi      [ ].mov      [ ].mpe      [ ].mpeg [ ].mpg [v].mp4                [ ].qt
 [ ].rm       [v].wmv      [ ].3gp      [ ].3gpp     [ ].3gpp2 [ ].3g2 [ ].flv               [ ].swf
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Categoría de audio:
 [v].aac [v].aiff [v].au [v].mp3 [v].m4a [v].m4p [v].ogg [v].ra
 [v].ram [v].vox [v].wav [v].wma
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Categoría Java:
 [ ].clase [ ].jad [ ].jar [ ].jav [ ].java [ ].jcm [ ].js [ ].jse
 [ ].jsp [ ].jtk
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Categoría ActiveX:
 [ ].alx      [ ].apb [ ].axs [ ].ocx [ ].olb [ ].ole [ ].tlb [ ].viv
 [ ].vrm
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Categoría de compresión:
 [ ].as       [ ].arj [ ].bzip2 [ ].bz2 [ ].cab [ ].gz [ ].gzip [ ].rar
 [ ].sentarse [ ].cremallera
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Categoría de ejecución:
 [ ].bas [ ].bat [ ].com [ ].exe [ ].inf [ ].pif [ ].reg [ ].scr
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Categoría P2P:
 [ ].torrente
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Categoría del documento:
```

[ ].doc	[ ].docx [ ].odp [ ].ods [ ].odt [ ].pdf [ ].ppt [ ].pptx
[ ].xls	[ ].xlsx

Comando Telnet: objeto sms

Este comando se utiliza para crear un perfil de objeto de mensaje corto.

Sintaxis

mostrar objeto sms

objeto sms establecido por defecto

objeto sms obj*ÍNDICE -v* **objeto sms obj***ÍNDICE -n NOMBRE* **objeto sms obj***ÍNDICE -s Proveedor de servicios* **objeto sms obj***ÍNDICE -u Nombre de usuario* **objeto sms obj***ÍNDICE -p Contraseña* **objeto sms obj***ÍNDICE -q Cuota* **objeto sms obj** *ÍNDICE -i Intervalo* **objeto sms obj***ÍNDICE -l URL*

Sintaxis Descripción

Parámetro	Descripción
espectáculo	Significa mostrar los contenidos para todos los perfiles.
establecer predeterminado	Significa volver a la configuración predeterminada para todos los perfiles.
<ÍNDICE>	Significa el número de índice (de 1 a 10) del perfil de objeto de SMS especificado.
-v	Significa ver la información del perfil de objeto de SMS especificado.
- n <NOMBRE>	Significa definir un nombre para el perfil del objeto SMS. NOMBRE: escriba un nombre con menos de 15 caracteres.
- s <Proveedor de servicios>	Significa especificar el número del proveedor de servicios que ofrece el servicio de SMS. Diferentes números representan diferentes proveedores de servicios. 0 : kotsms.com.tw (TW) 2 : textmarketer.co.uk (Reino Unido) 4 : messagemedia.co.uk (Reino 5 : Unido) bulksms.com (INT) 6 : bulksms.co.uk (Reino Unido) 7 : bulksms.2way.co.za (ZA) 8 : bulksms.com.es (ES) 9 : usa.bulksms.com (EE. UU.) 10: bulksms.de (DE) 11: www.pswin.com (UE) 12: www.messagebird.com (UE) 13: www.lusosms.com (UE) 14: www.vibeactivemedia.com (Reino Unido)
- u <Nombre de usuario>	Significa definir un nombre de usuario para el perfil del objeto SMS. Escriba un nombre de usuario que el remitente pueda usar para registrarse en el proveedor de SMS seleccionado.
- p <Contraseña>	Significa definir una contraseña para el perfil del objeto SMS. Escriba una contraseña que el remitente pueda usar para registrarse en el SMS seleccionado

	proveedor.
- q <Cuota>	Ingrese el número del crédito que compra del proveedor de servicios. Tenga en cuenta que un crédito equivale a un mensaje de texto SMS en la ruta estándar.
- Yo <Intervalo>	Significa establecer el intervalo de envío para que se entregue el SMS. Ingrese el intervalo de tiempo más corto para que el sistema envíe SMS.
- l <URL>	Significa establecer la URL para los perfiles Personalizado 1 y Personalizado 2. El nombre de perfil para Custom 1 y Custom 2 se definen de forma predeterminada y no se pueden cambiar.

Ejemplo

```
> objeto sms obj 1 -n CTC
> objeto sms obj 1 -s 0
> objeto sms obj 1 -u carrie
> objeto sms obj 1 -p 19971125cm
> objeto sms obj 1 -q 2
> objeto sms obj 1 -i 50
> objeto sms obj 1 -v Índice
de perfil: 1
Nombre de perfil:[CTC]
Proveedor de SMS:[kotsms.com.tw (TW)]
Nombre de usuario:[carrie]
Contraseña:[******]
Cuota:[2]
Intervalo de envío: [50 (segundos)]
```

Comando Telnet: objeto de correo

Este comando se utiliza para crear un perfil de objeto de correo.

Sintaxis

espectáculo de correo de objeto
objeto correo setdefault
objeto correo obj*ÍNDICE -v*
objeto correo obj*ÍNDICE -n <Nombre de perfil>* **objeto correo obj***ÍNDICE -s <Servidor SMTP>* **objeto correo obj** *INDEX -l <Seguridad de la conexión>* **objeto correo obj** *ÍNDICE -m <Puerto SMTP>* **objeto correo obj***ÍNDICE -a <Dirección del remitente>* **objeto correo obj***ÍNDICE -t <Autenticación>* **objeto correo obj***ÍNDICE -u <Nombre de usuario>* **objeto correo obj***ÍNDICE -p <Contraseña>* **objeto correo obj***ÍNDICE -i <Intervalo de envío>* **objeto correo obj***ÍNDICE -w <Interfaz>* **objeto correo obj** *ÍNDICE -x <Índice IP de alias>*

Sintaxis Descripción

Parámetro	Descripción
espectáculo	Significa mostrar los contenidos para todos los perfiles.
establecer predeterminado	Significa volver a la configuración predeterminada para todos los perfiles.
[ÍNDICE]	Significa el número de índice (de 1 a 10) del perfil de objeto de correo especificado.
-v	Significa ver la información del perfil de objeto de correo especificado.

- n <Nombre de perfil>	Significa definir un nombre para el perfil del objeto de correo. *Nombre de perfil*: Escriba un nombre con menos de 15 caracteres.
- s <Servidor SMTP>	Significa establecer la dirección IP del servidor de correo.
- l <Seguridad de la conexión>	Significa establecer la seguridad de la conexión para el perfil del objeto. 0 - (Texto sin formato) 1 - (SSL) 2 - (StartTLS, es bueno tenerlo) 3 - (StartTLS, DEBE)
- m <Puerto SMTP>	Significa establecer el número de puerto para el servidor SMTP.
- una <Dirección del remitente>	Significa establecer la dirección de correo electrónico (p. ej., johnwash@abc.com.tw) del remitente.
- t <Autenticación>	El servidor de correo debe estar autenticado con el nombre de usuario y la contraseña correctos para tener derecho a enviar mensajes. 0 – deshabilitar 1: habilitar para usar el número de puerto.
- u <Nombre de usuario>	Escriba un nombre para la autenticación. La longitud máxima del nombre que puede establecer es de 31 caracteres.
- p <Contraseña>	Escriba una contraseña para la autenticación. La longitud máxima de la contraseña que puede establecer es de 31 caracteres.
- i <Intervalo de envío>	Defina el intervalo para que el sistema envíe el SMS. La unidad es segunda.
- w <Interfaz>	Configure la interfaz del perfil del servidor de correo.
- x <Índice IP de alias>	Configure el alias IP del perfil del servidor de correo (1 a 10).

Ejemplo

```
> objeto correo obj 1 -n comprador
> objeto correo obj 1 -s 192.168.1.98
> objeto correo obj 1 -m 25
> objeto correo obj 1 -t 1
> objeto correo obj 1 -u john
> objeto correo obj 1 -p happy123456
> objeto correo obj 1 -i 25
> objeto correo obj 1 -v Índice
de perfil: 1
Interfaz: [WAN1]
Índice IP de alias:[0]
Nombre de perfil: [comprador]
Servidor SMTP:[192.168.1.98]
Puerto SMTP:[25]
Dirección del remitente: [ carrie@draytek.com ] Seguridad
de conexión: [StartTLS (Es bueno tener)] Autenticación:
[habilitar]
Nombre de usuario: [juan]
Contraseña:[******]
 Intervalo de envío: [25 (segundos)]
```

Comando Telnet: objeto noti

Este comando se utiliza para crear un perfil de objeto de notificación.

Sintaxis

objeto noti mostrar
objeto notificado por defecto
objeto noti obj*ÍNDICE -v*
objeto noti obj*ÍNDICE -n <Nombre de perfil>* **objeto correo obj***ÍNDICE –e <Categoría><Estado>*

objeto correo obj*ÍNDICE –d <Categoría><Estado>*

Sintaxis Descripción

Parámetro	Descripción
espectáculo	Significa mostrar los contenidos para todos los perfiles.
establecer predeterminado	Significa volver a la configuración predeterminada para todos los perfiles.
<ÍNDICE>	Significa el número de índice (de 1 a 8) del perfil de objeto de notificación especificado.
-v	Significa ver la información del perfil del objeto de notificación especificado.
- n <Nombre de perfil>	Significa definir un nombre para el perfil del objeto de notificación. *Nombre de perfil*: Escriba un nombre con menos de 15 caracteres.
– mi	Significa habilitar el estado de la categoría especificada.
- d	Significa desactivar el estado de la categoría especificada.
<Categoría>	Las categorías disponibles son: 1: WAN; 2: Túnel VPN; 3: alerta de temperatura; 4: Presupuesto de la WAN; 5: CVM; 6: alta disponibilidad; 9: Seguridad
<estado>	Para WAN: 1: desconectado; 2: Reconectado. Para Túnel VPN - 1: desconectado; 2: Reconectado. Para alerta de temperatura – 1: Fuera de rango. Para el presupuesto de WAN: 1: Límite alcanzado. Para CVM- 1: CPE fuera de línea; 2: falla de copia de seguridad; 3: falla de restauración; 4: Error de actualización de FW; 5: Error de configuración del perfil de VPN. Para alta disponibilidad: 1: Ocurrió conmutación por error, falla de sincronización de configuración y enrutador inestable por seguridad - 1 : Se produce un evento de inicio de sesión web. 2 : Se produce un evento de inicio de sesión de Telnet. 3 : Ocurre un evento de inicio de sesión SSH. 4 : TR069 Se produce un evento de inicio de sesión. 5 : Se produce un evento de inicio de sesión de usuario de FTP. 6 : Ocurre un evento de cambio de configuración.

Ejemplo

```
> objeto noti obj 1 –n mercado
> objeto noti obj 1 –e 1 1
> objeto noti obj 1 –e 2 1
> objeto noti obj 1 –e 5 3
> objeto noti obj 1 –v Índice
de perfil: 1
Nombre de perfil:[]
        Categoría                    Estado
   PÁLIDO                [v]Desconectado        [ ]Reconectado
   Túnel VPN             [v]Desconectado        [ ]Reconectado
```

Alerta de temperatura	[ ]Temperatura USB fuera de rango
Alerta de presupuesto de WAN	[ ]Límite alcanzado
Alerta CVM	[ ] CPE fuera de línea
	[ ]Error en la copia de seguridad de la configuración de CPE
	[v]Error de restauración de configuración de CPE
	[ ]Error de actualización de firmware de CPE
	[ ]Error en la configuración del perfil VPN de CPE
Alta disponibilidad	[ ] Se produjo una conmutación por error
	Error de sincronización de configuración
	Enrutador inestable
Seguridad	[ ] Ocurre un evento de inicio de sesión web
	[ ] Ocurre un evento de inicio de sesión de Telnet
	[ ] Ocurre un evento de inicio de sesión SSH
	[ ]TR069 Se produce un evento de inicio de sesión
	[ ] Ocurre un evento de inicio de sesión de usuario de FTP
	[ ] Ocurre un evento de cambio de configuración

Comando Telnet: programación de objetos

Este comando se utiliza para crear un perfil de objeto de programación.

Sintaxis

conjunto de horarios de objetos*opción ÍNDICE* **vista**

de programación de objetos

programación de objetos establecida por defecto

Sintaxis Descripción

Parámetro	Descripción
colocar	Significa establecer el perfil de programación.
<ÍNDICE>	Significa el número de índice (de 1 a 15) del perfil de objeto especificado.
opción	Opciones disponibles para el horario.
- e <valor>	Significa habilitar la configuración del horario. 0 – deshabilitar 1 – habilitar
- c <comentario>	Significa establecer una breve descripción para el perfil especificado. El rango de longitud del comentario: 0 ~ 32 caracteres.
- D <año><mes><día>	Significa establecer la fecha de inicio del perfil. [año]: debe estar entre 2000 y 2049. [mes]: debe estar entre 1 y 12. [día]: debe estar entre el 1 y el 31. Por ejemplo: para establecer la fecha de inicio 2015/10/6, escriba *> conjunto de programación de objetos 1 -D "2015 10 6"*
- T <hora><minuto>	Significa establecer la hora de inicio del perfil. [hora]: debe estar entre 0 y 23. [minuto]: debe estar entre 0 y 59. Por ejemplo: para configurar la hora de inicio 10:20, escriba *> programa de objetos establecido 1 -T "10 20"*
- d <hora><minuto>	Significa establecer el tiempo de duración del perfil. [hora]: debe estar entre 0 y 23. [minuto]: debe estar entre 0 y 59. Por ejemplo: para configurar el tiempo de duración 3:30, escriba *> programa de objetos establecido 1 -d "3 30"*
- un <valor>	Significa establecer la acción utilizada para el perfil. [valor] - 0:Forzar encendido, 1:Forzar abajo, 2:Habilitar marcación bajo demanda, 3:Deshabilitar

	Marque cuando lo desee
- Yo <valor>	Significa establecer el tiempo de inactividad. [valor]: debe estar entre 0 y 255 (minuto). El valor predeterminado es 0.
- h <opción><día>	Establezca la frecuencia con la que se aplicará la programación. [opción] - 0: Una vez, 1: Días de semana, 2: Mensual, 3: Días de ciclo [día] – Dom LUN Mar MIE JUE VIE SAB Si la [opción] establece Días de la semana, entonces debe seleccionar qué días de la semana. ejemplo: Para seleccionar domingo, lunes, jueves, escriba *> programa de objetos establecido 1 -h "1 dom lun jue"*
ver [ÍNDICE]	Significa mostrar el contenido del perfil.
establecer predeterminado	Significa volver a la configuración predeterminada para todos los perfiles.

Ejemplo

```
> conjunto de programación de objetos 1 –e 1
> conjunto de programación de objetos 1 –c Trabajando
> programa de objetos establecido 1 –D "2021 10 8"
> programa de objetos establecido 1 –T "8 1"
> conjunto de programación de objetos 1 –d "2 30"
> conjunto de programación de objetos 1 –a 0
> conjunto de programaciones de objetos 1 –h "1 lun mié"
> vista de programación de objetos 1
Índice No.1

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[v] Habilitar comentario de configuración de
        programación [Trabajando]
        Fecha de inicio (aaaa-mm-dd) [ 2021 ]-[ 10 ]-[ 8 ] Hora de inicio
        (hh:mm)                      [   8 ]:[ 1 ]
        Duración Tiempo (hh:mm)      [   2 ]:[ 30 ]
        Acción                       [ Forzar ]
        Tiempo de inactividad        [ 0 ] minuto(s).(máx. 255, 0 por defecto)

        - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - Con qué
        frecuencia
          [ ] Una vez
          [v] Días de semana
              [ ]domingo [v]lunes [ ]martes [v]miércoles [ ]jueves [ ]viernes [ ]sábado
>
```

Comando Telnet: puerto

Este comando permite a los usuarios establecer la velocidad para un puerto específico del enrutador.

Sintaxis

puerto *<1, 2, 3, 4, 5, todos> <AN, 1G, 100F, 100H, 10F, 10H, estado>* **puerto** *< wan1, wan2> <AN, 1000F, 100F, 100H, 10F, 10H, estado>* **puerto** *<habilitar, deshabilitar> <1, 2, 3, 4, 5, todo>* **estado del puerto**

olfatear puerto *<encendido, apagado, puerto, txrx, reinicio, estado>*

puerto 802.1x*<habilitar, deshabilitar, estado, agregar puerto, eliminar>*

puerto jumbo

puerto wanfc

Sintaxis Descripción

Parámetro	Descripción
1, 2, 3, 4, 5, wan1, wan2, todos	Significa el número de puerto LAN y puerto WAN.
UNA... 10H	Significa el tipo físico para el puerto específico. AN: negociación automática. 1G: 1G 100F: 100M dúplex completo. 100H: 100M semidúplex. 10F: 10M dúplex completo. 10H: 10M semidúplex.
estado	Significa ver el estado del puerto Ethernet.
oler <on,off,port,txrx,restart,status>	Significa establecer la configuración para el sniffer. <on,off,port,txrx,restart,status>: vea lo siguiente, on - Encienda el sniffer. off: apaga el rastreador. puerto: especifique un puerto LAN (p1, p2, p3, p4, p5 o p6). reiniciar: reinicia el sistema para activar la configuración. estado: muestra la configuración actual. rxrx: establezca las velocidades de transmisión y recepción para un puerto LAN/WAN. por ejemplo, > puerto sniff txrx 30000 p2
802.1x <habilitar, deshabilitar, estado, agregar puerto, eliminar>	Significa establecer la configuración para 802.1x. <habilitar, deshabilitar, estado, agregar puerto, eliminar>: Consulte lo siguiente, habilitar - Habilitar la función. deshabilitar: deshabilitar la función. estado: muestra la configuración actual. addport - Agrega un número de puerto (1 a 5). delport - Elimina un número de puerto (1 a 5).
gigante <activar/desactivar>	Significa habilitar (encender) o deshabilitar (apagar) la función de marco gigante.
tamaño gigante <valor>	Si jumbo está habilitado, establezca un tamaño jumbo. <valor>: 1537 a 9022. Establezca un número.
wanfc <ÍNDICE> <encendido/apagado/estado>	Significa establecer el control de flujo WAN. <ÍNDICE>: Ingrese el número de índice (1 a 4) de la interfaz WAN. <on/off/status>: Ingrese "on" para habilitar la función; ingrese "off" para deshabilitar la función; ingrese "estado" para ver la configuración actual.

Ejemplo

```
> puerto 1 100F
%Establecer puerto 1 Forzar velocidad 100 Dúplex completo OK !!!
```

Comando Telnet: portmaptime

Este comando le permite establecer un tiempo para mantener la conexión de la sesión para el protocolo especificado.

Sintaxis

portmaptime*[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede ingresar varios comandos en una línea.
- t <seg>	Significa protocolo “TCP”. <seg>: escriba un número para establecer el tiempo de espera de la sesión TCP.
- tu <seg>	Significa protocolo “UDP”. <seg>: escriba un número para configurar el tiempo de espera de la sesión UDP.
- yo <seg>	Significa protocolo “IGMP”. <seg>: escriba un número para configurar el tiempo de espera de la sesión IGMP.
- w <seg>	Significa protocolo “TCP WWW”. <seg>: escriba un número para establecer el tiempo de espera de la sesión TCP WWW.
- s <seg>	Significa protocolo “TCP SYN”. <seg>: escriba un número para configurar el tiempo de espera de la sesión TCP SYN.
- f	Significa vaciar todos los mapas de puertos (útil para diagnósticos).
- l <Lista>	Enumere todas las configuraciones.

Ejemplo

```
> portmaptime -t 86400 -u 300          - I 10
> portmaptime -l
- - - - - - Configuración actual ------ Tiempo de
espera de TCP          : 86400 seg.
Tiempo de espera UDP   : 300 seg.
Tiempo de espera de IGMP   : 10 seg.
Tiempo de espera TCP WWW: 60 seg.
Tiempo de espera TCP SYN: 60 seg.
```

Comando Telnet: ppa

Este comando le permite configurar el modo PPA.

papá*[-<comando> <parámetro> | ...]*
papá n*[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede ingresar varios comandos en una línea.
-z<1/0>	Habilite o deshabilite la aceleración de hardware PPA. 1: Habilitar; 0: Deshabilitar
- m <modo>	Especifique un modo. 1=automático 2=manual(tráfico) 3=manual(qos) 0=deshabilitar
- p <prototipo>	Especifique un protocolo. proto-1-TCP; 2-UDP; 3-Ambos.
- b 1/0	Activar/desactivar la aceleración de hardware bidireccional.
- M habilitar/deshabilitar	Activar/desactivar la aceleración de hardware de multidifusión.

- S	Mostrar tabla de multidifusión en aceleración HW
- Yo <1/0>	Habilite o deshabilite la aceleración de HW de IPSec. 1: Habilitar; 0: Deshabilitar
- Yo -T <1/0>	Habilite o deshabilite el Protocolo TCP para la aceleración de IPSec HW. 1: Habilitar; 0: Deshabilitar
- Yo -U <1/0>	Habilite o deshabilite el Protocolo UDP para la aceleración de HW IPSec. 1: Habilitar; 0: Deshabilitar
-v	Muestre PPA_WAN_Table y PPA_LAN_Table como referencia.
- C	Limpia todos los ajustes.
- X	Mostrar información de aceleración de hardware.
- k	Limpie la mesa de PPA.
papá n-utilizado en QoS o host específico	
- l <regla>	Especifique un número de índice de perfil de regla para el modo QoS.
- E-e <1/0>	Habilitar/deshabilitar la lista de excepciones. 1: Habilitar; 0: Deshabilitar
- E -a <mac> <tipo>	Agregar cliente de excepción. <tipo> : nacional|ipsec
- E -u <índice> <opción> <valor>	Actualice la información del cliente de excepción. - m <mac>: Introduzca la dirección MAC. - t <tipo> : nat|ipsec. - d <descripción>: Ingrese una breve descripción. ejemplo:*-m 12:34:56:78:90:00 -t nat|ipsec -d portátil*
- E -d -i <valor>	Elimine el cliente de excepción especificando un número de índice.
- E -d -m <valor>	Elimine el cliente de excepción especificando una dirección mac.
- E-c	Borrar lista de excepciones.
- E-v	Muestra la lista de excepciones.

Ejemplo

```
> ppa n -E -e 1
> ppa n -E -a 12:34:56:78:90:00 nat|ipsec
> ppa n -E -u 12:34:56:78:90:00 -t nat|ipsec -d notebook
> ppa n -E -v
> ppa-v
%PPA está habilitado
%PPA NAT está habilitado %PPA el
modo es Automático %PPA Protocolo
TCP 1, UDP 0 %PPA Multidifusión está
habilitado %PPA IPSec está
deshabilitado
%PPA Protocolo IPSec TCP deshabilitado
%PPA Protocolo IPSec UDP deshabilitado
%PPA habilitado de dos vías
%PPA el tiempo es 10
El rango de %PPA es 8000 El
rango de %PAE es 2048 El
rango de %MPE es 5952
%PPA Entradas LAN 0, trabajando 0 %PPA
Entradas WAN 0, trabajando 0 %PPA
intervalo de estadísticas: 5 segundos
>
```

Comando Telnet: hwaccswap

Debido a la limitación de las sesiones aceleradas por el enrutador Vigor, este comando le permite intercambiar la sesión de paquetes en función de la prioridad de las sesiones (reglas definidas en Gestión de ancho de banda>>Calidad de servicio) para garantizar que las sesiones con mayor prioridad serán entregado temprano.

Sintaxis

estado de intercambio de hwacc

hwaccswap sessnum *<1 ~ 60000>* **umbral de**

intercambio de hwacc *<xxM/xxK/xx>*

temporizador de intercambio de hwacc *ciclo <xxx>/ duración <xxx>/ bloque <xxx>*

Sintaxis Descripción

Parámetro	Descripción
estado	Muestra la configuración actual para el intercambio de aceleración de hardware.
sesnum <1 ~ 60000>	Establezca un número de sesión válido. Cuando las sesiones de paquetes alcancen el número definido aquí, se activará la función de intercambio.
umbral <xxM/xxK/xx>	Establecer un umbral de tráfico. La unidad puede ser MB, KB y bytes.
ciclo de temporizador <xxx>	Establezca un tiempo de ciclo para repetir el intercambio de sesiones. <xxx> - Introduzca un valor de tiempo. La unidad es seg.
duración del temporizador <xxx>	Establezca una duración para realizar el intercambio de sesiones. <xxx> - Introduzca un valor de tiempo. La unidad es seg.
bloque de tiempo <xxx>	Establezca un tiempo para bloquear el intercambio de sesiones. <xxx> - Introduzca un valor de tiempo. La unidad es seg.

Ejemplo

```
> hwaccswap sessnum 5000 Establecer
  max_swap_sess_num: 5000

> estado de intercambio de hwacc
  Ajustes relacionados con el intercambio de sesión
  de HW acc: swap_cycle_timer: 1200 tics
  stat_duration_timer: 0 tics
  swap_block_time:              0 marca
  umbral_de_tráfico:            3000 bytes
  max_swap_sess_num:            5000

  método_mapa_grupo:
Grupo 0: Siempre En
Grupo 1: Ordenar tráfico e intercambiar
Grupo 2: Ordenar tráfico e intercambiar
Grupo 3: En una vez
Grupo 4: Siempre adentro
>
```

Comando Telnet: prn

Este comando le permite ver el estado actual (interfaz y controlador) de la impresora USB.

Sintaxis

estado prn

depuración prn

prn habilitar *<0/1>*

Sintaxis Descripción

Parámetro	Descripción
habilitar <0/1>	*Significa habilitar/deshabilitar la función de impresora USB. 0: deshabilitar* *1: habilitar*

Ejemplo

```
> estado prn
Interfaz: USB bus 2.0
Impresora: NotReady

> prn depuración
conexión[0]:
ninguno
conexión[1] :
ninguno
conexión[2] :
ninguno
conexión[3] :
ninguno
LPD_datos_total=0

usblp_ptr=0
UsbPrintReady=0, UsbIsPrinting=0
```

Comando Telnet: configuración qos

Este comando permite al usuario establecer la configuración general de QoS.

Sintaxis

configuración qos*[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede ingresar varios comandos en una línea.
- h	Escríbalo para mostrar el uso de este comando.
- W <1~6>	Significa seleccionar una interfaz. <1~6>: 1 es WAN1; 2 es WAN2 y etc. El valor predeterminado es WAN1.
- m <modo>	Significa definir a qué tráfico se aplicará la configuración de control de QoS y habilitar el control de QoS. 0: deshabilitar. 1: en, se aplica solo al tráfico entrante.

	2: fuera, se aplica solo al tráfico saliente. 3: ambos, se aplican tanto al tráfico entrante como al saliente. El valor predeterminado es habilitar (para el tráfico saliente).
- i <ancho de banda>	Significa configurar el ancho de banda de entrada en kbps (solo Ethernet WAN) La configuración disponible es de 1 a 100000.
- o <ancho de banda>	Significa configurar el ancho de banda de salida en kbps (solo Ethernet WAN). La configuración disponible es de 1 a 100000.
- r <índice:razón>	Significa establecer la relación para el índice de clase, en %.
- tu <modo>	Significa habilitar el control de ancho de banda para UDP. 0: deshabilitar 1: habilitar El valor predeterminado es deshabilitar.
- p <proporción>	Significa habilitar la relación de límite de ancho de banda para UDP.
- t <modo>	Significa habilitar/deshabilitar Priorizar ACK de TCP saliente. 0: deshabilitar 1: habilitar
-V	Mostrar todos los ajustes.
- Yo <ancho de banda>	Significa el ancho de banda de entrada no VoIP mínimo disponible cuando se detecta VoIP (Kbps). <ancho de banda>: Introduzca un valor. Valor predeterminado: la mitad del ancho de banda de entrada de la WAN.
- O <ancho de banda>	Significa el ancho de banda de salida no VoIP mínimo disponible cuando se detecta VoIP (Kbps). <ancho de banda>: Introduzca un valor. Valor predeterminado: la mitad del ancho de banda de salida de la WAN.
-v<0/1>	Significa ajustarse a la configuración mínima de ancho de banda de entrada/salida (o la mitad del ancho de banda de QoS). 0: Ajuste automático de ancho de banda. 1: Cuando se detecta VoIP, el ancho de banda de entrada/salida de QoS se ajustará a los valores mínimos.
- D	Establezca todo a los valores predeterminados de fábrica (para todas las WAN).

Ejemplo

```
> configuración qos -W 2 -m 3 -i 9500 -o 8500 -r 3:20 -u 1 -p 50 -t 1 Configuración
WAN2 !!!!
  El modo QOS de WAN2 es el ancho de banda
  entrante establecido en 9500. El ancho de banda
  saliente establecido en 8500. La relación WAN2
  clase 3 establecida en 20.
  control de ancho de banda WAN2 udp configurado para habilitar la tasa
  de límite de ancho de banda WAN2 udp configurado en 50 WAN2
  Outbound TCP ACK Prioritizel configurado para habilitar QoS WAN2
configurado completo; reiniciar QoS
>
```

Comando Telnet: clase qos

Este comando permite al usuario establecer la clase de QoS.

Sintaxis

qos clase -c*<no> -<a|e|d <no>>[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede ingresar varios comandos en una línea.
- h	Escríbalo para mostrar el uso de este comando.
- c <no>	Especifique el número de índice para la clase. El valor disponible para <no> contiene 1, 2 y 3. La configuración predeterminada es clase 1.
- n <nombre>	Significa escribir un nombre para la clase.
- a	Significa agregar una regla para una clase específica.
- e <no>	Significa editar la regla especificada. <no>: ingrese el número de índice para la regla.
- d <no>	Significa eliminar la regla especificada. <no>: ingrese el número de índice para la regla.
- m <modo>	Significa habilitar o deshabilitar la regla especificada. 0: deshabilitar, 1: habilitar
- I <dirección>	Configure la dirección local. *Dirección1*–Significa dirección única. Especifique la dirección IP directamente, por ejemplo, "*-I 172.16.3.9*". *dir1:dir2*–Significa Dirección de rango. Especifique las direcciones IP, por ejemplo, "*-I 172.16.3.9: 172.16.3.50*." *addr1: subred*–Significa la dirección de subred con la dirección IP de inicio. Ingrese la subred y la dirección IP, por ejemplo, "*-I 172.16.3.9:255.255.0.0".0* *cualquier* -Significa Cualquier dirección. tipo sencillo "*-I*" para especificar cualquier dirección para este comando.
- r <dirección>	Configure la dirección remota. *dirección1*–Significa dirección única. Especifique la dirección IP directamente, por ejemplo, "*-I 172.16.3.9*". *dir1:dir2*–Significa Dirección de rango. Especifique las direcciones IP, por ejemplo, "*-I 172.16.3.9: 172.16.3.50*." *addr1: subred*–Significa la dirección de subred con la dirección IP de inicio. Ingrese la subred y la dirección IP, por ejemplo, "*-I 172.16.3.9:255.255.0.0".0* *cualquier* -Significa Cualquier dirección. tipo sencillo "*-I*" para especificar cualquier dirección para este comando.
- I/-r	Establezca el Tipo de dirección en "cualquiera". No es necesario ingresar ninguna dirección IP.
- p <ID de DSCP>	Especifique la identificación.
- s <Tipo de servicio>	Especifique el tipo de servicio predefinido escribiendo el número. Los tipos disponibles se enumeran a continuación: 1:CUALQUIER 2:DNS 3:FTP 4:GRE 5:H.323 6:HTTP 7:HTTPS 8:IKE 9:IPSEC-AH 10:IPSEC-ESP 11:IRC 12:L2TP 13:NOTICIAS 14:NFS 15:NNTP 16:PING 17:POP3 18:PPTP 19:REAL-AUDIO 20: RTSP 21:SFTP 22:SIP 23:SMTP 24:SNMP 25:SNMP-TRAPS 26:SQL-NET 27:SSH 28:SYSLOG 29:TELNET 30:TFTP
- u <Tipo de servicio>	Especifique el tipo de servicio definido por el usuario escribiendo el número (1 a 40).
- S <d/s>	Muestra el contenido para el ID de DSCP especificado (0 a 20)/Tipo de servicio (1 a 40). En el cual, el ID de DSCP significa;

	0: predeterminado, 1: precedencia de IP 1, 2: precedencia de IP 2, 3: IP precedencia 3, 4: IP precedencia 4, 5: IP precedencia 5, 6: IP precedencia 6, 7: IP precedencia 7, 8: AF Class1 (Low Drop), 9: AF Class1 (Medium Drop), 10: AF Clase 1 (caída alta), 11: AF Clase 2 (caída baja), 12: AF Clase 2 (caída media) 13: AF Clase 2 (caída alta), 14: AF Clase 3 (caída baja), 15: AF Clase 3 (caída media), 16: AF Clase 3 (caída alta) Drop) 17: AF Class4 (Low Drop), 18: AF Class4 (Medium Drop), 19: AF Class4 (High Drop), 20: EF Class
- V <1/2/3>	Muestra la regla en la clase especificada.

Ejemplo

```
> qos clase -c 2 -n draytek -a -m 1 -l 192.168.1.50:192.168.1.80

  La siguiente configuración se establecerá en el nombre
  class2 class 2 establecido en draytek
  Agregar una regla en class2
  Class2 la 1 regla habilitada
  Establezca el tipo de dirección local en Rango, 192.168.1.50:192.168.1.80
>
```

Comando Telnet: tipo qos

Este comando permite al usuario configurar el tipo de protocolo y el número de puerto para QoS.

Sintaxis

tipo qos*[-un <nombre del servicio> | -e <no> | -d <no>]***.**

Sintaxis Descripción

Parámetro	**Descripción**
- un <nombre>	Significa agregar regla.
- e <no>	Significa editar el tipo de servicio definido por el usuario. “no” significa el número de índice. Los números disponibles son 1~40.
- d <no>	Significa eliminar el tipo de servicio definido por el usuario. “no” significa el número de índice. Los números disponibles son 1~40.
- n <nombre>	Significa el nombre del servicio.
- t <tipo>	Significa tipo de protocolo. 6: tcp (predeterminado) 17: upp 0: TCP/UDP <1~254>: otro
- p <puerto>	Significa puerto de servicio. El formato de escritura debe ser [inicio:fin] (ej., 510:330).
- yo	Lista de tipos definidos por el usuario. “no” significa el número de índice. Los números disponibles son 1~40.

Ejemplo

```
> qos tipo -a draytek -t 6 -p 510:1330

  nombre de servicio establecido en draytek
  tipo de servicio establecido en 6:TCP
```

```
  Tipo de puerto establecido en Rango Puerto de
  servicio establecido en 510 ~ 1330
>
```

Comando Telnet: qos voip

Este comando permite al usuario habilitar o deshabilitar QoS para VoIP y RTP.

Sintaxis

qos voip *<encendido/apagado>*

Sintaxis Descripción

Parámetro	Descripción
encendido apagado	Activado: habilite QoS para VoIP. Desactivado: deshabilitar QoS para VoIP.

Ejemplo

```
> qos voip apagado
QoS para VoIP: Deshabilitar; Puerto SIP: 5060
```

Comando Telnet: hwqos

Este comando permite al usuario configurar la QoS del hardware.

Sintaxis

configuración hwqos*[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede ingresar varios comandos en una línea.
- W <1/2>	Especifique la interfaz WAN. <1/2> - 1 significa WAN1; 2 significa WAN2
-P <1/2/3/4>	Especifique la interfaz LAN. <1/2/3/4>: 1 significa LAN1, 2 significa LAN2, etc.
- mi <1/0>	Activa o desactiva la función. <1/0> - 1 significa Habilitar; 0 significa Deshabilitar
- o <ancho de banda>	Configure el ancho de banda para el tráfico saliente (en kbps). *<ancho de banda>: ingrese un valor (>0).*
- r <índice:razón>	Establezca la relación de cada clase (1 ot 3). *<index:ratio> - El rango del índice incluye de 1 a 3; proporción en %.*
-V	Muestra la configuración actual.
- D	Restablezca la configuración predeterminada de fábrica de QoS de hardware.

Ejemplo

```
> configuración hwqos -W 2 -e 1 -o 100000 -r 1:60 -r 2:25 -r 3:10 Configuración
WAN2 !!!!
  El modo WAN2 QoS está habilitado para el ancho de
  banda de salida establecido en 100000. La relación
  total supera los 100
```

```
>
```

Comando Telnet: salir

Este comando puede salir de la pantalla de comandos de telnet.

Comando Telnet: mostrar lan

Este comando muestra el estado actual de la configuración de la dirección IP de LAN.

Ejemplo

```
> mostrar lan
La LAN ajustes:
          ip                mascarilla        dhcp  estrella_ip          piscina  puerta
-----------------------------------------------------------------------------------------
[V]LAN1   192.168.1.230     255.255.255.0     V     192.168.1.10         200      192.168.1.230
[X]LAN2   192.168.2.1       255.255.255.0     V     192.168.2.10         100      192.168.2.1
[X]LAN3   192.168.3.1       255.255.255.0     V     192.168.3.10         100      192.168.3.1
[X]LAN4   192.168.4.1       255.255.255.0     V     192.168.4.10         100      192.168.4.1
[X]LAN5   192.168.5.1       255.255.255.0     V     192.168.5.10         100      192.168.5.1
[X]LAN6   192.168.6.1       255.255.255.0     V     192.168.6.10         100      192.168.6.1
[X]LAN7   192.168.7.1       255.255.255.0     V     192.168.7.10         100      192.168.7.1
[X]LAN8   192.168.8.1       255.255.255.0     V     192.168.8.10         100      192.168.8.1
[X]Ruta   192.168.0.1       255.255.255.0     V     0.0.0.0              0        192.168.0.1
>
```

Comando Telnet: mostrar dmz

Este comando muestra el estado actual del host DMZ.

Ejemplo

```
> mostrar DMZ
%        Estado de mapeo WAN1 DMZ:
 Índice    Estado WAN1 IP auxiliar        ip privada
-------------------------------------------------------- 1
    Deshabilitar 0.0.0.0

%        Estado de asignación de WAN2 DMZ:
 Índice    Estado WAN2 IP auxiliar        ip privada
-------------------------------------------------------- 1
    Deshabilitar 0.0.0.0

%        Estado de mapeo WAN3 DMZ:
 Índice    Estado WAN3 aux IP             ip privada
-------------------------------------------------------- 1
    Deshabilitar 0.0.0.0

%        Estado de mapeo WAN4 DMZ:
 Índice    Estado WAN4 IP auxiliar        ip privada
-------------------------------------------------------- 1
    Deshabilitar 0.0.0.0

%        Estado de mapeo WAN5 DMZ:
 Índice    Estado WAN5 IP auxiliar        ip privada
```

```
----------------------------------------------------------1
          Deshabilitar 0.0.0.0
%         Estado de mapeo WAN6 DMZ:
 Índice    Estado WAN6 IP auxiliar          ip privada
----------------------------------------------------------1
    Deshabilitar 0.0.0.0
>
```

Comando Telnet: mostrar dns

Este comando muestra el estado actual de la configuración de DNS

Ejemplo

```
> mostrar DNS
%%        Configuración del servidor de nombres de dominio:
%  LAN1   DNS primario: [No establecido] DNS
%  LAN1   secundario: [No establecido]

%  LAN2   DNS primario: [No establecido] DNS
%  LAN2   secundario: [No establecido]

%  LAN3   DNS primario: [No establecido] DNS
%  LAN3   secundario: [No establecido]

%  LAN4   DNS primario: [No establecido] DNS
%  LAN4   secundario: [No establecido]

%  LAN5   DNS primario: [No establecido] DNS
%  LAN5   secundario: [No establecido]
. .
```

Comando Telnet: mostrar puerto abierto

Este comando muestra el estado actual de la configuración del puerto abierto.

Ejemplo

```
> mostrar puerto abierto

%%        Configuración de puerto abierto:

Índice      Comentario de estado              Dirección IP local

**********************************************************

                          Sin entrada de datos.
```

Comando Telnet: mostrar nat

Este comando muestra el estado actual de NAT.

Ejemplo

```
> mostrar nat
  Tabla de ejecución de redirección de puertos:

Índice    Protocolo     Puerto Público      ip privada          Puerto privado
 1              0              0     0.0.0.0                        0
 2              0              0     0.0.0.0                        0
```

3	0	0	0.0.0.0	0
4	0	0	0.0.0.0	0
5	0	0	0.0.0.0	0
6	0	0	0.0.0.0	0
7	0	0	0.0.0.0	0
8	0	0	0.0.0.0	0
9	0	0	0.0.0.0	0
10	0	0	0.0.0.0	0
11	0	0	0.0.0.0	0
12	0	0	0.0.0.0	0
13	0	0	0.0.0.0	0
14	0	0	0.0.0.0	0
15	0	0	0.0.0.0	0
dieciséis	0	0	0.0.0.0	0
17	0	0	0.0.0.0	0
18	0	0	0.0.0.0	0
19	0	0	0.0.0.0	0
20	0	0	0.0.0.0	0
- - - MÁS ---	['q': Salir, 'Entrar': Líneas nuevas, 'Barra espaciadora': Página siguiente]			

Comando Telnet: mostrar mapa de puertos

Este comando muestra la tabla de NAT Active Sessions.

Ejemplo

```
> mostrar mapa de puertos

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

   Private_IP:Puerto Pseudo_IP:Puerto Peer_IP:Puerto [Tiempo de espera/Protocolo/Bandera]

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Comando Telnet: mostrar pmtime

Este comando muestra el tiempo de reutilización de la sesión NAT.

Level0: Es la configuración por defecto.

Nivel 1: se aplicará cuando las sesiones NAT sean inferiores al 25 % del valor predeterminado.

Nivel 2: Se aplicará cuando las sesiones NAT sean inferiores a la octava parte del valor predeterminado.

Ejemplo

```
> mostrar la hora de la tarde

   Nivel 0 TCP=86400001 UDP=300001 ICMP=10001

   Nivel 1 TCP=600000 UDP=90000 ICMP=7000

   Nivel 2 TCP=60000 UDP=30000 ICMP=5000
```

Comando Telnet: mostrar sesión

Este comando muestra el estado actual de la sesión actual.

Ejemplo

```
> mostrar sesión
```

```
% Número máximo de sesión: 60000
% de uso máximo de sesión: 0
% de uso de la sesión actual: 0
% de sesión actual utilizada (incluye espera gratis): 6
% de uso de sesión actual de WAN1: 0
% de uso de sesión actual de WAN2: 0
% de uso de sesión actual de WAN3: 0
% de uso de sesión actual de WAN4: 0
% de uso de sesión actual de WAN5: 0
% de uso de sesión actual de WAN6: 0
```

Comando Telnet: mostrar estado

Este comando muestra el estado actual de las conexiones LAN y WAN.

Ejemplo

```
> mostrar estado

Tiempo de actividad del sistema: 95: 4: 44
Estado de la LAN
DNS primario: 8.8.8.8                  DNS secundario: 8.8.4.4
Dirección IP: 192.168.1.1              Tasa Tx:125096 Tasa Rx:41045

Estado de WAN 1: Desconectado
Habilitar: Sí          Línea:Ethernet          Nombre:
Modo: Cliente DHCP Tiempo activo: 0:00:00      IP:---          IP de GW:---
Paquetes TX: 0         Tasa de transmisión (bps): 0    Paquetes RX: 0         Tasa de RX (bps): 0

Estado de WAN 2: Desconectado
Habilitar: Sí          Línea:Ethernet          Nombre:
Modo: Cliente DHCP Tiempo activo: 0:00:00      IP:---          IP de GW:---
Paquetes TX: 0         Tasa de transmisión (bps): 0    Paquetes RX: 0         Tasa de RX (bps): 0

Estado de WAN 3: Desconectado
Habilitar: No          Línea:Ethernet          Nombre:
Modo:---               Hora de actividad:0:00:00      IP:---          IP de GW:---
Paquetes TX: 0         Tasa de transmisión (bps): 0    Paquetes RX: 0         Tasa de RX (bps): 0

Estado de WAN 4: Desconectado
Habilitar: No          Línea:Ethernet          Nombre:
. . .
```

Comando Telnet: mostrar tráfico

Este comando puede mostrar el gráfico de tráfico para WAN1 a WAN4, bytes transmitidos, bytes recibidos y sesiones.

Sintaxis

mostrar tráfico*[wan1/..wan6] [tx/rx] [semanalmente]*

mostrar tráfico*[direcciónip] [tx/rx]* **mostrar sesión de tráfico***[semanalmente]*

Ejemplo

```
>   mostrar la sesión de tráfico semanalmente ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0

  , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
, 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
  , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
, 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
  , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,2 ,1 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
, 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,1 ,3 ,0 ,0 ,0 ,0 ,0 ,2 ,15 ,5 ,4 ,1 ,0 ,0 ,
, 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 0 ,0 , 0 ,0
> Mostrar tráfico wan1 tx semanal0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0

  , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0

  , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0

  , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
, 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
  , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0
```

Comando Telnet: muestre el tráfico del cliente

Este comando muestra la información del paquete para el dispositivo externo especificado.

Sintaxis

mostrar tráfico de clientes*[índice de dispositivo] [wan# o lan#] [tx/rx] [semanalmente]*

Sintaxis Descripción

Parámetro	Descripción
[índice de dispositivo]	Ingrese el índice del dispositivo (01 – 30) en dos dígitos (por ejemplo, 01, 02) para el dispositivo externo. Use la "lista de interruptores" para verificar qué VigorSwitch se conecta a este enrutador. Luego, ingrese el número de índice de este VigorSwitch en este campo.
[wan# o lan#]	wan# - Especifique la interfaz WAN (WAN1 a WAN2) para el enrutador Vigor. lan#- Especifique la interfaz LAN (LANA / LANB) para el enrutador Vigor.
[tx/rx]	Tx: indica los datos transmitidos. Rx – Indica datos recibidos.
[semanalmente]	Muestra los datos transmitidos o los datos recibidos recopilados semanalmente.

Ejemplo

```
> mostrar tráfico de clientes 01 lana tx semanalmente
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0 , 0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 , 0
```

Comando Telnet: mostrar estadística

Este comando muestra estadísticas para la interfaz WAN.

Sintaxis

Mostrar estadística

mostrar restablecimiento de estadísticas*<interfaz>*

Sintaxis Descripción

Parámetro	Descripción
reiniciar	Significa restablecer los bytes transmitidos/recibidos a cero.
interfaz	Significa especificar la interfaz WAN1 ~ WAN5 (incluidos varios PVC) para mostrar las estadísticas relacionadas.

Ejemplo

```
> mostrar estadística
  WAN1 total TX: 0 bytes, RX: 0 bytes WAN2 total
TX: 0 bytes, RX: 0 bytes WAN3 total TX: 0 bytes,
RX: 0 bytes WAN4 total TX: 0 bytes, RX: 0 bytes
WAN5 total TX: 0 bytes ,RX: 0 Bytes WAN6 total
TX: 0 Bytes ,RX: 0 Bytes WAN7 total TX: 0
Bytes ,RX: 0 Bytes WAN8 total TX: 0 Bytes ,RX: 0
Bytes WAN9 total TX: 0 Bytes ,RX: 0 Bytes



 >
```

Comando Telnet: configuración de smb

Este comando se utiliza para configurar los ajustes de uso compartido de archivos para el servidor SMB.

Sintaxis

ajuste smb*<habilitar/deshabilitar>*

ajuste smb*estado*

ajuste smb*establecer grupo de trabajo <Nombre del grupo de trabajo>* **ajuste smb***establecer host <nombre de host>* **ajuste smb***establecer acceso <LAN / LANWAN>* **ajuste smb***establecer versión <v1v2/v2>*

Sintaxis Descripción

Parámetro	Descripción
<habilitar/deshabilitar>	Habilite o deshabilite el servicio SMB.
estado	Muestra el estado actual del servicio SMB.
Establecer grupo de trabajo <Nombre del grupo de trabajo>	Significa establecer un nombre de grupo de trabajo para el servicio SMB.
establecer host <nombre de host>	Significa establecer un nombre de host para el servicio SMB.
establecer acceso <LAN / LANWAN>	Significa configurar el acceso al servidor SMB por LAN o por LAN y WAN.
establecer versión <v1v2/v2>	Significa configurar la versión del servidor SMB.

Ejemplo

```
> smb setting enable El servicio
SMB está habilitado.

> configuración smb establecer acceso LAN
Permitir el acceso SMB solo desde LAN.
> configuración smb establecer versión
v1v2 Versión SMB: v1 y v2.
```

Comando Telnet: srv dhcp dhcp2

Este comando se utiliza para habilitar el servidor DCHP2.

Sintaxis

srv dhcp dhcp2*[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
- l <habilitar>	El servidor DHCP asigna las direcciones IP a los clientes a través del puerto LAN. <habilitar>: ingrese 0 (deshabilitar) o 1 (habilitar).
- m <habilitar>	El servidor DHCP asigna las direcciones IP a los clientes a través de la configuración de direcciones MAC. <habilitar>: ingrese 0 (deshabilitar) o 1 (habilitar).
- e <id>	Encienda la bandera de LAN 1 o LAN 2 si el puerto LAN está habilitado. <id>: Introduzca 1 o 2.
- d <identificación>	Desactive la bandera del puerto LAN 1 o puerto LAN 2. <id>: Ingrese 1 o 2.
-v	Ver el estado actual.

Ejemplo

```
> srv dhcp dhcp2 -l 1 -e 1,2
> srv dhcp dhcp2 -v
 Segundo estado de la bandera del servidor DHCP --
    El servidor funciona en la dirección MAC especificada: ON El
    servidor funciona en el puerto LAN especificado: ON Indicador
    del puerto 1: ON
    Indicador del puerto 2: ENCENDIDO
>
```

Comando Telnet: srv dhcp público

Este comando permite a los usuarios configurar el servidor DHCP para la segunda subred.

Sintaxis

srv dhcp público*iniciar <dirección IP>*

srv dhcp público*cnt <recuentos de IP>*

srv dhcp público*estado*

srv dhcp público*agregar <Dirección MAC XX-XX-XX-XX-XX-XX>* **srv dhcp público***del <Dirección MAC XX-XX-XX-XX-XX-XX/todas/TODAS>*

Sintaxis Descripción

Parámetro	Descripción
iniciar <dirección IP>	Significa el punto de partida del grupo de direcciones IP para el servidor DHCP. *<dirección IP>:*Especifique una dirección IP como punto de partida en el grupo de direcciones IP.
cnt <recuentos de IP>	Significa el número de recuento de IP. *<Recuentos de IP>:*Especifique el número de direcciones IP en el grupo. El máximo es 10.
estado	Significa el resultado de la ejecución de este comando.
añadir <Dirección MAC XX-XX-XX-XX-XX-XX>	Significa crear una lista de hosts para ser asignados. <Dirección MAC XX-XX-XX-XX-XX-XX>:*S*Especifique la dirección MAC del host.
del <Dirección MAC XX-XX-XX-XX-XX-XX/todos/TODOS>	Significa eliminar la dirección MAC seleccionada. <Dirección MAC XX-XX-XX-XX-XX-XX>:*S*Especifique la dirección MAC del host. all/ALL: Significa todas las direcciones MAC.

Ejemplo

```
> ruta IP agregar 192.168.1.56 255.255.255.0 192.168.1.12 3 por defecto
> srv dhcp public status Índice
Dirección MAC
```

Comando Telnet: srv dhcp dns1

Este comando permite a los usuarios configurar la dirección IP principal para el servidor DNS en LAN.

Sintaxis

srv dhcp dns1*<lan1/lan2/lan3/lan4/lan5/lan6/lan7/lan8> <dirección IP DNS>*

Sintaxis Descripción

Parámetro	Descripción
<lan1/lan2/lan3/lan4/lan5/lan6/lan7/lan8>	Significa especificar la interfaz LAN para configurar el servidor DNS.
<Dirección IP DNS>	Significa la dirección IP que desea utilizar como DNS1. **Nota:**El DNS de la subred enrutada por IP debe ser el mismo que el DNS de la subred NAT).

Ejemplo

```
> srv dhcp dns1 lan1 168.95.1.1
% srv dhcp dns1 lan1 <dirección IP DNS> % Ahora:
168.95.1.1
(Subred IP enrutada dns igual que lan1)
```

Comando Telnet: srv dhcp dns2

Este comando permite a los usuarios establecer una dirección IP secundaria para el servidor DNS en LAN.

Sintaxis

srv dhcp dns2*<lan1/lan2/lan3/lan4/lan5/lan6/lan7/lan8> <dirección IP DNS>*

Sintaxis Descripción

Parámetro	Descripción
<lan1/lan2/lan3/lan4/lan5/ lan6/lan7/lan8>	Significa especificar la interfaz LAN para configurar el servidor DNS.
<Dirección IP DNS>	Significa la dirección IP que desea utilizar como DNS2. **Nota:**El DNS de la subred enrutada por IP debe ser el mismo que el DNS de la subred NAT).

Ejemplo

```
> srv dhcp dns2 lan3 10.1.1.1
% srv dhcp dns2 lan3 <dirección IP DNS> % Ahora:
10.1.1.1
```

Comando Telnet: srv dhcp frcdnsmanl

Este comando puede obligar al enrutador a invocar la dirección IP del servidor DNS.

Sintaxis

srv dhcp frcdnsmanl <*encendido/apagado>*

Sintaxis Descripción

Parámetro	Descripción
?	Significa mostrar el estado actual.
en	Significa usar la configuración manual para la configuración de DNS.
apagado	Significa usar configuraciones automáticas adquiridas de ISP.

Ejemplo

```
> srv dhcp frcdnsmanl en
¡% El servidor de nombres de dominio ahora está usando configuraciones manuales!
> srv dhcp frcdnsmanl apagado
¡% El servidor de nombres de dominio ahora está usando la configuración automática!
```

Comando Telnet: puerta de enlace srv dhcp

Este comando permite a los usuarios especificar la dirección de la puerta de enlace para el servidor DHCP.

Sintaxis

puerta de enlace srv dhcp*<Puerta de enlace IP>*

Sintaxis Descripción

Parámetro	Descripción
IP de acceso	Significa especificar una dirección de puerta de enlace utilizada para el servidor DHCP.

Ejemplo

```
> puerta de enlace srv dhcp 192.168.2.1
  Esta configuración tendrá efecto después de reiniciar. Utilice el
  comando "sys reboot" para reiniciar el enrutador.
```

Comando Telnet: srv dhcp ipcnt

Este comando permite a los usuarios especificar recuentos de IP para el servidor DHCP.

Sintaxis

srv dhcp ipcnt *<recuentos de IP>*

Sintaxis Descripción

Parámetro	Descripción
recuentos de IP	Significa el número que debe especificar para el servidor DHCP.

Ejemplo

```
> srv dhcp ipcnt?
% srv dhcp ipcnt <Recuentos de IP> %
Ahora: 150
```

Comando Telnet: srv dhcp apagado

Esta función permite a los usuarios apagar el servidor DHCP. Necesita reiniciar el enrutador, escriba el comando "sys reboot" para reiniciar el enrutador.

Comando Telnet: srv dhcp en

Esta función permite a los usuarios activar el servidor DHCP. Necesita reiniciar el enrutador, escriba el comando "sys reboot" para reiniciar el enrutador.

Comando Telnet: relé srv dhcp

Este comando permite a los usuarios establecer la configuración de retransmisión DHCP.

Sintaxis

servicio de retransmisión srv dhcp *<IP del servidor>* **srv**

dhcp relé 2nd_servip *<IP del servidor>* **subred de**

retransmisión srv dhcp *<índice>*

Sintaxis Descripción

Parámetro	Descripción
servidor IP	Significa la dirección IP que desea utilizar como servidor DHCP.
Índice	Significa subred 1 o 2. Escriba 1 o 2. El enrutador invocará esta función de acuerdo con la subred 1 o 2 especificada aquí.

Ejemplo

```
> servicio de retransmisión srv dhcp 192.168.1.46
> srv dhcp relé subred 2
> servip srv dhcp relé?
% srv dhcp relay servip <ip del servidor> %
Ahora: 192.168.1.46
```

Comando Telnet: srv dhcp starttip

Sintaxis

punta de inicio srv dhcp*<dirección IP>*

Sintaxis Descripción

Parámetro	Descripción
dirección IP	Significa la dirección IP que puede especificar para el servidor DHCP como punto de partida.

Ejemplo

```
> srv dhcp punta de inicio 192.168.1.53
  Esta configuración tendrá efecto después de reiniciar. Utilice el
  comando "sys reboot" para reiniciar el enrutador.
```

Comando Telnet: estado srv dhcp

Este comando puede mostrar información general del servidor DHCP, como la dirección IP, la dirección MAC, el tiempo arrendado, la ID del host, etc.

Sintaxis

estado de srv dhcp*<LAN1/2/3/4/5/6/7/8/ip_routed_subnet>*

Sintaxis Descripción

Parámetro	Descripción
<LAN1/2/3/4/5/6/7/8 /subred_enrutada_ip>	Significa mostrar el estado actual de la interfaz seleccionada.

Ejemplo

```
> estado srv dhcp LAN1
                : Servidor DHCP activado        Grupo IP: 192.168.1.10 ~ 192.168.1.209
                  Puerta de enlace predeterminada: 192.168.1.1:
IP enrutada     servidor DHCP desactivado
---------------------------------------------------------------------------------
Índice Dirección IP             Dirección MAC                   ID de HOST de tiempo arrendado
--------------------------------------------------------------------------------- LAN1

1       192.168.1.10        00-1D-AA-0F-2E-68           17:24:58
2       192.168.1.11        00-1D-AA-4F-E2-98           17:54:14
>
```

Comando Telnet: srv dhcp leasetime

Este comando puede establecer el tiempo de concesión para el servidor DHCP.

Sintaxis

tiempo de concesión srv dhcp*<Tiempo de alquiler (seg)>*

Sintaxis Descripción

Parámetro	Descripción
Tiempo de arrendamiento (seg)	Significa el tiempo de concesión (500 a 1661992960) que puede usar el servidor DHCP. La unidad es segunda.

Ejemplo

```
> srv dhcp tiempo de concesión?
% srv dhcp leasetime <Tiempo de arrendamiento (seg.)>
% Ahora: 86400
>
```

Comando Telnet: tipo de nodo srv dhcp

Este comando puede establecer el tipo de nodo para el servidor DHCP.

Sintaxis

tipo de nodo srv dhcp*<contar>*

Sintaxis Descripción

Parámetro	Descripción
contar	Significa especificar un tipo para el nodo. 1. nodo B 2. nodo P 4. nodo M 8. H-nodo

Ejemplo

```
> tipo de nodo srv dhcp 1
> tipo de nodo srv dhcp? %% srv tipo
de nodo dhcp <recuento>
%% 1. Nodo B 2. Nodo P 4. Nodo M 8. Nodo H % Ahora: 1
```

Comando Telnet: srv dhcp primWINS

Este comando puede establecer la dirección IP principal para el servidor DHCP.

Sintaxis

srv dhcp primWINS *<Dirección IP de WINS>*

srv dhcp primWINS claro

Sintaxis Descripción

Parámetro	Descripción
dirección IP gana	Significa la dirección IP del servidor WINS principal.
claro	Significa eliminar la configuración de la dirección IP del servidor WINS principal.

Ejemplo

```
> servidor dhcp primWINS 192.168.1.88
> srv dhcp primWINS?
%% srv dhcp primWINS <dirección IP de WINS> %%
srv dhcp primWINS borrar
% Ahora: 192.168.1.88
```

Comando Telnet: srv dhcp secWINS

Este comando puede establecer la dirección IP secundaria para el servidor DHCP.

Sintaxis

srv dhcp secWINS *<Dirección IP de WINS>*

srv dhcp secWINS claro

Sintaxis Descripción

Parámetro	Descripción
dirección IP gana	Significa la dirección IP del servidor WINS secundario.
claro	Significa eliminar la configuración de la dirección IP del segundo servidor WINS.

Ejemplo

```
> srv dhcp secWINS 192.168.1.180
> srv dhcp secWINS?
%% srv dhcp secWINS <dirección IP de WINS> %%
srv dhcp secWINS claro
% Ahora: 192.168.1.180
```

Comando Telnet: srv dhcp expRecycleIP

Este comando puede configurar el tiempo para verificar si el servidor DHCP puede asignar nuevamente la dirección IP o no.

Sintaxis

srv dhcp expRecycleIP *<segundo tiempo>*

Sintaxis Descripción

Parámetro	Descripción
segundo tiempo	Significa configurar el tiempo (5~300 segundos) para verificar si la IP se puede asignar nuevamente o no.

Ejemplo

```
Vigor> srv dhcp expRecycleIP 250 % DHCP
expired_RecycleIP = 250
```

Comando Telnet: srv dhcp tftp

Este comando puede configurar el servidor TFTP como el servidor DHCP.

Sintaxis

srv dhcp tftp *<Nombre del servidor TFTP>*

Sintaxis Descripción

Parámetro	Descripción
nombre del servidor TFTP	Significa Ingresar el nombre del servidor TFTP.

Ejemplo

```
> srv dhcp tftp TF123
> srv dhcp tftp?
%% srv dhcp tftp <nombre del servidor TFTP> %
Ahora: TF123
```

Comando Telnet: srv dhcp tftpdel

Este comando puede eliminar el nombre definido para el servidor TFTP.

Sintaxis

srv dhcp tftpdel

Ejemplo

```
> srv dhcp tftp TF123
> srv dhcp tftp?
%% srv dhcp tftp <nombre del servidor TFTP> %
Ahora: TF123
> srv dhcp tftpdel
% ¡El nombre del servidor TFTP se ha eliminado!
```

Comando Telnet: opción srv dhcp

Este comando puede establecer la opción personalizada para el servidor DHCP.

Sintaxis

opción srv dhcp-*h* **opción**
srv dhcp-*yo* **opción srv**
dhcp-*d <idx>*
opción srv dhcp-*e <1 o 0> -i <número de LAN> -s <Dirección IP del servidor siguiente>*
opción srv dhcp-*e <1 o 0> -i <número de LAN> -c <número de opción> -v <valor de opción>*
opción srv dhcp-*e <1 o 0> -i <número de LAN> -c <número de opción> -x <valor de opción>*
opción srv dhcp -*e <1 o 0> -i <número de LAN> -c <número de opción> -a <valor de opción>*
opción srv dhcp-*u <número idx>*

Sintaxis Descripción

Parámetro	Descripción
- h	Significa mostrar el uso de este comando.
- yo	Significa mostrar todas las opciones de DHCP definidas por el usuario.
- d <idx>	Significa eliminar el número de opción especificando su número de índice.
- mi <1/0>	Significa habilitar/deshabilitar la función de opciones personalizadas. 1: Habilitar; 0: Deshabilitar
- i <número de lan>	<número de red>.Significa especificar la interfaz LAN. 1: lan1 R: todas las LAN r: subred enrutada d: DMZ
- s <Dirección IP del servidor siguiente>	Significa establecer la siguiente dirección IP del servidor. Siguiente dirección IP del servidor: Ingrese una dirección IP.
- c <opción número>	Significa establecer el número de opción. El número disponible varía de 0 a 255. número de opción: Ingrese un número.
- v <valor de opción>	Significa establecer el número de opción escribiendo una cadena. Valor de la opción: Introduzca una cadena.
- x <valor de opción>	Significa establecer el número de opción con el formato de caracteres hexadecimales. valor de la opción: Introduzca un número (hexadecimal).
- un <valor de opción>	Significa establecer el valor de la opción especificando la dirección IP. Valor de la opción: Introduzca una dirección IP.
- u <número idx>	Significa actualizar el valor de la opción del índice especificado. número idx*r*: Introduzca el número de índice del valor de la opción.
-r	Significa eliminar todas las opciones del servidor DHCP.

Ejemplo

```
> opción srv dhcp -e 1 -i 1/2 -s 8.8.8.8
> opción srv dhcp -l
% interfaz de idx de estado          tipo de opción      datos

% habilitar 1      LAN1/2          0    Dirección SI    0.0.0.0
```

Comando Telnet: srv nat dmz

Este comando permite a los usuarios configurar el host DMZ. Antes de usar este comando, configure primero el alias de IP de WAN.

Sintaxis

srv nat dmz nm*[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
norte	Significa asignar la IP WAN seleccionada a cierto host. 1: wan1 2: wan2
metro	Significa el número de índice (1 a 32) del host DMZ. La configuración predeterminada es "1" (WAN 1). Solo está disponible para el modo de IP estática. Si usa otro modo, puede configurar 1 ~ 32 en este campo. Si se configuró el alias de IP de WAN, entonces se puede agregar más el número de host DMZ.
[<comando> <parámetro>/...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede ingresar varios comandos en una línea.
- mi	Significa habilitar/deshabilitar dicha característica. 1: habilitar 0: deshabilitar
- i	Significa especificar la dirección IP privada del host DMZ.
-r	Significa eliminar la configuración del host DMZ.
-v	Significa mostrar el estado actual.

Ejemplo

```
> srv nat dmz 1 1 -i 192.168.1.96
> srv nat dmz -v %
        Estado de mapeo WAN1 DMZ:
 Índice    Estado WAN1 IP auxiliar          ip privada
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 1
   Deshabilitar 0.0.0.0 192.168.1.96

%       Estado de asignación de WAN2 DMZ:
 Índice    Estado WAN2 IP auxiliar          ip privada
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 1
   Deshabilitar 0.0.0.0

%       Estado de mapeo WAN3 DMZ:
 Índice    Estado WAN3 aux IP               ip privada
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 1
   Deshabilitar 0.0.0.0

%       Estado de mapeo WAN4 DMZ:
 Índice    Estado WAN4 IP auxiliar          ip privada
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 1
   Deshabilitar 0.0.0.0
```

```
%        Estado de mapeo WAN5 DMZ:
 Índice    Estado WAN5 IP auxiliar          ip privada
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 1
    Deshabilitar 0.0.0.0

%        Estado de mapeo WAN6 DMZ:
 Índice    Estado WAN6 IP auxiliar          ip privada
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -


    1      Deshabilitar 0.0.0.0
>
```

Comando Telnet: srv nat ipsecpass

Este comando permite a los usuarios habilitar o deshabilitar el paso del túnel IPSec ESP y la preservación del puerto de origen IKE (500).

Sintaxis

srv nat ipsecpass *<opciones>*

Sintaxis Descripción

Parámetro	Descripción
<opciones>	Los comandos disponibles con parámetros se enumeran a continuación.
en	Significa habilitar el paso del túnel IPSec ESP y la conservación del puerto de origen IKE (500).
apagado	Significa deshabilitar el paso del túnel IPSec ESP y la conservación del puerto de origen IKE (500).
estado	Significa mostrar el estado actual para verificar.

Ejemplo

```
> estado de srv nat ipsecpass
%% Estado: IPsec ESP pass-thru y IKE src_port:500 preservación está DESACTIVADA.
```

Comando Telnet: srv nat openport

Este comando permite a los usuarios establecer la configuración de puerto abierto para el servidor NAT.

Sintaxis

srv nat puerto abierto nm *[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
norte	Significa el número de índice para los perfiles. El rango es de 1 a 40.
metro	Significa especificar el número de subelemento para este perfil. El rango es de 1 a 10.
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]* significa que puede ingresar varios comandos en una línea.
- un <habilitar>	Significa habilitar o deshabilitar el perfil de regla de puerto abierto. 0: deshabilitar 1: habilitar

- c <comentario>	Significa Ingresar la descripción (menos de 23 caracteres) para el servicio de red definido.
- l <idx de IP de origen>	Significa establecer el objeto IP de origen. 1 a 192: para objeto IP 1 a 32: para grupo IP 0: cualquiera Por ejemplo: srv nat openport 1 1 -l 1 -g 0
- g <tipo de IP de origen>	Significa establecer el tipo de IP. 0: objeto IP 1: grupo de IP Por ejemplo: srv nat openport 1 1 -l 1 -g 0
- yo <ip local>	Significa configurar la dirección IP para la computadora local. IP local: escriba una dirección IP en este campo.
- w <widx><ipidx>	widx: Especifique la IP pública. 1: WAN1 predeterminado, 2: alias 1 de WAN1, ...etcétera. ipidx: Especifique el número de índice de una IP de alias (1 a 32).
- p <protocolo>	Especifique el protocolo de la capa de transporte. Los valores disponibles son TCP, UDP y TODOS.
- s<puerto de inicio>	Significa especificar el número de puerto inicial del servicio ofrecido por el host local. El rango es de 0 a 65535.
- e<puerto final>	Significa especificar el número de puerto final del servicio ofrecido por el host local. El rango es de 0 a 65535.
-v	Significa mostrar la configuración actual.
- r <eliminar>	Significa eliminar la configuración de puerto abierto especificada. eliminar: Introduzca el número de índice del perfil.
- f	Significa volver a la configuración de fábrica para todos los perfiles de puertos abiertos.

Ejemplo

```
> srv nat openport 1 1 -a 1 -c juegos -i 192.168.1.55 -w 1 1 -p TCP -s 56 -e 83

  ¡Establezca el puerto WAN bien!

> srv nat openport 1 1 -v %%
Estado: Habilitar
%% Comentario: juegos
%% Interfaz WAN: WAN1
%% Dirección IP privada: 192.168.1.55
Protocolo de índice          Puerto de inicio          Puerto final
**********************************************************************
   1.TCP                     56                  83
> srv nat puerto abierto 1 1 -f
> srv nat openport 1 1 -v %%
Estado: Deshabilitar
%% Comentario:
%% Interfaz WAN: WAN1
%% Dirección IP privada: 0.0.0.0
Protocolo de índice          Puerto de inicio          Puerto final
```

```
**********************************************************************
>
```

Comando Telnet: mapa de puertos srv nat

Este comando permite a los usuarios configurar la tabla de redirección de puertos para el servidor NAT.

Sintaxis

mapa de puerto srv nat*add <idx> <nombre del servidor> <proto> <puerto pub> <tipo de ip src> <idx ip src> <ip pri> <puerto pri> <idx wan> <ip alias>*

mapa de puerto srv nat*del <idx>* **mapa de puerto srv**

nat*deshabilitar <idx>* **mapa de puerto srv nat***habilitar*

<idx><proto> **mapa de puerto srv nat***enjuagar* **mapa**

de puerto srv nat*mesa* **mapa de puerto srv nat***vista*

Sintaxis Descripción

Parámetro	Descripción
añadir <idx>	Significa agregar una nueva tabla de redirección de puertos con un número de índice. El número de índice disponible es del 1 al 40.
<nombre del servidor>	Significa escribir un nombre como nombre de servicio.
<prototipo>	Significa especificar TCP o UDP como protocolo.
<Puerto de pub>	Significa especificar qué puerto (0 a 65535) se puede redirigir a la IP privada y el puerto especificados del host interno.
<tipo de IP de origen>	Significa especificar el tipo de IP (objeto o grupo). tipo de ip: 0 significa objeto IP; 1 significa grupo de IP.
<idx de ip de origen>	Significa especificar el número de índice del perfil del objeto. ip idx: 1 a 192 para perfil de objeto IP; 1 a 32 para perfil de grupo IP. 0 significa cualquier objeto o grupo.
<ip principal>	Significa especificar la dirección IP privada del host interno que proporciona el servicio.
<puerto principal>	Significa especificar el número de puerto privado (0 a 65535) del servicio ofrecido por el host interno.
<wan idx>	Significa especificar la interfaz WAN para la redirección del puerto. Idx: wan1 a wan6, todos
<IP de alias>	Significa especificar una IP de alias ingresando el número de índice (1 a 32). IP: 1 a 32.
del <idx>	Significa eliminar la configuración de redirección de puerto seleccionada.
deshabilitar <idx>	Significa desactivar la configuración de redirección de puerto seleccionada.
habilitar <idx>	Significa activar la configuración de redirección de puerto seleccionada.
enjuagar	Significa borrar todas las configuraciones de mapeo de puertos.
mesa	Significa mostrar la tabla de configuración de redirección de puertos.

Ejemplo

```
> srv nat portmap agregar 1 nombre tcp 100 0 0 192.168.1.10 200 wan1 1
> tabla portmap srv nat
```

Tabla de configuración de redirección de puertos NAT:

Nombre del servicio de índice	Protocolo	Puerto Público	ip privada	Puerto privado	si no
1 nombre	TCP	100	192.168.1.10	20	0 - 1
2	Desactivado	0		0	- 2
3	Desactivado	0		0	- 2
4	Desactivado	0		0	- 2
5	Desactivado	0		0	- 2
6	Desactivado	0		0	- 2
7	Desactivado	0		0	- 2
8	Desactivado	0		0	- 2
9	Desactivado	0		0	- 2
10	Desactivado	0		0	- 2
11	Desactivado	0		0	- 2
. . .					

Comando Telnet: disparador srv nat

Este comando permite a los usuarios configurar los ajustes de activación de puertos para NAT.

Sintaxis

srv nat trigger setdefault

srv nat trigger vista

disparador srv nat*n [-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
establecer predeterminado	Establecido en la configuración predeterminada de fábrica.
vista	Muestre todas las configuraciones de activación de puertos.
norte *<comando><parámetro>|...]*	"n" significa el número de regla. Los comandos disponibles con parámetros se enumeran a continuación. *[...]* significa que puede escribir varios comandos en una línea.
- c <XXX>	Escriba un comentario para dicha regla si es necesario.
- mi <0/1>	Habilite (1) o deshabilite (0) una regla (especificada con el número de regla).
- s <valor>	Significa el número de índice para la IP de origen. <valor> - Cualquiera, Objeto IP (0 a 191); Grupo IP (0 a 31).

- gramo <0/1>	Significa el tipo de IP de origen. 0 - Objeto IP; 1 - Grupo IP.
- pag <1/2/3>	Especifique el protocolo para dicha regla de activación. 1 – TCP 2 – UDP 3 - Todos
- t	Especifique el número de puerto (0~65535) para el disparador.
- P <1/2/3>	Especifique el protocolo de entrada para dicha regla de activación. 1 – TCP 2 – UDP 3 - Todos
- i	Especifique el número de puerto (0~65535) para el protocolo de entrada.
- d	Eliminar la regla de activación seleccionada.
-v	Muestra la configuración de activación del puerto para la regla especificada.

Ejemplo

```
> srv nat disparador 1 -c after_dinner
> disparador srv nat 1 -e 1
> disparador srv nat 1 -p 1
> disparador srv nat 1 -t 2000
> disparador srv nat 1 -P 2
> disparador srv nat 1 -i 3000
> desencadenador srv nat 1 -v

Índice de regla de activación de puerto: 1

Estado: Habilitar
Comentario: after_dinner2000
Protocolo de activación: TCP
Puerto de activación: 2000
Protocolo entrante: UDP
Puerto entrante: 3000
```

Comando Telnet: estado srv nat

Este comando permite a los usuarios ver la tabla de ejecución de redirección de puertos NAT.

Ejemplo

```
> estado srv nat
Tabla de ejecución de redirección de puertos NAT:

Índice    Protocolo    Puerto Público    ip privada        Puerto privado
 1            6            80     192.168.1.11                100
 2            0             0     0.0.0.0                      0
 3            0             0     0.0.0.0                      0
 4            0             0     0.0.0.0                      0
 5            0             0     0.0.0.0                      0
 6            0             0     0.0.0.0                      0
 7            0             0     0.0.0.0                      0
```

```
 8          0          0    0.0.0.0                 0
 9          0          0    0.0.0.0                 0
10          0          0    0.0.0.0                 0
11          0          0    0.0.0.0                 0
12          0          0    0.0.0.0                 0
13          0          0    0.0.0.0                 0
14          0          0    0.0.0.0                 0
15          0          0    0.0.0.0                 0
dieciséis   0          0    0.0.0.0                 0
17          0          0    0.0.0.0                 0
18          0          0    0.0.0.0                 0
19          0          0    0.0.0.0                 0

20          0          0    0.0.0.0                 0

- - - MÁS ---        ['q': Salir, 'Entrar': Líneas nuevas, 'Barra espaciadora': Página siguiente] ---
```

Comando Telnet: srv nat showall

Este comando permite a los usuarios ver un resumen de la configuración de redirección de puerto NAT, puerto abierto y configuración de DMZ.

Ejemplo

```
> srv nat showall? Índice Proto
WAN IP:Puerto                                   IP privada: Puerto          Acto
**********************************************************************
******* R01 TCP 0.0.0.0:100                    192.168.1.10:200            Y

O01     TCP     0.0.0.0:56~83                 192.168.1.55:56~83          Y

D01     Todo    0.0.0.0                       192.168.1.96                Y

R: Redirección de puertos, O: Puertos abiertos, D: DMZ
>
```

Comando Telnet: srv nat pseudoctl

Este comando permite a los usuarios verificar el número de pseudo puerto para evitar conflictos de puertos.

Sintaxis

srv nat pseudoctl*sesión <valor>*
srv nat pseudoctl*función <0-3>*

Sintaxis Descripción

Parámetro	Descripción
sesión <valor>	Establecer el umbral de la sesión. <valor>: o al 2147483647.
función <0-3>	0: Significa "Automático". Verifique el número de pseudo puerto creado automáticamente cuando el número de sesión supere el umbral. 1: Significa "No". Cree un número de pseudo puerto basado en la configuración de la subred. Sin verificación. 2: Significa "debe". Compruebe el número de pseudo puerto creado si lo utiliza otro cliente. 3: Cree un número de pseudo puerto. Sin verificación.

Ejemplo

```
> función pseudoctl srv nat 2
  puerto pesudo: obtener hash pseudo puerto + subred.
  búsqueda de pseudo puerto: verifique el pseudo puerto (debe).

> srv nat pseudoctl función 3 puerto pesudo:
  obtener pseudo puerto hash.

> función pseudoctl srv nat 0
  puerto pesudo: obtener hash pseudo puerto + subred.
  búsqueda de pseudo puerto: verifique el pseudo puerto (Auto).
```

Comando Telnet: srv nat RSTTimeout

Este comando se usa para reenviar RST a través de TCP después de un período de tiempo.

Sintaxis

srv nat RSTTimeout*<valor>*

Sintaxis Descripción

Parámetro	Descripción
<valor>	Establezca el valor de tiempo de espera. <valor>: 0 a 10 (una unidad es 10mseg).

Ejemplo

```
> srv nat RSTTimeout 2 Establecer
tiempo de espera 2 unidad

> srv nat RSTTimeout?
%% srv RSTtimeout <valor> (la unidad es 10 mseg). (0<=valor<=10)
---------------------------- ahora
tiempo de espera establecido 2 unidades

>
```

Comando Telnet: cambiar -i

Este comando se utiliza para obtener los datos TX (transmitidos) o RX (recibidos) de cada conmutador conectado.

Sintaxis

cambiar -i*<cambiar idx_no><opción>*

Sintaxis Descripción

Parámetro	Descripción
cambiar idx_no	Significa el número de índice (1 a 8) del perfil del interruptor.
opción	Los comandos disponibles con parámetros se enumeran a continuación. *cmd* *cuenta*

	tráfico <encendido/apagado/estado/tx/rx>
cmd	Significa enviar comando al cliente.
cuenta	Significa configurar la cuenta de autenticación del cliente y la contraseña.
tráfico <encendido/apagado/estado/tx/rx>	Significa encender/apagar o mostrar la transmisión de datos del cliente.

Ejemplo

```
> activa el tráfico -i 1
N° de dispositivo externo 1 función de estadísticas de tráfico está habilitada
>
```

Comando Telnet: estado del interruptor

Este comando se utiliza para comprobar el estado de la detección automática de dispositivos externos.

Ejemplo

```
> estado del interruptor
Estado de detección automática de dispositivos externos: Deshabilitar

Sin respuesta a dispositivo externo: Habilitar
```

Comando Telnet: cambiar not_respond

Este comando se utiliza para detectar el dispositivo externo automáticamente y mostrarlo en esta página.

Sintaxis

cambiar not_respond 0
cambiar not_respond 1

Sintaxis Descripción

Parámetro	Descripción
0	Deshabilite la opción de "No responder a paquetes de dispositivos externos".
1	Habilite la opción de "No responder a paquetes de dispositivos externos".

Ejemplo

```
> cambiar not_respond 1
esclavo no responde!
>
```

Comando Telnet: encender

Este comando se utiliza para activar la detección automática de dispositivos externos.

Ejemplo

```
> encender
¡Habilite la detección automática de dispositivos externos!
```

Comando Telnet: apagar

Este comando se utiliza para desactivar la detección automática de dispositivos externos.

Ejemplo

```
> apagar
¡Desactive la detección automática de dispositivos externos!
```

Comando Telnet: lista de interruptores

Este comando se utiliza para mostrar el estado de conexión del conmutador.

Ejemplo

```
> cambiar lista?
No.  Mac  IP  estado  Tiempo de duración  CWMP  ACS_CTL  Modificación
el_Nombre  versión de firmware
-------------------------------------------------------------------------------
---------------------------------
[1] 00-1d-aa-7c-f5-a4 192.168.1.12  En línea  01:03:57  - 1  - 1
VigorAP1060C, VigorAP1060C
[2] 14-49-bc-41-33-f4  192.168.1.11  En línea  01:03:57  - 1  - 1
G2121
[3] 14-49-bc-43-e5-79  192.168.1.13  En línea  01:03:57  - 1  - 1
G2100
```

Comando Telnet: cambiar claro

Este comando se usa para restablecer la tabla de interruptores y reiniciar el enrutador.

Sintaxis

interruptor claro*<idx>*

Sintaxis Descripción

Parámetro	Descripción
idx	Significa el número de índice de cada elemento que se muestra en la tabla. El rango es de 1 a 8.
- f	Significa borrar todos los datos.

Ejemplo

```
> cambiar claro 1
Cambio de borrado de datos exitoso

> cambiar borrar -f Cambiar datos
borrar con éxito
```

Comando Telnet: cambiar consulta

Este comando se utiliza para habilitar o deshabilitar la consulta de cambio.

Ejemplo

```
> activar la consulta
La consulta de estado del dispositivo externo está habilitada
> desactivar consulta
La consulta de estado del dispositivo externo está deshabilitada
```

Comando Telnet: cambiar syslog

Este comando se usa para habilitar o deshabilitar el syslog del dispositivo externo.

Ejemplo

```
> activar syslog
El estado del dispositivo externo es Habilitar
> apagar syslog
El estado del dispositivo externo es deshabilitado
```

Comando Telnet: administrador del sistema

Este comando se usa para que el ingeniero de RD acceda al modo de prueba del enrutador Vigor.

Comando Telnet: sys adminuser

Este comando se usa para crear una cuenta de usuario y especificar el servidor LDAP. El servidor autenticará al usuario local que desea acceder a la interfaz de usuario web del enrutador Vigor.

Sintaxis

usuario administrador del sistema <*opción*>

sys adminuser editar*<índice> nombre de usuario contraseña*

Sintaxis Descripción

Parámetro	Descripción
opción	Las opciones disponibles incluyen: Local <0-1> LDAP <0-1> editar <ÍNDICE> borrar <ÍNDICE> ver <ÍNDICE>
<0-1> locales	0: deshabilitar el usuario local. 1 – Habilitar el usuario local.
LDAP <0-1>	0: deshabilitar el LDAP. 1 – Habilitar el LDAP.
editar <ÍNDICE> nombre de usuario contraseña	Edite una cuenta de usuario existente o cree una nueva cuenta de usuario local. [ÍNDICE] – 1 ~8. Hay ocho perfiles para agregar/editar. Nombre de usuario: escriba un nuevo nombre para el usuario local. Contraseña: escriba una contraseña para el usuario local.
borrar <ÍNDICE>	Eliminar una cuenta de usuario local.
ver <ÍNDICE>	Muestra la información detallada de la cuenta de usuario/contraseña.

Ejemplo

```
> sys adminuser Local 1 ¡El
usuario local ha habilitado!
> sys adminuser LDAP 1
¡LDAP ha habilitado!
> sys adminuser editar 1 carrie test123
¡Actualizado!
> sys adminuser vista 1

Índice: 1
```

Nombre de usuario: carrie

Contraseña de usuario:
0F1AD8240CF4F7566E75F78B6113E1A8595977BB9A98633C12D8AFBD1F019854

Comando Telnet: placa sys

Este comando se utiliza para deshabilitar/habilitar y configurar el control del panel.

Sintaxis

definición del botón del tablero del sistema *<encendido/apagado>* **botón del tablero del sistema wlan** *<encendido/apagado>* **control de led de la placa del sistema** *<encendido/apagado>* **modo de suspensión LED de la placa del sistema** *<encendido/apagado>* **sys board led sleepMode tiempo** *<minuto>* **placa del sistema usb** *<p1/p2> <activar/desactivar>*

Sintaxis Descripción

Parámetro	Descripción
botón def <activar/desactivar>	El botón de reinicio predeterminado no será válido si lo apaga. Activado: el botón es válido. Desactivado: el botón no es válido.
Botón wlan <activar/desactivar>	El botón inalámbrico no será válido si lo apaga. Activado: el botón es válido. Desactivado: el botón no es válido.
mando led <encendido/apagado>	Todos los LED del panel frontal no serán válidos si se apagan. Encendido: los LED son válidos. Apagado: los LED no son válidos.
led modo dormir <encendido/apagado>	Todos los LED del panel frontal se configurarán en modo de suspensión. Activado: el modo de suspensión está activado. Desactivado: el modo de suspensión está desactivado. Si el modo de suspensión está activado, presione el "botón inalámbrico" y el "botón de reinicio de fábrica" para encender el LED (incluso los botones están desactivados).
tiempo de modo de sueño led <minutos>	Después de habilitar el modo de suspensión para todos los LED, se dormirán después de los minutos configurados aquí. Minutos: Introduzca el número de la hora.
usb <p1/p2> <encendido/apagado>	El puerto USB no será válido si lo apaga. Activado: el puerto es válido. Apagado: el puerto no es válido.

Ejemplo

```
> sys board led sleepMode on LEDs
  Sleep Mode is on now.

> sys board led sleepMode time 10 Sleep Countdown
  Time establecido en 10 minutos. Restablecer el éxito del
  temporizador de sueño LED ..
```

Comando Telnet: sys bonjour

Este comando se usa para deshabilitar/habilitar y configurar el servicio Bonjour.

Sintaxis

sistema bonjour*[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
- e <habilitar>	Se utiliza para deshabilitar/habilitar el servicio bonjour (0: deshabilitar, 1: habilitar).
- h <habilitar>	Se utiliza para deshabilitar/habilitar el servicio http (web) (0: deshabilitar, 1: habilitar).
- t <habilitar>	Se utiliza para deshabilitar/habilitar el servicio telnet (0: deshabilitar, 1: habilitar).
- f <habilitar>	Se utiliza para deshabilitar/habilitar el servicio FTP (0: deshabilitar, 1: habilitar).
- s <habilitar>	Se utiliza para deshabilitar/habilitar el servicio SSH (0: deshabilitar, 1: habilitar).
- p <habilitar>	Se utiliza para deshabilitar/habilitar el servicio de impresora (0: deshabilitar, 1: habilitar).
- 6 <habilitar>	Se utiliza para deshabilitar/habilitar IPv6 (0: deshabilitar, 1: habilitar).

Ejemplo

```
> sys bonjour -s 1
>
```

Comando Telnet: sys cfg

Este comando restablece el enrutador con la configuración predeterminada de fábrica. Cuando un usuario escribe este comando, toda la configuración se restablecerá a la configuración predeterminada.

Sintaxis

sys cfg por defecto

estado del cfg del sistema

Sintaxis Descripción

Parámetro	Descripción
por defecto	Significa restablecer la configuración actual con los valores predeterminados.
estado	Significa mostrar la versión y el estado del perfil actual.

Ejemplo

```
> sys cfg status Versión del
perfil: 3.0.0                    Estado: 1 (0x491e5e6c)
> sys cfg por defecto
>
```

Comando Telnet: sys cmdlog

Este comando muestra el historial de los comandos que ha escrito.

Ejemplo

```
> registro de cmd del sistema
% Registro de comandos: (¡El índice más bajo es el más nuevo!)
    [1] registro de cmd del sistema
    [2] registro de cmd del sistema?
    [3] sistema?
    [4] estado de cfg del sistema
    [5] sys cfg?
```

Comando Telnet: sys ftpd

Este comando muestra el estado actual del servidor FTP.

Sintaxis

sistema ftpd*en*

sistema ftpd*apagado*

Sintaxis Descripción

Parámetro	Descripción
en	Significa encender el servidor FTP del sistema.
apagado	Significa apagar el servidor FTP del sistema.

Ejemplo

```
> sistema ftpd en
% sys ftpd encienda !!!
```

Comando Telnet: nombre de dominio sys

Este comando puede establecer y eliminar el nombre de dominio del sistema cuando se selecciona el modo DHCP para WAN.

Sintaxis

nombre de dominio del sistema*<wan1/wan2> <Sufijo de nombre de dominio>*

nombre de dominio del sistema*<wan1/wan2> claro*

Sintaxis Descripción

Parámetro	Descripción
wan1/wan2	Significa especificar la interfaz WAN para asignarle un nombre.
Sufijo de nombre de dominio	Significa el nombre del dominio del sistema. El número máximo de caracteres que puede establecer es 39.
claro	Significa eliminar el nombre de dominio del sistema.

Ejemplo

```
> sys nombre de dominio wan1 inteligente
> sys nombre de dominio wan2 inteligente
> sys nombre de dominio?
% sys nombre de dominio <wan1/wan2> <Sufijo de nombre de dominio (máx. 39 caracteres)> % sys
nombre de dominio <wan1/wan2> borrar
% Ahora: wan1 == listo, wan2 ==inteligente
>
```

Comando Telnet: sys iface

Este comando muestra el estado actual de la conexión de la interfaz (ARRIBA o Abajo) con la dirección IP, la dirección MAC y la máscara de red del enrutador.

Ejemplo

```
> iface del sistema
Interfaz 0Ethernet:
Estado: ARRIBA
Dirección IP: 192.168.1.1          Máscara de red: 0xFFFFFF00 (Privado)
```

```
Dirección IP: 0.0.0.0                Máscara de red: 0xFFFFFFFF
MAC: 00-50-7F-00-00-00
Interfaz 4Ethernet:
Estado: ABAJO
Dirección IP: 0.0.0.0                Máscara de red: 0x00000000
MAC: 00-50-7F-00-00-02
Interfaz 5Ethernet:
Estado: ABAJO
Dirección IP: 0.0.0.0                Máscara de red: 0x00000000
MAC: 00-50-7F-00-00-03
Interfaz 6Ethernet:
Estado: ABAJO
Dirección IP: 0.0.0.0                Máscara de red: 0x00000000
MAC: 00-50-7F-00-00-04
Interfaz 7Ethernet:
Estado: ABAJO
Dirección IP: 0.0.0.0                Máscara de red: 0x00000000
MAC: 00-50-7F-00-00-05
Interfaz 8Ethernet:
Estado: ABAJO
Dirección IP: 0.0.0.0                Máscara de red: 0x00000000
MAC: 00-50-7F-00-00-06

Interfaz 9Ethernet:
Estado: ABAJO
Dirección IP: 0.0.0.0                Máscara de red: 0x00000000
MAC: 00-50-7F-00-00-07
- - - MÁS --- ['q': Salir, 'Entrar': Líneas nuevas, 'Barra espaciadora': Página siguiente] ---
>
```

Comando Telnet: nombre del sistema

Este comando puede establecer y eliminar el nombre del enrutador cuando se selecciona el modo DHCP para WAN.

Sintaxis

nombre del sistema *<wan1/wan2> <cadena ASCII>*

nombre del sistema *<wan1/wan2>* **claro**

Sintaxis Descripción

Parámetro	Descripción
<wan1/wan2>	Significa especificar la interfaz WAN para asignarle un nombre.
cadena ASCII	Significa el nombre del enrutador. El carácter máximo que puede establecer es 39.

Ejemplo

```
> nombre del sistema wan1 drayrouter
> nombre del sistema?
% nombre del sistema <wan1/wan2> <cadena ASCII (máx. 39 caracteres)> %
nombre del sistema <wan1/wan2> borrar
% Ahora: wan1 == drayrouter, wan2 ==
```

Nota:*Dicho nombre se puede utilizar para reconocer la identificación del enrutador en el cuadro de diálogo SysLog.*

Comando Telnet: sys passwd

Este comando permite a los usuarios establecer una contraseña para el administrador.

contraseña del sistema*<contraseña antigua> <contraseña nueva>*

Sintaxis Descripción

Parámetro	Descripción
Contraseña anterior	Ingrese la contraseña anterior.
Nueva contraseña	Ingrese una cadena como la nueva contraseña para el administrador. El carácter máximo que puede establecer es 83.

Ejemplo

```
> sys passwd admin admin123 ¡Cambio
de contraseña exitoso!
>
```

Comando Telnet: reinicio del sistema

Este comando permite a los usuarios reiniciar el enrutador inmediatamente.

Ejemplo

```
> reinicio del sistema

>
```

Comando Telnet: reinicio automático del sistema

Este comando permite a los usuarios reiniciar el enrutador automáticamente dentro de un tiempo determinado.

Sintaxis

reinicio automático del sistema*<encendido/apagado/hora(s)>*

Sintaxis Descripción

Parámetro	Descripción
encendido apagado	Encendido: significa habilitar la función de reinicio automático. Apagado: significa desactivar la función de reinicio automático.
horas	Significa establecer el horario para el reinicio del enrutador. Por ejemplo, si escribe "2" en este campo, el enrutador se reiniciará con un**intervalo**de dos horas.

Ejemplo

```
> sys autoreboot en
  autoreboot está activado
> sys autoreboot 2
  autoreboot está activado
  el tiempo de reinicio automático es de 2 hora(s)
```

Comando Telnet: confirmación del sistema

Este comando permite a los usuarios guardar la configuración actual en FLASH. Por lo general, la configuración actual se guardará en SRAM. Sin embargo, este comando guardará el archivo en FLASH.

Ejemplo

```
> confirmación del sistema
```

```
>
```

Comando Telnet: sys tftpd

Este comando puede activar el servidor TFTP para actualizar el firmware.

Ejemplo

```
> sistema tftpd
% servidor TFTP habilitado !!!
```

Comando Telnet: sys cc

Este comando puede mostrar el código de país actual y la región inalámbrica de este dispositivo.

Ejemplo

```
> sistema cc
Código de país              : 0x 0 [Internacional]
Código de región inalámbrica: 0x30
>
```

Comando Telnet: versión sys

Este comando puede mostrar la versión actual del sistema.

Ejemplo

```
> versión del sistema
Modelo de enrutador: Vigor2927Vac        Versión: 4.4.0 Inglés
Versión del perfil: 4.0.0                Estado: 1 (0x9de81d8f)
IP del enrutador: 192.168.1.1            Máscara de red: 255.255.255.0
Fecha y hora de compilación del firmware: 19 de abril de 2022 15:48:29
Nombre del enrutador: DrayTek
Revisión: 3075_6ffc5c5drayos2015_V2927_440
Número de serie del enrutador: Ninguno
>
```

Comando Telnet: sys qrybuf

Este comando puede mostrar el estado de la memoria del sistema y la lista de fugas.

Ejemplo

```
> sistema qrybuf
Estado de la memoria del sistema y lista de fugas

Buf sk_buff       (200B), n.° usado: 1647, n.° en caché:       30
Buf KMC4088       (4088B), n.° usado: 0, n.° en caché:         8
Buf KMC2552       (2552B), n.° usado: 1641, n.° en caché:      42
Buf KMC1016       (1016B), n.° usado:       7, en caché #:     1
Buf KMC504        (504B), usado#:           8, en caché #:     8
Buf KMC248        (248B), usado#:          26, en caché #:    22
Buf KMC120        (120B), usado#:          67, en caché #:    61
Buf KMC56         (56B), usado #:          20, en caché #:    44
```

Buf KMC24 (24B), usado #: 58, caché #: 70
Memoria dinámica: 13107200B; 4573168B usado; 190480B/0B en caché de nivel 1/2.

Estado de la memoria FLOWTRACK
de gratis = 12000
de máximo = 0
de estado de flujo = 12000
de perdidas por firma = 0
de perdidos por lista = 0

Comando Telnet: sys pollbuf

Este comando puede activar o desactivar el búfer de sondeo para el enrutador.

Sintaxis

sondeo del sistema*<encendido/apagado>*

Sintaxis Descripción

Parámetro	Descripción
en	Significa activar el búfer de extracción.
apagado	Significa desactivar el búfer de extracción.

Ejemplo

> sondeo del sistema activado
¡El sondeo de % de búfer está activado!

> encuesta del sistema desactivada
¡El sondeo de % de búfer está desactivado!

Comando Telnet: sys britask

Este comando puede mejorar la calidad del triple play.

Sintaxis

sistema británico*<encendido/apagado>*

Sintaxis Descripción

Parámetro	Descripción
en	Significa activar la tarea del puente para mejorar la calidad del triple play.
apagado	Significa apagar la tarea del puente.

Ejemplo

> sistema britask en
% de la tarea de puente está ACTIVADA, ahora

Comando Telnet: sys tr069

Este comando puede establecer la configuración de CPE para aplicar en VigorACS.

Sintaxis

sistema tr069 obtener *<parm> <opción>*

sistema tr069 conjunto *<parámetro>*

<valor> **sys tr069 getnoti** *<Parm>*

sys tr069 setnoti *<parámetro> <valor>* **registro**

del sistema tr069

depuración del sistema tr069 *<encendido/*

apagado> **sistema tr069 guardar**

sys tr069 informar *<código de evento>* **puerto**

del sistema tr069 *<número de puerto>* **sys tr069**

cert_auth *<activar/desactivar>*

sys tr069 only_standard_parm *<encendido/apagado>*

sys tr069 notificar -S

sys tr069 notificar -n *<encendido/apagado>*

sys tr069 notificar -l *<encendido/apagado>*

sys tr069 notificar -c *<encendido/apagado>*

sys tr069 notificar -b *<encendido/apagado>*

sys tr069 notificar -B *"<Número de WAN> <Umbral medio> <Umbral alto> <Velocidad de TX>Mb <Velocidad de RX>Mb"*

Sintaxis Descripción

Parámetro	Descripción
obtener <parámetro> <opción>	Significa obtener parámetros para tr-069. option=<nextlevel>: solo obtiene el siguiente nivel para GetParameterNames.
establecer <parámetro> <valor>	Significa establecer parámetros para tr-069.
getnoti <parám>	Significa obtener el valor de notificación del parámetro.
setnoti <parámetro> <valor>	Significa establecer el valor de notificación del parámetro.
registro	Significa mostrar el registro TR-069.
depurar <activar/desactivar>	on: activa la función de enviar un mensaje de depuración a syslog. off: apaga la función de enviar un mensaje de depuración a syslog.
ahorrar	Significa guardar los parámetros en la memoria flash del enrutador.
Informar <código de evento>	Significa informar parámetros para tr069 con diferentes códigos de evento. [código de evento] incluye: 0-"0 INICIO", 1-"1 BOTA", 2- "2 PERIÓDICOS", 3- “3 PROGRAMADOS”, 4-"4 CAMBIO DE VALOR", 5- "5 PATADAS", 6- “6 SOLICITUD DE CONEXIÓN”, 7- “7 TRANSFERENCIA COMPLETA”, 8- “8 DIAGNÓSTICO COMPLETO”, 9- “M Reiniciar”
puerto <número de puerto>	Significa cambiar el número de puerto de escucha tr069.
cert_auth <activar/desactivar>	on: activa la autenticación basada en certificados. off: desactiva la autenticación basada en certificados.
only_standard_parm	Significa activar o desactivar para excluir todos los proveedores específicos ("X_")

<activar/desactivar>	parámetros, y solo envía parámetros estándar.
notificar -n <activar/desactivar>	Significa establecer la configuración de notificación de CPE. Significa registrar/no registrar el registro de notificación de CPE en Syslog. on: Registro en el Syslog. off: No grabar en el Syslog.
notificar -i <activar/desactivar>	Significa registrar/no registrar el registro de inicio de sesión web en Syslog. on: Registro en el Syslog. off: No grabar en el Syslog.
notificar -c <activar/desactivar>	Significa registrar/no registrar el registro de cambios web en Syslog. on: Registro en el Syslog. off: No grabar en el Syslog.
notificar -h <activar/desactivar>	Significa registrar/no registrar el registro de alta disponibilidad en Syslog. on: Registro en el Syslog. off: No grabar en el Syslog.
notificar -b [activar/desactivar]	Significa registrar/no registrar el registro de utilización del ancho de banda en Syslog. on: Registro en el Syslog. off: No grabar en el Syslog.
notificar -B "<Número de WAN> <Umbral medio> <Umbral alto> <Velocidad de TX>Mb <Velocidad de RX>Mb"	Significa establecer la configuración de utilización del ancho de banda. <Número WAN>: Ingrese el número de índice de las interfaces WAN. <Umbral medio>: Introduzca un valor. <Umbral alto>: Introduzca un valor. <Velocidad TX>Mb: Introduzca un valor. <Velocidad RX>Mb: Introduzca un valor.
- S	Muestra la configuración de notificaciones de CPE.

Ejemplo

```
> sys tr069 obtener Int. nextlevel El número total de
parámetros es 24 La longitud total del contenido del
parámetro es 915
InternetGatewayDevice.LANDeviceNumberOfEntries
InternetGatewayDevice.WANDeviceNumberOfEntries
InternetGatewayDevice.DeviceInfo.
InternetGatewayDevice.ManagementServer.
InternetGatewayDispositivo.Tiempo.
InternetGatewayDevice.Layer3Forwarding.
InternetGatewayDevice.LANDevice. Dispositivo de
puerta de enlace de Internet. Dispositivo WAN.
InternetGatewayDevice.Services.
InternetGatewayDevice.X_00507F_InternetAcc. Dispositivo de
puerta de enlace de Internet.X_00507F_LAN. Dispositivo de
puerta de enlace de Internet.X_00507F_NAT. Dispositivo de
puerta de enlace de Internet.X_00507F_Firewall.
InternetGatewayDevice.X_00507F_Bandwidth.
InternetGatewayDevice.X_00507F_Aplicaciones. Dispositivo de
puerta de enlace de Internet.X_00507F_VPN.
Dispositivo de puerta de enlace de Internet.X_00507F_VoIP.
InternetGatewayDevice.X_00507F_WirelessLAN.
InternetGatewayDevice.X_00507F_System. Dispositivo de
puerta de enlace de Internet.X_00507F_Estado.

InternetGatewayDevice.X_00507F_Diagnóstico.
```

```
- - - MÁS --- ['q': Salir, 'Entrar': Líneas nuevas, 'Barra espaciadora': Página siguiente] ---
. .
> sys tr069 notificar -B "1 30 60 100 100"
Habilite el registro de notificación de uso de ancho de banda.
> sys tr069 notificar -n en
> sys tr069 notificar -b en Establecer
Aceptar
> sys tr069 notificar -B "1 30 60 100 100"
> sys tr069 notificar -S Configuración
de notificación de CPE:
  Notificar CPE                 Permitir
  - Inicio de sesión web        Desactivar
  - Web cambiada                Desactivar
  - Alta disponibilidad         Desactivar
  - Utilización de ancho de banda  Permitir

          Límite(%)          Velocidad (Mb)
  WAN1 Media: 0 Alta:   60TX:     0 RX:     0
  WAN2 Media: 0 Alto:    0 TX:    0 RX:     0
  WAN3 Med:   0 Alto:    0 TX:    0 RX:     0
  WAN4 Med:   0 Alto:    0 TX:    0 RX:     0
  WAN5 Med:   0 Alto:    0 TX:    0 RX:     0
  WAN6 Med:   0 Alto:    0 TX:    0 RX:     0
```

Comando Telnet: sys alg

Este comando puede habilitar o deshabilitar el interruptor maestro ALG (Application Layer Gateway).

Sintaxis

alg del sistema*<1/0>*

Sintaxis Descripción

Parámetro	Descripción
1	Significa habilitar el interruptor maestro ALG.
0	Significa desactivar el interruptor maestro ALG.

Ejemplo

```
> alg del sistema -e 1
  Habilitar ALG

> alg del sistema
Uso: sys alg <comando> <parámetro>
  - e: habilitar ALG (0: deshabilitar, 1: habilitar)

Estado actual de ALG
  - Interruptor maestro ALG: Habilitado
```

Comando Telnet: sys sip_alg

Este comando puede activar/desactivar SIP ALG (Puerta de enlace de capa de aplicación) para el cruce.

Sintaxis

sistema sip_alg*<comando> <parámetro>|...*

Sintaxis Descripción

Parámetro	Descripción
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]* significa que puede escribir varios comandos en una línea.
- mi <0/1>	0: Deshabilitar la función de SIP ALG. 1: Habilite la función de SIP ALG.
- p <parámetro>	Significa configurar el puerto de escucha para SIP ALG. <parámetro> : Va de 1 a 65535.
- tu	Significa habilitar o deshabilitar la escucha a lo largo de la configuración de la ruta UDP. 0: Deshabilitar 1: Habilitar
- t	Significa habilitar o deshabilitar la escucha a lo largo de la configuración de la ruta TCP. 0: Deshabilitar 1: Habilitar

Ejemplo

```
> sys sip_alg -e 1
  Habilitar SIP ALG
> sys sip_alg -p 65535 Puerto de escucha
  actual: 65535
> sistema sip_alg?
Uso: sys sip_alg <comando> <parámetro>
  - e: habilitar SIP ALG (0: deshabilitar, 1: habilitar)
  - p: configure su puerto de escucha para SIP ALG
  - u: habilitar escuchar a lo largo de la ruta UDP (0: deshabilitar, 1: habilitar)
  - t: habilitar escuchar a lo largo de la ruta TCP (0: deshabilitar, 1: habilitar)

Estado actual de SIP ALG
  - Interruptor maestro ALG: Habilitado
  - SIP ALG: Habilitado
  - Escuchar a lo largo de la ruta UDP: Sí
  - Escuchar a lo largo de la ruta TCP: Sí
  - Puerto de escucha: 65535
  - Max sipalg número de sesión: 512
  - Permanecer sipalg sesión num: 512
```

Comando Telnet: sys rtsp_alg

Este comando puede activar/desactivar RTSP ALG (Puerta de enlace de capa de aplicación) para el cruce.

Sintaxis

sistema rtsp_alg*[<comando> <parámetro>|...]*

Sintaxis Descripción

Parámetro	Descripción
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]* significa que puede escribir varios comandos en una línea.
- mi <0/1>	0: deshabilitar la función de RTSP ALG. 1: Habilite la función de RTSP ALG.
- p <parámetro>	Significa configurar el puerto de escucha para RTSP ALG. <parámetro> : Va de 1 a 65535.

- tu	Significa habilitar o deshabilitar la escucha a lo largo de la configuración de la ruta UDP. 0: Deshabilitar 1: Habilitar
- t	Significa habilitar o deshabilitar la escucha a lo largo de la configuración de la ruta TCP. 0: Deshabilitar 1: Habilitar
-v	Muestra información de mapas de puertos RTP y RTCP de RTSP ALG.

Ejemplo

```
> sys rtsp_alg -e 1
  Habilitar RTSP ALG

> sys rtsp_alg -p 60000 Puerto RTSP de escucha
  actual: 60000

> sys rtsp_alg-v
  PortMap abierto actual Número de RTSP ALG: 0

> sistema rtsp_alg?
Uso: sys rtsp_alg <comando> <parámetro>
  - e: habilitar RTSP ALG (0: deshabilitar, 1: habilitar)
  - p: configure su puerto de escucha para RTSP ALG
  - u: habilitar escuchar a lo largo de la ruta UDP (0: deshabilitar, 1: habilitar)
  - t: habilitar escuchar a lo largo de la ruta TCP (0: deshabilitar, 1: habilitar)
  - v: muestra la información del mapa de puertos rtp y rtcp de RTSP ALG

Estado actual de RTSP ALG
  - Interruptor maestro ALG: Habilitado
  - ALG RTSP: Habilitado
  - Escuchar a lo largo de la ruta UDP: Sí
  - Escuchar a lo largo de la ruta TCP: Sí
  - Puerto de escucha: 60000
  - Max RTSP número de sesión: 256
  - Permanecer número de sesión RTSP: 256
```

Comando Telnet: licencia sys

Este comando puede procesar la licencia del sistema.

Sintaxis

licencia de sistema*reset_regser*

licencia de sistema*licera*

licencia de sistema*licifno <AUTO/WAN#>*

licencia de sistema*licalias <índice>* **licencia**

de sistema*lic_trigger* **licencia de sistema**

piojos

sistema lic_https*establecer <0/1>*

Sintaxis Descripción

Parámetro	Descripción
reset_regser	Significa la configuración del servidor de registro de licencias o el servicio de registro en

	portal.
licera	Significa borrar la configuración de la licencia.
licifno <AUTO/WAN#>	Significa configuración de interfaz de descarga de licencia y firma.
licalias <índice>	Significa especificar un alias de IP ingresando el número de índice del perfil de alias de IP.
lic_trigger	Significa activar la licencia.
piojos	Significa mostrar el registro de autenticación.
lic_https conjunto <0/1>	0: establezca el tipo de conexión de lic en HTTP. 1 - Establezca el tipo de conexión lic en HTTPs.

Ejemplo

```
> sys licencia licifno wan3
La interfaz de descarga está configurada como "WAN3" ahora.
>
```

Comando Telnet: sys diag_log

Este comando se usa para la depuración de RD.

Sintaxis

sys diag_log*<estado| habilitar| deshabilitar| al ras| lino <w> | nivel <x> | característica <on|off><y>| voip_feature <on|off> <vf_name>| registro>*

Sintaxis Descripción

Parámetro	Descripción
estado	Significa mostrar el estado del registro de diagnóstico.
permitir	Significa habilitar la función de diag_log.
desactivar	Significa deshabilitar la función de diag_log.
enjuagar	Significa el búfer de registro de descarga.
lino <w>	Significa el total de líneas para mostrar el mensaje. w - El valor disponible varía de 100 a 50000.
nivel<x>	Determina el nivel de datos mostrados. x: el valor disponible varía de 0 a 12. Cuanto mayor es el número, más detallados se muestran los datos.
función <activar/desactivar> <y>	Se utiliza para especificar la función del registro. Las funciones admitidas incluyen SYS, VoIP y EthOAM.
función_voip <activar/desactivar> <vf_nombre>	Significa función de VoIP. Escriba on para habilitar la función o escriba off para deshabilitarla. vf_name: las configuraciones disponibles incluyen DRVTAPI, DRVVMMC, DRVMPS, DRVFXO, DRVHAL, PSMPHONE, PSMSUPP, PSM, FXO, PSMISDN, DTMFPSER, CALLERID (sin distinción entre mayúsculas y minúsculas).
registro	Significa el búfer de registro de volcado.

Ejemplo

```
> estado del sistema diag_log
Estado:
  diag_log está deshabilitado.
  linono : 10000.
  nivel 3.
```

```
  Característica habilitada: SYS
> sys diag_log registro
   0:00:02      [DSL] Firmware actual del módem: AnnexA_548006_544401 [DSL]
0:00:02         Característica del firmware del módem: 5, ADSL_A, VDSL2 [DSL]
0:00:02         xtseCfg=04 00 04 00 0c 01 00 07
0:00:02         ¡[DSL] no tiene el último modo showtime! ¡establezca el siguiente modo en VDSL!
0:00:02         [DSL] El estado ha cambiado: Detenido (0) -> FwWait (3)
0:00:02         [DSL] El estado ha cambiado: FwWait(3) -> Inicio(1) [DSL] El estado ha
0:00:02         cambiado: Inicio(1) -> Ejecutándose(2) [DSL] El estado ha cambiado:
0:00:02         firmwareReady(3) a Init(5)
```

Comando Telnet: sys arp_AutoReq

Este comando se usa para habilitar/deshabilitar la función de que el enrutador Vigor envíe solicitudes ARP a los dispositivos conectados periódicamente.

Sintaxis

sys arp_AutoReq-d *<valor>*

Sintaxis Descripción

Parámetro	Descripción
- d [valor]	Deshabilite la función de solicitud automática de ARP. 0 – Habilitar 1 – Deshabilitar

Ejemplo

```
> sys arp_AutoReq -d 1 Arp solicitud
   automática deshabilitada.
>
```

Comando Telnet: sys ahorro de luz del día

Este comando se usa para conifgurar el horario de verano.

Sintaxis

ahorro de luz del sistema *[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
[<comando><parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]* significa que puede escribir varios comandos en una línea.
-v	Muestra la configuración de ahorro de luz diurna.
-r	Establecido en la configuración predeterminada de fábrica.
- mi <1/0>	Habilitar (1) / deshabilitar (0) el horario de verano.
- t <0/1/2>	Especifique el tipo de ahorro para la configuración de luz diurna. 0 – Predeterminado 1 – Rango de tiempo 2 - Anual
- s <año> <mes> <día> <hora>	Establezca la configuración detallada del día de inicio para el tipo de intervalo de tiempo. año: debe ser el año posterior a 2013. mes - 1 ~ 12

	día – 1 ~ 31 hora – 0 ~ 23 por ejemplo, sys ahorro de luz del día -s 2014 3 10 12
- d <año> <mes> <día> <hora>	Establezca la configuración detallada del día de finalización para el tipo de intervalo de tiempo. año – Después de 2013. mes - 1 ~ 12 día – 1 ~ 31 hora – 0 ~ 23 por ejemplo, sys ahorro de luz del día -d 2014 9 10 12
- y <mes> <día de la semana> <día de la semana> <hora>	Establezca la configuración detallada del día de inicio para el tipo anual. mes - 1 ~ 12 th día de la semana – 1 ~ 5, 9: última semana día de la semana - 0:domingo, 1:lunes, 2:martes, 3:miércoles, 4:jueves, 5:viernes, 6:sábado hora – 0 ~ 23 por ejemplo, sys ahorro de luz del día -y 9 1 0 14
- z <mes> <día de la semana> <día de la semana> <hora>	Establezca la configuración detallada del día de finalización para el tipo anual. mes - 1 ~ 12 th día de la semana – 1 ~ 5, 9: última semana día de la semana - 0:domingo, 1:lunes, 2:martes, 3:miércoles, 4:jueves, 5:viernes, 6:sábado hora – 0 ~ 23 por ejemplo, sys ahorro de luz del día -z 3 1 6 14

Ejemplo

```
> sys de ahorro de luz del día -y 9 1 0 14 % Comienzo:
Anualmente el 1 de septiembre Domingo 14:00
```

Comando Telnet: sys dnsCacheTbl

Este comando se utiliza para configurar los ajustes de TTL que se mostrarán en la tabla de caché de DNS.

Sintaxis

sys dnsCacheTbl*[<comando><parámetro>|...]*

Sintaxis Descripción

Parámetro	Descripción
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]* significa que puede escribir varios comandos en una línea.
- yo	Significa mostrar la entrada DNS IPv4 en la tabla de caché de DNS.
- s	Significa mostrar la entrada DNS IPv6 en la tabla de caché de DNS.
-v	Significa mostrar el valor límite de TTL en la tabla de caché de DNS.
- t <ttl>	Significa establecer el valor límite TTL. <ttl>: 0 (sin límite) o un número mayor que 5.
- C	Significa borrar la tabla de caché de DNS.

Ejemplo

```
> sys dnsCacheTbl -t 50
> % Establecer límite TTL: 50 segundos.
% Cuando el TTL sea superior a 50 s, elimine la entrada de DNS en la memoria caché de DNS del enrutador
```

```
mesa
mi.
> sys dnsCacheTbl -v % límite
TTL: 50 segundos
% Cuando el TTL sea mayor de 50 s, elimine la entrada de DNS en la tabla de caché de DNS del enrutador
```

Comando Telnet: sys syslog

Este comando se usa para conifgurar el horario de verano.

Sintaxis

registro del sistema del sistema*-a <habilitar> [-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
[<comando><parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]* significa que puede escribir varios comandos en una línea.
- un <1/0>	Habilite (1) o deshabilite (0) la configuración de acceso a Syslog.
-s <1/0>	Habilite (1) o deshabilite (0) Syslog Save to Syslog Server.
- i <dirección IP>	Defina la dirección IP del servidor Syslog.
- d <número de puerto>	Defina el número de puerto (1 ~ 65535) como el puerto de destino.
- tu <1/0>	Habilite (1) o deshabilite (0) Syslog Save to USB Disk.
- m<1/0>	Habilitar (1) o deshabilitar (0) Mail Syslog.
-f<1/0>	Habilite (1) o deshabilite (0) el registro de Filewall.
-v <1/0>	Habilite (1) o deshabilite (0) el registro de VPN.
- mi <1/0>	Habilite (1) o deshabilite (0) el registro de acceso de usuario.
-c<1/0>	Habilite (1) o deshabilite (0) el registro de llamadas.
- w <1/0>	Habilite (1) o deshabilite (0) el registro WAN.
- yo <1/0>	Habilite (1) o deshabilite (0) el registro WLAN.
-r <1/0>	Habilite (1) o deshabilite (0) la información del enrutador/DSL.
- pag	Actualice la dirección IP del servidor.
- W <1/0>	Configure el modo para escribir Syslog. 0: sobrescribir los registros más antiguos; 1: detener el registro.
-Tú <1/0>	Configure la unidad para el Syslog guardado en un disco USB. 0: GB; 1 MB
- S <capacidad>	Configure la capacidad de la carpeta para el syslog guardado en el disco USB. 1 ~ 16 (GB); 1 ~1024(MB)

Ejemplo

```
> sys syslog -a 1 -s 1 -i 192.168.1.25 -d 514
>
```

Comando Telnet: sys mailalert

Este comando se utiliza para configurar los ajustes de la alerta de correo de syslog.

Sintaxis

alerta de correo del sistema*[-<comando> <parámetro>]*

Sintaxis Descripción

Parámetro	Descripción
[<comando><parámetro>]	Los comandos disponibles con parámetros se enumeran a continuación.
- mi <0/1>	Activar/desactivar Alerta de correo. 0 – Deshabilitar. 1 – Habilitar.
- w <0/1/2/...>	Establecer interfaz (física) Cualquiera/WAN1/WAN2/WAN... y etc.
- x <Índice de alias de IP de WAN>	Establezca el alias de IP de WAN. El índice 1 está reservado y primero debe establecer una interfaz.
- i <IP del servidor SMTP>	Establezca la dirección IP para el servidor SMTP.
- o <Puerto del servidor SMTP>	Establezca el número de puerto para el servidor SMTP..
- una <Dirección de correo>	Establezca la dirección de correo electrónico para el receptor de correo de alerta.
- r <Dirección de correo>	Establezca la dirección de correo electrónico para la devolución de correo.
-s <0/1/2/3>	Establecer seguridad de conexión 0 - Texto sin formato 1 - SSL 2 - Iniciar TLS 3 - Forzar inicio TLS
- h<0/1>	Habilitar/deshabilitar la autenticación SMTP. 0 – Deshabilitar. 1 – Habilitar.
- u <Nombre de usuario>	Establezca el nombre de usuario para la autenticación SMTP.
- p <Contraseña>	Establezca la contraseña para la autenticación SMTP.
- l <tipo><0/1>	Activar/desactivar alerta de correo para diferentes tipos. Los números 0 ~ 6 representan diferentes tipos. "0 <0/1>" : habilitar/deshabilitar la alerta de correo del ataque DoS. : "1 <0/1>" habilitar/deshabilitar la alerta de correo de la APPE. "2 <0/1>" : habilita/deshabilita la alerta de correo del registro de VPN. "3 <0/1>" : habilitar/deshabilitar la alerta de correo de la firma APPE. : habilitar/ "6 <0/1>" deshabilitar la alerta de correo del registro de depuración de reinicio. En el cual, 0 – Deshabilitar. 1 – Habilitar.
- f	Restablezca la configuración de Alerta de correo a los valores predeterminados de fábrica.
-v	Muestra la configuración actual de Alerta de correo.
- D <0/1>	Establezca el modo de registro de depuración de reinicio de alerta de correo. 0: modo limitado 1: Modo ilimitado.

Ejemplo

> sys mailalert -e 1 Configure
Habilitar alerta de correo.
> alerta de correo del sistema -v
- - - - - - Configuración actual para Mail Alert ------ Mail Alert:
Habilitar
Dirección IP del servidor SMTP: 0.0.0.0
Puerto del servidor SMTP: 25
Dirección de correo electrónico del receptor de correo de alerta:
Dirección de correo electrónico de devolución de correo:
Usar SSL: Deshabilitar
Autenticación SMTP: Deshabilitar Nombre de usuario para autenticación SMTP: Contraseña para autenticación SMTP: Alerta de correo para ataque DoS: Habilitar.

Alerta de correo para APPE: Habilitar. Alerta de correo para el registro de VPN: Habilitar. Alerta de correo para la firma APPE: deshabilitar.
Alerta de correo para reiniciar el registro de depuración: Deshabilitar, Modo: Limitado.
- -

Comando Telnet: hora del sistema

Este comando se utiliza para configurar la hora y la fecha del sistema.

Sintaxis

servidor de tiempo del sistema *<dominio>*

consulta de tiempo del sistema

espectáculo de tiempo del sistema

tiempo del sistema wan *<opción>* **zona**

horaria del sistema *<índice>* **tiempo**

del sistema pseudo

Sintaxis Descripción

Parámetro	Descripción
servidor <dominio>	Introduzca el nombre de dominio del servidor horario. <dominio>: la longitud máxima es de 39 caracteres.
preguntar	Obtenga la hora según la configuración del servidor del temporizador.
espectáculo	Muestra la configuración actual del servidor.
wan <opción>	Configure la interfaz WAN. 0 - Automático 1 - WAN1 2 - WAN2 3 - WAN3 4 - WAN4 5 - WAN5 6 - WAN6
zona <índice>	Un número diferente significa una zona horaria diferente. 1 - GMT-12:00 Eniwetok, Kwajalein 2 - GMT-11:00 Isla Midway, Samoa 3 - GMT-10:00 Hawái 4 - GMT-09:00 Alaska 5 - GMT-08:00 Hora del Pacífico (EE. UU. y Canadá) 6 - GMT-08:00 Tijuana 7 - GMT-07:00 Hora de la montaña (EE. UU. y Canadá) 8 - GMT-07:00 Arizona 9 - GMT-06:00 Hora central (EE. UU. y Canadá) 10 - GMT-06:00 Saskatchewan 11 - GMT-06:00 Ciudad de México, Tegucigalpa 12 - GMT-05:00 Hora del Este (EE. UU. y Canadá) 13 - GMT-05:00 Indiana (Este) 14 - GMT-05:00 Bogotá, Lima, Quito 15 - GMT-04:00 Hora del Atlántico (Canadá) 16 - GMT-04:00 Caracas, La Paz 17 - GMT-04:00 Santiago 18 - GMT-03:30 Terranova 19 - GMT-03:00 Brasilia 20 - GMT-03:00 Buenos Aires, Georgetown

	21 - GMT-02:00 Medio Atlántico 22 - GMT-01:00 Azores, Islas de Cabo Verde. 23 - GMT Hora media de Greenwich: Dublín 24 - GMT Edimburgo, Lisboa, Londres 25 - GMT Casablanca, Monrovia 26 - GMT+01:00 Belgrado, Bratislava 27 - GMT+01:00 Budapest, Ljubljana, Praga 28 - GMT+01:00 Sarajevo, Skopje, Sofija 29 - GMT+01:00 Varsovia, Zagreb 30 - GMT+01:00 Bruselas, Copenhague 31 - GMT+01:00 Madrid, París, Vilna 32 - GMT+01:00 Ámsterdam, Berlín, Berna 33 - GMT+01:00 Roma, Estocolmo, Viena 34 - GMT+ 02:00 Bucarest 35 - GMT+02:00 El Cairo 36 - GMT+02:00 Helsinki, Riga, Tallin 37 - GMT+02:00 Atenas, Estambul, Minsk 38 - GMT+02:00 Jerusalén 39 - GMT+02:00 Harare, Pretoria 40 - GMT+03:00 Volgograd 41 - GMT+03:00 Bagdad, Kuwait, Riad 42 - GMT+03:00 Nairobi 43 - GMT+03:00 Moscú, San Petersburgo 44 - GMT+03:30 Teherán 45 - GMT+04:00 Abu Dabi, Mascate 46 - GMT+04:00 Bakú, Tbilisi 47 - GMT+04:30 Kabul 48 - GMT+05:00 Ekaterimburgo 49 - GMT+05:00 Islamabad, Karachi, Tashkent 50 - GMT+05:30 Bombay, Calcuta 51 - GMT+05:30 Madrás, Nueva Delhi 52 - GMT+06:00 Astana, Almaty, Dhaka 53 - GMT+06:00 Colombo 54 - GMT+07:00 Bangkok, Hanoi, Jakarta 55 - GMT+08:00 Beijing, Chongqing 56 - GMT+08:00 Hong Kong, Urumqi 57 - GMT+08:00 Singapur 58 - GMT+08:00 Taipéi 59 - GMT+08:00 Perth 60 - GMT+09:00 Seúl 61 - GMT+09:00 Osaka, Sapporo, Tokio 62 - GMT+09:00 Yakutsk 63 - GMT+09:30 Darwin 64 - GMT+09:30 Adelaida 65 - GMT+10:00 Canberra, Melbourne, Sídney 66 - GMT+10:00 Brisbane 67 - GMT+10:00 Hobart 68 - GMT+10:00 Vladivostok 69 - GMT+10:00 Guam, Puerto Moresby 70 - GMT+11:00 Magadan, Islas Salomón. 71 - GMT+11:00 Nueva Caledonia 72 - GMT+12:00 Fiyi, Kamchatka, Islas Marshall. 73 - GMT+12:00 Auckland, Wellington
pseudo -E <1/0>	Habilita (1) o deshabilita (0) la hora del pseudo sistema.
pseudo -T <año> <mes> <día> <hora> <minuto>	Establezca el valor de pseudo tiempo. <año>: ingrese cuatro dígitos. <mes> - Ingrese 1 t0 12. <día> - Ingrese el día en un mes. <hora> - Introduzca el número de la hora (1 a 23). <minuto> - Ingrese el número del minuto (1 a 59).

pseudo -S	Muestra la hora del pseudosistema.

Ejemplo

```
> tiempo del sistema pseudo -E 1
> zona horaria del sistema 8
   Establecer zona horaria OK


> mostrar la hora del sistema
   * * * * * * * * * * * * * * * Hora del sistema **********
   Hora actual del sistema: [2000 Jan 01 Sat 02:40:41] Servidor de
   hora: [pool.ntp.org]
   Índice de zona horaria: [8]. GMT-07:00 Enviar
   solicitud NTP a través de: Automático
   * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
>
```

Comando Telnet: sys eap_tls

Este comando se usa para deshabilitar o habilitar EAP-TLS.

Es posible que deba habilitar la compatibilidad con EAP-TLS para evitar problemas de compatibilidad con algunos sistemas operativos. Pero tenga en cuenta que habilitar la compatibilidad con EAP-TLS reducirá el nivel de seguridad de la conexión.

Sintaxis

sistema eap_tls conjunto <*0/1***>**

Sintaxis Descripción

Parámetro	Descripción
0	¡Desactive la compatibilidad con EAP-TLS!
1	¡Habilite la compatibilidad con EAP-TLS!

Ejemplo

```
> sys eap_tls set 1 ¡Habilite la
compatibilidad con EAP_TLS!
```

Comando Telnet: tablero sys

Este comando se usa para mostrar/ocultar elementos (como información del sistema, interfaz...) en el tablero.

Sintaxis

tablero del sistema*[-<comando> <valor> | ...]* **mostrar**

el tablero del sistema

Sintaxis Descripción

Parámetro	Descripción
[<comando> <valor>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede escribir varios parámetros en una línea. <comando> “0 ~ 9” y “a” representan diferentes secciones que se mostrarán en el tablero.

		0 : Panel frontal 1 : Información del sistema 2 : Información de LAN IPv4 3 : Acceso a Internet IPv4 4 : Acceso a Internet IPv6 5 : Interfaz 6: Seguridad 7: Recurso del sistema 8: Estado de LTE 9 : Acceso rápido a : VoIP
	<valor>	1 : Habilitar 0 : Deshabilitar
espectáculo	Muestra el estado actual (activado/desactivado) de cada elemento.	

Ejemplo

```
> sys dashboard -0 1 Panel
  frontal habilitado
> el tablero del sistema muestra
  el panel frontal habilitado
  Información del sistema habilitada
  Información de LAN IPv4 habilitada
  Acceso a Internet IPv4 habilitado
  Acceso a Internet IPv6 habilitado
  Interfaz habilitada
  Seguridad habilitada
  Recurso del sistema habilitado
  Estado LTE habilitado
  Acceso rápido habilitado
  VoIP habilitado
```

Comando Telnet: sys app_statistic

Este comando se utiliza para habilitar/deshabilitar las estadísticas de los servicios de la aplicación. Para verificar el tráfico de cada servicio de la aplicación, acceda al servidor VigorACS para obtener información detallada.

Sintaxis

sys app_statistic *-v* **sys**
app_statistic *-mi <0/1>* **sys**
app_statistic *-yo*

sys app_statistic *-p <idx de la aplicación>*

sys app_statistic *-q <idx de la aplicación>*

Sintaxis Descripción

Parámetro	Descripción
-v	Muestra el estado actual de la función de la estadística de servicio de la aplicación.
- mi <0/1>	Habilite o deshabilite la función de estadística de servicio de la aplicación.
- yo	Muestra todas las aplicaciones ordenadas con números de índice.
- p <idx de la aplicación>	Habilite la función estadística para la aplicación especificada. <app idx>: las aplicaciones admitidas por este CPE podrían aumentar en el futuro. Actualmente, el rango disponible es de 0 a 156.
- q <idx de la aplicación>	Deshabilite la función estadística para la aplicación especificada.

	<app idx>: las aplicaciones admitidas por este CPE podrían aumentar en el futuro. Actualmente, el rango disponible es de 0 a 156.

Ejemplo

```
> sys app_statistic -e 1
  Mecanismo de estadísticas del servicio de aplicaciones: habilitar
```

Comando Telnet: sys webhook

Este comando se usa para enviar un informe (mensaje webhook) que incluye WAN arriba, abajo, uso de CPU, uso de memoria, etc. a un servidor de monitoreo periódicamente.

Sintaxis

webhook del sistema*enviar*

webhook del sistema*estado*

webhook del sistema*habilitar <0/1>*

webhook del sistema*url <servidor_url>*

webhook del sistema*punto <valor>*

Sintaxis Descripción

Parámetro	Descripción
enviar	Active el informe de webhook inmediatamente.
estado	Muestra la configuración actual del webhook.
habilitar <0/1>	Habilite (1) o deshabilite (1) la función de webhook.
url <servidor_url>	Especifique la URL del servidor de webhook. <server_url>: ingrese la URL.
punto <valor>	Establezca el período del informe del webhook. <valor> - Rango de 1 a 1440 (minutos).

Ejemplo

```
> sys webhook habilitar 1
Establecer webhook ok
> sys webhook period 100
Establecer webhook ok

> estado del webhook del sistema
webhook está activado
URL del servidor de supervisión:
Período del informe: 100
```

Comando Telnet: correo de prueba

Este comando se utiliza para mostrar la configuración actual para enviar correo de prueba.

Ejemplo

```
> correo de prueba
Enviar correo de prueba
  Alerta de correo: [Habilitar]
  Interfaz: Cualquiera
```

```
Índice WAN_Alias:[0]
Servidor_SMTP:[255.255.255.255]
Puerto_SMTP:[25]
Correo a:[]
Vía de retorno:[]
Seguridad de conexión: [Texto sin formato]
```

Comando Telnet: upnp desactivado

Este comando puede cerrar la función UPnP.

Ejemplo

```
> upnp apagado
UPNP decir adiós
```

Comando Telnet: upnp en

Este comando puede habilitar la función UPnP.

Ejemplo

```
> upnp en
Inicio UPNP.
```

Comando Telnet: upnp nat

Este comando puede mostrar el estado de IGD NAT.

Ejemplo

```
> upnp nacional?
* * * * * * * * * * * * * * * * * * Estado NAT IGD ****************

((0))
Cliente interno >>192.168.1.10<<, Host remoto >>0.0.0.0<< Puerto interno
>>21<<, Puerto externo >>21<<
Protocolo de mapa de puertos >>TCP<<
El índice del servidor virtual tmp >>0<< PortMapLeaseDuration
>>0<<, PortMapEnabled >>0<< Ejemplo de Ftp [MICROSOFT]

((1))
Cliente interno >>0.0.0.0<<, Host remoto >>0.0.0.0<< Puerto interno
>>0<<, Puerto externo >>0<<
PortMapProtocol >><NULL><< El índice del servidor virtual tmp
>>0<< PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
PortMapProtocol >><NULL><<

El índice del servidor tmpvirtual >>0<< PortMapLeaseDuration
>>0<<, PortMapEnabled >>0<< 0<<



- - - MÁS --- ['q': Salir, 'Entrar': Líneas nuevas, 'Barra espaciadora': Página siguiente] ---
```

Comando Telnet: servicio upnp

Este comando puede mostrar la información del servicio UPnP. El servicio UPnP debe estar habilitado primero.

Ejemplo

```
> upnp en
Inicio UPNP.

> servicio upnp
> > > > > TABLA DE SERVICIO1 <<<<<
   serviceType urn:schemas-microsoft-com:service:OSInfo:1 serviceId
                     urna:microsoft-com:serviceId:OSInfo1 /upnp/
   SCPDURL           OSInfo.xml
   URL de control    /OSInfo1
   URL del evento    /OSInfoEvent1
   UDN               uuid:774e9bbe-7386-4128-b627-001daa843464

> > > > > TABLA DE SERVICIO2 <<<<<
   serviceType urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1 serviceId
                     urn:upnp-org:ID de servicio:WANCommonIFC1 /
   SCPDURL           upnp/WComIFCX.xml
   URL de control    /upnp?control=WANCommonIFC1 /upnp?
   URL del evento    event=WANCommonIFC1
   UDN               uuid:2608d902-03e2-46a5-9968-4a54ca499148
.
.
.
```

Comando Telnet: suscripción upnp

Este comando puede mostrar todos los servicios UPnP suscritos.

Ejemplo

```
> upnp en
Inicio UPNP.
> upnp suscríbete
> upnp suscríbete
> > > > (1) tipo de servicio urn:schemas-microsoft-com:servicio:OSInfo:1

   - - - - - Suscripción1 -------

      sid = 7a2bbdd0-0047-4fc8-b870-4597b34da7fb

      clave de evento = 1, ToSendEventKey = 1

      tiempo de caducidad = 6926

      activo =1

      URL de entrega
=<http://192.168.1.113:2869/upnp/eventing/twtnpnsiun>

> > > > (2) tipo de servicio urn:schemas-upnp-
org:servicio:WANCommonInterfaceConfig:1

   - - - - - Suscripción1 -------

      sid = d9cd47a5-d9c9-4d3d-8043-d03a82f27983
```

```
        clave de evento = 1, ToSendEventKey = 1
.
.
.
```

Comando Telnet: upnp tmpvs

Este comando puede mostrar el estado actual del servidor virtual temporal de su enrutador.

Ejemplo

```
> upnp tmpvs
* * * * * * * * * * * * * * * * * * Estado del servidor virtual temporal ***************

((0))
dirección_real >>192.168.1.10<<, dirección_pseudo >>172.16.3.229<
puerto_real >>0<<, puerto_pseudo >>0<<
hit_portmap_index >>0<< El
protocolo >>TCP<<
hora >>0<<

((1))
dirección_real >>0.0.0.0<<, dirección_pseudo >>0.0.0.0<<
puerto_real >>0<<, puerto_pseudo >>0<<
hit_portmap_index >>0<< El
protocolo >>0<<
hora >>0<<
- - - MÁS --- ['q': Salir, 'Entrar': Líneas nuevas, 'Barra espaciadora': Página siguiente] ---
```

Comando Telnet: upnp wan

Este comando se usa para especificar la interfaz WAN para aplicar UPnP.

Sintaxis

upnp wan *<n>*

Sintaxis Descripción

Parámetro	Descripción
norte	Significa especificar la interfaz WAN (0 a 6) para aplicar UPnP. n=0, significa seleccionar automáticamente la interfaz WAN. n=1, WAN1 n=2, WAN2. . . n=6, WAN6

Ejemplo

```
> upnp wan 1
usa wan1 ahora.
```

Comando Telnet: lista usb

Este comando se usa para mostrar la información sobre la marca y el modelo de los módems USB que son compatibles con el enrutador Vigor.

Ejemplo

```
> lista de usb?
Marca          Módulo                          Estándar
- - - - - - - - - - - - - - - - - - - - - - -   - - - - - - - -
Sistema 4G     XSPenchufe P3                   3.5G                 Y
Aiko           Aiko 76E                        3.5G                 Y
Alcatel        AlcatelX500                     3.5G                 Y
Esparto        ALFA Flyppp                     3.5G                 Y
amoi           Amoi H01                        3.5G                 Y
BandRich       Bandluxe C321                   3.5G                 Y
BandRich       Bandluxe C330                   3.5G                 Y
BandRich       Bandluxe C331                   3.5G                 Y
BandRich       Bandluxe C502                   3.5G                 Y
Gran charco    BigPond Next G Wir              3.5G                 Y
Gran charco    banda ancha USB Mobi            3.5G                 Y
huawei         Huawei E150                     3.5G                 Y
huawei         Huawei E153                     3.5G                 Y
huawei         Huawei E172                     3.5G                 Y
huawei         Huawei E176c                    3.5G                 METRO
huawei         Huawei E270                     3.5G                 Y
huawei         Huawei E3131                    3.5G                 Y
huawei         Huawei E3272                    3.5G                 Y
huawei         Huawei E3276s                   LTE                  Y
huawei         Huawei E367                     3.5G                 Y
huawei         Huawei E398                     LTE                  Y

huawei         Huawei EC228                    3.5G                 Y
- - - MÁS --- ['q': Salir, 'Entrar': Líneas nuevas, 'Barra espaciadora': Página siguiente] ---
```

Comando Telnet: usuario usb

Este comando se utiliza para establecer perfiles para usuarios de FTP/SMB.

Sintaxis Descripción

agregar usuario usb *<Índice> <Nombre de usuario> <Contraseña> <Permiso> <Ruta de inicio>* **usuario usb**

rm *<Índice>* **habilitación de usuario usb** *<Índice>* **deshabilitar usuario usb** *<Índice>* **lista de usuarios usb**

Sintaxis Descripción

Parámetro	Descripción
agregar <Índice> <Nombre de usuario> <Contraseña> <Permiso> <Ruta de inicio>	Agregar un nuevo perfil de usuario. <Índice>: Significa el número de índice del perfil de usuario. Hay 16 perfiles que se pueden configurar. Entonces, el rango de dicha opción es 1 ~ 16. <Nombre de usuario>: Introduzca un texto (máximo 131 caracteres) como nombre de usuario para el perfil de usuario. <Contraseña>: Introduzca un texto (máximo 131 caracteres) como contraseña para el perfil de usuario. <Permiso>: Especifique la acción (RWDLCR) permitida. Si una de las acciones no está permitida, simplemente escriba "-" en su lugar.

	R – Leer archivo. W – Escribir archivo. D – Eliminar archivo. L – Lista de directorios. C – Crear directorio. R: elimina el directorio seleccionado. <Ruta de inicio>: establezca la ruta (máximo 159 caracteres) para el perfil de usuario USB.
rm <Índice>	Eliminar un perfil de usuario existente. <Índice>: Significa el número de índice del perfil de usuario.
habilitar <Índice>	Habilitar un perfil de usuario. <Índice>: Significa el número de índice del perfil de usuario.
deshabilitar <Índice>	Deshabilitar un perfil de usuario. <Índice>: Significa el número de índice del perfil de usuario.
lista	Mostrar todo el perfil de usuario.

Ejemplo

```
> usuario usb agregar 1 root 1234 R-DLCR /usr
> ¡No hay almacenamiento USB disponible!
```

Comando Telnet: temperatura usb

Este comando es para configurar la temperatura del USB.

Sintaxis Descripción

conjunto de temperatura usb<*-c*|*-f*|*-a*|*-b*|*-m*|*-u*|*-l*|*-r*> **espectáculo**

de temperatura usb

usb temp todos los datos

Sintaxis Descripción

Parámetro	Descripción
conjunto -c	Configure la unidad de temperatura (Celsius).
conjunto -f	Configure la unidad de temperatura (Fahrenheit).
conjunto -a	Configure el sensor de temperatura utilizando una sonda o el sensor incorporado automáticamente. La sonda se detectará y usará primero, y volverá al sensor incorporado si no se detecta la sonda.
conjunto -b	Configúrelo para usar el sensor incorporado.
conjunto -m	Habilite o deshabilite la configuración de alarma. 1: Habilitar 0: Deshabilitar
establecer -u <valor>	Establezca el límite de temperatura superior. <valor>: Introduzca un valor, por ejemplo, 30,35.
establecer -l <valor>	Establezca el límite de temperatura inferior. <valor>: Introduzca un valor, por ejemplo, 10,35.
conjunto -r	Muestra el ajuste de la unidad de temperatura y el tipo de sensor.
espectáculo	Muestra la temperatura actual.
toda la información	Muestra todos los datos de temperatura.

Ejemplo

> usb temp set -r Mostrar
configuración:temp set -r

Configuraciones de alarma: 1 (0: Deshabilitar, 1: Habilitar.)
Límite superior de temperatura: 30.0 C
límite inferior de temperatura: 18,0 C unidad: 0 (0:
Celsius, 1: Fahrenheit.) sensor: 1 (0: selección
automática, 1: integrado)

> conjunto de temperatura usb

-c Establecer Celsius.

Comando Telnet: zumbido usb

Este comando es para configurar la humedad del USB.

Sintaxis Descripción

conjunto de zumbido usb*<m|-u|-l|-r>*

Espectáculo de zumbido USB

usb zumbido todos los datos

Sintaxis Descripción

Parámetro	Descripción
conjunto -m	Habilite o deshabilite la configuración de alarma. 1: Habilitar 0: Deshabilitar
establecer -u <valor>	Establezca el límite superior de humedad. <valor>: Introduzca un valor, por ejemplo, 80,85.
establecer -l <valor>	Establezca el límite inferior de humedad. <valor>: Ingrese un valor, por ejemplo, 30.12.
conjunto -r	Muestra el ajuste de la humedad.
espectáculo	Muestra la humedad actual.
toda la información	Muestra todos los datos de humedad.

Ejemplo

> usb hum set -m 1 Habilite la
configuración de alarma.
>

Comando Telnet: conjunto vigbrg

Este comando es para configurar la WAN especificada como modo puente.

Sintaxis Descripción

conjunto vibrg*-v <versión IP> -w <idx_WAN> -l <idx_LAN> -e <0/1> -f <0/1>*

Sintaxis Descripción

Parámetro	Descripción
- v <versión IP>	Indique la versión de IP para la dirección IP. 4-IPv4. 6-IPv6.

w <idx_WAN>	WAN_idx: indica la interfaz WAN. 1 – WAN1 2 – WAN2 3 – WAN3 4 – WAN4 5 - WAN5
- l <LAN_idx>	LAN_idx: indica la interfaz LAN. 1 – LAN1 2 – LAN2 3 – LAN3 4 – LAN4 5 - LAN5 6 - LAN6 .... 15 - LAN15
- mi <0/1>	Habilite (1) o deshabilite (0) Vigor Bridge para WAN y/o LAN.
-f<0/1>	Habilite (1) o deshabilite (0) las funciones del firewall.

Ejemplo

```
> conjunto vigbrg -v 4 -w 5 -l 1 -e 1
[WAN5] El puente IPv4 está habilitado. Establecer subred[LAN1]
```

Comando Telnet: vigbrg closeall

Este comando puede deshabilitar la función de puente vigor.

Ejemplo

```
> cierre vigbrg
Cerrar todos los puentes y cortafuegos de puente
```

Comando Telnet: estado vigbrg

Este comando puede mostrar si la función Vigor Bridge está habilitada o deshabilitada.

Ejemplo

```
> estado vibrg
Mostrar la configuración de gConfig del modo puente

¡La gestión de %Wan1 está desactivada!
```

Comando Telnet: vigbrg cfgip

Este comando permite a los usuarios transferir un módem puente al enrutador ADSL accediendo y ajustando la dirección IP especificada. Los usuarios pueden acceder a la interfaz de usuario web del enrutador para administrar el enrutador a través de la dirección IP configurada aquí.

Sintaxis

vigbrg cfgip*<Dirección IP>*

Sintaxis Descripción

Parámetro	Descripción
Dirección IP	Significa escribir una dirección IP para que los usuarios administren el enrutador.

Ejemplo

```
> vigbrg cfgip 192.168.1.15
> vigbrgcfgip?
% Vigor Bridge Config IP, %
Ahora: 192.168.1.15
```

Comando Telnet: vigbrg wanstatus

Este comando puede mostrar el estado de la conexión WAN existente para el módem (cambio de enrutador ADSL a módem puente), incluido el número de índice, la dirección MAC, la hora del sello, el PVC, el puerto VLAN para la función Vigor Bridge.

Ejemplo

```
> estado de alerta de vigbrg
Puente Vigor: Correr
Tabla mac WAN:
Dirección MAC del índice        Tiempo de sello   CLORURO DE POLIVINILO   VLan   Puerto
```

Comando Telnet: vigbrg wlanstatus

Este comando puede mostrar el estado de la conexión WLAN existente para el módem (cambio de enrutador a módem puente), incluido el número de índice, la dirección MAC, la hora del sello, el PVC, el puerto VLAN para la función Vigor Bridge.

Ejemplo

```
> vigbrg wlanstatus
Puente Vigor: Correr
Tabla mac WAN:
Dirección MAC del índice        Tiempo de sello   CLORURO DE POLIVINILO   VLan   Puerto
```

Comando Telnet: fullbrg

El comando se usa para habilitar el modo de puente completo para que el enrutador funcione como un módem puente que puede reenviar paquetes entrantes con etiquetas VLAN.

Sintaxis

estado completo

conjunto completo -i *<Índice WAN>* **-norte** *<Índice de subred>* **-b** *<Modo puente>*

Sintaxis Descripción

Parámetro	Descripción
- i <Índice WAN>	Índice WAN: Rangos de 1 a 16. 1: WAN1, 2: WAN2, ...etc., En el cual, WAN3 y WAN 4 son WAN USB.
- n <Índice de subred>	Índice de subred: Rangos de 1 a 8. 1: Subred 1, 2: Subred 2, ...etc.
- b <Modo puente>	Significa habilitar/deshabilitar el modo Bridge. 0: APAGADO 1: ENCENDIDO

Ejemplo

```
> estado completo?
Muestre la configuración de gConfig de puente completo
WAN 1 puente completo a LAN 1, modo = APAGADO.
Puente completo de WAN 2 a LAN 1, modo = APAGADO.
Puente completo de WAN 3 a LAN 1, modo = APAGADO.
Puente completo de WAN 4 a LAN 1, modo = APAGADO.
Puente completo de WAN 7 a LAN 1, modo = APAGADO.
Puente completo de WAN 8 a LAN 1, modo = APAGADO.
Puente completo de WAN 9 a LAN 1, modo = APAGADO.
Puente completo WAN10 a LAN 1, modo = APAGADO.
Puente completo WAN11 a LAN 1, modo = APAGADO.
Puente completo WAN12 a LAN 1, modo = APAGADO.
Puente completo WAN13 a LAN 1, modo = APAGADO.
Puente completo WAN14 a LAN 1, modo = APAGADO.
Puente completo WAN15 a LAN 1, modo = APAGADO.
Puente completo WAN16 a LAN 1, modo = APAGADO.
> conjunto completo -i 2 -n 5 -b 1
¡Configurar bien! Reinicie el dispositivo para que sea efectivo.
> estado completo
Muestre la configuración de gConfig de puente completo
WAN 1 puente completo a LAN 1, modo = APAGADO. Puente
completo de WAN 2 a LAN 5, modo = ENCENDIDO. Puente
completo de WAN 3 a LAN 1, modo = APAGADO. Puente
completo de WAN 4 a LAN 1, modo = APAGADO. Puente
completo de WAN 7 a LAN 1, modo = APAGADO. Puente
completo de WAN 8 a LAN 1, modo = APAGADO. Puente
completo de WAN 9 a LAN 1, modo = APAGADO. Puente
completo WAN10 a LAN 1, modo = APAGADO. Puente
completo WAN11 a LAN 1, modo = APAGADO. Puente
completo WAN12 a LAN 1, modo = APAGADO. Puente
completo WAN13 a LAN 1, modo = APAGADO. Puente
completo WAN14 a LAN 1, modo = APAGADO. Puente
completo WAN15 a LAN 1, modo = APAGADO. Puente
completo WAN16 a LAN 1, modo = APAGADO.
>
```

Comando Telnet: depuración voip

Este comando puede mostrar un mensaje de depuración en la pantalla.

Sintaxis

depuración voip*<al ras>*

depuración voip*<mostrarmsg>*

Sintaxis Descripción

Parámetro	Descripción
enjuagar	Significa borrar el registro actual.
mostrarmsg	Significa mostrar el registro actual.

Ejemplo

```
> showmsg de depuración de voip
```

```
- - > Enviar Mensaje a 192.168.1.2:5060 <02:35:16> INVITE
sip:192.168.1.2 SIP/2.0
Vía: SIP/2.0/UDP 192.168.1.1:5060;branch=z9hG4bK-YMa-3630;rport De: <sip:
change_me@192.168.1.1 >;tag=WLJ-11782
Para: <sip:192.168.1.2>
ID de llamada: PbU-25312@192.168.1.1
CSeq: 1 INVITE
Contacto: <sip: change_me@192.168.1.1 >
Reenvíos máximos: 70
soportado: 100rel, reemplaza
Agente de usuario: DrayTek UA-1.2.3 DrayTek Vigor2910
Permitir: INVITE, ACK, CANCEL, OPTIONS, BYE, INFO, REFER, NOTIFY, PRACK Tipo de
contenido: application/sdp
Longitud del contenido: 264

v=0
o=cambiarme 5972727 56415 EN IP4 192.168.1.1
```

Comando Telnet: plan de marcación voip

Este comando permite a los usuarios establecer la configuración de la guía telefónica.

Sintaxis

bloque de plan de marcación voip*n [-<comando><parámetro>]*
agenda voip dialplan*n [-<comando><parámetro>]* **región del plan de marcación voip***[-<comando><parámetro>]* **voip dialplan local***< 1/0>*

Sintaxis Descripción

Parámetro	Descripción
bloque de plan de marcación voip	
norte	Significa el número de índice de la configuración de VoIP. n=1 ~ 20
- <comando><parámetro>	Los comandos disponibles con parámetros se enumeran a continuación.
-m 0/1	Significa habilitar o deshabilitar el modo de bloqueo. 0 – Deshabilitar 1 - Habilitar
- p <ruta>	Determina la ruta del bloque. 1:en_url, 2:en_número 3:out_url, 4:out_number 5:(entrada y salida)_url, 6:(entrada y salida)_número))
- n <número>	Determina el número de bloque (máximo 29 caracteres).
- d <dominio>	Bloquear el dominio especificado.
- yo <inf>	Bloquee las interfaces especificadas o todas las interfaces.
- s <Horario>	Especifique los perfiles de programación indicando el número de índice del perfil de programación. Se pueden usar cuatro perfiles de horario a la vez.
- w	Eliminar la entrada seleccionada. N = nulo (borrar todo)
-v	Muestra la configuración actual.

agenda voip dialplan	
norte	Significa el número de índice de la configuración de VoIP. n=1 ~ 60
- <comando><parámetro>	Los comandos disponibles con parámetros se enumeran a continuación.
- d <número>	Especifique el número de marcación rápida.
- c <url>	Contacto SIP URL l (máx. 59 caracteres)
- n <nombre>	Nombre de contacto (máx. 23 caracteres)
- un <habilitar>	Habilitar/deshabilitar la entrada específica.
- m <modo>	Especifique el modo de número de respaldo. 0 – ninguno 2 - RTPC
- b <número>	Especifique el número de respaldo.
- o <número de cuenta>	Especifique la cuenta de marcado. 0 – predeterminado 1 - cuenta1, 2 - cuenta2... ~ 12:=cuenta12
-z <habilitar>	Habilitar/deshabilitar la seguridad VoIP ZRTP/SRTP. 1 – habilitar 0 - deshabilitar
- yo	Elimine la entrada específica.
-V	Muestra la configuración actual de VoIP.
región del plan de marcación voip	
- mi	Activa o desactiva la función regional. 1 – habilitar 0 - deshabilitar
- m <número>	Devuelve la última llamada perdida.
- Yo <número>	Devolver la última llamada entrante.
- o <número>	Devolver la última llamada saliente.
- F <número>	Tecla de acceso rápido para habilitar la función de desvío de llamadas (todas).
- f <número>	Tecla de acceso directo para habilitar la función de desvío de llamadas (ocupado).
- C <número>	Tecla de acceso rápido para habilitar la función de desvío de llamadas (sin respuesta).
- c <número>	Tecla de acceso rápido para deshabilitar la función de desvío de llamadas.
- W <número>	Tecla de acceso rápido para habilitar la función de llamada en espera.
- w <número>	Tecla de acceso rápido para deshabilitar la función de llamada en espera.
- H <número>	Tecla de acceso rápido para habilitar la función de ocultar la identificación de llamadas.
- h <número>	Tecla de acceso rápido para deshabilitar la función de ocultar la identificación de llamadas.
- D <número>	Tecla de acceso rápido para habilitar la función DND.
- d <número>	Tecla de acceso rápido para deshabilitar la función DND.
- Un <número>	Tecla de acceso rápido para habilitar la función de bloqueo de llamadas anónimas.
- un <número>	Tecla de acceso rápido para deshabilitar la función de bloqueo de llamadas anónimas.
- U <número>	Tecla de acceso rápido para habilitar la función de bloqueo de llamadas de dominio desconocido.
- tu <número>	Tecla de acceso rápido para deshabilitar la función de bloqueo de llamadas de dominio desconocido.
- P <número>	Tecla de acceso rápido para deshabilitar la función de bloqueo de llamadas IP.
- p <número>	Tecla de acceso rápido para deshabilitar la función de bloqueo de llamadas IP.
- l <número>	Tecla de acceso rápido para bloquear la última llamada entrante.
-v	Muestra el estado actual de la configuración regional.
voip dialplan local	

habilitar deshabilitar	Activa o desactiva las llamadas locales. 1 – habilitar 0 - deshabilitar

Ejemplo

> agenda telefonica voip dialplan 1 -d 1125
> región del plan de marcación voip -l 8
> voip dialplan region -v Su configuración para
Regional Función regional es: Habilitar
Devolver la última llamada perdida: 20
Devolver la última llamada entrante: *12
Devolver la última llamada saliente: 1

Tecla de acceso rápido para habilitar la función de desvío de llamadas (todas): 0 Tecla de acceso rápido para habilitar la función de desvío de llamadas (ocupado): *90 Tecla de acceso rápido para habilitar la función de desvío de llamadas (sin respuesta): *92 Tecla de acceso rápido para deshabilitar la función de desvío de llamadas: 12
Tecla de acceso directo para activar la función de llamada en espera: *56 Tecla de acceso directo para desactivar la función de llamada en espera: *57 Tecla de acceso directo para activar la función Ocultar identificación de llamadas: *67 Tecla de acceso directo para desactivar la función Ocultar identificación de llamadas: *68 Tecla de acceso directo para activar la función DND: *78
Tecla de acceso rápido para desactivar la función DND: *79
Tecla de acceso rápido para habilitar la función Bloquear llamadas anónimas: *77 Tecla de acceso rápido para deshabilitar la función Bloquear llamadas anónimas: *87 Tecla de acceso rápido para habilitar la función Bloquear llamadas de dominio desconocido: *40 Tecla de acceso rápido para deshabilitar la función Bloquear llamadas de dominio desconocido: *04 Tecla de acceso rápido para habilitar la función Bloquear llamadas IP: *50
Tecla de acceso rápido para deshabilitar la función Bloquear llamadas IP: *05
Tecla de acceso rápido para deshabilitar la función Bloquear la última llamada entrante: 8

Comando Telnet: voip dsp

Sintaxis

voip dsp countrytone*[canal] [valor]* **voip dsp discaltonepwr***[canal] [ValorAbsoluto]* **voip dsp cancelador de eco***[tipo] [w_size] [nlp]* **tipo de cid dsp voip***[canal] [valor]* **micrófono dsp voip***[canal] [valor/(1~10)]* **voip dsp spkgain***[canal] [valor/(1~10)]* **voip dsp jb***[puerto] [modo] [valor]* **temporizador dsp voip***[Temporizador]*

VoIP dsp dtmfDetset*[nNivel] [nTorsión]* **voip dsp dtmftonepwr***[Nivel]* **voip dsp cwtonepwr***[ch] [valor]* **voip dsp pstnringfxs***[1|2] [encendido|apagado]* **voip dsp relaydbounce***[encendido | apagado]*
voip dsp setRingPat*[ring_pattern_index] [patten_num]* **dsp voip***establecerFaxECmode*
dsp voip*setDtmfCidlevel –l**[valor]* **dsp voip*establecerDtmfCidlevel –h****[valor]*

dsp voip*setDtmfCidlevel –r 0*
dsp voip*setfxoCY*
dsp voip*cidplusdigito**[1/0] [canal] [valor]*** **dsp**
voip*setfxoringl*
dsp voip*setfxoCid*
dsp voip*cidplusdigito*
dsp voip*establecerAnilloTres*
dsp voip*setCidDetGain*
dsp voip*Anillo ilimitado*

Sintaxis Descripción

Parámetro	Descripción
voip dsp countrytone	
[canal] [valor]	Este comando permite a los usuarios establecer la región para la configuración del tono. Las diferentes regiones generalmente necesitan diferentes configuraciones de tono. Canal – 1 o 2. Valor: se muestra de la siguiente manera: [2] Reino Unido, [3] EE. UU., [4] Dinamarca, [5] Italia, [6] Alemania, [7] Países Bajos, [8] Portugal, [9] Suecia, [10] Australia, [11] Eslovenia, [12] República Checa, [13] Eslovaquia, [14] Hungría, [15] Suiza , [16] Francia , [17] Malta
voip dsp discaltonepwr	
canal	Esta configuración se utiliza para ajustar el volumen del tono de marcación. Cuanto más pequeño es el número, más fuerte es el tono de marcación. Se recomienda que utilice la configuración predeterminada. Canal - Número de canal disponible: 1 – 2
Valor absoluto	AbsoluteValue: en incrementos de -1 dB, con 1 correspondiente a 6 dBm. Rango - 1 a 30
voip dsp cancelador de eco	
tipo	Este comando se utiliza para establecer el tipo de reducción de eco. 0 - Deshabilitar el procesamiento LEC. 1 - Cancelar usando la ventana fija. 2 - Cancelar usando la ventana fija y móvil. 3 - Cancelar usando ventana fija + Supresor de Eco.
w_size	El tamaño de la ventana del Line Echo Canceller (LEC) es de 4, 6, 8 o 16 (ms).
PNL	Nlp: procesamiento no lineal (NLP) para transiciones más suaves. 1 - deshabilitar 0 - habilitar
tipo de cid dsp voip	
canal	Configure el tipo de identificador de llamadas para FXS 1 (Canal 1) o FXS 2 (Canal 2). 1 – FXS 1 2 – FXS 2
valor	Cada número (del 1 al 6) representa un tipo diferente. 1 – FSK_ETSI 2 - FSK_ETSI (Reino Unido) 3 - FSK_BELLCORE (EE. UU./AU) 4 - DTMF 5 - DTMF (Dk) 6 - DTMF(SE,NL,FIN) Por ejemplo :

	Vigor> voip dsp cidtype 2 6 canal=2, actual cidType: 6 Eso significa que el tipo de identificador de llamadas para FXS2 (Channel2) es DTMF (SE, NL, FIN).
micrófono dsp voip	
canal	Ajuste el volumen del micrófono ingresando un número del 1 al 10 para FXS 1 o FXS 2. 1 – FXS 1 2 – FXS 2
valor/(1~10)	Cuanto mayor sea el número, mayor será el volumen.
voip dsp spkgain	
canal	Ajuste el volumen del altavoz ingresando un número del 1 al 10 para FXS 1 o FXS 2. 1 – FXS 1 2 – FXS 2
valor/(1~10)	Cuanto mayor sea el número, mayor será el volumen.
voip dsp jb	
puerto	Establezca el tamaño del búfer de fluctuación. Los ajustes disponibles son 0 (FXS1) y 1 (FXS2).
modo	Los ajustes disponibles son**Fijado**y**Adaptado**(Configuración predeterminada).
valor	Los ajustes disponibles son 1 ~ 180 (unidad: mseg). p.ej, Vigor > voip dsp jb 1 FIJO 100
temporizador dsp voip	
[Temporizador]	Configure el tiempo de espera para marcar. Significa establecer la configuración del temporizador. La unidad es el minisegundo. El rango es de 1 a 255. El valor “1” corresponde a 500ms. Es decir, el valor "6" corresponde a 3000ms (es decir, 3 segundos) Temporizador: 1 ~ 20. Vigor> voip dsp timer 20 Configurar el temporizador: 20
Mensaje de depuración VoIP DSP	
?	Las configuraciones disponibles incluyen: clrev: borrar el estado de conexión del teléfono. getev: obtiene el estado de conexión del teléfono. clrfskcid: borra los datos fsk para el identificador de llamadas de la línea PSTN. getfskcid: obtenga datos fsk para el identificador de llamadas de la línea PSTN. clrdtmfcid: borra los datos dtmf para el identificador de llamadas de la línea PSTN. getdtmfcid: obtenga datos dtmf para el identificador de llamadas de la línea PSTN. voicebuf: recibe un mensaje para el grupo de búfer de voz disponible. clrint - borra el estado de la interrupción. getint: obtiene el estado de la interrupción. Vigor> voip dsp debugMsg getint el estado de interrupción para ad0 = 21 el estado de interrupción para ad1 = 0 el estado de interrupción para vc = 0
VoIP dsp dtmfDetset	
nNivel	Establezca el nivel de señal mínimo en dB, para la detección de DTMF. Rango – (-96 ~ -1)
giro	Giro de señal máximo permitido en dB, para detección DTMF. Rango – (0 ~ 12)
voip dsp dtmftonep	

Nivel	Establece el nivel de potencia para la frecuencia DTMF. Nivel – 0 ~ 100. Nivel de potencia para frecuencia dtmf en pasos de 0,3 dB. 0 mapa a 0dB 1 mapa a -0.3dB .... 100 mapa a -30dB
voip dsp cwtonepwr	
ch	Configure el nivel de potencia del tono de llamada en espera. 1 – FXS 1 2 – FXS 2.
valor	1 ~ 30, en incrementos de -1 dB, con 1 correspondiente a 8 dBm.
voip dsp pstnringfxs	
1|2	Habilite o deshabilite el timbre PSTN en FXS 1/FXS 2. 1 significa FXS1; 2 significa FXS2.
encendido | apagado	On significa habilitar; apagado significa deshabilitar.
voip dsp relaydbounce	
encendido | apagado	on: habilitar el ruido del filtro de relé. ¡Pero tal vez ignore el identificador de llamadas! off: deshabilitar el ruido del filtro de relé. ¡Pero el ruido hará que el relé cambie a PSTN!
voip dsp setRingPat	
ring_pattern_index	Este comando puede cambiar el patrón de timbre en el Índice (2) ~ Índice (6). ring_pattern_index: el índice (1) se bloqueó para su país.
patten_num	Es el número de patrón de timbre (1~12) de un país. - *patten_num=1 Patrón de timbre de Australia:* *cadenceOneOn=400, cadenceOneOff=200* *cadenceTwoOn=400, cadenceTwoOff=2000* *patten_num=2 Patrón de timbre de Dinamarca:* *cadenceOneOn=1000, cadenceOneOff=4000* *.....*
voip dsp setFaxECmode -s	
ch	Configure el modo de corrección de errores de FAX. canal: rango (0 ~ 1)
modo	modo: EC (corrección de errores) ch (x) modo (0): REDUNDANCIA CE (corrección de errores) ch (x) modo (1): FEC
voip dsp setDtmfCidlevel –l / voip dsp setDtmfCidlevel –h*[valor]* ***dsp voip setDtmfCidlevel –r 0***	
valor	"setDtmfCidLevel" se utiliza para configurar la intensidad de la señal para transferir a la identificación de llamadas FXS DTMF. valor - 0 ~ 64 voip dsp setDtmfCidLevel -l [valor] voip dsp setDtmfCidLevel -h [valor] voip dsp setDtmfCidLevel -r 0/1 r - restablecer el nivel DTNF bajo/alto a la configuración predeterminada. 0 significa Desactivar; 1 significa Habilitar. Nota: Esta función solo es compatible con el modo especial.
dsp voip setfxoCY	
valor	Se utiliza para aplicar la configuración de país de FXO. 0: "usar país del sistema" 1: "Taiwán" 2: "Alemania" 3: "Suecia" 4: "Francia"

	5: "Suiza" 6: "Holanda" 7: "Finlandia" 8: "Dinamarca" 9: "REINO UNIDO" 10: "Australia" 12: "Italia" 14: "China_Roja" 15: "Singapur" 17: "España" 18: "Portugal" 20: "Polonia" 21: "Checo" 22: "Hungría" 23: "Eslovenia" 25: "Eslovaquia" 37: "Brasil" 61: "A NOSOTROS"
voip dsp setfxoringl	
valor	Se utiliza para configurar el umbral de voltaje del anillo de detección para aplicar a FXO. La configuración disponible incluye: 0: usar el valor predeterminado del controlador 1 : Umbral de tensión mínima: 25V 2 : Umbral de tensión mínima: 35V 3 : Umbral de tensión mínima: 45V Nota: Esta función solo es compatible con el modo especial.
voip dsp setfxoCid	
valor	Configure FXO para detectar el tipo de identificador de llamadas. Está disponible solo para el modelo con puerto FXO.
voip dsp cidplusdigit	
[1/0] [canal] [valor]	Configure la sustitución (0~9) del dígito '+' en el identificador de llamadas. 1 – habilitar la sustitución. 0: deshabilita la sustitución. canal – 0 (FXS 1) -1 (FXS 2) valor – 0 – 9
voip dsp setRingThres	
puerto	Configure el umbral para la señal de llamada. La configuración del puerto es "0" solamente.
valor	Configuraciones disponibles 0-250. La unidad es ms. El tiempo es un valor aproximado.
voip dsp setCidDetGain	
ganancia tx|rx	Establezca el valor de ganancia del identificador de llamadas detectado. Ganancia Tx: configuraciones disponibles: -24 ~ 12. El valor predeterminado es 0. Ganancia Rx: configuraciones disponibles: -24 ~ 12. El valor predeterminado es -6.

Ejemplo

```
> voip dsp countrytone ?
VoIP ha sido deshabilitado.Habilite VoIP primero.
> voip sip misc –D 0
¡Reinicio del sistema ahora!
> voip dsp countrytone ?
```

```
> vigor> voip dsp countrytone? uso:

  voip dsp countrytone [canal][valor] [canal]: 1-2

  [valor]: ( [2] Reino Unido, [3] EE. UU., [4] Dinamarca, [5] Italia, [6] Alemania, [7] Holanda
s, [8] Portugal, [9] Suecia, [10] Australia, [11] Eslovenia, [12] República Checa, [13] Eslovaquia, [14]
Hungría, [15] Suiza, [16] Francia, [17] Malta)
============ Canal=1 ================== Tono del
  país actual: definido por el usuario

- - - - - - - - - - - (Tono de marcación) ---------- Feq1=425, Feq2=0,
  OneOn=0, Off=0 , DosEncendido=0, DosApagado=0
- - - - - - - - - - - ( Tono de llamada ) ----------
  Feq1=425, Feq2=0, OneOn=1500, OneOff=3000, TwoOn=0, TwoOff=0
- - - - - - - - - - - (Tono de ocupado) ---------- Feq1=425, Feq2=0, OneOn=200,
  OneOff=200 , DosEncendido=0, DosApagado=0

============ Canal=2 ================== Tono del
  país actual: definido por el usuario
> voip dsp dialtoneepwr 1 20
Nivel de potencia actual del tono de marcación: 20 (-13 db), canal = 1
> voip dsp setCidDetGain tx 1
  Ganancia Tx de detección de CID actual [1], Ganancia Rx [-6]
> voip dsp setCidDetGain rx 3
  Ganancia Tx de detección de CID actual [1], Ganancia Rx [3]
```

Comando Telnet: voip rtp

Sintaxis

códec voip rtp*[sip acc index][tipo|tamaño|vad|uno][valor]*
voip rtp dtmf*[índice] [modo|tipo de carga útil][valor]* **puerto**
voip rtp*[inicio|fin] [valor]* **voip rtp simetrico***[valor]* **voip rtp**
tos?

Sintaxis Descripción

Parámetro	Descripción
códec voip rtp	
[sip acc índice][tipo|tamaño|vad|uno] [valor]	Configure la codificación de voz. sip acc index: número de índice de cuenta SIP. Número disponible, 1 ~ 12. tipo: las configuraciones disponibles incluyen 0. G.711MU 1. G.711A 2. G.729A/B 3. G.723 4. G.726_32 tamaño: cinco opciones, 0 significa 10 ms 1 significa 20ms 2 significa 30ms 3 significa 40ms 5 significa 60ms Vad - 0 significa Deshabilitar la función de Voice Active Detector (vad); 1 significa habilitar la función de Voice Active Detector

	(vad). Uno – 0 significa Deshabilitar la función de códec único; 1 significa Habilitar la función de códec único.
voip rtp dtmf	
[índice] [modo | tipo de carga útil][valor]	Configure el modo DTMF y el tipo de carga útil para DTMF. Índice: número de índice de la cuenta SIP. Número disponible, 1 ~ 12. Modo: cuatro opciones para seleccionar. 0. En banda 1. Fuera de banda 2. INFORMACIÓN SIP (cisco) 3. INFORMACIÓN SIP (nortel) Tipo de carga útil: configuraciones disponibles 96 ~ 127. Valor: escriba 0~3 o 96~127 según el modo especificado. Por ejemplo, > voip rtp dtmf 1 modo 1
puerto voip rtp	
comienzo|fin	Especifica el puerto de inicio/fin para la transmisión RTP.
valor	El valor predeterminado es 10050/15000.
voip rtp simetrico	
valor	Haga que la transmisión de datos se realice en ambos extremos del enrutador local y del enrutador remoto sin que sea engañoso debido a la pérdida de IP. 1 – Habilitar 0 - Deshabilitar
voip rtp tos	
valor	Establezca la configuración del tipo de servicio (TOS) para los paquetes RTP. Por ejemplo, > voip rtp tos 0x899 Establecer TOS: 0x899

Ejemplo

```
> voip rtp codec 1 tipo 3
> voip rtp dtmf 2 modo 3
> voip puerto rtp inicio 10070 final 14400
Establecer puerto de inicio: 10070
> extremo del puerto voip rtp 14400
Establecer puerto final: 14400
> voip rtp simétrico 1 Establezca rtp
simétrico en Habilitar
```

Comando Telnet: voip sip

Este comando permite a los usuarios configurar una cuenta SIP.

Sintaxis

cuenta voip sorbo*[-<comando> <parámetro> | ...]* **alias de sorbo voip***[-<comando> <parámetro> | ...]* **registro de llamadas voip sip**

voip sorbo ep n*[-<comando> <parámetro> | ...]* **voip sorbo misceláneo***[-<comando> <parámetro> | ...]*

voip sorbo nat*[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
cuenta voip sorbo -Permite a los usuarios configurar una cuenta SIP.	
norte	n = 1 a 12 Significa el número de índice de la configuración de VoIP.
- P [perfil]	Significa el nombre del perfil de la cuenta (máximo 11 caracteres).
- r [modo de registro]	Establecer el modo de registro para la cuenta SIP. 0 – ninguno 1 – automático 2 - solo wan1 3 - solo wan2 4 - LAN/VPN 5 – PVC 6 - solo wan3 7 - solo wan4 8 - wan1 primero 9 - wan2 primero 10 - wan3 primero 11 - wan4 primero
- o [puerto]	Configure el número de puerto para enviar/recibir mensajes SIP para crear una sesión. El valor predeterminado es 5060.
- d [dominio]	Configure el nombre de dominio o la dirección IP del servidor SIP Registrar. El máximo es de 63 caracteres.
- y [apoderado]	Establezca el nombre de dominio o la dirección IP del servidor proxy SIP. El máximo es de 63 caracteres.
- b [habilitar]	Habilitar / deshabilitar el proxy de salida por cuenta SIP. 0 – deshabilitar 1 - habilitar
- s [habilitar]	Activar/desactivar para localizar servidor SIP (rfc 3263). 0 – deshabilitar 1 - habilitar
-N [nombre]	Establezca el nombre para mostrar de la cuenta SIP. Nombre - máx. 23 caracteres.
- n [número]	Establezca el número de cuenta SIP. Número - máx. 63 caracteres.
- ayuda]	Establecer ID de autenticación SIP. Identificación - máx. 63 caracteres.
- A [habilitar]	Habilite o deshabilite el uso de la ID de autenticación SIP. 0 – deshabilitar 1 - habilitar
- p [contraseña]	Configure la contraseña de la cuenta SIP (máx. 63 caracteres).
- e [seg]	Establezca el tiempo de caducidad (predeterminado 3600) para la cuenta SIP.
- w [habilitar]	Habilite para hacer llamadas telefónicas sin registrarse.
- m [modo]	Establezca el modo transversal de NAT. 0 – deshabilitar 1 - aturdir 2-manual 3 - norte
- F [modo]	Establecer el modo de desvío de llamadas. 0 – deshabilitar 1 – siempre

	2 – ocupado 3 - sin respuesta 4 - ocupado o sin respuesta
- tu [url]	Configure la URL SIP para el desvío de llamadas (máx. 63 caracteres).
- t [seg]	Configurar el temporizador de desvío de llamadas. Por ejemplo, voip sip acc 1 –t 30
- g [puerto]	Configure el puerto de timbre para la llamada entrante. Por ejemplo, Puerto - r1 significa FXS1; r2 significa FXS2.
-z [patrón]	Establezca el patrón de timbre de la cuenta (1 ~ 6).
- yo [habilitar]	Elimine todos los enlaces mientras no estén registrados. 0 significa Desactivar; y 1 significa Habilitar.
- B <habilitar>	Activar/desactivar la función de Broadsoft Call Control. 0 – deshabilitar 1 - habilitar
- S [idx]	Habilite y use alias de IP para registrarse. idx - 1 a 31. Si se usa 0, dicha función será deshabilitada.
- k [num1 numero2...]	Establezca la lista de wan de respaldo (primer wan, segundo wan...). rango: 1 a 4.
-v	Ver el estado actual de la configuración de la cuenta.
alias de voip	
norte	n = 1 a 30
- e <habilitar>	Habilite o deshabilite este perfil de alias. 0: Deshabilitar. 1: Habilitar.
- un <nombre de usuario>	Establezca el nombre del alias (máximo 23 caracteres).
- n <número>	Establezca el número de alias (máximo 63 caracteres).
- t <idx de cuenta>	Configure el alias de la cuenta SIP. (rango: 1~12)
- v <idx>	mostrar información de la lista de alias.
registro de llamadas voip sip	Muestra el estado actual del registro de llamadas SIP.
voip sorbo ep	
norte	El número de índice de la configuración de VoIP. n-1, 2.
- o [ac]	Cuenta de marcación disponible (1 ~ 12).
- L [url]	Configure la URL SIP (máx. 63 caracteres) para la línea directa.
- yo [habilitar]	Activar/desactivar la función de línea directa. 0 – deshabilitar 1 - habilitar
- W [habilitar]	Activar/desactivar la función de línea cálida. 0 – deshabilitar 1 - habilitar
- w [habilitar]	Activar/desactivar la función de activación de llamada en espera. 0 – deshabilitar 1 - habilitar
- E [habilitar]	Habilite / deshabilite la función de habilitar la llamada en espera, pero solo recuerde una vez. 0 – deshabilitar 1 - habilitar
- x <habilitar>	Activar/desactivar la función de transferencia de llamadas.

	0 – deshabilitar 1 - habilitar
- d [habilitar]	Habilitar/deshabilitar la función de DND (Do Not Disturb) 0 – deshabilitar 1 - habilitar
- s [identificación]	Indicar horario DND. Id - s1, s2, s3, s4 (máx. 4 horarios)
- h [habilitar]	Habilita/deshabilita la función de restricción de identificación de línea llamante (CLIR). 0 – deshabilitar 1 - habilitar
- tu [modo]	Configure el modo CLIR. 0 - significa "draft-ietf-sip-privacy" 1 - significa "rfc 3323/3325)"
- z [habilitar]	Activar/desactivar la reproducción del tono de marcación cuando se registra en el servidor SIP. 0 – deshabilitar 1 - habilitar
- n [habilitar]	Habilitar/deshabilitar el temporizador de sesión. 0 – deshabilitar 1 - habilitar
- m [seg]	Establezca el valor del temporizador de sesión (unidad: seg).
- R [mín, máx]	Establezca el rango de tiempo de gancho de flash 100 ~ 2000 (unidad: ms).
- 8 [habilitar]	Habilite o deshabilite la función de transmisión de fax T.38. 0 – deshabilitar 1 - habilitar
-V	Ver la configuración actual.
sorbo misc voip -Permite a los usuarios establecer configuraciones misceláneas para el dispositivo.	
- c [habilitar]	Habilite el encabezado compacto para acortar el paquete (0: deshabilitar, 1: habilitar).
- s [habilitar]	Cambie "#" a un número de dígito. 0 - deshabilitar 1 - habilitar
- e [habilitar]	Habilite el modo de operación de gancho de flash de estilo europeo. 0 - deshabilitar 1 - habilitar
- h [habilitar]	Habilitar/deshabilitar el modo de espera de llamadas basado en el protocolo RFC2543 (0: deshabilitar, 1: habilitar).
- yo [habilitar]	Habilite el cambio de CODEC sin Re-INVITE. 0 - deshabilitar 1 - habilitar
- p [habilitar]	Habilitar mensaje PRACK. 0: no es compatible con PRACK. 1 – Soporte PRACK.
- P [habilitar]	Habilitar llamada IP. 0: deshabilitar la llamada IP. 1 – Habilitar llamada IP.
- H [habilitar]	El paquete SIP INFO se enviará cuando se encuentre un evento de flash de gancho. 0 - deshabilitar 1 - habilitar
- t [valor]	Configure el modo de agente de usuario (por ejemplo, teléfono, software y dispositivo) para el paquete SIP.

	0 - Ocultar encabezado SIP "User-Agent". 1 - Mostrar encabezado SIP "User-Agent". 2 - Utilice el valor predeterminado de "Agente de usuario". 3 - Utilice el valor "User-Agent" definido por el usuario.
- u UAValor	Para cada agente de usuario SIP que se identifica con una cadena, este comando le permite establecer el valor (por ejemplo, dirección IP, número de teléfono, dirección de correo electrónico) de Agente de usuario. La longitud de la cadena debe ser inferior a 64 caracteres.
- D [deshabilitar]	Deshabilite el servicio de VoIP. 1 – deshabilitar el servicio de VoIP. 0: habilitar el servicio de VoIP. El sistema se reiniciará automáticamente para activar el servicio voip
-V	Ver el estado actual de las configuraciones misceláneas.
voip sorbo nat -Permite a los usuarios establecer la configuración transversal de NAT.	
- s [servidor]	Configure la dirección IP para el servidor STUN.
- t [seg]	Establezca el intervalo de ping para la cuenta SIP. Segundo – 6 ~ 600
- yo [ip]	Indicar dirección IP externa.
-V	Ver la configuración actual de SIP NAT.

Ejemplo

```
> voip sip misc -t 1 incluye
encabezado de agente de usuario

> voip sip misc -u 91704688carrie definido por el
usuario User-Agent:91704688carrie
> voip sorbo acc 1 -P carrie_1 -r 1 -d 172.16.3.133
> voip sorbo acc 1 -t 30
> voip sip misc -h 1
> voip sorbo acc 1 -v
índice                  :   1
perfil                  :   carrie_1
modo de registro        :   1 | registro [No]
alias_ip_idx                :   0
lista de respaldo           :
dominio                 :   172.16.3.133
apoderado               :     | saliente [No] | DNS-SRV [No] No
llamada no registrada   :
disipar Nombre          :
número de cuenta        :   - - -
aut. IDENTIFICACIÓN     :     | [desactivar]
expiración              :   3600
modo NAT                :   0
puertos de anillo       :   0
toque de anillo         :   1
modo de desvío de llamadas      :   0
url de desvío de llamada        :
temporizador de desvío de llamadas      :   30
Broadsoft:              desactivar
Modificación del ITSP italiano: deshabilitar
```

Comando Telnet: voip seguro

Este comando permite a los usuarios habilitar o deshabilitar la función de teléfono seguro y el mensaje de voz de SAS.

Sintaxis

voip seguro general*[-<comando> <parámetro> | ...]*

Sintaxis Descripción

Parámetro	Descripción
- mi <0/1>	Habilitar/deshabilitar la función de teléfono seguro. 0 - deshabilitar 1 - habilitar
- pag <0/1>	Habilitar/deshabilitar el aviso de voz SAS. 0 - deshabilitar 1 - habilitar
-V	ver solo la configuración general del teléfono seguro

Ejemplo

```
> VoIP Secure General -V La función de
teléfono seguro está deshabilitada El aviso de
voz de SAS está habilitado
> voip seguro general -p 0 El mensaje
de voz SAS está deshabilitado
```

Comando Telnet: grupo vlan

Este comando le permite configurar el grupo VLAN. Puede establecer cuatro grupos de VLAN. Por favor, corre *reiniciar vlan*después de cambiar cualquier configuración.

Sintaxis

grupo vlan*identificación<establecer/establecer_ex> <p1/p2/p3/p4/p5/s1/s2/s3/s4/5gs1/5gs2/5gs3/5gs4>*

Sintaxis Descripción

Parámetro	Descripción
identificación	Significa el grupo 0 a 7 para VLAN.
colocar	Indica que cada puerto puede unirse a más de un grupo de VLAN.
conjunto_ex	Indica que cada puerto puede unirse a un grupo de VLAN a la vez.
p1/p2/p3/p4/p5	Indica el puerto LAN 1 al puerto LAN 5. Para agrupar LAN1, LAN2, LAN3, LAN4 y/o LAN5 en un grupo de VLAN, escriba los números de puerto que desee.
s1/s2/s3/s4	Solo está disponible para los modelos WALN.
5gs1/5gs2/5gs3/5gs4	Solo está disponible para los modelos WALN n plus.

Ejemplo

```
> vlan grupo 3 conjunto p1 s3 s4
 VLAN p1 p2 p3 p4 s1                    s2    s3    s4 5gs1 5gs2 5gs3 5gs4
 ----------------------------------------------------------------------3
 V                                        vv
>
```

Comando Telnet: vlan desactivado

Este comando le permite deshabilitar la función VLAN.

Sintaxis

apagado

Ejemplo

```
> vlan apagado
  ¡VLAN está deshabilitada!
    ¡Fuerza la subred LAN2/3/4/5/6/7/8/9/10/11/12/13/14/15/16 para ser deshabilitada!
```

Comando Telnet: vlan activado

Este comando le permite habilitar la función VLAN.

Sintaxis

vlan en

Ejemplo

```
> vlan activado
  ¡VLAN está habilitada!
```

Comando Telnet: vlan pri

Este comando se utiliza para definir la prioridad de cada configuración de perfil de VLAN.

Sintaxis

vlan pri*n pri_no*

Sintaxis Descripción

Parámetro	Descripción
norte	Significa número de identificación de VLAN. n=Número de ID de VLAN (de 0 a 7).
pri_no	Significa la prioridad del perfil VLAN. pri_no=0 ~7 (desde ninguno hasta la prioridad más alta).

Ejemplo

```
> vlanpri 1 2
  VLAN1: Prioridad=2
```

Comando Telnet: reiniciar vlan

Este comando puede hacer que la configuración de VLAN se reinicie con la configuración más reciente.

Sintaxis

reiniciar vlan

Ejemplo

```
> reiniciar vlan? ¡¡¡VLAN
  se reinicia!!!
```

Comando Telnet: estado de vlan

Este comando muestra el estado actual de la VLAN.

Sintaxis

estado vlan

Ejemplo

```
> estado vlan
VLAN está deshabilitado:
-------------------------------------------------------------------------------
------
VLAN Habilitar VID Pri          p1 p2 p3 p4 p5 s1 s2 s3 s4 5gs1 5gs2 5gs3 5gs4 subred
-------------------------------------------------------------------------------
------
 0      APAGADO    0   0                                                  2:LAN2
 1      APAGADO    0   0                                                  1:LAN1
 2      APAGADO    0   0                                                  1:LAN1
 3      APAGADO    0   0    V                        V   V                 1:LAN1
 4      APAGADO    0   0                                                  1:LAN1
 5      APAGADO    0   0                                                  1:LAN1
 6      APAGADO    0   0                                                  1:LAN1
 7      APAGADO    0   0                                                  1:LAN1
 8      APAGADO    0   0                                                  1:LAN1
 9      APAGADO    0   0                                                  1:LAN1
10      APAGADO    0   0                                                  1:LAN1
11      APAGADO    0   0                                                  1:LAN1
12      APAGADO    0   0                                                  1:LAN1
13      APAGADO    0   0                                                  1:LAN1
14      APAGADO    0   0                                                  1:LAN1
15      APAGADO    0   0                                                  1:LAN1
-------------------------------------------------------------------------------
------
 Nota: solo se pueden desetiquetar para s1/s2/s3/s4/5gs1/5gs2/5gs3/5gs4, pero pueden unirse

n etiquete vlan con puertos lan.
 Permitir que el dispositivo sin etiquetar en P1 acceda al enrutador: ON....
```

Comando Telnet: subred vlan

Este comando se utiliza para configurar la interfaz LAN utilizada por el grupo VLAN.

Sintaxis

subred vlan group_id*<1/2/3/4/5/6/7/8>*

Sintaxis Descripción

Parámetro	Descripción
<1/2/3/4/5/6/7/8>	Significa interfaces, LAN1 ~ LAN8.

Ejemplo

```
> vlan subnet group_id 2 % Vlan
Group-0 usando LAN2                    !

 Esta configuración tendrá efecto después de reiniciar. Utilice el
 comando "sys reboot" para reiniciar el enrutador.
```

Comando Telnet: submodo vlan

Este comando cambia los mecanismos de encapsulación de VLAN en el controlador de LAN.

Sintaxis

submodo vlan *<encendido/apagado/estado>*

Sintaxis Descripción

Parámetro	Descripción
en	Significa habilitar el modo promiscuo.
apagado	Significa habilitar el modo normal.
estado	Significa mostrar si el submodo es el modo normal o el modo promiscuo.

Ejemplo

```
> estado del submodo vlan
% modo de subred vlan: modo normal
> submodo vlan activado
% modo de subred vlan modificado a modo promiscuo.
> estado del submodo vlan
% modo de subred vlan: modo promiscuo
```

Comando Telnet: vlan etiquetado

Este comando se usa para habilitar o deshabilitar la entrada de paquetes sin etiquetar.

Sintaxis

vlan etiquetado *<n> <activar/desactivar>* **vlan**

etiquetado *<ilimitado> <activar/desactivar>* **vlan**

etiquetado *<p1_untag> <activar/desactivar>*

Sintaxis Descripción

Parámetro	Descripción
<n>	Significa número de VLAN. El rango es de 0 a 15.
<activar/desactivar>	Significa habilitar/deshabilitar la VLAN etiquetada.
<ilimitado> <activar/desactivar>	Unlimited on: permite la entrada de paquetes sin etiquetar, incluso si todas las VLAN están etiquetadas. Desactivado ilimitado: No permite la entrada de paquetes sin etiquetar.
<p1_untag> <activar/desactivar>	P1_untag on: Permite la entrada de paquetes sin etiquetar desde el puerto LAN 1. P1_untag off: No permite la entrada de paquetes sin etiquetar desde el puerto LAN 1.

Ejemplo

```
> vlan etiquetado ilimitado en
  Modo ilimitado está activado
>
```

Comando Telnet: vlan vid

Este comando se usa para configurar el número de VID para cada canal VLAN.

Sintaxis

vídeo vlan *<n> <vid_no>*

Sintaxis Descripción

Parámetro	Descripción
<n>	Significa canal VLAN. El rango es de 0 a 7.
<vid_no>	Significa el valor de ID de VLAN. Escriba el valor como el número de ID de VLAN. El rango es de 0 a 4095.

Ejemplo

```
> vlan vídeo 1 4095
  VLAN1, vídeo=4095
```

Comando Telnet: vlan sysvid

Este comando se utiliza para modificar y mostrar el alcance (reservado 78) de los ID de VLAN utilizados internamente por el sistema.

Sintaxis

vlan sysvid*<mostrar / n>*

Sintaxis Descripción

Parámetro	Descripción
espectáculo	Significa mostrar el alcance de la ID de VLAN utilizada internamente.
norte	Significa el valor que se establecerá como ID de VLAN. El rango es de 0 a 3980.

Ejemplo

```
> vlan sysvid 100
  Ha establecido el ID de VLAN del sistema en el rango: 100 ~ 215.
  Le recomendamos que reinicie el sistema ahora.

> vlan sysvid200
  Ha establecido el ID de VLAN del sistema en el rango: 200 ~ 315.
  Le recomendamos que reinicie el sistema ahora.
> mostrar vlan sysvid
  El ID de VLAN del sistema está dentro del rango: 200 ~ 263
```

Comando Telnet: vpn l2lset

Este comando permite a los usuarios establecer parámetros avanzados para la función LAN a LAN.

Sintaxis

vpn l2lset*<índice de lista>***peidid***<ID de usuario>*

vpn l2lset*<índice de lista>***ID local***<localid>*

vpn l2lset*<índice de lista>***principal***<índice de auto/propuesta>*

vpn l2lset*<índice de lista>***agresivo***<desg1/desg2/aesg1/aesg2/aesg5/aesg14>* **vpn l2lset***<índice de lista>***por favor***<encendido/apagado>* **vpn l2lset***<índice de lista>***fase***1 <vida>* **vpn l2lset***<índice de lista>***fase 2***<toda la vida>* **vpn l2lset***<índice de lista>***x509localid***<0/1>* **vpn l2lset***<índice de lista>***comprimir***<0/1/2/3>*

Sintaxis Descripción

Parámetro	Descripción
<índice de lista>	Significa el número de índice del perfil L2L (LAN a LAN).
ID de usuario <identificador de usuario>	Significa la identidad de pares para el modo agresivo.
localid <localid>	Significa la identidad local para el modo agresivo.
principal <auto/índice de propuesta>	Significa elegir la propuesta para el modo principal. <auto>: elige propuestas predeterminadas. <índice de propuesta>: elija la propuesta especificada.
agresivo <desg1/desg2/aesg1/aesg2/ aesg5/aesg14>	Significa el grupo DH elegido para el modo agresivo.
pfs <activar/desactivar>	Significa "secreto perfecto hacia adelante". <on/ off>: activa o desactiva la función PFS.
fase1 <vida útil> / fase2 <vida útil>	Significa fase 1 o 2 de IKE. <vida útil>: establece el valor de vida útil (en segundos) para la fase 1 y la fase 2.
x509localid <0/1>	Significa habilitar (1) o deshabilitar (0) el ID local X509.
comprimir <0/1/2/3>	Seleccione un método para comprimir los paquetes para reducir el uso de ancho de banda mientras transfiere los paquetes comprimidos. <0/1/2/3> - Los valores disponibles son: 0 : Desactiva la función de compresión. 1: No. Utilice el método adaptativo para la compresión de paquetes. 2: LZ4. Utilice el algoritmo de LZ4 para la compresión de paquetes. 3: LZO. Para uso futuro.

Ejemplo

```
> VPN l2lset 1 peerid 10226
```

Comando Telnet: vpn l2lDrop

Este comando permite a los usuarios finalizar la conexión actual de LAN a LAN VPN.

Sintaxis

vpn l2lDrop*l2lname <nombre>*
vpn l2lDrop*l2lidx <idx>* **vpn**
l2lDrop*h2lname <nombre>* **vpn**
l2lDrop*h2idx <idx>* **vpn l2lDrop***<*
si no> **vpn l2lDrop**

Sintaxis Descripción

Parámetro	Descripción
l2lname <nombre>	Significa desconectar la conexión VPN especificando el nombre del perfil de LAN a LAN.
l2lidx <idx>	Significa desconectar la conexión VPN especificando el número de índice del perfil de LAN a LAN.
h2lname <nombre>	Significa interrumpir la conexión VPN especificando el nombre del perfil de usuario de marcado remoto.
h2idx <idx>	Significa desconectar la conexión VPN especificando el número de índice del perfil de usuario de marcado remoto.

<si no>	Significa desconectar la conexión VPN usando VPN ifno.
l2lDrop	Significa abandonar todas las conexiones VPN.

Ejemplo

```
> vpn l2lDrop
  Descartar todas las VPN
```

Comando Telnet: vpn l2lDialout

Este comando permite a los usuarios finalizar la conexión actual de LAN a LAN VPN (marcación de salida).

Sintaxis

vpn l2lDialout*<idx>*
vpn l2lDialout*lista*

Sintaxis Descripción

Parámetro	Descripción
l2lDialout <idx>	Significa crear una conexión VPN especificando el número de índice del perfil de LAN a LAN de marcación de salida. <idx>: Ingrese un número de índice (1 a 64).
lista	Significa mostrar perfiles de LAN a LAN (habilitado).

Ejemplo

```
> VPN l2lLista de llamadas
  Mostrar perfiles de LAN a LAN del estado como Habilitar estado
de perfil de índice
```

Comando Telnet: vpn dinset

Este comando permite a los usuarios configurar los ajustes para el perfil VPN de marcación remota.

Sintaxis

precio vpn*<índice de lista>*

precio vpn*<índice de lista> <activar/desactivar>*

precio vpn*<índice de lista>***nombre de usuario***<NOMBRE DE USUARIO>* **precio vpn***<índice de lista>***contraseña***<CONTRASEÑA>*

precio vpn*<índice de lista>***motp***<encendido/apagado>*

precio vpn*<índice de lista>***pin_secreto***<pin> <secreto>* **precio vpn***<índice de lista>***se acabó el tiempo***<0~9999>* **precio vpn***<índice de lista>***tipo de sonido***<Tipo> <activar/desactivar>* **precio vpn***<índice de lista>***subred***<0~8>* **precio vpn***<índice de lista>***asignacion***<encendido/apagado>* **precio vpn***<índice de lista>***srnodo***<encendido/apagado>*

precio vpn*<índice de lista>***IP remota***<Dirección_IP_de_Cliente_Remoto>* **precio vpn***<índice de lista>***par***<Peer_ID>* **precio vpn***<índice de lista>***nombrando***<pasar/bloquear>* **precio vpn***<índice de lista>***multicastvpn***<pasar/bloquear>*

precio vpn*<índice de lista>***preclave***<encendido/apagado>*

precio vpn*<índice de lista>***asignar clave***<Pre_Shared_Key>*

precio vpn *<índice de lista>* **cavar** *<encendido/apagado>*

precio vpn *<índice de lista>* **ipsec** *<Método> <activar/*

desactivar> **precio vpn** *<índice de lista>* **ID local** *<ID_local>*

Sintaxis Descripción

Parámetro	Descripción
<índice de lista>	Significa el número de índice del perfil.
<índice de lista> <activar/desactivar>	Significa habilitar o deshabilitar el perfil. <índice de lista>: ingrese el número de índice del perfil de VPN. <encendido/apagado> - encendido: Habilitar; apagado: deshabilitar.
<índice de lista> motp <activar/desactivar>	Significa habilitar o deshabilitar la autenticación con la función mOTP. <índice de lista>: ingrese el número de índice del perfil de VPN. <encendido/apagado> - encendido: Habilitar; apagado: deshabilitar.
<índice de lista> pin_secret<pin> <secreto>	Significa establecer el código PIN con secreto. <índice de lista>: ingrese el número de índice del perfil de VPN. <pin>-Escriba el código de autenticación (p. ej., 1234). <secreto>-Use el número secreto de 32 dígitos generado por mOTP en el teléfono móvil (p. ej., e759bb6f0e94c7ab4fe6)
<índice de lista> tiempo de espera <0~9999>	Significa establecer el tiempo de inactividad. El valor predeterminado es 300 (segundos). <índice de lista>: ingrese el número de índice del perfil de VPN. < 0~9999>-Introduzca un valor.
<índice de lista> dintype <Tipo> <activar/ desactivar>	Significa habilitar/deshabilitar el tipo de acceso telefónico permitido. <índice de lista>: ingrese el número de índice del perfil de VPN. <Tipo> - 0 a 3. En el cual, 0 significa PPTP; 1 significa Túnel IPsec; 2 significa L2TP con política IPsec; 3 significa Túnel SSL. <encendido/apagado> - encendido: Habilitar; apagado: deshabilitar.
vpn dinset <índice de lista> subred <0~8>	Significa configurar la subred LAN para el perfil VPN seleccionado. <índice de lista>: ingrese el número de índice del perfil de VPN. <0~8>: ingrese un número para especificar la subred LAN. En el cual, 0 significa LAN1 1 significa LAN2 2 significa LAN3 3 significa LAN4 4 significa LAN5 5 significa LAN6 6 significa LAN7 7 significa LAN8 8 significa DMZ
vpn dinset <índice de lista> asignacion <activar/desactivar>	Significa habilitar o deshabilitar la función de asignación de la dirección IP estática. <índice de lista>: ingrese el número de índice del perfil de VPN. <encendido/apagado> - encendido: Habilitar; apagado: deshabilitar.
vpn dinset <índice de lista> srnode <activar/desactivar>	Significa habilitar o deshabilitar la función de especificar el nodo remoto. <índice de lista>: ingrese el número de índice del perfil de VPN. <encendido/apagado> - encendido: Habilitar; apagado: deshabilitar.
vpn dinset <índice de lista> remoteip	Significa habilitar o deshabilitar la función de asignación de IP de cliente remoto.

<dirección_IP_del_cliente_remoto >	<índice de lista>: ingrese el número de índice del perfil de VPN. <Remote_Client_IP_Address>: establezca la dirección IP del cliente remoto.
vpn dinset <índice de lista> peer <Peer_ID>	Significa asignar la ID del par. <índice de lista>: ingrese el número de índice del perfil de VPN. <Peer_ID>: ingrese la cadena de la ID del par.
vpn dinset <índice de lista> naming <contraseña/bloque>	Significa configurar el paquete de nombres de Netbiod para el perfil VPN. <índice de lista>: ingrese el número de índice del perfil de VPN. <pasar/ bloquear>: deja pasar el paquete o bloquea el paquete.
vpn dinset <índice de lista> multicastvpn <contraseña/bloqueo>	Significa configurar la multidifusión a través de VPN para IGMP, IP-CAM, relé DHCP, etc. <índice de lista>: ingrese el número de índice del perfil de VPN. <pasar/bloquear>: deja pasar el paquete o bloquea el paquete.
vpn dinset <índice de lista> preclave <on/off>	Significa habilitar/deshabilitar la configuración de clave precompartida para el método de autenticación IKE. <índice de lista>: ingrese el número de índice del perfil de VPN. <encendido/apagado> - encendido: Habilitar; apagado: deshabilitar.
vpn dinset <índice de lista> asignar clave <Pre_Shared_Key>	Significa configurar la clave precompartida para el método de autenticación IKE. <índice de lista>: ingrese el número de índice del perfil de VPN. <Pre_Shared_Key>: ingrese una cadena como PSK.
vpn dinset <índice de lista> digsig <activar/desactivar>	Significa habilitar/deshabilitar la firma digital (X.509) para el método de autenticación IKE. <índice de lista>: ingrese el número de índice del perfil de VPN. <encendido/apagado> - encendido: Habilitar; apagado: deshabilitar.
vpn dinset <índice de lista> ipsec <Método> <activar/desactivar>	Significa habilitar/deshabilitar y configurar el protocolo para el método de seguridad IPsec. <índice de lista>: ingrese el número de índice del perfil de VPN. <Método>: ingrese un número (0 a 3) para especificar el protocolo. 0 significa Medio (AH) Alto (ESP), 1 significa DES 2 significa 3DES 3 significa AES <encendido/apagado> - encendido: Habilitar; apagado: deshabilitar.
vpn dinset <índice de lista> localid <ID_local>	Significa configurar la identificación local (opcional) para el método de seguridad IPsec. <índice de lista>: ingrese el número de índice del perfil de VPN. <local_ID>: ingrese la cadena de identificación local.

Ejemplo

```
> vpn dinset 1
Índice de perfil de acceso telefónico
1 Nombre de perfil: ???
Estado: Desactivado
OTP móvil: deshabilitado
Contraseña:
Tiempo de espera inactivo: 300 segundos
> vpn dinset 1 en %
establecer perfil activo
> vpn dinset 1 motp en % ¡Habilitar
el modo OTP móvil!>
> vpn dinset 1 pin_secret 1234 e759bb6f0e94c7ab4fe6
> vpn dinset 1
Índice de perfil de acceso telefónico
1 Nombre de perfil: ???
```

Estado: Activo
OTP móvil: Habilitado
PIN: 1234
Secreto: e759bb6f0e94c7ab4fe6 Tiempo de
espera inactivo: 300 segundos

Comando Telnet: subred vpn

Este comando permite a los usuarios especificar una selección de subred para el perfil de VPN de marcado remoto especificado.

Sintaxis

subred vpn *<índice><1/2/3/4/5/6/7/8>*

Sintaxis Descripción

Parámetro	Descripción
<índice>	Significa el número de índice del perfil VPN.
<1/2/3/4/5/6/7/8>	1 – significa LAN1 2 – significa LAN2. 3 – significa LAN3 4 – significa LAN4. 5 – significa LAN5 6 – significa LAN6. 7 – significa LAN7. 8 – significa LAN8.

Ejemplo

```
> subred vpn 1 2
>
```

Comando Telnet: configuración de VPN

Este comando permite a los usuarios configurar VPN para diferentes tipos.

Sintaxis

Comando de marcación de salida PPTP

configuración vpn *<índice> <nombre>* **pptp_fuera** *<ip> <usr> <contraseña> <nip> <nmask>*

Comando de IPSec Dial-Out

configuración vpn *<índice> <nombre>* **salida_ipsec** *<ip> <clave> <nip> <nmáscara>*

Comando de L2Tp Dial-Out

configuración vpn *<índice> <nombre>* **l2tp_fuera** *<ip> <usr> <contraseña> <nip> <nmask>* **Comando de acceso telefónico**

configuración vpn *<índice> <nombre>* **Marcar** *<ip> <usr> <contraseña> <clave> <nip> <nmask>*

Comando de 6in4

configuración vpn *<índice> <nombre>* **6 en 4** *<habilitar> <lan> <rem_lan_ip> <lan_pfx> <pfx_len><rem_pfx> <pre_len> <ttl>*

Sintaxis Descripción

Parámetro	Descripción

Para marcación de salida PPTP	
<índice>	Significa el número de índice del perfil.
<nombre>	Significa el nombre del perfil.
<ip>	Significa la dirección IP para marcar.
<usr> <contraseña>	Significa el usuario y la contraseña requerida para la conexión PPTP.
<pellizcar> <nmáscara>	Significa la IP de la red remota y la máscara. p.ej, configuración vpn 1 nombre1 pptp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
Para marcación IPsec	
<índice>	Significa el número de índice del perfil.
<nombre>	Significa el nombre del perfil.
<ip>	Significa la dirección IP para marcar.
<clave>	Significa el valor de la clave precompartida IPsec.
<pellizcar> <nmáscara>	Significa la IP de la red remota y la máscara. p.ej, configuración vpn 1 nombre1 ipsec_out 1.2.3.4 1234 192.168.1.0 255.255.255.0
Para marcación de salida L2TP	
<índice>	Significa el número de índice del perfil.
<nombre>	Significa el nombre del perfil.
<ip>	Significa la dirección IP para marcar.
<usr> <contraseña>	Significa el usuario y la contraseña necesarios para la conexión L2TP.
<pellizcar> <nmáscara>	Significa la IP de la red remota y la máscara. p.ej,, configuración vpn 1 nombre1 l2tp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
Para acceso telefónico	
<índice>	Significa el número de índice del perfil.
<nombre>	Significa el nombre del perfil.
<ip>	Significa la dirección IP permitida para marcar.
<usr> <contraseña>	Significa el usuario y la contraseña necesarios para la conexión PPTP/L2TP.
<clave>	Significa el valor de la clave precompartida IPsec.
<pellizcar> <nmáscara>	Significa la IP de la red remota y la máscara. p.ej, configuración vpn 1 nombre1 marcación 1.2.3.4 vigor 1234 abc 192.168.1.0 255.255.255.0
Para 6 en 4	
<índice>	Significa el número de índice del perfil.
<nombre>	Significa el nombre del perfil.
<habilitar>	Significa habilitar (1) o deshabilitar (0) el perfil.
<lan>	Elija la interfaz LAN (0 a 16) o DMZ (17).
<rem_lan_ip>	Significa especificar la dirección IP de LAN remota.
<lan_pfx>	Significa establecer el prefijo LAN IPv6.
<pfx_len>	Significa establecer la longitud del prefijo IPv6 (32 a 128).

<rem_pfx>	Significa establecer un prefijo IPv6 remoto.
<pre_len>	Significa establecer la longitud del prefijo IPv6 remoto (32 a 128).
<ttl>	Significa configurar el túnel TTL (1 a 255). Ex. configuración vpn 1 nombre1 6in4 1 1 192.168.10.1 193:: 64 192:: 64 255

Ejemplo

```
> vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0 255.255.255.0 % Registro de cambios de perfil...

% Índice de perfil: 1 %
Nombre de perfil: nombre1 %
Nombre de usuario: vigor %
Contraseña: 1234
% Clave precompartida: abc % Dirección de
la llamada: Acceso telefónico
% Tipo de Servidor : ISDN PPTP IPSec L2TP % Marcar
desde : 1.2.3.4
% IP de red remota: 192.168.1.0 % Máscara de red
remota: 255.255.255.0
>
```

Comando Telnet: opción vpn

Este comando permite a los usuarios configurar los ajustes para el perfil de LAN a LAN.

Sintaxis

opcion vpn *<índice> <cmd1>=<param1> [<cmd2>=<param2> | ...]*

Sintaxis Descripción

Parámetro	Descripción
<índice>	Significa el número de índice del perfil. Números de índice disponibles: 1 ~ 32
Para configuraciones comunes	
<índice>	Significa el número de índice del perfil.
pname	Significa el nombre del perfil.
ena	Significa habilitar o deshabilitar el perfil. encendido – Habilitar apagado - Deshabilitar
thr	Significa la forma en que pasa la conexión VPN. Los ajustes disponibles son wlf, wlo, w2f, w2o y .... w1f – WAN1 Primero. w1o: solo WAN1. w2f – WAN2 Primero. w2o: solo WAN2. w1oB: solo WAN1 (solo establecer VPN si WAN2 está inactivo) w2oB: solo WAN2 (solo establecer VPN si WAN1 está inactivo)
thr_ai	Significa conexión a través de un alias de IP wan. 0 - no usar alias. 1/2/.../31 - Utilice el alias IP (número de índice 1 a 31).

nnpkt	Significa el paquete de nombres de NetBios. on: activa la función para pasar el paquete. off: deshabilita la función para bloquear el paquete.
directorio	Significa la dirección de la llamada. Los ajustes disponibles son b, o e i. b – Ambos o – Llamada de salida i – Acceso telefónico.
inactivo	Significa Siempre encendido y Tiempo de espera inactivo. Los valores disponibles incluyen: - 1: significa que siempre está activado para llamadas de salida. 0: significa que siempre está activado para marcar. Otros números (por ejemplo, inactivo = 200, inactivo = 300, inactivo = 500) significan que el enrutador estará inactivo después del intervalo (segundos) configurado aquí.
pálido	Significa permitir que PING se mantenga vivo. - 1 – deshabilitar la función. 1,2,3,4: habilite la función y PING IP 1.2.3.4 para mantener vivo.
monitor	Significa habilitar el Monitoreo de Calidad. Activado: active el control de calidad. Desactivado: desactiva el control de calidad.
Para la configuración de marcación de salida	
ctipo	Significa "Tipo de servidor al que estoy llamando". ctype=t significa PPTP. ctype=s significa IPSec. ctype= l significa L2TP (Política IPSec Ninguna). ctype= l1 significa L2TP (política IPSec agradable de tener). ctype= l2 significa L2TP (Política IPSec Obligatoria). ctype= c significa Túnel SSL ctype=o [0/1/2/3/4/5] [0/1/2/3] significa Openvpn TCP Tunnel[AES128/ AES256/NONE/AES128_GCM/AES192_GCM/AES256_ GCM] [SHA1/ SHA256/NONE/ SHA512] ctype= u[0/1/2/3/4/5][0/1/2/3] significa Openvpn UDP Tunnel[AES128/ AES256/NONE/AES128_GCM/AES192_GCM/AES256_ GCM][SHA1/ SHA256/NONE/ SHA512]
marcar	Significa Servidor IP/Nombre de host para VPN. (como draytek.com o 123.45.67.89).
tipo	Significa Tipo de enlace. “ltype=0” significa “Deshabilitar”. “ltype=1” significa “64kbps”. “ltype=2” significa “128kbps”. “ltype=3” significa “DBO”.
un nombre	Significa Nombre de usuario de marcación de salida. “oname=admin” significa establecer Nombre de usuario = admin.
opwd	Significa Contraseña de marcación de salida "opwd = 1234" significa establecer Contraseña = 1234.
camino	Significa autenticación PPP. “pauth=pc” significa establecer Autenticación PPP = PAP&CHAP. “pauth=p” significa establecer Autenticación PPP = Solo PAP
ovj	Significa compresión VJ. “ovj=on/off” significa activar/desactivar la compresión VJ.
bueno	Significa clave precompartida IKE. “okey=abcd” significa configurar la clave precompartida de IKE = abcd.
meta	Significa Método de seguridad IPSec.

	“ometh=ah[a/s/S]” significa AH auto/sha1/Sha2. “ometh=espd/espda[a/s/S/” significa ESP DES sin/con autenticación automática/sha1/Sha2 “ometh=esp3/esp3a[a/s/S]/” significa ESP 3DES sin/con autenticación automática/sha1/Sha2 “ometh= espa[1/9/2]/espaa[a/s/S][1/9/2] ” significa ESP AES[128/192/256] sin/con Autenticación auto/sha1/Sha2 (AES128/ 192/256).
tls_auth	Significa Activar/desactivar la opción tls-auth.
tls_auth_key	Significa configurar la clave de opción OpenVPN tls-auth. tls-auth_key=<1/2/3> Introduzca el número para seleccionar el PSK.
tls_key_show	Significa mostrar el PSK seleccionado.
sch	Significa Índice (1-15) en Configuración de programación. sch=1,3,5,7 Establecer horario 1->3->5->7
modo ike	Significa modo IKE fase 1. ikemode=m, Modo principal. ikemode=a, Modo agresivo.
ikeid	Significa identificación local de IKE. “ikeid=vigor” significa Establecer ID local = vigor.
Oporto	Significa puerto de acceso telefónico OpenVPN. puerto=1194. Establezca el puerto de acceso telefónico OpenVPN = 1194
Para la configuración de acceso telefónico	
yo tecleo	Significa Tipo de acceso telefónico permitido. Las configuraciones disponibles incluyen: “type=t” significa PPTP. “type=s” significa IPSec. “tipo=L” significa L2TP (Ninguno). “type=l1” significa L2TP (agradable de tener). "tipo = l2" significa L2TP (debe). “type=c” significa Túnel SSL “type=i” significa Openvpn UDP/TCP “type=i[0/1/2][0/1/2]" significa Túnel[AES128/AES256/ NINGUNO][SHA1/SHA256/NINGUNO]/ “type=o[0/1/2][0/1/2]” significa Openvpn TCP Tunnel[AES128/AES256/NONE][SHA1/SHA256/NONE]/ “tipo=u[0/1/2][0/1/2]” significa Openvpn Túnel UDP[AES128/ AES256/NINGUNO][SHA1/SHA256/NINGUNO]
par	Significa especificar la IP del servidor Peer VPN para Remote VPN Gateway. Escriba "203.12.23.48" significa permitir el marcado de VPN con la dirección IP de 203.12.23.48. Escriba "apagado" significa que cualquier IP remota puede marcar.
peidid	Significa la ID de par para Remote VPN Gateway. Escriba "draytek" significa que la palabra se usa como identificación local.
nombre	Significa Nombre de usuario de acceso telefónico. “iname=admin” significa establecer el nombre de usuario como “admin”.
ipwd	Significa Contraseña de acceso telefónico. “ipwd=1234” significa establecer la contraseña como “1234”.
ivj	Significa compresión VJ. “ivj=on/off” significa activar/desactivar la compresión VJ.
clave	Significa clave precompartida IKE. “ikey=abcd” significa configurar la clave precompartida de IKE = abcd.
imeth	Significa Método de seguridad IPSec

	"imeth=h" significa "Permitir AH". "imeth=d" significa "Permitir DES". "imeth=3" significa "Permitir 3DES". "imeth=a" significa "Permitir AES.
Para la configuración de TCP/IP	
miwip	Significa Mi IP WAN. "mywip=1.2.3.4" significa configurar Mi IP WAN como "1.2.3.4".
rgip	Significa IP de puerta de enlace remota. "rgip=1.2.3.4" significa configurar la IP de la puerta de enlace remota como "1.2.3.4".
cortar	Significa IP de red remota. "rnip=1.2.3.0" significa configurar la IP de red remota como "1.2.3.0".
rnmask	Significa Máscara de red remota. "rnmask=255.255.255.0" significa configurar la máscara de red remota como "255.255.255.0".
lnip	Significa IP de red local. "lnip=1.2.3.0" significa configurar la IP de red local como "1.2.3.0".
máscara	Significa Máscara de red local. "lnmask=255.255.255.0" significa configurar la máscara de red local como "255.255.255.0".
rotura	Significa Dirección RIP. "rip=d" significa configurar la Dirección RIP como "Deshabilitar". "rip=t" significa establecer la Dirección RIP como "TX". "rip=r" significa establecer la Dirección RIP como "RX". "rip=b" significa establecer la Dirección RIP como "Ambos".
modo	Significa la opción de "Desde la primera subred a la red remota, lo que tienes que hacer". "mode=r" significa establecer el modo de ruta. "mode=n" significa configurar el modo NAT.
druta	Significa cambiar la ruta predeterminada a este túnel VPN (solo una WAN única admite esto). droute=on/off significa activar/desactivar la función.

Ejemplo

```
> vpn opción 1 inactivo = 250 %
Cambiar registro ..

% de tiempo de espera inactivo = 250
```

Comando Telnet: vpn mroute

Este comando permite a los usuarios enumerar, agregar o eliminar rutas estáticas para un determinado perfil de LAN a LAN VPN.

Sintaxis

mruta vpn *<índice>* **lista**
mruta vpn *<índice>* **agregar** *<IP de red>/<máscara>*
mruta vpn *<índice>* **del** *<IP de red>/<máscara>*

Sintaxis Descripción

Parámetro	Descripción
lista	Significa mostrar todos los ajustes de la ruta.

agregar	Significa agregar una nueva ruta.
del	Significa eliminar la ruta especificada.
<índice>	Significa el número de índice del perfil. Números de índice disponibles: 1 ~ 32
<ip de red>/<máscara>	Introduzca la dirección IP con la dirección de la máscara de red.

Ejemplo

```
> vpn mroute 1 agregar 192.168.5.0/24 %
192.168.5.0/24
% Agregar nueva ruta 192.168.5.0/24 al perfil 1
```

Comando Telnet: lista vpn

Este comando permite a los usuarios ver los perfiles VPN de LAN a LAN.

Sintaxis

lista vpn*<índice>***toda la**

lista de vpn*<índice>***lista**

com vpn*<índice>***fuera de la**

lista de vpn*<índice>***en la**

lista de vpn*<índice>***neto**

Sintaxis Descripción

Parámetro	Descripción
todo	Significa enumerar la configuración del perfil especificado.
com	Significa listar configuraciones comunes del perfil especificado.
afuera	Significa enumerar la configuración de marcación de salida del perfil especificado.
en	Significa enumerar la configuración de acceso telefónico del perfil especificado.
neto	Significa enumerar la configuración de red del perfil especificado.
<índice>	Significa el número de índice del perfil. Números de índice disponibles: 1 ~ 32

Ejemplo

```
> lista vpn 32 todos %
Configuraciones comunes

% Nombre de perfil                : ???
% Estado del perfil               : Desactivar
% Paquete de nombres de Netbios   : Aprobar
% Dirección de llamada            : Ambos
% Tiempo de inactividad           : 300
% PING para mantener vivo         : apagado

% Configuración de marcación de salida

% Tipo de servidor %              : PPTP
Tipo de enlace:                   : 64kbps
% Nombre de usuario               : ???
```

```
% Contraseña                    :
% de autenticación PPP          : PAP/CHAP
% Compresión VJ                 : en
% clave precompartida           :
% Método de seguridad IPSec     : Ah
% Horario                       : 0,0,0,0
% de devolución de llamada remota : apagado
% Proporcione el número         : apagado
ISDN % Modo de fase 1 de IKE    : modo principal
% ID local de IKE               :


% Configuración de acceso telefónico

- - - MÁS --- ['q': Salir, 'Entrar': Líneas nuevas, 'Barra espaciadora': Página siguiente] ---
> lista vpn 1 com %
Configuración común

% Nombre de perfil              : ???
% Estado del perfil             : Desactivar
% Paquete de nombres de Netbios : Aprobar
% Dirección de llamada          : Ambos
% Tiempo de inactividad         : 300
% PING para mantener vivo       : apagado
>
```

Comando Telnet: vpn remoto

Este comando permite a los usuarios habilitar o deshabilitar *PPTP/IPSec/L2TP* servicio VPN.

Sintaxis

vpn control remoto *<PPTP/IPsec/L2TP/SSLVPN> <activar/desactivar>*

Sintaxis Descripción

Parámetro	Descripción
PPTP/IPSec/L2TP/SSLVPN	Se pueden seleccionar cuatro tipos.
encendido apagado	on: habilita la configuración remota de VPN. off: deshabilita la configuración remota de VPN.

Ejemplo

```
> vpn PPTP remoto activado
Establecer servicio VPN PPTP: Activado

¡Reinicia el enrutador!
```

Comando Telnet: troncal vpn

Este comando permite a los usuarios configurar la copia de seguridad de VPN, el equilibrio de carga de VPN, GRE sobre IPsec y la política de túnel de enlace.

tronco vpn show_usable

copia de seguridad del tronco vpn *<agregar/eliminar> <nombre> <Miembro#1> <Miembro#2>* **copia de seguridad del tronco vpn more_syslog** *<ENCENDIDO/APAGADO>*

vpn tronco copia de seguridad ERD *<nombre> <Normal/Recuperar/Reanudar><segundo>*

vpn troncal lb *<agregar/eliminar> <nombre> <Miembro#1> <Miembro#2>* **vpn troncal lb more_syslog** *<ENCENDIDO/APAGADO>* **algoritmo vpn trunk lb** *<nombre> <RR>*

algoritmo vpn trunk lb *<nombre><W-RR><Auto> <Según relación> <Miembro1:Miembro2>* **algoritmo vpn trunk lb** *<nombre><Más rápido>* **uso de enlace de tronco vpn** *<Índice de enlace>* **demostración del enlace del tronco vpn** *<Nombre de equilibrio de carga>* **enlace troncal vpn reset_default**

enlace troncal vpn more_syslog *<ENCENDIDO/APAGADO>*

conjunto de enlaces troncales vpn *<BindIndex> <ACT> <TrunkName> <Miembro> <SrcIp:A~B> <DstIp:A~B> <DstPort:A~B> <Proto> <Frag>*

inserto de enlace de tronco vpn *<After_BindIndex> <ACT> <TrunkName> <Miembro> <SrcIp:A~B> <DstIp:A~B> <DstPort:A~B> <Proto> <Frag>*

vpn troncal SetGre show *<Índice_de_llamadas>*

tronco vpn SetGre *<Activo/Inactivo><Dialout_Index><GRE_MyIP><GRE_PeerIP><Logical_Traffic>*

troncal vpn An_Gre GreIPsecAnalyze *<ENCENDIDO/APAGADO>*

Sintaxis Descripción

Parámetro	Descripción
mostrar_usable	Muestra una lista de perfiles de marcación de LAN a LAN.
copia de seguridad <agregar/eliminar> <nombre> <Miembro n.º 1> <Miembro n.º 2>	Establezca múltiples túneles VPN (perfiles de LAN a LAN) como túnel de respaldo. agregar/eliminar-Agregue o elimine un perfil para usar en VPN Trunk. nombre: especifique el nombre del tronco VPN. Member#1: indica el primer perfil de LAN a LAN. Miembro n.º 2: indica el segundo perfil de LAN a LAN.
copia de seguridad more_syslog <ENCENDIDO/APAGADO> *lb more_syslog <ENCENDIDO/APAGADO> bind more_syslog <ENCENDIDO/APAGADO>*	Estos comandos se utilizan para la depuración de RD.
respaldo ERD <nombre> <Normal/Recuperar/Reanudar> <segundo>	ERD significa Medio Ambiente Recupera Detección. nombre: especifique el nombre del tronco VPN. Normal: indica el modo Normal. Todos los perfiles de copia de seguridad de VPN TRUNK de marcación de salida se activarán alternativamente. Recuperar: indica la duración de la operación de copia de seguridad de VPN. Reanudar: cuando la conexión VPN se rompe o se desconecta, el Miembro 1 será la máxima prioridad para que el sistema realice la conexión VPN. Segundo: "0" significa marcar cada seis segundos automáticamente. "60 ~ 2147483647" significa manejo temprano por menos de 30 segundos dentro del tiempo designado.
lb <agregar/eliminar> <nombre> <Miembro#1> <Miembro#2>	Significa crear un tronco VPN con equilibrio de carga. agregar/eliminar-Agregue o elimine un perfil para usar en VPN Trunk. nombre: especifique el nombre del tronco VPN.

	Member#1: indica el primer perfil de LAN a LAN. Miembro n.º 2: indica el segundo perfil de LAN a LAN.
algoritmo lb <nombre> <RR/W-RR/Más rápido>	Establezca múltiples túneles VPN para usar como túnel de equilibrio de carga de tráfico. Dicho comando es para configurar el algoritmo (con modo round robin) de Load Balance. nombre: especifique el nombre del tronco VPN. RR – Significa modo round robin. Todos los perfiles de marcación se turnarán por igual.
algoritmo lb <nombre><W-RR><Auto> <SegúnRatio> <Miembro1:Miembro2>	Dicho comando es para configurar el algoritmo (con modo round robin) de Load Balance. nombre: especifique el nombre del tronco VPN. W-RR: significa mod ponderado de todos contra todos basado en la relación de velocidad. - *Automático: la velocidad debe basarse en Lay2. Según relación: la velocidad* - *debe basarse en una relación determinada.* Miembro n.º 1: indica el primer perfil de LAN a LAN. Member#2: indica el segundo perfil de LAN a LAN.
algoritmo lb <nombre><el más rápido>	Dicho comando es para configurar el algoritmo (con el modo más rápido) de Load Balance. La mayoría de los tráficos se dirigirán al canal con la conexión más rápida. nombre: especifique el nombre del tronco VPN.
uso de enlace <BindIndex>	Muestre información detallada para el enlace de túnel de equilibrio de carga de VPN. BindIndex: indica el número de índice del enlace del túnel.
espectáculo de enlace <Nombre de equilibrio de carga>	Muestra la información de vinculación para el perfil de Equilibrio de carga de VPN. LoadBalanceName: escriba el nombre del perfil de equilibrio de carga de VPN
vincular reset_default	Restablezca el túnel de vinculación para el equilibrio de carga de VPN a la configuración de restablecimiento de fábrica.
bind set <BindIndex> <ACT> <TrunkName> <Miembro> <SrcIp:A~B> <DstI p:A~B> <DstPort:A~B> <Proto> <fragmento>	Establezca la política de enlace del túnel. BindIndex: indica el número de índice (1 ~ 64) para vincular el túnel. *vpn trunk bind set 1 y vpnlb 1 192.168.10.1~192.168.10.2 192.168.99.1~192.168.99.254 1~65535 0 APAGADO* ACT: especifique la acción. “y” significa activo; “n” significa inactivo o eliminar. TrunkName - TrunkName: especifique el nombre del tronco VPN creado mediante el comando "vpn trunk lb". Miembro: especifique el número de índice del perfil de LAN a LAN (marcación de salida) que se vinculará. SrcIp:A~B: especifique el rango de IP de origen (p. ej., 192.168.10.0~192.168.10.255. DstI p:A~B - Especifique el rango de IP de destino (p. ej., 192.168.1.0~192.168.1.255. DstPort:A~B: especifique el intervalo de puertos de destino (1~65535). Proto: especifique el protocolo. 0 - cualquiera 1 – ICMP 2-IGMP 6 – TCP 17 – UDP 255 – TCP/UDP Frag – “ON” significa vincular el paquete fragmentado; “OFF” significa que no me importa. Es la configuración predeterminada.
enlazar insertar <After_BindIndex> <ACT> <TrunkName> <Miembro>	Se utiliza para insertar una política de equilibrio de carga adicional en una política existente. After_BindIndex–Especifique un número de índice que nuevo adicional

<SrcIp:A~B> <DstIp:A~B> <DstPort:A~B> <Proto> *<fragmento>*	la política debe insertarse antes. Vea el siguiente ejemplo: *vpn trunk bind insert 1 y vpnlb 2* *192.168.10.3~192.168.10.200* *192.168.99.200~192.168.99.200 80~80 TCP APAGADO* ACT: especifique la acción. “y” significa activo; “n” significa inactivo o eliminar. TrunkName: especifique el nombre del tronco VPN. Miembro: especifique el número de índice del perfil de LAN a LAN (marcación de salida) que se vinculará. SrcIp:A~B: especifique el rango de IP de origen (p. ej., 192.168.10.0~192.168.10.255. DstI p:A~B - Especifique el rango de IP de destino (p. ej., 192.168.1.0~192.168.1.255. DstPort:A~B: especifique el intervalo de puertos de destino (1~65535). Proto: especifique el protocolo. 0 - cualquiera 1 – ICMP 2-IGMP 6 – TCP 17 – UDP 255 – TCP/UDP Frag – “ON” significa vincular el paquete fragmentado; “OFF” significa que no me importa. Es la configuración predeterminada.
Mostrar SetGre *<Índice_de_llamadas>*	Muestra la configuración de GRE sobre IPSec en el perfil de LAN a LAN especificado. Dialout_Index: número de índice del perfil de LAN a LAN (dial-out).
EstablecerGre *<Activo/Inactivo><Dialout_Index><GRE_MyIP><GRE_PeerIP><Logical_Traffic>*	Activo/Inactivo: especifique la acción. “y” significa activo; “n” significa inactivo. Dialout_Index: número de índice del perfil de LAN a LAN (dial-out). GRE_MyIP: ingrese la IP virtual del enrutador para que sea verificada por pares. GRE_PeerIP: ingrese la IP virtual del host del mismo nivel para ser verificada por el enrutador. Logical_Traffic: especifique la acción para RFC2890. “y” significa activo; “n” significa inactivo.
An_Gre GreIPsecAnalizar *<ENCENDIDO/APAGADO>*	Estos comandos se utilizan para la depuración de RD.

Ejemplo

```
> vpn setup 1 name1 pptp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0 % Registro de cambios de perfil...

% Índice de perfil: 1 % Nombre
de perfil: name1j % Nombre de
usuario: vigor
% Contraseña: 1234
% Dirección de llamada : Dial-Out %
Tipo de servidor : PPTP % Marcar a :
1.2.3.4
% IP de red remota: 192.168.1.0 % Máscara de red
remota: 255.255.255.0
> vpn setup 2 market pptp_out 5.6.7.8 vigor 5678 192.168.1.31 255.255.255.0 % Registro de cambios de perfil...

% Índice de perfil: 2 % Nombre
de perfil: mercado % Nombre
de usuario: vigor
% Contraseña: 5678
```

```
% Dirección de la llamada : Dial-Out
% Tipo de servidor : PPTP % Marcar
a : 5.6.7.8
% IP de red remota: 192.168.1.31 % Máscara de
red remota: 255.255.255.0
> vpn troncal lb agregar comp 1 2
%% Lista de perfil de equilibrio de carga VPN combinada:
   <Índice>     <     Nombre     >     <     Tipo de miembro 1 (activo)     > <
Miembro2(Acto
ive)Tipo     >
      1          borrador                    1(SI)PPTP                              2(SÍ)PPTP

%% Nota: <Activo: NO> El perfil de LAN a LAN está deshabilitado o en Dial-In (Dirección de llamada)
en este momento.
================================================ ==================

% Configuración OK.
> vpn trunk bind set 1 y comp 2 192.168.10.1~192.168.10.2
192.168.99.1~192.168.99.254 1~65535 0 APAGADO
% Índice de tabla de enlace de túnel de equilibrio de carga de VPN[1] detalle:
================================== ====================== Acción
                                  = ACTIVO
 Perfil de línea troncal (000) Nombre = comp
 Índice de marcación de enlace saliente = 2 IP de
 origen de enlace                = 192.168.10.1 ~ 192.168.10.2 =
 IP de destino vinculante        192.168.99.1 ~ 192.168.99.254 = 1 ~ 65535
 Puerto de destino vinculante
 Unión fragmentada                = NO
 Protocolo de enlace              = CUALQUIER protocolo
>
```

Comando Telnet: vpn NetBios

Este comando permite a los usuarios habilitar o deshabilitar NetBios para cuentas de usuario de acceso remoto o perfil de LAN a LAN.

Sintaxis

vpn conjunto NetBios*<H2l/L2l> <índice> <Bloquear/Pasar>*

Sintaxis Descripción

Parámetro	Descripción
<H2l/L2l>	H2l significa Cuentas de usuario de acceso remoto. L2l significa perfil de LAN a LAN. Especifique cuál será aplicado por NetBios.
<índice>	El número de índice (1 a 48) del perfil.
<Bloquear/Pasar>	**Aprobar**–Haga una consulta para la transmisión de datos entre los hosts ubicados a ambos lados del Túnel VPN mientras se conecta. **Bloquear**–Cuando se produce un conflicto entre los hosts en ambos lados del túnel VPN al conectarse, configúrelo para bloquear la transmisión de datos del paquete de nombres de Netbios dentro del túnel.

Ejemplo

```
> vpn NetBios conjunto H2l 1 Pase
```

```
% Índice de perfil de marcación remota [1] : %
Bloqueo/aprobación de NetBios: [PASS]
```

Comando Telnet: vpn mss

Este comando permite a los usuarios configurar el tamaño máximo de segmento (MSS) para diferentes tipos de TCP.

Sintaxis

mostrar mss vpn

valor predeterminado mss vpn

conjunto vpn mss *<tipo de conexión> <rango de tamaño máximo de segmento TCP>*

Sintaxis Descripción

Parámetro	Descripción
espectáculo	Significa mostrar el estado de configuración actual.
por defecto	El tamaño máximo del segmento TCP para toda la conexión VPN se establecerá en 1360 bytes.
colocar	Úselo para especificar el tipo de conexión y el valor de MSS.
<tipo de conexión>	1~4 representan varios tipos. 1 – PPTP 2 – L2TP 3-IPSec 4 – L2TP sobre IPSec 5 - vpn 2.ª subred en 6 - Túnel SSL
<segmento máximo de TCP rango de tamaño>	Cada tipo tiene un rango de tamaño de segmento diferente. pptp- 1 ~ 1412 L2TP- 1 ~ 1408 IPSec – 1 ~ 1381 L2TP sobre IPSec – 1 ~ 1361 GRE sobre IPsec - 1 ~ 1365 Túnel SSL - 1 ~ 1360

Ejemplo

```
> vpn mss conjunto 1 1400
% VPN TCP tamaño máximo de segmento (MSS) :
   PPTP    = 1400
   L2TP    = 1360
   IPSec = 1360
   L2TP sobre IPSec        = 1360
   GRE sobre IPsec         = 1360
   Túnel SSL = 1260
> mostrar mss vpn
  Tamaño máximo de segmento VPN TCP (MSS):
  PPTP    = 1400
  L2TP    = 1360
  IPSec = 1360
  L2TP sobre IPSec        = 1360
  GRE sobre IPsec         = 1360
  Túnel SSL = 1260
```

Comando Telnet: vpn ike

Este comando se usa para mostrar el estado de la memoria IKE y la lista de fugas.

Sintaxis

vpn ike-q

vpn ike-s

Ejemplo

```
> vpn ike -q
Estado de la memoria IKE y lista de fugas

# de L-Buffer libre=95, mínimo=94, fuga=1
# de M-Buffer libre=529, mínimo=529 fuga=3
# de S-Buffer libre=1199, mínimo=1198, fuga=1
# de Msgid-Buffer libre=1024, mínimo=1024
```

Comando Telnet: multidifusión vpn

Este comando permite a los usuarios pasar o bloquear el paquete de multidifusión a través de VPN.

Sintaxis

conjunto de multidifusión vpn*<H2L/L2L> <índice> <Bloquear/Pasar>*

Sintaxis Descripción

Parámetro	Descripción
<H2L/L2L>	H2l significa Host to LAN (Cuentas de usuario de acceso remoto). L2l significa perfil de LAN a LAN.
<índice>	El número de índice (1 a 64) del perfil.
<Bloquear/Pasar>	Configure Bloquear/Pasar los paquetes de multidifusión. El valor predeterminado es Bloquear.

Ejemplo

```
> vpn Multicast set L2l 1 Pass % Lan to Lan
Profile Index [1] : % Status Block/Pass:
[PASS]
```

Comando Telnet: vpn pass2nd

Este comando permite a los usuarios determinar si los paquetes que provienen de la segunda subred pasan por el túnel VPN utilizado actualmente.

Sintaxis

contraseña vpn 2*<encendido/apagado>*

Sintaxis Descripción

Parámetro	Descripción
encendido apagado	on: los paquetes pueden pasar a través de NAT. apagado: los paquetes no pueden pasar a través de NAT.

Ejemplo

> paso vpn 2 en
¡Se permite que % de la segunda subred pase el túnel VPN!

Comando Telnet: vpn pass2nat

Este comando permite a los usuarios determinar si los paquetes pasan por NAT o no cuando el túnel VPN se desconecta.

Sintaxis

pass2nat vpn<*encendido/apagado*>

Sintaxis Descripción

Parámetro	Descripción
encendido apagado	on: los paquetes pueden pasar a través de NAT. apagado: los paquetes no pueden pasar a través de NAT.

Ejemplo

> vpn pass2nat encendido
¡El % de los paquetes pasarían por NAT cuando la VPN se desconecte!

Comando Telnet: vpn misma subred

Este comando permite a los usuarios crear una VPN entre clientes a través de una subred virtual.

Sintaxis

vpn misma subred-*yo <valor>* **vpn misma subred**–*mi <0/1>* **vpn misma subred**–*e <valor>* **vpn misma subred**-*I <Subred virtual>* **vpn misma subred**-*o <agregar/eliminar>* **vpn misma subred**-*v* **vpn misma subred**-*metro*

Sintaxis Descripción

Parámetro	Descripción
- yo <valor>	Especifique el número de índice del perfil VPN.
– Mi <0/1>	Habilite o deshabilite el IPsec con la misma subred. 1 – habilitar. 0 – deshabilitar.
– e <valor>	Traduce la LAN especificada a la subred virtual. 1 – LAN1 2 – LAN2 3 – LAN3...
- Yo <Subred virtual>	Configure la subred virtual (p. ej., 172.16.3.250).
-v	Muestra el estado actual de la subred virtual.
- metro <1/2>	Establezca el Tipo traducido. *<1/2>* -1 para subred completa, 2 para IP específica.

Ejemplo

```
> vpn sameSubnet -i 1 -e 1 -E 1 -e 1 -I 10.10.10.0 -o add ¡Habilitar IPsec con la
misma subred!

  Añadir entrada ¡Éxito!
> vpn sameSubnet -v IPsec con la
misma subred: perfil VPN 1
habilitado,
   Subred completa:
      LAN1 traducido a subred virtual: 10.10.10.0 LAN1 traducido a
      subred virtual: 10.10.10.0 LAN1 traducido a subred virtual:
      10.10.10.0
>
```

Comando Telnet: vpn ovpn

Este comando permite a los usuarios crear VPN entre clientes a través de OpenVPN.

Sintaxis

vpn opn*modo*<0/1> **vpn**
opn*espectáculo*
vpn opn*modo_upd*<0/1> **vpn opn**
modo_tcp<0/1> **vpn opn***el puerto*
UDP<1-65535> **vpn opn***puerto_tcp*<
1-65535> **vpn opn***certificado*<0/1>
vpn opn*repetición*<0/1> **vpn opn**
modo de certificación<0/1/2> **vpn**
opn*modo hmac*<0/1/2> **vpn opn**
aproximadamente <0/1/2/3> **vpn**
opn*tlsauth_del <1/2/3>*

Sintaxis Descripción

Parámetro	Descripción
modo<0/1>	Habilite o deshabilite la función OpenVPN. 1 – habilitar. 0 – deshabilitar.
espectáculo	Muestra la configuración actual de OpenVPN.
modo_upd<0/1>	Activa o desactiva el modo UDP. 1 – habilitar. 0 – deshabilitar.
modo_tcp<0/1>	Habilite o deshabilite el modo TCP. 1 – habilitar. 0 – deshabilitar.
el puerto UDP<1-65535>	Ingrese un número de puerto (1-65535) para el modo UDP.
puerto_tcp<1-65535>	Ingrese un número de puerto (1-65535) para el modo TCP.
repetición<0/1>	Activa o desactiva la opción de reproducción. 1 – habilitar. 0 – deshabilitar.

modo de certificación<0/1/2>	Configure el modo de algoritmo de cifrado. 0:AES128, 1:AES256, 2:Ninguno
modo hmac<0/1/2>	Establezca el modo HMAC de cifrado. 0:SHA1, 1:SHA256, 2:Ninguno
aproximadamente <0/1/2/3>	Establezca el certificado Trust CA.
tlsauth_del <1/2/3>	Elimine la primera, segunda o tercera clave de autenticación TLS.

Ejemplo

```
> Modo vpn ovpn 1
Habilitar openvpn
> mostrar vpn ovpn

  Openvpn: Habilitar
  soporte UDP: Habilitar
  Puerto UDP: 1194
  soporte TCP: Habilitar
  Puerto TCP: 1194
  Usar autenticación de certificado: Habilitar opción
  de reproducción: Habilitar
  Algoritmo de cifrado: AES256
  Algoritmo HMAC: SHA256
  Certificado uid: 65535
  Confianza CA uid: 0
```

Comando Telnet: wan ppp_mru

Este comando permite a los usuarios ajustar el tamaño de PPP LCP MRU. Se utiliza para una red específica.

Sintaxis

wan ppp_mru*<Número de interfaz WAN> <Tamaño de MRU>*

Sintaxis Descripción

Parámetro	Descripción
<Número de interfaz WAN>	Escriba un número para representar la interfaz física. Para Vigor130, el número es 1 (lo que significa WAN1).
<Tamaño de MRU>	Significa el número de PPP LCP MRU. El rango disponible es de 1400 a 1600.

Ejemplo

```
> wan ppp_mru 1 ? %
Ahora: 1492

> wan ppp_mru 1 1490
>
> wan ppp_mru 1 ? %
Ahora: 1490

> wan ppp_mru 1 1492
> wan ppp_mru 1 ? %
Ahora: 1492
```

Comando Telnet: wan mtu / wan mtu2

Este comando permite a los usuarios ajustar el tamaño de MTU para WAN1/WAN2.

Sintaxis

quiero mtu *<valor>*

quiero mtu2 *<valor>*

Sintaxis Descripción

Parámetro	Descripción
valor	Significa el número de MTU para PPP. El rango disponible es de 1000 a 1500. Para IP estática/DHCP, el número máximo será 1500. Para PPPoE, el número máximo será 1492. Para PPTP/L2TP, el número máximo será 1460.

Ejemplo

```
> wan mtu 1100
> quieres mtu?
IP estática/DHCP (MSS máx.: 1500)
PPPoE (MSS máx.: 1492)
PPTP/L2TP (MSS máx.: 1460)
% wan ppp_mss <tamaño MSS: 1000 ~ 1500>
% Ahora: 1100
```

Comando Telnet: wan dns

Este comando permite a los usuarios configurar el servidor DNS primario y/o secundario.

Sintaxis

dns wan *<wan_no> <dns_select> <dirección_ipv4>*

Sintaxis Descripción

Parámetro	Descripción
<wan_no>	Seleccione la interfaz WAN. 1 ~4 - WAN1 ~ WAN4.
<dns_seleccionar>	Especifique el servidor DNS primario y/o secundario. pri – Significa servidor DNS primario. sec – Significa servidor DNS secundario.
<dirección_ipv4>	Introduzca la dirección IP del servidor DNS.

Ejemplo

```
> wan dns 1 pri 168.95.1.1 %
Establecer DNS primario WAN1 hecho.
% Ahora: 168.95.1.1
```

Comando Telnet: wan DF_check

Este comando le permite habilitar o deshabilitar la función de DF (No fragmentar)

Sintaxis

wan DF_check*<encendido/apagado>*

Sintaxis Descripción

Parámetro	Descripción
encendido apagado	Significa habilitar o deshabilitar DF.

Ejemplo

```
> wan DF_check en %DF bit
check enable!
> wan DF_marcar apagado
Deshabilitar verificación de bits %DF (reiniciar bit DF)!
```

Comando Telnet: wan deshabilitar

Este comando le permite deshabilitar la conexión WAN.

Ejemplo

```
> wan deshabilitar WAN
 %WAN deshabilitado.
```

Comando Telnet: habilitar wan

Este comando le permite deshabilitar la conexión wan.

Ejemplo

```
> wan habilitar WAN
 %WAN1 habilitado.
```

Comando Telnet: wan wan2lan

Cuando WAN2 está deshabilitado o WAN2 está configurado como modo físico inalámbrico, el puerto Ethernet se configura como puerto LAN.

Sintaxis

wan wan2lan*<wan> <encendido/apagado/estado>*

Sintaxis Descripción

Parámetro	Descripción
<wan>	Seleccione una interfaz WAN (1 a 4). Actualmente, solo WAN2 está disponible.
<encendido/apagado/estado>	0n: activa el modo de puerto WAN a LAN. Apagado: deshabilitar el modo de puerto WAN a LAN. Estado: muestra el modo actual.

Ejemplo

```
> wan wan2lan 2 estado % WAN2
actual es modo WAN
```

```
% de uso: muestra la configuración de WAN a LAN, actualmente solo admite WAN2
% Cuando WAN2 está deshabilitado o WAN2 está configurado en modo físico inalámbrico, el puerto eth está configurado como LAN
% El puerto eth WAN2 actual está en modo WAN
> wan wan2lan 2 en
% WAN2 convertido a LAN6, la interfaz WAN2 se desactivará
% de uso: muestra la configuración de WAN a LAN, actualmente solo admite WAN2
% Cuando WAN2 está deshabilitado o WAN2 está configurado en modo físico inalámbrico, el puerto eth está configurado como LAN
% El puerto eth WAN2 actual está en modo LAN
```

Comando Telnet: wan adelante

Este comando le permite habilitar o deshabilitar la función de reenvío WAN. Los paquetes pueden transmitirse entre diferentes WAN.

Sintaxis

va hacia adelante *<encendido/apagado>*

Sintaxis Descripción

Parámetro	Descripción
encendido apagado	Significa habilitar o deshabilitar el reenvío de WAN.

Ejemplo

```
> ¿quieres avanzar?
¡El reenvío de %WAN está desactivado!

> wan adelante en
¡El reenvío de %WAN está habilitado!
```

Comando Telnet: estado wan

Este comando le permite mostrar el estado de la conexión WAN, incluido el modo de conexión, los paquetes TX/RX, la configuración de DNS y la dirección IP.

Ejemplo

```
> estado pálido
WAN1: fuera de línea, parada = N
  Modo: ---, Tiempo activo=00:00:00
  IP=---, GW IP=---
  Paquetes de TX = 0, Velocidad de TX (Bps) = 0, Paquetes de RX = 0, Velocidad de RX
  (Bps) = 0 DNS primario = 0.0.0.0, DNS secundario = 0.0.0.0

PVC_WAN3: Fuera de línea,
  bloqueo=N Modo: ---, Tiempo
  activo=00:00:00 IP=---, GW IP=---
  Paquetes de TX = 0, Tasa de TX (Bps) = 0, Paquetes de RX = 0, Tasa de RX (Bps) = 0

PVC_WAN4: Fuera de línea,
  bloqueo=N Modo: ---, Tiempo
  activo=00:00:00 IP=---, GW IP=---
```

```
  Paquetes de TX = 0, Tasa de TX (Bps) = 0, Paquetes de RX = 0, Tasa de RX (Bps) = 0

PVC_WAN5: Fuera de línea,
  bloqueo=N Modo: ---, Tiempo
  activo=00:00:00 IP=---, GW IP=---
  Paquetes de TX = 0, Tasa de TX (Bps) = 0, Paquetes de RX = 0, Tasa de RX (Bps) = 0
```

Comando Telnet: módem wan / módem wan2

Este comando, wan modem, le permite configurar un módem USB 3G/4G (modo PPP) de WAN3.

El comando, wan modem2, le permite configurar un Módem USB 3G/4G (modo PPP) de WAN4.

Sintaxis

módem pálido *<init/init2/marcar/pin><cadena>* **wan modem**

paponly *<encendido/apagado>* **copia de seguridad_espera**

del módem wan *<valor>*

tubo de módem wan < *Int><Din><Dout> (solo para USB WAN3)* **activación del**

módem wan *<on/off/value> (solo para USB WAN3)* **vídeo de módem wan** *<*

identificación> **pid de módem wan** *<identificación>* **estado del módem wan**

Sintaxis Descripción

Parámetro	Descripción
en eso	Configure el comando AT del módem inicial (el valor predeterminado es “AT&FE0V1X1&D2&C1S0=0”).
Init2	Configure el segundo comando AT del módem inicial.
marcar <cadena>	Configure el comando AT del módem de marcación (el valor predeterminado es “ATDT*99#”).
alfiler <0>	Establezca el código PIN para la tarjeta SIM. “0”: deshabilitar
papel <activar/desactivar>	Significa Solo PAP. Configure la autenticación PPP de la WAN USB. en: Ninguno. apagado: PAP o CAP.
backup_wait <valor>	Configure el tiempo de espera después del arranque si la WAN USB está en modo de copia de seguridad. Este tiempo de espera está reservado para el marcado de las WAN principales, de modo que la WAN USB de respaldo no se active primero. La configuración disponible es de 1 a 255. La unidad es el segundo.
tubo	Es solo para depuración de RD. Por favor, no lo use sin nuestro consejo.
despertar <activar/desactivar/valor>	Es solo para depuración de RD. Por favor, no lo use sin nuestro consejo.
vídeo	Establezca la coincidencia VID de VID/PID para enlazar el módem USB para especificar la interfaz WAN. De manera predeterminada, esta coincidencia no está configurada (0x0/0x0) y el enrutador especifica la interfaz WAN por puerto USB.
pid	Establezca la coincidencia de PID de VID/PID para vincular el módem USB para especificar la interfaz WAN. De manera predeterminada, esta coincidencia no está configurada (0x0/0x0) y el enrutador especifica la interfaz WAN por puerto USB.
estado	Muestra el estado actual del módem USB.

Ejemplo

```
> pin de módem wan 0000
> estado del módem wan Velocidad
  de enlace del módem = 0
  Intensidad de la señal actual = 0
  Último mensaje de error:
  Etapa de conexión actual:
```

Comando Telnet: wan lte

Este comando le permite configurar LTE WAN (solo para el modelo L).

Sintaxis

autenticación wan lte *<*
0/1> **banda wan lte**
wan lte del <*índice #/todos>*
quiero pasar lte*<cadena>*
wan lte pre_banda
cuota wan lte*[-<comando><parámetro>|...]*
quiero leer <*índice #/todos>*
reinicio wan lte*[-<comando><parámetro>|...]* **wan lte respuesta***[-<comando><parámetro>|...]* **quiero enviar lte***<número><mensaje>* **quiero lte sms***[-<comando><parámetro>|...]* **escaneo wan lte***[-<comando><parámetro>|...]* **conjunto wan lte***[-<comando><parámetro>|...]* **quiero lte stus**

quiero etiqueta lte <*índice #/todos>*
usuario wan lte*<cadena>*
wan lte wms*<enviar<cdma/gwpp>/recv<cdma/gwgw>/configuración>*

Sintaxis Descripción

Parámetro	Descripción
autorización <0/1>	Configure la autenticación PPP de LTE WAN. 0: Ninguno. 1: PAP o CAP.
banda	Muestra información de la banda de trabajo para la conexión de red LTE.
del<índice #/todos>	Elimine un SMS de la tarjeta SIM LTE especificando el número de índice. Use "todos" para borrar todos.
pasar <cadena>	Configure la contraseña de LTE WAN.
cuota [-<comando><parámetro>|...]	Establezca la configuración de la función de límite de cuota de SMS. Los comandos disponibles con parámetro se enumeran a continuación: [...] significa que puede ingresar varios comandos en una línea. - a <0/1>: establezca si se enviará una alerta por correo electrónico cuando se exceda la cuota de SMS. (0: no 1: sí) - c <ciclo>: establece el orden de hoy en el ciclo de actualización. - d <día>: establece el día de actualización. - e <0/1>: activa o desactiva la función de límite de cuota de SMS. (0: deshabilitar 1: habilitar)

	- h <hora>: establece la hora de actualización. - m <0/1/2>: establece el modo de actualización de la cuota de SMS. (0: ninguno 1: mensual 2: periódicamente) - n <número>: Establecer cuota de SMS. El número disponible está entre 1 y 1000000. - s <0/1>: establezca si se debe dejar de enviar SMS después de que se exceda la cuota de SMS. (0: no 1: sí)
leer<índice #/todos>	Muestra información de un SMS en la tarjeta SIM LTE especificando el número de índice. Use "todos" para mostrar todos.
reiniciar	Establezca la configuración de la función Reiniciar en mensaje SMS. <comando> <parámetro> | ... Los comandos disponibles con parámetros se enumeran a continuación. significa que puede ingresar varios comandos en una línea. - a <0/1>: Habilitar o deshabilitar la Lista de control de acceso. (0: deshabilitar 1: habilitar) - e <0/1>: habilite o deshabilite la función Reiniciar en mensaje SMS. (0: deshabilitar 1: habilitar) - p <contraseña>: Establece la Contraseña/PIN. Este ajuste es necesario si esta función está habilitada. - x <número>: establezca el primer número de teléfono en la lista de control de acceso. - y <número>: establece el segundo número de teléfono en la lista de control de acceso. - z <número>: establezca el tercer número de teléfono en la lista de control de acceso.
responder	Establezca la configuración de la función Responder con el mensaje de estado del enrutador. <comando> <parámetro> | ... Los comandos disponibles con parámetros se enumeran a continuación. significa que puede ingresar varios comandos en una línea. - a <0/1>: Habilitar o deshabilitar la Lista de control de acceso. (0: deshabilitar 1: habilitar) - c <0/1>: establece si se responde con la dirección MAC. (0: no 1: sí) - e <0/1>: habilite o deshabilite la función Reiniciar en mensaje SMS. (0: deshabilitar 1: habilitar) - f <0/1>: establece si se responde con la dirección IP WAN1. (0: no 1: sí) - g <0/1>: Establezca si responder con la dirección IP WAN2. (0: no 1: sí) - h <0/1>: establece si se responde con la dirección IP de WAN LTE. (0: no 1: sí) - i <0/1>: Establezca si responder con la dirección IP WAN4. (0: no 1: sí) - j <0/1>: establece si se responde con el uso de datos WAN1. (0: no 1: sí) - k <0/1>: establece si se responde con el uso de datos WAN2. (0: no 1: sí) - l <0/1>: establezca si responder con el uso de datos de WAN LTE. (0: no 1: sí) - m <0/1>: establezca si responder con el uso de datos WAN4. (0: no 1: sí) - n <0/1>: establece si se responde con el nombre del enrutador. (0: no 1: sí) - p <contraseña>: Establece la Contraseña/PIN. Este ajuste es necesario si esta función está habilitada. - u <0/1>: establece si se responde con el tiempo de actividad del sistema del enrutador. (0: no 1: sí) - v <0/1>: establece si se responde con la versión de firmware del enrutador. (0: no 1: sí) - x <número>: establezca el primer número de teléfono en la lista de control de acceso. - y <número>: establece el segundo número de teléfono en la lista de control de acceso. - z <número>: establezca el tercer número de teléfono en la lista de control de acceso.
enviar<número><mensaje>	Envíe un mensaje SMS al número de teléfono especificado a través de la tarjeta SIM LTE.
SMS	Significa establecer configuraciones avanzadas para SMS.

	- a <0/1>: Alerta al administrador con correo electrónico cuando la bandeja de entrada de SMS está llena. - d <0/1>: elimina los SMS leídos más antiguos cuando la bandeja de entrada de SMS está llena. - f <0/1> : Reenviar nuevos SMS por correo electrónico al administrador. - s <0/1> : Almacene el caché de la bandeja de salida de SMS con el disco USB. (0: deshabilitar 1: habilitar)
escanear <todos/4g/3g/2g/mostrar>	Significa escanear redes visibles. [all/4g/3g/2g]: Escanee todas las redes 4g, 3g o 2g. Mostrar: Muestra el resultado del escaneo.
colocar	Significa establecer el nombre de APN, mantener el tiempo activo, etc. apn <apn_name>: establece una cadena como APN. pin <pin_code>: establece un código pin. power_recycle <backoff_time(0~20)>: establece el tiempo de reciclaje de energía (segundos) para volver a marcar después del apagado. dial_on: Desactiva la función de marcación. Se utiliza para la depuración de RD. dial_off: Desactiva la función de marcación. Se utiliza para la depuración de RD. keep_alive_on <IP>: Desactiva la función de Keep Alive On. Especifique la dirección IP (xxxx). keep_alive_off: Desactiva la función de Keep Alive On. dhcp<on/off>: activa o desactiva el servidor DHCP, según la configuración de su ISP. <IP> fijo: especifique una dirección IP si DHCP está configurado como "apagado". Además, depende de la configuración de su ISP. manual_dns <on/off>: encendido, configura el servidor DNS manualmente; Desactivado, utilice la configuración del servidor DNS predeterminado. El valor predeterminado es "desactivado". Primary_dns <IP>: establezca la dirección IP del DNS principal (xxxx) obtenida de su ISP si manual_dns está configurado como "activado". dns_secundario <ip): establezca la dirección IP del DNS secundario (xxxx) obtenida de su ISP si manual_dns está configurado como "activado". specific_mccmnc <on/off>: activa o desactiva el MCC y el MNC específicos. mcc <mcc_value>: establece el valor (0~999) para MCC (código de país móvil) mnc <mnc_value>: establece el valor (0~999) para MNC (código de red móvil). timeout <valor>: establezca el intervalo de tiempo de espera (50 a 255 segundos). fail_threshold: establezca los tiempos (2 ~ 20 veces) de intentar la conexión a través de LTE.
estado	Muestra el estado de la conexión LTE.
etiqueta	Configure un SMS en la tarjeta SIM LTE como estado de lectura especificando el número de índice. Use "todos" para configurar todos los SMS como estado de lectura.
usuario	Establezca el nombre de usuario de LTE WAN.
wms	Este comando es solo para depuración de RD. Lo usamos para probar nuevos módems USB. Por favor, no lo use sin nuestro consejo.

Ejemplo

```
> banda wan lte

Tecnología de acceso: LTE
Acceder a la información de la banda: E-UTRA Op Band 3
Interferir con WLAN 2.4G: NO
Canal activo: 1725
> wan lte estado
Estado: Operativo. (En línea) Tecnología
de acceso: LTE
```

```
Banda: E-UTRA Op Band 3 ISP:
Chunghwa
MCC: 466, MNC: 92, LAC: 65534, ID de celda: 81023501 Velocidad
máxima de transmisión de canal: 50000000 bps
Velocidad máxima de RX de canal: 100000000
bps IMEI: 356318040749422
IMSI: 466924200859808
RSSI: -61dBm
SMS no leídos: 4
Dirección de SMSC: +886932400821
Estado del servicio de SMS: Listo
Número de SMS enviados: 0
```

Comando Telnet: wan sim2

Este comando le permite configurar los ajustes para SIM2. Está disponible para el modelo LTE.

Sintaxis

quiero sim2*autorización <0/1>* **quiero sim2***usuario <nombre de usuario>* **quiero sim2***pasar <contraseña>* **quiero sim2** *establecer apn <apn_name>* **quiero sim2***establecer pin <pin_code>* **quiero sim2***establecer modo <0~3>* **quiero sim2** *establecer keep_alive_on <IP>* **quiero sim2***establecer keep_alive_off* **quiero sim2***establecer el tiempo de espera <50 ~ 255 seg>* **quiero sim2***establecer fail_threshold <2~20 veces>*

Sintaxis Descripción

Parámetro	Descripción
autorización <0/1>	Configure la autenticación LTE para la conexión. 0 - PAP o CAP. 1 - Solo PAP.
usuario <nombre de usuario>	Configure el nombre de usuario para SIM2. <nombre de usuario>: ingrese una cadena.
pasar <contraseña>	Configure la contraseña para SIM2. <contraseña>: ingrese una cadena.
establecer apn <apn_name>	Configure el nombre APN para el SIM2. <apn_name>: ingrese una cadena como nombre de APN.
establecer pin <pin_code>	Configure el código PIN para la SIM2.
establecer modo <0~3>	Configure el modo de red para el SIM2. 0-4G/3G/2G; 1- Solo 4G; 2- Solo 3G; 3- Solo 2G
establecer keep_alive_on <IP>	IP: especifique una dirección IP.
establecer keep_alive_off	Desactiva la función de Keep Alive On.
establecer el tiempo de espera <50 ~ 255 seg>	Introduzca un valor (de 50 a 255, la unidad es el segundo) como tiempo de espera.

establecer fail_threshold <2~20 veces>	Establezca los tiempos máximos (de 2 a 20) de accesos telefónicos fallidos. Después de eso, el sistema dejará de marcar y usará otra tarjeta SIM para marcar en su lugar.

Ejemplo

```
> wan sim2 establecer tiempo de espera 100
Establecer tiempo de espera de acceso telefónico: 100
>
```

Comando Telnet: wan detectar

Este comando le permite configurar la detección de conexión WAN. Cuando la detección de ping está habilitada (para modo IP estático o DHCP o PPPoE), el enrutador hace ping a las direcciones IP especificadas para detectar la conexión WAN.

Sintaxis

quiero detectar *<wan1/../wan9><encendido/apagado/estricto/siempre_encendido>* **quiero detectar** *<wan1/../wan9><activar/desactivar>***-t<***tiempo>* **quiero detectar** *<wan1/../wan9> <activar/desactivar>***-i** *<intervalo>* **quiero detectar** *<wan1/../wan9>***objetivo <** *dirección IP>* **quiero detectar** *<wan1/../wan9>***objetivo2 <** *dirección IP>* **quiero detectar** *<wan1/../wan9>***objetivo_gw <** *1/0>* **quiero detectar** *<wan1/../wan9>***ttl <** *valor>* **quiero detectar** *<wan1/../wan9>***intervalo <** *intervalo>* **quiero detectar** *<wan1/../wan9>***reintentar <** *reintentar>*

wan detectar estado

Sintaxis Descripción

Parámetro	Descripción
<activado/desactivado/estricto/siempre_activado>	Activado: activa la detección de ping. Se establecerá la dirección IP del objetivo. Desactivado: activa la detección de ARP (predeterminado). Se debe establecer el tiempo y el intervalo. estricto: habilite la detección estricta de ARP. Se debe establecer el tiempo y el intervalo. always_on: deshabilitar la detección de enlaces, siempre conectado (solo admite IP estática)
- t <tiempo>	Configure el tiempo para la detección ARP o la detección ARP estricta.
- i <intervalo>	Configure el intervalo para la detección ARP o la detección ARP estricta.
objetivo <dirección IP>	Establezca el objetivo de ping. <ip addr>: Significa la dirección IP utilizada para la detección. Escriba una dirección IP (p. ej., 192.168.1.10) en este campo.
objetivo2<dirección IP>	Establezca el objetivo de ping secundario. <ip addr>: Significa la dirección IP utilizada para la detección. Escriba una dirección IP (p. ej., 192.168.1.10) en este campo.
objetivo_gw <1/0>	Establezca si usar la puerta de enlace como destino de ping. 1: si 0: no Tenga en cuenta que la WAN USB (modo PPP) no admite la puerta de enlace PING
ttl <1-255>	Significa establecer el valor TTL de ping (funciona como ruta de rastreo)

	Si no establece ningún valor para ttl aquí o simplemente escribe 0 aquí, el sistema utilizará la configuración predeterminada (255) como el valor ttl.
intervalo <intervalo>	Establezca el intervalo entre cada operación de ping. La configuración disponible está entre 1 y 3600. La unidad es la segunda. *<intervalo>*:Escriba un valor.
reintentar <reintentar>	Establezca cuántas operaciones de ping se reintentan antes de que el enrutador juzgue que la conexión WAN está desconectada. El ajuste disponible es entre 1 y 255. La unidad es el tiempo. <reintentar>: escriba un número.
estado	Significa mostrar el estado actual.

Ejemplo

```
> wan detectar estado
  WAN1: detección arp, tiempo de envío=30, intervalo = 5
  WAN2: detección arp, tiempo de envío=30, intervalo = 5
  WAN3: detección arp, tiempo de envío=30, intervalo = 5
  WAN4: detección arp, tiempo de envío=30, intervalo = 5
  WAN5: detección arp, tiempo de envío=30, intervalo = 5
  WAN6: detección arp, tiempo de envío=30, intervalo = 5
  WAN7: detección de ping, Target=0.0.0.0, TTL=255, Target2=0.0.0.0, TargetGW=off, Interval=1,
  Retry=10
  WAN8: detección de ping, Target=0.0.0.0, TTL=255, Target2=0.0.0.0, TargetGW=off, Interval=1,
  Retry=10
  WAN9: detección de ping, Target=0.0.0.0, TTL=255, Target2=0.0.0.0, TargetGW=off, Interval=1,
  Retry=10>
```

Comando Telnet: wan lb

Este comando le permite Habilitar/Deshabilitar el modo de equilibrio de carga para cada WAN.

Sintaxis

libra pálida<*wan1/wan2/...> activado*

libra pálida<*wan1/wan2/...> apagado*

wan lb <*IP/sesión***> estado de peso**

ligero en libras

Sintaxis Descripción

Parámetro	Descripción
wan1 a wanx	Especifique qué WAN se aplicará con equilibrio de carga.
en	Haga que la interfaz WAN sea miembro del equilibrio de carga.
apagado	Cancele la interfaz WAN como miembro del equilibrio de carga.
ip/sesión	Establezca el balance de carga en modo basado en IP o basado en sesión.
estado	Mostrar el estado actual.

Ejemplo

```
> estado de libras wan
  WAN1: encendido
  WAN2: encendido
  WAN3: activado
  WAN4: encendido
  WAN5: activado
```

WAN6: activado

WAN7: activado

WAN8: encendido

WAN9: encendido

El modo de equilibrio de carga está basado en IP

Comando Telnet: wan lbel

Este comando le permite configurar la lista de excepciones de equilibrio de carga.

Sintaxis

wan lbel *<idx> <habilitar> <protocolo> <tipo de ip> <obj_grp idx> <puerto> <fin_puerto> <comentario>* **estado de wan lbel** *<idx>*

Sintaxis Descripción

Parámetro	Descripción
Idx	Ingrese el número de índice (1 a 32) para la lista de excepciones.
permitir	Ingrese 1 (habilitar) o 0 (deshabilitar) el perfil seleccionado.
protocolo	<protocolo>: Introduzca TCP, UDP, TCP+UDP.
tipo de ip	Configure el tipo de IP (0, 1 o 2) para el perfil seleccionado. 0: cualquiera 1: objeto IP 2: grupo de IP
obj_grp idx	Ingrese el número de índice (1 a 32 para grupo IP; 1 a 192 para objeto IP). Si se configura con "0", el tipo de IP se configurará como "Cualquiera".
puerto	Introduzca un número (0 a 65535) como puerto de inicio. Si se establece en "0", el rango de puertos (1 a 65535) no se aplicará con el equilibrio de carga.
presagiar	Ingrese un número (0 a 65535) como puerto final (debe ser mayor que el puerto inicial).
comentario	Introduzca una cadena (menos de 11 caracteres) como comentario.
estado	Mostrar el estado actual.

Ejemplo

```
> wan lbel 1 1 tcp 0 1 0 300 prueba para cargar
> wan lbel estado 1
  lista [1] estado: habilitado, protocolo: tcp, tipo de IP: cualquiera, IP idx: 0, puerto: 0 ~ 300, comentario:
prueba para cargar
  list[2] status:habilitar, protocolo:udp, tipo de IP:cualquiera, IP idx:0, puerto:19302~19302,
comentario:Google STUN
  list[3] status:habilitar, protocolo:tcp+udp, tipo de IP:cualquiera, IP idx:0, puerto:5060~5060, comentario:SIP

  lista[4] estado: deshabilitado, protocolo: tcp, tipo de IP: cualquiera, IP idx: 0, puerto: 80~80, comentario:
  HTTP
  lista [5] estado: deshabilitado, protocolo: tcp, tipo de IP: cualquiera, idx de IP: 0, puerto: 443 ~ 443,
comentario: SSL
. . .
```

Comando Telnet: wan mvlan

Este comando le permite configurar múltiples VLAN para WAN y LAN. Es compatible con el modo puente puro (modo módem) entre la WAN Ethernet y el puerto LAN 2~4.

Sintaxis

wan mvlan *<pvc_no/status/save/enable/disable> <on/off/clear/tag tag_no> <tipo de servicio/prioridad de vlan> <px ... >*

wan mvlan *etiqueta de conservación <pvc_no> <activar/desactivar>*

Sintaxis Descripción

Parámetro	Descripción
pvc_no	Significa número de índice de PVC. Hay 8 PVC, 0 (Canal-1) a 7 (Canal-8) que se pueden configurar. Sin embargo, el modo puente se puede establecer en el número de PVC 2 a 7.
estado	Significa mostrar todo el estado del puente.
ahorrar	Significa guardar la configuración en la memoria flash del enrutador Vigor.
habilitar deshabilitar	Significa habilitar/deshabilitar la función Multi-VLAN.
encendido apagado	Significa activar/desactivar el modo puente para el canal específico.
claro	Significa apagar/borrar el puerto.
etiqueta tag_no	Significa etiquetar un número para la VLAN. - 1: No es necesario agregar el número de etiqueta. 1-4095: Números de configuración disponibles utilizados como número etiquetado.
Tipo de servicio	Significa especificar el tipo de servicio para VLAN. 0: normales. 1: IGMP.
prioridad vlan	Significa especificar la prioridad para la configuración de VALN. El rango es de 0 a 7.
píxeles	Significa puerto LAN. El número de configuración disponible es de 2 a 4. El número de puerto 1 está bloqueado para el uso de NAT.
etiqueta	Significa que los paquetes de VLAN múltiples mantendrán sus encabezados de VLAN en LAN.

Ejemplo

El PVC 7 se asignará al puerto LAN 2/3/4 en modo puente; el tipo de servicio es Normal. No se agregó ninguna etiqueta.

```
> wan mvlan 7 en p2 p3 p4 Puente
de PVC p1 p2 p3 p4 p5                Tipo de servicio    Etiqueta    Prioridad    Mantener etiqueta
 ----------------------------------------------------------------------------7
 ENCENDIDO    0 0 1 1 0 0             Normal    0 (APAGADO)    0    APAGADO
>
```

Comando Telnet: wan multifno

Este comando le permite especificar un canal (en Multi-PVC/VLAN) para realizar una conexión de puente a una interfaz WAN específica.

Sintaxis

wan multifno *<canal #><interfaz WAN #>*
wan multifno *estado*

Sintaxis Descripción

Parámetro	Descripción
canal #	Hay varios canales, incluidos VLAN y PVC. Los ajustes disponibles son: 7 a 16

	Los ajustes disponibles son: 7=Canal 7 . . . 16=Canal 16
interfaz WAN #	Escriba un número para indicar la interfaz WAN. *1=WAN1* *2=WAN2*
estado	Significa mostrar el estado actual del puente.

Ejemplo

```
> wan multifno 5 1
> wan multifno 7 1
% Enlace ascendente del canal 7 configurado a WAN1
> wan multifno status % Ifno de enlace
ascendente del canal 7: 3 % Ifno de
enlace ascendente del canal 8: 3 % Ifno
de enlace ascendente del canal 9: 3 %
Ifno de enlace ascendente del canal 10: 3
% Ifno de enlace ascendente del canal 11:
3 % Ifno de enlace ascendente del canal
12: 3 % Ifno de enlace ascendente del
canal 13 ifno: 3 % canal 14 uplink ifno: 3
% canal 15 uplink ifno: 3
>
```

Comando Telnet: wan vlan

Este comando le permite configurar la etiqueta VLAN de WAN1 o WAN2.

Sintaxis

wan vlan wan<*#*>**etiqueta** <*valor*> **wan vlan**

wan<*#*> <*habilitar/deshabilitar*> **estadística de**

wan vlan

Sintaxis Descripción

Parámetro	Descripción
pálido<*#*>	Especifique qué interfaz WAN se etiquetará.
etiqueta<*valor*>	Escriba un número para etiquetar en la interfaz WAN.
habilitar deshabilitar	Habilitar: se etiquetará la interfaz WAN especificada. Deshabilitar: deshabilite la función de etiquetado en la interfaz WAN.
estadística	Muestra el estado actual de la VLAN.

Ejemplo

```
> estadística de wan vlan
% Interfaz          pri        Etiqueta        Activado
% ===================================== %
WAN1                0          0
% WAN2              0          0
```

```
% WAN3          0        0
% WAN4          0        0
>
```

Comando Telnet: wan phyvlan

Este comando se utiliza para configurar la inserción de la etiqueta VLAN para la etiqueta externa (servicio) para la interfaz WAN. Las interfaces WAN deben configurarse primero antes de configurar la encapsulación de VLAN.

Sintaxis

wan phyvlan wan*<#>***etiqueta <***valor***> wan phyvlan wan***<#>***pri <***valor***> wan phyvlan wan***<#>***<habilitar/deshabilitar> estadística de wan phyvlan**

Sintaxis Descripción

Parámetro	Descripción
<#>	Significa interfaz WAN. 1 ~4 - WAN1 ~ WAN4
etiqueta<valor>	Significa etiquetar un valor (1 a 4095) en la interfaz WAN seleccionada.
pri<valor>	Significa establecer el valor (0 a 7) de prioridad para dicha etiqueta VLAN.
<habilitar/deshabilitar>	Significa habilitar/deshabilitar la etiqueta VLAN.
estadística	Muestra el estado de configuración.

Ejemplo

```
> wan phyvlan wan 1 etiqueta 22
% Establezca la etiqueta del puerto físico en 22 para WAN1 %
Establezca la etiqueta del puerto físico en 22 para WAN1
% Debe reiniciar el enrutador para que la configuración sea efectiva
> wan phyvlan wan 1 habilitar
% Establezca la etiqueta del puerto físico en 22 para WAN1 %
Establezca la etiqueta del puerto físico en 22 para WAN1
% Debe reiniciar el enrutador para que la configuración sea efectiva
> wan phyvlan estadística?

% Interfaz        pri        Etiqueta        Activado
% ======================================== %
WAN1             0          0
% WAN2           0          0
% WAN3           0          0
% WAN4           0          0
>
```

Comando Telnet: presupuesto wan

Este comando le permite determinar los datos*volumen de tráfico*para cada interfaz WAN respectivamente para evitar sobrecargas por la transmisión de datos por parte del ISP.

Sintaxis

wan presupuesto wan*<#>***fecha***<día><hora>* **wan presupuesto wan***<#> <activar/desactivar>*

wan presupuesto wan<*#*>**tres**<*límite de presupuesto (MB)*> **wan**

presupuesto wan<*#*>**gthres**<*límite de presupuesto (GB)*> **wan**

presupuesto wan<*#*>**modo**<*mensual|periódico|ninguno*> **wan**

presupuesto wan<*#*>**psday**<*día en periódico*> **wan presupuesto**

wan<*#*>**modo personalizado**<*0/1*>

wan presupuesto wan<*#*>**custom_mode_reset_hora**<*hora*> **wan**

presupuesto wan<*#*>**acción**<*mapa de bits de acción*> **estado de**

presupuesto débil

Sintaxis Descripción

Parámetro	Descripción
pálido<#> rdate <día><hora>	wan <#>: especifique la interfaz WAN. *rdate <día><hora>*:Especifique el tiempo de actualización del presupuesto de WAN. día: las configuraciones disponibles son de 1 a 30. hora: las configuraciones disponibles son de 1 a 23. Por ejemplo,presupuesto wan wan 1 rdate 5 10 Si se selecciona el modo mensual: el presupuesto de WAN se actualizará el quinto día a las 10:00 de cada mes. Si se selecciona el modo periódico: el presupuesto de WAN se actualizará cada 5 días y 10 horas.
<activar|desactivar>	enable - Habilita la función de presupuesto wan. deshabilitar: deshabilita la función de presupuesto wan.
Thres <límite de presupuesto (MB)>	Especifique el valor máximo para el límite de presupuesto de WAN. (Unidad: MB) límite de presupuesto: escriba un número.
gthres <límite de presupuesto (GB)>	Especifique el valor máximo del límite de presupuesto wan. (Unidad: GB) límite de presupuesto: escriba un número.
modo <mensual|periódico|ninguno>	Especifique el modo de cálculo (mensual, periódico o ninguno) para el presupuesto de WAN.
psdy <th día en periódico>	Se usa solo cuando el modo está configurado como "periódico". Especifique el orden de “hoy” en el ciclo. P.ej,wan presupuesto wan 5 psday -Significa “hoy” es el 5el día en el ciclo de facturación.
modo_personalizado <0/1>	Configure el modo personalizado (ciclo en horas o en días). 0: ciclo_en_horas 1: ciclo_en_días
custom_mode_reset_hora <hora>	Establezca el valor de la hora de reinicio. hora: Ingrese 1 a 23.
acción <mapa de bits de acción>	Determine la acción que se realizará cuando alcance el límite de presupuesto de la WAN. *mapa de bits de acción* –Escriba un número total de acciones a ejecutar. Diferentes números representan diferentes acciones. 1: derribo wan 2: enviar alerta por correo 4: enviar alerta por sms Por ejemplo, si escribe “5” (5=1+4), el sistema enviará una alerta por SMS cuando se detecte una caída de WAN.
estado	Muestra el estado de configuración actual del presupuesto de WAN.

Ejemplo

```
> presupuesto wan wan 1 acción 5 % WAN 1
acción presupuestaria establecida en 5
```

> presupuesto wan wan 1 gthres 10 % Límite de
presupuesto WAN 1 establecido en 10 GB

Comando Telnet: wan detect_mtu

Este comando le permite ejecutar un descubrimiento de MTU de WAN. El usuario puede especificar un destino IPv4 para hacer ping y encontrar el tamaño de MTU adecuado de la interfaz WAN.

Sintaxis

wan detectar_mtu*-i <Host/dirección IP> -s <tamaño_mtu> -d <reducir tamaño> -w <número WAN> -c <1~10>*

Sintaxis Descripción

Parámetro	Descripción
- i <Host/dirección IP>	Especifique el objetivo IPv4 para detectar. Si puede ser una dirección IPv4 o un nombre de dominio. Host/dirección IP: Ingrese la dirección IP/nombre de dominio del objetivo.
- s <tamaño_mtu>	Establezca la base de tamaño de MTU para Discovery. base_size: la configuración disponible es 1000 ~ 1500.
- d <disminuir tamaño>	Configure el tamaño de MTU para que disminuya entre detecciones. Disminuir tamaño: la configuración disponible es 1 ~ 100.
- w <número wan>	Especifique la interfaz WAN. Valor: Introduzca el número de interfaz WAN. 1: WAN1; 2: WAN2... y etc.
- c <valor>	Establezca los tiempos máximos de falla de ping durante un descubrimiento. conteo: Las configuraciones disponibles son 1 ~ 10. El valor predeterminado es 3.

Ejemplo

> wan detect_mtu -w 2 -i 8.8.8.8 -s 1500 -d 30 -c 10 detectando el
tamaño de mtu: 1500!!!

tamaño mtu: 1470!!!

Comando Telnet: wan detect_mtu6

Este comando le permite ejecutar un descubrimiento de MTU de WAN. El usuario puede especificar un objetivo IPv6 para hacer ping y encontrar el tamaño de MTU adecuado de la interfaz WAN.

Sintaxis

wan detectar_mtu6*-i <Host/dirección IP> -s <tamaño_mtu> -w <número WAN>*

Sintaxis Descripción

Parámetro	Descripción
- Yo <host/dirección IPv6>	Especifique el objetivo de IPv6 para detectar. Debe ser una dirección IP IPv6 o un nombre de host. Dirección IPv6: escriba la dirección IPv6 del destino.
- s <tamaño_base>	Especifique el tamaño de MTU. base_size: la configuración disponible es 1280 ~ 1500.
- w <número>	Especificar la interfaz WAN número: Introduzca el número de interfaz WAN. 1: WAN1; 2: WAN2... y etc.

Ejemplo

```
> wan detectar_mtu6 -w 2 -i 2404:6800:4008:c06::5e -s 1500
>
```

Comando Telnet: conmutación por error wan

Este comando se utiliza para configurar la WAN de conmutación por error.

Sintaxis

conmutación por error wan desactivada *<índice>*

conmutación por error wan en *<1><2><3><4><5><6>*

espectáculo de conmutación por error wan *<índice>* **wan**

conmutación por error newlb *<índice><argumento>*

Sintaxis Descripción

Parámetro	Descripción
conmutación por error desactivada <índice>	Configure la interfaz WAN especificada para que siempre esté activada. índice – Rangos de 1 a 6.
conmutación por error en *<1><2><3><4><5><6>*	Hay seis campos que representan diferentes opciones. Campo 1: especifique la interfaz WAN como WAN de conmutación por error escribiendo del 1 al 4. Campo 2: habilitar/deshabilitar la acción para la WAN de conmutación por error. Dicha acción es "Activo cuando se selecciona WAN [desconectar/alcanzar el umbral de tráfico]". 0 – Deshabilitar 1 - Habilitar Campo 3: habilitar/deshabilitar la acción para la WAN de conmutación por error. Dicha acción es "Activa cuando [alguna/todas] las WAN seleccionadas se desconectan o alcanzan el umbral de tráfico". 0 – Deshabilitar 1 - Habilitar Campo 4: especifique la WAN principal escribiendo del 1 al 4. La WAN principal se configurará para estar siempre encendida. Campo 5: especifique el umbral de tráfico [Umbral de descarga (Kbps)]. Campo 6 - Especifique el umbral de tráfico [Umbral de carga (Kbps)]. Por ejemplo, la WAN 2 se configurará como conmutación por error y estará activa cuando cualquiera de las WAN seleccionadas haya alcanzado el umbral de tráfico. WAN 4 es la WAN seleccionada. Umbral de descarga: 50 Kbpsl; Umbral de carga: 20 Kbps. Puede escribir de la siguiente manera: *conmutación por error wan en 2 1 0 4 50 20*
mostrar <índice>	Muestra la configuración de los parámetros para la interfaz WAN. índice – Rangos de 1 a 6.
newlb <índice><arg>	Establezca la latencia, la inestabilidad y el umbral de pérdida de paquetes de la interfaz WAN. índice - 1 a 6 arg - enumera lo siguiente: - a [todos]: 0=cualquier encuentro, 1=todos cumplen. - u [verificar] : 0=n/a, 1=verificar carga. - d [verificar] : 0=n/a, 1=verificar descarga. - l [verificar] : 0=n/a, 1=verificar latencia. - j [verificar] : 0=n/a, 1=verificar fluctuación. - p[verificar] : 0=n/a, 1=verificar pérdida de paquetes. - m[value] : valor de umbral de carga.

	- n [valor] : valor umbral de descarga. - x [valor] : valor del umbral de latencia. - y [valor] : valor umbral de fluctuación. - z [valor] : valor de umbral de pérdida de paquetes.

Ejemplo

```
> conmutación por error wan en 2 1 0 4 50 20
> wan failover show 2 wan2 Modo activo:
   Conmutación por error
         Activo cuando: cualquiera de las WAN seleccionadas alcanzó el umbral de tráfico, cualquier
  encuentro seguido:
>
```

Comando Telnet: configuración de hsportal

Este comando se utiliza para configurar un perfil (Hospot Web Portal) con una URL específica para acceder o mostrar un mensaje cuando un usuario inalámbrico/LAN se conecta a Internet a través de este enrutador.

Sintaxis

configuración deportiva -p*<perfil> [-l <lan>] [-s <ssid>] ...*

configuración deportiva -p*<perfil> -c*

Sintaxis Descripción

Parámetro	Descripción
- p <perfil>	Indicar perfil disponible para configurar. <perfil>: Introduzca el número de índice (1 a 4) del perfil.
- yo	Aplicar a las interfaces LAN (1 a 8). Por ejemplo: hsportal setup -p 1 -l 1, 2 (aplica LAN1 y LAN2)
- s	Aplicar a las interfaces WLAN (1 a 4). Por ejemplo: hsportal setup -p 1 -s 1, 2 (aplicar SSID1 y SSID2)
- a	Aplicar a las interfaces WLAN5G (1 a 4). Por ejemplo: hsportal setup -p 1 -a 1, 2 (aplicar SSID1 y SSID2)
- m	Seleccione el modo de inicio de sesión. 0: saltar 1: hacer clic 2: sociales 3: alfiler 4: social o pin Por ejemplo: configuración hsportal -p 1 -m 0
-f<0/1>	Significa habilitar o deshabilitar la función de Configurar inicio de sesión de Facebook. 0: deshabilitar. 1: habilitar.
- gramo <0/1>	Significa habilitar o deshabilitar la función de Configurar el inicio de sesión de Google. 0: deshabilitar. 1: habilitar.
- h<0/1>	Significa habilitar o deshabilitar la función de redirección HTTPS. 0: deshabilitar.

	1: habilitar.
-v<0/1>	Significa habilitar o deshabilitar la función de detección de portal. 0: deshabilitar. 1: habilitar.
- yo <cadena>	Significa configurar la ID de la aplicación. <cadena>: ingrese una cadena como ID de aplicación. Por ejemplo, para configurar la identificación de la aplicación de Facebook, puede escribir: > hsportal set -p 1 -f 1 -i this_is_app_id Perfil 1 establecido inicio de sesión de Facebook habilitado ... [OK] Perfil 1 establecido API ID. . . [DE ACUERDO]
- k <cadena>	Significa establecer la clave de la aplicación. <cadena>: ingrese una cadena como clave de aplicación. Por ejemplo, para configurar la clave de la aplicación de Google, puede escribir: > hsportal set -p 1 -g 1 -k keyforapp Perfil 1 establecido inicio de sesión de google habilitado ... [OK] Perfil 1 establecido CLAVE API. . . [DE ACUERDO]
-r <0/1/2>	Significa establecer el modo de página de destino. 0: URL fija. 1: solicitud del usuario. 2: boletín. Por ejemplo, > conjunto deportivo -p 1 -r 0 Perfil 1 establecer modo de página de destino 0 ... [OK]
- mi	Habilite el perfil especificado.
- d	Deshabilitar el perfil especificado.
- c <1/2/3/4>	Restablecer el perfil especificado. <1/2/3/4>: Introduzca el número de índice del perfil. Por ejemplo, > hsportal set -p 1 -c Restablecer perfil 1 ... [OK]
- o	Perfiles claros para todos los clientes.
- t <valor>	Establezca el tiempo de caducidad para el perfil especificado. <valor>: Ingrese un número de período de tiempo (unidad: minutos). Por ejemplo, k> configuración deportiva -p 1 -t 300 El perfil 1 establece el tiempo de caducidad 300 minutos... [OK]

Ejemplo

```
> hsportal setup -p 1 -c
Restablecer perfil 1 ... [OK]
> configuración deportiva -p 1 -r 0
Perfil 1 establecer modo de página de destino 0 ... [OK]
> hsportal setup -p 2 -g 1 -k app_key_google Perfil 2
configurado inicio de sesión de google habilitado... [OK] Perfil 2
configurado CLAVE API. . . [DE ACUERDO]
>
```

Comando Telnet: información deportiva

Este comando permite al usuario configurar los ajustes para la base de datos de puntos de acceso.

Sintaxis

información deportiva *<-e/-c/-n/-a/-m/-s>*

Sintaxis Descripción

Parámetro	Descripción
- mi <0/1>	Significa habilitar o deshabilitar la base de datos para registrar información. 0: deshabilitar. 1: habilitar.
- C	Significa borrar la base de datos de información del usuario.
- norte <0/1>	Significa habilitar o deshabilitar la notificación de información del usuario. 0: deshabilitar. 1: habilitar.
- un <0/1>	Significa habilitar o deshabilitar la función de copia de seguridad automática e iniciar un nuevo registro para la información del usuario. 0: deshabilitar. 1: habilitar.
- m <valor>	Significa configurar el objeto de notificación por correo electrónico. <valor>: ingrese el número de índice (1 a 10) de los objetos de notificación por correo electrónico.
- s <valor>	Significa establecer el objeto del proveedor de SMS. <valor>: Ingrese el número de índice (1 a 10) del objeto del servidor SMS para enviar correo cuando se exceda el almacenamiento de la base de datos.

Ejemplo

```
> info deportivo -e 1
Base de datos habilitada para registrar información... [OK]
> info deportivo -n 1
Notificación habilitada para información del usuario... [OK]
> info deportivo -a 1
Habilitó la copia de seguridad automática y comenzó un nuevo registro para la información del usuario ... [OK]
> info deportivo -m 1
El objeto de notificación por correo electrónico está bien configurado.
>
```

Comando Telnet: nivel deportivo

Este comando permite al usuario configurar el ancho de banda y la cuota de sesiones que solo se aplica a los clientes del portal web.

Sintaxis

nivel deportivo *-p <índice> [-e <habilitar>] [-t <mins>] ...*

Sintaxis Descripción

Parámetro	Descripción
- p <índice>	Significa especificar (agregar) un perfil de política de cuotas. <índice>: Ingrese el número de índice (1 a 20) del perfil de la política de cuotas.
- mi <0/1>	Significa habilitar o deshabilitar el perfil de la política de cuotas. 0: deshabilitar. 1: habilitar.

- t <valor>	Significa establecer el tiempo de expiración para la política de cuotas. <valor>: Introduzca un número (unidad:minutos).
- i <0/1> -o <valor>	Significa habilitar o deshabilitar la función de tiempo de espera inactivo 0: deshabilitar. 1: habilitar. Si está habilitado, - o <valor>: establezca el tiempo de espera de inactividad (unidad: minutos) si el tiempo de espera de inactividad está habilitado. Por ejemplo: nivel deportivo -p 1 -e 1 -i 1 -o 300
- d <valor>	Significa establecer la cantidad máxima de dispositivos que se pueden conectar a la red usando la misma cuenta. <valor>: Introduzca un número (0 a 100). "0" significa ilimitado. Por ejemplo: nivel deportivo -p 1 -e 1 -d 0
-b <0/1>	Significa habilitar o deshabilitar la función de límite de ancho de banda. 0: deshabilitar. 1: habilitar.
- ru <0/1>	Significa especificar la unidad de descarga del límite de ancho de banda. 0: kbps 1: Mbps
- tu <0/1>	Significa especificar la unidad de carga del límite de ancho de banda. 0: kbps. 1: Mbps.
-s<0/1>	Significa habilitar o deshabilitar el límite de sesión. 0: deshabilitar. 1: habilitar.
- n <valor>	Significa establecer un límite máximo de sesiones. <valor>: Introduzca un valor (0 a 6000). Por ejemplo: nivel deportivo -p 1 -s 1 -n
-U <kbps/mbps>	Significa especificar el límite de carga de ancho de banda. kbps mbps
- D <kbps/mbps>	Significa especificar el límite de descarga de ancho de banda. kbps mbps
- c <índice>	Significa eliminar un perfil de política de cuotas. <índice>: Ingrese el número de índice (1 a 20) del perfil de la política de cuotas.
-r<0/1>	Significa habilitar o deshabilitar la función de restricción de tiempo de reconexión. 0: deshabilitar. 1: habilitar.
- f <valor>	Significa establecer un período de tiempo para bloquear el mismo usuario que se vuelve a conectar a la red. <valor>: Ingrese un número (1 a 1439 minutos). Por ejemplo: nivel deportivo -p 1 -e 1 -r 1 -f 300
- g <valor>	Significa establecer un tiempo de reconexión para evitar que el mismo usuario se vuelva a conectar antes del tiempo establecido. <valor>: Introduzca la hora (01 a 23) y los minutos (0~59) (unidad: minutos). Por ejemplo: hsportal level -p 1 -e 1 -r 1 -f 23:15 (El mismo usuario

	puede volver a conectarse después de las 23:15 todos los días)

Ejemplo

```
> nivel deportivo -p 1 -e 1 -r 1 -f 30000
>
```

Comando Telnet: hsportal pin_gen

Este comando es para uso futuro.

Comando Telnet: hsportal json_pin_gen

Este comando permite al usuario configurar los ajustes de JSON para obtener el código PIN.

Sintaxis

json_pin_gen *<activar/desactivar/estado>* **json_pin_gen código de autenticación** *<código de autenticación>* **json_pin_gen filtro IP** *<activar/desactivar/estado>* **json_pin_gen filtro ipv4** *<FilterIdx> <obj> <ObjIndex>* **json_pin_gen filtro ipv6** *<FilterIdx> <obj> <ObjIndex>* **json_pin_gen filtro ipv4** *<FiltroIdx> borrar* **json_pin_gen filtro ipv6** *<FiltroIdx> borrar* **json_pin_gen AccFromInternet** *<activar/desactivar/estado>*

Sintaxis Descripción

Parámetro	Descripción
json_pin_gen <habilitar/deshabilitar/estado>	Significa habilitar/deshabilitar la función de JSON para obtener el código pin.
json_pin_gen código de autenticación <código de autenticación>	Significa establecer el código de autenticación para el mecanismo de código pin JSON. <authCode>: ingrese una cadena como autenticación de identidad.
json_pin_gen filtro IP <habilitar/deshabilitar/estado>	Significa habilitar/deshabilitar la autenticación basada en el objeto IPv4 o IPv6.
json_pin_gen ipv4Filter <Idx de filtro> <obj> <ÍndiceObj>	Significa configurar el objeto IPv4 para la autenticación. <Filteridx>: especifique el número de índice del perfil de objeto IPv4. <obj>: varía de 1 a 10. Se pueden configurar diez objetos. <ObjIndex>: ingrese el número de índice del perfil de objeto IPv4.
json_pin_gen ipv6Filter <Idx de filtro> <obj> <ÍndiceObj>	Significa configurar el objeto IPv6 para la autenticación. <Filteridx>: especifique el número de índice del perfil de objeto IPv6. <obj>: varía de 1 a 10. Se pueden configurar diez objetos. <ObjIndex>: ingrese el número de índice del perfil de objeto IPv6.
json_pin_gen ipv4Filter <FilterIdx> borrar	Significa borrar el filtro de objetos IPv4. <Filteridx>: especifique el número de índice del perfil de objeto IPv4.

json_pin_gen ipv6Filter <Idx de filtro> borrar	Significa borrar el filtro de objetos IPv6. <Filteridx>: especifique el número de índice del perfil de objeto IPv6.
json_pin_gen AccDesdeInternet <habilitar/deshabilitar/estado>	Significa establecer el mecanismo Generar código PIN desde Internet.

Ejemplo

```
> hsportal json_pin_gen habilitar json obtener
  mecanismo de código PIN: habilitar
> hsportal json_pin_gen authCode passcode1 Establecer
  el authCode
```

Comando Telnet: wl acl

Este comando permite al usuario configurar los ajustes de control de acceso inalámbrico.

Sintaxis

wl acl habilitar *<ssid1 ssid2 ssid3 ssid4>* **wl**

acl deshabilitar *<ssid1 ssid2 ssid3 ssid4>*

wl acl añadir *<MAC><ssid1 ssid2 ssid3 ssid4><comentario><aislar>* **wl**

acl del *<MAC>*

modo wl acl *<ssid1 ssid2 ssid3 ssid4><blanco/negro>* **wl**

acl mostrar

modo de presentación wl acl

wl acl claro

Sintaxis Descripción

Parámetro	Descripción
habilitar <ssid1 ssid2 ssid3 ssid4>	Significa habilitar la configuración para SSID1, SSID2, SSID3 y SSID4.
deshabilitar <ssid1 ssid2 ssid3 ssid4>	Significa deshabilitar la configuración de SSID1, SSID2, SSID3 y SSID4.
agregar <MAC><ssid1 ssid2 ssid3 ssid4><comentario><aislar>	Significa asociar una dirección MAC a la configuración de control de acceso de ciertas interfaces SSID. La configuración de aislamiento limitará las capacidades de red del cliente inalámbrico para acceder únicamente a la LAN inalámbrica. Formato [MAC]: xx-xx-xx-xx-xx-xx o xx:xx:xx:xx:xx:xx o xx.xx.xx.xx.xx.xx
del<MAC>	Significa eliminar una entrada de dirección MAC definida en la lista de control de acceso.
modo <ssid1 ssid2 ssid3 ssid4><blanco/negro>	Significa establecer una lista blanca/negra para cada SSID.
espectáculo	Significa mostrar el estado del control de acceso.
modo de exhibición	Significa mostrar el modo para cada SSID.
claro	Significa limpiar toda la configuración de control de acceso.

Ejemplo

```
> wl acl showmode
  ssid1: ninguno
  ssid2: ninguno
  ssid3: ninguno
  ssid4: ninguno
> wl acl agregar 14:49: BC: 0D: 8F: 00 ssid1 ssid2 prueba aislar Conjunto
Listo !!
> mostrar wl acl
- - - - - - - - - - Estado del filtro de direcciones Mac---------
  SSID1: Deshabilitar
  SSID2: Deshabilitar
  SSID3: Deshabilitar
  SSID4: Deshabilitar

  - - - - - - - - - - Lista de direcciones MAC----------
  Índice    Atributo    Dirección MAC    SSID asociados    Comentario
     1         s        14:49:bc:0d:8f:00   SSID1 SSID2      prueba

  s: Aislar la estación de LAN
>
```

Comando Telnet: configuración wl

Este comando permite a los usuarios configurar ajustes generales y ajustes de seguridad para la conexión inalámbrica.

Sintaxis

modo de configuración wl*<valor>* **modo de**

configuración wl muestra el canal de

configuración wl*<número>* **canal de**

configuración wl mostrar preámbulo de

configuración wl*<habilitar>* **wl configuración**

txburst*<habilitar>*

wl config ssid*<ssid_num habilitar ssid_name <hidden_ssid>>*

seguridad de configuración wl*<SSID_NUMBER><modo>*

tasa de configuración de wl*<ssid_num habilitar carga descargar >* **wl**

config aislar*<ssid_num miembro de LAN>* **wl configuración dtim***<*

valor>/ mostrar

período de baliza de configuración de wl*<valor> / mostrar* **wl**

configuración de radio*<1/0>/mostrar* **fragmento de**

configuración wl*<valor>/ mostrar* **rts de configuración de wl***<*

valor> / mostrar **wl configuración rate_alg***<valor> / mostrar*

país de configuración wl*<valor> / mostrar*

Sintaxis Descripción

Parámetro	Descripción
modo <valor>	Significa seleccionar el modo de conexión para la conexión inalámbrica. Los ajustes disponibles son: "11bgn", "11gn", "11n", "11bg", "11g" o "11b".
espectáculo de modo	Significa mostrar cuál es el modo inalámbrico actual.
canal <número>	Significa el canal de frecuencia de la LAN inalámbrica.

	Los ajustes disponibles son 0,1,2,3,4,5,6,7,8,9,10,11,12 y 13. número=0, significa Auto numero=1, significa Canal 1.... numero=13, significa Canal 13.
preámbulo <habilitar>	Significa definir la longitud del campo de sincronización en un paquete 802.11. La mayoría de las redes inalámbricas modernas utilizan un preámbulo corto con un campo de sincronización de 56 bits en lugar de un preámbulo largo con un campo de sincronización de 128 bits. Sin embargo, algunos dispositivos de red inalámbrica 11b originales solo admiten un preámbulo largo. 0: deshabilitar para usar un preámbulo largo. 1: habilitar el uso de un preámbulo largo.
txburst <habilitar>	Significa mejorar el rendimiento en la transmisión de datos alrededor de un 40%* más (habilitando**Ráfaga de transmisión**). Está activo solo cuando ambos lados del punto de acceso y la estación (en el cliente inalámbrico) invocan esta función al mismo tiempo. 0: deshabilitar la función. 1: habilitar la función.
ssid <ssid_num habilitar nombre_ssid <ssid_oculto>>	Significa establecer el nombre del SSID, ocultar el SSID si es necesario. *ssid_num:* Escriba 1, 2, 3 o 4 para especificar SSID1, SSID2, SSID3 o SSID4. *nombre_ssid*: Asigne un nombre para el SSID especificado. *oculto_ssid*: Escriba 0 para ocultar el SSID o 1 para mostrar el SSID
seguridad <SSID_NUMBER><modo><clave> <índice>	Significa configurar los ajustes de seguridad para la conexión inalámbrica. *SSID_NUMBER*: Escriba 1, 2, 3 o 4 para especificar SSID1, SSID2, SSID3 o SSID4. *modo*: Los ajustes disponibles son: deshabilitar: Sin seguridad. wpa1x: Solo WPA/802.1x wpa21x: Solo WPA2/802.1x wpamix1x: mixto (solo WPA+WPA2/802.1x) wep1x: Solo WEP/802.1x PSK WPA: PSK WPA wpa2psk: WPA2/PSK wpamixpsk: Mixto (WPA+WPA2)/PSK wep: WEP *Índice de Clave*: Además, tienes que añadir claves para*wpapsk, wpa2psk, wpamixpsky Wep*y especifique el número de índice de los perfiles de programación que seguirá la conexión inalámbrica. Las claves WEP deben estar en formato de cadena de texto 5/13 ASCII o 10/26 dígitos hexadecimales; Las claves WPA deben tener una cadena de texto ASCII de 8~63 o un formato de 64 dígitos hexadecimales.
ratectl <ssid_num habilitar carga descarga>	Significa establecer el control de velocidad para el SSID especificado. *ssid_num:*Elija 1, 2, 3 o 4 para especificar SSID1, SSID2, SSID3 o SSID4. *permitir*: Significa habilitar la función de control de tasa para el SSID especificado. 0: deshabilitar y 1: habilitar. *subir*: Significa configurar el control de velocidad para la carga de datos. La unidad es kbps. *descargar*: Significa configurar el control de velocidad para la descarga de datos. La unidad es kbps.
aislar <ssid_num lan miembro>	Significa aislar la conexión inalámbrica para LAN y/o Miembro. *lan*–Puede hacer que los clientes inalámbricos (estaciones) con marcación remota y usuarios de LAN a LAN no accedan entre sí. *miembro*–Puede hacer que los clientes inalámbricos (estaciones) con el mismo SSID no accedan entre sí.

dtim <valor> / mostrar	Establezca el valor DTIM. valor: 1 a 255 show: muestra la configuración de DTIM.
período de baliza <valor> / *espectáculo*	Establezca el valor del período de baliza. valor: 20 a 1023 (milisegundos) show: muestra la configuración del período de la baliza.
radio <1/0>/programa	Habilite o deshabilite la radio inalámbrica. 1/0: Escriba 1 para habilitar; 0 para deshabilitar. show: muestra la configuración de la radio.
frag <valor>/ mostrar	Establezca el valor del fragmento. valor: 256 a 2346 show: muestra la configuración del fragmento.
rts <valor> / mostrar	Establezca el valor RTS. valor: 1 a 2347 show: muestra la configuración RTS.
rate_alg <valor>/ mostrar	Configure el algoritmo para la tasa ALG. valor: 0 para algoritmo antiguo; 1 para el nuevo algoritmo. show: muestra la configuración de tasa de ALG.
país <valor>/ mostrar	Configure el código de país para un país. valor: dos letras mayúsculas, p. ej., TW, Reino Unido mostrar: muestra la configuración del código del país.

Ejemplo

```
> modo wl config 11bgn El
  modo actual es 11bgn
% <Nota> Reinicie la conexión inalámbrica después de configurar el canal
> wl config canal 13 El canal
  actual es 13
% <Nota> Reinicie la conexión inalámbrica después de configurar el canal.
> wl config preámbulo 1 El
  preámbulo largo está habilitado
% <Nota> Reinicie la conexión inalámbrica después de configurar los parámetros.
> wl config ssid 1 habilitar dray SSID
  Habilitar Hide_SSID Nombre 1 1
                        0                carro pesado
% <Nota> Reinicie la conexión inalámbrica después de configurar los parámetros.
> wl config seguridad 1 wpa1x
%% Configuración de seguridad Wlan configurada:
% SSID1
%% Modo: wpa1x
%% La tarjeta inalámbrica debe restablecerse para que las configuraciones surtan
efecto %% (Comando Telnet: reinicio wl)
> wl config country TW Establecer
  código de país inalámbrico TW
% <Nota> Reinicie la conexión inalámbrica después de configurar los parámetros.
```

Comando Telnet: conjunto wl

Este comando permite a los usuarios configurar los ajustes inalámbricos básicos.

Sintaxis

conjunto*<SSID><CHAN[Es]>* **wl**

establecer txburst*<habilitar>*

Sintaxis Descripción

Parámetro	Descripción
SSID	Significa Ingresar el SSID para el enrutador. El carácter máximo que puede utilizar es 32.
CHAN[Es]	Significa especificar el canal requerido para el enrutador. *CAN:*El rango para el número está entre 1 ~ 13. *es*: tipo*en*para habilitar la función; tipo*apagado*para deshabilitar la función.
txburst <habilitar>	Significa mejorar el rendimiento en la transmisión de datos alrededor de un 40%* más (habilitando**Ráfaga de transmisión**). Está activo solo cuando ambos lados del punto de acceso y la estación (en el cliente inalámbrico) invocan esta función al mismo tiempo. 0: deshabilitar la función. 1: habilitar la función.

Ejemplo

```
> wl establece MKT 2 en % Nueva
configuración de Wlan es: % SSID
= MKT
% Canal=2
% Wl está habilitado
```

Comando Telnet: acto wl

Este comando permite a los usuarios activar la configuración inalámbrica.

Sintaxis

actuaremos*<es>*

Sintaxis Descripción

Parámetro	Descripción
es	Significa habilitar o deshabilitar la función de aislamiento VPN. 0: diablo 1: habilitar

Ejemplo

```
> actuaremos en
% Establezca Wlan en Habilitar.
```

Comando Telnet: escaneo wl

Este comando permite a los usuarios realizar escaneos AP.

Sintaxis

escanear*<inicio>*

escanear*colocar**<wlist/blist> <MAC>**

escanear*colocar**<tiempo> <tiempo>**

escanear*del**<wlist/blist><MAC>**

escanear *filtrar* *<ssid/canal/mac>*

escanear *espectáculo* *<0/1/2/3/4/5>*

Sintaxis Descripción

Parámetro	Descripción
comenzar	Significa iniciar el escaneo AP.
establecer <wlist/blist> <MAC>	Establecer lista blanca/lista de bloqueo/tiempo de escaneo. *lista* -Significa establecer una lista blanca para aprobar. La dirección MAC debe agregarse al final. p.ej,*conjunto de exploración wl wlist 001122aabbcc* *lista* -Significa establecer una lista negra para el bloqueo. La dirección MAC debe agregarse al final.
colocar<tiempo> <tiempo>	Configure el tiempo de escaneo. tiempo–Significa establecer el tiempo de escaneo. time - El valor de tiempo (2~5 segundos) debe agregarse al final. p.ej,*tiempo de ajuste de escaneo wl 5*
del <wlist/blist><MAC>	Eliminar lista blanca/lista de bloqueo. p.ej, *wl scan del wlist 001122aabbcc*
filtrar <ssid/canal/mac>	Establece el filtro que quieras. *ssid*-escaneando el AP basado en la configuración de SSID*. canal* - escaneando el AP basado en la configuración del canal*. Mac* -escanear el AP basado en la configuración de la dirección MAC*..*
mostrar <0/1/2/3/4/5>	Se utiliza para mostrar la lista de puntos de acceso. 0 - mostrar la lista blanca 1 - mostrar la lista de bloques, 2 - mostrar lista gris/desconocida, 3 - mostrar toda la lista 4. lista blanca (en configuración) 5. lista de bloqueo (en configuración) Nota: 0~3 es la lista de exploración del enrutador, 4~5 es la lista almacenada en la configuración.

Ejemplo

```
> conjunto de exploración wl wlist 001122aabbcc
> inicio de escaneo wl
> wl escaneo mostrar 3
>
```

Comando Telnet: wl stamgt

Este comando se usa para configurar el tiempo de conexión y el tiempo de reconexión para cada SSID que el cliente inalámbrico usó para acceder a Internet.

Sintaxis

wl stamgt *<habilitar/deshabilitar> <ssid_num>* **wl**

stamgt *mostrar <ssid_num>* **wl stamgt** *establecer*

<ssid_num> <c> <r> **wl stamgt** *restablecer*

<ssid_num>

Sintaxis Descripción

Parámetro	Descripción

habilitar deshabilitar	Significa habilitar/deshabilitar el control de gestión de la estación.
ssid_num	Significa selección de canal. Canal disponible para 2.4G: 0/1/2/3 Canal disponible para 5G: 4/5/6/7.
espectáculo	Significa mostrar el estado o la configuración del canal seleccionado.
C	Significa tiempo de conexión. La unidad es minuto.
r	Significa tiempo de reconexión. La unidad es minuto.

Ejemplo

```
> wl stamgt habilitar 1
% Estado de gestión de la estación: habilitado
> wl stamgt set 1 60 60
> wl stamgt mostrar 1
NO. SSID          BSSID              Tiempo de conexión   Tiempo de reconexión
1. Draytek        00:11:22:aa:bb:cc  0d:0:58:26           0d:0:0
```

Comando Telnet: wl iso_vpn

Este comando permite a los usuarios activar la función de aislamiento de VPN.

Sintaxis

wl iso_vpn *<ssid> <Es>*

Sintaxis Descripción

Parámetro	Descripción
ssid	Significa el número de SSID. 1: SSID1 2: SSID2 3: SSID3 4: SSID4
es	Significa habilitar o deshabilitar la función de aislamiento VPN. 0: deshabilitar 1: habilitar

Ejemplo

```
> wl iso_vpn 1 en
% ssid: 1 aislar vpn en: 1
```

Comando Telnet: wl wmm

Este comando permite a los usuarios configurar WMM para conexión inalámbrica. Define los niveles de prioridad para cuatro categorías de acceso derivadas de 802.1d (pestañas de priorización).

Sintaxis

wl wmm ap *QueIdx Aifsn Cwmin Cwmax Txop ACM* **wl wmm bss** *QueIdx Aifsn Cwmin Cwmax Txop ACM* **wl wmm ack** *Que0_Ack Que1_Ack Que2_Ack Que3_Ack* **wl wmm habilitar** *SSID0 SSID1 SSID2 SSID3* **wl wmm apsd** *valor* **wl wmm espectáculo**

Sintaxis Descripción

Parámetro	Descripción
ap	Significa configurar WMM para el punto de acceso.
bss	Significa configurar WMM para clientes inalámbricos.
reconocer	Significa mapear a la configuración de la política Ack de AP WMM.
permitir	Significa habilitar el WMM para cada SSID. 0: deshabilitar 1: habilitar
apsd <valor>	Significa activar/desactivar la función ASPD (entrega automática de ahorro de energía). 0: deshabilitar 1: habilitar
espectáculo	Muestra el estado actual de WMM.
QueIdx	Significa el número de la cola a la que se aplicará la configuración de WMM. Hay cuatro colas, mejor esfuerzo, fondo, voz y video.
aifsn	Controla cuánto tiempo espera el cliente para cada transmisión de datos.
Cwmín/ Cwmáx	**CWMín**significa contención Window-Min y**CW Máx.**significa contención Window-Max. Especifique el valor entre 1 y 15.
Txop	Quiere decir oportunidad de transmisión. Especifique el valor entre 0 y 65535.
MCA	Puede restringir que las estaciones usen una clase de categoría específica si está habilitada. 0: deshabilitar 1: habilitar

Ejemplo

```
> wl wmm ap 0 3 4 6 0 0
  QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
> wl wmm habilitar 1 0 1 0
  WMM_SSID0 =1, WMM_SSID1 =0,WMM_SSID2 =1,WMM_SSID3 =0
> wl wmm mostrar
  Habilitar WMM: SSID0 = 1, SSID1 = 0, SSID2 = 1, SSID3 = 0 APSD =
  0
  QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0 QueIdx=1:
  APAifsn=7,APCwmin=4,APCwmax=10, APTxop=0,APACM=0 QueIdx=2:
  APAifsn=1,APCwmin=3,APCwmax=4, APTxop=94,APACM=0 QueIdx=3:
  APAifsn=1,APCwmin=2,APCwmax=3, APTxop=47,APACM=0 QueIdx=0: BSSAifsn=3,
  BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0 QueIdx=1:
  BSSAifsn=7,BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0 QueIdx=2:
  BSSAifsn=2,BSSCwmin=3, BSSCwmax=4, BSSTxop=94,BSSACM=0 QueIdx=3:
  BSSAifsn=2,BSSCwmin=2,BSSCwmax=3, BSSTxop=47,BSSACM=0 AckPolicy[0]=0:
  AckPolicy[1]=0,AckPolicy[ 2]=0,AckPolicy[3]=0
```

Comando Telnet: wl ht

Este comando le permite configurar los ajustes inalámbricos.

Sintaxis

peso alto peso corporal*valor*

wl ht gi*valor*

wl ht badecline*valor*
wl ht autoba*valor* **wl**
ht rdg*valor*
wl ht msdu*valor* **wl ht**
txpower*valor* **wl ht**
antena*valor* **wl ht**
greenfield*valor*

Sintaxis Descripción

Parámetro	Descripción
valor bw	El valor que puede escribir es 0 (para BW_20) y 1 (para BW_40).
valor gi	El valor que puede escribir es 0 (para GI_800) y 1 (para GI_4001)
valor de declinación	El valor que puede escribir es 0 (para deshabilitar) y 1 (para habilitar).
valor de autoba	El valor que puede escribir es 0 (para deshabilitar) y 1 (para habilitar).
valor de lectura	El valor que puede escribir es 0 (para deshabilitar) y 1 (para habilitar).
valor msdu	El valor que puede escribir es 0 (para deshabilitar) y 1 (para habilitar).
valor de txpower	El valor que puede escribir oscila entre 1 y 6 (nivel).
valor de la antena	El valor que puede escribir oscila entre 0 y 3. 0: 2T3R 1: 2T2R 2: 1T2R 3: 1T1R
valor de campo nuevo	El valor que puede escribir es 0 (para modo mixto) y 1 (para campo verde).

Ejemplo

```
> wl ht bw valor 1 BW=0

 <Nota> Reinicie la conexión inalámbrica después de establecer nuevos parámetros.
> reiniciaremos
 Reinicio inalámbrico .....
```

Comando Telnet: reinicio wl

Este comando le permite reiniciar la configuración inalámbrica.

Ejemplo

```
> reiniciaremos
 Reinicio inalámbrico .....
```

Comando Telnet: wl wds

Este comando le permite configurar los ajustes de WDS.

Sintaxis

modo wds*[valor]*
seguridad wds*[valor]*
wl wdsap*[valor]* **wl wds**
hola*[valor]* **wl wds**
estado

wl wds mostrar

wl wds mac*[valor]*

wl wds al ras

Sintaxis Descripción

Parámetro	Descripción
modo [valor]	Significa especificar el modo de conexión para WDS. [valor]: Los ajustes disponibles son: d: Deshabilitar b: Puente r: repetidor
seguridad [valor]	Significa configurar el modo de seguridad con claves cifradas para WDS. *modo*: Los ajustes disponibles son: deshabilitar: Sin seguridad. wep: WEP wpapsk [clave]: PSK WPA wpa2psk [clave]: WPA2/PSK *llave*: Además, tienes que añadir claves para *wpapsk, wpa2psk*, y *Wep* y especifique el número de índice de los perfiles de programación que seguirá la conexión inalámbrica. Las claves WEP deben estar en formato de cadena de texto 5/13 ASCII o 10/26 dígitos hexadecimales; Las claves WPA deben tener una cadena de texto ASCII de 8~63 o un formato de 64 dígitos hexadecimales. p.ej, *wl seguridad dual wds deshabilitar wl seguridad dual wds wep 12345 wl seguridad dual wds wpa2psk 12345678*
ap [valor]	Significa habilitar o deshabilitar la función AP. Valor: 1 – habilitar la función. 0 – deshabilitar la función.
hola [valor]	Significa enviar un mensaje de saludo al extremo remoto (par). Valor: 1 – habilitar la función. 0 – deshabilitar la función.
estado	Significa mostrar el estado del enlace WDS para una conexión de 2,4 GHz.
espectáculo	Significa mostrar la configuración WDS actual.
mac agregar [dirección de índice]	agregar *[dirección de índice]* – *A*Agregue la entrada de MAC del par en la tabla MAC de WDS de repetidor/puente.
borrar/deshabilitar/habilitar mac [índice/todos]	borrar/deshabilitar/habilitar *[índice/todos]*-Borre, deshabilite, habilite las entradas de MAC especificadas o todas en la tabla MAC de WDS de repetidor/puente. p.ej, *wl dual wds mac habilitar 1*
enjuagar	Significa restablecer toda la configuración de WDS.

Ejemplo

```
> estado wds wl
Habilite primero la función de saludo de WDS.

> wl wds hola 1
% <Nota> Reinicie el enrutador después de configurar los parámetros.

> estado wds wl
```

Comando Telnet: wl apcli

Este comando permite a los usuarios configurar el modo de cliente AP para conexión inalámbrica (2,4 GHz).

Sintaxis

wl aplicación mostrar

wl apcli habilitar *<1/0>* **wl**

aplicación de seguridad *<modo>*

wl appli ssid *<nombre_ssid>* **wl**

apcli bssid *<dirección mac>*

Sintaxis Descripción

Parámetro	Descripción
espectáculo	Muestra el estado actual del cliente AP inalámbrico.
habilitar <1/0>	Significa habilitar el modo de cliente AP inalámbrico de 2,4 GHz. 1 – habilitar 0 – deshabilitar
seguridad <modo>	Se pueden seleccionar varios modos: Deshabilitar: deshabilita la configuración de seguridad. wpapsk [clave]: se utilizará la clave precompartida WPA. Las claves deben comenzar con 0x para ser identificadas como una clave numérica hexadecimal. Las claves WPA deben estar en formato de 8~63 cadenas ASCII o 64 dígitos hexadecimales. wpa2psk [clave]: se utilizará la clave precompartida WPA2. Las claves deben comenzar con 0x para ser identificadas como una clave numérica hexadecimal. Las claves WPA deben estar en formato de 8~63 cadenas ASCII o 64 dígitos hexadecimales. wpamixpsk [clave]: se utilizará la clave precompartida mixta WPA. Las claves deben comenzar con 0x para ser identificadas como una clave numérica hexadecimal. Las claves WPA deben estar en formato de 8~63 cadenas ASCII o 64 dígitos hexadecimales. wep [clave] [índice]: se utilizará la clave WEP. Debe ingresar la cadena de clave y especificar el número de índice del perfil que se aplicará. Las claves WEP deben estar en formato de cadena 5/13 ASCII o 10/26 dígitos hexadecimales.
ssid <nombre_ssid>	Especifique el SSID para el cliente AP inalámbrico de 2,4 GHz.
bssid <dirección mac>	Ingrese la dirección MAC para el cliente AP inalámbrico de 2,4 GHz.

Ejemplo

```
> wl apcli enable 1 Wireless AP-Clinet
está habilitado
> wl apcli mostrar
% AP-Clinet inalámbrico habilitado % SSID
actual en prueba
%% Modo de seguridad: deshabilitar
% El cliente inalámbrico está desconectado %%
velocidad de datos=---, modo=---, señal=0%
```

Comando Telnet: wl btnctl

Este comando le permite habilitar o deshabilitar el control de botón inalámbrico.

Sintaxis

wl btnctl *<valor>*

Sintaxis Descripción

Parámetro	Descripción
valor	0: deshabilitar 1: habilitar

Ejemplo

```
> wl btnctl 1
Habilitar control de botón inalámbrico El control de
botón inalámbrico actual está activado
>
```

Comando Telnet: wl iwpriv

Este comando está reservado para la depuración de RD. No los use.

Comando Telnet: wl ce_cert

Para compartir la red inalámbrica, los clientes WiFi pueden ser autenticados por el enrutador Vigor con un certificado específico.

Sintaxis

wl ce_cert*<on/off>[<comando><parámetro>|...]*

rendimiento wl ce_cert

wl ce_cert*R61 <valor>* **wl**

ce_cert*espectáculo R61*

Sintaxis Descripción

Parámetro	Descripción
<activar/desactivar>	Habilite o deshabilite el certificado. encendido - Habilitar. apagado - Deshabilitar.
[<comando><parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede ingresar varios comandos en una línea. Hay diez parámetros; Ráfaga de Tx HT_RDG HT_AutoBA HT_BARechazar EDCCA_AP_STA_TH EDCCA_AP_AP_TH EDCCA_FALSE_CCA_TH EDCCA_ED_TH <valor> - EDCCA_BLOCK_CHECK_TH EDCCA_AP_RSSI_TH
Ráfaga de transmisión <0/1>	Habilite o deshabilite la función TxBurst. 1 - Habilitar; 0 - Deshabilitar
HT_RDG <0/1>	Habilite o deshabilite la función HT_RDG. 1 - Habilitar; 0 - Deshabilitar

HT_AutoBA <0/1>	Habilite o deshabilite la función HT_AutoBA. 1 - Habilitar; 0 - Deshabilitar
HT_BARechazar <0/1>	Habilite o deshabilite la función HT_BADecline. 1 - Habilitar; 0 - Deshabilitar
EDCCA_AP_STA_TH <valor	Establezca un número para EDCCA_AP_STA_TH. <valor> - Rangos de 1 a 255.
EDCCA_AP_AP_TH <valor>	Establezca un número para EDCCA_AP_AP_TH. <valor> - Rangos de 1 a 255.
EDCCA_FALSE_CCA_TH <valor>	Establezca un número para EDCCA_FALSE_CCA_TH. <valor>: cualquier número mayor que 0 (entero).
EDCCA_ED_TH <valor>	Establezca un número para EDCCA_ED_TH. <valor> - Rangos de 1 a 255.
EDCCA_BLOCK_CHECK_TH <valor>	Establezca un número para EDCCA_BLOCK_CHECK_TH. <valor>: cualquier número mayor que 0 (entero).
EDCCA_AP_RSSI_TH <valor>	Establezca un número para EDCCA_AP_RSSI_TH. <valor> - Rangos de 0 a 25.
actuación	Muestra los parámetros con los valores para obtener el mejor rendimiento.
R61 <valor>	Establezca un número para BBP_R61. <valor> - Rangos de 1 a 10.
espectáculo R61	Muestra el estado de configuración de R61.

Ejemplo

```
> wl ce_cert on 0 1 1 0 255 255 3000 90 8 -80
<Nota> Reinicie la conexión inalámbrica después de establecer nuevos parámetros.

ED_CERT está habilitado
Ráfaga de Tx                :0 (predeterminado: 0)
HT_RDG                      :1 (por defecto :0)
HT_AUTO_BA      :1 (predeterminado :1)
HT_BA_DECLINE           :0 (predeterminado: 0)
EDCCA_AP_STA_TH             :255
EDCCA_AP_AP_TH              :255
EDCCA_FALSE_CCA_TH          :3000
EDCCA_ED_TH                 :90
EDCCA_BLOCK_CHECK_TH        :8
EDCCA_AP_RSSI_TH            :-80
> wl ce_cert performance Parámetros para el
mejor rendimiento: ED_CERT está habilitado

Ráfaga de Tx            :0
HT_RDG                  :1
HT_AUTO_BA      :1
HT_BA_DECLINE :0
EDCCA_AP_STA_TH         :20
EDCCA_AP_AP_TH          :20
EDCCA_FALSE_CCA_TH      :180
EDCCA_ED_TH             :90
EDCCA_BLOCK_CHECK_TH:2
EDCCA_AP_RSSI_TH :-80
<Nota> Reinicie la conexión inalámbrica.
>
```

Comando Telnet: wl stalist

Este comando se utiliza para mostrar la estación inalámbrica que accede a Internet a través del enrutador Vigor.

Sintaxis

wl estalista

Ejemplo

```
> wl estalista
wl espectáculo estalista        : muestra la lista de estaciones :
wl stalist num                  muestra el número de estaciones
wl stalist vecino: muestra la lista de estaciones vecinas
```

Comando Telnet: wl set8021x

Este comando le permite configurar el servidor externo o interno utilizado por el enrutador Vigor para la autenticación inalámbrica.

Sintaxis

wl set8021x –t <*0/1***>**

conjunto wl8021x –v

Sintaxis Descripción

Parámetro	Descripción
- t	Especifique el tipo (externo o interno) del servidor de autenticación inalámbrica. 0: indica el servidor RADIUS externo. 1- Indicar el servidor local 802.1x.
-v	Ver la configuración de 802.1x.

Ejemplo

```
> conjunto wl8021x -t 1
% <Nota> Reinicie la conexión inalámbrica después de configurar los parámetros.
> conjunto wl8021x -v
  El tipo 802.1X es: Local 802.1X
>
```

Comando Telnet: wl bndstrg

Este comando permite a los usuarios configurar los ajustes para Band Steering (2.4GHz).

Sintaxis

espectáculo wl bndstrg

wl bndstrg habilitar*<1/0>* **wl bndstrg chk_time***<valor>*

Sintaxis Descripción

Parámetro	Descripción
espectáculo	Muestra el estado actual de la función Band Steering.
habilitar<1/0>	Significa habilitar el modo de cliente AP inalámbrico de 2,4 GHz. 1 – habilitar

	0 – deshabilitar
chk_time <valor>	Si la estación inalámbrica no tiene la capacidad de conexión a la red de 5 GHz, el sistema deberá esperar y verificar durante varios segundos (15 segundos, de forma predeterminada) para realizar la conexión a la red de 2,4 GHz. Especifique el límite de tiempo para que el enrutador Vigor detecte al cliente inalámbrico. *[valor] – 1 a 60 segundos.*

Ejemplo

```
> wl bndstrg muestra la dirección
de la banda: deshabilitar
chk_time: 15 segundos
> wl bndstrg chk_time 50 30 argv[0]:chk_time,
argv[1]:50, argv[2]:30

%% La tarjeta inalámbrica debe restablecerse para que las configuraciones surtan
efecto %% (Comando Telnet: reinicio wl)
```

Comando Telnet: wl artfns

Este comando permite a los usuarios configurar la función de imparcialidad del tiempo aire para la conexión inalámbrica (2,4 GHz).

Sintaxis

wl artfns habilitar *<valor>* **wl**
artfns trg_num *<valor>* **show**
de wl artfns

Sintaxis Descripción

Parámetro	Descripción
habilitar <valor>	Significa habilitar la función de imparcialidad del tiempo aire inalámbrico. 1 – habilitar 0 – deshabilitar
trg_num <valor>	Establezca un umbral cuando el número de la estación activa alcance este número, se aplicará la función de equidad de tiempo aire. Los valores disponibles serán de 2 a 64.
espectáculo	Mostrar el estado actual (habilitar o deshabilitar) y activar el número de cliente para la función de equidad de tiempo aire.

Ejemplo

```
> wl artfns habilitar 1
> wl artfns trg_num 3
> wl artfns muestra equidad en el
tiempo de uso: habilitar trg_num:
3
>
```

Comando Telnet: wl drayrs

Este comando permite al usuario configurar los ajustes de Roaming para clientes inalámbricos.

Sintaxis

wl drayrs *establecer <modo><rs_low><rs_low_security><delta>* **wl**
drayrs *Reanudar*

wl drayrs*espectáculo*

Sintaxis Descripción

Parámetro	Descripción
establecer <modo> <rs_low> <rs_baja_seguridad><delta>	Seleccione un modo para itinerancia. 0 - deshabilitar 1 - RSSI estrictamente mínimo 2 - RSSI mínimo rs_low: establece un valor de RSSI estrictamente mínimo (62~86). rs_low_security: establezca un valor de RSSI mínimo (62~86). delta: establezca un valor de RSSI AP adyacente (1~20).
Reanudar	Reinicie para activar la función de roaming.
espectáculo	Muestra la configuración actual de la función de roaming.

Ejemplo

```
> wl drayrs show %
Mode : Deshabilitar %
    rs_bajo              : -73
%   rs_low_secure        : -66
%   delta                : 5
>
```

Comando Telnet: wl_dual acl

Este comando permite al usuario configurar los ajustes de control de acceso inalámbrico (5 GHz).

Sintaxis

habilitar wl_dual acl*<ssid1 ssid2 ssid3 ssid4>*

wl_dual acl deshabilitar*<ssid1 ssid2 ssid3 ssid4>*

wl_dual acl añadir <*MAC><ssid1 ssid2 ssid3 ssid4> <comentario> aislar*

wl_dual acl del <*MAC>*

modo wl_dual acl*<ssid1 ssid2 ssid3 ssid4> <blanco/negro>*

espectáculo wl_dual acl

modo de presentación wl_dual acl

wl_dual acl claro

Sintaxis Descripción

Parámetro	Descripción
habilitar <ssid1 ssid2 ssid3 ssid4>	Significa habilitar la configuración para SSID1, SSID2, SSID3 y SSID4.
deshabilitar <ssid1 ssid2 ssid3 ssid4>	Significa deshabilitar la configuración de SSID1, SSID2, SSID3 y SSID4.
agregar<MAC><ssid1 ssid2 ssid3 ssid4><comentario>	Significa asociar una dirección MAC a la configuración de control de acceso de ciertas interfaces SSID. La configuración de aislamiento limitará las capacidades de red del cliente inalámbrico para acceder únicamente a la LAN inalámbrica. Formato [MAC]: xx-xx-xx-xx-xx-xx o xx:xx:xx:xx:xx:xx o xx.xx.xx.xx.xx.xx
Aislar	Significa aislar la conexión inalámbrica del cliente inalámbrico (identificado con la dirección MAC) de la LAN.
del<MAC>	Significa eliminar una entrada de dirección MAC definida en el acceso

	lista de control Formato [MAC]: xx-xx-xx-xx-xx-xx o xx:xx:xx:xx:xx:xx o xx.xx.xx.xx.xx.xx
modo <ssid1 ssid2 ssid3 ssid4> <blanco/negro>	Significa establecer una lista blanca/negra para cada SSID.
espectáculo	Significa mostrar el estado actual del control de acceso.
modo de exhibición	Significa mostrar el modo para cada SSID.
claro	Significa borrar todas las configuraciones de control de acceso.

Ejemplo

```
> wl_dual acl showmode
  SSID1: Ninguno
  SSID2: Ninguno
  SSID3: Ninguno
  SSID4: Ninguno
> wl_dual acl agregar 14-49-BC-0D-8F-00 ssid1 ssid2 tet111 aislar
Conjunto Listo !!
> mostrar wl_dual acl
  - - - - - - - - - - Estado del filtro de direcciones Mac ---------
  SSID1: Deshabilitar SSID2: Deshabilitar SSID3: Deshabilitar SSID4: Deshabilitar
  - - - - - - - - - - Lista de direcciones MAC ---------- Índice
          Atributo          Dirección MAC          SSID asociados          Comentario
    1         s            14:49:bc:0d:8f:00        SSID1 SSID2            tet111

  s: Aislar la estación de LAN
```

Comando Telnet: wl_dual apscan

Este comando se usa para escanear el punto de acceso instalado cerca de la ubicación del enrutador Vigor.

Sintaxis

wl_dual apscan*comenzar*

wl_dual apscan*espectáculo*

Sintaxis Descripción

Parámetro	Descripción
comenzar	Significa ejecutar el escaneo AP.
espectáculo	Significa mostrar el contenido de la lista AP.

Ejemplo

```
> wl_dual apscan inicio
> wl_dual apscan muestra que el
  escaneo AP está en curso.
> wl_dual apscan?
% wl_dual apscan [inicio/mostrar] %
inicio: escanear AP
% mostrar: mostrar la lista de puntos de acceso

> wl_dual apscan muestra la
lista de puntos de acceso 5G:
```

BSSID	Canal	SSID

Comando Telnet: configuración wl_dual

Este comando permite a los usuarios configurar los ajustes generales y los ajustes de seguridad para la conexión inalámbrica (5 GHz).

habilitar configuración wl_dual *<valor>* **wl**
dual config enable show wl_dual config
mode *<valor>* **modo de configuración**
wl_dual muestra el canal de configuración
wl_dual *<número>* **canal de configuración**
wl_dual mostrar preámbulo de
configuración wl_dual *<habilitar>* **wl_dual**
config preámbulo mostrar wl_dual config
bw *<valor>*
SSID de configuración wl_dual *<ssid_num habilitar ssid_name>*
wl_dual config ssid ocultar *<ssid_num habilitado>* **Mostrar ssid de**
configuración wl_dual
tasa de configuración wl_dual *<ssid_num habilitar carga descarga>* **demostración del**
ratectl de la configuración de wl_dual
wl_dual config aislar lan *<ssid_num habilitado>* **wl_dual**
config aislar miembro *<ssid_num habilitado>* **wl_dual**
config aislar vpn *<ssid_num habilitado>* **wl_dual config**
aislar mostrar wl_dual config frag *<valor>* **wl_dual**
config frag show wl_dual config rts *<valor>* **wl_dual**
config rts show wl_dual config rate_alg *<valor>* **país de**
configuración wl_dual *<valor>* **wl_dual configuración**
txpower *<valor>* **wl_dual configuración nss** *<valor>*

Sintaxis Descripción

Parámetro	Descripción
habilitar <valor>	Significa habilitar/deshabilitar la función inalámbrica de 5GHz. 1: habilitar 0: deshabilitar
espectáculo	Significa mostrar si la función inalámbrica 5G está habilitada o no.
modo <valor>	Significa seleccionar el modo de conexión para la conexión inalámbrica. Los ajustes disponibles son: "11a", "11n_5g", "11n" y "11an".
espectáculo de modo	Significa mostrar cuál es el modo inalámbrico actual.
canal <número>	Significa el canal de frecuencia de la LAN inalámbrica. Los ajustes disponibles son: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 y 140. numero=0, significa Automático numero=36, significa Canal 36.... Número=52, significa Canal 52.

programa de canal	Significa mostrar cuál es el canal actual.
preámbulo <habilitar>	Significa definir la longitud del campo de sincronización en un paquete 802.11. La mayoría de las redes inalámbricas modernas utilizan un preámbulo corto con un campo de sincronización de 56 bits en lugar de un preámbulo largo con un campo de sincronización de 128 bits. Sin embargo, algunos dispositivos de red inalámbrica 11b originales solo admiten un preámbulo largo. 0: deshabilitar para usar un preámbulo largo. 1: habilitar el uso de un preámbulo largo.
espectáculo de preámbulo	Significa mostrar si el preámbulo está habilitado o no.
bw <valor>	Significa seleccionar el ancho de banda del canal para WLAN para la transmisión y recepción de datos entre el enrutador y las estaciones inalámbricas. valor - 0, 1, 2 0 significa BW_20, 1 significa BW_20_40; 2 significa BW20_40_80.
ssid <ssid_num habilitar nombre_ssid>	Significa establecer el nombre del SSID, ocultar el SSID si es necesario. *ssid_num:* Escriba 1, 2, 3 o 4 para especificar SSID1, SSID2, SSID3 o SSID4. *nombre_ssid*: Asigne un nombre para el SSID especificado.
ssid ocultar <ssid_num habilitar>	Significa ocultar el nombre del SSID si es necesario. *ssid_num*:Escriba 1, 2, 3 o 4 para especificar SSID1, SSID2, SSID3 o SSID4. habilitar: escriba 0 para ocultar el SSID o 1 para mostrar el SSID.
espectáculo ssid	Significa mostrar una tabla de configuración de SSID.
ratectl <ssid_num habilitar carga descarga>	Significa establecer el control de velocidad para el SSID especificado. *ssid_num:*Elija 1, 2, 3 o 4 para especificar SSID1, SSID2, SSID3 o SSID4. *permitir*: Significa habilitar la función de control de tasa para el SSID especificado. 0: deshabilitar y 1: habilitar. *subir*: Significa configurar el control de velocidad para la carga de datos. La unidad es kbps. *descargar*: Significa configurar el control de velocidad para la descarga de datos. La unidad es kbps. (ejemplo:*tasa de configuración dual wlctl 1 1 25 25*)
mostrar tasactl	Significa mostrar la velocidad de transmisión de datos (carga y descarga) para SSID1, SSID2, SSID3 y SSID4.
aislar lan <ssid_num habilitar>	Significa aislar la conexión inalámbrica de la LAN. Puede hacer que los clientes inalámbricos (estaciones) con marcación remota y usuarios de LAN a LAN no accedan entre sí. *ssid_num*:Elija 1, 2, 3 o 4 para especificar SSID1, SSID2, SSID3 o SSID4. *permitir*: Significa habilitar dicha función. 0: deshabilitar y 1: habilitar
aislar miembro <ssid_num enable>	Significa aislar la conexión inalámbrica del Miembro. Puede hacer que los clientes inalámbricos (estaciones) con el mismo SSID no accedan entre sí. *ssid_num*:Elija 1, 2, 3 o 4 para especificar SSID1, SSID2, SSID3 o SSID4. *permitir*: Significa habilitar dicha función. 0: deshabilitar y 1: habilitar.
aislar vpn <ssid_num habilitar>	Significa aislar la conexión inalámbrica de VPN. *ssid_num:*Elija 1, 2, 3 o 4 para especificar SSID1, SSID2, SSID3 o SSID4. *permitir*: Significa habilitar dicha función. 0: deshabilitar y 1: habilitar.
espectáculo aislado	Significa mostrar el estado del aislamiento inalámbrico.
fragmento <valor>	Significa establecer el umbral de fragmentos. valor: Ingrese un número (256 a 2346).
espectáculo de fragmentos	Significa mostrar el valor actual del umbral del fragmento.
rts <valor>	Significa establecer el umbral RTS.

	valor: Ingrese un número (1 a 2347).
espectáculo de rts	Significa mostrar el valor actual del umbral RTS.
rate_alg <valor>	Significa seleccionar la tasa de transmisión inalámbrica. Por lo general, el rendimiento del algoritmo "nuevo" es mejor que el "antiguo". 0 - algoritmo antiguo, 1 - algoritmo nuevo
país <valor>	Significa establecer el código de país. Cada país estará representado con dos dígitos. valor: Introduzca dos letras mayúsculas (p. ej., TW, UK, CN..)
txpower <valor>	Significa establecer la potencia de TX. Valor: Ingrese un número (1 a 6).
nss <valor>	Significa establecer NSS. Valor: Introduzca un número (0 a 4).

Ejemplo

```
> wl_modo de configuración dual
  11a El modo actual es 11a
% <Nota> Reinicie 5G inalámbrico después de configurar el canal
> wl_dual config channel 60 El canal
  actual es 60
% <Nota> Reinicie 5G inalámbrico después de configurar el canal.
> wl_dual config preamble 1 El
preámbulo largo está habilitado
% <Nota> Reinicie 5G inalámbrico después de configurar los parámetros.
> wl_dual config ssid 1 habilitar dray SSID
Habilitar Hide_SSID Nombre
  1 1             0          carro pesado
% <Nota> Reinicie 5G inalámbrico después de configurar los parámetros.
> wl_dual config ssid mostrar SSID
  Habilitar Hide_SSID Nombre 1
          1         0          carro pesado
  2       0         0          DrayTek_5G_Invitado
  3       0         0
  4       0         0
```

Comando Telnet: reinicio wl_dual

Este comando le permite reiniciar la configuración inalámbrica (5GHz).

Ejemplo

```
> reinicio wl_dual

  reinicio inalámbrico 5G ..............
```

Comando Telnet: seguridad wl_dual

Este comando permite a los usuarios configurar los ajustes de seguridad para la conexión inalámbrica (5 GHz).

Sintaxis

wl_doble seguridad <*SSID_NUMBER><modo><clave><índice>* **espectáculo**

de seguridad wl_dual

Sintaxis Descripción

Parámetro	Descripción

seguridad <SSID_NUMBER> <modo> <clave> <índice>	*SSID_NUMBER*: Escriba 1, 2, 3 o 4 para especificar SSID1, SSID2, SSID3 o SSID4. *modo*: Los ajustes disponibles son: deshabilitar: Sin seguridad. wpa1x: Solo WPA/802.1x wpa21x: Solo WPA2/802.1x wpamix1x: Mixto (WPA+WPA2/802.1x únicamente) WEP/ wep1x: 802.1x únicamente PSK WPA: PSK WPA wpa2psk: WPA2/PSK wpamixpsk: Mixto (WPA+WPA2)/PSK wpa3sae: WPA3/SAE wpa3mixsae: Mixto (WPA2+WPA3)/SAE wep: WEP *Índice de Clave*: Además, tienes que añadir claves para*wpapsk, wpa2psk, wpamixpsky Wep*y especifique el número de índice de los perfiles de programación que seguirá la conexión inalámbrica. Las claves WEP deben estar en formato de cadena de texto 5/13 ASCII o 10/26 dígitos hexadecimales; Las claves WPA deben tener una cadena de texto ASCII de 8~63 o un formato de 64 dígitos hexadecimales.
espectáculo	Significa mostrar la selección de modo actual para cada SSID.

Ejemplo

```
> wl_doble seguridad 1 wpa2psk 123456789e
% <Nota> Reinicie 5G inalámbrico después de configurar los parámetros.

> espectáculo de seguridad wl_dual
%% Configuración de seguridad de LAN inalámbrica 5G:
% SSID1
%% Modo: WPA2/PSK
%SSID2
Modo %%: Deshabilitar
%SSID3
Modo %%: Deshabilitar
% SSID4
Modo %%: Deshabilitar
```

Comando Telnet: wl_dualstalist

Este comando se utiliza para mostrar la estación inalámbrica que accede a Internet a través del enrutador Vigor.

Sintaxis

espectáculo estalista wl_dual

wl_dual stalist num

wl_dual stalist vecino wl_dual

stalist validtime*<tiempo>* **wl_dual**

stalist maxmum*<número>*

Sintaxis Descripción

Parámetro	Descripción
tiempo valido <tiempo>	Configure la hora válida de la lista de estaciones vecinas.

	<tiempo> - 0 a 300000.
Maxnum <num>	Establezca el número máximo de lista de estaciones vecinas. <valor> - 10 a 512

Ejemplo

```
> wl_dual vecino estalista
Lista de estaciones vecinas inalámbricas 5G:
Dirección MAC |Nombre del proveedor |RSSI(%)|RSSI(dbm)|SSID|tiempo(ms) |24
F2:C6:DB:2B:25:E0|                  |-84    |ninguna|20
D6: FC: CB: DC: C1: E8 |           |24     |-84    |ninguno|0
80:00:0B:04:CE:5A|Intel             |11     |-88    |ninguno|7230880
00:1D:AA:80:FE:D6|DrayTek           |15     |-87    |ninguno|7210610
A6:99:E2:27:7F:A0|                  |50     |-76    |ninguna|20
0A:32:AB:06:88:2C|                  |40     |-79    |ninguno|0
F8:63:3F:56:06:C6|                  |15     |-87    |ninguno|881950
1E:B9:C9:03:04:52|                  |87     |-62    |ninguna|20
8E:DF:E3:0A:F4:02|                  |3      |-92    |ninguna|20
E2:41:8F:4B:1A:11|                  |50     |-76    |ninguna|20
BA:96:81:7D:11:BD|                  |24     |-84    |ninguna|10
7C:2A:31:10:1B:11|                  |2      |-93    |ninguno|0
```

Comando Telnet: wl_dual wds

Este comando permite a los usuarios configurar WDS para conexión inalámbrica (5 GHz).

Sintaxis

modo wl_dual wds *<valor>*
seguridad wl_dual wds *<valor>*
wl_dual wdsap *<valor>* **wl_dual**
wds hola *<valor>* **estado de**
wl_dual wds
wl_dual wds mostrar
wl_dual wds mac añadir *<dirección de índice>*
wl_dual wds mac borrar/deshabilitar/habilitar *<índice/todos>*
wl_dual wds al ras

Sintaxis Descripción

Parámetro	Descripción
modo <valor>	Significa especificar el modo de conexión para WDS. [valor]: Los ajustes disponibles son: d: Deshabilitar b: Puente r: repetidor
seguridad <valor>	Significa configurar el modo de seguridad con claves cifradas para WDS. *modo*: Los ajustes disponibles son: deshabilitar: Sin seguridad. wep: WEP wpapsk [clave]: PSK WPA wpa2psk [clave]: WPA2/PSK *llave*: Además, tienes que añadir claves para *wpapsk, wpa2psk,* y *Wep,*

	y especifique el número de índice de los perfiles de programación que seguirá la conexión inalámbrica. Las claves WEP deben estar en formato de cadena de texto 5/13 ASCII o 10/26 dígitos hexadecimales; Las claves WPA deben tener una cadena de texto ASCII de 8~63 o un formato de 64 dígitos hexadecimales. p.ej, *wl_dual seguridad wds deshabilitar wl_dual seguridad wds wep 12345 wl_dual seguridad wds wpa2psk 12345678*
ap <valor>	Significa habilitar o deshabilitar la función AP. Valor: 1 – habilitar la función. 0 – deshabilitar la función.
hola <valor>	Significa enviar un mensaje de saludo al extremo remoto (par). Valor: 1 – habilitar la función. 0 – deshabilitar la función.
estado	Significa mostrar el estado del enlace WDS para una conexión de 5 GHz.
espectáculo	Significa mostrar la configuración WDS actual.
mac agregar <dirección de índice>	**agregar***[dirección de índice] – A*Agregue la entrada de MAC del par en la tabla MAC de WDS de repetidor/puente.
mac borrar/deshabilitar/habilitar <índice/todos>	**borrar/deshabilitar/habilitar***[índice/todos]*-Borre, deshabilite, habilite las entradas de MAC especificadas o todas en la tabla MAC de WDS de repetidor/puente. p.ej, *wl_dual wds mac habilitar 1*
enjuagar	Significa restablecer toda la configuración de WDS.

Ejemplo

```
> estado de wl_dual wds
Habilite primero la función de saludo de WDS.

> wl_dual wds hola 1
% <Nota> Reinicie el enrutador después de configurar los parámetros.
> wl modo dual wds b
> wl dual wds seguridad wep
> wl_dual wds muestra la
configuración WDS inalámbrica 5G

Modo : Puente
Seguridad : WEP
Función AP: Habilitar Enviar función
de saludo: Habilitar

Puente :
Índice    Permitir    Dirección MAC
  1         0         00:00:00:00:00:00
  2         0         00:00:00:00:00:00
  3         0         00:00:00:00:00:00
  4         0         00:00:00:00:00:00

Repetidor:
Índice    Permitir    Dirección MAC
  5         0         00:00:00:00:00:00
  6         0         00:00:00:00:00:00
  7         0         00:00:00:00:00:00
  8         0         00:00:00:00:00:00
> wl_dual wds wep 12345
```

% <Nota> Reinicie el enrutador después de configurar los parámetros.

Comando Telnet: wl_dual wps

Este comando permite a los usuarios configurar WPS para conexión inalámbrica (5GHz).

Sintaxis

wl_dual wps habilitar *<valor>* **wl**

dual wps pbc

pin wl_dual wps *<código>*

Mostrar wl_dual wps

Sintaxis Descripción

Parámetro	Descripción
habilitar <valor>	Significa habilitar WPS. 1 – habilitar 0 – deshabilitar
pbc	Significa iniciar WPS presionando el botón WLAN ON/OFF WPS en el enrutador Vigor.
pin <código>	Significa iniciar WPS usando el código PIN del cliente. [código]: código PIN del cliente (número de dígito).
espectáculo	Significa mostrar la configuración actual de WPS.

Ejemplo

```
> wl_dual wps enable 1 WPS
  está habilitado.
> wl_dual wps pin 88563337 WPS se ha
  activado por código PIN.
  El AP esperará la solicitud de WPS de su cliente durante 2 minutos...
```

Comando Telnet: wl_dual set8021x

Este comando le permite configurar el servidor externo o interno utilizado por el enrutador Vigor para la autenticación inalámbrica (5GHz).

Sintaxis

wl_dual set8021x –t <*0/1***>**

wl_dual set8021x –v

Sintaxis Descripción

Parámetro	Descripción
- t	Especifique el tipo (externo o interno) del servidor de autenticación inalámbrica. 0: indica el servidor RADIUS externo. 1- Indicar el servidor local 802.1x.
-v	Ver la configuración de 802.1x.

Ejemplo

```
> wl_dual set8021x -t 1
% <Nota> Reinicie 5G inalámbrico después de configurar los parámetros.
> wl_dual set8021x -v
  El tipo 802.1X es: Local 802.1X
```

```
>
```

Comando Telnet: wl_dual apcli

Este comando permite a los usuarios configurar el modo cliente AP para conexión inalámbrica (5GHz).

Sintaxis

Mostrar aplicación wl_dual

habilitar wl_dual apcli *<valor>*

seguridad wl_dual appli *<modo>*

wl_dual apcli ssid *<nombre_ssid>*

wl_dual appcli bssid *<dirección MAC>*

Sintaxis Descripción

Parámetro	Descripción
espectáculo	Muestra el estado actual del cliente AP inalámbrico.
habilitar <valor>	Significa habilitar el modo de cliente AP inalámbrico de 5 GHz. 1 – habilitar 0 – deshabilitar
seguridad <modo>	Se pueden seleccionar varios modos: Deshabilitar: deshabilita la configuración de seguridad. wpapsk [clave]: se utilizará la clave precompartida WPA. Las claves deben comenzar con 0x para ser identificadas como una clave numérica hexadecimal. Las claves WPA deben estar en formato de 8~63 cadenas ASCII o 64 dígitos hexadecimales. wpa2psk [clave]: se utilizará la clave precompartida WPA2. Las claves deben comenzar con 0x para ser identificadas como una clave numérica hexadecimal. Las claves WPA deben estar en formato de 8~63 cadenas ASCII o 64 dígitos hexadecimales. wpamixpsk [clave]: se utilizará la clave precompartida mixta WPA. Las claves deben comenzar con 0x para ser identificadas como una clave numérica hexadecimal. Las claves WPA deben estar en formato de 8~63 cadenas ASCII o 64 dígitos hexadecimales. wep [clave] [índice]: se utilizará la clave WEP. Debe ingresar la cadena de clave y especificar el número de índice del perfil que se aplicará. Las claves WEP deben estar en formato de cadena 5/13 ASCII o 10/26 dígitos hexadecimales.
ssid <nombre_ssid>	Especifique el SSID para el cliente AP inalámbrico de 5 GHz.
bssid <dirección MAC>	Ingrese la dirección MAC para el cliente AP inalámbrico de 5 GHz.

Ejemplo

```
> wl_dual apcli enable 1 Wireless 5G AP-
Clinet está habilitado Vigor> wl_dual apcli
show
% Wireless 5G AP-Clinet está habilitado % SSID
actual es
%% Modo de seguridad: deshabilitar
% El cliente 5G inalámbrico está desconectado %%
velocidad de datos=---, modo=---, señal=0%
> wl_dual apcli ssid carrie
% <Nota> Reinicie 5g inalámbrico después de configurar los parámetros. El SSID actual
 se lleva
```

Comando Telnet: wl_dual artfns

Este comando permite a los usuarios configurar la función de imparcialidad del tiempo aire para la conexión inalámbrica (5 GHz).

Sintaxis

wl_dual artfns habilitar *<valor>*

wl_dual artfns trg_num *<valor>*

espectáculo wl_dual artfns

estado de wl_dual artfns

Sintaxis Descripción

Parámetro	Descripción
habilitar <valor>	Significa habilitar la función de imparcialidad del tiempo aire inalámbrico. 1 – habilitar 0 – deshabilitar
trg_num <valor>	Establezca un umbral cuando el número de la estación activa alcance este número, se aplicará la función de equidad de tiempo aire. Los valores disponibles serán de 2 a 64.
espectáculo	Mostrar el estado actual (habilitar o deshabilitar) y activar el número de cliente para la función de equidad de tiempo aire.
estado	Muestra si la función de tiempo aire justo está habilitada o deshabilitada.

Ejemplo

```
> wl_dual artfns muestra equidad de
tiempo aire para 5G: deshabilitar trg_num:
2
> estado de wl_dual artfns
¡La equidad de tiempo aire para 5G está deshabilitada!

> wl_dual artfns habilitar 0
> wl_dual artfns trg_num 2
> wl_dual artfns muestra equidad de
tiempo aire para 5G: deshabilitar trg_num:
2
> estado de wl_dual artfns
¡La equidad de tiempo aire para 5G está deshabilitada!
```

Comando Telnet: wl_dual drayrs

Este comando permite al usuario configurar los ajustes de Roaming para clientes inalámbricos.

Sintaxis

wl_dual Drayrs *establecer <modo> <rs_low> <rs_low_security> <delta>*

wl_dual Drayrs *Reanudar*

wl_dual Drayrs *espectáculo*

Sintaxis Descripción

Parámetro	Descripción
establecer <modo> <rs_low> <rs_baja_seguridad> <delta>	Seleccione un modo para itinerancia. 0 - deshabilitar 1 - RSSI estrictamente mínimo 2 - RSSI mínimo

	rs_low: establece un valor de RSSI estrictamente mínimo (62~86). rs_low_security: establezca un valor de RSSI mínimo (62~86). delta: establezca un valor de RSSI AP adyacente (1~20).
Reanudar	Reinicie para activar la función de roaming.
espectáculo	Muestra la configuración actual de la función de roaming.

Ejemplo

```
> wl_dual drayrs show %
Mode : Deshabilitar
%  rs_bajo              : -73
%  rs_low_secure        : -66
%  delta                : 5
> juego de wl_dual drayrs 1 68 66 2
> Mostrar wl_dual drayrs
% Modo : RSSI estrictamente mínimo %
    rs_bajo             : -68
%  rs_low_secure         : -66
%  delta                : 2
```

Comando Telnet: radio

Este comando le permite configurar ajustes detallados para el servidor RADIUS

Sintaxis

habilitar radio*<0/1>* **autorización de radio***<*
número de puerto> **radio set_auth_method***<*
método idx>
cliente de radio*add <idx> -i <dirección> -m <máscara> -p <prefijo> -l <longitud> -s <secreto>* **cliente de radio***del <idx>* **espectáculo de radio**

radio enable_dot1x*<0/1>*
radio set_dot1x_method -e*<método_idx>*
radio set_dot1x_method -d <*método_idx>*

Sintaxis Descripción

Parámetro	Descripción
habilitar <0/1>	Habilite (1) o deshabilite (0) el servidor RADIUS.
puerto de autorización <número de puerto>	Configure el número de puerto para la autenticación. Número de puerto: el rango disponible es de 0 a 65535. El valor predeterminado es "1812".
set_auth_method <método idx>	Especifique qué método se utilizará para la autenticación. Método idx: "0" es "Solo PAP"; “1” es “PAP/CHAP/MS-CHAP/MS-CHAPv2”.
cliente agregar <idx> -i <dirección> - m <máscara> -p <prefijo> -l <longitud> -s <secreto>	Especifique un cliente para ser autenticado por el servidor RADIUS escribiendo la información requerida de la siguiente manera: - i <dirección>: dirección IPv4 del cliente (dominio) - m <máscara>: máscara IPv4 del cliente - p <prefijo>: prefijo IPv6 del cliente - l <longitud>: longitud del prefijo IPv6 del cliente - s <secreto>: secreto compartido ejemplo: radio cliente agregar 1 -i 192.168.1.1 -m 255.255.255.0 -s 123

cliente del <idx>	*del*-Eliminar configuraciones relacionadas para el cliente seleccionado. *Idx* - Especifique el número de índice de los perfiles de clientes.
espectáculo	Muestra el estado del servidor RADIUS.
habilitar_punto1x <0/1>	Habilite (1) o deshabilite (0) la función de autenticación 802.1X del servidor RADIUS. El valor predeterminado está deshabilitado.
set_dot1x_method -e <método_idx>	Establezca un método para la autenticación 802.1X del servidor RADIUS. "-e" significa establecer el método para dot1x_fase1 o dot1x_fase2. Método idx: 1 a 4. 1: EAP_PEAP/MSCHAPv2 2: EAP_TTLS/PAP 3: EAP_TTLS/MSCHAP 4: EAP_TTLS/MSCHAPv2
set_dot1x_método -d <método_idx>	Elimine el método de autenticación 802.1X del servidor RADIUS. "-d" significa eliminar el método para dot1x_fase1 o dot1x_fase2. Método idx: 1 a 4. 1: EAP_PEAP/MSCHAPv2 2: EAP_TTLS/PAP 3: EAP_TTLS/MSCHAP 4: EAP_TTLS/MSCHAPv2

Ejemplo

```
> Radius cliente agregar 1 -i 192.168.1.1 -m 255.255.255.0 -s 123 Establezca
  Radius Server Client OK
>
```

Comando Telnet: radio externo

Este comando le permite configurar ajustes detallados para el servidor RADIUS externo.

Sintaxis

radio externo*<opciones>...*

Sintaxis Descripción

Parámetro	Descripción
<opciones>...	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede escribir varios parámetros en una línea.
-V	Muestra la configuración actual del servidor RADIUS externo.
- v <índice>	Significa mostrar la configuración actual del servidor RADIUS. <índice>: Introduzca el número de índice (1).
- l <índice>	Significa mostrar el registro del servidor RADIUS externo. <índice>: Introduzca el número de índice (1).
- c "<índice><comentario>"	Significa establecer un comentario para el servidor RADIUS externo. <índice>: Introduzca el número de índice (1). <comentario>: Introduzca una breve descripción (menos de 23 caracteres).
- f <índice>	Configure el perfil seleccionado como el perfil RADIUS externo predeterminado. <índice>: Introduzca el número de índice del perfil.
- t <parámetro>	Establezca el valor de tiempo de espera. <parámetro>: Introduzca un valor.
- e "<índice><parámetro>"	Habilite o deshabilite el perfil RADIUS externo. <índice>: Introduzca el número de índice del perfil.

	<param>: 0 o 1. 0 está deshabilitado; 1 es habilitar. ej: -e "2 1" para habilitar el perfil 2
- i "<índice><índice2> <nombre de host/ip>"	Configure el nombre de host o la dirección IP para el perfil de servidor RADIUS seleccionado. <índice>: Introduzca el número de índice del perfil. <index2>: 0 o 1. 0 significa el servidor principal; 1 significa el servidor secundario. ej: -i "1 0 192.168.1.1" o -i "2 1 www.google.com"
- p "<índice><índice2> <número_puerto>"	Configure el puerto de destino para el servidor RADIUS seleccionado. <índice>: Introduzca el número de índice del perfil. <index2>: 0 o 1. 0 significa el servidor principal; 1 significa el servidor secundario. <número_puerto>: 1 ~ 65535. ejemplo: -p "1 1 1812"
- s "<índice><índice2><secreto>"	Establezca el secreto compartido para el servidor RADIUS seleccionado. <índice>: Introduzca el número de índice del perfil. <index2>: 0 o 1. 0 significa el servidor principal; 1 significa el servidor secundario. <secreto>: 1 ~ 65535. ejemplo: -s "3 0 123"
- r "<índice><índice2><reintentar>"	Establezca el número de reintentos para el servidor RADIUS seleccionado. <índice>: Introduzca el número de índice del perfil. <index2>: 0 o 1. 0 significa el servidor principal; 1 significa el servidor secundario. <reintentar>: 1 a 3. ej.: -s "3 0 2"
- un "<índice><parámetro>"	Habilite o deshabilite el puerto de contabilidad para el servidor RADIUS seleccionado. <índice>: Introduzca el número de índice del perfil. <param>: 0 o 1. 0 está deshabilitado; 1 es habilitar.
- b "<índice><índice2> <número_puerto>"	Configure el puerto de contabilidad para el servidor RADIUS seleccionado. <índice>: Introduzca el número de índice del perfil. <index2>: 0 o 1. 0 significa el servidor principal; 1 significa el servidor secundario. <número_puerto>: 1 ~ 65535. ejemplo: -b "1 0 1813"
- d "<índice><índice2> <número_puerto>"	Desconecte el puerto de mensajes del servidor RADIUS seleccionado. <índice>: Introduzca el número de índice del perfil. <index2>: 0 o 1. 0 significa el servidor principal; 1 significa el servidor secundario. <número_puerto>: 1 ~ 65535. ejemplo: -d "1 1 3799"
- u "<índice> <índice2> <intervalo de actualización>"	Establezca el intervalo provisional de contabilidad para el servidor RADIUS seleccionado. <índice>: Introduzca el número de índice del perfil. <index2>: 0 o 1. 0 significa el servidor principal; 1 significa el servidor secundario. <número_puerto>: 10 ~ 1440 (minutos) ej: -u "1 0 10"

Ejemplo

```
> radio externo -i "1 0 192.168.1.1"
  Esta configuración tendrá efecto después de reiniciar. Utilice el
  comando "sys reboot" para reiniciar el enrutador.
> radio externo -V
```

Perfil predeterminado habilitar comentario %
1 v
Tiempo de espera de RADIO: 2 segundos

Comando Telnet: local_8021x

El comando se utiliza para configurar los ajustes generales para el servidor local 802.1X integrado en el enrutador Vigor.

Sintaxis

habilitar local_8021x*<0/1>*
local_8021x set_localdot1x_método -e <*número de método>*
local_8021x set_localdot1x_método -d <*número de método>*
espectáculo local_8021x

Sintaxis Descripción

Parámetro	Descripción
permitir	Habilitar o deshabilitar la configuración. 0: deshabilitar. 1: habilitar.
set_puntolocal1x_método -e < *número de método>*	Agrega el método. - e [número de método]: establece el método. Los números de índice del método son: 1 - EAP_PEAP/MSCHAPv2 2 - EAP_TTLS/PAP 3 - EAP_TTLS/MSCHAP 4 - EAP_TTLS/MSCHAPv2 por ejemplo, local_8021x set_localdot1x_method-e 1
set_puntolocal1x_método -d < *número de método>*	Eliminar el método. - d [número de método]: Elimina el método. Los números de índice del método son: 1 - EAP_PEAP/MSCHAPv2 2 - EAP_TTLS/PAP 3 - EAP_TTLS/MSCHAP 4 - EAP_TTLS/MSCHAPv2 por ejemplo, local_8021x set_localdot1x_method-d 3
espectáculo	Muestra la configuración actual del servidor 802.1x local.

Ejemplo

```
> local_8021x set_localdot1x_method -e 3 Esta configuración tendrá
  efecto después de reiniciar. Utilice el comando "sys reboot" para
  reiniciar el enrutador.
>
```

Comando Telnet: wol

Este comando le permite al administrador configurar la lista blanca de direcciones IP/subredes WAN, de modo que el paquete mágico de estas direcciones IP/subredes sea elegible para pasar a través de NAT y despertar al cliente LAN. También debe configurar la regla NAT para el cliente LAN.

Sintaxis

guau*<Dirección MAC> / <Dirección IP>*

wol de Wan*<encendido/apagado/cualquiera>*

wol deWan_Setting*<idx><dirección IP><máscara>*

Sintaxis Descripción

Parámetro	Descripción
<Dirección MAC>	Significa la dirección MAC del host.
<dirección IP>	Significa la dirección IP de LAN del host. Si desea activar el host de la LAN utilizando la dirección IP, asegúrese de que esa dirección IP se haya vinculado con la dirección MAC (IP BindMAC).
<activar/desactivar/cualquiera>	Significa habilitar o deshabilitar la función de WOL desde WAN. en: habilitar apagado: deshabilitar any: significa que cualquier dirección IP de origen puede pasar a través de NAT y reactivar el cliente LAN. Este comando permitirá al usuario elegir si los paquetes WoL se pueden pasar de Internet a la red LAN desde una interfaz WAN específica.
<idx><dirección IP><máscara>	Significa el número índice (del 1 al 4). Estos comandos permitirán al usuario configurar los clientes LAN que el usuario puede activar desde Internet mediante el uso del paquete WoL. *dirección IP* -Significa la dirección IP WAN. *mascarilla* -Significa la máscara de la dirección IP.

Ejemplo

```
> wol deWan en
> wol deWan_Setting 1 192.168.1.45 255.255.255.0
>
```

Comando Telnet: usuario

El comando se utiliza para crear nuevos perfiles de cuenta de usuario.

Sintaxis

conjunto de usuarios*<-a|-b|-c|-d|-e|-l|-o|-q|-r|-s|-u>*

edición de usuario*<PERFIL_IDX> <-a|-d|-e|-f|-i|-o|-m|-n|-p|-q|-r|-s|-t|-u|-v|-w |-x|-A|-H|-T|-P|-I|-L|-D>*

cuenta de usuario*<NOMBRE_USUARIO><-t|-d|-q|-r|-w>* **usuario**

establecido por defecto

Sintaxis Descripción

Parámetro	Descripción
colocar	Significa configurar la configuración general para la gestión de usuarios.
editar	Significa modificar el perfil de usuario seleccionado.
cuenta	Significa establecer una cuota de tiempo y datos para una cuenta de usuario específica.
establecer predeterminado	Significa restablecer la configuración predeterminada de fábrica.
Conjunto de usuario	
- un <Idx de perfil> <Nombre de usuario><Dirección_IP>	Significa pasar una dirección IP. Profile idx: escriba el número de índice del perfil seleccionado.

	Nombre de usuario: escriba el nombre de usuario que desea que pase. IP_Address: escriba la dirección IP que desea que pase.
- b <nombre de usuario> *- b ip <dirección IP>*	El bloque especifica el usuario o la dirección IP. *nombre de usuario* -escriba el nombre de usuario que desea bloquear. *dirección IP* --escriba la dirección IP que desea bloquear.
- c <nombre de usuario> *- llamar*	Borrar el registro de usuario. *nombre de usuario* -escriba el nombre de usuario que desea obtener el registro correspondiente claro. *todo* -todos los registros serán eliminados.
- d	Habilite la gestión de usuarios en el modo basado en reglas.
- mi	Habilite la gestión de usuarios en el modo basado en usuarios.
- yo todo *- yo usuario* *- labio*	Mostrar usuario en línea. *todo* -todos los usuarios se mostrarán en la pantalla. *nombre de usuario* -escriba el nombre de usuario que desea ver en la pantalla. *ip*-escriba la dirección IP que desea ver en la pantalla.
- o	Significa mostrar información de la cuenta de usuario. p.ej,*-o*
-q	Significa activar la herramienta de alerta para realizar la autenticación.
- r <nombre de usuario/todos>	Eliminar el registro de usuario. *nombre de usuario* -escriba el nombre del perfil de usuario. *todo* -se eliminarán todas las configuraciones del perfil de usuario.
-s<0/1>	Significa configurar el servicio de inicio de sesión. 0: HTTPS 1: HTTP p.ej,*-s1*
- u usuario <nombre de usuario> *- u ip <dirección IP>*	Desbloquear especifica el usuario o la dirección IP. *nombre de usuario* -escriba el nombre de usuario que desea desbloquear. *dirección IP* --escriba la dirección IP que desea desbloquear.

Edición de usuario

PERFIL_IDX	Escriba el número de índice del perfil que desea editar.
- un <0/1>	Habilite (1) o deshabilite (0) el RADIUS interno.
- d	Deshabilitar la función de perfil de usuario.
- mi	Habilite la función de perfil de usuario.
-f<0/1>	Habilite (1) o deshabilite (0) el usuario local 802.1x.
- yo <0-255>	Significa configurar el tiempo de inactividad (de 0 a 255, 0 significa ilimitado). p.ej,*-yo 60*
-o <0-65535>	Significa configurar el cierre de sesión automático (de 0 a 65535, 0 significa ilimitado).
-m <0-2000>	Significa establecer el número de usuario de inicio de sesión máximo (de 0 a 2000). p.ej,*-m 200*
- n <parámetro>	Significa establecer un nombre de usuario para un perfil. Param: ingrese una cadena, por ejemplo, *-n fuerte.*
- p <parámetro>	Significa configurar la contraseña del usuario. Param: Introduzca una cadena, por ejemplo,*-pág. 60fortest.*
- q <parámetro>	Significa establecer la cuota de tiempo (0-65535) del perfil de usuario. Param: Introduzca un valor, por ejemplo,*-q 200.*
- r <parámetro>	Significa establecer una cuota de datos.

	Param: Introduzca un valor, por ejemplo,*-r 1000.*
- s <sch_idx1,sch_idx2,sch_idx3 y sch_idx4>	Significa establecer el índice de programación. Las configuraciones disponibles son" sch_idx1,sch_idx2,sch_idx3 y sch_idx4.
- t<0/1>	Significa habilitar / deshabilitar la limitación de cuota de tiempo para el perfil de usuario 0: Deshabilitar 1: Habilitar
- tu <0/1>	Significa habilitar / deshabilitar la limitación de cuota de datos para el perfil de usuario 0: Deshabilitar 1: Habilitar
-v	Significa ver los perfiles de usuario.
- w <MB/GB>	Significa especificar la unidad de cuota de datos (MB/GB). por ejemplo, -w MB
-x<0-3>	Significa configurar la autenticación del servidor externo 0: Ninguno 1: LDAP 2: Radio 3: TACAS p.ej,*-x2*
- yo <0-3>	Significa establecer el tipo de registro. 0: Ninguno 1: Iniciar sesión 2: Evento 3: Todo
-P <0/1>	Significa habilitar / deshabilitar la ventana de seguimiento del navegador emergente para el perfil de usuario 0: Deshabilitar 1: Habilitar
- T <0/1>	Significa habilitar/deshabilitar la autenticación por telnet. 0: Deshabilitar 1: Habilitar
- H <0/1>	Significa habilitar/deshabilitar la autenticación por página web. 0: Deshabilitar 1: Habilitar
- Un <0/1>	Significa habilitar/deshabilitar la autenticación mediante la herramienta de alerta. 0: Deshabilitar 1: Habilitar
- L <índice>	Significa establecer perfiles de directorio activo/LDAP. Índice: especifique el número de índice (profile_idx1 a profile_idx8) del perfil.
- D	Significa enumerar todos los perfiles de Active Directory/LDAP.
- O <0/1>	Significa restablecer la cuota automáticamente. 0: Deshabilitar 1: Habilitar
- Q <parámetro>	Significa establecer la cuota de tiempo predeterminada. param: Introduzca un número (1 a 65535).
- R <parámetro>	Significa establecer la cuota de datos predeterminada. param: Introduzca un número (1 a 65535).
- M <parámetro>	Significa establecer el tipo de cuota predeterminado.

	0: cuando expiró el programa de permisos de inicio de sesión. 1: a la hora de inicio del horario.
yo <parámetro>	Significa especificar el índice de programación de cuota predeterminado para realizar el trabajo a la hora de inicio.
- S	Significa mostrar el tipo de cuota predeterminada de restablecimiento y el índice de programación.
Cuenta de usuario	
NOMBRE DE USUARIO	Significa escribir un nombre de la cuenta de usuario.
- d<0/1>	Significa habilitar / deshabilitar la limitación de cuota de datos para la cuenta de usuario. 0: Deshabilitar 1: Habilitar
-q	Significa establecer la cuota de tiempo de la cuenta. p.ej,*-q 200*
-r	Significa establecer la cuota de datos de la cuenta. p.ej,*-$ 1000*
- t<0/1>	Significa habilitar / deshabilitar la limitación de cuota de tiempo para la cuenta de usuario. 0: Deshabilitar 1: Habilitar
- w	Significa establecer la unidad de cuota de datos (MB/GB).

Ejemplo

```
> administrador de cuenta de usuario -d 1
  Habilitar la cuota de datos [admin] limitada
```

Comando Telnet: appqos

El comando se usa para configurar QoS para APP.

Sintaxis

vista de appqos

habilitar appqos <*0/1***>**

appqos rastreable <*-v | -e CLASE AP_ÍNDICE | -d ÍNDICE_AP***> appqos**

imposible de rastrear <*-v | -e CLASE AP_ÍNDICE | -d ÍNDICE_AP***>**

Sintaxis Descripción

Parámetro	Descripción
vista	Significa mostrar el estado actual de APP QoS.
permitir<0/1>	Significa habilitar o deshabilitar la función de APP QoS.
rastreable / no rastreable	Las APP se dividen en trazables e ilocalizables en función de sus propiedades.
-v	Significa ver el contenido de todos los AP rastreables. Use "appqos rastreable –v" para mostrar todos los APS rastreables con el número de índice especificado. Use “appqos untraceable –v” para mostrar todos los APS no rastreables con el número de índice especificado.
- mi	Significa habilitar QoS para aplicaciones y asignar clases de QoS.
AP_ÍNDICE	Cada número de índice representa una aplicación. Número de índice: 50, 51, 52, 53, 54, 58, 60, 62, 63, 64, 65, 66, 68 se utilizan para 13 aplicaciones de seguimiento.

	Número de índice: 0~49, 55~59, 61, 67, 69 y 70~123 se utilizan para 125 AP no rastreables.
CLASE	Especifica la clase de QoS de la aplicación, de 1 a 4 1:Clase 1, 2:Clase 2, 3:Clase 3, 4:Otra clase
- d	Significa deshabilitar QoS para la(s) aplicación(es).

Ejemplo

```
> appqos habilitar 1

APP QoS establecido en Habilitar.
> appqos rastreable -e 68 2

TELNET: HABILITADO, QoS Clase 2.
```

Comando Telnet: nand mal uso de /nand

"Uso de NAND" se utiliza para mostrar el uso de NAND Flash; “nand bad” se utiliza para mostrar bloques defectuosos de NAND Flash.

Sintaxis

y malo

uso de nand

Ejemplo

```
> uso de nand
Mostrar uso de flash NAND:
partición       Total       Usado       Disponible  Usar%
cfg             4194304     7920        4186384     0%
bin_web         33554432    11869493    21684939    35%
cfg-bak         4194304     7920        4186384     0%
bin_web-bak 33554432        11869493    21684939    35%
> y malo
Mostrar bloques defectuosos de flash NAND:
bloque  DIRECCIÓN       Dividir
1020    0x07f80000      no usado
1021    0x07fa0000      no usado
1022    0x07fc0000      no usado
1023    0x07fe0000      no usado
```

Comando Telnet: apm habilitar/deshabilitar/mostrar/borrar/descubrir/consultar

Los comandos apm se utilizan para mostrar, eliminar, descubrir o consultar la información de VigorAP registrada en Vigor2927.

Sintaxis

activar apm

deshabilitar apm

espectáculo apm

apm claro

apm descubrir

consulta apm

Sintaxis Descripción

Parámetro	Descripción
permitir	Significa habilitar la función APM.
desactivar	Significa desactivar la función APM.
espectáculo	Muestra información actual del perfil APM.
claro	Se utiliza para eliminar todo el perfil de APM.
descubrir	Se utiliza para buscar VigorAP en LAN.
consulta	Se utiliza para consultar cualquier VigorAP que se haya registrado en APM (Administración central de AP) en Vigor2927. La información relacionada con el AP registrado se enviará de vuelta a Vigor2927 para actualizar la página web de Central AP Management.

Ejemplo

```
> apm claro?
Borrar todos los clientes... hecho
```

Comando Telnet: perfil apm

Este comando permite configurar perfiles inalámbricos para ser utilizados en la Gestión de AP Central.

Sintaxis

clon de perfil apm *<del índice><al índice><nuevo nombre>* **apm**

perfil del *<índice>* **restablecimiento de perfil apm**

resumen del perfil de apm

Mostrar perfil de apm *<índice de perfil>*

aplicar perfil apm *<perfil índice> <cliente índice1 índice2 .. índice5>*

Sintaxis Descripción

Parámetro	Descripción
clon	Se utiliza para copiar la misma configuración de parámetros de un perfil a otro perfil APM.
del	Se utiliza para eliminar un perfil de APM específico. El valor predeterminado (índice n.° 1) no debe eliminarse.
reiniciar	Se utiliza para restablecer la configuración de fábrica para el perfil WLAN.
resumen	Se utiliza para enumerar todos los perfiles de APM con la información necesaria.
espectáculo	Se utiliza para mostrar el perfil APM especificado.
aplicar	Se utiliza para aplicar el perfil APM seleccionado en el VigorAP especificado.
<del índice>	Escriba un número de índice en este campo. Es el perfil de APM original que se clonará en otro perfil de APM.
<para indexar>	Escriba un número de índice en este archivo. Es el perfil objetivo el que clonará la configuración de los parámetros de un perfil APM existente.
<nuevo nombre>	Escriba un nombre para un nuevo perfil de APM.
<índice de perfil>	Introduzca el número de índice del perfil existente.
<cliente índice1 índice2 .. índice5>	Es útil para aplicar el perfil APM seleccionado al VigorAP especificado.

Ejemplo

```
> apm perfil clon 1 2 forcarrie (Listo)


> resumen del perfil de apm
# Nombre              SSID                Seguridad        LCA       TasaCtrl(U/D)
----------------------------------------------------------- 0
Predeterminado       DrayTek-LAN-A       WPA+WPA2/PSK x             - /        -
                     DrayTek-LAN-B       WPA+WPA2/PSK x             - /        -

1 -                  -                   -                -                    -
2 para llevar          DrayTek             Desactivar       X          - /        -

3 -                  -                   -                -                    -
4 -                  -                   -                -                    -
```

Comando Telnet: caché apm

Este comando se utiliza para mostrar o eliminar la información de VigorAP registrado, incluida la dirección MAC, el nombre y la autenticación. Se pueden almacenar y mostrar hasta 30 entradas de información registrada.

Sintaxis

caché apm *<mostrar>*

borrado de caché apm

Sintaxis Descripción

Parámetro	Descripción
espectáculo	Significa mostrar la información relacionada con VigorAP registrado Vigor2927.
claro	Significa eliminar la información relacionada con VigorAP registrado Vigor2927.

Ejemplo

```
> apm caché mostrar
MAC            Nombre                    Autorización
--------------------------------------------------------


>
```

Comando Telnet: apm lbcfg

Este comando permite establecer parámetros relacionados con el control de gestión de AP.

Sintaxis

apm lbcfg conjunto *<valor>*

apm lbcfg mostrar

Sintaxis Descripción

Parámetro	Descripción
colocar	Significa establecer el archivo de configuración de equilibrio de carga para APM.
Espectáculo	Muestra el valor de configuración.

<valor>	Debe escribir 10 números en este campo. Cada número representa un valor de configuración diferente. [1]: el primer número significa la función de equilibrio de carga. Tipo 1: habilitar el equilibrio de carga, 0: deshabilita el equilibrio de carga. [2] – El segundo número significa la función de límite de estación. Tipo 1: habilitar límite de estación, 0: deshabilita el límite de estación. [3] – El tercer número significa la función de límite de tráfico. Tipo 1: habilitar el límite de tráfico, 0: deshabilitar el límite de tráfico. [4] – El cuarto número significa el número límite de estaciones. El rango disponible es 3~64. [5] – El quinto número significa la función de límite de carga. Tipo 1: habilitar el límite de carga, 0: deshabilita el límite de carga. [6] – El sexto número significa la función de límite de descarga. Tipo 1: habilitar el límite de descarga, 0: deshabilitar el límite de descarga. [7] – El séptimo número significa disociación por tiempo de inactividad. Tipo 1: habilitar la disociación, 0: deshabilitar la disociación. [8]: el octavo número significa habilitar o deshabilitar la disociación según la intensidad de la señal. Tipo 1: habilitar la disociación, 0: deshabilitar la disociación. [9] – El noveno número significa determinar la unidad de límite de tráfico (para cargar) 1 – Mbps 0 - kbps [10] – El décimo número significa determinar la unidad de límite de tráfico (para descarga) 1 – Mbps 0 - kbps [11] - El undécimo número significa establecer el umbral de RSSI. El rango disponible es -200 ~ -50 dbm.

Ejemplo

```
> apm lbcfg show apm
LoadBalance Config: 1. Habilitar
LoadBalance: 0
2. Habilitar límite de estación: 0
3. Habilitar límite de tráfico: 0
4. número límite: 64
5. Límite de carga: 0
6. Límite de descarga: 0
7. Habilitar la disociación por tiempo de inactividad: 0
8. Habilitar la disociación por intensidad de la señal: 0
9. Unidad de límite de tráfico (carga): 0
10. Unidad de límite de tráfico (descarga): 0
11. Umbral RSSI: 0 indicador:
0
```

```
> apm lbcfg conjunto 1 1 0 15 0 0 0 0 1 1 -100
> apm lbcfg show apm
LoadBalance Config: 1. Habilitar
LoadBalance: 1
2. Habilitar límite de estación: 1
3. Habilitar límite de tráfico: 0
4. número límite: 15
5. Límite de carga: 0
6. Límite de descarga: 0
7. Habilitar la disociación por tiempo de inactividad: 0
8. Habilitar la disociación por intensidad de la señal: 0
9. Unidad de límite de tráfico (carga): 1
10. Unidad de límite de tráfico (descarga): 1
11. Umbral RSSI: -100 indicador:
49
>
```

Comando Telnet: apm apsyslog

Este comando se utiliza para mostrar los datos de registro del sistema AP que provienen de VigorAP.

Sintaxis

apm apsislog *<AP_Índice>*

Sintaxis Descripción

Parámetro	Descripción
AP_Índice	Especifique el número de índice (1 a 20) que representa VigorAP.

Ejemplo

```
> apm apsyslog 1 8d
02:46:09        syslog: [APM] Enviar datos de detección de puntos de acceso no autorizados.
8d 02:53:04     syslog: [APM] Ejecutar detección/descubrimiento de AP. syslog: [APM] Enviar
8d 02:56:09     datos de detección de puntos de acceso no autorizados. kernel: 60:fa:cd:55:f5:ea
8d 03:00:42     se había desvinculado. syslog: [APM] Ejecutar detección/descubrimiento de AP.
8d 03:03:12     syslog: [APM] Enviar datos de detección de puntos de acceso no autorizados.
8d 03:06:09     syslog: [APM] Ejecutar detección/descubrimiento de AP. syslog: [APM] Enviar
8d 03:13:21     datos de detección de puntos de acceso no autorizados. kernel: 60:fa:cd:55:f5:ea
8d 03:16:10     se había asociado con éxito kernel: 60:fa:cd:55:f5:ea se había desasociado.
8d 03:16:41
8d 03:16:55
```

Comando Telnet: apm syslog

Este comando se utiliza para mostrar datos de syslog relacionados desde la administración central de puntos de acceso.

Sintaxis

registro del sistema apm

Ejemplo

```
> registro del sistema apm
"2015-11-04 12:24:21", "[APM] [VigorAP900_01daa902080] Obtener datos de detección de AP no autorizados de AP"
2015-11-04 12:24:56", "[APM] [VigorAP900_01daa902080] Obtener datos de detección de AP no autorizados de AP Success"
2015-11-04 12:34:21", "[APM] [VigorAP900_01daa902080] Obtener detección de puntos de acceso no autorizados
```

```
Datos de AP"
2015-11-04 12:34:57", "[APM] [VigorAP900_01daa902080] Obtener datos de detección de AP no
autorizados de AP Success"
```

Comando Telnet: apm stanum

Este comando se usa para mostrar el número total de clientes inalámbricos, sin importar qué modo de conexión inalámbrica (2.4G WLAN o 5G WLAN) usen los clientes inalámbricos para acceder a Internet a través de VigorAP.

Sintaxis

estaño apm*<AP_Índice>*

Sintaxis Descripción

Parámetro	Descripción
AP_Índice	Especifique el número de índice que representa a VigorAP.

Ejemplo

```
> estaño apm

% Muestra los datos del número de estación AP de
APM. % apm stanum AP_Index.
%       ej: apm stanum 1
%               Idx Cercano (2.4/5G) Conexión (2.4/5G) 1
%                       2     5               0     0
%                 2     2     5               1     0
%                 3     2     5               1     0
```

Comando Telnet: ha establecido

Este comando se puede utilizar para configurar los ajustes de HA para los enrutadores Vigor.

Sintaxis

ha puesto*[-<comando> <parámetro>| ...]*

Sintaxis Descripción

Parámetro	Descripción
[<comando> <parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede introducir varios parámetros en una línea.
- mi <1/0>	1: Habilitar la función de Alta Disponibilidad (HA). 0: Deshabilitar la función de Alta Disponibilidad (HA).
- yo <1/0>	1: Habilite la función de grabar el registro de operación de HA en Syslog. 0: deshabilite la función de grabar el registro de operación de HA en Syslog.
-M<1/0>	Especifique el método de redundancia para HA. 1: Activo-Espera 0: espera caliente
-v<1-255>	Especifique el ID de grupo (VHID) 1- 255: Rango de configuración.
-R	Establezca la configuración de alta disponibilidad en los valores predeterminados de fábrica.
- pag <1-30>	Especifique el ID de prioridad. 1-30: Rango de ajuste.

- k <clave>	Especifique la clave de autenticación. Clave: Máx. 31 caracteres.
- tu <1/0>	Habilite o deshabilite la función de Actualizar DDNS. 1: Habilitar. Cuando un enrutador cambia el estado HA a principal, actualizará DDNS automáticamente. 0: Deshabilitar.
- m <interfaz>	Especifique la interfaz de gestión. Interfaz: LAN1 ~ LAN6, DMZ.
- s	Significa obtener el estado más reciente de otro enrutador (excepto el enrutador local).
- y	Significa sincronizar la configuración local con otro enrutador. La lata primaria ejecuta este comando. Secundario no puede ejecutar este comando.
-c<1/0>	Habilite o deshabilite la función de Config Sync. 1: Habilitar. 0: Deshabilitar.
- i -<E|S> <valor>	Especifique la configuración de herencia de configuración. - E <1/0> - Habilitar/deshabilitar herencia de configuración - S <min> - Config Inherit Resync Time (1-60 min) ej: ha set -i -S 15
- I - <M/H/D> <intervalo>	Establezca el Intervalo de sincronización de configuración para HA. El intervalo mínimo es de 15 minutos. - M: Minuto. El rango de configuración es 0/15/30/45. (p. ej., ha set -I -M 30) - H: Hora. El rango de configuración es de 0 a 23. (p. ej., ha set -I -H 12) - D: Día. El rango de configuración es de 0 a 30. (p. ej., ha set -I -D 15)
- h -<4/6><Subred> <IP virtual>	Habilite y configure la IP virtual para la subred. 4: IPv4; 6: IPv6. Subred: LAN1 a LAN6, DMZ. IP virtual.El formato de tipo será “xxx.xxx.xxx.xxx”. (por ejemplo, 192.168.1.0) Por ejemplo, para habilitar una IP virtual a la sunet, simplemente escriba: *ha establecido –h LAN1 192.168.1.5*
- d -<4/6><Subred>	Deshabilite una IP virtual para la subred. 4: IPv4; 6: IPv6. Subred: LAN1 a LAN8, DMZ. Por ejemplo, para deshabilitar una IP virtual en la subred, simplemente escriba: *ha establecido –h LAN1*
- o <1/0>	Ejecute el protocolo DARP en IPv4 o IPv6. 0: IPv4 1: IPv6

Ejemplo

```
> ha establecido -h -4 LAN1 192.168.1.1
% Habilitar IP virtual IPv4 en LAN1
¡% La IP virtual no puede ser la misma que la IP del enrutador (192.168.1.1)!
>
```

Comando Telnet: ha show

Este comando se puede utilizar para mostrar el*información de configuración*sobre sincronización de configuración y configuración general.

Sintaxis

ja mostrar -c

ja mostrar -g

Sintaxis Descripción

Parámetro	Descripción
- C	Muestra la configuración de la sincronización de configuración.
- g	Muestra los ajustes de la configuración general.

Ejemplo

```
> ha espectáculo -g
%   Alta disponibilidad              : Desactivar
%   Método de redundancia            : Activo-Espera
%   Identificación del grupo         : 1
%   ID de prioridad                  : 10
%   Actualizar DNS                   : Desactivar
%   Protocolo                        : IPv4
%   Interfaz de administración: clave de
%   autenticación LAN1               : Draytek
%   registro del sistema             : APAGADO
%
%   [ Índice | Habilitar | IP virtual]
%      LAN1      -          192.168.1.2
%      LAN2      -          192.168.2.2
%      LAN3      -          192.168.3.2
%      LAN4      -          192.168.4.2
%      LAN5      -          192.168.5.2
%      LAN6      -          192.168.6.2
%      LAN7      -          192.168.7.2
%      LAN8      -          192.168.8.2
%      DMZ       -          192.168.254.2
%
%   [ Índice | Habilitar | IPv6 virtual]
%      LAN1      En         FE80::200:5EFF:FE00:101
%      LAN2      En         FE80::200:5EFF:FE00:101
%      LAN3      En         FE80::200:5EFF:FE00:101
%      LAN4      En         FE80::200:5EFF:FE00:101
%      LAN5      En         FE80::200:5EFF:FE00:101
%      LAN6      En         FE80::200:5EFF:FE00:101
%      LAN7      En         FE80::200:5EFF:FE00:101
%      LAN8      En         FE80::200:5EFF:FE00:101
%      DMZ       En         FE80::200:5EFF:FE00:101
>
```

Comando Telnet: ha estado

Este comando se utiliza para mostrar*Información de estado de alta disponibilidad.*

Sintaxis

ha estado –a<*Nivel de detalle*>

ha estado –m*<Nivel de detalle>*

Sintaxis Descripción

Parámetro	Descripción
- a	Muestra el estado de todos los enrutadores en el grupo HA.
- m	Muestra el estado del enrutador local solamente.
<Nivel de detalle>	0: Estado importante. 1: Estado importante, más alguna información. 2: Mostrar configuración

Ejemplo

```
> ha estado -m 2 %
      [Enrutador local] DrayTek
%     IP                          : 192.168.1.230 (FE80::C3F7:MAL:C1EF:CC4E)
%     Estado                      : !
%     Alta disponibilidad         : ! Desactivar
%     Método de redundancia       : Activo-Espera
%     Identificación del grupo    : 1
%     ID de prioridad             : 10
%     Actualizar DNS              : Desactivar
%     Protocolo                   : IPv4
%     Interfaz de administración: LAN1 Clave de
%     autenticación: draytek IP virtual: (Máx. 9 IP
%     virtuales)
%        ! APAGADO
%     IPv6 virtual: (Máx. 9 IPv6 virtuales)
%        EN          LAN1   FE80::200:5EFF:FE00:101
%        EN          LAN2   FE80::200:5EFF:FE00:101
%        EN          LAN3   FE80::200:5EFF:FE00:101
%        EN          LAN4   FE80::200:5EFF:FE00:101
%        EN          LAN5   FE80::200:5EFF:FE00:101
%        EN          LAN6   FE80::200:5EFF:FE00:101
%        EN          LAN7   FE80::200:5EFF:FE00:101
%        EN          LAN8   FE80::200:5EFF:FE00:101
%        EN          DMZ    FE80::200:5EFF:FE00:101
%     Sincronización de configuración          : Desactivar
%     Intervalo de sincronización de configuración   : 0 Día 0 Hora 15 Minuto
%     Tiempo en caché             : 0 (s)
%
>
```

Comando Telnet: espectáculo swm

Este comando se utiliza para mostrar la configuración general de VigorSwitch que se conecta al enrutador Vigor en LAN.

Sintaxis

espectáculo de natación *<puerto_LAN>*

Sintaxis Descripción

Parámetro	Descripción
Puerto LAN	Especifique el número de puerto LAN (1 a 6).

Ejemplo

```
DrayTek> espectáculo de natación

* * Si desea mostrar el registro de depuración de SWM: "swm show debug log"
* * Habilitar/deshabilitar el registro de depuración de la consola SWM: "swm show console log en/dis"
* * Habilitar/deshabilitar el registro de depuración de syslog de SWM: "swm show syslog log en/dis"

* * Si conectó un VigorSwitch pero no aparece aquí.
* * Verifique que LLDP esté habilitado y que la ID de VLAN coincida con VigorSwitch.
```

```
*****************************************************************************
*********************************************
Puerto LAN    Nivel        ARRIBA - Modelo de enlace    ARRIBA-MAC        UP - Nombre del modelo de puerto        MAMÁ
C              Dirección IP          Abajo - Puerto
-------------------------------------------    ------------------------------------
-------------------------------------------------- 2
            1            enrutador                          6          G2100                1
449BC43E579 192.168.1.13
-------------------------------------------------------------------------------
-------------------------------------------------

* * * Mensaje de advertencia: Se detectó el cambio del interruptor externo
*****************************************************************************

La VLAN interna está [Deshabilitada]
Error de configuración de análisis de LAN (2)
-------------------------------------------------------------------------------

No hay configuraciones de VLAN de VigorSwitch.
*****************************************************************************

*****************************************************************************
*********************************************
Puerto LAN    Nivel        ARRIBA - Modelo de enlace    ARRIBA-MAC        UP - Nombre del modelo de puerto        MAMÁ
C              Dirección IP          Abajo - Puerto
-------------------------------------------    ------------------------------------
-------------------------------------------------- 4
            1            enrutador                          2          G2121                1
449BC4133F4 192.168.1.11
-------------------------------------------------------------------------------
-------------------------------------------------

* * * Mensaje de advertencia: Se detectó el cambio del interruptor externo
*****************************************************************************

La VLAN interna está [Deshabilitada]
Error de configuración de análisis de LAN (4)
-------------------------------------------------------------------------------

No hay configuraciones de VLAN de VigorSwitch.
*****************************************************************************
```

(Total 0 Cambio)

Comando Telnet: swm get

Este comando se utiliza para**conseguir**información de configuración de VigorSwitch que se conecta al enrutador Vigor en LAN. Antes de usar dicho comando, asegúrese de que VigorSwitch se haya administrado en el enrutador Vigor (consulte Comando Telnet: perfil swm para agregar un dispositivo VigorSwitch al enrutador Vigor).

Sintaxis

nadar conseguir*<MAC>*

Sintaxis Descripción

Parámetro	Descripción
MAC	Ingrese la dirección MAC (p. ej., 001DAA0CCD08) del VigorSwitch.

Ejemplo

```
> nadar obtener 001DAA0CCD08
Comience a obtener cfg desde el interruptor externo 001daa0ccd08

Por favor espere unos segundos...

Resultado: [OK].

>
```

Comando Telnet: publicación swm

Este comando se utiliza para transferir la configuración del conmutador a VigorSwitch, que se conecta al enrutador Vigor en la LAN.

Sintaxis

publicación de natación*<MAC>*

Sintaxis Descripción

Parámetro	Descripción
MAC	Ingrese la dirección MAC (p. ej., 001DAA0CCD08) del VigorSwitch.

Ejemplo

```
> swm puesto 001DAA0CCD08
Iniciar post cfg a 001daa0ccd08 interruptor externo con la configuración actual. Por favor
espere unos segundos...
Resultado: [OK].
>
```

Comando Telnet: activar/desactivar swm

Este comando se utiliza para habilitar/deshabilitar el dispositivo externo.

Ejemplo

```
> habilitar swm
```

Comando Telnet: grupo swm

Este comando se utiliza para agregar, editar o mostrar el grupo de administración de conmutadores.

Sintaxis

grupo de natación*configurar <IDX> <NOMBRE> <1> <CONTRASEÑA>* **grupo de natación***establecer <IDX> <NOMBRE> <0>* **grupo de natación***espectáculo*

grupo de natación*añadir <IDX> <MAC>* **grupo de natación***eliminar <IDX> <MAC>*

Sintaxis Descripción

Parámetro	Descripción
configurar <IDX> <NOMBRE> <1> <CONTRASEÑA>	Significa establecer el nombre del grupo y la contraseña del grupo. <IDX>: Introduzca el número de índice (1 a 10) del grupo. <NOMBRE>: Introduzca el nombre del grupo. <1>: Significa el indicador de contraseña. <CONTRASEÑA>: Introduzca una cadena como contraseña.
espectáculo	Significa mostrar el estado del grupo de interruptores.
añadir <IDX> <MAC>	Significa agregar un conmutador al grupo como conmutador miembro. <IDX>: Introduzca el número de índice (1 a 10) del grupo. <MAC>: Introduzca la dirección MAC de VigorSwitch.
eliminar <IDX> <MAC>	Significa eliminar un conmutador del grupo. <IDX>: Introduzca el número de índice (1 a 10) del grupo. <MAC>: Introduzca la dirección MAC de VigorSwitch.

Ejemplo

```
> conjunto de grupo swm 10 guisantes 1 jpsword
> swm group show Index Group Name
asswd Flag                                  Cambio de miembro
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - -     - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - 1
         Por defecto             0
2                               0
3                               0
4                               0
5                               0
6                               0
7                               0
8                               0
9                               0
10       guisantes               1

Nombre            Dirección IP        MAC
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - -             192.168.1.13        1449bc43e579
- - -             192.168.1.11        1449bc4133f4 >
```

Comando Telnet: perfil swm

Este comando se usa para agregar, editar o mostrar el perfil de administración del conmutador.

Sintaxis

perfil de natación*agregar/eliminar <MAC>* **perfil de natación***espectáculo*

perfil de natación*habilitar_todo/deshabilitar_todo <MAC>*

Sintaxis Descripción

Parámetro	Descripción
agregar/eliminar <MAC>	Significa agregar o eliminar un cambio de miembro del perfil. <MAC>: Introduzca la dirección MAC del conmutador.
espectáculo	Significa mostrar el perfil del interruptor.

habilitar_todo/deshabilitar_todo <MÁC>	Significa habilitar o deshabilitar todos los puertos LAN del conmutador especificado administrado por el enrutador Vigor. <MAC>: ingrese la dirección MAC del conmutador miembro.

Ejemplo

```
> Mostrar perfil de swm
Nombre              Dirección IP          MAC               Grupo modelo
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Dirección IP          MAC               Modelo
- - - - - - - - - - - - - - - - - - - - - - - - -      - - - - - -
192.168.1.13          1449bc43e579 G2100
192.168.1.11          1449bc4133f4 G2121

>
```

Comando Telnet: detalle swm

Este comando se utiliza para configurar los ajustes generales (p. ej., el nombre del interruptor, la contraseña) y los ajustes del puerto para VigorSwitch.

Sintaxis

detalle de notación*comentario <MAC> <COMENTARIO>* **detalle**

de notación*nombre <MAC> <NOMBRE>* **detalle de notación**

contraseña <MAC> <CONTRASEÑA> **detalle de notación**

configuración <MAC> <configuración> **detalle de notación**

espectáculo

detalle de notación*Mostrar puerto <MAC>*

detalle de notación*puerto <MAC> <PUERTO> <BANDERA> <HORARIO1> <HORARIO2> <DESCRIPCIÓN>* **detalle**

de notación*velocidad <MAC> <PORT> <i/e> <e/d>* **detalle de notación***velocidad <MAC> <PORT> <i/e> <límite de velocidad>*

Sintaxis Descripción

Parámetro	Descripción
comentario <MAC> <COMENTARIO>	Significa establecer un comentario para VigorSwitch. <MAC>: Introduzca la dirección MAC del VigorSwitch a modificar. <COMENTARIO>: Agregue una explicación adicional para el cambio.
nombre <MAC> <NOMBRE>	Significa establecer un nombre para VigorSwitch. <MAC>: Introduzca la dirección MAC del VigorSwitch a modificar. <NOMBRE>: Introduzca el nombre de VigorSwitch.
contraseña <MAC> <CONTRASEÑA>	Significa establecer una contraseña de inicio de sesión para VigorSwitch. <MAC>: Introduzca la dirección MAC del VigorSwitch a modificar. <NOMBRE>: Introduzca la contraseña de inicio de sesión de VigorSwitch.
configuración <MAC> <configuración>	Significa aplicar la configuración de VigorSwitch B a otro VigorSwitch A. <MAC>: Introduzca la dirección MAC del VigorSwitch A a modificar. <config>: ingrese el número de índice del perfil establecido en VigorSwitch B.
espectáculo	Significa mostrar comentarios, MAC y estado de conexión del conmutador.
Mostrar puerto <MAC>	Significa mostrar una lista de puertos LAN del VigorSwitch. <MAC>: Introduzca la dirección MAC del VigorSwitch a modificar.

puerto <MAC> <PUERTO> <BANDERA> <HORARIO1> <HORARIO2> <DESCRIPCIÓN>	Significa establecer una descripción y un perfil de programación para cada puerto de VigorSwitch. <MAC>: Introduzca la dirección MAC del VigorSwitch a modificar. <PORT>: Ingrese el número de índice (por ejemplo, 1 a 28) del puerto LAN VigorSwitch. El número de puertos LAN variará según el Switch a modificar. <HORARIO1> <HORARIO2>:Determine y escriba dos números de índice de los perfiles de horario que desea. <DESCRIPCIÓN>: Ingrese una descripción para cada puerto de VigorSwitch.
velocidad <MAC> <PORT> <i/e> <e/d>	Significa habilitar/deshabilitar el límite de velocidad para cada puerto de VigorSwitch. <MAC>: Introduzca la dirección MAC del VigorSwitch a modificar. <PORT>: Ingrese el número de índice (por ejemplo, 1 a 28) del puerto LAN VigorSwitch. El número de puertos LAN variará según el Switch a modificar. <i/e>: "i" significa tasa de ingreso; "e" significa tasa de salida. <e/d>" "e" significa habilitar; "d" significa deshabilitar la configuración.
velocidad <MAC> <PORT> <i/e> <límite de velocidad>	Significa modificar el límite de velocidad para cada puerto de VigorSwitch. <MAC>: Introduzca la dirección MAC del VigorSwitch a modificar. <PORT>: Ingrese el número de índice (por ejemplo, 1 a 28) del puerto LAN VigorSwitch. El número de puertos LAN variará según el Switch a modificar. <i/e>: "i" significa tasa de ingreso; "e" significa tasa de salida. <límite de tasa>: Introduzca un valor.

Ejemplo

```
> tasa de detalle swm 1449bc43e579 6 i 3000
> tasa de detalle swm 1449bc43e579 6 e 5000
> detalles de swm mostrar
nombre Idx                MAC          Comentario          Configuración          Estado
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - 1  - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
      G2100              1449bc43e579                    0 Ninguno              Conectar
>
```

Comando Telnet: mantenimiento swm

Este comando se usa para reiniciar o restablecer el interruptor a la configuración predeterminada de fábrica.

Sintaxis

nadar mantener *reiniciar <MAC>* **nadar**

mantener *restablecer <MAC>* **nadar**

mantener *espectáculo*

Sintaxis Descripción

Parámetro	Descripción
reiniciar <MAC>	Significa reiniciar VigorSwitch con la configuración actual. <MAC>: Introduzca la dirección MAC del VigorSwitch a modificar.
restablecer <MAC>	Significa restablecer VigorSwitch con la configuración predeterminada de fábrica. <MAC>: Introduzca la dirección MAC del VigorSwitch a modificar.
espectáculo	Significa mostrar comentarios, MAC y estado de conexión del conmutador.

Ejemplo

```
> swm mantener mostrar
nombre              Dirección IP          MAC              Modelo
```

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
G2100                  192.168.1.13 1449bc43e579 G2100
>
```

Comando Telnet: búsqueda swm

Este comando se utiliza para buscar Vigor Switch por MAC/dirección IP/descripción específica e información de visualización.

Sintaxis

búsqueda de natación*mac <MAC>*

búsqueda de natación*IP <IP>*

búsqueda de natación*descripción <Entrada>*

Sintaxis Descripción

Parámetro	Descripción
mac <MAC>	<MAC>: Introduzca la dirección MAC del VigorSwitch a buscar.
IP <IP>	<IP>: Introduzca la dirección IP del VigorSwitch a buscar.
descripción <entrada>	<entrada>: Ingrese el nombre del modelo del VigorSwitch que se buscará.

Ejemplo

```
> swm buscar mac 1449bc43e579
Escriba la dirección IP        MAC                 Descripción / Nombre            Puerto LAN
 Puerto de enlace ascendente        Nivel     Puerto
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - -
 - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Cambiar 192.168.1.13          14:49:BC:43:E5:79 G2100 2                              P2
    Enrutador Vigor 0

>
```

Comando Telnet: swm db

Este comando se usa para habilitar/deshabilitar la base de datos para registrar información de administración del switch.

Sintaxis

nadar db*ctl es/des* **nadar db**

mostrar control remoto

nadar db*alerta notificar <N/S>*

nadar db*acción de alerta <S/B>*

nadar db*SMS de alerta <IDX>*

nadar db*correo de alerta <IDX>*

Sintaxis Descripción

Parámetro	Descripción
ctl es/des	Significa habilitar o deshabilitar la función de mostrar el estado de control de la base de datos. es: Habilitar la función. dis: deshabilitar la función.
mostrar control remoto	Significa mostrar el estado de control de la base de datos.
alerta notificar <N/S>	Significa establecer la condición de notificación de alerta (N o S) cuando se excede el almacenamiento. N: No enviar notificación.

	S: Enviar notificación.
acción de alerta <S/B>	Significa establecer la condición de acción de alerta (S o B) cuando se excede el almacenamiento. S: Deja de grabar la información del usuario. B: Haga una copia de seguridad y limpie toda la información del usuario, y comience un nuevo registro.
SMS de alerta <IDX>	Significa establecer un objeto SMS que obtendrá la información del enrutador Vigor si hay algún problema con VigorSwitch. <IDX>: Introduzca el número de índice del objeto de correo.
correo de alerta <IDX>	Significa establecer un objeto de correo que obtendrá la información del enrutador Vigor si hay algún problema con VigorSwitch. <IDX>: Introduzca el número de índice del objeto de correo.

Ejemplo

```
> swm db ctl es
Habilite la base de datos para registrar la información de SWM.
```

Comando Telnet: alerta swm

Este comando se utiliza para definir el nombre de la alerta, el nivel de alerta (en color) y determinar registrar los datos en la base de datos o enviar un mensaje de notificación al usuario según el nivel.

Sintaxis

alerta de natación*habilitar deshabilitar*

alerta de natación*espectáculo*

alerta de natación*es/dis <Idx>* **alerta de natación**

establecer <Idx> registro <e/d> **alerta de natación**

establecer <Idx> nombre <nombre> **alerta de natación**

establecer <Idx> color <O/R/N> **alerta de natación**

establecer <Idx> notif <e/d>

alerta de natación*establecer <Idx> obj <objeto idx> <valor del objeto>*

alerta de natación*mostrar*

alerta de natación*en/dis <sw/puerto> <mac>*

alerta de natación*sw mostrar <mac>*

alerta de natación*establecer sw <mac> <idx de incidente> <idx de nivel>* **alerta**

de natación*Mostrar puerto <mac>*

alerta de natación*establecer puerto <mac> <número de puerto><idx de incidente> <idx de nivel>*

Sintaxis Descripción

Parámetro	Descripción
habilitar deshabilitar	Significa habilitar/deshabilitar el mecanismo de Alerta. habilitar: habilitar el mecanismo. deshabilitar: deshabilitar el mecanismo.
espectáculo	Significa mostrar una lista de todas las configuraciones de alerta.
es/dis <Idx>	Significa habilitar / deshabilitar la configuración de Acción de Alerta. es: Habilitar la configuración. dis: deshabilita la configuración. <Idx>: Ingrese el número de índice (1 a 8) del elemento de acción de alerta.
establecer <Idx> registro <e/d>	Significa habilitar/deshabilitar la función de crear un registro de alerta.

	e: habilite la configuración. d: Deshabilitar la configuración. <Idx>: Ingrese el número de índice (1 a 8) del elemento de acción de alerta. Tenga en cuenta que No Log para el índice 1; y el registro para el índice 2 está habilitado de forma predeterminada.
establecer <Idx> nombre <nombre>	Significa establecer el nombre del nivel de cada alerta. <Idx>: Ingrese el número de índice (1 a 8) del elemento de acción de alerta. <nombre>: ingrese una breve descripción de la alerta.
establecer <Idx> color <O/R/N>	Significa definir el color para cada nivel de alerta. El color del índice 1 es Sin color y no se puede cambiar. <Idx>: Ingrese el número de índice (2 a 8) del elemento de acción de alerta. <O/R/N>: "O" significa naranja; "R" significa rojo; "N" significa sin color.
establecer <Idx> notif <e/d>	Significa habilitar o deshabilitar la función de envío de notificaciones a un número de teléfono específico a través de SMS. <Idx>: Ingrese el número de índice (3 a 8) del elemento de acción de alerta. e: habilite la configuración. d: Deshabilitar la configuración.
establecer <idx> obj <idx de objeto> <valor de objeto>	Significa especificar objetos de servicio de SMS/correo electrónico para el elemento de alerta. Cada alerta se puede configurar con hasta cuatro objetos. <Idx>: Ingrese el número de índice (3 a 8) del elemento de acción de alerta. <idx de objeto>: ingrese el número de cola (1 a 4) para especificar un perfil de objeto. <valor del objeto>:Ingrese el número de índice (1 a 10) del perfil de objeto de servicio de SMS/Correo electrónico.
mostrar	Significa mostrar todos los conmutadores con estado de alerta de puerto.
en/dis <sw/puerto> <mac>	Significa habilitar o deshabilitar la acción Switch Alert/Port Alert. es: Habilitar la función. dis: deshabilitar la función. <sw/port>: "sw" significa Switch Alert; "puerto" significa alerta de puerto. <mac>: Ingrese la dirección MAC del VigorSwitch.
sw mostrar <mac>	Significa mostrar el tipo de incidente y alerta del VigorSwitch. <mac>: Ingrese la dirección MAC del VigorSwitch.
establecer sw <mac> <idx de incidente> <idx de nivel>	Significa configurar el tipo de incidente y alerta del VigorSwitch. <mac>: Ingrese la dirección MAC del VigorSwitch. <idx de incidente>: Rango 1 - 4. <idx de nivel>: 1 - 8.
Mostrar puerto <mac>	Alerta de incidente del puerto de visualización. <mac>: Ingrese la dirección MAC del VigorSwitch.
establecer puerto <mac> <número de puerto> <idx de incidente> <idx de nivel>	Establecer alerta de incidente de puerto. <mac>: Ingrese la dirección MAC (p. ej., 001DAA0EB0DB) del VigorSwitch. <número de puerto>: rango 1 - 28. <idx de incidente>: rango 1 - 4. <idx de nivel>: 1 - 8.

Ejemplo

```
>  habilitación de alerta de swm
> conjunto de alertas swm 2 colores N
> alerta de natación  espectáculo
Idx En/Dis    Nivel                  Color      Crear      Registro      Enviar  Notificación (1-4)
--------    ------------------------------------------------------Sin   --------------
1     es    alerta                 No  Color  Desactivar  Desactivar  0  ,  0  ,  0  ,  0
2     es    Alerta menor           No  Color  Permitir    Desactivar   0  ,  0  ,  0  ,  0
3     es    Moderado   Alerta      Naranja    Permitir    Desactivar   0  ,  0  ,  0  ,  0

4     es    Alerta mayor           Rojo       Permitir    Desactivar   0 , 0 , 0 , 0
```

```
5      Dis                              No  Color   Desactivar   Desactivar   0 , 0 , 0 , 0
6      Dis                              No  Color   Desactivar   Desactivar   0 , 0 , 0 , 0
7      Dis                              No  Color   Desactivar   Desactivar   0 , 0 , 0 , 0
8      Dis                              No  Color   Desactivar   Desactivar   0 , 0 , 0 , 0
>
```

Comando Telnet: registro swm

Este comando se usa para mostrar el registro de administración del conmutador.

Sintaxis

registro de natación*Mostrar filtro*

registro de natación*día del espectáculo*

registro de natación*mostrar semana*

registro de natación*activar/desactivar el nivel <idx>* **registro**

de natación*activar/desactivar el tipo <idx>* **registro de**

natación*activar/desactivar interruptor <mac>*

Sintaxis Descripción

Parámetro	Descripción
Mostrar filtro	Significa mostrar la configuración del filtro de registro.
día del espectáculo	Significa mostrar la cantidad de registro diario.
mostrar semana	Significa mostrar la cantidad de registro semanal.
activar/desactivar el nivel <idx>	Significa encender o apagar el nivel de alerta. <idx>: 1 a 8. on/off: establece el estado (on o off) de la alerta.
activar/desactivar el tipo <idx>	Significa activar o desactivar la alerta de puerto/alerta de conmutador. <idx>: 1 a 2. "1" significa alerta de puerto; "2" significa Alerta de cambio. on/off: establece el estado (on o off) de la alerta.
activar/desactivar interruptor <mac>	Significa configurar Cambiar filtro: <mac>: Ingrese la dirección MAC del VigorSwitch. on/ off: establece el estado (on o off) de la alerta.

Ejemplo

```
> swm log show filter Nivel
de estado del índice                    En/Des
-------------------------------------- 1
      apagado      Sin alerta          es
2     apagado      Alerta menor              es
3     apagado      Alerta moderada           es
4     apagado      Alerta mayor        es
5     apagado                          Dis
6     apagado                          Dis
7     apagado                          Dis
8     apagado                          Dis

Tipo de estado de índice
-------------------------- 1
      en           Alerta de puerto
2     apagado      Cambiar alerta

Nombre del interruptor de estado del índice     Modelo Dirección Mac
-------------------------------------------------- 1
        apagado G2100                   G2100 1449bc43e579
> registro de swm establecido nivel 8 en
```

Comando Telnet: swm snmp

Este comando se utiliza para mostrar la información del conmutador a través de una consulta SNMP.

Sintaxis

nadar snmp*sistema <MAC>*

nadar snmp*iftbl <MAC> <número_puerto>*

nadar snmp*poe <MAC>* **nadar snmp***trpcom*

muestra <MAC> **nadar snmp***conjunto trpcom*

<MAC> <nombre>

Sintaxis Descripción

Parámetro	Descripción
sistema <MAC>	Significa mostrar la información del sistema. <MAC>: Ingrese la dirección MAC del VigorSwitch.
iftbl <MAC> <número_puerto>	Significa mostrar información de la interfaz del puerto. <MAC>: Ingrese la dirección MAC del VigorSwitch. <port_num>: Ingrese el número de índice (por ejemplo, 1 a 28) del puerto LAN VigorSwitch. El número de puertos LAN variará según el Switch a modificar.
poe <MAC>	Significa mostrar información de la interfaz snmp POE. <MAC>: Ingrese la dirección MAC del VigorSwitch.
trpcom muestra <MAC>	Significa mostrar Trap Community. <MAC>: Ingrese la dirección MAC del VigorSwitch.
conjunto trpcom <MAC> <nombre>	Significa establecer Trap Community. <MAC>: Ingrese la dirección MAC del VigorSwitch. <nombre>: Ingrese una cadena como comunidad vagabunda.

Ejemplo

```
> swm snmp sys 1449BC43E579
sysDescr:
sysObjectID:1.3.6.1.4.1.7367
sysUpTime:988 h 19 m 39 s
sysContact:Predeterminado
nombre del sistema: G2100
sysUbicación:Predeterminado
servicios del sistema: 79
siNúmero:0
>
```

Comando Telnet: swm tr069

Este comando permite al usuario configurar los ajustes de TR-069 para que el enrutador Vigor se comunique con el servidor VigorACS.

Sintaxis

swm tr069 mostrar

usuario swm tr069*<xxx>* **swm**

tr069 contraseña*<xxx>*

nadar tr069*<https/http>*

puerto swm tr069*<xxx>*

encuesta swm tr069*<xxx>*

Sintaxis Descripción

Parámetro	Descripción
espectáculo	Muestra la configuración del servidor de gestión de conmutadores TR069.
usuario <xxx>	Establezca un nombre de usuario para el servidor de gestión de conmutadores TR069. <xxx> - Introduzca una cadena (máx. 31 caracteres)
contraseña <xxx>	Establezca una contraseña para la gestión de conmutadores para el servidor TR069. <xxx> - Introduzca una contraseña (máx. 31 caracteres).
<https/http>	Configure el protocolo para la gestión de conmutadores para el servidor TR069. <https/http>: elija https o http.
puerto <xxx>	Establezca el número de puerto para la gestión del conmutador para el servidor TR069. <xxx>- Rango de 1 a 65535.
encuesta <xxx>	Establezca el intervalo de sondeo para la gestión de conmutadores para el servidor TR069. <xxx>- Rango de 1 a 999999.

Ejemplo

```
> swm tr069 mostrar

SWM TR069 a través de HTTP
Puerto del servidor SWM TR069: 8003
Nombre de usuario SWM TR069: acs
SWM TR069 Contraseña HTTP: contraseña
SWM TR069 poll_interval: 600

> swm tr069 encuesta 710
Establezca el intervalo de sondeo SWM TR069 en 710
```

Comando Telnet: fw_backupmode

Este comando se utiliza para hacer una copia de seguridad del firmware en el enrutador. El firmware se recuperará para reiniciar el enrutador Vigor después de que falle más de tres veces.

Sintaxis

modo fw_backup*[<comando><parámetro>|...]*

Sintaxis Descripción

Parámetro	Descripción
[<comando><parámetro>|...]	Los comandos disponibles con parámetros se enumeran a continuación. *[...]*significa que puede ingresar varios comandos en una línea.
- tn	Configure el tiempo de copia de seguridad. n : 1 ~ 168 horas
- min	Configure el modo de copia de seguridad del firmware. 1: copia de seguridad después del tiempo de espera. 0: copia de seguridad después de la actualización.
- b	Haga una copia de seguridad del firmware de forma manual e inmediata.
- rn	Configure el modo de recuperación del firmware.

	1: el firemware se recuperará cuando el sistema falle. 0: Sin recuperación.

Ejemplo

```
> modo de copia de seguridad -b
¡Haga una copia de seguridad del firmware ahora!
```

Comando Telnet: servicio

Este comando se utiliza para mostrar información sobre el servicio Myvigor. Además, permite transferir el servicio MyVigor de la cuenta original a otra cuenta.

Sintaxis

servicio -s

servicio -r

servicio -l*<cuenta><contraseña>*

servicio -yo*<nuevo_propietario><nuevo_propietario_correo*

electrónico> **servicio -t***<sí>/<no>* **servicio -c**

Sintaxis Descripción

Parámetro	Descripción
- s	Mostrar el estado del servicio.
-r	Actualizar el estado del servicio
- l <cuenta><contraseña>	Inicie sesión en el servidor MyVigor. Ingrese la cuenta y la contraseña registradas en el servidor MyVigor cuenta: ingrese el nombre de la cuenta. Contraseña: ingrese la contraseña de la cuenta.
- yo <nuevo_propietario> <correo_electrónico_del_nuevo_propietario>	Ingrese el nombre y la dirección de correo electrónico del nuevo propietario para la transferencia del servicio. New_owner: ingrese el nombre de cuenta del nuevo propietario. New_owner_email: ingrese la dirección de correo electrónico del nuevo propietario.
- t <sí>/<no>	Transferir este dispositivo Vigor a un nuevo propietario.
- C	Borrar la información de la cuenta del propietario actual.

Ejemplo

```
> servicio
> servicio -l carrieni ttt0016ttt5 Iniciar sesión
Cuenta:carrieni, Pw:ttt0016ttt5
¡Acceso exitoso! ¡Vuelva a comprobar el estado del servicio!
> servicio -s
Mostrar el estado del servicio.
Ahora el estado es [SS_STATE_REG_ACC_VALID]
Estado del servicio:
Nombre del modelo: Serie Vigor2927
Número de serie: 2019053108580701
Dirección MAC: 00:1D:AA:73:4A:78 Cuenta
del propietario: carrieni
Correo electrónico          : ca****** i@draytek.com

Estado de soporte del servicio del
dispositivo: Servicio WCF, ID = [1]
      Proveedor de servicios [Cyren] Fecha de inicio
      de la licencia [2019-09-26] Fecha de
      vencimiento de la licencia [2019-10-26]
```

Servicio APPE, ID=[4]
Proveedor de servicios [No activado]
Licencia Fecha de inicio []
Fecha de caducidad de la licencia []

Servicio DDNS, ID=[6]
Proveedor de servicios [No activado]
Licencia Fecha de inicio []
Fecha de caducidad de la licencia []

Comando Telnet: dmn

Este comando se utiliza para establecer la configuración relacionada con la red de malla, la visualización del estado o activar las acciones de la malla.

Sintaxis

habilitar *<1/0>* **dmn**

restablecer_grupo

nivel de registro dmn *<1/0>*

buscar *<iniciar/mostrar>* **estado**

maldito

maldito minodo

descubre *<iniciar/mostrar>*

maldición acs

mesa *<0/1/2/3>* **maldita**

sea desconectar

dmn auto_reseleccionar

volver a seleccionar

Sintaxis Descripción

Parámetro	Descripción
habilitar <1/0>	Activa o desactiva la función de malla. 1 - Habilitar. 0 - Deshabilitar.
restablecer_grupo	Restablezca la lista de grupos y la clave de grupo.
nivel de registro<1/0>	Establezca el nivel de registro de malla. 1 - información detallada. 0 - información básica.
inicio de busqueda *programa de búsqueda*	Buscar**disponible**nodos de malla en el entorno para unirse a la red de malla. start - Empezar a buscar. show - Muestra el resultado de la búsqueda.
estado	Mostrar el estado del grupo.
minodo	Muestra el estado local de este dispositivo. Por ejemplo, DrayTek> dmn mynode % [dmn_cmd] mi nodo: Enlace ascendente inalámbrico preferido: Modo de funcionamiento automático: MeshNode (cableado) Root MAC: 00:00:00:00:00:00 Salto : 0 Enlace ascendente: ninguno Enlace descendente (0):

	Modelo : Vigor2927 Nombre del dispositivo: DrayTek MAC : 00:1D:AA:70:33:E0 Estado : Nodo de malla (enlace ascendente cableado) - Aislar : Estado Nuevo
descubrir empezar *descubrir mostrar*	Busque dispositivos de malla (incluida la raíz de malla y el nodo de malla) alrededor de este enrutador. start - Empezar a buscar. show - Muestra el resultado de la búsqueda.
ac	Obtenga información enviando solicitudes al servidor de autoconfiguración de Mesh. Los subcomandos disponibles incluyen: (g)et - obtener mynode y lista de estaciones (s)et - establece todos los parámetros print(t) - imprime toda la lista (c)lear - borra todo el método (p) causa - pausa acs (r)esume - reanudar acs st(a)tus - estado del grupo acs sta(l)ist - imprimir la lista de estaciones de todos los nodos (u)p_sta_status - imprimir actualizar el estado de la lista de estaciones r(e)set - restablecer dmn acs
mesa <0/1/2>	Muestre una tabla de dispositivos de la red en malla. 0 - Tabla de originadores 1 - Mesa de cliente local 2 - Mesa de cliente remota
desconectar <mac>	Desconecte un nodo de malla inalámbrica en línea. En general, el nodo de malla se volverá a conectar a la red de malla más tarde. <mac>: ingrese la dirección MAC del nodo de malla en un grupo de malla. (Ej. dmn desconectar 00:1d:aa:22:33:44)
auto_reseleccionar	Habilite (1) o deshabilite (0) la función de reselección automática. Si está habilitada, la raíz de malla inicia automáticamente una reselección de malla después de cambiar la red de malla.
volver a seleccionar	Inicie una Reselección de malla inmediatamente. Un nodo de malla inalámbrica en línea puede volver a conectarse a un enlace ascendente inalámbrico mejor.

Ejemplo

> dmn actualizar 2
% Elimine el nodo [2] y deje que se recupere automáticamente
> dmn establecer rssi 50
> maldito