DrayTek

Vigor2926 系列

雙WAN口安全防護路由器

Your reliable networking solutions partner



使用手冊

V1.0

Vigor2926 系列
雙 WAN 口安全防護路由器

使用手冊

版本: 1.0

韌體版本: V3.8.9.1

(請造訪居易網站，隨時獲取更新資訊)

日期: 2018 年 7 月 19 日

版權資訊

©版權所有，翻印必究。此出版物所包含資訊受版權保護。未經版權所有人書面許可，不得對其進行拷貝、傳播、轉錄、摘錄、儲存到檢索系統或轉譯成其他語言。交貨以及其他詳細資料的範圍若有變化，恕不預先通知。

商標

本手冊內容使用以下商標:

- Microsoft 爲微軟公司註冊商標
- Windows 視窗系列，包括 Windows 95, 98, Me, NT, 2000, XP, Vista, 7 以及其 Explorer 均屬微軟公司商標
- Apple 以及 Mac OS 均屬蘋果電腦公司的註冊商標
- 其他產品則爲各自生產廠商之註冊商標

安全說明和保障

- 在設置前請先閱讀安裝說明。
- 由於路由器是複雜的電子產品，請勿自行拆除或是維修本產品。
- 請勿自行打開或修復路由器。
- 請勿把路由器置於潮濕的環境中，例如浴室。
- 請將本產品放置在足以遮風避雨之處，適合溫度在攝氏 5 度到 40 度之間。
- 請勿將本產品暴露在陽光或是其他熱源下，否則外殼以及零件可能遭到破壞。
- 請勿將 LAN 網線置於戶外，以防電擊危險。
- 請將本產品放置在小孩無法觸及之處。
- 若您想棄置本產品時，請遵守當地的保護環境的法律法規。

保固

自使用者購買日起二年內爲保固期限(保固: 原廠一年,需線上註冊加給一年,合計二年)，請將您的購買收據保存二年，因爲它可以證明您的購買日期。當本產品發生故障乃導因於製作及(或)零件上的錯誤，只要使用者在保固期間內出示購買證明，居易科技將採取可使產品恢復正常之修理或更換有瑕疵的產品(或零件)，且不收取任何費用。居易科技可自行決定使用全新的或是同等價值且功能相當的再製產品。下列狀況不在本產品的保固範圍內：(1)若產品遭修改、錯誤(不當)使用、不可抗力之外力損害，或不正常的使用，而發生的故障；(2) 隨附軟體或是其他供應商提供的授權軟體；(3) 未嚴重影響產品堪用性的瑕疵。.

成爲一個註冊用戶

- 建議在 Web 介面進行註冊。您可以到 http://www.draytek.com.tw 註冊您的 Vigor 路由器。

韌體及工具的更新

- 請造訪 DrayTek 主頁以獲取有關最新韌體、工具及檔案文件的資訊。
  http://www.draytek.com.tw

目錄

第一篇 安裝 i

I-1 簡介 1

I-1-1 指示燈與介面說明 2

I-1-1-1 Vigor2926 / Vigor2926L 2
I-1-1-2 Vigor2926n / Vigor2926ac / Vigor2926Lac / Vigor2926Ln 4
I-1-1-3 Vigor2926Vac 8

I-1-2 天線安裝注意事項("L" 系列機種) 10

I-2 硬體安裝 12

I-2-1 安裝 Vigor 路由器 12

I-2-2 壁掛安裝 13

I-2-3 安裝 USB 印表機至 Vigor 路由器 14

I-3 進入設定網頁 20

I-4 變更密碼 22

I-5 儀表板簡介 23

I-5-1 虛擬面板 24

I-5-2 底線連結 24

I-5-3 LTE 狀態 25

I-5-4 常用功能的快速存取 25

I-5-5 圖形介面地圖(GUI Map) 26

I-5-6 網頁操作台(Web Console) 27

I-5-7 設定備份(Config Backup) 28

I-5-8 登出 28

I-5-9 連線狀態 29

I-5-9-1 實體連線 29
I-5-9-2 虛擬 WAN 31

I-6 快速設定精靈(Quick Start Wizard) 32

I-6-1 對於 WAN1/WAN2 介面(乙太網路) 33

I-6-2 對於 WAN3/WAN4 (USB) 41

I-6-3 對於 LTE WAN 44

I-7 服務啓動精靈 46

I-8 註冊 Vigor 路由器 48

第二篇 連線設定 51

II-1 WAN 52

網頁使用者介面 54

II-1-1 基本設定(General Setup) 54

II-1-1-1 乙太網路的 WAN1/WAN2 介面 56
II-1-1-2 USB 的 WAN3/WAN4 介面 58

II-1-2 網際網路連線(Internet Access) 60
II-1-2-1 WAN1/WAN2 中的 PPPoE 模式細節設定(實體模式：乙太網路) *63*
II-1-2-2 WAN1/WAN2 中的固定或是動態 IP 模式細節設定(實體模式：乙太網路) *66*
II-1-2-3 WAN1/WAN2 中的 PPTP/L2TP 模式細節設定(實體模式：乙太網路) *69*
II-1-2-4 WAN3/WAN4 中的 3G/4G USB 數據機模式細節設定(PPP 模式) *71*
II-1-2-5 WAN3/WAN4 中的 3G/4G USB 數據機模式細節設定(DHCP 模式) *73*
II-1-2-6 LTE WAN 中的 3G/4G USB 數據機模式細節設定(DHCP 模式) *75*
II-1-2-7 WAN1/WAN2/WAN3/WAN4 的斷線模式細節設定(IPv6) *77*
II-1-2-8 WAN1/WAN2 的 PPP 模式細節設定(IPv6) *77*
II-1-2-9 WAN1/WAN2/WAN3/WAN4 的 TSPC 模式細節設定(IPv6) *79*
II-1-2-10 WAN1/WAN2/WAN3/WAN4 的 AICCU 模式細節設定(IPv6) *81*
II-1-2-11 WAN1/WAN2 的 DHCPv6 用戶端模式細節設定(IPv6) *82*
II-1-2-12 WAN1/WAN2 的固定 IPv6 模式細節設定(IPv6) *83*
II-1-2-13 WAN1/WAN2 的 6in4 固定通道模式細節設定(IPv6) *85*
II-1-2-14 WAN1/WAN2 的 6rd 模式細節設定(IPv6) *86*
II-1-3 多重 VLAN (Multi-VLAN) 88
II-1-4 WAN 計量收費(WAN Budget) 93
II-1-4-1 基本設定(General Setup) *93*
II-1-4-2 狀態(Status) *95*
應用說明 97
A-1 如何設定多重 VLAN 以便因應三合一服務? *97*
A-2 多重 WAN Vigor 路由器的負載平衡與備援 *102*
II-2 LAN 104
網頁使用者介面 106
II-2-1 基本設定(General Setup) 106
II-2-1-1 LAN1–乙太網路 TCP/IP 與 DHCP 設定之細節設定 *108*
II-2-1-2 LAN2 ~ LAN8 與 DMZ 之細節設定 *110*
II-2-1-3 IP 路由子網之細節設定 *113*
II-2-1-4 LAN IPv6 設定之細節設定 *114*
II-2-1-5 進階 DHCP Options 設定 *118*
應用說明 120
A-1 多網段應用-如何使用不做 NAT 的 Vigor 路由器? *120*
II-2-2 虛擬區域網路(VLAN) 123
II-2-3 綁定 IP 與 MAC 位址(Bind IP to MAC) 127
II-2-4 埠口監控(LAN Port Mirror) 130
II-2-5 有線 802.1x(Wired 802.1x) 131
II-3 硬體加速(Hardware Acceleration) 132
II-3-1 設定(Setup) 132
II-4 NAT 135
網頁使用者介面 136
II-4-1 通訊埠重導向(Port Redirection) 136
II-4-2 DMZ 主機(DMZ Host) 140
II-4-3 開放通訊埠(Open Ports) 143
II-4-4 埠號觸發(Port Triggering) 145

II-4-5 應用層閘道(ALG) 147
II-5 其他應用(Applications) 148
網頁使用者介面 150
II-5-1 動態 DNS(Dynamic DNS) 150
II-5-2 LAN DNS / DNS 轉送(LAN DNS / DNS Forwarding) 155
II-5-3 DNS 安全性(DNS Security) 158
II-5-3-1 基本設定(General Setup) *158*
II-5-3-2 網域自我診斷(Domain Diagnose) *159*
II-5-4 排程(Schedule) 160
II-5-5 RADIUS/TACACS+ 163
II-5-5-1 外接 RADIUS(External RADIUS) *163*
II-5-5-2 內部 RADIUS(Internal RADIUS) *164*
II-5-5-3 外接 TACACS+(External TACACS+) *166*
II-5-6 Active Directory/LDAP 167
II-5-6-1 基本設定(General Setup) *167*
II-5-6-2 Active Directory / LDAP 設定檔(Active Directory / LDAP Profiles) *168*
II-5-7 UPnP 170
II-5-8 IGMP 171
II-5-8-1 基本設定(General Setting) *171*
II-5-8-2 工作群組(Working Groups) *171*
II-5-9 網路喚醒(Wake on LAN,WOL) 173
II-5-10 簡訊(SMS)/郵件警示服務(SMS / Mail Alert Service) 174
II-5-10-1 簡訊警示(SMS Alert) *174*
II-5-10-2 郵件警示(Mail Alert) *175*
II-5-11 Bonjour 176
II-5-12 高可靠度(High Availability) 179
II-5-12-1 基本設定(General Setup) *180*
II-5-12-2 設定同步化(Config Sync) *182*
II-5-13 本機 802.1X 基本設定(Local 802.1X General Setup) 184
應用說明 186
A-1 如何使用高可靠度(HA)? *186*
A-2 如何使用 DrayDDNS? *194*
A-3 如何設定客製化 DDNS? *199*
A-4 如何實施 LDAP/AD 驗證以應使用者管理? *203*
II-6 路由(Routing) 206
網頁使用者介面 207
II-6-1 固定路由(Static Route) 207
II-6-2 負載平衡/策略路由(Load-Balance /Route Policy) 213
II-6-2-1 基本設定(General Setup) *213*
II-6-2-2 自我診斷(Diagnose) *218*
II-6-3 BGP 221
II-6-3-1 基本設定(Basic Settings) *221*
II-6-3-1 固定網路(Static Network) *222*

應用說明 223
A-1 如何利用路由策略設定位址對應(Address Mapping)? 223
A-2 如何使用路由策略中的目標網域名稱? 225
A-3 如何使用區域網路(LAN)中的真實 IP? 227
A-4 簡要說明負載平衡/策略路由(Load Balance/Route Policy) 232
II-7 LTE 234
網頁使用者介面 235
II-7-1 基本設定(General Settings) 235
II-7-1-1 簡訊額度(SMS Quota) 235
II-7-1-2 簡訊收件匣/寄件匣策略(SMS Inbox/Outbox Policy) 236
II-7-2 簡訊收件匣(SMS Inbox) 237
II-7-3 傳送簡訊(Send SMS) 240
II-7-4 路由器指令(Router Commands) 241
II-7-5 狀態(Status) 243

第三篇 無線區域網路設定 245

III-1 無線區域網路設定(Wireless LAN (2.4GHz/5GHz)) 246
網頁使用者介面 249
III-1-1 無線網路設定精靈(Wireless Wizard) 249
III-1-2 基本設定(General Setup) 253
III-1-3 安全性設定(Security) 254
III-1-4 連線控制(Access Control) 257
III-1-5 WPS 258
III-1-6 WDS 261
III-1-7 進階設定(Advanced Setting) 265
III-1-8 無線用戶控制(Station Control) 267
III-1-9 頻寬管理(Bandwidth Management) 268
III-1-10 搜尋無線基地台(AP Discovery) 269
III-1-11 無線頻寬均化(Airtime Fairness) 270
III-1-12 頻段操控(Band Steering) 272
III-1-13 漫遊(Roaming) 276
III-1-14 無線用戶端列表(Station List) 277

第四篇 VoIP 語音設定 279

IV-1 VoIP 280
網頁使用者介面 282
IV-1-1 VoIP 設定精靈(VoIP Wizard) 282
IV-1-2 基本設定(General Settings) 284
IV-1-3 SIP 帳號(SIP Accounts) 287
IV-1-4 撥號對應表(DialPlan) 291

IV-1-4-1 電話簿(Phone Book) *291*
IV-1-4-2 數字對應設定(Digit Map) *293*
IV-1-4-3 限撥等級(Call Barring) *295*
IV-1-4-4 區域設定(Regional) *297*
IV-1-4-5 PSTN 設定(PSTN Setup) *299*
IV-1-5 電話設定(Phone Settings) 300
IV-1-6 狀態(Status) 304
IV-1-7 自我診斷(Diagnostics) 306
IV-1-7-1 來電者 ID (Caller ID) *306*
IV-1-7-2 音調(Tone) *306*

第五篇 VPN 連線設定 307

V-1 VPN 與遠端存取(VPN and Remote Access) 308
網頁使用者介面 309
V-1-1 VPN 用戶端設定精靈(VPN Client Wizard) 309
V-1-2 VPN 伺服器端精靈(VPN Server Wizard) 316
V-1-3 遠端存取控制(Remote Access Control) 320
V-1-4 PPP 基本設定(PPP General Setup) 321
V-1-5 IPSec IPSec 基本設定(IPsec General Setup) 323
V-1-6 IPSec 端點辨識(IPsec Peer Identity) 324
V-1-7 遠端撥入使用者(Remote Dial-in User) 326
V-1-8 LAN to LAN 329
V-1-9 VPN TRUNK 管理(VPN Trunk Management) 340
V-1-10 連線管理(Connection Management) 349
應用說明 351
A-1 如何在總公司與遠端分公司建立 LAN-to-LAN VPN 連線通道(透過 Main 模式) *351*
V-2 SSL VPN 356
網頁使用者介面 357
V-2-1 基本設定(General Setup) 357
V-2-2 使用者帳號(User Account) 358
V-2-3 使用者群組(User Group) 362
V-2-4 線上使用者狀態(Online User Status) 364
V-3 憑證管理(Certificate Management) 365
網頁使用者介面 366
V-3-1 本機憑證(Local Certificate) 366
V-3-2 具公信力之 CA 憑證(Trusted CA Certificate) 370
V-3-3 憑證備份(Certificate Backup) 372

第六篇 安全性設定 373

VI-1 防火牆(Firewall) 374

網頁使用者介面 376
VI-1-1 基本設定(General Setup) 376
VI-1-2 過濾器設定(Filter Setup) 381
VI-1-3 DoS 攻擊防禦功能設定(DoS Defense) 391
VI-1-4 診斷(Diagnose) 393
應用說明 396
A-1 如何限定特定電腦存取網際網路 396
VI-2 數位內容安全管理(CSM) 400
網頁使用者介面 401
VI-2-1 應用程式管控設定檔(APP Enforcement Profile) 401
VI-2-2 APPE 特徵碼更新(APPE Signature Upgrade) 405
VI-2-3 URL 內容過濾器設定檔(URL Content Filter Profile) 407
VI-2-4 網頁內容過濾器設定檔(Web Content Filter Profile) 411
VI-2-5 DNS 過濾器設定檔(DNS Filter Profile) 415
應用說明 417
A-1 如何建立一個 MyVigor 帳號 417
A-2 用網頁內容過濾器(WCF) / URL 內容過濾器來阻擋使用者存取 Facebook 服務 425

第七篇 管理設定 431

VII-1 系統維護(System Maintenance) 432
網頁使用者介面 433
VII-1-1 系統狀態(System Status) 434
VII-1-2 TR-069 436
VII-1-3 系統管理員密碼(Administrator Password) 439
VII-1-4 使用者密碼(User Password) 441
VII-1-5 登入頁面設定(Login Page Greeting) 444
VII-1-6 設定備份(Configuration Backup) 446
VII-1-7 Syslog/郵件警示設定(Syslog/Mail Alert) 449
VII-1-8 時間和日期(Time and Date) 452
VII-1-9 SNMP 454
VII-1-10 管理(Management) 456
VII-1-11 面板控制(Panel Control) 459
VII-1-12 自行簽核憑證(Self-Signed Certificate) 463
VII-1-13 重啓路由器(Reboot System) 465
VII-1-14 韌體升級(Firmware Upgrade) 466
VII-1-15 韌體備份(Firmware Backup) 467
VII-1-16 開啓授權碼(Activation) 468
VII-1-17 內部服務使用者清單(Internal Service User List) 469
VII-2 頻寬管理(Bandwidth Management) 470

網頁使用者介面 472
VII-2-1 連線數限制(Sessions Limit) 472
VII-2-2 頻寬限制(Bandwidth Limit) 474
VII-2-3 服務品質(QoS) 476
VII-2-4 APP QoS 483
應用說明 486
A-1 如何利用 QoS 來最佳化頻寬管理 486
VII-3 使用者管理(User Management) 490
網頁使用者介面 491
VII-3-1 基本設定(General Setup) 491
VII-3-2 使用者設定檔(User Profile) 493
VII-3-3 使用者群組(User Group) 498
VII-3-4 使用者線上狀態(User Online Status) 499
應用說明 501
A-1 如何透過使用者管理驗證用戶端 501
A-2 如何使用指定首頁功能 510
VII-4 客製化入口網站設定(Hotspot Web Portal) 514
網頁使用者介面 514
VII-4-1 設定檔配置(Profile Setup) 514
VII-4-1-1 登入模式(Login Modes) 515
VII-4-1-2 設定入口網站設定檔步驟 516
VII-4-2 使用者資訊(User Information) 529
VII-4-2-1 使用者資訊(User Info) 529
VII-4-2-2 資料庫設定(Database Setup) 531
應用說明 533
A-1 如何建立臉書 APP ID 以利網頁入口驗證？ 533
A-2 如何建立 Google APP ID 以利網頁入口驗證 539
VII-5 中央管理(VPN) 541
網頁使用者介面 542
VII-5-1 基本設定(General Setup) 542
VII-5-1-1 基本設定(General Setup) 542
VII-5-1-2 IPsec VPN 設定(IPsec VPN Settings) 543
VII-5-2 CPE 管理(CPE Management) 544
VII-5-2-1 受管理的裝置清單(Managed Device List) 544
VII-5-2-2 CPE 維護(CPE Maintenance) 547
VII-5-2-3 Google 地圖(Google Map) 550
VII-5-3 VPN 管理(VPN Management) 551
VII-5-4 紀錄與警示(Log & Alert) 552
應用說明 553
A-1 CVM 應用-如何透過 Vigor2926 管理 CPE (路由器)? 553
A-2 CVM 應用-如何於 Vigor2926 與遠端設備之間建立 VPN 連線? 557
A-3 CVM 應用-如何透過 Vigor2926 更新遠端 CPE 韌體? 559

VII-6 中央管理(AP) 562
網頁使用者介面 563
VII-6-1 儀表板(Dashboard) 563
VII-6-2 狀態(Status) 564
VII-6-3 WLAN 設定檔(WLAN Profile) 565
VII-6-4 AP 維護(AP Maintenance) 570
VII-6-5 AP 地圖(AP Map) 571
VII-6-6 流量圖表(Traffic Graph) 575
VII-6-7 非法 AP 偵測(Rogue AP Detection) 576
VII-6-8 事件日誌(Event Log) 579
VII-6-9 全部流量(Total Traffic) 579
VII-6-10 站台數目(Station Number) 580
VII-6-11 負載平衡(Load Balance) 580
VII-6-12 功能支援列表(Function Support List) 581
應用說明 582
A-1 如何使用 AP 管理功能來檢查 AP 狀態並部署 WALN 設定檔? 582
VII-7 中央管理(交換器) 585
VII-7-1 狀態(Status) 585
VII-7-1-1 交換器狀態(Switch Status) 585
VII-7-1-2 交換器層次結構(Switch Hierarchy) 588
VII-7-2 設定檔(Profile) 589
VII-7-3 群組(Group) 592
VII-7-4 維護(Maintenance) 594
VII-7-5 警示與日誌(Alert and Log) 595
VII-7-5-1 警示設定(Alert Setup) 595
VII-7-5-2 交換器與埠口設定(Switch and Port Setup) 596
VII-7-5-3 警示日誌(Alert Logs) 598
VII-7-6 資料庫設定(Database Setup) 599
VII-7-7 支援清單(Support List) 600
VII-8 中央管理(外接裝置)(Central Management (External Devices)) 601
VII-8-1 全部裝置(ll Devices) 601
第八篇 其他設定 603
VIII-1 物件設定(Objects Settings) 604
網頁使用者介面 605
VIII-1-1 IP 物件設定檔(IP Object) 605
VIII-1-2 IP 群組(IP Group) 609
VIII-1-3 IPv6 物件(IPv6 Object) 611
VIII-1-4 IPv6 群組(IPv6 Group) 613

VIII-1-5 服務類型物件(Service Type Object) 614
VIII-1-6 服務類型群組(Service Type Group) 616
VIII-1-7 關鍵字物件(Keyword Object) 618
VIII-1-8 關鍵字群組(Keyword Group) 620
VIII-1-9 副檔名物件(File Extension Object) 621
VIII-1-10 簡訊(SMS)/郵件服務物件(SMS/Mail Service Object) 623
VIII-1-11 通知物件(Notification Object) 628
VIII-1-12 字串物件(String Object) 631
VIII-1-13 國家物件(Country Object) 632
應用說明 634
A-1 當 WAN 斷線時如何使用 SMS 簡訊服務寄發通知至指定的電話號碼 634
VIII-2 USB 應用(USB Application) 638
網頁使用者介面 639
VIII-2-1 USB 基本設定(USB General Settings) 639
VIII-2-2 USB 使用者管理(USB User Management) 640
VIII-2-3 檔案瀏覽(File Explorer) 642
VIII-2-4 USB 磁碟狀態(USB Device Status) 642
VIII-2-5 溫度感應器(Temperature Sensor) 643
VIII-2-6 數據機支援清單(Modem Support List) 646
VIII-2-7 SMB 用戶端支援清單(SMB Client Support List) 647
應用說明 648
A-1 如何取得連接至 Vigor 路由器的 USB 裝置內的檔案? 648

第九篇 故障排除 651

IX-1 自我診斷工具(Diagnostics) 652
網頁使用者介面 653
IX-1-1 撥號觸發器(Dial-out Triggering) 653
IX-1-2 路由表(Routing Table) 654
IX-1-3 ARP 快取表(ARP Cache Table) 655
IX-1-4 IPv6 芳鄰表(IPv6 Neighbour Table) 656
IX-1-5 DHCP 表(DHCP Table) 657
IX-1-6 NAT 連線數狀態表(NAT Sessions Table) 658
IX-1-7 DNS 快取表(DNS Cache Table) 659
IX-1-8 Ping 自我診斷(Ping Diagnosis) 660
IX-1-9 資料流量監控(Data Flow Monitor) 661
IX-1-10 流量圖表(Traffic Graph) 664
IX-1-11 VPN 圖表(VPN Graph) 665
IX-1-12 追蹤路由(Trace Route) 666

IX-1-13 Syslog 系統資源管理 (System Explorer) 667
IX-1-14 IPv6 TSPC 狀態(IPv6 TSPC Status) 669
IX-1-15 高可靠度狀態(High Availability Status) 669
IX-1-16 認證資訊 (Authentication Information) 672
IX-1-17 DoS Flood 表格(DoS Flood Table) 673
IX-1-18 路由策略診斷(Route Policy Diagnosis) 675
IX-2 檢查路由器硬體狀態是否正常 677
IX-3 檢查您電腦的網路連接設置是否正確 678
IX-4 從電腦上 Ping 路由器 682
IX-5 檢查 ISP 的設置是否正常 684
IX-6 3G/4G 網路連線相關問題 685
IX-7 還原路由器原廠預設組態 686
IX-8 聯絡居易 688

第十篇 Telnet 指令設定 689

進入路由器 Telnet 690

索引 948

第一篇 安裝



Installation

本篇將介紹路由器並引導使用者進行硬體安裝及軟體的設定。

I-1 簡介

This is a generic International version of the user guide. Specification, compatibility and features vary by region. For specific user guides suitable for your region or product, please contact local distributor.

Vigor2926 系列爲寬頻路由器，整合 IP 層級的 QoS、NAT 連線數/頻寬管理等功能，讓使用者能以較大的頻寬進行工作調配的需要。

藉由採用硬體 VPN 平臺及 AES/DES/3DS 硬體加密方式，Vigor2925 系列大大提昇了 VPN 的效用，並在 VPN 通道中提供數種協定(諸如 IPSec/PPTP/L2TP) 應用。

在 SPI (Stateful Packet Inspection)防火牆中提供的物件式設計，讓使用者能輕鬆的設定防火牆策略，數位內容安全管理(CSM, Content Security Management)讓使用者能更有效率的控制即時通訊軟體及點對點軟體，此外，URL/網頁內容過濾器及 DoS/DDoS 防止功能強化了路由器的外部安全性管理及內部的控制。

使用者管理功能可防止任一電腦，在沒有使用者名稱或是密碼的驗證下進行網際網路存取連線，這個功能還可讓雇主給辦公室的員工分別給予不同的時間額度。

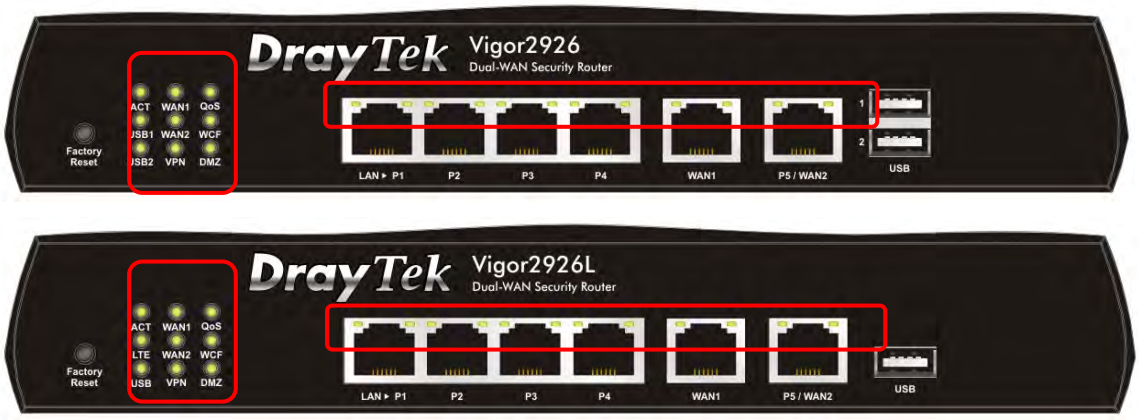
在具備無線功能的機種上(Vigor2926n/n-plus/Vn/Vn-plus/ac/Vac)，每個無線 SSID 皆可群組在 VLAN 上。

此外，Vigor2926 系列支援 USB 介面，可供連接 USB 印表機分享列印或是 USB 儲存裝置分享檔案。

I-1-1 指示燈與介面說明

不同機種路由器之 LED 顯示面板以及背板連接介面有些許的差異，詳列如下：

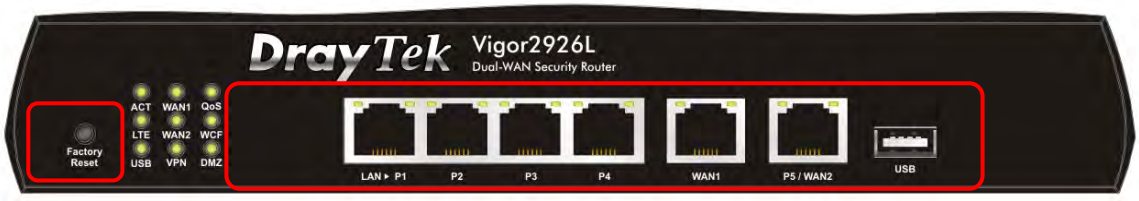
I-1-1-1 Vigor2926 / Vigor2926L



LED	狀態	說明
ACT (Activity)	閃爍	路由器已開機並可正常運作。
	熄燈	路由器已關機。
WAN1~WAN2	亮燈	網際網路連線預備妥當可以使用。
	熄燈	網際網路尚未預備妥當。
	閃爍	正在傳輸資料中。
QoS	亮燈	QoS 功能已開啓。
LTE	亮燈	LTE 裝置已連接，等待使用中。
	熄燈	LTE 裝置未被偵測出來，或是發生嚴重問題 (例如沒有安裝 SIM 卡，SIM pin 碼錯誤，SIM 卡無法啓用等等)
	閃爍	緩慢：LTE 裝置撥號中。 快速：正在傳輸資料中。
USB1~USB2/ USB	亮燈	USB 裝置已連接，等待使用中。
	閃爍	正在傳輸資料中。
WCF	亮燈	網頁內容過濾器已啓動(此功能是在**防火牆>>基本設定 (Firewall >> General Setup)**中所驅動)。
VPN	亮燈	VPN 通道已建立。
	熄燈	VPN 服務已停用。
	閃爍	資料透過 VPN 通道傳輸中。
DMZ	亮燈	DMZ 子網路功能已啓用。
	熄燈	DMZ 子網路功能尚未啓用。
	閃爍	資料傳輸中。
連接器上的指示燈		
LAN1~LAN4	左邊 亮燈	介面網路已連接。
	熄燈	介面網路未連接。
	閃爍	正在傳輸資料中。
	右邊 亮燈	介面的連接速度爲 1000Mbps。
	熄燈	介面的連接速度爲 10/100Mbps。
WAN1~	左邊 亮燈	介面網路已連接。
	熄燈	介面網路未連接。

WAN2		閃爍	正在傳輸資料中。
	右邊	亮燈	介面的連接速度爲 1000Mbps。
		熄燈	介面的連接速度爲 10/100Mbps。







背面開關

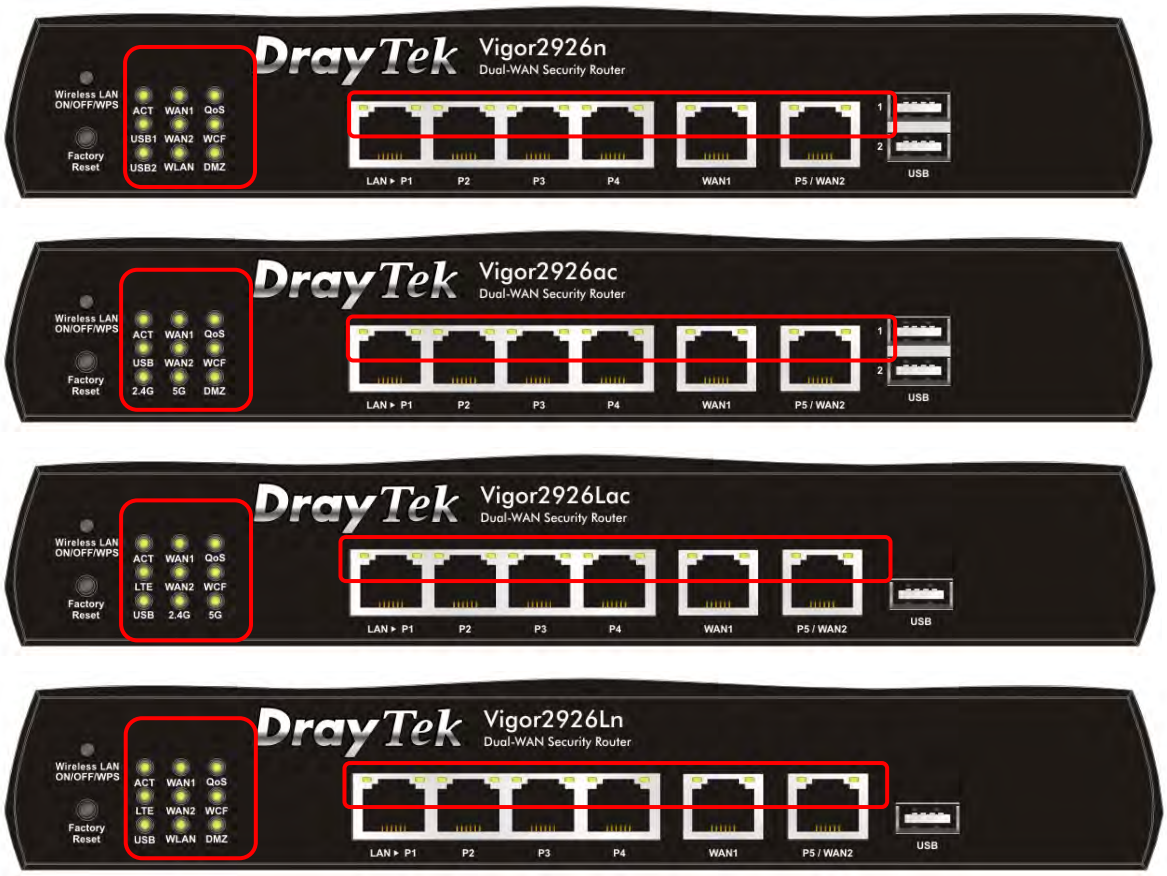


(適用 LTE 機種)

介面	說明
Factory Reset(出廠預設值按鈕)	還原成出廠預設值。 使用方法：開啓路由器（ACT LED 閃動）。用圓珠筆按下小孔內的按鈕，然後維持 5 秒左右。當您發現 ACT LED 快速閃動時，請鬆開按鈕。路由器隨後將重新啓動，並回復出廠預設值。
LAN1~LAN5	連接到電腦或網路設備。
WAN1~WAN2	連接到 ADSL 或是 Cable Modem 裝置。
USB1~USB2	連接到 USB 3G/4G 數據機、印表機或是環境溫度計。
PWR	連接電源變壓器。
ON/OFF	電源開關。
SIM Card Slot	連接 SIM 卡。

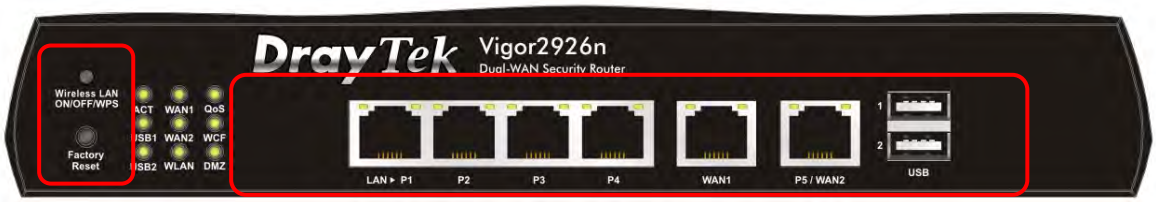
埠口“P5 / WAN2”是可切換的，依照網頁設定介面的設定資訊，此埠口可以用於 LAN 連線或是 WAN 連線。

I-1-1-2 Vigor2926n / Vigor2926ac / Vigor2926Lac / Vigor2926Ln



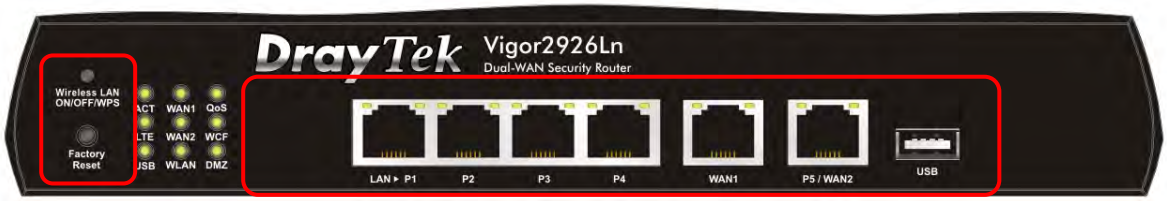
LED	狀態	說明
ACT (Activity)	閃爍	路由器已開機並可正常運作。
	熄燈	路由器已關機。
WAN1~WAN2	亮燈	網際網路連線預備妥當可以使用。
	熄燈	網際網路尚未預備妥當。
	閃爍	正在傳輸資料中。
QoS	亮燈	QoS 功能已開啓。
LTE	亮燈	LTE 裝置已連接，等待使用中。
	熄燈	LTE 裝置未被偵測出來，或是發生嚴重問題 (例如沒有安裝 SIM 卡，SIM pin 碼錯誤，SIM 卡無法啓用等等)
	閃爍	緩慢：LTE 裝置撥號中。 快速：正在傳輸資料中。
USB	亮燈	USB 裝置已連接，等待使用中。
	閃爍	正在傳輸資料中。
WCF	亮燈	網頁內容過濾器已啓動(此功能是在**防火牆>>基本設定 (Firewall >> General Setup)**中所驅動)。
2.4G/5G/WLAN	亮燈	2.4G/5G：頻寬爲 2.4GHz/5GHz 之無線基地台已準備妥當，等待使用中。 WLAN：無線基地台已準備妥當，等待使用中。
	閃爍	無線資料傳輸時，此燈號會慢速閃爍。當 WPS 運作時，ACT 和 WLAN 燈號會同時快速閃爍，2 分鐘後會回到正常狀態(您需要在 2 分鐘內設定 WPS。)
DMZ	亮燈	DMZ 子網路功能已啓用。

		熄燈	DMZ 子網路功能尚未啓用。
		閃爍	資料傳輸中。
連接器上的指示燈			
LAN1~ LAN4	左邊	亮燈	介面網路已連接。
		熄燈	介面網路未連接。
		閃爍	正在傳輸資料中。
	右邊	亮燈	介面的連接速度爲 1000Mbps。
		熄燈	介面的連接速度爲 10/100Mbps。
WAN1 ~ WAN2	左邊	亮燈	介面網路已連接。
		熄燈	介面網路未連接。
		閃爍	正在傳輸資料中。
	右邊	亮燈	介面的連接速度爲 1000Mbps。
		熄燈	介面的連接速度爲 10/100Mbps。











背面開關



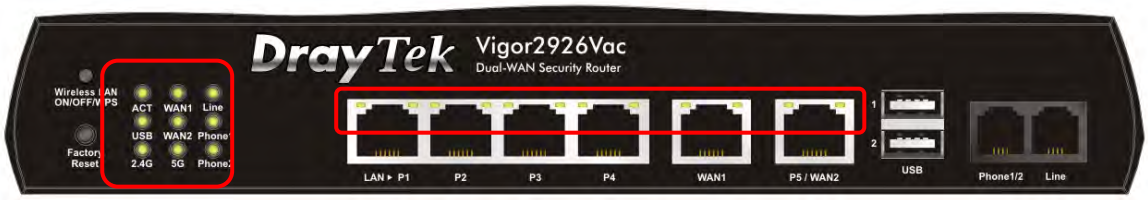
(適用 LTE 機種)

介面	說明
Wireless LAN ON/OFF/WPS	Vigor2926n： ● 按住此按鈕並於 2 秒內放開，可開啓(亮綠燈)無線網路。 ● 按住此按鈕並於 2 秒內放開，可關閉(熄燈)無線網路。 Vigor2926ac/Vigor2926Lac/Vigor2926Ln: 無線頻寬切換/變更，依照按鈕的按壓方式而定，例如， ● 2.4G (啓用) and 5G (啓用) – 預設值 ● 2.4G (停用) and 5G (啓用) – 壓下並放開，一次 ● 2.4G (啓用) and 5G (停用) – 壓下並放開，二次 ● 2.4G (停用)and 5G (停用) – 壓下並放開，三次 若使用者介面已經啓用 WPS 功能，則按住 WPS 按鈕 2 分鐘等待用戶裝置透過 WPS 執行網路連線，當燈號亮起時，即表示 WPS 連線成功。
Factory Reset(出廠預設值按鈕)	還原成出廠預設值。 使用方法：開啓路由器（ACT LED 閃動）。用圓珠筆按下小孔內的按鈕，然後維持 5 秒左右。當您發現 ACT LED 快速閃動時，請鬆開按鈕。路由器隨後將重新啓動，並回復出廠預設值。
LAN1~LAN5	連接到電腦或網路設備。
WAN1~WAN2	連接到 ADSL 或是 Cable Modem 裝置。
USB1~2 / USB	連接到 USB 3G/4G 數據機、印表機或是環境溫度計。

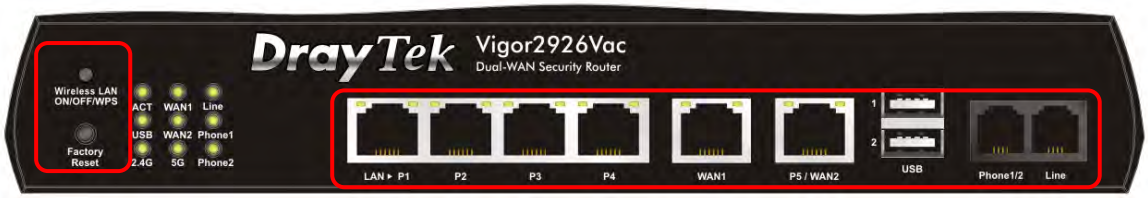
PWR	連接電源變壓器。
ON/OFF	電源開關。
SIM Card Slot	連接 SIM 卡。

埠口“P5 / WAN2”是可切換的，依照網頁設定介面的設定資訊，此埠口可以用於 LAN 連線或是 WAN 連線。

I-1-1-3 Vigor2926Vac



LED		狀態	說明
ACT (Activity)		閃爍	路由器已開機並可正常運作。
		熄燈	路由器已關機。
WAN1~ WAN2		亮燈	網際網路連線預備妥當可以使用。
		熄燈	網際網路尚未預備妥當。
		閃爍	正在傳輸資料中。
Line		亮燈	PSTN 來電(入與出)，但是當來電中斷後，LED 將會熄燈。
		熄燈	沒有 PSTN 來電。
USB		亮燈	USB 裝置已連接，等待使用中。
		閃爍	正在傳輸資料中。
Phone1/Phone2		亮燈	連接本埠之電話使用中。
		熄燈	連接本埠之電話未被使用。
		閃爍	電話來電。
2.4G/5G		亮燈	2.4G/5G：頻寬爲 2.4GHz/5GHz 之無線基地台已準備妥當，等待使用中。 WLAN：無線基地台已準備妥當，等待使用中。
		閃爍	無線資料傳輸時，此燈號會慢速閃爍。當 WPS 運作時，ACT 和 WLAN 燈號會同時快速閃爍，2 分鐘後會回到正常狀態(您需要在 2 分鐘內設定 WPS。)
連接器上的指示燈			
LAN1~ LAN4	左邊	亮燈	介面網路已連接。
		熄燈	介面網路未連接。
		閃爍	正在傳輸資料中。
	右邊	亮燈	介面的連接速度爲 1000Mbps。
		熄燈	介面的連接速度爲 10/100Mbps。
WAN1 ~ WAN2	左邊	亮燈	介面網路已連接。
		熄燈	介面網路未連接。
		閃爍	正在傳輸資料中。
	右邊	亮燈	介面的連接速度爲 1000Mbps。
		熄燈	介面的連接速度爲 10/100Mbps。



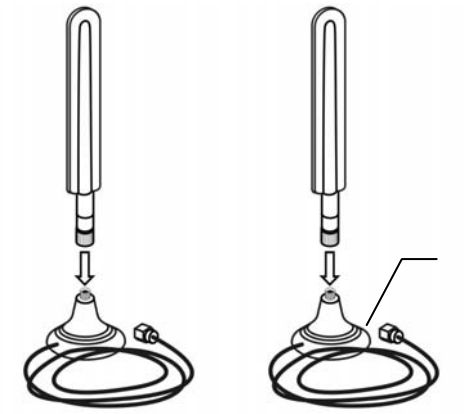


介面	說明
Wireless LAN ON/OFF/WPS	無線頻寬切換/變更，依照按鈕的按壓方式而定，例如， ● 2.4G (啓用) and 5G (啓用) – 預設值 ● 2.4G (停用) and 5G (啓用) – 壓下並放開，一次 ● 2.4G (啓用) and 5G (停用) – 壓下並放開，二次 ● 2.4G (停用)and 5G (停用) – 壓下並放開，三次 若使用者介面已經啓用 WPS 功能，則按住 WPS 按鈕 2 分鐘等待用戶裝置透過 WPS 執行網路連線，當燈號亮起時，即表示 WPS 連線成功。
Factory Reset(出廠預設值按鈕)	還原成出廠預設值。 使用方法：開啓路由器（ACT LED 閃動）。用圓珠筆按下小孔內的按鈕，然後維持 5 秒左右。當您發現 ACT LED 快速閃動時，請鬆開按鈕。路由器隨後將重新啓動，並回復出廠預設值。
USB1~USB2	連接到電腦或網路設備。
LAN1~LAN5	連接到 ADSL 或是 Cable Modem 裝置。
WAN1~WAN2	連接到 USB 3G/4G 數據機、印表機或是環境溫度計。
Phone 1/2	連接類比電話機，以便使用 VoIP 通話功能。
Line	連接 PSTN 線路。
PWR	連接電源變壓器。
ON/OFF	電源開關。

埠口 “P5 / WAN2” 是可切換的，依照網頁設定介面的設定資訊，此埠口可以用於 LAN 連線或是 WAN 連線。

I-1-2 天線安裝注意事項(“L” 系列機種)

在連接天線與路由器之前，磁性天線必須先安裝在天線底座上。



在 Vigor 路由器上，有二個安裝孔洞，用以安裝天線底座。



如果只要安裝一根天線，請使用靠近 SIM 卡插槽端的安裝孔(這是主要訊號傳輸孔)。

安裝 SIM 卡進入插槽時，請注意先移除 SIM 卡插槽背版，卡片上的缺口請依照指示方向進行安裝。



Vigor2926Ln/Vigor2926Lac 有二種類型的天線，請務必小心謹慎以期正確安裝，錯誤的安裝可能會造成無線連線訊號不良，因此安裝時請參考下圖。

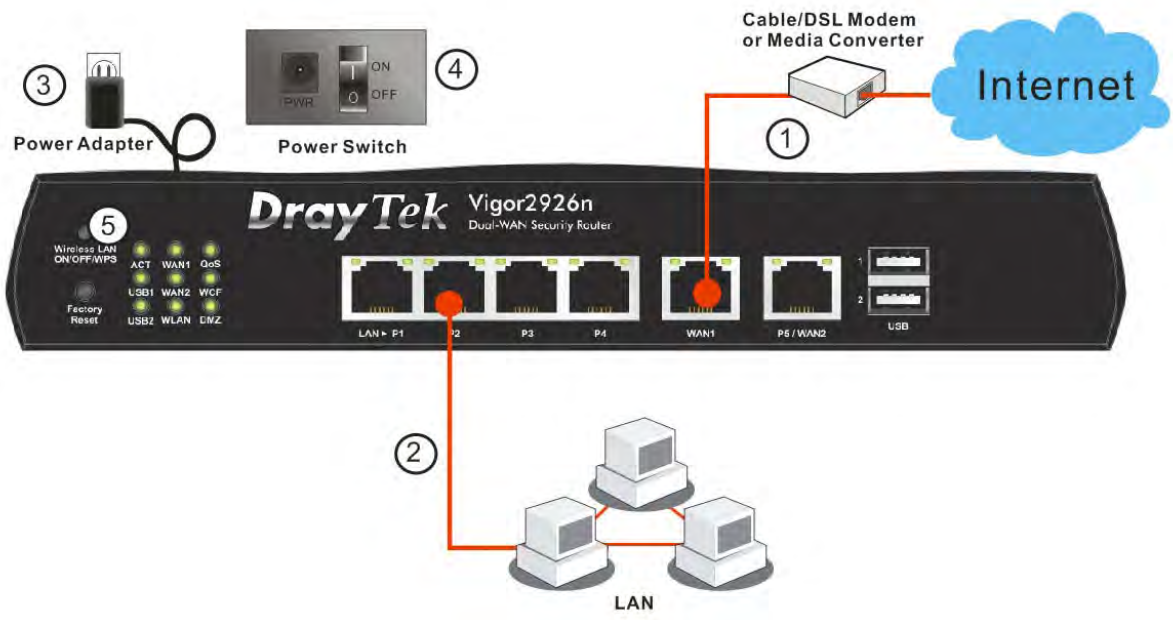


I-2 硬體安裝

I-2-1 安裝 Vigor 路由器

本節引導您透過硬體連線安裝路由器。舉 Vigor2926n 爲例。

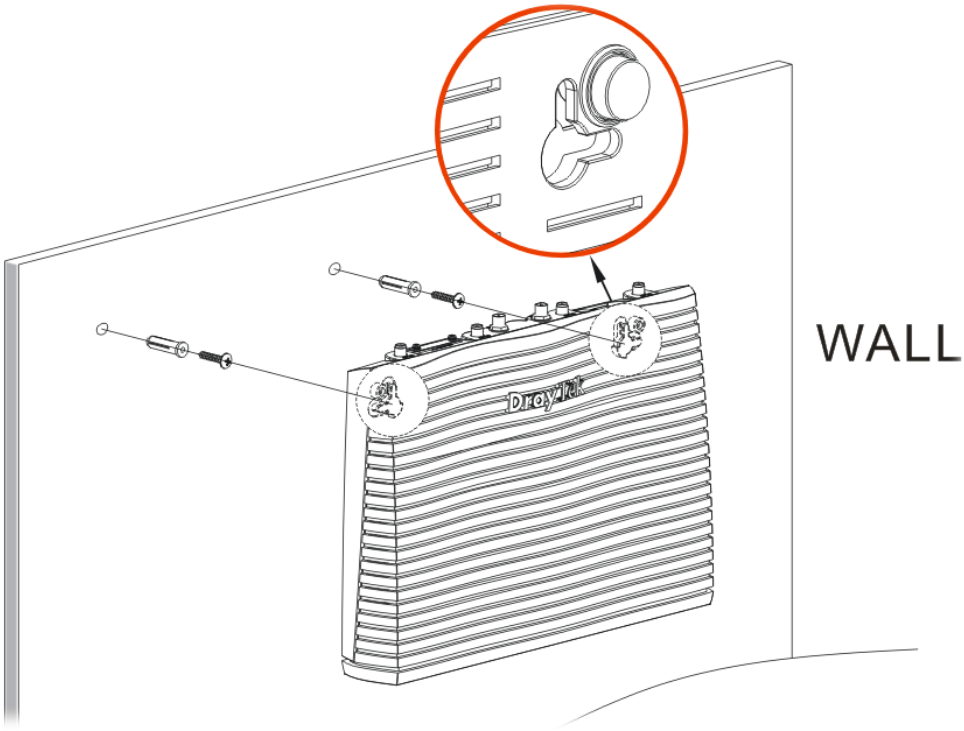
1. 利用乙太網路纜線(RJ-45)連接纜線數據機/DSL 數據機/媒體轉換器至路由器的 WAN 埠口。
2. 利用 RJ-45 纜線連接路由器(LAN 連接埠中選定其中一個)與您的電腦。
3. 將電源轉換器一端連接至路由器，另一端則連至牆上電源輸出孔。
4. 開啓路由器電源。
5. 系統開始初始化，完成測試後，檢查 **ACT** 與 **LAN** 燈號是否亮燈以確保連線無誤。



I-2-2 壁掛安裝

Vigor 路由器的背面有鎖孔式的安裝插槽，方便壁掛安裝使用。

1. 路由器包裝盒內可見一張示意圖，可讓您將螺絲正確鎖入牆面。
2. 將示意圖放在牆壁上，依照上面的指示說明鑽鑿孔洞。
3. 用適當類型的螺絲套管將螺絲鎖進牆壁。

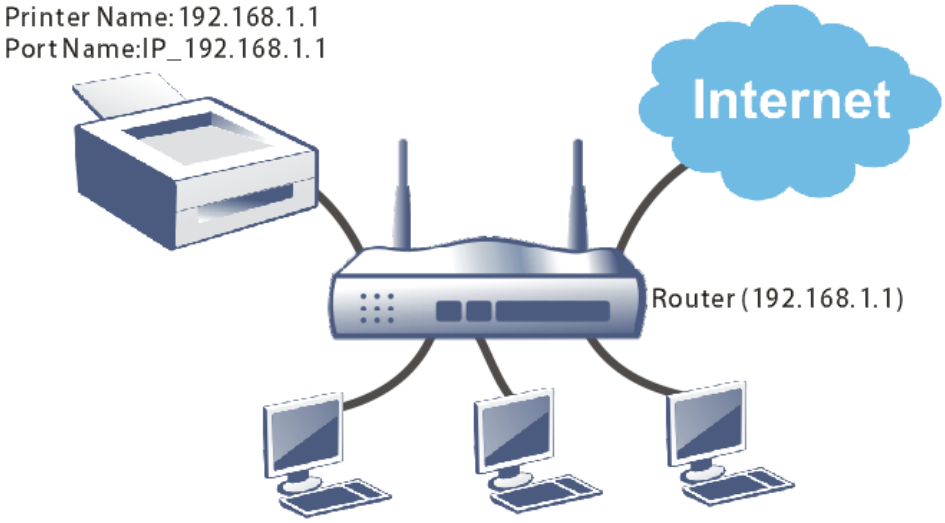


附註 建議的孔洞尺寸爲 6.5釐米(1/4吋)。

4. 完成上述步驟後，路由器及可穩妥安置在牆壁上。

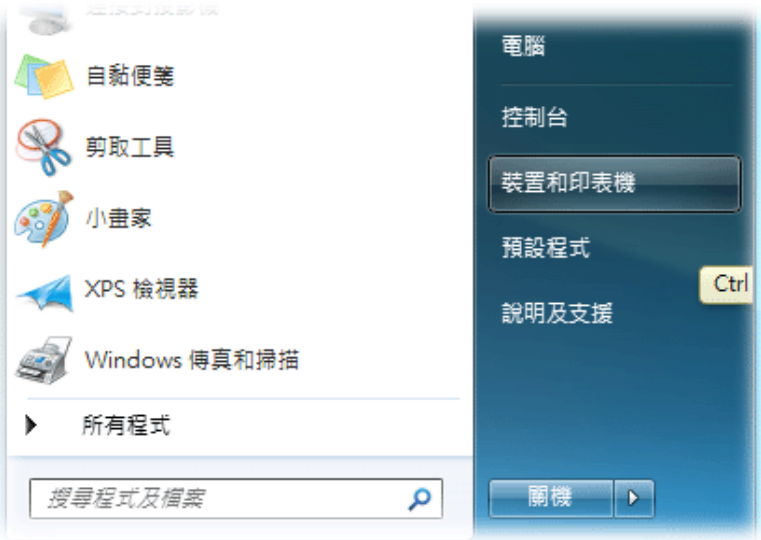
I-2-3 安裝 USB 印表機至 Vigor 路由器

您可以在路由器上連接印表機來分享列印功能，這樣路由器的區域網路上所有的電腦都可透過它列印檔，以下設定範例是以 Windows 7 爲主。

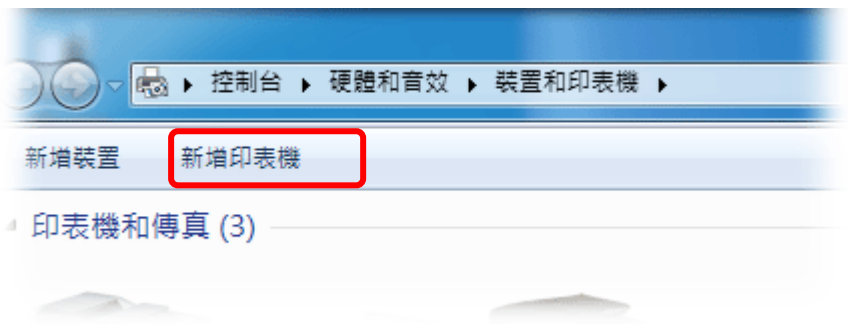


使用之前，請務必按照下列步驟來設定您的電腦（或無線用戶）：

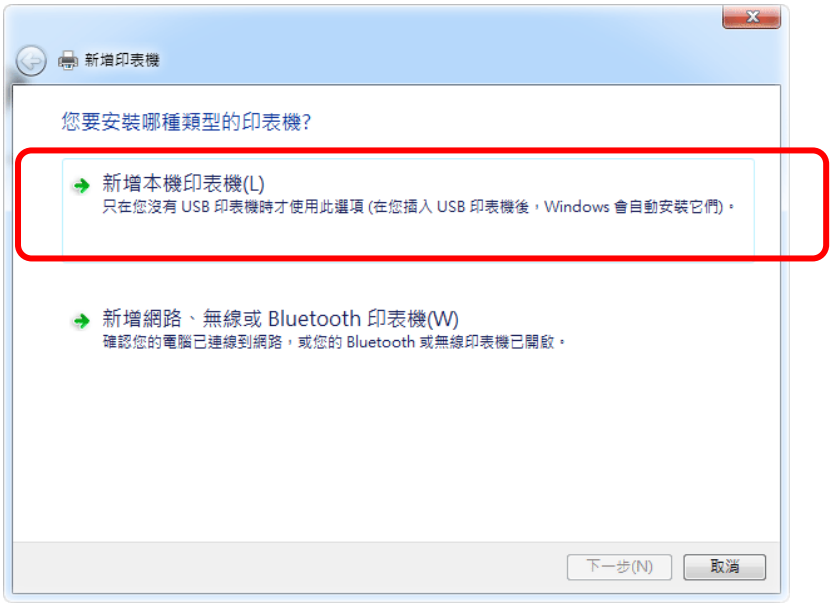
1. 請透過 USB 連接埠連接印表機與路由器。
2. 開啓**開始>>所有程式>>裝置和印表機**。



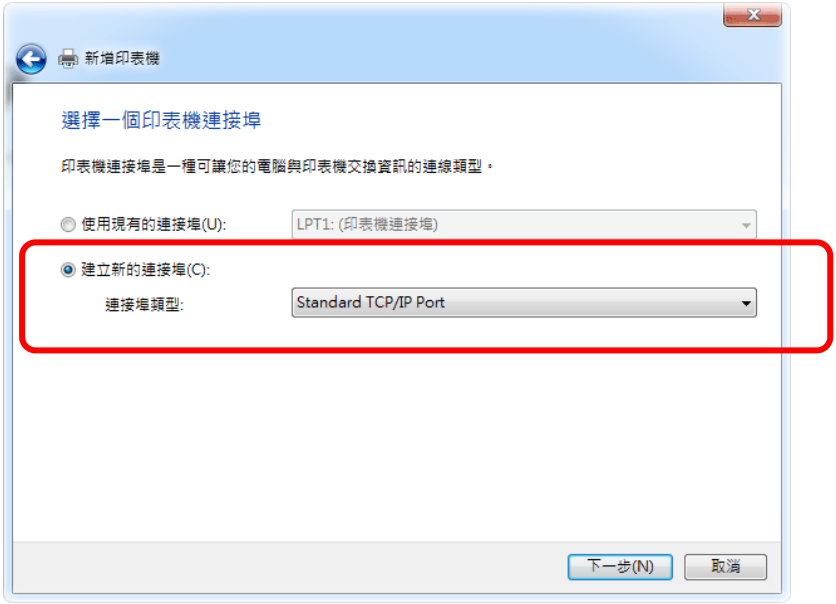
3. 按下**新增印表機**。



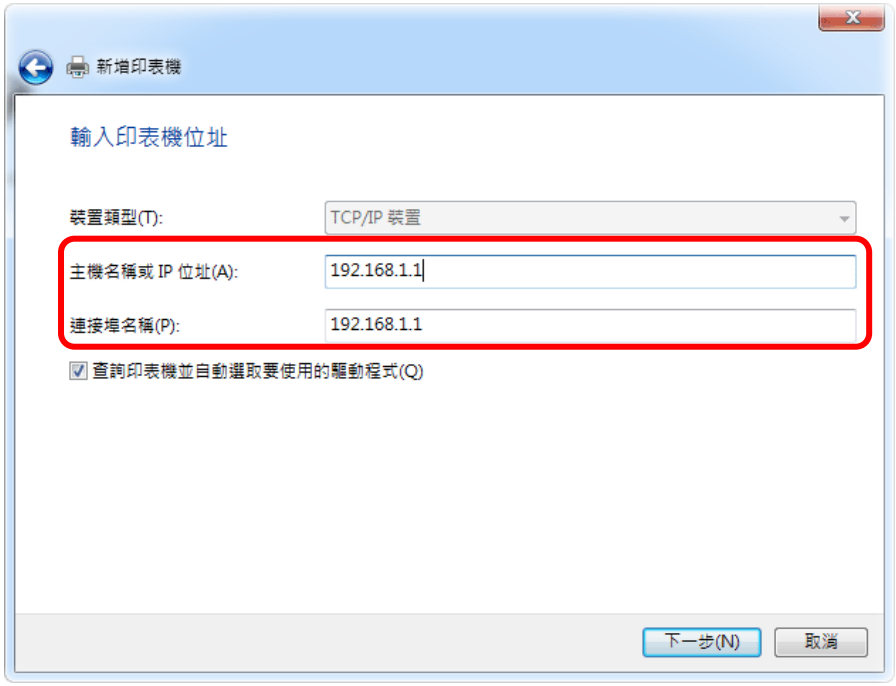
4. 選擇“**新增本機印表機.**”並按**下一步**。



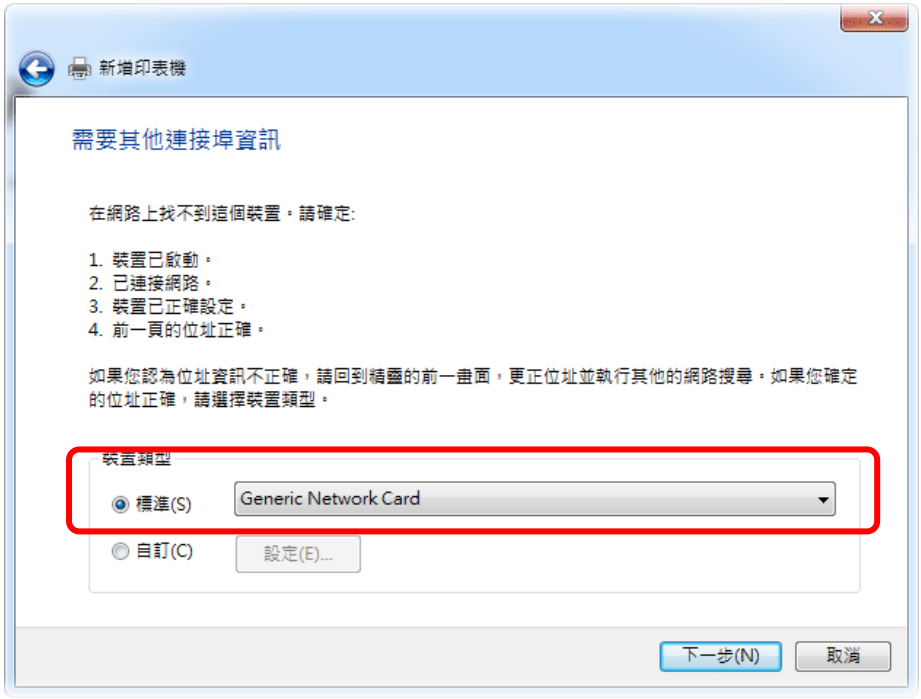
5. 接著請選擇“**建立新的連接埠**”，用下拉式選項選擇“**Standard TCP/IP Port**”，按**下一步**。



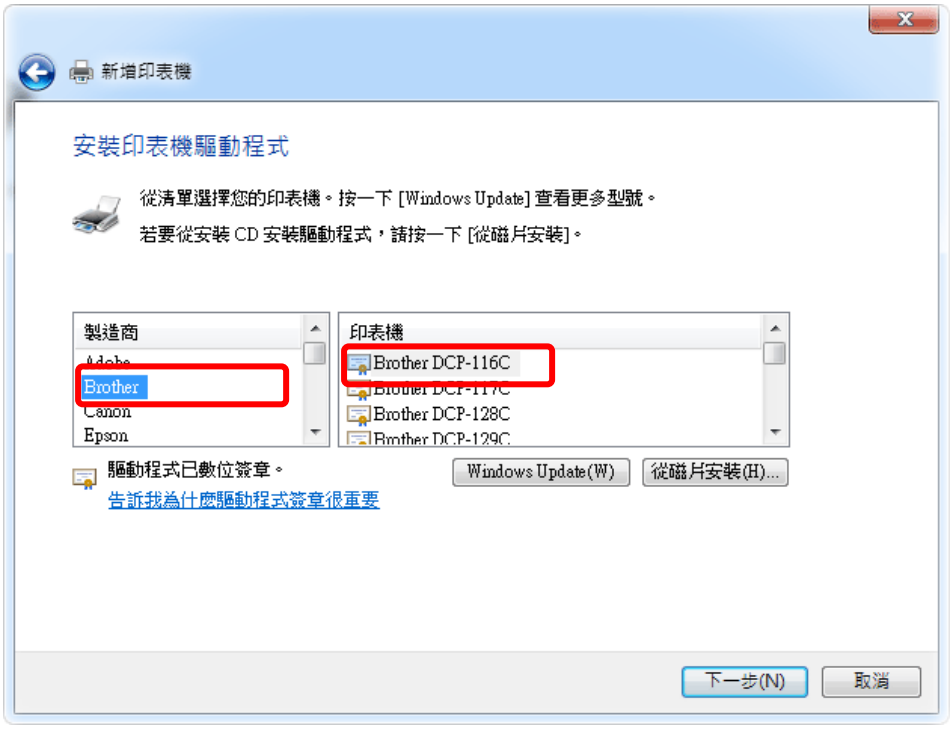
6. 在下面的對話方塊中，請在主機名稱或 IP 位址欄位輸入 **192.168.1.1** (路由器的 LAN IP)，再按**下一步**。請輸入 **192.168.1.1** (路由器的 LAN IP)，**IP_192.168.1.1** 會自動帶出，再按**下一步**。



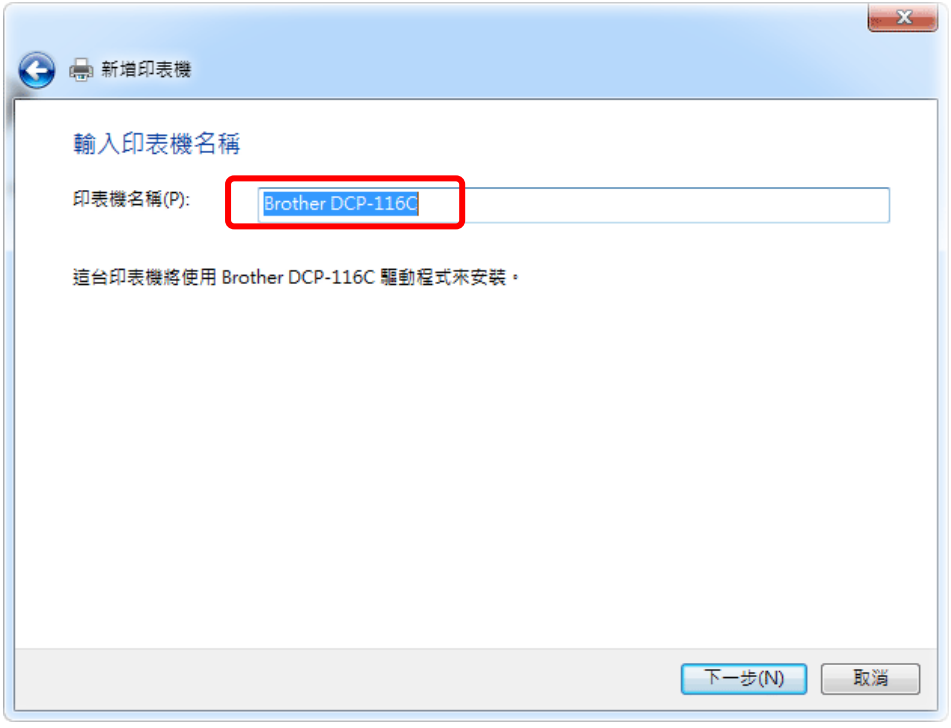
7. 請選擇**標準**，並自下拉式選項中選取 **Generic Network Card**，再按**下一步**。



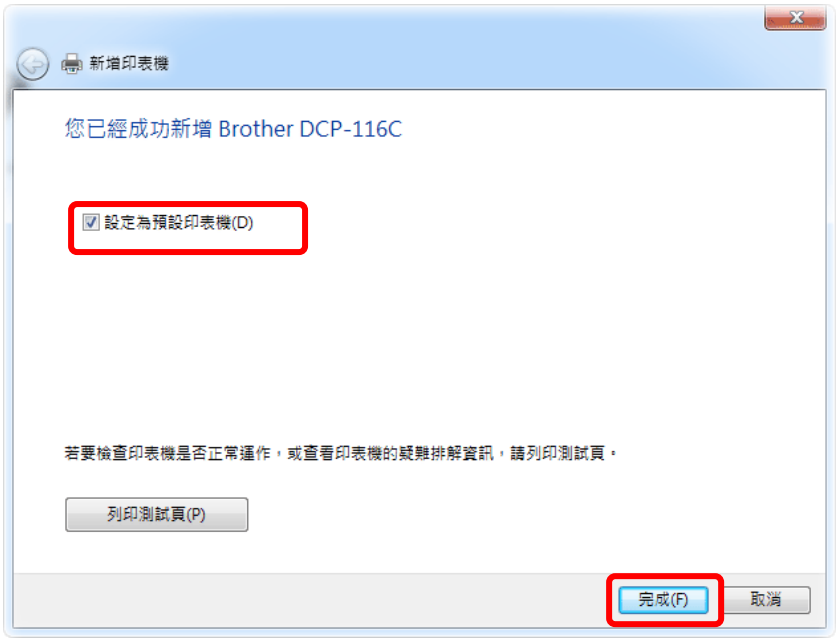
8. 現在系統將會要求您選擇您安裝至路由器上的印表機名稱，這個步驟可以讓您的電腦安裝正確的驅動程式，當您完成項目選擇之後，請按**下一步**。



9. 輸入印表機名稱，繼續按**下一步**。



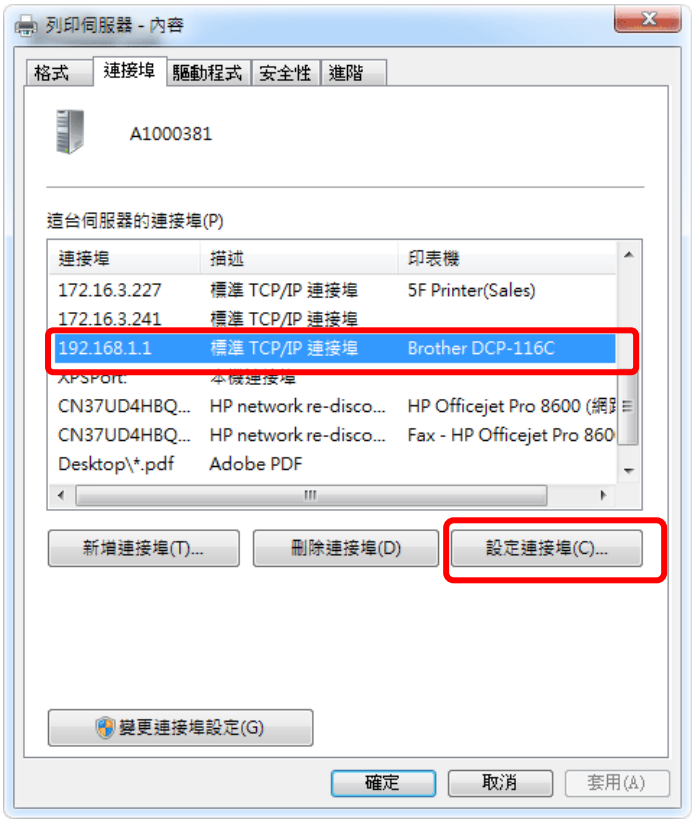
10. 在如下的對話盒，請按**完成**。



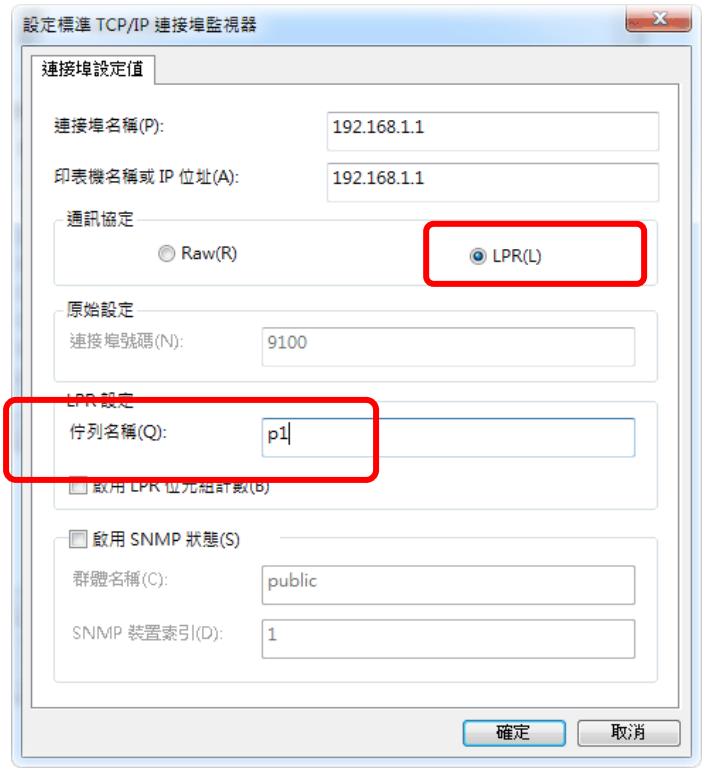
11. 新的印表機圖示已出現在**印表機和傳真**區域中，請按新圖示然後再按下**列印伺服器內容**標籤。



12. 如下頁面出現後，請按**設定連接埠**，編輯新增印表機的內容。



13. 在通訊協定欄位中，選擇"**LPR**"，佇列名稱則請輸入"p1"，按下**確定**鈕。



14. 您現在可以使用新增的印表機了，大多數的印表機都與 Vigor 路由器相容。

I-3 進入設定網頁

1. 確保您的電腦已經和路由器正確的連接。

   您可以選擇直接設定電腦的網路設定爲動態取得 IP 位址 (DHCP)，或者是將 IP 設定爲和 IP 分享器的預設 IP 位址 (**192.168.1.1**) 於同一個子網路。如需更多訊息，請參考後面的章節 – 疑難排解。

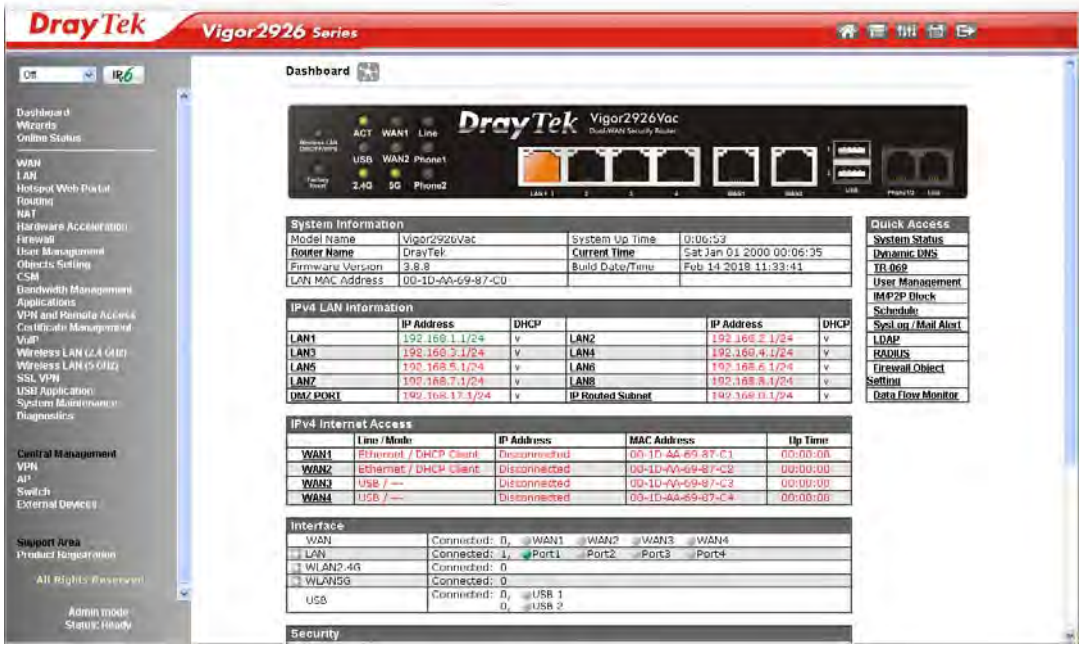
2. 開啓網頁瀏覽器並輸入位址 http://192.168.1.1，登入視窗將會出現。



3. 請輸入“admin/admin”，再按下**登入**進入路由器網頁設定畫面。

注意	如果您無法進入網頁設定畫面，請參考“疑難排解”以解決您所面臨的問題。

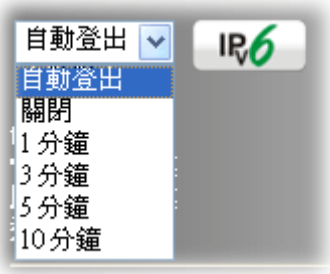
4. 現在，設定介面的主選單會出現。舉 Vigor2926ac 爲例：



注意

因爲首頁會依照您的路由器的功能做些微改變，所以設定介面不一定都會如上圖所示。

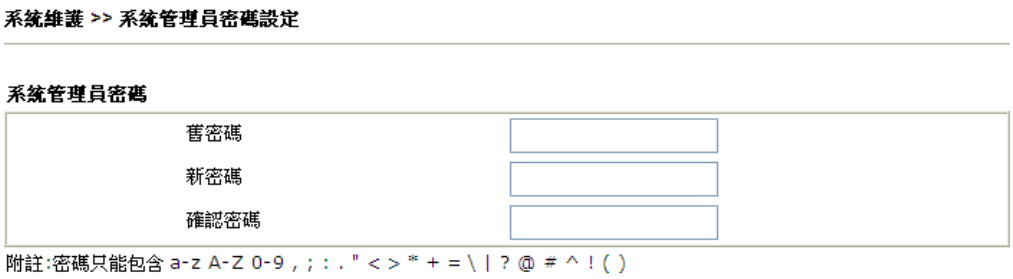
5. 網頁將會依照您所選擇的條件開啓不同的頁面，預設值通常爲自動登出，若操作者沒有進行任何動作時，網頁會在 5 分鐘後自動離開，您可以視需要改變登出的時間設定。



I-4 變更密碼

爲了路由器的安全起見，建議您將先行變更密碼。

1. 開啓網頁瀏覽器並輸入位址 http://192.168.1.1。登入視窗將會出現並要求您輸入使用者名稱與密碼。
2. 請輸入 “admin/admin”進入管理者模式。
3. 進入**系統維護(System Maintenance)**頁面並選擇**系統管理員密碼(Administrator Password)**。



4. 輸入舊密碼 (預設值爲空白)。 在**新密碼(New Password)**及**確認密碼(Confirm Password)**輸入您想要設定的密碼，然後按**確定(OK)**儲存設定。
5. 現在密碼已經變更，下次登入時請使用新設定的密碼。



注意 即使密碼已經變更，登入使用者介面的使用者名稱仍然爲“admin。

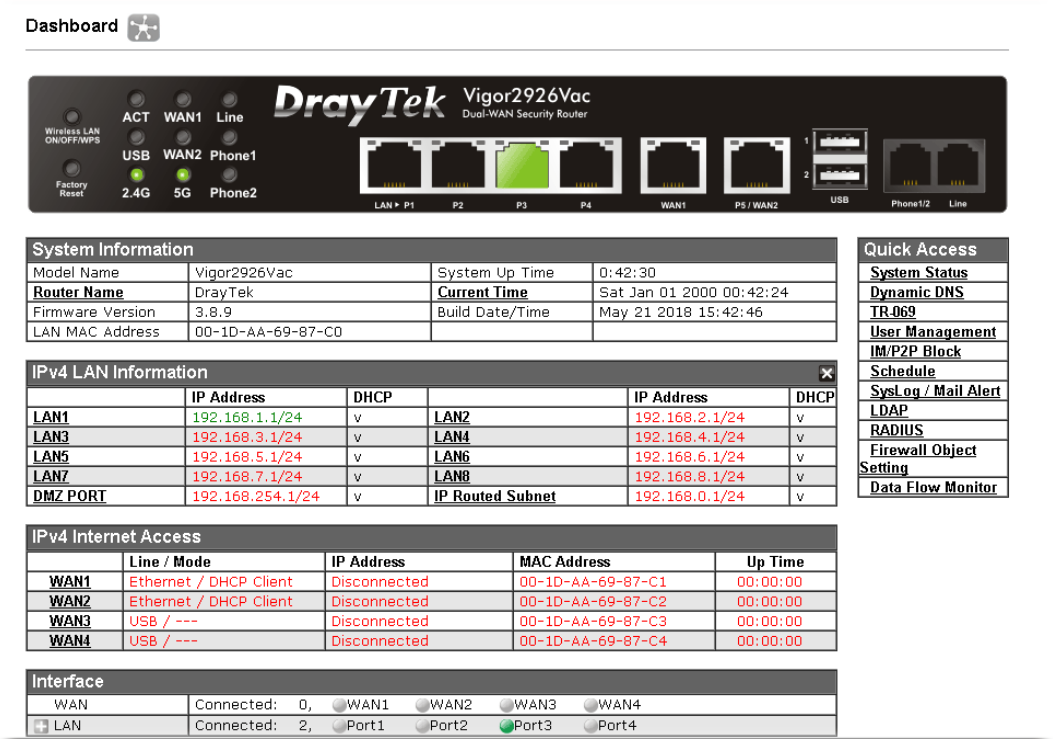
I-5 儀表板簡介

儀表板(Dashboard)顯示各種連線狀態，諸如系統資訊、IPv4 網際網路連線、IPv6 網際網路連線、介面(實體連線)、安全性設定與快速存取等等。

自左手邊的主選單上按下**儀表板(Dashboard)**功能。

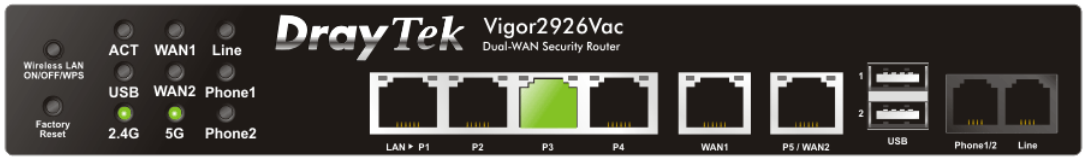


預設值網頁將會顯示在螢幕上，請參考下圖：



I-5-1 虛擬面板

在儀表板的正上方，您可以看到路由器的虛擬面板，顯示實體連線的狀態，每隔數秒，畫面會重新顯示一次。



項目	顏色顯示	說明
LED 燈號 (左邊)	黑色	表示該功能尚未運作。
	綠色	表示該功能正在運作當中。
USB	黑色	表示目前沒有連接 USB 裝置。
	綠色	表示已經連接上 USB 裝置。
乙太網路埠 (WAN/LAN)	黑色	表示該埠目前並未連接。
	綠色	表示該埠目前已經連接上路由器(傳輸速度達 Giga)。
	橘色	表示該埠目前已經連接上路由器。

有關燈號的詳細說明，請參考 **I-1-1 LED 指示燈與介面說明**一節。

I-5-2 底線連結

任何一個名稱下方含有底線者(如路由器名稱、目前時間、WAN1/2/3 等等.)表示您可以按下該連結開啓設定頁面。

System Information

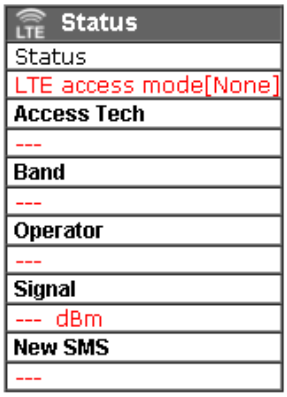
Model Name	Vigor2926Vac	System Up Time	0:42:30
Router Name	DrayTek	**Current Time**	Sat Jan 01 2000 00:42:24
Firmware Version	3.8.9	Build Date/Time	May 21 2018 15:42:46
LAN MAC Address	00-1D-AA-69-87-C0		

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

I-5-3 LTE 狀態

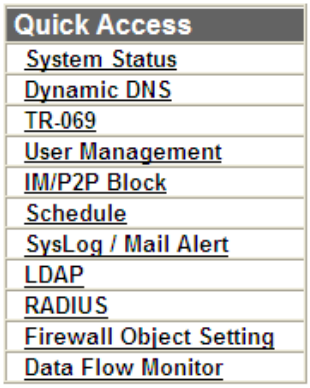
顯示 LTE 機種目前的狀態，包含使用的連線模式、採用的連線技術、頻寬運用、操作者、訊號強度以及接收到的新簡訊通知等等。



I-5-4 常用功能的快速存取

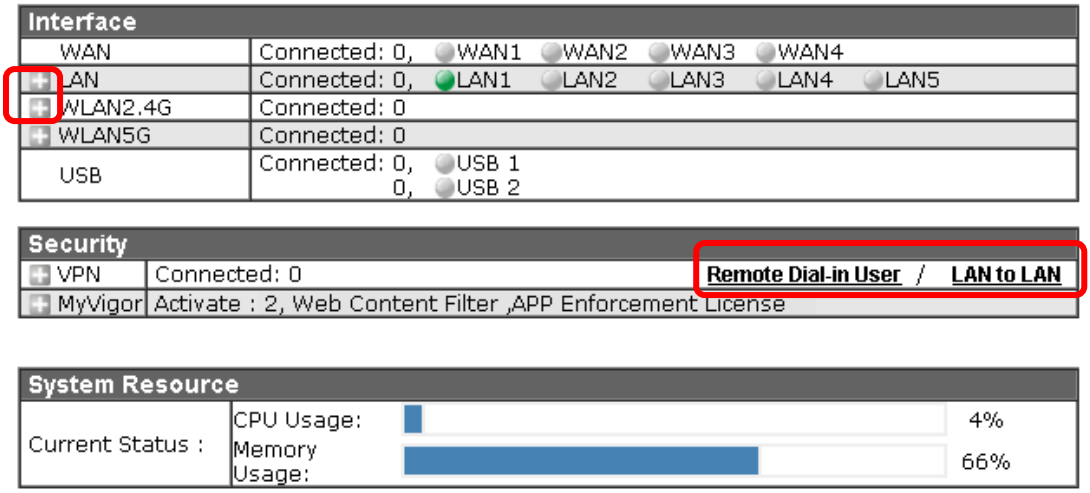
所有的項目都可以依照您的需要從左邊的主要功能區存取，不過針對一些較重要或是常用的項目，系統提供一個更爲方便快速快速的方式來開啓。

請移動前往儀表板的右邊，您可以**在快速存取(Quick Access)**一區中看到常用功能群。

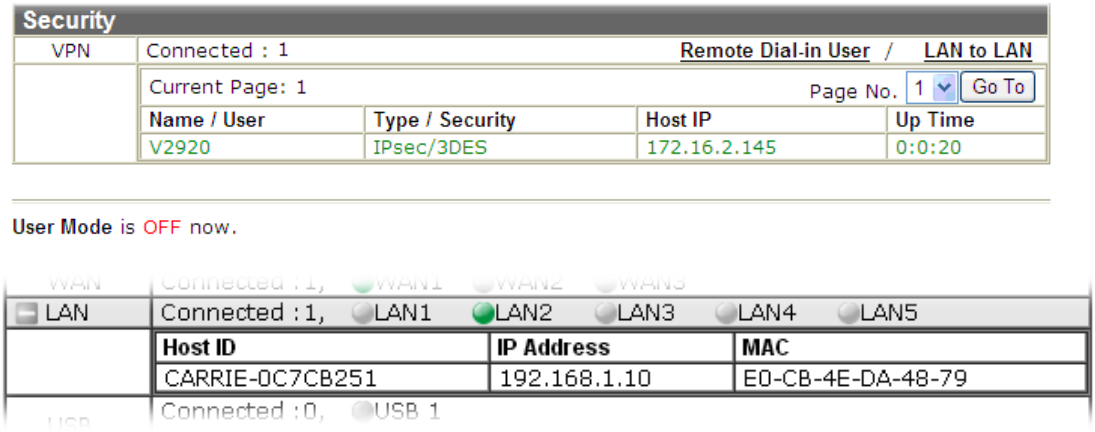


本區將系統狀態、動態 DNS、TR-069、使用者管理、IM/P2P 封鎖、排程、Syslog/郵件警示、LDAP、RADIUS、防火牆物件設定以及資料流量監控等常用連結歸納於此，移動您的滑鼠至任何一個連結在輕輕按下，相應頁面即可立刻開啓。

此外，VPN 安全設定的快速存取連結像是**遠端撥入使用者(Remote Dial-in User)**以及 **LAN to LAN** 位於本頁的底端，請利用滑鼠在此頁面向下捲動即可見到相關內容。



請注意在 LAN/WLAN/VPN/MyVigor 的左邊有加號( ) 圖示，請按下該圖示檢視目前 LAN/WLAN/VPN/MyVigor 狀態。



透過 LAN 埠口實體連接至路由器的主機會以綠色圓燈來呈現，表示目前該埠口是連接的。

所有列出主機 ID、IP 位址以及 MAC 位址的主機(包含無線用戶端)表示資料傳輸乃透過該 LAN 端及 WAN 端進出。這些清楚的標示目的在進行主機的流量監控作業。

I-5-5 圖形介面地圖(GUI Map)



路由器支援的全部功能可在此頁面下全部呈現出來，使用者可以按此功能連結進入相關頁面進行細部設定。機種不同，呈現的圖形介面地圖也會有所差異。

GUI Map

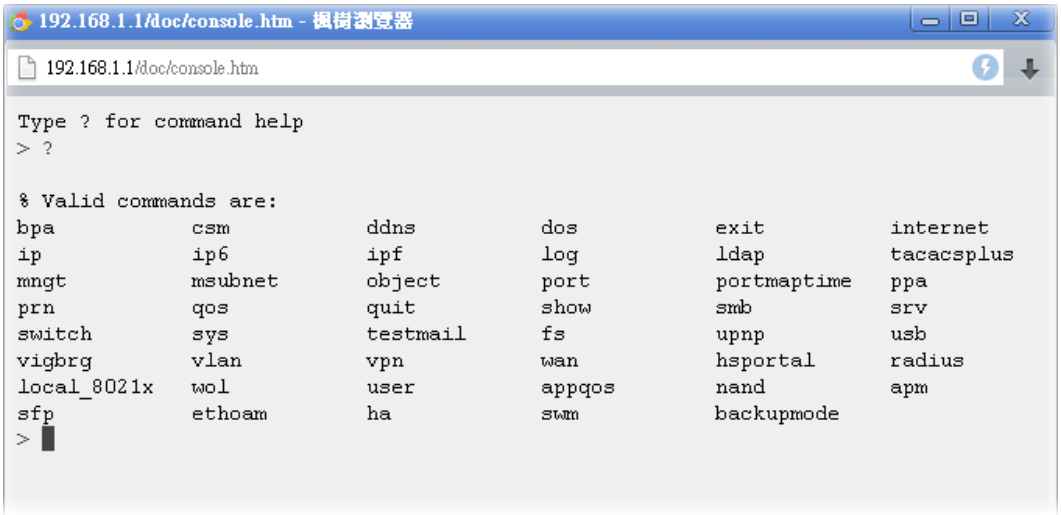
Dashboard		**Certificate Management**	
Wizards			Local Certificate
	Quick Start Wizard		Trusted CA Certificate
	Service Activation Wizard		Certificate Backup
	VPN Client Wizard	**VoIP**	
	VPN Server Wizard		General Settings
	Wireless Wizard	**Wireless LAN(2.4GHz)**	
	VoIP Wizard		General Setup
Online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

I-5-6 網頁操作台(Web Console)



透過這個功能可不必透過 DOS 提示頁面使用 Telnet 指令。使用網頁操作台所做的任何變更與透過網頁使用者介面所進行的改變是相同的。在此操作台下所玩的功能/設定修正可以同時在網頁使用者介面中呈現。

請按主頁面上方的 **Web Console** 圖示即可開啓如下視窗。

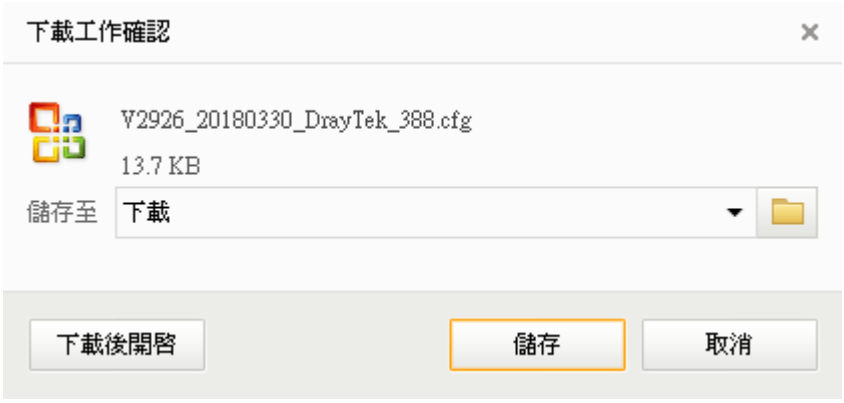


I-5-7 設定備份(Config Backup)



快速儲存目前使用中的設定可以透過設定備份(**Config Backup**)圖示來完成，將目前的設定儲存爲檔案，這個檔案後續還能利用**系統維護>>設定備份(System Maintenance>>Configuration Backup)**來還原。

請按主頁面上方的 **Config Backup** 圖示即可開啓如下視窗。



按下**儲存(Save)**將設定儲存起來。

I-5-8 登出



登出按鈕即可離開此使用者設定介面。

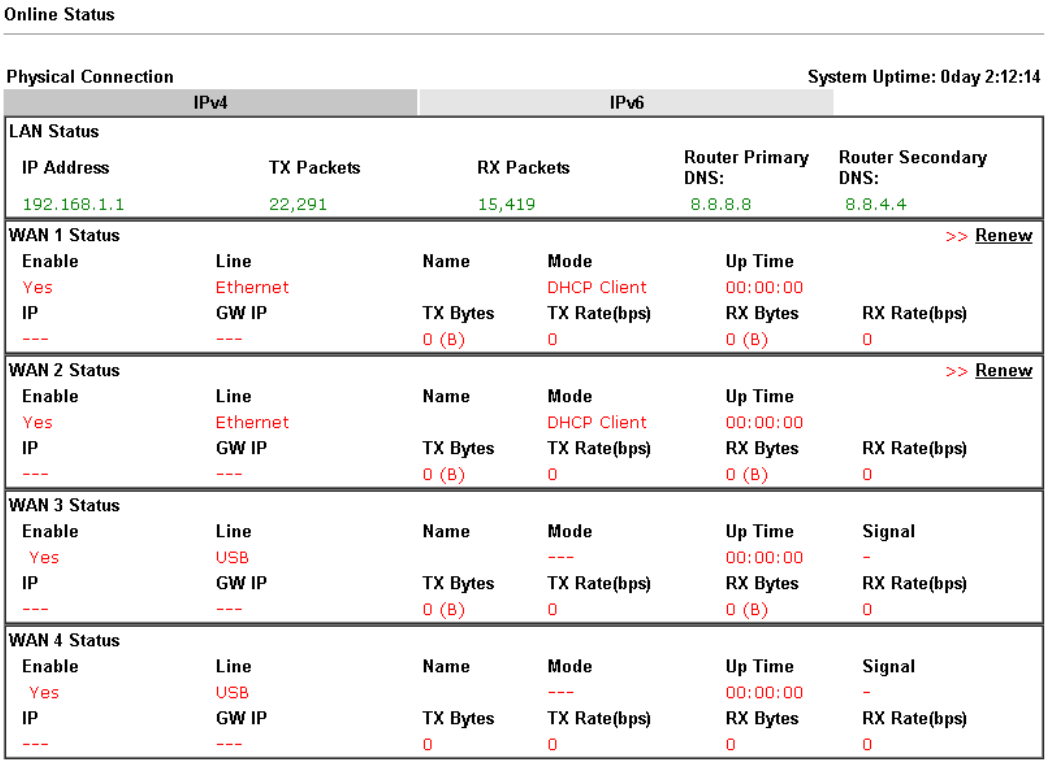
I-5-9 連線狀態



I-5-9-1 實體連線

本頁顯示實體連線狀態，諸如 LAN 連線狀態、WAN 連線狀態、ADSL 連線狀態等等。

IPv4 協定的實體連線



Online Status

Physical Connection — System Uptime: 0day 2:12:14

IPv4 | IPv6

LAN Status

IP Address	TX Packets	RX Packets	Router Primary DNS:	Router Secondary DNS:
192.168.1.1	22,291	15,419	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

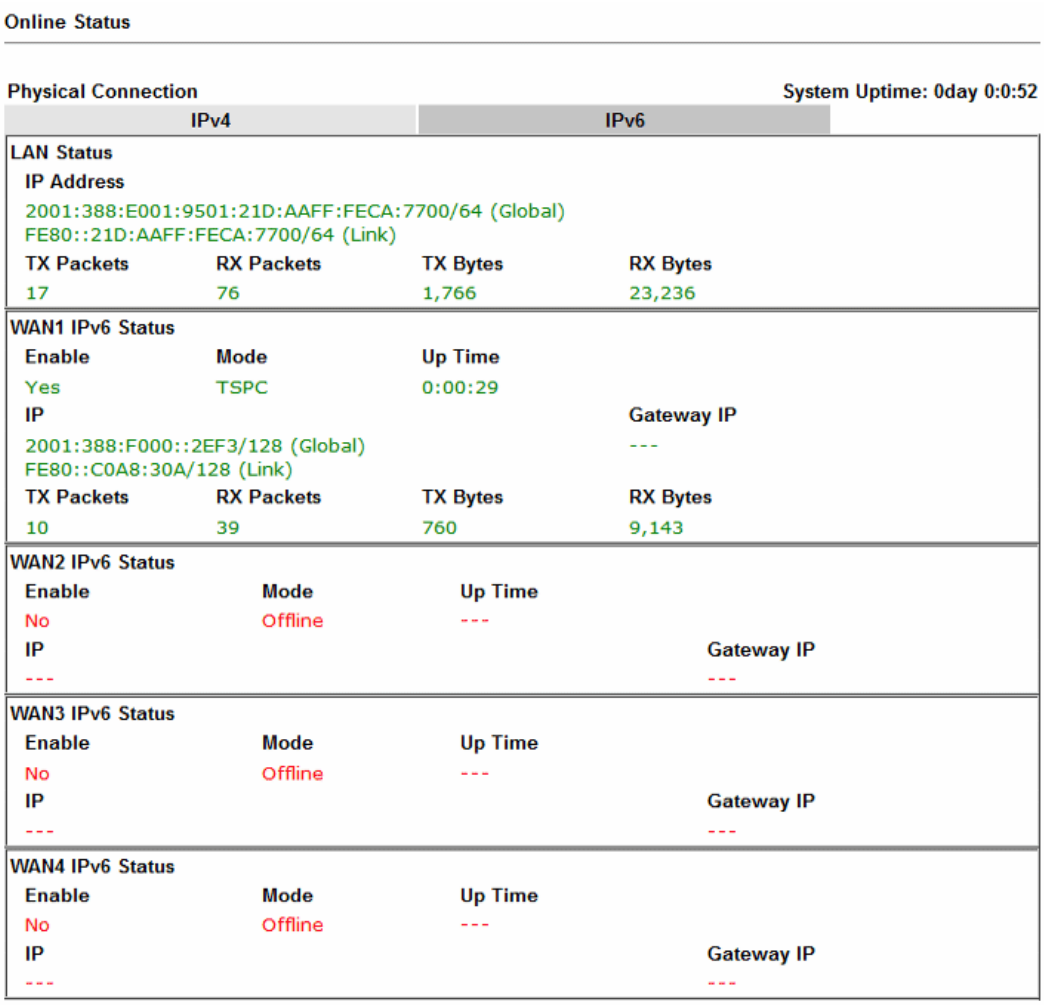
WAN 3 Status

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

WAN 4 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

IPv6 協定的實體連線



詳細說明於後(IPv4):

項目	說明
LAN 狀態	**主要 DNS** - DNS.顯示主要 DNS 的 IP 位址。 **次要 DNS** - 顯示次要 DNS 的 IP 位址。 **IP 位址**- 顯示 LAN 介面的 IP 位址。 **傳送封包** - 顯示在區域網路全部的傳送封包量。。 **接收封包**- 顯示區域路網路中全部的接收封包量。
WAN 1 狀態 ~ WAN 4 狀態	**啓用 - 是**(紅色字體) 表示此介面可以運用但尚未連接，**是**(藍色字體) 表示此介面已連接。 **線路** - 顯示此介面的實體連線類型。 **名稱** - 顯示 WAN1~WAN3 網頁上所顯示的名稱。 **模式** - 顯示 WAN 連線的模式類型(例如 PPPoE)。 **上線時間** - 顯示介面上全部的上傳時間。 **IP** - 顯示 WAN 介面的 IP 位址。 **閘道 IP** - 顯示預設閘道的 IP 位址。 **傳送位元** - 顯示 WAN 介面上全部傳送的封包數。 **傳送速率** - 顯示 WAN 介面上全部傳送速率位元數。

項目	說明
	接收位元 - 顯示 WAN 介面上全部接收的封包數。 **接收速率** - 顯示 WAN 介面上全部接收速率位元數。

詳細說明於後(IPv6):

項目	說明
LAN 狀態	**IP 位址 -** 顯示 WAN 介面上的 IPv6 位址。 **傳送封包** - 顯示在區域網路中全部的傳送封包量。 **接收封包 -** 顯示區域路網路中全部的接收封包量 **傳送位元** - 顯示區域網路上全部傳送的位元數。 **接收位元** - 顯示區域網路上全部接收的位元數。
WAN IPv6 狀態	**啓用 - 是**(紅色字體) 表示此介面可以運用但尚未連接，**是**(藍色字體) 表示此介面已連接。 **模式** - 顯示 WAN 連線的模式類型(例如 TSPC)。 **上線時間** - 顯示介面上全部的上傳時間。 **IP** - 顯示 WAN 介面的 IP 位址。 **閘道 IP** - 顯示預設閘道的 IP 位址。

注意

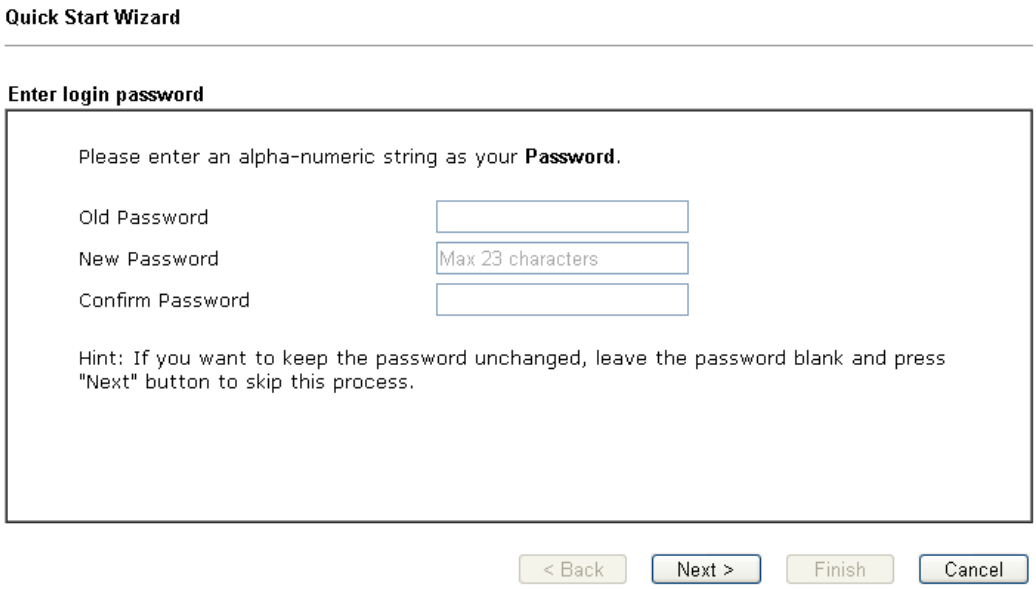
綠色字樣表示該WAN連接已預備妥當，隨時可以存取網際網路資料，紅色字樣則表示該WAN連接尚未預備妥當，也還無法透過路由器存取網際網路資料。

I-5-9-2 虛擬 WAN

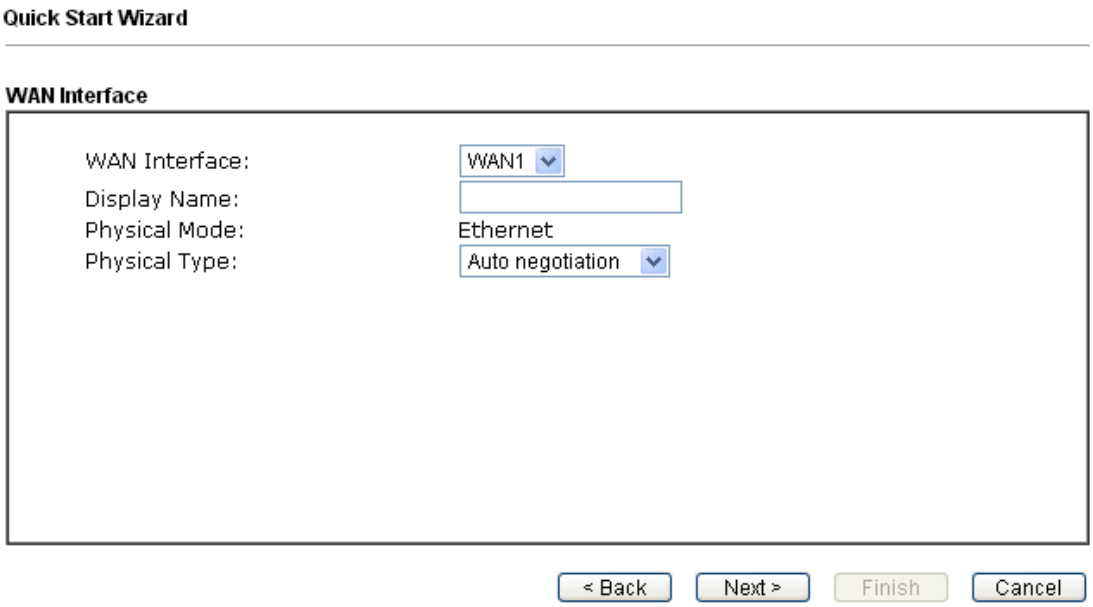
本頁顯示虛擬 WAN 介面的資訊，虛擬 WAN 用於 TR-069 管理、VoIP 服務等方面，應用一欄可顯示此 WAN 連線的目地。

I-6 快速設定精靈(Quick Start Wizard)

您可以依照下列的步驟**使用快速設定精靈(Quick Start Wizard)**設定您的路由器。快速設定精靈的第一個畫面會要求您輸入密碼，輸入密碼之後，請按**下一步(Next)**。



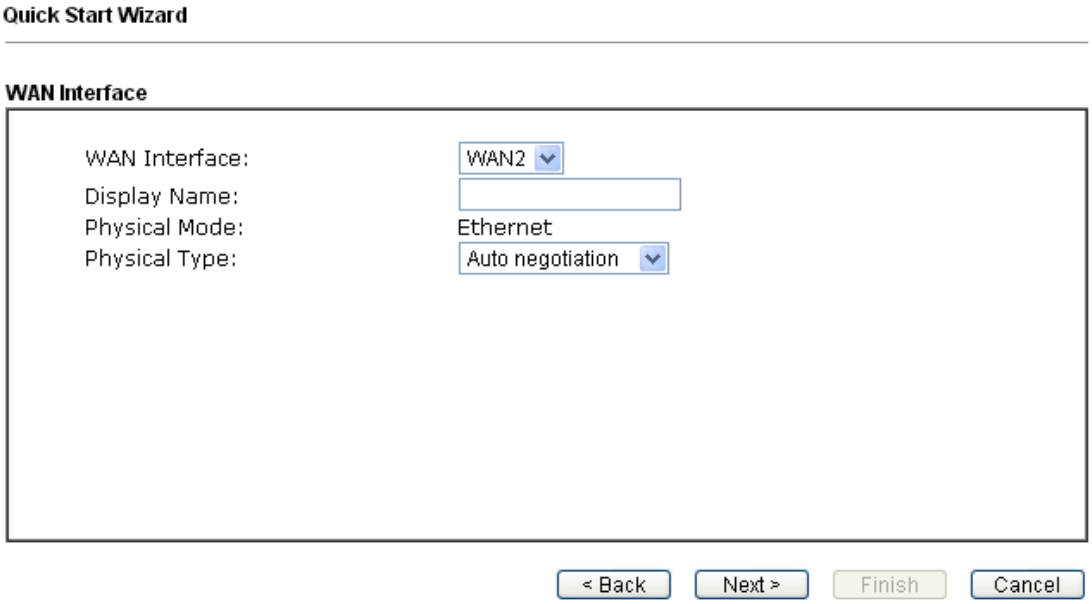
在下述頁面，請選擇使用的 WAN 介面，如果使用的是乙太網路介面，請選擇 WAN1/WAN2(以硬體連線爲基準)，若使用的是 3G/4G USB 數據機，請選擇 WAN3/WAN4。並選擇**自動偵測(Auto negotiation)** 作爲路由器的傳送資料模式，然後按**下一步(Next)**。



WAN1/WAN2 與 WAN3/WAN4 帶來的設定頁面所不同，請參考下述細部說明。

I-6-1 對於 WAN1/WAN2 介面(乙太網路)

WAN1/WAN2 專用於乙太網路的實體連線模式，如果您選擇 WAN1/WAN2，請先指定傳送資料模式，然後按**下一步(Next)**。

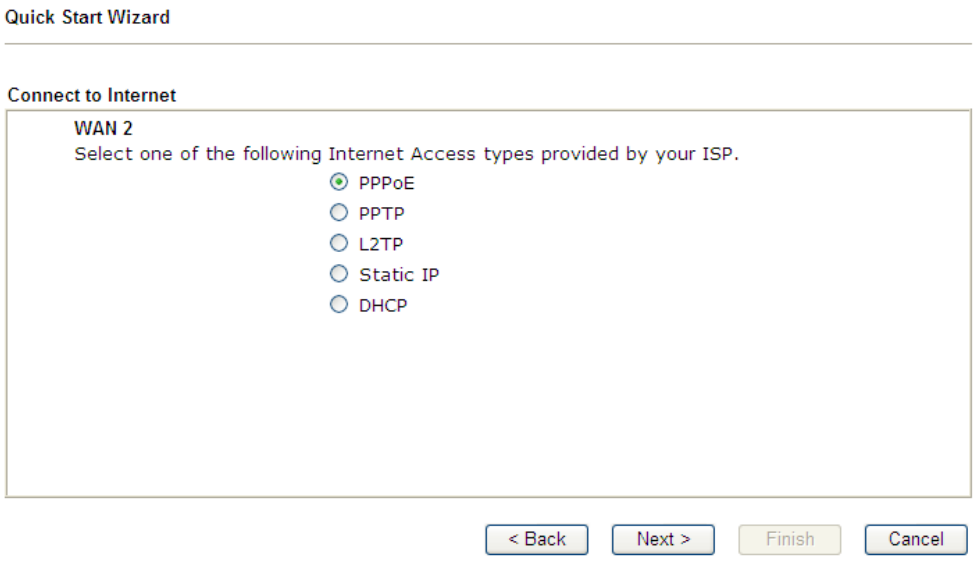


請依照 ISP 業者提供給您的資訊選擇適當的網際網路連線類型，舉例來說，如果 ISP 提供給您的是 PPPoE 介面，您應該選擇 PPPoE 模式，然後按**下一步(Next)**繼續進行。

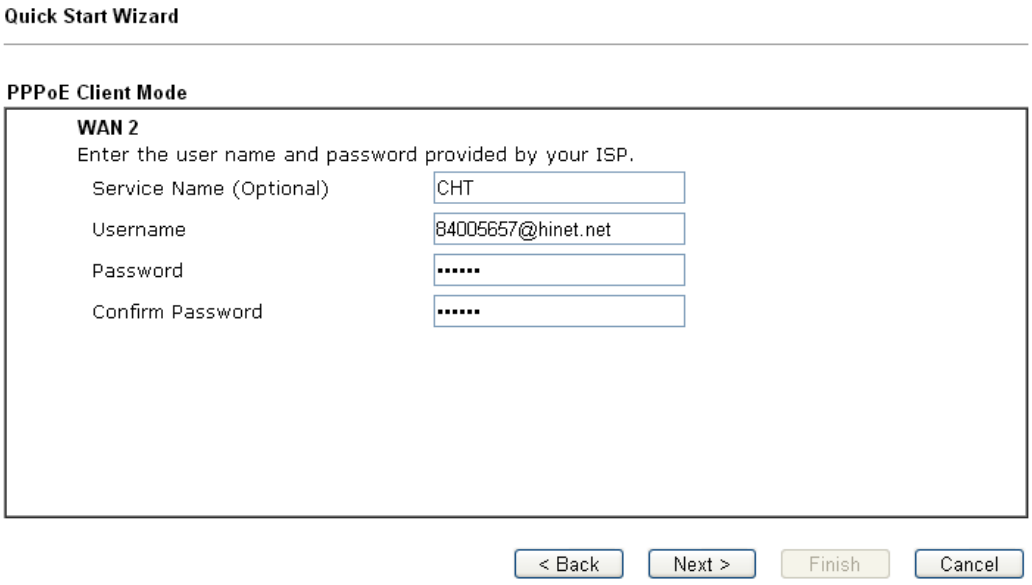
PPPoE

PPPoE 爲 Point-to-Point Protocol over Ethernet 的縮寫，是一種利用個人電腦透過寬頻連接設備(如 xDSL、Cable、Wireless)連接至高速寬頻網路的技術，用戶僅需在個人的電腦上加裝乙太網路卡，然後向電信線路提供者(如：中華電信)與網際網路服務提供者(ISP，如：亞太線上)申請 ADSL 服務，就可以以類似傳統撥接的方式，透過一般的電話線連上網際網路。另外，PPPoE 也同時被用來在 ADSL 網路架構上進行用戶認證、紀錄用戶連線時間，以及取得動態 IP。

1. 選擇 **WAN1/WAN2** 作爲 WAN 介面，按**下一步(Next)**按鈕後，下圖將會出現讓您指定網際網路連線類型。



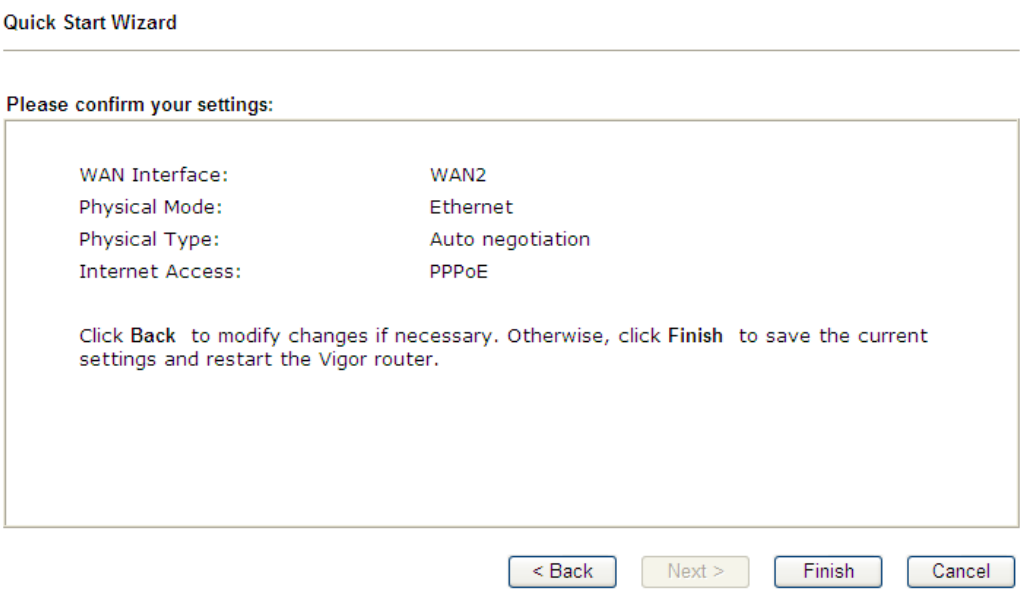
2. 選擇 **PPPoE** 然後按**下一步(Next)**開啓如下頁面。



可用設定說明如下：

項目	說明
服務名稱(Service Name) (選填)	輸入特定網路服務的說明。
使用者名稱 (Username)	指定 ISP 提供之有效使用者名稱。
密碼(Password)	指定 ISP 提供之有效密碼。
確認密碼(Confirm Password)	重新輸入密碼以確認。
上一步(Back)	按此鈕回到上一頁面。
下一步(Next)	按此鈕進入下一頁面。
取消(Cancel)	按此鈕放棄快速設定精靈。

3. 請依照您的 ISP 業者提供的資料輸入使用者名稱與密碼。按**下一步**檢視連線的設定狀態。



4. 按完成，快速設定精靈安裝完畢頁面將會出現。

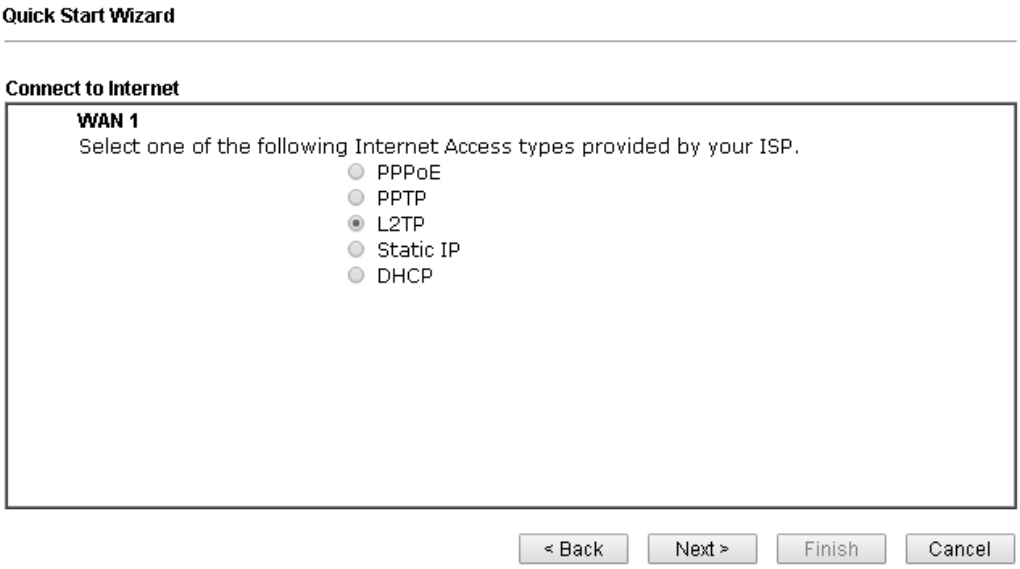
Quick Start Wizard Setup OK!

5. 現在您可以遨遊網際網路了。

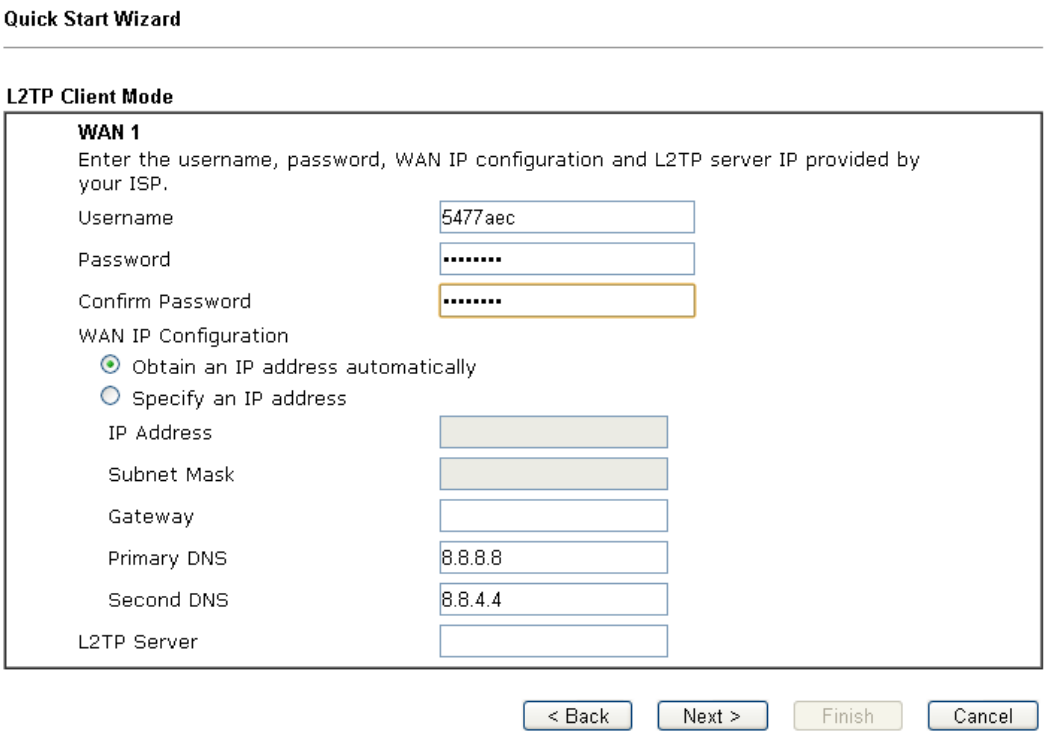
PPTP/L2TP

PPTP 則是 Point-to-Point Tunneling Protocol 的簡稱。有些 DSL 服務提供者採用一種特別的 DSL 數據機(例如：阿爾卡特的 DSL 數據機)。這種數據機只支援 PPTP Tunnel 方法存取 Internet。在這種情形下，您建立一個到 DSL 數據機並且帶有 PPP Session 的 PPTP Tunnel。一但 Tunnel 建立後，這種 DSL 數據機會將 PPP Session 送往 ISP。當 PPP Session 建立後，當地的使用者共用這個 PPP Session 存取 Internet。如果您需要使用 PPPTP 連線，請先在視窗中選擇適當的模式，然後輸入相關資訊。

1. 選擇 **WAN1/WAN2** 作爲 WAN 介面，按**下一步(Next)**按鈕後，下圖將會出現讓您指定網際網路連線類型。



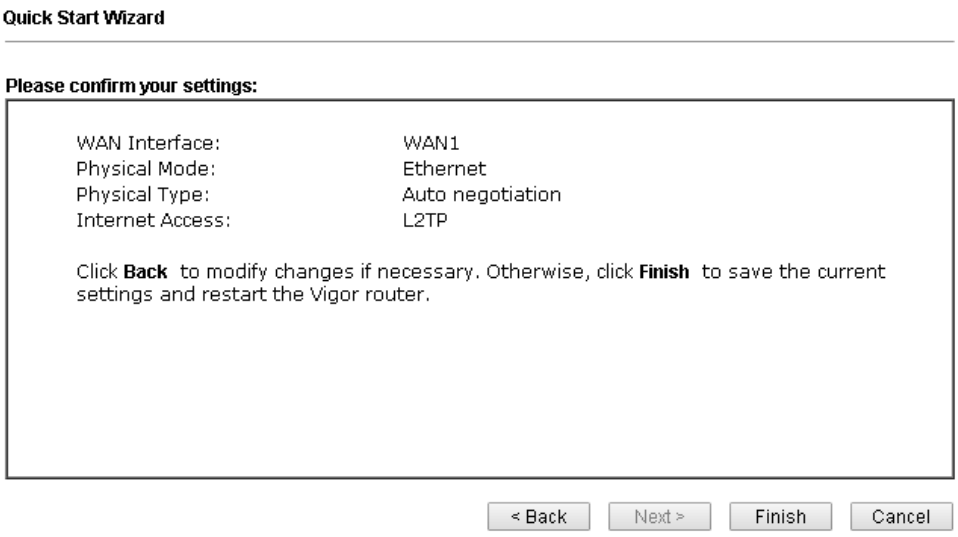
2. 選擇 **PPTP/L2TP** 然後按**下一步(Next)**開啓如下頁面。



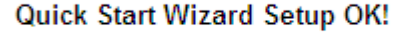
可用設定說明如下：

項目	說明
使用者名稱 (Username)	指定 ISP 提供之有效使用者名稱。
密碼(Password)	指定 ISP 提供之有效密碼。
確認密碼(Confirm Password)	重新輸入密碼以確認。
WAN IP 組態設定 (WAN IP Configuration)	**自動取得 IP 位址(Obtain an IP address automatically)**– 路由器可自 DHCP 伺服器自動取得 IP 位址。 **指定 IP 位址(Specify an IP address)** – 使用者須手動輸入相關設定。 **IP 位址(IP Address)** – 輸入 IP 位址。 **子網路遮罩(Subnet Mask)** – 輸入子網路遮罩。 **閘道(Gateway)** –輸入閘道 IP 位址。 **主要 DNS (Primary DNS)** – 輸入路由器主要的 DNS IP 位址。 **次要 DNS (Second DNS)** – 必要時輸入路由器次要的 DNS IP 位址。
PPTP 伺服器 / L2TP 伺服器 (PPTP Server / L2TP Server)	輸入伺服器的 IP 位址。
上一步(Back)	按此鈕回到上一頁面。
下一步(Next)	按此鈕進入下一頁面。
取消(Cancel)	按此鈕放棄快速設定精靈。

3. 請依照您的 ISP 業者提供的資料輸入相關資訊。按**下一步(Next)**檢視連線的設定狀態。



4. 按完成，快速設定精靈安裝完畢頁面將會出現。

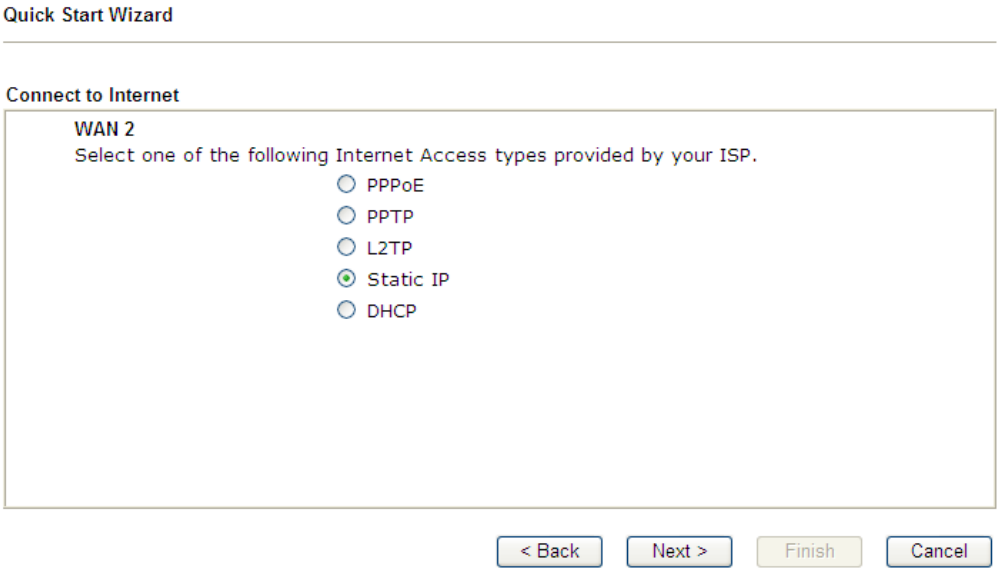


5. 現在您可以遨遊網際網路了。

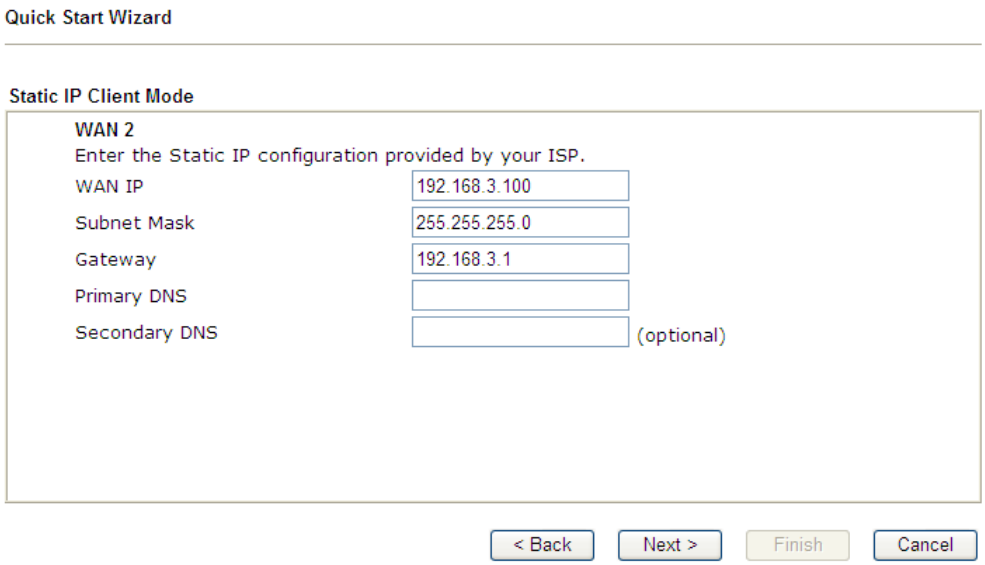
固定 IP

在這種應用當中，您會從 ISP 取得一個固定真實 IP 位址或一個真實子網路(多個公開 IP 位址)。通常纜線(Cable) ISP 會提供一個固定的真實 IP，而 DSL ISP 則有可能會提供一個真實子網路。如果您擁有一個真實子網路，您可以選擇一個或多個 IP 位址設定在 WAN 介面。如果您需要使用固定 IP / 動態 IP，請先在視窗中選擇適當的模式，然後輸入相關資訊：

1. 選擇 **WAN1/WAN2** 作爲 WAN 介面，按**下一步(Next)**按鈕後，下圖將會出現讓您指定網際網路連線類型。



2. 選擇**固定 IP(Static IP)**然後按**下一步(Next)**開啓如下頁面。

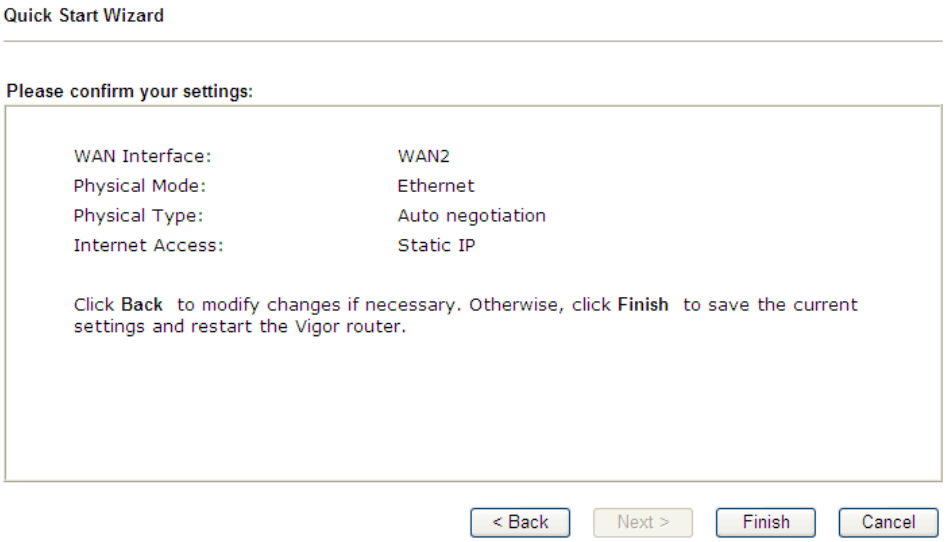


可用設定說明如下：

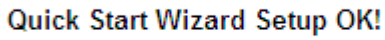
項目	說明
WAN IP	輸入 IP 位址。
子網路遮罩(Subnet Mask)	輸入子網路遮罩。
閘道(Gateway)	輸入閘道 IP 位址。

主要 DNS (Primary DNS)	輸入路由器主要的 DNS IP 位址。
次要 DNS (Secondary DNS)	必要時輸入路由器次要的 DNS IP 位址。
上一步(Back)	按此鈕回到上一頁面。
下一步(Next)	按此鈕進入下一頁面。
取消(Cancel)	按此鈕放棄快速設定精靈。

3. 請依照您的 ISP 業者提供的資料輸入使用者名稱與密碼。按**下一步(Next)**檢視連線的設定狀態。



4. 按完成，快速設定精靈安裝完畢頁面將會出現。

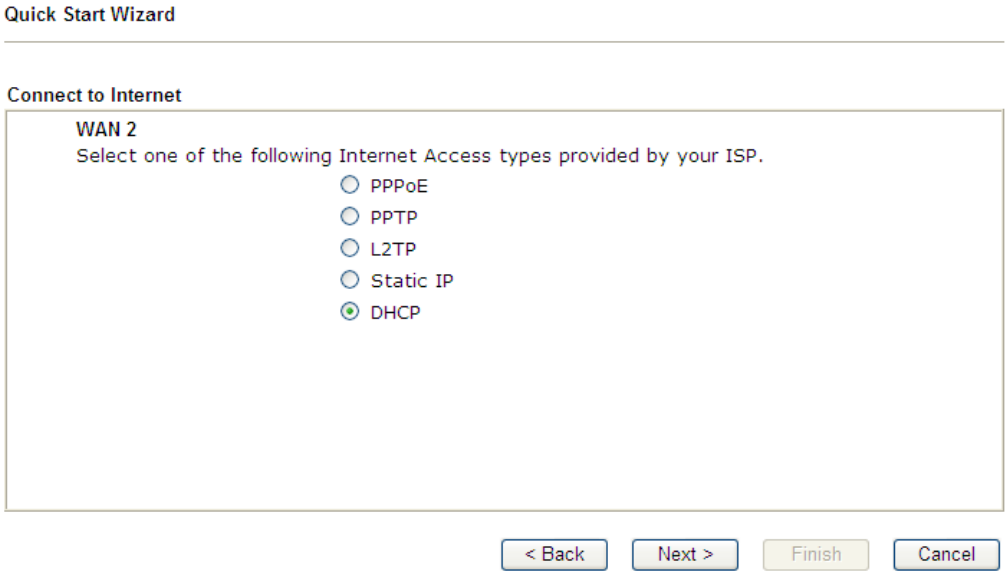


5. 現在您可以遨遊網際網路了。

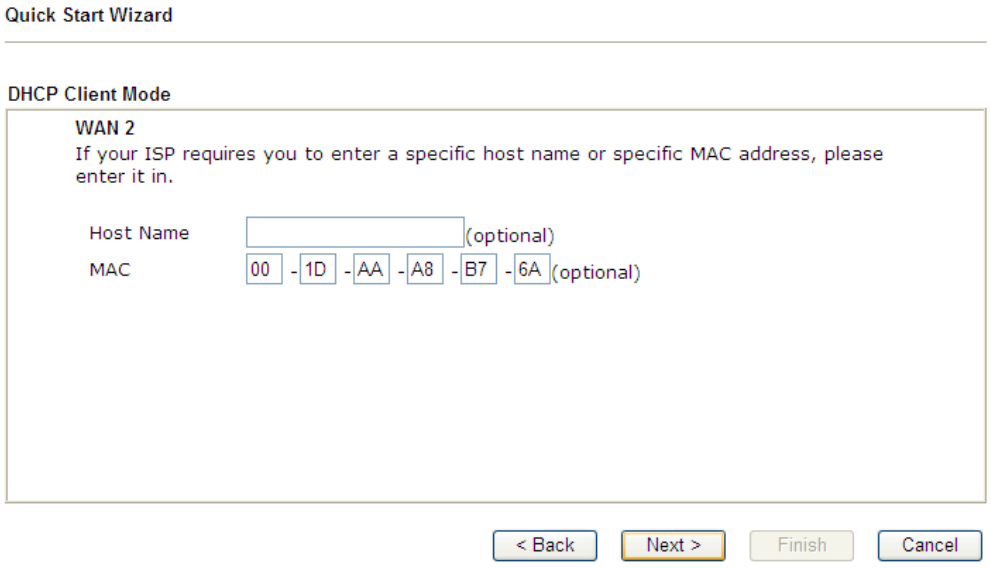
DHCP

選擇 **DHCP** 作爲通訊協定，並在頁面上輸入 ISP 提供給您的全部訊息。

1. 選擇 **WAN2** 作爲 WAN 介面，按**下一步**按鈕後，下圖將會出現讓您指定網際網路連線類型。



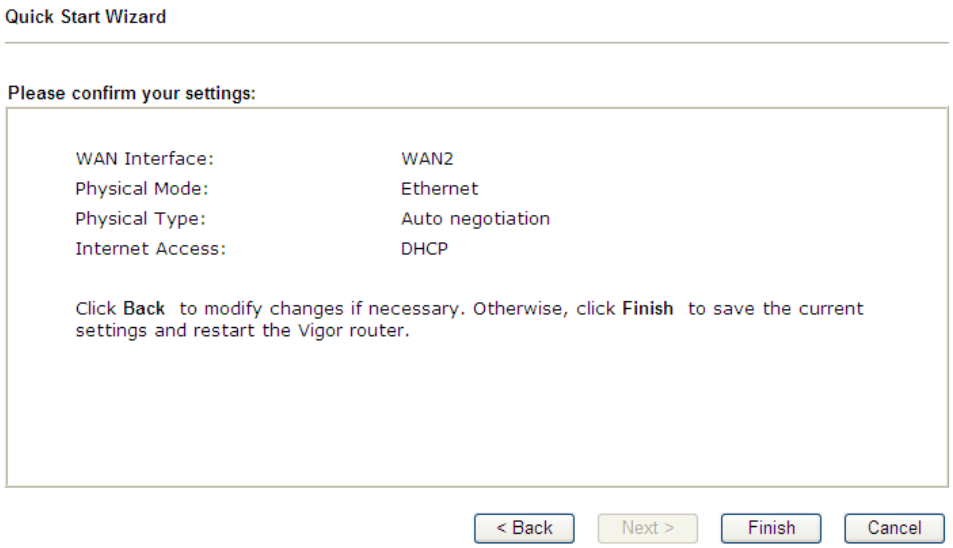
2. 選擇 **DHCP** 並按**下一步(Next)**按鈕。



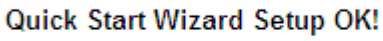
可用設定說明如下：

項目	說明
主機名稱(Host Name)	輸入主機名稱。
MAC	某些纜線服務供應商會要求提供 MAC 位址作爲驗證，在此情況下，請於此欄位輸入 MAC 位址。
上一步(Back)	按此鈕回到上一頁面。
下一步(Next)	按此鈕進入下一頁面。
取消(Cancel)	按此鈕放棄快速設定精靈。

3. 完成上述設定之後，按下一步**(Next)**檢視連線的設定狀態。



4. 按完成，快速設定精靈安裝完畢頁面將會出現。

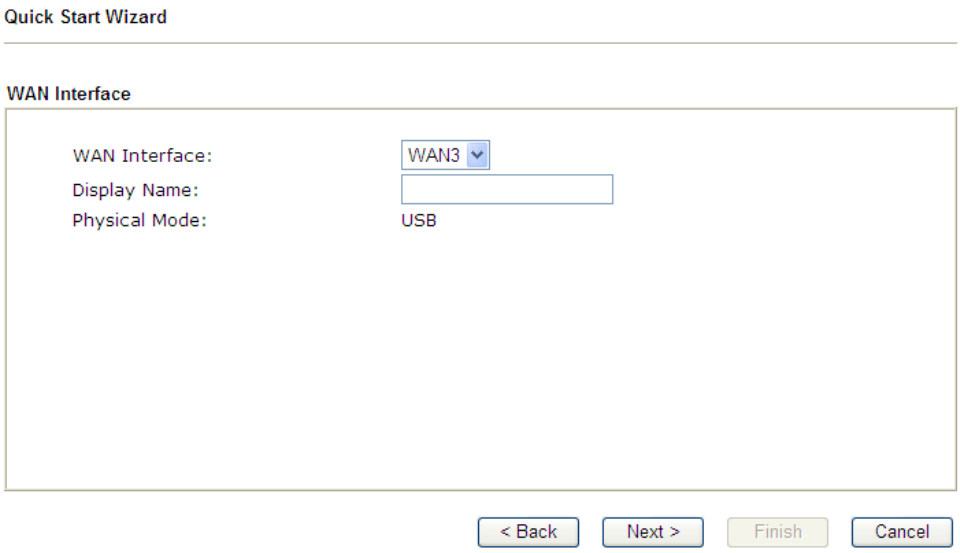


5. 現在您可以遨遊網際網路了。

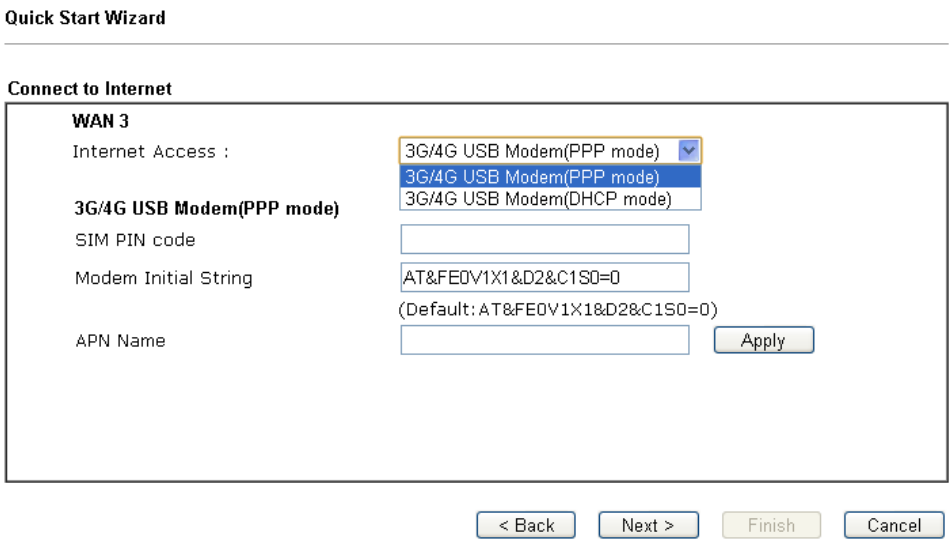
I-6-2 對於 WAN3/WAN4 (USB)

如果要使用 3G /4G USB 數據機進行網路連線，請選擇 WAN3/WAN4。

1. 選擇 **WAN3/WAN4** 作爲 WAN 介面。



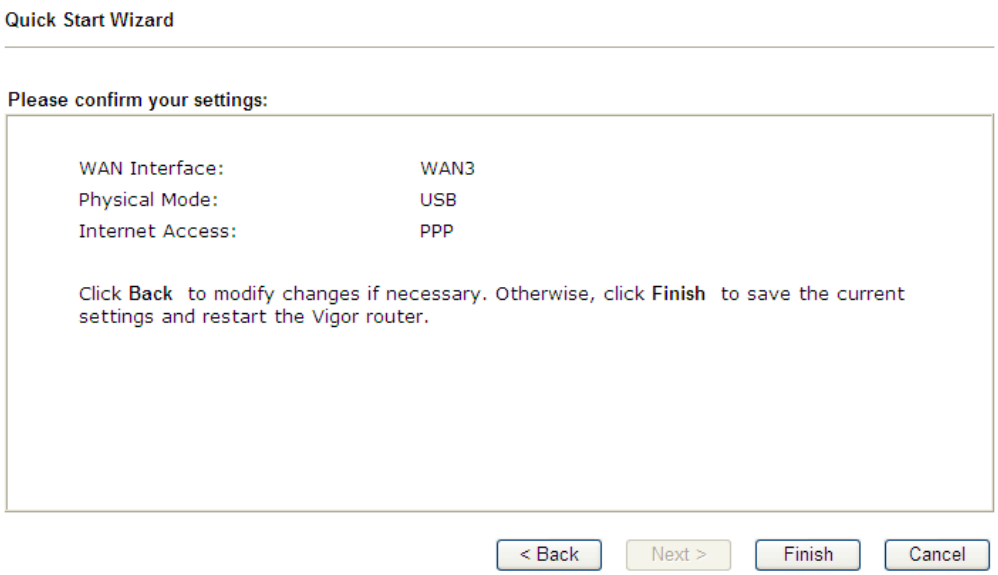
2. 按下一步**(Next)**，系統將會出現讓您指定網際網路連線類型。



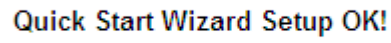
可用設定說明如下：

項目	說明
網際網路連線模式 (Internet Access)	選擇存取網際網路的連線模式。
3G/4G USB 數據機 (PPP 模式) **(3G/4G USB Modem (PPP mode))**	**SIM PIN 碼(SIM Pin code)**– 輸入用來登入網際網路之 SIM 卡的 PIN 代碼，最大長度爲 15 個字元。 **數據機初始字串(Modem Initial String)** – 這個數值，用來初始化 USB 數據機，請使用預設值，如果您有任何疑問，請與當地 ISP 業者聯絡。 **APN 名稱(APN Name)** – APN 表示基地台的名稱，通常是由 ISP 業者提供並要求您在此輸入，請輸入相關名稱並按下**套用 (Apply)**按鈕。
3G/4G USB 數據機 (DHCP 模式) **(3G/4G USB Modem (DHCP mode))**	**SIM PIN 碼(SIM Pin code)** – 輸入用來登入網際網路之 SIM 卡的 PIN 代碼，最大長度爲 15 個字元。 **網路模式(Network Mode)** – 選擇適用的連線模式。 **APN 名稱(APN Name)** – APN 表示基地台的名稱，通常是由 ISP 業者提供並要求您在此輸入，請輸入相關名稱。

3. 按下**一步(Next)**檢視此連線的設定狀態。



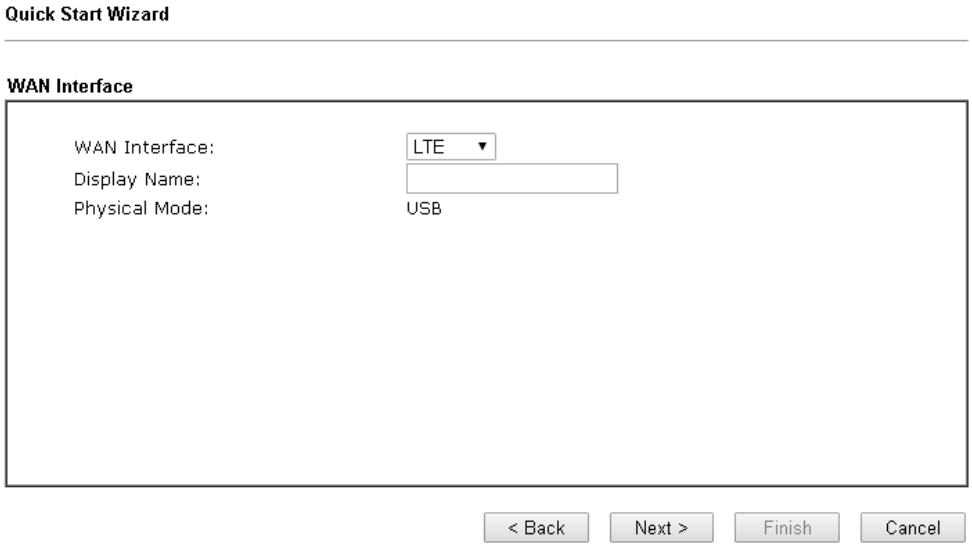
4. 按完成，快速設定精靈安裝完畢頁面將會出現。



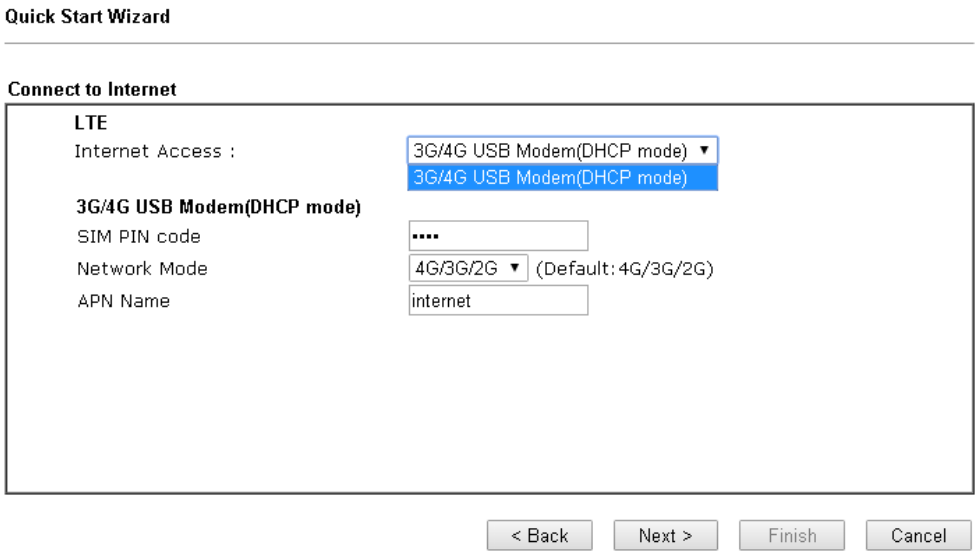
5. 現在您可以遨遊網際網路了。

I-6-3 對於 LTE WAN

1. 選擇 **LTE** 作爲 WAN 介面。



2. 按下一步**(Next)**，系統將會出現讓您指定網際網路連線類型。



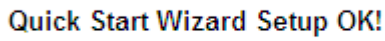
可用設定說明如下：

Item	Description
網際網路連線模式 (Internet Access)	目前 LTE WAN 選項模式僅有 DHCP。
3G/4G USB Modem (DHCP mode)	**SIM PIN 碼(SIM Pin code)** – 輸入用來登入網際網路之 SIM 卡的 PIN 代碼，最大長度爲 15 個字元。 **網路模式(Network Mode)** – 選擇適用的連線模式。 **APN 名稱(APN Name)** – APN 表示基地台的名稱，通常是由 ISP 業者提供並要求您在此輸入，請輸入相關名稱並按下**套用**按鈕。

3. 按下一步**(Next)**檢視此連線的設定狀態。



4. 按完成，快速設定精靈安裝完畢頁面將會出現。



5. 現在您可以遨遊網際網路了。

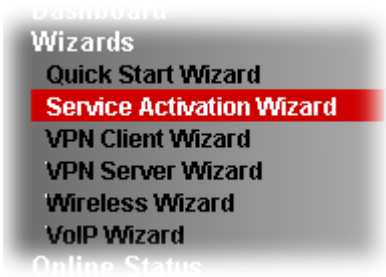
I-7 服務啟動精靈

服務啓用精靈可利用快速及簡便方式，幫助您啓用網頁內容過濾器服務機制(WCF)。服務啓用精靈是一個提供您使用試用版或是更新 WCF 授權憑證的工具，有了這項工具，您可不需要進入位於 http://myvigor.draytek.com 中的伺服器(***MyVigor***)。關於使用網頁內容過濾器的設定檔，請參考後續網頁內容過濾一節。

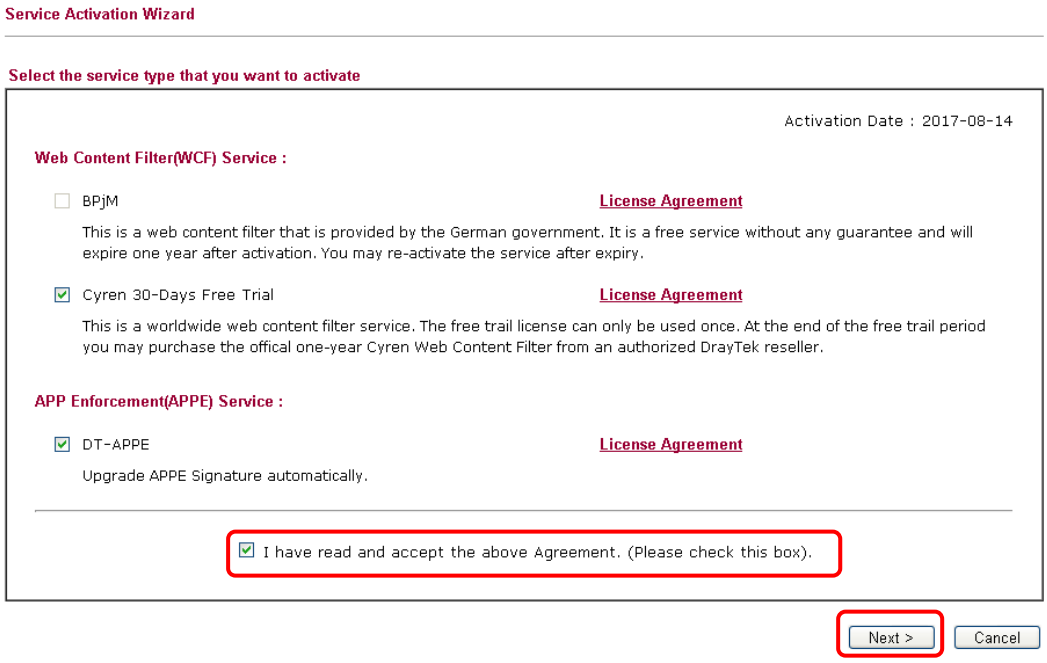
現在，請參考下述步驟進行啓用 WCF 功能作業。

資訊 此功能僅能於 Admin 模式下使用。

1. 開啓**設定精靈>>服務啓動精靈 (Wizards>>Service Activation Wizard)** 。



2. 服務啓用精靈畫面顯示如下，您可以啓用 WCF 服務、APP 應用程式管控服務，勾選 “I have read....” 之後，按下**一步(Next)**。



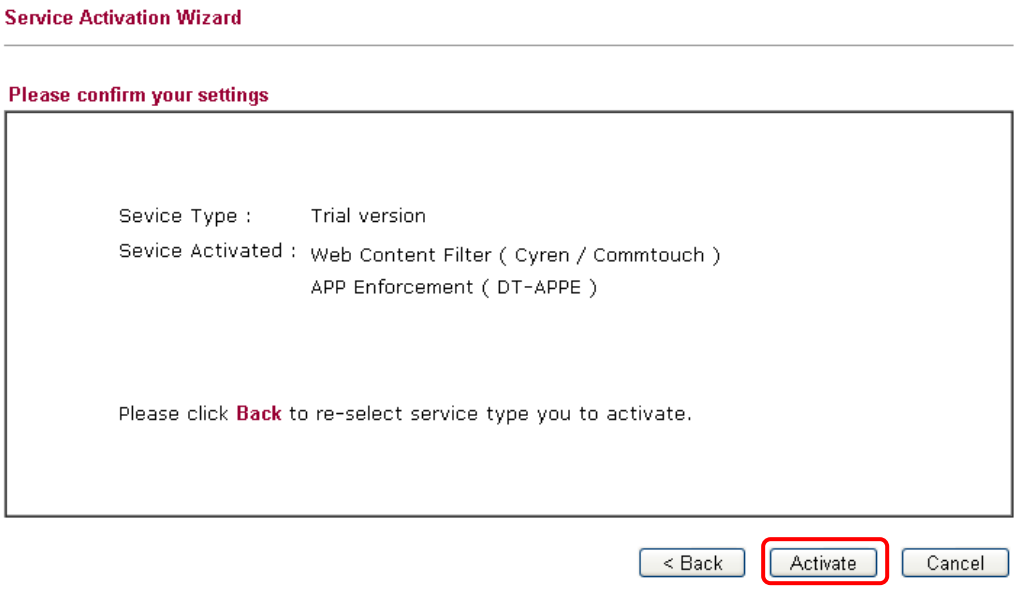
資訊

BPjM 是針對使用德語之用戶提供之服務，可爲家庭與年輕人提供提供更安全的網際網路環境。

Cryan 提供30天試用版，之後您可以向Cryan GlobalView 採購正式版本。

DT-APPE是居易公司提供的免費服務，可自動更新APPE授權碼。

3. Setting confirmation page will be displayed as follows, please click **Activate**.



資訊 此項服務在**防火牆>>基本設定(Firewall>>General Setup)**中，可被視爲預設規則啓用及套用

4. 現在，網頁將顯示您已經啓用的服務內容，有效時間亦顯示在畫面上。



I-8 註冊 Vigor 路由器

您已經完成快速安裝設定精靈，可隨時上網瀏覽您需要的資料與網站。現在您可以將 Vigor 路由器向 MyVigor 網站註冊登錄，以便取得更多的服務。請依下列步驟完成路由器註冊登錄作業。

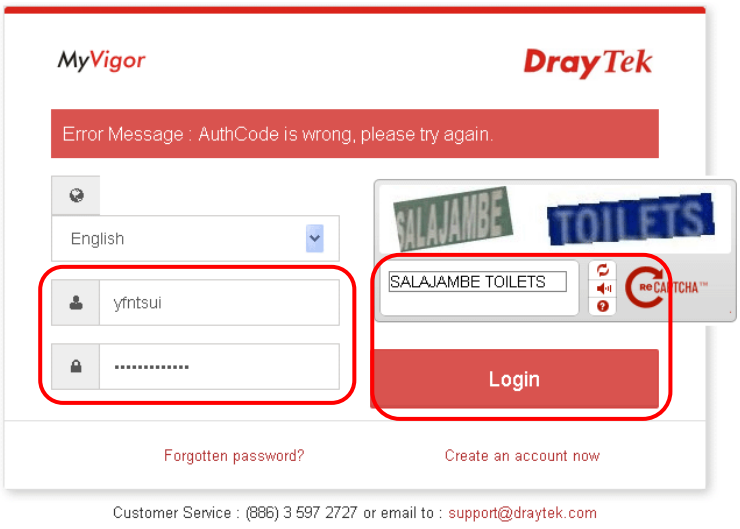
1 請登錄路由器的網頁設定介面，並在使用者名稱與密碼欄位皆輸入 **admin**。



2 按下位於首頁上的**支援區域>>產品註冊(Support Area>>Production Registration)**。



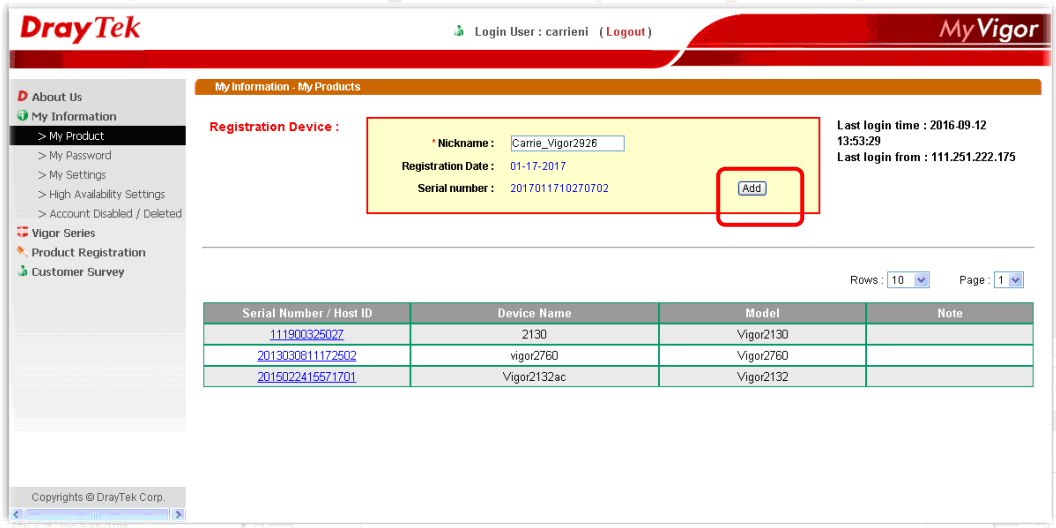
3 登入頁面出現如下圖，請輸入您先前即建立的帳號與密碼，然後按下**登入(Login)**。



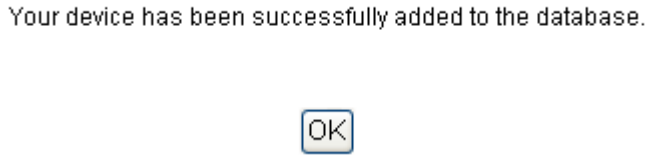
資訊

如果您尚未申請過帳號與密碼，您可以按此頁下方**"現在就建立一個帳號"** 連結先建立個人的帳密，再回來本頁繼續進行。

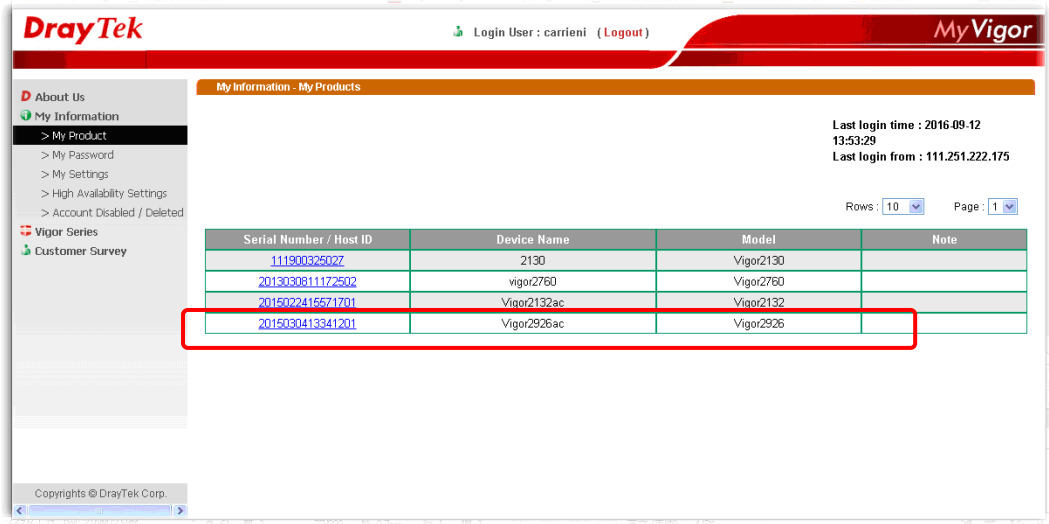
4 按下登入後，將會出現如下的畫面，請按下**新增(Add)**。



5 下述頁面出現後，您的路由器資訊已經加入 MyVigor 的資料庫中。



6 按下確定(**OK**)，新增的路由器將會列在清單中。



本頁留白

第二篇 連線設定



WAN

WAN表示寬頻網路，通常使用的是真實IP。



LAN

LAN代表區域網路，使用的是虛擬IP位址，基本上LAN是路由器規定且管理的子網群組，網路結構設計與取自ISP之真實IP位址類型有關聯。



NAT

當資料流量通過時，路由器的網路位址轉換(NAT)功能可以進行真實/虛擬IP位址轉換，封包可傳送至區域網路中正確的主機PC上。



Applications

應用的部份包含DDNS, LAN DNS, IGMP, LDAP, UPnP, WOL, RADIUS, SMS, Bonjour, HA, Local 802.1X 等等



Routing

包含有固定路由、負載平衡、路由策略等等

II-1 WAN

可讓使用者登入網際網路。

網路的基本概念

IP 表示網際網路通訊協定，在以 IP 爲主的網路像是路由器、列印伺服器和主機電腦的每一種裝置，都需要一組 IP 位元址作爲網路上身分辨識之用。爲了避免位址產生衝突，IP 位址都必須於網路資訊中心(NIC) 公開註冊，擁有個別 IP 位址對那些於真實網路分享的裝置是非常必要的，但在虛擬網路上像是路由器所掌管下的主機電腦就不是如此，因爲它們不需要讓外人從真實地區進入存取資料。因此 NIC 保留一些永遠不被註冊的特定位址，這些被稱之爲虛擬 IP 位址，範圍條列如下：

From 10.0.0.0 to 10.255.255.255
From 172.16.0.0 to 172.31.255.255
From 192.168.0.0 to 192.168.255.255

什麼是真實 IP 位址和虛擬 IP 位址

由於路由器扮演著管理及保護其區域網路的角色，因此它可讓主機群間互相聯繫。每台主機都有虛擬 IP 位址，是由路由器的 DHCP 伺服器所指派，路由器本身也會使用預設之虛擬 IP 位址 192.168.1.1 與本地主機達成聯繫目的，同時，Vigor 路由器可藉由真實 IP 位址與其他的網路裝置溝通連接。當資料經過時，路由器的網路位址轉換(NAT)功能將會在真實與虛擬位址間執行轉換動作，封包將可傳送至本地網路中正確的主機電腦上，如此一來，所有的主機電腦就都可以共用一個共同的網際網路連線。

取得 ISP 提供的真實 IP 位址

在 ADSL 之部署中，PPP (Point to Point)型態之驗證和授權是橋接用戶前端設備所需要的。PPPoE (Point to Point Protocol over Ethernet)透過一台存取裝置連接網路主機至遠端存取集中器，此種應用讓使用者覺得操作路由器是很簡單的，同時也可依照使用者的需要提供存取控制及服務類型。

當路由器開始連接至 ISP 時，路由器將執行一系列過程以尋求連線，然後即可產生一個連線數，您的使用者辨識名稱和密碼由 **RADIUS** 驗證系統的 **PAP** 或 **CHAP** 來驗證，通常您的 IP 位址、DNS 伺服器和其他相關資訊都是由 ISP 指派的。

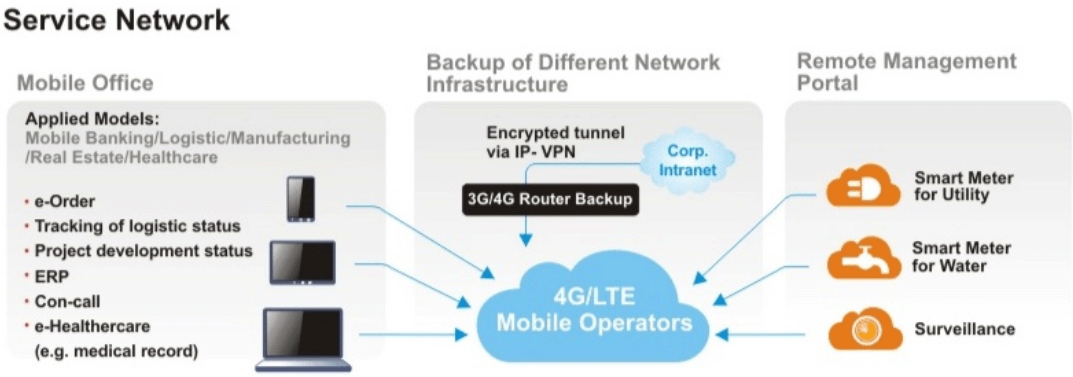
3G/4G USB Modem 網路連線

由於透過基地台 3G 行動通訊越來越普遍，因而 Vigor 2926 新增了 3G 網路通訊功能。藉著連接 3G/4G USB Modem 至 Vigor2925 的 USB 埠，路由器可支援 HSDPA/UMTS/EDGE/GPRS/GSM 以及未來 3G 標準(HSUPA, etc)，有了 3G USB Modem 的 Vigor2926n 可讓您隨時隨地接收 3G/4G 信號，不論是在汽車上或是在戶外地區舉行活動時，都可讓多數人共用頻寬。使用者可以利用四個區域網路 LAN 埠連上網際網路，此外也可以透過 Vigor2926n 的 11n 無線功能存取網路資料，享受路由器強大的防火牆、頻寬管理、VPN、VoIP 等功能。



在連接上路由器後，3G/4G USB Modem 即被視爲第二個 WAN 埠，雖然如此原本的乙太網路 WAN1 仍可作爲負載平衡之用，此外 3G/4G USB Modem 也可被視爲備存裝置。因此當 WAN1 無法使用時，路由器將自動改用 3G/4G USB Modem 以應需要。目前路由器支援哪些 3G/4G USB Modem，可在居易網站上取得，歡迎造訪 www.draytek.com。

LTE 應用



網頁使用者介面

下圖爲 WAN 的功能項目：



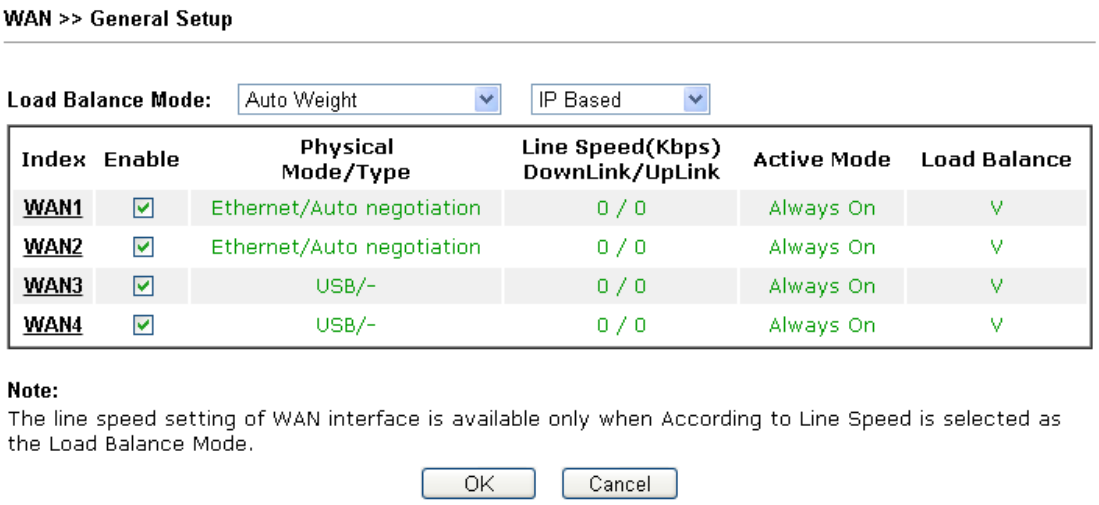
II-1-1 基本設定(General Setup)

本節介紹數種網際網路的一般設定，並詳細說明 WAN1、WAN2, WAN3(或是 LTE) 與 WAN4 介面。

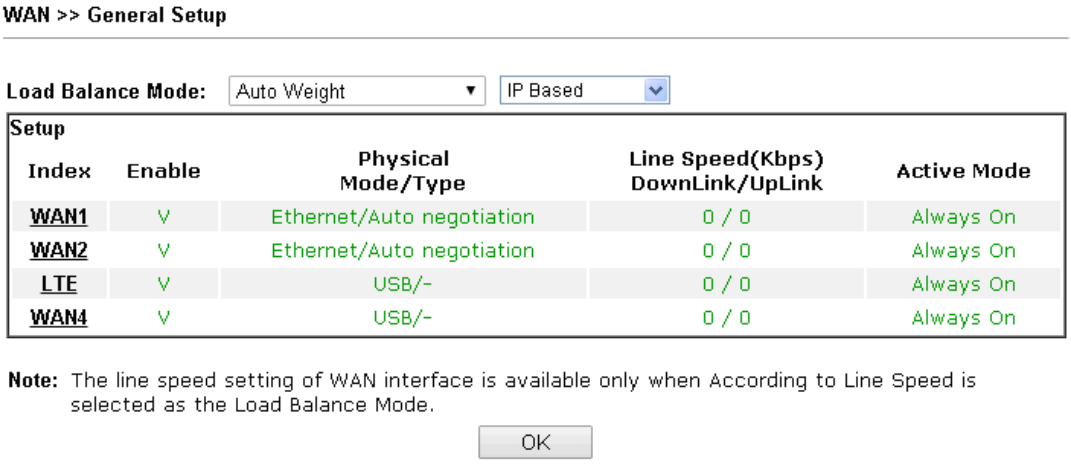
路由器支援雙 WAN 口功能，可讓使用者存取網際網路並整合雙 WAN 口的頻寬以加速網路資料傳輸。每個 WAN 連接埠(WAN1--透過 WAN 連結埠/WAN2--透過 LAN1 連接埠)可以連接到不同的 ISP，即使 ISP 使用不同的技術提供不同的電信服務(如 DSL, Cable 數據機等等)也都沒有問題。如果任何一個 ISP 連線出了問題，全部的傳輸動作都將引導並切換至正常的 WAN 口連接埠並繼續運行。

本頁讓您分別設定 WAN1, WAN2, WAN3(或是 LTE) 與 WAN4 介面的基本資訊，在預設值中，WAN2 是停用的，如果您想要啓用該 WAN 埠口，點入該連結然後再選擇**是**即可啓用。

除了 Vigor2926L 與 Vigor2926Ln 以外的機種---



針對 Vigor2926L 與 Vigor2926Ln 二機種----



可用設定說明如下：

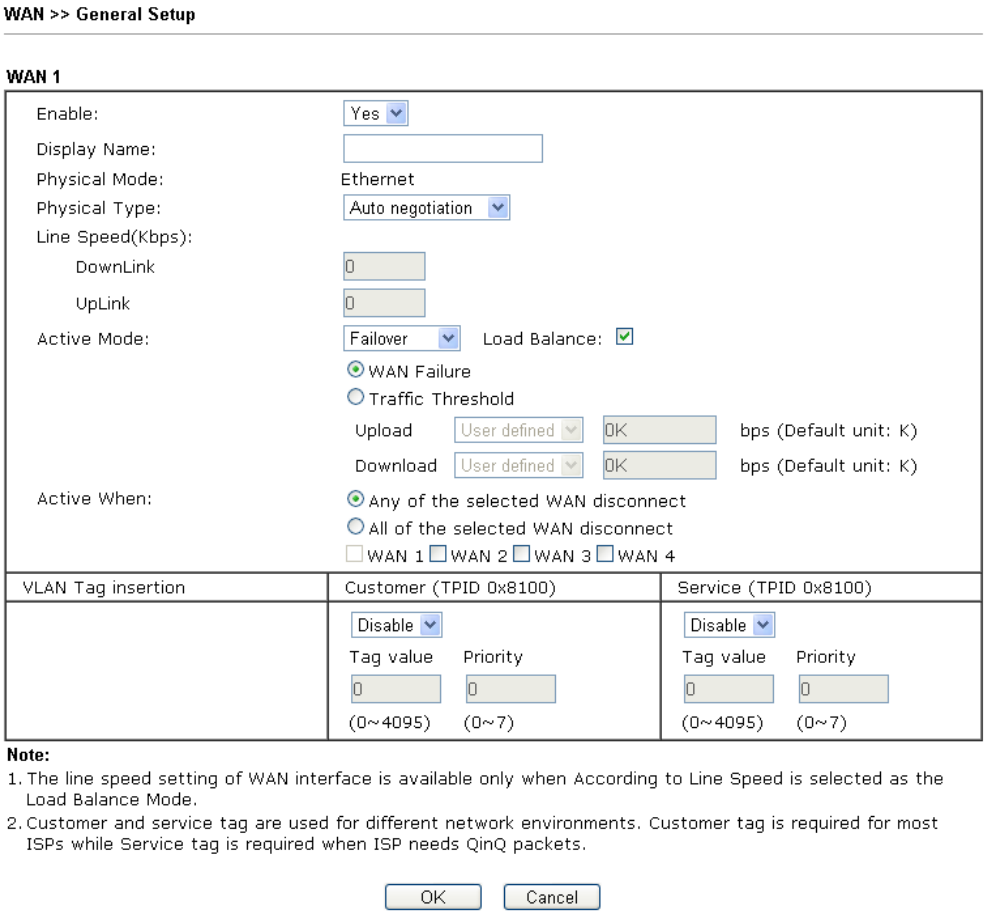
項目	說明
負載平衡模式(Load Balance Mode)	這個選項主要是對多重 WAN 設定中提供每個 WAN 口足夠的頻寬。如果您知道使用 WAN 埠口實際的頻寬，請選擇**依照連線速度(According to Line Speed)**，否則請勾選**自動權重(Auto Weight)**讓系統決定最佳的負載量。 **IP 式(IP Based)** - 來源/目的 IP 皆相同者，可選擇相同的 WAN 介面，這是預設值。 **連線數式(Sesseion Based)**- 所有的 WAN 介面(作爲對外 WAN)皆可用以通過新的連線數以便取得較佳的傳輸速度。雖然可以達到良好的速度測試結果，然而某些網站可能無法順利開啓，尤其是需要驗證的網站如 FTP 更是如此。 如果您對於速度測試結果的需求並不強烈，建議使用預設值即可。
索引編號(Index)	點選索引編號下的 WAN 介面連結，以登入 WAN 設定頁面。
啓用(Enable)	**V** 代表此 WAN 介面已經啓用，並可以使用。
實體模式/類型(Physical Mode / Type)	Display the physical mode and physical type of such WAN interface. 顯示此 WAN 介面的實體模式以及實體類型。
線路速度(Kbps) 下行/上行 **(Line Speed(Kbps) DownLink/UpLink)**	顯示此 WAN 介面下載速率與上傳速率。
啓動模式(Active Mode)	顯示此 WAN 介面目前是主動裝置或是備援裝置。

資訊	預設狀態下，每個WAN都是啓動的。

完成上述設定之後，按下**確定(OK)**儲存設置內容。

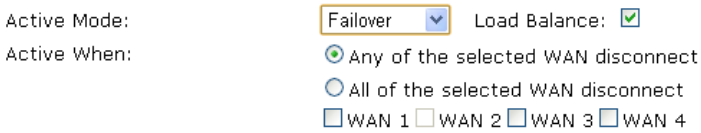
II-1-1-1 乙太網路的 WAN1/WAN2 介面

WAN1/WAN2 介面的實體模式固定爲乙太網路。



可用設定說明如下：

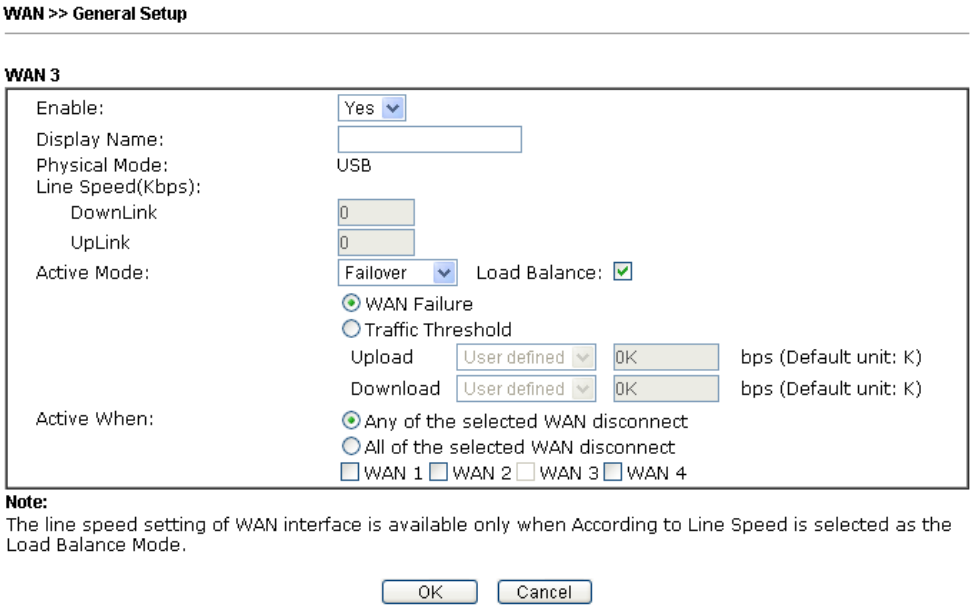
項目	說明
啓用(Enable)	選擇**是(Yes)**啓動此 WAN 介面的設定，選擇**否(No)**則關閉此介面的設定。
顯示名稱(Display Name)	輸入 WAN1 的說明內容。
實體連線模式(Physical Mode)	顯示此 WAN 介面的實體連線模式。
傳送資料模式(Physical Type)	您可以改變 WAN 的傳送資料模式，或是選擇**自動偵測(Auto negotiation)**讓系統自行處理。 
連線速度(Line Speed)	如果您選擇**依照連線速度(According to Line Speed)**作爲**負載平衡模式(Load Balance Mode**,)，請您輸入連線速度以便透過 WAN1/WAN2 介面上傳下載資料。單位是 kbps。

啓動模式(Active Mode)	**永遠連線(Always On):** 讓 WAN 連線永遠啓動。 **負載平衡(Load Balance)**: 針對此 WAN 介面，採取自動負載平衡。 當資料流量過大時，啓用負載平衡之 WAN 介面，將可在所有連線的 WAN 介面上自動平衡流量傳輸。 **備援(Failover)** – 選擇此項讓 WAN 連線做爲備援連線。 ● **WAN 失敗(WAN Failure)** – 當啓用運作中的 WAN 連線失敗，此 WAN 介面將可被啓用作爲主要網路連線。 ● **流量門檻(Traffic Threshold)** – 當資料流量或是運作中的 WAN 達到流量門檻(此處指定)時，此備援 WAN 將自動啓動以便分享過載的資料流量。
何時活躍(Active When)	如果您選擇**備援(Failover)**作爲**啓動模式(Active Mode)**，**備援類型**選項將會出現在畫面上，請指定哪個 WAN 介面要做爲備援 WAN 介面。  **當任何一個 WAN 介面中斷連線時(Any of the selected WAN disconnect)** – 當任何一個主要的 WAN 介面突然中斷連線時，此備援 WAN 介面將會立即啓動。 **當所有的 WAN 介面皆中斷連線時(All of the selected WAN disconnect)** – 當所有的主要 WAN 介面都中斷連線時，此備援 WAN 介面將會立即啓動。
VLAN 標籤插入(VLAN Tag insertion)	此功能主要是提供給支援 IEEE_802.1ad 環境的用戶使用，其中服務(service)用在對外標籤(outer tag)；客戶(customer)用在對內標籤(inner tag)。 **啓用(Enable)** – 啓動夾帶標籤的 VLAN 設定。 路由器將會加上特定的 VLAN 號碼於所有透過此 WAN 口傳出的封包上。 請輸入標籤值並指定由此 WAN 口傳送的封包的優先順序。 **停用(Disable)** – 停止夾帶標籤的 VLAN 設定。 **標籤值(Tag value)** – 輸入準備作爲 VLAN ID 編號的數值，可填範圍爲 0 到 4095。 **優先權(Priority)** – 輸入此 VLAN 設定的優先權限，可選範圍從 0 到 7。

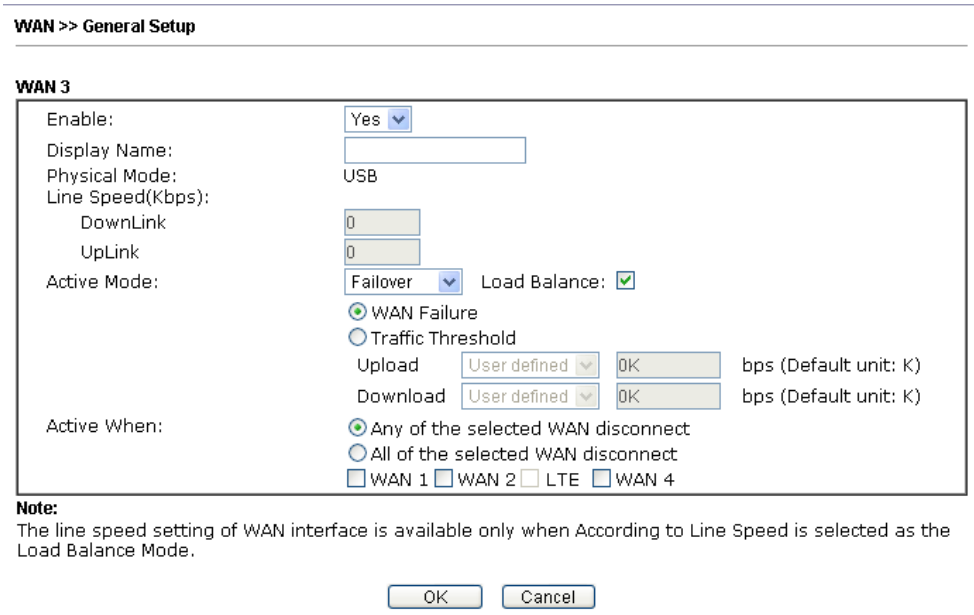
完成上述設定之後，按下**確定(OK)**儲存設置內容。

II-1-1-2 USB 的 WAN3/WAN4 介面

如果要透過 3G/4G USB 數據機來使用 3G/4G 網路連線，請設定 WAN3/WAN4 介面：

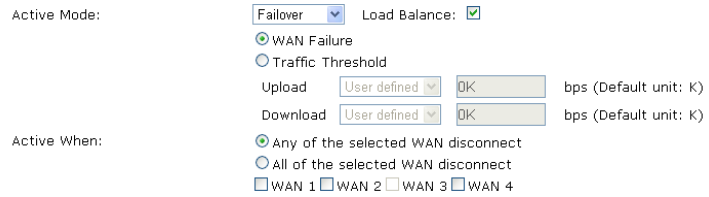


或是(針對 LTE 型號)



可用設定說明如下：

項目	說明
啓用(Enable)	選擇**是(Yes)**啓動此 WAN 介面的設定，選擇**否(No)**則關閉此介面的設定。
顯示名稱(Display Name)	輸入 WAN1 的說明內容。
實體連線模式(Physical Mode)	顯示此 WAN 介面的實體連線模式。
連線速度(Line Speed)	如果您選擇**依照連線速度(According to Line Speed)**作爲**負載平衡模式(Load Balance Mode**,)，請您輸入連線速度以便透過 WAN1/WAN2 介面上傳下載資料。單位是 kbps。

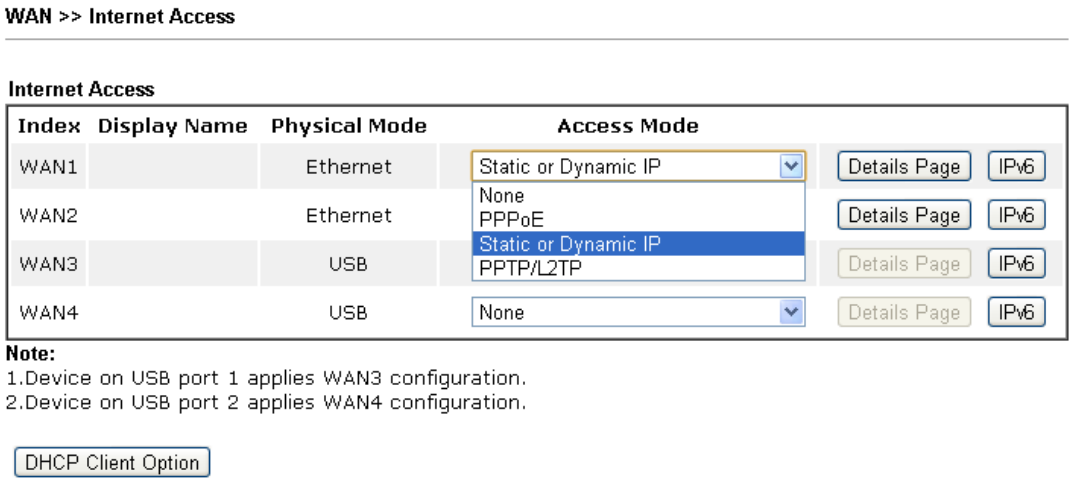
啓動模式(Active Mode)	**永遠連線(Always On):** 讓 WAN 連線永遠啓動。 **負載平衡(Load Balance)**: 針對此 WAN 介面，採取自動負載平衡。 當資料流量過大時，啓用負載平衡之 WAN 介面，將可在所有連線的 WAN 介面上自動平衡流量傳輸。 **備援(Failover)** – 選擇此項讓 WAN 連線做爲備援連線。 ● **WAN 失敗(WAN Failure)** – 當啓用運作中的 WAN 連線失敗，此 WAN 介面將可被啓用作爲主要網路連線。 ● **流量門檻(Traffic Threshold)** – 當資料流量或是運作中的 WAN 達到流量門檻(此處指定)時，此備援 WAN 將自動啓動以便分享過載的資料流量。
何時活躍(Active When)	如果您選擇**備援(Failover)**作爲**啓動模式(Active Mode)**，**備援類型**選項將會出現在畫面上，請指定哪個 WAN 介面要做爲備援 WAN 介面。  **當任何一個 WAN 介面中斷連線時(Any of the selected WAN disconnect)** – 當任何一個主要的 WAN 介面突然中斷連線時，此備援 WAN 介面將會立即啓動。 **當所有的 WAN 介面皆中斷連線時(All of the selected WAN disconnect)** – 當所有的主要 WAN 介面都中斷連線時，此備援 WAN 介面將會立即啓動。

完成上述設定之後，按下**確定(OK)**儲存設置內容。

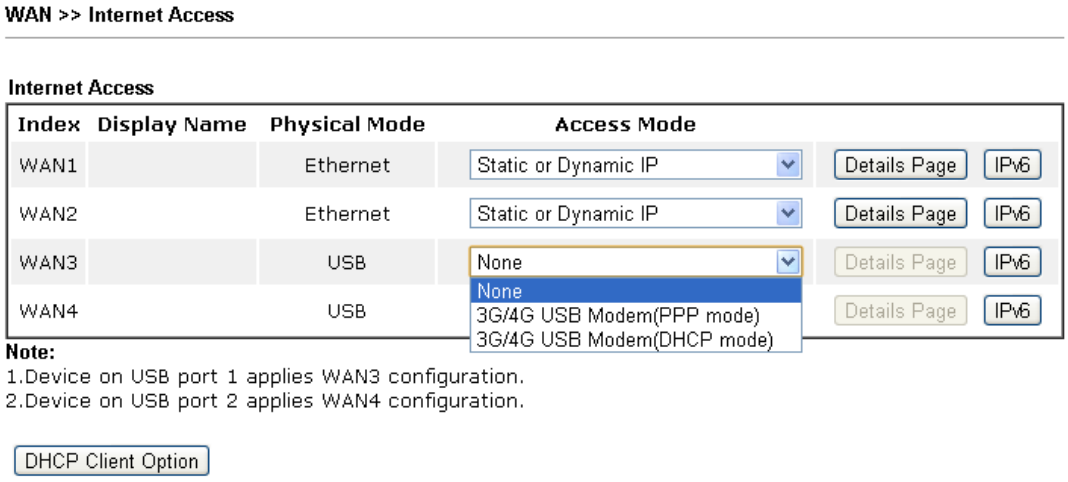
II-1-2 網際網路連線(Internet Access)

因爲路由器支援多 WAN 口功能，使用者得以設定不同的 WAN 設定供網際網路存取之用，又因爲 WAN1/WAN2/WAN3 或 LTE/WAN4 的實體連線並不同，二者的連線模式也會有些差異。

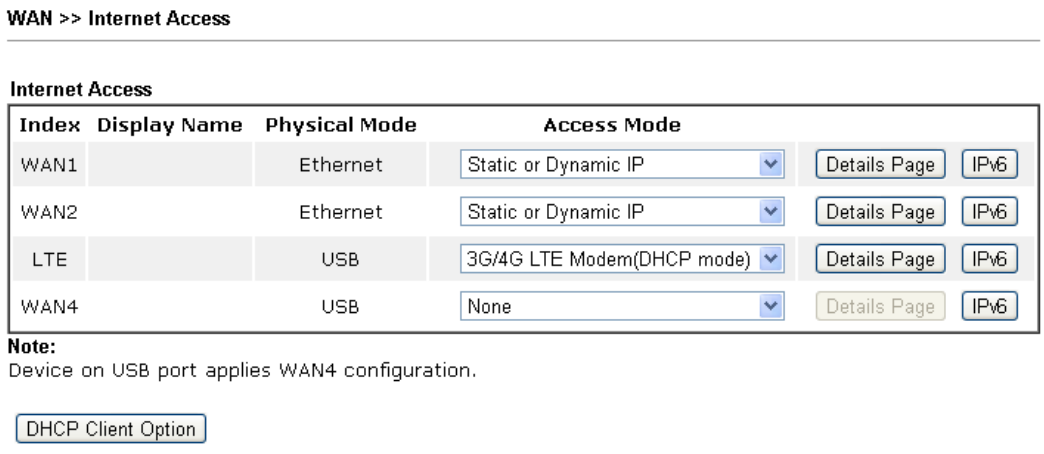
乙太網路下的連線模式：



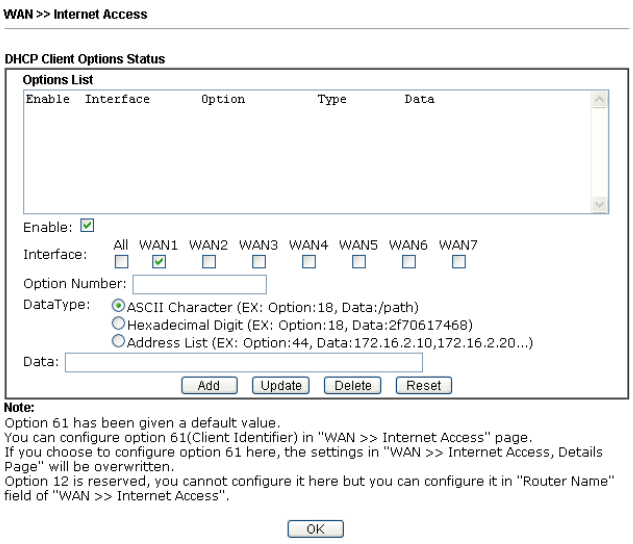
USB 下的連線模式：



LTE (僅限 L 型號)下的連線模式：



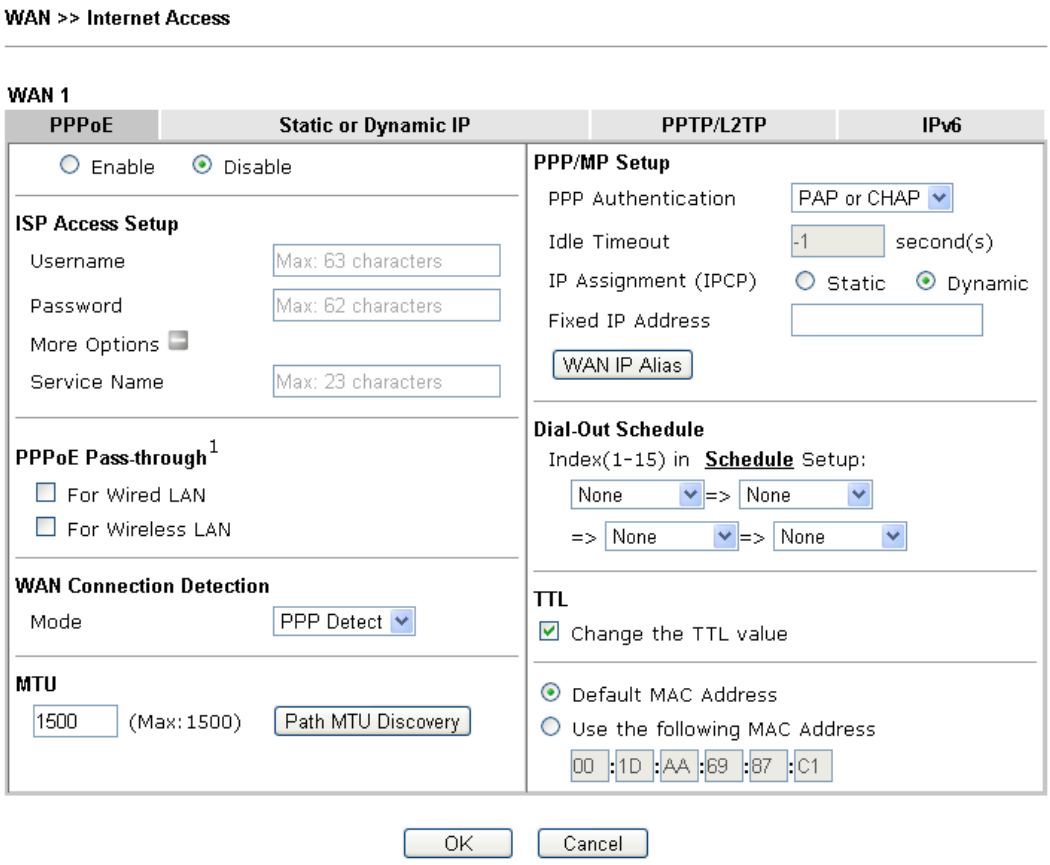
可用設定說明如下：

項目	說明
索引(Index)	顯示路由器支援的 WAN 介面。
顯示名稱(Display Name)	顯示 WAN 於一般設定中所輸入的名稱。
實體連線模式(Physical Mode)	按照實際網路連線狀況來顯示各個 WAN 實體連線。
連線模式(Access Mode)	使用下拉式清單選擇適當的網際網路連線模式，接著按右邊的 **細節設定(Details Page)**以設定詳細內容。 網頁提供數種網際網路連線模式。
細節設定(Details Page)	此按鈕將依照您在 WAN 所選擇的連線模式展現不同的網頁內容。
IPv6	此按鈕將會開啓不同的網頁(以實體連線模式爲基準)，針對 WAN 介面設定 IPv6 網際網路存取模式。 如果在 WAN 介面中 IPv6 已經啓動了，那麼您可以在網頁上看到綠色的 IPv6 字樣。
DHCP 用戶端選項 (DHCP Client Option)	此按鈕可設定 DHCP 用戶端選項(DHCP client options)。 DHCP 封包可利用新增之選項號碼及資料資訊進行不同的處理。  **啓用(Enable)** – 勾選此框啓用此 DHCP 選項功能。每個 DHCP 選項是由選項號碼與資料組合而成，例如 Option number:100 Data: abcd 當功能啓用時，指定的 DHCP option 數值將可現於 DHCP 回覆封包中。 **介面(Interface)** – 指定此功能可覆寫的 WAN 介面， WAN5 ~ WAN7 可透過 **WAN>>多重 VLAN(WAN>>Multi-PVC/VLAN)** 中指定。 **選項號碼(Option Number)** – 請針對此功能輸入需求數字。 **附註:** 若您選擇設定 option 61，那麼 **WAN>>網際網路連線(WAN>>Interface Access)**中的的細節設定內容將會被覆寫。

	資料類型(DataType) –選擇要儲存的資料類型(ASCII 或是十六進位)。 **資料(Data)** – 輸入 DHCP option 功能準備處理的資料內容。

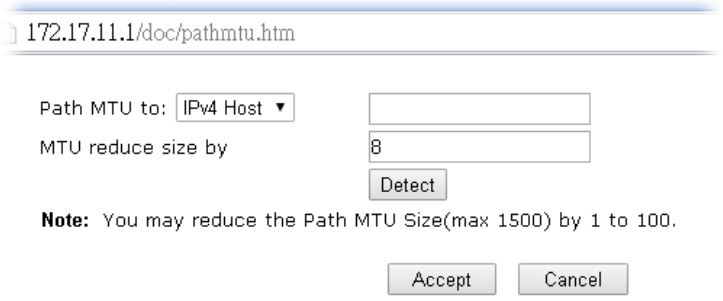
II-1-2-1 WAN1/WAN2 中的 PPPoE 模式細節設定(實體模式：乙太網路)

如果想要使用 PPPoE 作爲網際網路連線的通訊協定，請自 **WAN** 功能項目中選擇**網際網路連線 (Internet Access)**，接著在 WAN1 中選擇 PPPoE 模式，下面的細節設定網頁將會出現。



可用設定說明如下：

項目	說明
啓用/停用(Enable/Disable)	按下**啓用(Enable)**按鈕可啓動此功能，如果您選的是**停用(Disable)**，此項功能將會關閉，全部調整過的設定也都將立即失效。
ISP 存取設定(ISP Access Setup)	輸入使用者名稱、密碼和驗證參數，按照 ISP 所提供給您的訊息。 **使用者名稱(Username)** –在本區請輸入 ISP 提供的使用者名稱。 **密碼(Password)**– 在本區請輸入 ISP 提供的密碼。 **更多選項(More Options) –** 顯示更多的選項設定。 **服務名稱(選項)Service Name (Optional) -** 輸入特定網路服務的相關說明。
PPPoE 通透(PPPoE Pass-through)	路由器提供 PPPoE 撥號連線，除此之外，您也可以直接建立 PPPoE 連線，連接本機用戶端與 ISP 業者。當選定 PPPoA 通訊協定時，PC 傳送的 PPPoE 封包將可轉換爲 PPPoA 封包並傳送至 WAN 伺服器。如此一來，PC 可透過該傳輸方向存取網際網路。 **針對有線 LAN(For Wired LAN)** – 若勾選此框，相同網路上的 PC 可以使用另一組 PPPoE 連線數(不同於主機 PC)以存取網際

	網路。 **針對無線 LAN(For Wireless LAN)** – 這個功能僅適用 *n* 機種，若勾選此框，相同無線區域網路上的 PC 可以使用另一組 PPPoE 連線數(不同於主機 PC)以存取網際網路。 **附註:** 欲使用 PPPoA 通透，請先選擇 PPPoA 通訊協定，在勾選此出的方框，路由器將表現有如數據機，僅提供 LAN 端的 PPPoE 用戶相關的服務，亦即路由器將提供 PPPoA 撥號連線。
WAN 連線檢測(WAN Connection Detection)	這個功能讓您檢查目前網路是否還在連線中。可透過 ARP 檢測或是 Ping Detect 來完成。 **模式(Mode)** – 選擇 **ARP 檢測(ARP Detect)或 Ping 檢測(Ping Detect)**執行 WAN 檢測動作。 ● **主要/次要 Ping IP (Primary/Secondary Ping IP)** – 若您選擇了 **Ping 偵測(Ping Detect)** 作爲偵測模式，您必須在本區輸入主要或是次要 IP 位址。 ● **Ping 閘道 IP(Ping Gateway IP)** – 若您選擇了 **Ping 檢測(Ping Detect)** 作爲偵測模式，您也可以啓用此設定，以便使用目前的 WAN 閘道做爲 ping IP 位址。 藉由 IP 位址 ping，路由器可以檢查該 WAN 連線是啓用的或是中斷的。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。 ● **Ping 間隔(Ping Interval) –** 輸入執行 Ping 操作系統所需要的時間間隔。 ● **Ping 重試(Ping Retry) –** 輸入判斷 WAN 連線中斷之前，系統執行 Ping 操作時容許的嘗試次數。
MTU	代表封包的最大傳輸單位。 **路徑 MTU 搜尋(Path MTU Discovery)** – 用於偵測封包在特定傳輸路徑當中，不被分段的最大 MTU 尺寸。 按**檢測(Detect)** 開啓如下頁面：to open the following dialog.  ● **路徑最大傳輸單位至(Path MTU to)** – 輸入 IP 位址作爲特定傳輸路徑。 ● **MTU 值之降低乃透過(MTU reduce size by)** – 決定 MTU 值得降低大小，例如此區指定數字爲 8，最大的 MTU 大小爲 1500，在您按下檢測按鈕之後，系統將會計算並取得適合的 MTU 值，像是 1500、1492、1484 等等。 ● **檢測(Detect)** – 按此檢測出適合的 MTU 值。 ● **接受(Accept)** – 選了此項之後，檢測得到的值會顯示在 MTU 欄位中。
PPP/MP 設定 (PPP/MP Setup)	**PPP 驗證(PPP Authentication)** – 選擇 **PAP** 或是 **PAP 或 CHAP**。如果您想要永遠連接網際網路，請勾選**永遠連線**。 **閒置逾時(Idle Timeout)** – 設定網際網路在經過一段沒有任何

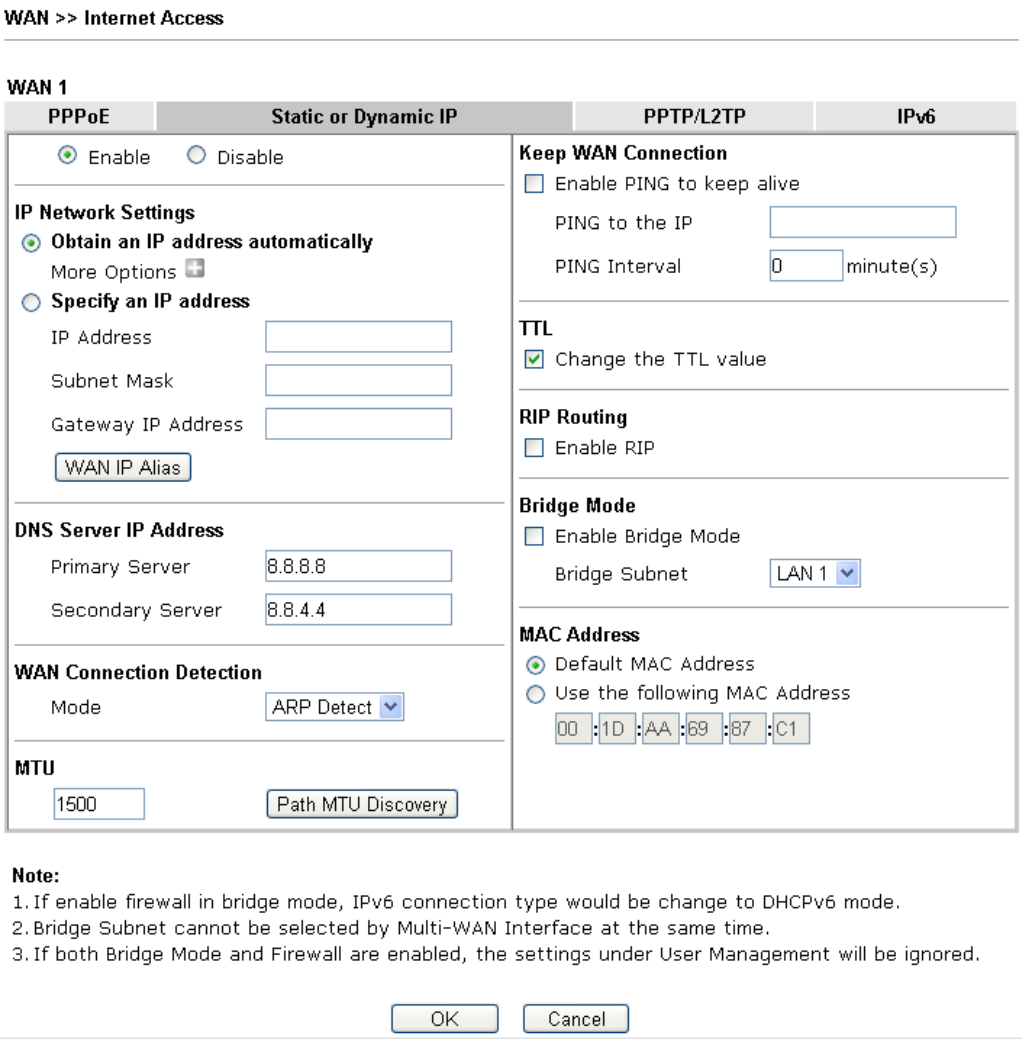
	動作的時間後自動斷線的時間。 **IP 分配 (IPCP) -** 通常每次的連線，ISP 會隨機指派 IP 位址給您，在某些情況下，您的 ISP 可以提供給您相同的 IP 位址，不論您何時提出要求。您只要在固定 IP 位址欄位中輸入 IP 位址就可以達成上述的目的。詳情請聯絡您的 ISP 業者。 **固定 IP 位址(Fixed IP)** – 按**是(Yes)**使用此功能並輸入一個固定的 IP 位址。 **WAN IP 別名(WAN IP Alias)** - 如果您有數個真實 IP 位址且想要在 WAN 介面上使用，請使用此功能。除了目前使用的這一組之外，您還可以設定多達 32 組的真實 IP 位址。
撥出排程(Dial-Out Schedule)	**索引編號(Index (1-15) in Schedule Setup) -** 您可以輸入四組時間排程，所有的排程皆可於**應用程式>>排程(Application >> Schedule)**頁面中事前設定，只要在此輸入該頁面設定的排成索引編號即可。
TTL	**變更 TTL 值(Change the TTL value) -**啓用或是停用封包透過路由器傳輸時的 TTL 功能。 ● **若勾選** – TTL 值會在通過路由器時降低(-1)，這會讓透過路由器存取網際網路的用戶端，在 TTL 的數值變爲 0 的時候，直接被指定 ISP 封鎖住。 ● **若未勾選** – TTL 值不會減少，之後當封包透過路由器傳送時，就不會被取消。也就是說，傳送此封包的用戶端並不會被 ISP 業者封鎖住。 **預設 MAC 位址(Default MAC Address)** – 您可以在此使用**預設 MAC 位址(Default MAC Address)** 或是指定另一組 MAC 位址。 **指定 MAC 位址(Specify a MAC Address) -** 手動輸入路由器需求之 MAC 位址。

完成上述設定之後，按下**確定(OK)**儲存設置內容。

II-1-2-2 WAN1/WAN2 中的固定或是動態 IP 模式細節設定(實體模式：乙太網路)

對固定 IP 模式來說，通常您會收到 DSL 或是 ISP 服務供應商提供給您的一個固定的真實 IP 位址或是真實子網路，在大多數的情形下，Cable 服務供應商將會提供一個固定的真實 IP，而 DSL 服務供應商提供的是真實子網路資料。如果您有一組真實的子網路，您可以指派一組或是多組 IP 位址至 WAN 介面。

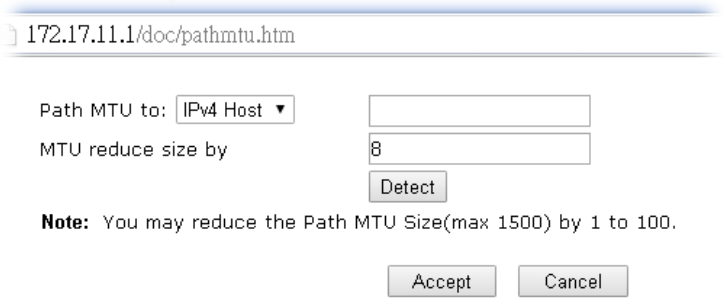
若要使用**固定或動態 IP(Static or Dynamic IP)**爲網際網路的連線協定，請自 **WAN** 中選擇**網際網路連線(Internet Access)**，接著選擇**固定或動態 IP(Static or Dynamic IP)**，即可出現下圖。



可用設定說明如下：

項目	說明
啓用/停用(Enable / Disable)	按下**啓用(Enable)**按鈕可啓動此功能，如果您選的是**停用(Disable)**，此項功能將會關閉，全部調整過的設定也都將立即失效。
IP 網路設定(IP Network Settings)	本區讓您自動取得 IP 位址或是手動輸入需求的 IP 位址。 **自動取得 IP 位址(Obtain an IP address automatically)** – 如果您想要使用**動態 IP** 模式，按此鈕以自動取得 IP 位址。 **更多選項(More Options)** - 顯示更多的設定選項。 ● **路由器名稱(Router Name)**: 輸入 ISP 的路由器名稱。 ● **網域功能變數名稱(Domain Name)**: 輸入指定的網

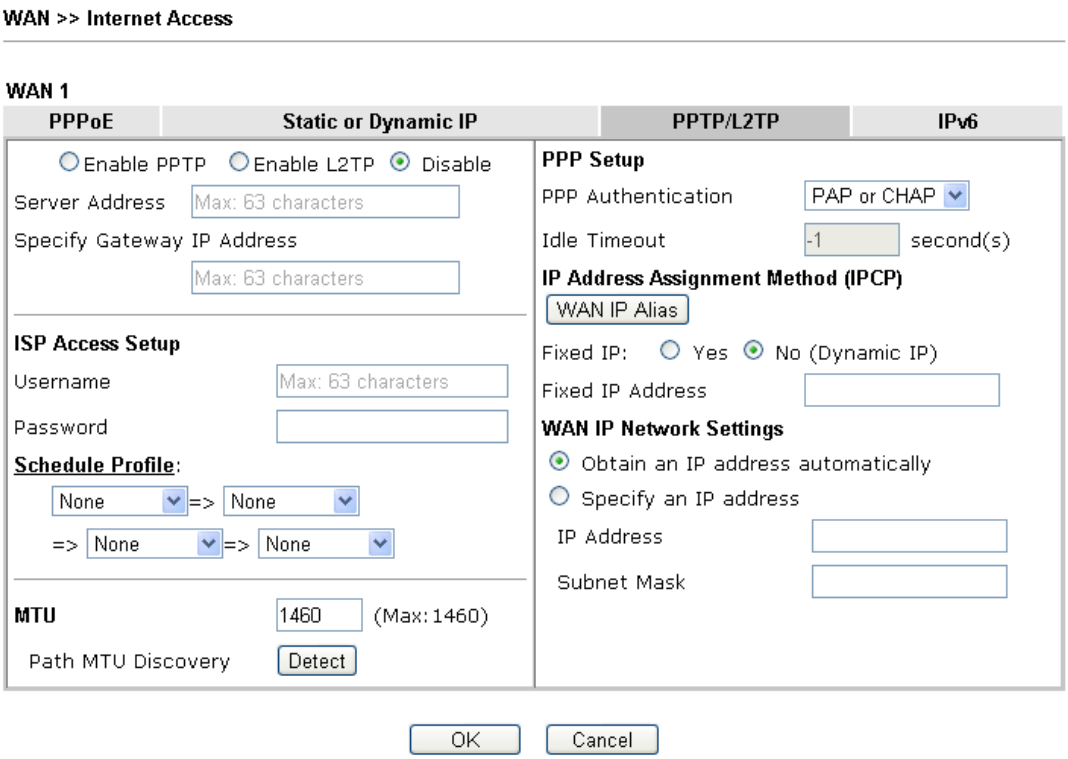
	域功能變數名稱。 ● **啓用 DHCP 用戶端辨識(Enable DHCP Client Identifier):** 勾選此框指定使用者名稱與密碼，做爲某些 ISP 需求的 DHCP 用戶端辨識之用。 ● **使用者名稱(Username):** 輸入任何名稱，最大長度不要超過 63 個字元。 ● **密碼(Password):** 輸入任何密碼，最大長度不要超過 62 個字元。 **指定 IP 位址(Specify an IP address)** – 按此鈕指定 IP 位址讓資料通過。 ● **IP 位址(IP Address)**:輸入 IP 位址。 ● **子網路遮罩(Subnet Mask)**:輸入子網路遮罩。 ● **閘道 IP 位址(Gateway IP Address)**: 輸入閘道 IP 位址。 **WAN IP 別名(WAN IP Alias)** - 如果您有多個真實 IP 位址，想要在 WAN 介面上利用這些 IP，請使用 WAN IP 別名。除了目前使用的 IP 外，您還可以另外設定 32 組真實 IP。
DNS 伺服器 IP 位址 (DNS Server IP Address)	若要使用固定 IP 模式，請輸入路由器的主要 IP 位址，如有必要，在將來，您也可以輸入次要 IP 位址以符合所需。
WAN 連線檢測(WAN Connection Detection)	這個功能讓您檢查目前網路是否還在連線中。可透過 ARP 檢測或是 Ping Detect 來完成。 **模式(Mode)** – 選擇 **ARP 檢測(ARP Detect)或 Ping 檢測(Ping Detect)或是永遠連線(Always On)**執行 WAN 檢測動作。 ● **主要/次要 Ping IP (Primary/Secondary Ping IP)** – 若您選擇了 **Ping 偵測(Ping Detect)** 作爲偵測模式，您必須在本區輸入主要或是次要 IP 位址。 ● **Ping 閘道 IP(Ping Gateway IP)** – 若您選擇了 **Ping 檢測 (Ping Detect)** 作爲偵測模式，您也可以啓用此設定，以便使用目前的 WAN 閘道做爲 ping IP 位址。 藉由 IP 位址 ping，路由器可以檢查該 WAN 連線是啓用的或是中斷的。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。 ● **Ping 間隔(Ping Interval) –** 輸入執行 Ping 操作系統所需要的時間間隔。 ● **Ping 重試(Ping Retry) –** 輸入判斷 WAN 連線中斷之前，系統執行 Ping 操作時容許的嘗試次數。
MTU	代表封包的最大傳輸單位。 **路徑 MTU 搜尋(Path MTU Discovery)** – 用於偵測封包在特定傳輸路徑當中，不被分段的最大 MTU 尺寸。 按**檢測(Detect)** 開啓如下頁面：to open the following dialog.

	 ● **路徑最大傳輸單位至(Path MTU to)** – 輸入 IP 位址作爲特定傳輸路徑。 ● **MTU 值之降低乃透過(MTU reduce size by)** – 決定 MTU 值得降低大小，例如此區指定數字爲 8，最大的 MTU 大小爲 1500，在您按下檢測按鈕之後，系統將會計算並取得適合的 MTU 值，像是 1500、1492、1484 等等。 ● **檢測(Detect)** – 按此檢測出適合的 MTU 值。 ● **接受(Accept)** – 選了此項之後，檢測得到的值會顯示在 MTU 欄位中。
維持 WAN 連線 **(Keep WAN Connection)**	正常情況下，這個功能是設計用來符合動態 IP 環境，因爲某些 ISP 會在一段時間沒有任何回應時中斷連線。請勾選**啓用 PING 以保持常態連線(Enable PING to keep alive)**。 ● **PING 到指定的 IP (PING to the IP)**– 如果您啓用此功能，請指定 IP 位址讓系統可以 PING 到該 IP 以保持連線 ● **PING 間隔(PING Interval)** - 輸入間隔時間讓系統得以執行 PING 動作。
TTL	**變更 TTL 值(Change the TTL value) -**啓用或是停用封包透過路由器傳輸時的 TTL 功能。 ● **若勾選** – TTL 值會在通過路由器時降低(-1)，這會讓透過路由器存取網際網路的用戶端，在 TTL 的數值變爲 0 的時候，直接被指定 ISP 封鎖住。 ● **若未勾選** – TTL 值不會減少，之後當封包透過路由器傳送時，就不會被取消。也就是說，傳送此封包的用戶端並不會被 ISP 業者封鎖住。
RIP 協定 **(RIP Protocol)**	指名路由器是如何變更路由表格資訊，勾選**啓用 RIP(Enable RIP)**此項目以啓動此功能。
橋接模式(Bridge Mode)	**啓用橋接模式(Enable Bridge Mode)** – 若啓用此功能，路由器可以當成橋接數據機來運作。 **啓用防火牆(Enable Firewall)** – 啓用橋接模式後，此功能亦可使用。當橋接模式與防火牆皆啓用時，在使用者管理下方的使用者設定檔內的設定將被忽略不計。而防火牆功能單中所定義並啓用的過濾器規則取而代之。 **橋接子網(Bridge Subnet)** – 在選定的 LAN 子網與此 WAN 介面之間建立橋接連線。
MAC 位址(MAC Address)	**預設 MAC 位址(Default MAC Address)**: 按此以使用路由器的預設 MAC 位址。 **指定 MAC 位址(Specify a MAC Address)**: 某些纜線服務供應商會指定一個 MAC 位址以應存取驗證。在此情況下，您需要按此鈕並輸入 MAC 位址。

完成上述設定之後，按下**確定(OK)**儲存設置內容。

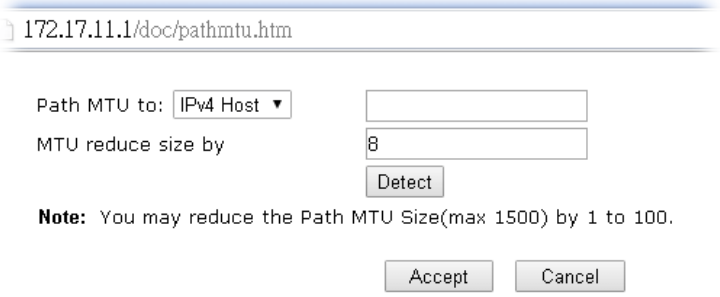
II-1-2-3 WAN1/WAN2 中的 PPTP/L2TP 模式細節設定(實體模式：乙太網路)

若要使用 **PPTP/L2TP** 爲網際網路的連線協定，請自 **WAN** 中選擇**網際網路連線(Internet Access)**，接著選擇 **PPTP/L2TP**，即可出現下圖。



可用設定說明如下：

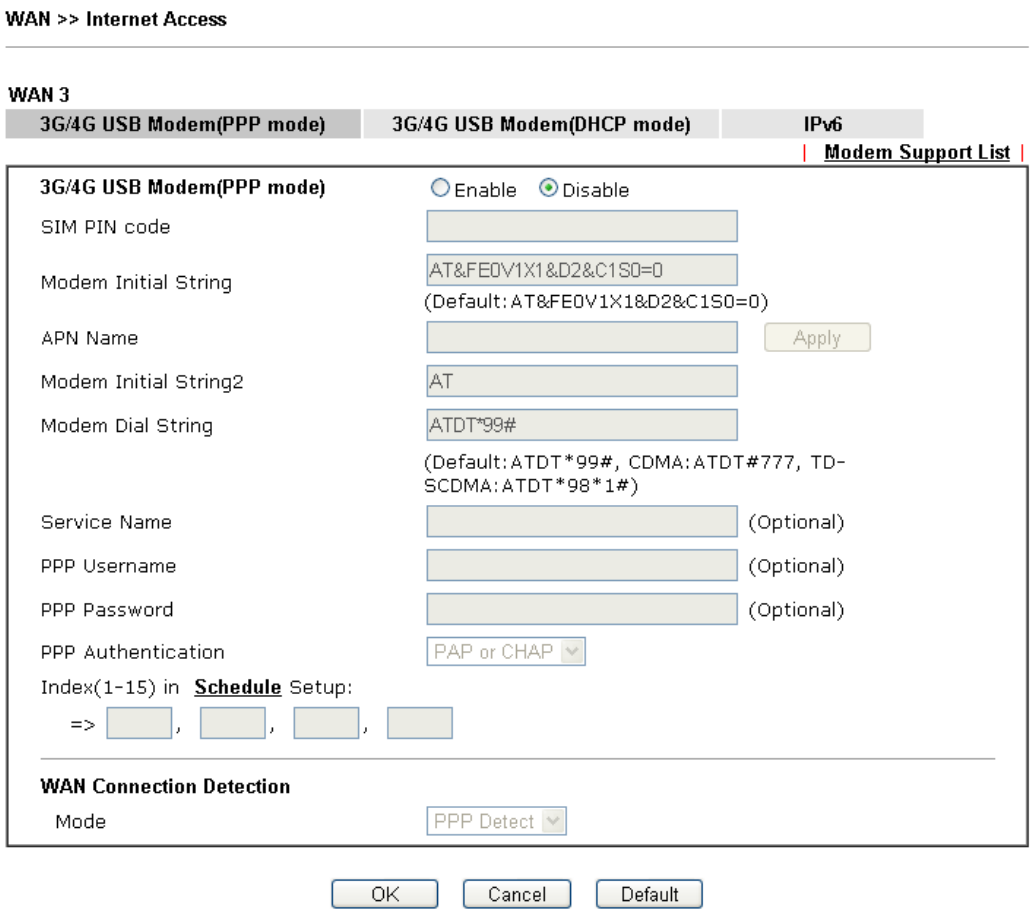
項目	說明
PPTP/L2TP	**啓用 PPTP(Enable PPTP)** - 選擇此鈕已啓用 PPTP 用戶端建立通往 WAN 介面的 DSL 數據機之通道。 **啓用 L2TP(Enable L2TP)** - 選擇此鈕已啓用 L2TP 用戶端建立通往 WAN 介面的 DSL 數據機之通道。 **停用(Disable)** - 選擇此鈕停用 PPTP 或 L2TP 連線通道。 **伺服器位址(Server Address)** - 指定 PPTP/ L2TP 伺服器的 IP 位址。 **指定閘道 IP 位址(Specify Gateway IP Address)** - 針對 PTP/L2TP 伺服器指定閘道 IP 位址。
ISP 存取設定 (ISP Access Setup)	**使用者名稱(Username)** - 輸入 ISP 業者提供給您的使用者名稱。 **密碼(Password)** - 輸入 ISP 業者提供的密碼。 **排程設定檔(Schedule Profile) -** 您可以輸入四組時間排程設定，所有的排程都是在時間**其他應用>>排程設定(Application >> Schedule)**網頁中事先設定完畢，您可直接輸入該時間排程的號碼即可。
MTU	代表封包的最大傳輸單位。 **路徑 MTU 搜尋(Path MTU Discovery)** – 用於偵測封包在特定傳輸路徑當中，不被分段的最大 MTU 尺寸。

	按**檢測(Detect)** 開啓如下頁面：to open the following dialog.  ● **路徑最大傳輸單位至(Path MTU to)** – 輸入 IP 位址作爲特定傳輸路徑。 ● **MTU 值之降低乃透過(MTU reduce size by)** – 決定 MTU 值得降低大小，例如此區指定數字爲 8，最大的 MTU 大小爲 1500，在您按下檢測按鈕之後，系統將會計算並取得適合的 MTU 值，像是 1500、1492、1484 等等。 ● **檢測(Detect)** – 按此檢測出適合的 MTU 值。 ● **接受(Accept)** – 選了此項之後，檢測得到的值會顯示在 MTU 欄位中。
PPP 設定 **(PPP Setup)**	**PPP 驗證(PPP Authentication)** – 選擇 **PAP** 或是 **PAP 或 CHAP**。 **閒置逾時(Idle Timeout)** - 閒置逾時表示路由器在一段時間內都沒有運作時，就會中斷連線。
IP 位址指派方式 (IPCP) **(IP Address Assignment Method(IPCP)**	**WAN IP 別名(WAN IP Alias)** - 如果您有多個真實 IP 位址，想要在 WAN 介面上利用這些 IP，請使用 WAN IP 別名。除了目前使用的 IP 外，您還可以另外設定 8 組真實 IP，要注意的是，本項設定僅針對 WAN1 有效用。 **固定 IP(Fixed IP)** - 通常每一次您要求連線時，ISP 會浮動指定 IP 位址給您使用，但在某些情況下，ISP 總是提供相同的 IP 位址予您，因此您可以在固定 IP 位址區域中輸入此 IP 位址，在您輸入並使用此項功能之前，請先聯絡您的 ISP 業者取得相關資訊，再選擇**是**並輸入固定 IP 位址以便使用。 **固定 IP 位址(Fixed IP Address)** – 請輸入固定 IP 位址。
WAN IP 網路設定 **(WAN IP Network Settings)**	**自動取得 IP 位址(Obtain an IP address automatically)** – 按此鈕以自動取得 IP 位址。 **指定 IP 位址(Specify an IP address)** – 按此鈕以指定 IP 位址。 ● **IP 位址(IP Address)** – 輸入 IP 位址。 ● **子網路遮罩(Subnet Mask)** – 輸入子網路遮罩。

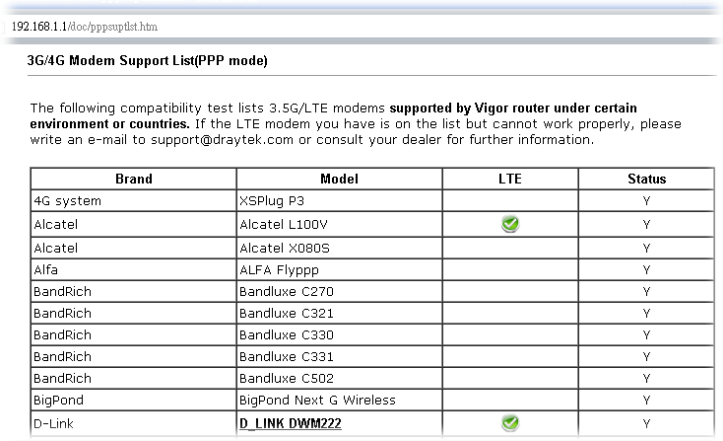
完成上述設定之後，按下**確定(OK)**儲存設置內容。

II-1-2-4 WAN3/WAN4 中的 3G/4G USB 數據機模式細節設定(PPP 模式)

如果要使用 3G/4G USB 數據機 (PPP 模式) (針對 3G/4G USB 數據機) 做爲網際網路連線協定，請自 **WAN** 中選擇**網際網路連線(Internet Access)**，接著在 WAN2 介面上選擇 **3G/4G USB 數據機 (PPP 模式)(3G/4G USB Modem (PPP mode))**，即可出現下圖。



可用設定說明如下：

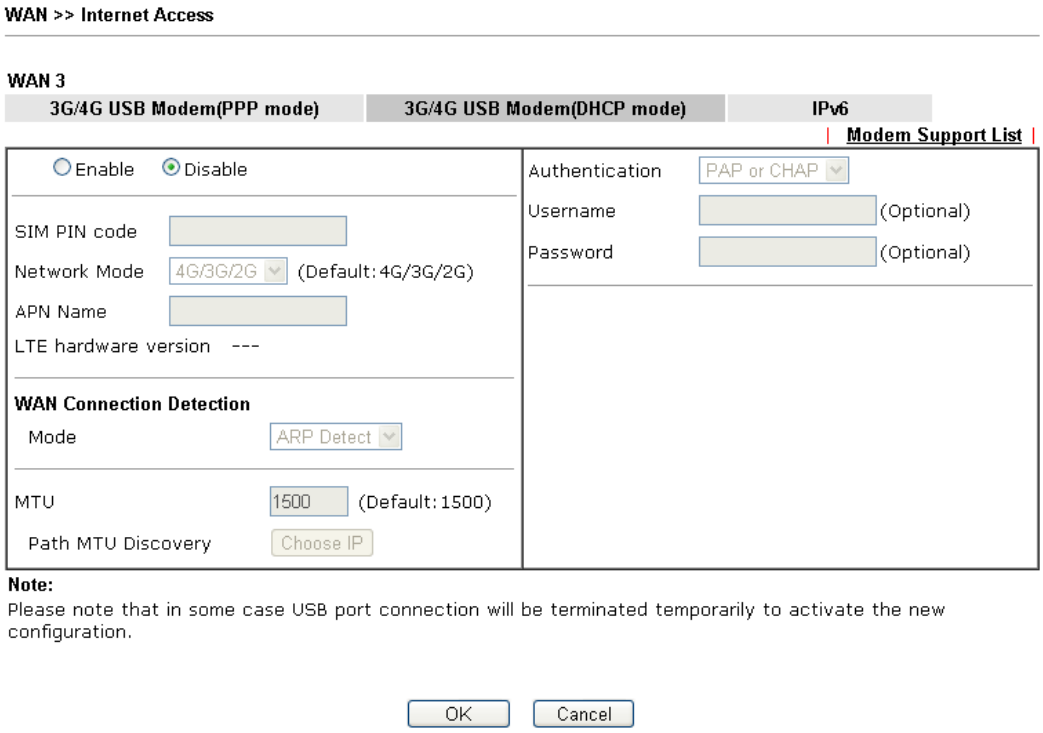
項目	說明
數據機支援清單(Modem Support List)	條列路由器支援的所有數據機。 
3G /4G USB 數據機 (PPP 模式)	選擇**啓用(Enable)**，開啓此功能。如果您選的是**停用(Disable)**，此功能將不再運作，所有設定也都會失效。
SIM PIN 碼(SIM PIN code)	輸入 SIM 卡 PIN 碼，以便連線網際網路。

數據機初始化字串(Modem Initial String)	這個數值，用來初始化 USB 數據機，請使用預設值，如果您有任何疑問，請與當地 ISP 業者聯絡。
APN 名稱(APN Name)	APN 代表接入點名稱(Access Point Name)是由您的 ISP 所提供的，必要時請輸入 ISP 提供的資料，然後按下**套用(Apply)**即可。
數據機初始化字串 2(Modem Initial String2)	初始化字串 1 是與 APN 搭配使用。 但在某些情況下，使用者可能會使用另外的初始化 AT 指令來限制 3G 頻寬或是其他特殊事宜。此時即可設定第二個數據機初始化字串。
數據機撥號字串(Modem Dial String)	這個數值，目的是在 USB 模式下撥號使用，請使用預設值，如果您有任何疑問，請與當地 ISP 業者聯絡。
服務名稱(Service Name)	輸入指定網路服務的相關說明。
PPP 使用者(PPP Username)	輸入 PPP 使用者名稱 (視您實際需要而設定)。
PPP 密碼(PPP Password)	輸入 PPP 密碼 (視您實際需要而設定)。
PPP 驗證(PPP Authentication)	選擇 **PAP** 或是 **PAP 或 CHAP**。
索引號碼(1-15)	可以輸入四組時間排程，全部的排程都是在**其他應用>>排程(Application >> Schedule)**網頁中事先設定完畢，您可在此輸入該排程的索引編號。
WAN 連線檢測(WAN Connection Detection)	這個功能讓您檢查目前網路是否還在連線中。可透過 ARP 檢測或是 Ping Detect 來完成。 **模式(Mode)** – 選擇 **ARP 檢測(ARP Detect)或 Ping 檢測(Ping Detect)**執行 WAN 檢測動作。 ● **主要/次要 Ping IP (Primary/Secondary Ping IP)** – 若您選擇了 **Ping 偵測(Ping Detect)** 作爲偵測模式，您必須在本區輸入主要或是次要 IP 位址。 ● **Ping 閘道 IP(Ping Gateway IP)** – 若您選擇了 **Ping 檢測(Ping Detect)** 作爲偵測模式，您也可以啓用此設定，以便使用目前的 WAN 閘道做爲 ping IP 位址。 藉由 IP 位址 ping，路由器可以檢查該 WAN 連線是啓用的或是中斷的。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。 ● **Ping 間隔(Ping Interval) –** 輸入執行 Ping 操作系統所需要的時間間隔。 ● **Ping 重試(Ping Retry) –** 輸入判斷 WAN 連線中斷之前，系統執行 Ping 操作時容許的嘗試次數。

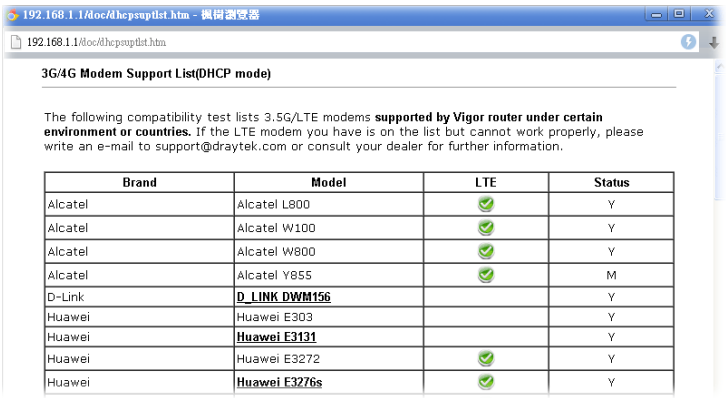
完成上述設定之後，按下**確定(OK)**儲存設置內容。

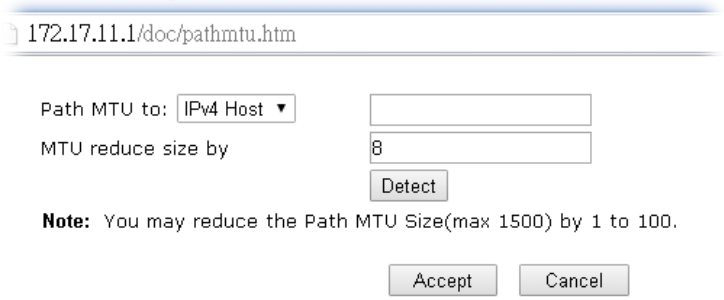
II-1-2-5 WAN3/WAN4 中的 3G/4G USB 數據機模式細節設定(DHCP 模式)

欲使用 3G/4G USB 數據機(DHCP 模式)作爲網際網路的存取協定，請開啓 **WAN>>網際網路連線(WAN>>Internet Access)**，然後自 WAN3/WAN4 連線模式下拉式清單中選擇 **3G/4G USB 數據機(DHCP 模式)**。接著即可看見如下頁面：



可用設定說明如下：

項目	說明
數據機支援清單(Modem Support List)	條列路由器支援的所有數據機。 
3G/4G USB 數據機(DHCP 模式)	按**啓用(Enable)**啓動此功能，如果您選擇**停用(Disable)**，此功能將會關閉，所有本頁的設定也將立即失效。
SIM PIN 碼(SIM PIN code)	輸入 SIM 卡 PIN 碼，以便連線網際網路。
網路連線模式(Network Mode)	路由器將以此處所選擇的模式進行網路連線，如果您選擇 4G/3G/2G，路由器將依據實際的無線網路訊號自行挑選適合的模式。
APN 名稱(APN Name)	APN 代表接入點名稱(Access Point Name)是由您的 ISP 所提供的，必要時請輸入 ISP 提供的資料，然後按下**套用**即可。

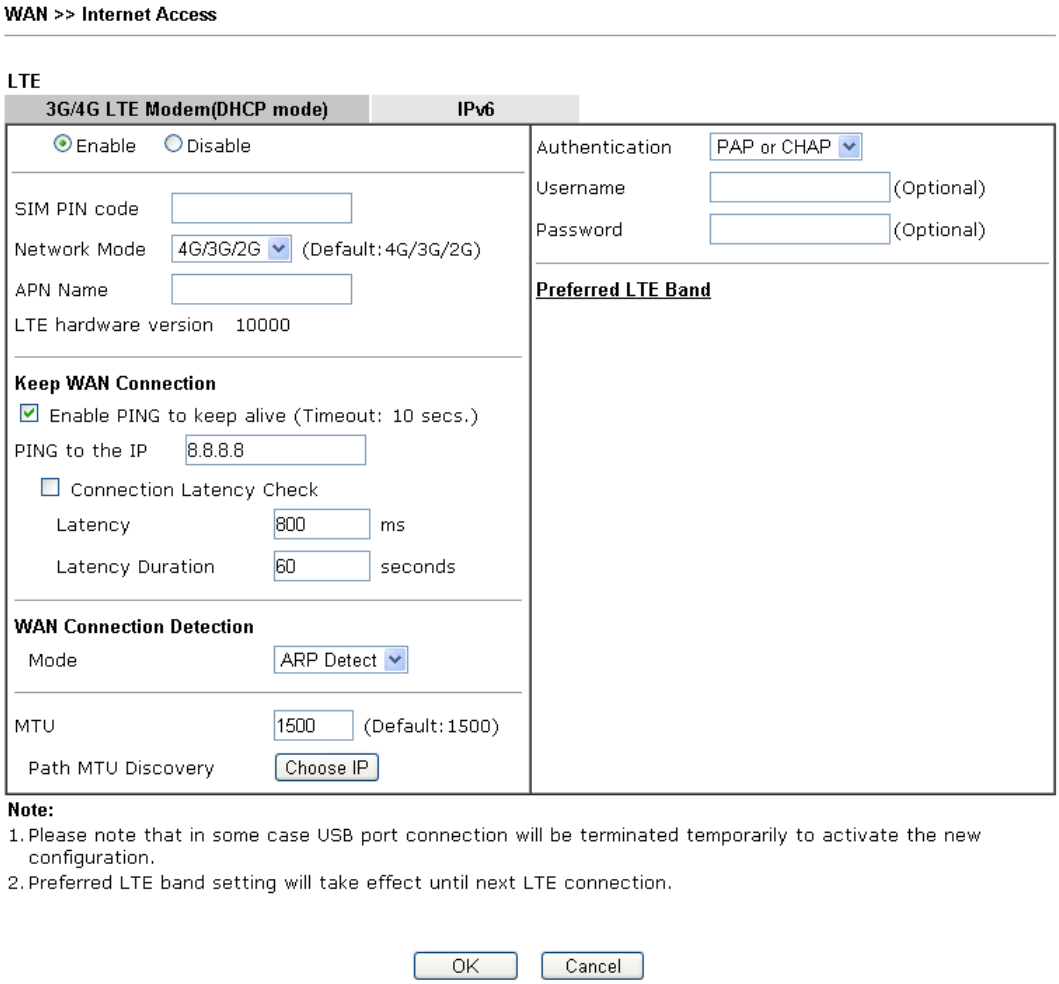
WAN 連線檢測(WAN Connection Detection)	這個功能讓您檢查目前網路是否還在連線中。可透過 ARP 檢測或是 Ping Detect 來完成。 **模式(Mode)** – 選擇 **ARP 檢測(ARP Detect)或 Ping 檢測(Ping Detect)**執行 WAN 檢測動作。 ● **主要/次要 Ping IP (Primary/Secondary Ping IP)** – 若您選擇了 **Ping 偵測(Ping Detect)** 作爲偵測模式，您必須在本區輸入主要或是次要 IP 位址。 ● **Ping 閘道 IP(Ping Gateway IP)** – 若您選擇了 **Ping 檢測(Ping Detect)** 作爲偵測模式，您也可以啓用此設定，以便使用目前的 WAN 閘道做爲 ping IP 位址。 藉由 IP 位址 ping，路由器可以檢查該 WAN 連線是啓用的或是中斷的。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。 ● **Ping 間隔(Ping Interval) –** 輸入執行 Ping 操作系統所需要的時間間隔。 ● **Ping 重試(Ping Retry) –** 輸入判斷 WAN 連線中斷之前，系統執行 Ping 操作時容許的嘗試次數。
MTU	代表封包的最大傳輸單位。 **路徑 MTU 搜尋(Path MTU Discovery)** – 用於偵測封包在特定傳輸路徑當中，不被分段的最大 MTU 尺寸。 按**檢測(Detect)** 開啓如下頁面：  ● **路徑最大傳輸單位至(Path MTU to)** – 輸入 IP 位址作爲特定傳輸路徑。 ● **MTU 值之降低乃透過(MTU reduce size by)** – 決定 MTU 值得降低大小，例如此區指定數字爲 8，最大的 MTU 大小爲 1500，在您按下檢測按鈕之後，系統將會計算並取得適合的 MTU 值，像是 1500、1492、1484 等等。 ● **檢測(Detect)** – 按此檢測出適合的 MTU 值。 ● **接受(Accept)** – 選了此項之後，檢測得到的值會顯示在 MTU 欄位中。
驗證(Authentication)	選擇 **PAP** 或是 **PAP 或 CHAP**。 **使用者名稱(Username)** – 輸入驗證需求之使用者名稱。 **密碼(Password)** – 輸入驗證需求之密碼。

完成上述設定之後，按下**確定(OK)**儲存設置內容。

II-1-2-6 LTE WAN 中的 3G/4G USB 數據機模式細節設定(DHCP 模式)

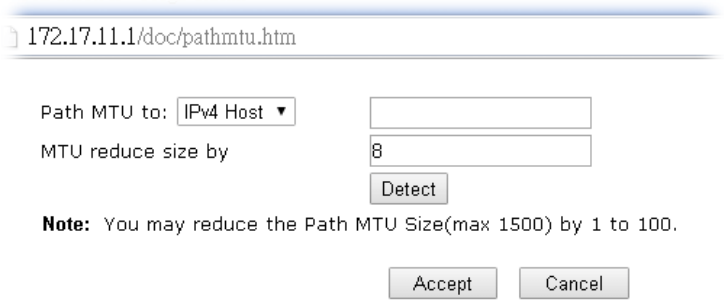
這個模式僅適用“L”機型。LTE WAN 使用內嵌的 LTE 模組以存取網際網路。

欲使用 3G/4G USB 數據機(DHCP 模式)作爲網際網路的存取協定，請開啓 **WAN>>網際網路連線(WAN>>Internet Access)**，然後自 LTE 連線模式下拉式清單中選擇 **3G/4G USB 數據機(DHCP 模式)**。接著即可看見如下頁面：



可用設定說明如下：

項目	說明
3G/4G USB 數據機 (DHCP 模式)	按**啓用(Enable)**啓動此功能，如果您選擇**停用(Disable)**，此功能將會關閉，所有本頁的設定也將立即失效。
SIM PIN 碼(SIM PIN code)	輸入 SIM 卡 PIN 碼，以便連線網際網路。
網路連線模式(Network Mode)	路由器將以此處所選擇的模式進行網路連線，如果您選擇 4G/3G/2G，路由器將依據實際的無線網路訊號自行挑選適合的模式。
APN 名稱(APN Name)	APN 代表接入點名稱(Access Point Name)是由您的 ISP 所提供的，必要時請輸入 ISP 提供的資料，然後按下**套用(Apply)**即可。
LTE 硬體版本(LTE hardware version)	內嵌 LTE 模組的硬體版本。
維持 WAN 連線(Keep WAN Connection)	正常情況下，這個功能設計主要是因應動態 IP 環境，因爲某些 ISP 會在一段時間沒有任何回應時中斷連線。請勾選**啓用 PING**

	以保持連線(Enable PING to keep alive)。 **啓用 PING 以維持連線(Enable PING to Keep alive)** –如果您啓用此功能，必須指定一個 IP 位址讓系統可以 PING 到該 IP 以保持連線。系統將於每秒發送封包至該 IP 位址，若在 10 秒內未收到任何回覆訊息，路由器便會中斷 LTE 連線，再重新撥接 LTE 直到連線爲止。 ● **PING 到指定的 IP (PING to the IP)**– 請輸入 IP 位址。 **連線延遲檢查(Connection Latency Check)** – 啓用封包回覆需求的延遲時間設定。啓用此功能時，系統會等待來自指定 IP 的封包回覆。當等待封包回覆的時間達到門檻值(latency，預設 800 微秒)值，且持續一段時間(Latency Duration，預設 60 秒)，路由器便會重新啓動 LTE 模組直到連線爲止。 ● **延遲(Latency)** – 設定封包回覆的時間門檻。 ● **延遲期間(Latency Duration)** – 設定持續時間。
WAN 連線檢測(WAN Connection Detection)	這個功能讓您檢查目前網路是否還在連線中。可透過 ARP 檢測或是 Ping Detect 來完成。 **模式(Mode)** – 選擇 **ARP 檢測(ARP Detect)或 Ping 檢測(Ping Detect)**執行 WAN 檢測動作。 ● **主要/次要 Ping IP (Primary/Secondary Ping IP)** – 若您選擇了 **Ping 偵測(Ping Detect)** 作爲偵測模式，您必須在本區輸入主要或是次要 IP 位址。 ● **Ping 閘道 IP(Ping Gateway IP)** – 若您選擇了 **Ping 檢測(Ping Detect)** 作爲偵測模式，您也可以啓用此設定，以便使用目前的 WAN 閘道做爲 ping IP 位址。 藉由 IP 位址 ping，路由器可以檢查該 WAN 連線是啓用的或是中斷的。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。 ● **Ping 間隔(Ping Interval) –** 輸入執行 Ping 操作系統所需要的時間間隔。 ● **Ping 重試(Ping Retry) –** 輸入判斷 WAN 連線中斷之前，系統執行 Ping 操作時容許的嘗試次數。
MTU	代表封包的最大傳輸單位。 **路徑 MTU 搜尋(Path MTU Discovery)** – 用於偵測封包在特定傳輸路徑當中，不被分段的最大 MTU 尺寸。 按**選擇 IP(Choose IP)** 開啓如下頁面：  ● **路徑最大傳輸單位至(Path MTU to)** – 輸入 IP 位址作爲特定傳輸路徑。 ● **MTU 值之降低乃透過(MTU reduce size by)** – 決定 MTU 值得降低大小，例如此區指定數字爲 8，最大的 MTU 大小爲 1500，在您按下檢測按鈕之後，系統將會計算並取得適

	合的 MTU 值，像是 1500、1492、1484 等等。 ● **檢測(Detect)** – 按此檢測出適合的 MTU 值。 ● **接受(Accept)** – 選了此項之後，檢測得到的值會顯示在 MTU 欄位中。
驗證(Authentication)	選擇 **PAP** 或是 **PAP 或 CHAP**。
使用者名稱(Username)	輸入 PPP 使用者名稱 (視您實際需要而設定)。
密碼(Password)	輸入 PPP 密碼 (視您實際需要而設定)。

完成上述設定之後，按下**確定(OK)**儲存設置內容。

II-1-2-7 WAN1/WAN2/WAN3/WAN4 的斷線模式細節設定(IPv6)

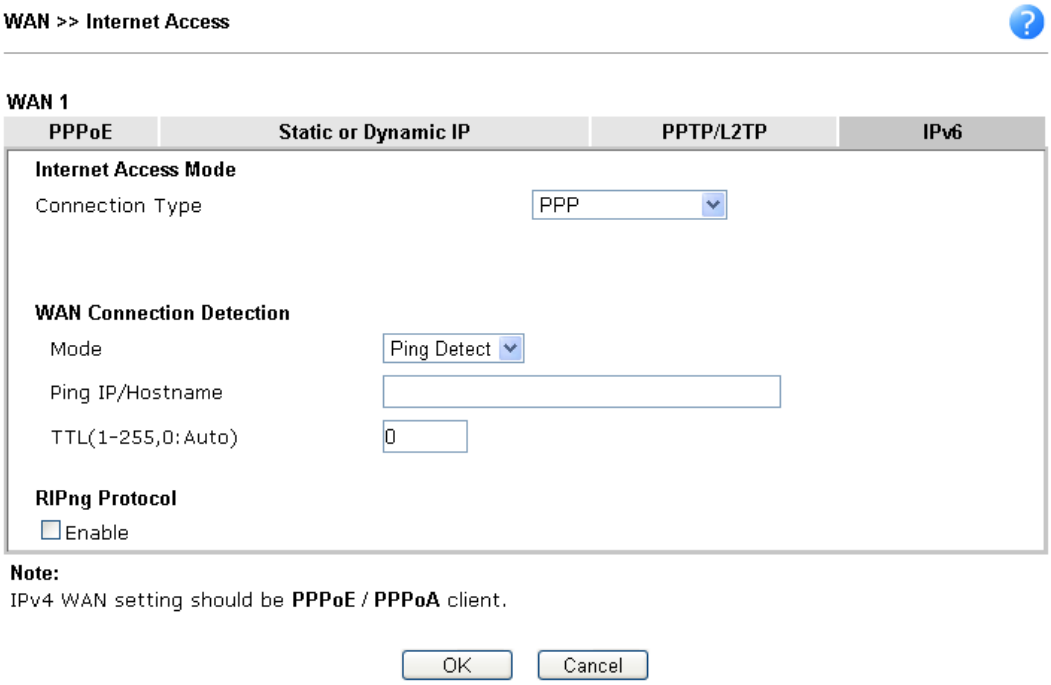
當選擇斷線(Offline)類型時，IPv6 連線是中斷的。



II-1-2-8 WAN1/WAN2 的 PPP 模式細節設定(IPv6)

在 IP4v4 PPPoE 連線中，我們可以在閘道器與 Vigor 路由器之間透過 IPv6CP 取得 IPv6 連線的本地位址。之後，使用 DHCPv6 或是接受 RA 來取得 IPv6 的前置碼位址(像是 2001:B010:7300:200::/64 等)，這些是由 ISP 所提供的。另外，在區域網路端的電腦也可以透過處理過的前置碼而擁有實際 IPv6 位址以便存取網際網路。

在 PPP 模式之下，不需進行任何設定。



可用設定說明如下：

項目	說明
WAN 連線檢測(WAN Connection Detection)	這個功能讓您檢查目前網路是否還在連線中。可透過 Ping Detect 來完成。 **模式(Mode)** – 選擇**永遠連線(Alaways On)或 Ping 檢測(Ping Detect)**執行 WAN 檢測動作。**永遠連線(Always On)**表示無需進行任何檢測，網路永遠連線。 ● **Ping IP/主機(Ping IP/Hostname)** – 若您選擇了 **Ping 檢測(Ping Detect)** 作爲偵測模式，您必須在本區輸入 IP 位址或主機名稱。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。
RIPng 通訊協定(RIPng Protocol)	下一代 RIP(RIPng) 提供與 IPv4 RIP v2 相同的功用。

下圖顯示 PPP 模式下，成功的 IPv6 連線運作範例圖。



資訊

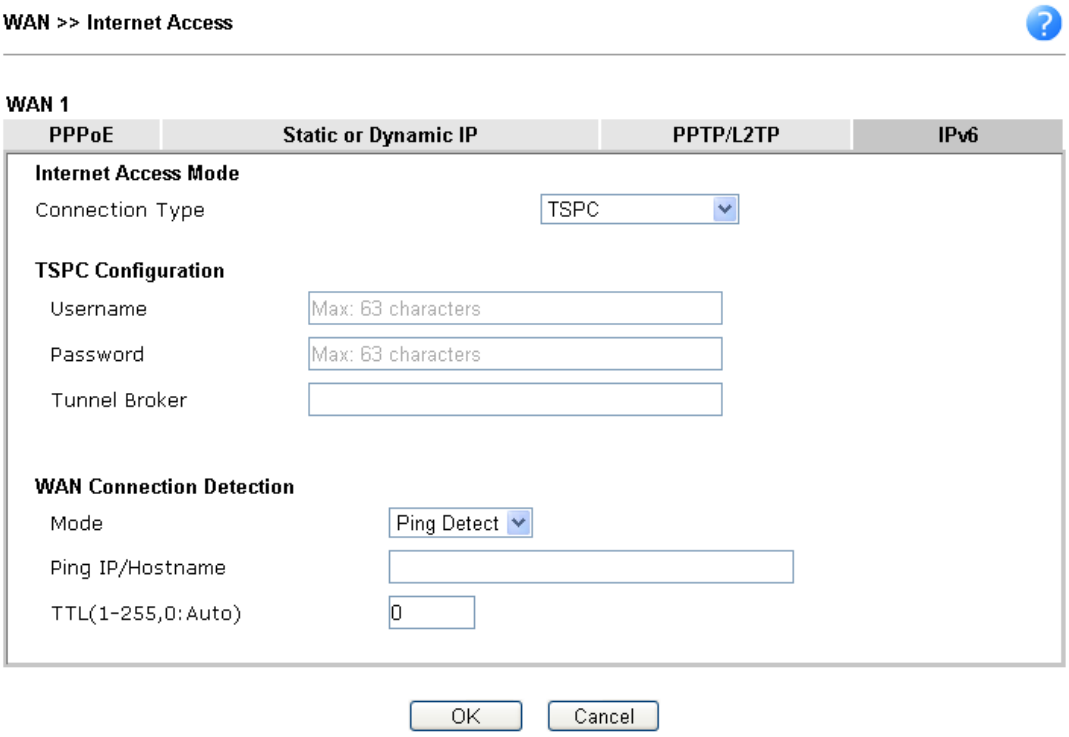
目前，IPv6前置碼可透過某些地區例如台灣(hinet)、荷蘭、澳洲及英國提供的PPP模式連線來取得。

II-1-2-9 WAN1/WAN2/WAN3/WAN4 的 TSPC 模式細節設定(IPv6)

TSPC(Tunnel setup protocol client)是一種應用，可幫助您輕鬆連至 IPv6 網路。

請先確認您的 IPv4 WAN 連線是可行的，並自 hexago (http://gogonet.gogo6.com/page/freenet6-account)此處先免費取得帳號，再來使用此連線。TSPC 可連接通道代理人(tunnel broker)並依照設定檔案內的規格來要求一條通道。這個模式可以自通道代理人處取得實際 IPv6 IP 位址以及前置碼，然後在背景處監督整個通道的資料運輸狀況。

在您取得 IPv6 前置碼並開始 RADVD 之後，路由器後方的電腦就可以直接連接到 IPv6 並登上網際網路。

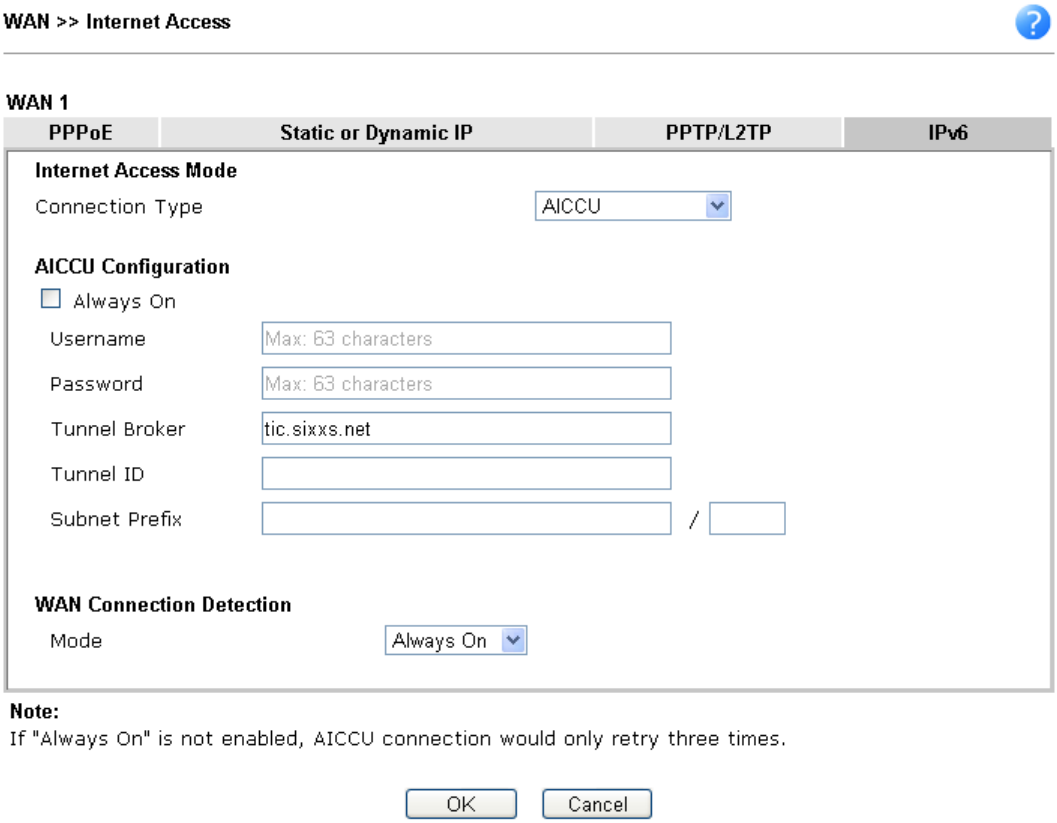


可用設定說明如下：

項目	說明
使用者名稱(Username)	輸入您自通道代理人取得的名稱，建議您先進入此網站 http://gogonet.gogo6.com/page/freenet6-account 申請一個使用者名稱以及密碼。
密碼(Password)	請輸入搭配使用者名稱所分派的密碼。
通道代理人(Tunnel Broker)	輸入通道代理人的的 IP 位址、FQDN 或是選項埠號。
WAN 連線檢測(WAN Connection Detection)	這個功能讓您檢查目前網路是否還在連線中。可透過 Ping Detect 來完成。 **模式(Mode)** – 選擇**永遠連線(Alaways On)或 Ping 檢測(Ping Detect)**執行 WAN 檢測動作。**永遠連線(Alaways On)**表示無需進行任何檢測，網路永遠連線。 ● **Ping IP/主機(Ping IP/Hostname)** – 若您選擇了 **Ping 檢測(Ping Detect)** 作爲偵測模式，您必須在本區輸入 IP 位址或主機名稱。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。

完成上述設定之後，按下**確定(OK)**儲存設置內容。

II-1-2-10 WAN1/WAN2/WAN3/WAN4 的 AICCU 模式細節設定(IPv6)



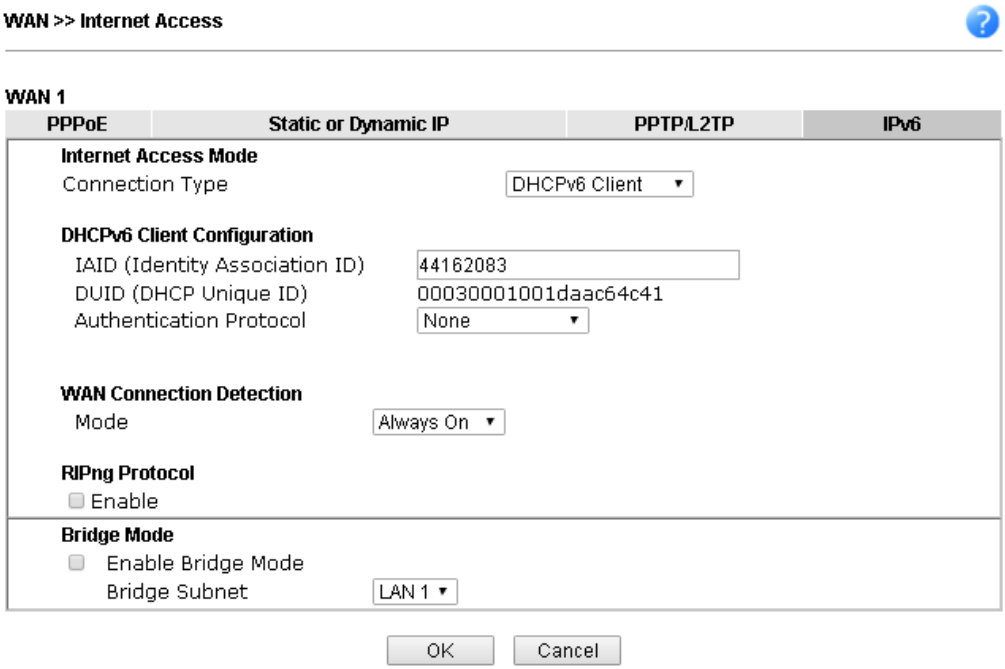
可用設定說明如下：

項目	說明
永遠連線(Always On)	勾選此方塊讓系統隨時保持連線。
使用者名稱(Username)	輸入通道代理人提供的名稱，請先自此網站 http://www.sixxs.net/申請使用者名稱與密碼。
密碼(Password)	請輸入搭配使用者名稱所分派的密碼。
通道代理人(Tunnel Broker)	輸入通道代理人的的 IP 位址、FQDN 或是選項埠號。
通道 ID(Tunnel ID)	一個使用者帳號可以有數個通道，每個通道可擁有一個指定的 ID (例如 T115394)。
子網前置碼(Subnet Prefix)	輸入取自服務供應商的子網前置碼。
WAN 連線檢測(WAN Connection Detection)	這個功能讓您檢查目前網路是否還在連線中。可透過 Ping Detect 來完成。 **模式(Mode)** - 選擇**永遠連線(Alaways On)或 Ping 檢測(Ping Detect)**執行 WAN 檢測動作。**永遠連線(Always On)**表示無需進行任何檢測，網路永遠連線。 ● **Ping IP/主機(Ping IP/Hostname)** - 若您選擇了 **Ping 檢測(Ping Detect)** 作爲偵測模式，您必須在本區輸入 IP 位址或主機名稱。 ● **TTL (Time to Live)** - 設定 ping 操作需要的 TTL 數值。

完成上述設定之後，按下**確定(OK)**儲存設置內容。

II-1-2-11 WAN1/WAN2 的 DHCPv6 用戶端模式細節設定(IPv6)

DHCPv6 用戶端模式可使用 DHCPv6 協定以便自伺服器取得 IPv6 位址。



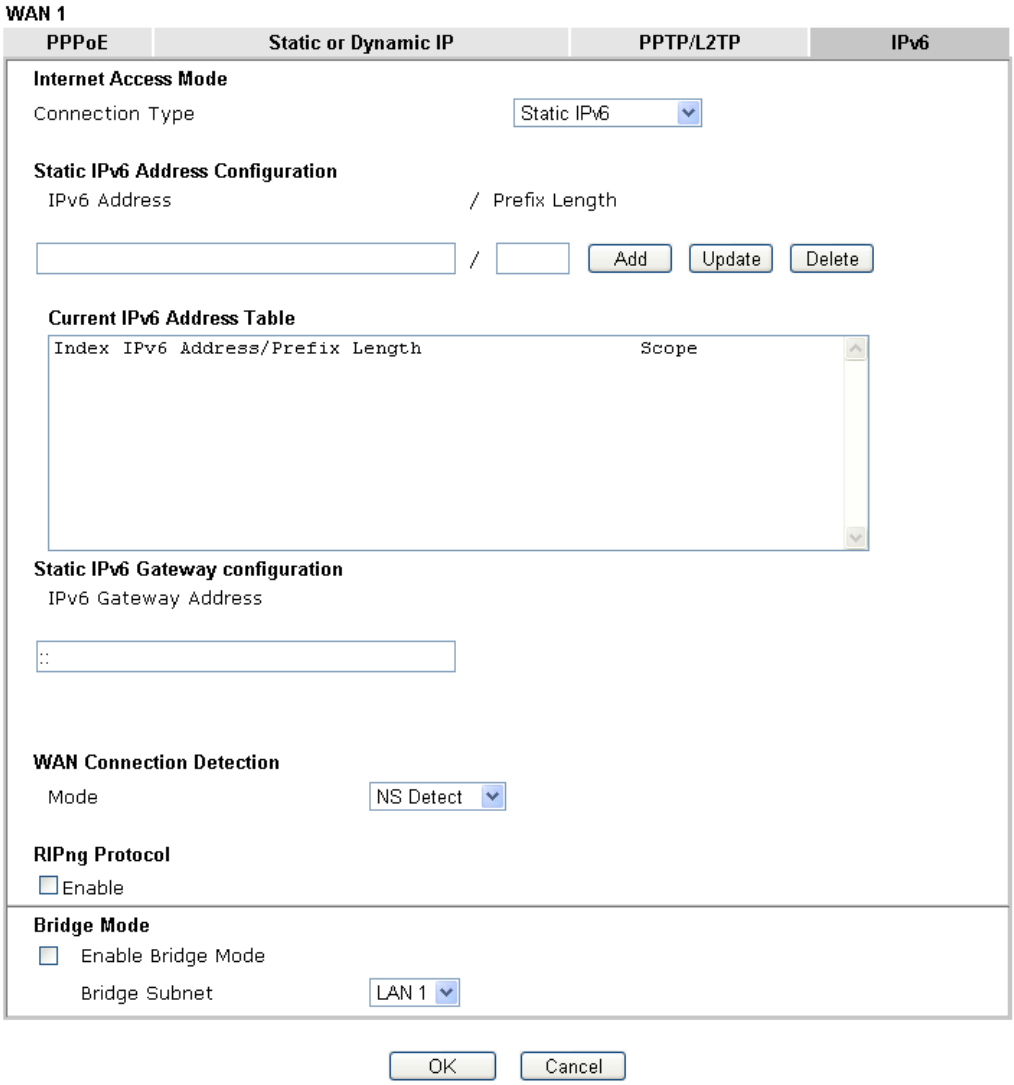
可用設定說明如下：

項目	說明
IAID	輸入號碼做爲 IAID。
WAN 連線檢測(WAN Connection Detection)	這個功能讓您檢查目前網路是否還在連線中。可透過 NS 檢測或是 Ping Detect 來完成。 **模式(Mode)** - 選擇**永遠連線(Alaways On)或 Ping 檢測(Ping Detect)或 NS 檢測(NS Detect)**執行 WAN 檢測動作。透過 NS 檢測，系統將檢查網路連線是否已經建立，就像 IPv4 ARP 檢測一般。**永遠連線(Alaways On)**表示無需進行任何檢測，網路永遠連線。 ● **Ping IP/主機(Ping IP/Hostname)** - 若您選擇了 **Ping 檢測(Ping Detect)** 作爲偵測模式，您必須在本區輸入 IP 位址或主機名稱。 ● **TTL (Time to Live)** - 設定 ping 操作需要的 TTL 數值。
RIPng 通訊協定(RIPng Protocol)	下一代 RIP(RIPng) 提供與 IPv4 RIP v2 相同的功用。
橋接模式(Bridge Mode)	**啓用橋接模式(Enable Bridge Mode)** - 若啓用此功能，路由器可以當成橋接數據機來運作。 **啓用防火牆(Enable Firewall)** - 啓用橋接模式後，此功能亦可使用。當橋接模式與防火牆皆啓用時，在使用者管理下方的使用者設定檔內的設定將被忽略不計。而防火牆功能單中所定義並啓用的過濾器規則取而代之。 **橋接子網(Bridge Subnet)** - 在選定的 LAN 子網與此 WAN 介面之間建立橋接連線。

完成上述設定之後，按下**確定(OK)**儲存設置內容。

II-1-2-12 WAN1/WAN2 的固定 IPv6 模式細節設定(IPv6)

這個類型可以您針對 WAN 介面設定固定的 IPv6 位址。



可用設定說明如下：

項目	說明
固定 IPv6 位址設定(Static IPv6 Address configuration)	**IPv6 位址(IPv6 Address) -** 輸入固定的 IPv6 位址。 **前置號碼長度(Prefix Length) -**輸入前置號碼長度固定值。 **新增(Add) -**按下此鈕新增位址。 **更新(Update)** - 按下此鈕修改既有的設定內容。 **刪除(Delete) -** 按下此鈕刪除現存的位址。
目前 IPv6 位址表格(Current IPv6 Address Table)	顯示目前 IPv6 位址的介面。
固定 IPv6 閘道設定(Static IPv6 Gateway Configuration)	**IPv6 閘道設定(IPv6 Gateway Address) -** 請在此輸入 IPv6 閘道的位址。
WAN 連線檢測(WAN Connection Detection)	這個功能讓您檢查目前網路是否還在連線中。可透過 NS 檢測或是 Ping Detect 來完成。 **模式(Mode)** - 選擇**永遠連線(Alaways On)或 Ping 檢測(Ping**

	Detect)執行 WAN 檢測動作。**永遠連線(Alaways On)**表示無需進行任何檢測，網路永遠連線。 ● **Ping IP/主機(Ping IP/Hostname)** – 若您選擇了 **Ping 檢測 (Ping Detect)** 作爲偵測模式，您必須在本區輸入 IP 位址或主機名稱。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。
橋接模式(Bridge Mode)	**啓用橋接模式(Enable Bridge Mode)** – 若啓用此功能，路由器可以當成橋接數據機來運作。 **啓用防火牆(Enable Firewall)** – 啓用橋接模式後，此功能亦可使用。當橋接模式與防火牆皆啓用時，在使用者管理下方的使用者設定檔內的設定將被忽略不計。而防火牆功能單中所定義並啓用的過濾器規則取而代之。 **橋接子網(Bridge Subnet)** – 在選定的 LAN 子網與此 WAN 介面之間建立橋接連線。

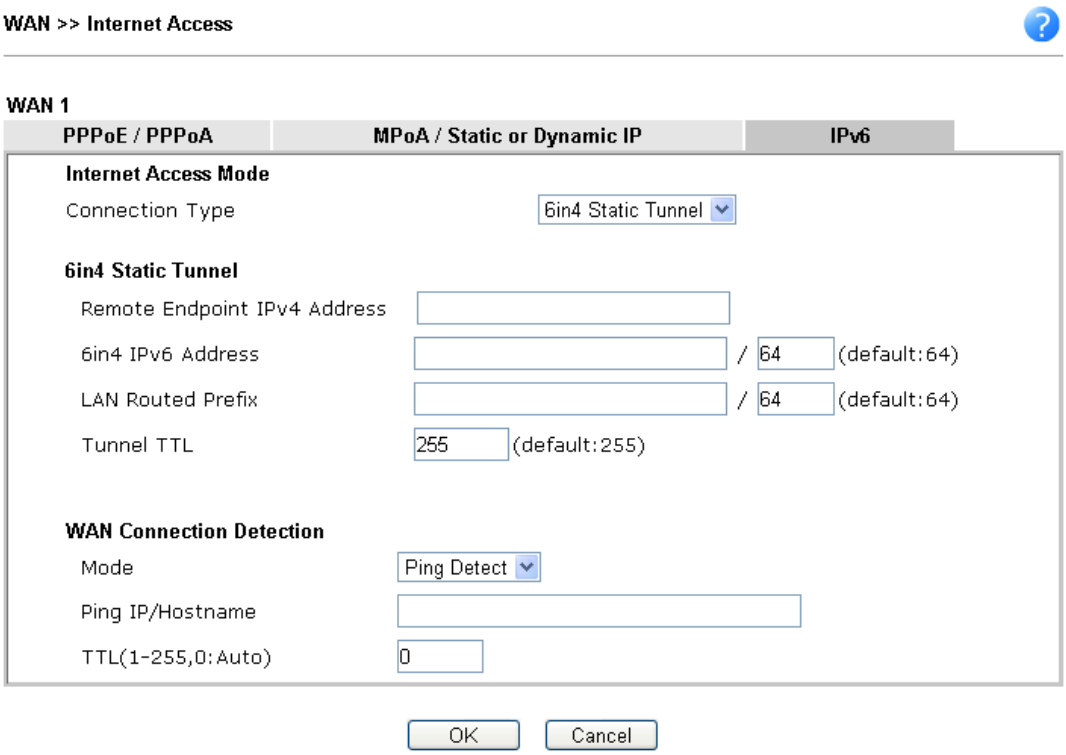
完成上述設定之後，按下**確定(OK)**儲存設置內容。

II-1-2-13 WAN1/WAN2 的 6in4 固定通道模式細節設定(IPv6)

此模式可讓您針對 WAN 界面設定 6in4 固定通道模式。

路由器可透過 IPv4 網路登入以 IPv6 爲基準的網路頁面。

不過，6in4 提供除了 2002::0/16 格式以外的前置代碼，因此您可以使用事先固定的終點.值，不必理會，模式的可靠度也相當高。

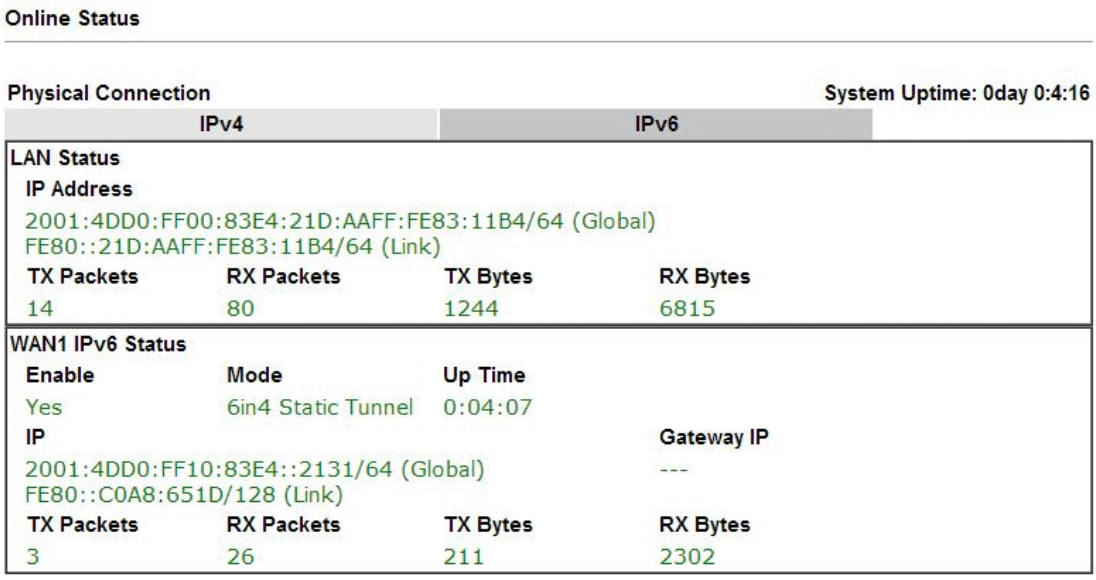


可用設定說明如下：

項目	說明
遠端終點 IPv4 位址(Remote Endpoint IPv4 Address)	輸入遠端伺服器的固定 IPv4 位址。
6in4 IPv6 位址(6in4 IPv6 Address)	針對 IPv4 通道輸入含前置代碼長度的固定 IPv6 位址。
LAN 路由前置代碼(LAN Routed Prefix)	針對 LAN 路由輸入含前置代碼長度固定 IPv6 位址。
通道 TTL(Tunnel TTL)	輸入通道內資料保存期限。
WAN 連線檢測(WAN Connection Detection)	這個功能讓您檢查目前網路是否還在連線中。可透過 NS 檢測或是 Ping Detect 來完成。 **模式(Mode)** – 選擇**永遠連線(Alaways On)或 Ping 檢測(Ping Detect)**執行 WAN 檢測動作。**永遠連線(Alaways On)**表示無需進行任何檢測，網路永遠連線。 ● **Ping IP/主機(Ping IP/Hostname)** – 若您選擇了 **Ping 檢測(Ping Detect)** 作爲偵測模式，您必須在本區輸入 IP 位址或主機名稱。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。

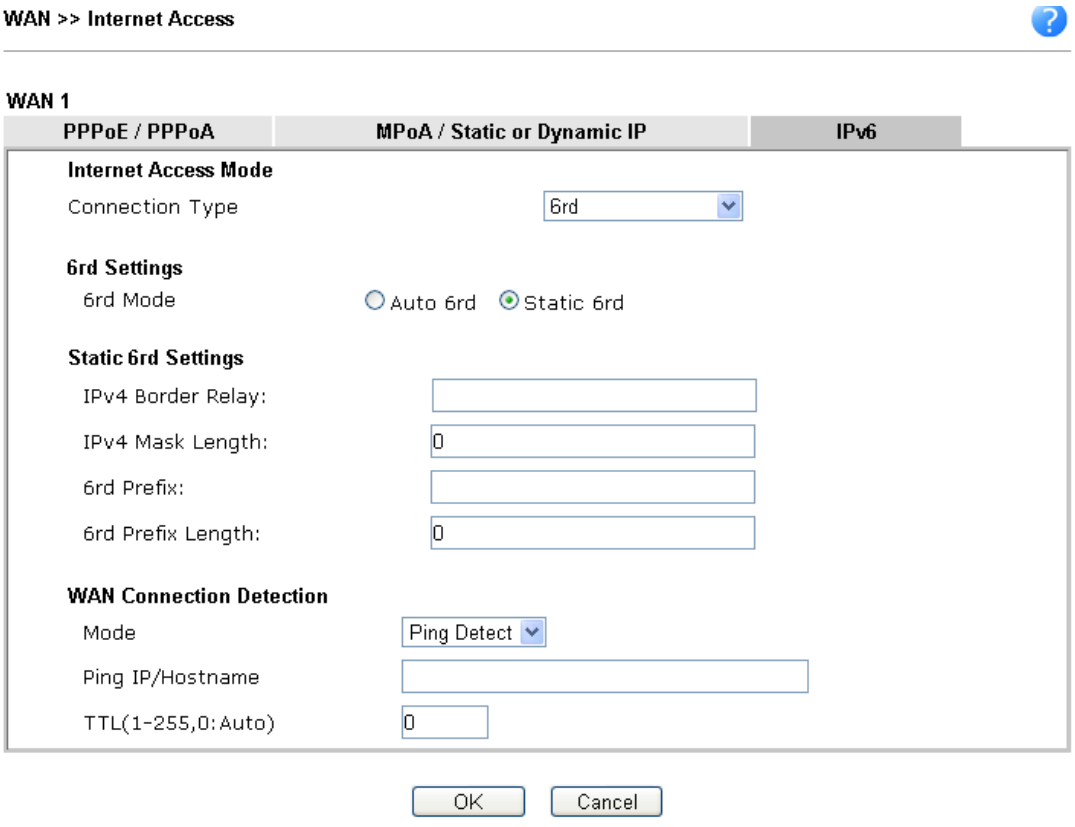
完成上述設定之後，按下**確定(OK)**儲存設置內容。

下圖顯示以此模式爲基準，成功設定的 IPv6 連線範例。



II-1-2-14 WAN1/WAN2 的 6rd 模式細節設定(IPv6)

本頁讓您針對 WAN 界面設定 6rd 模式。.



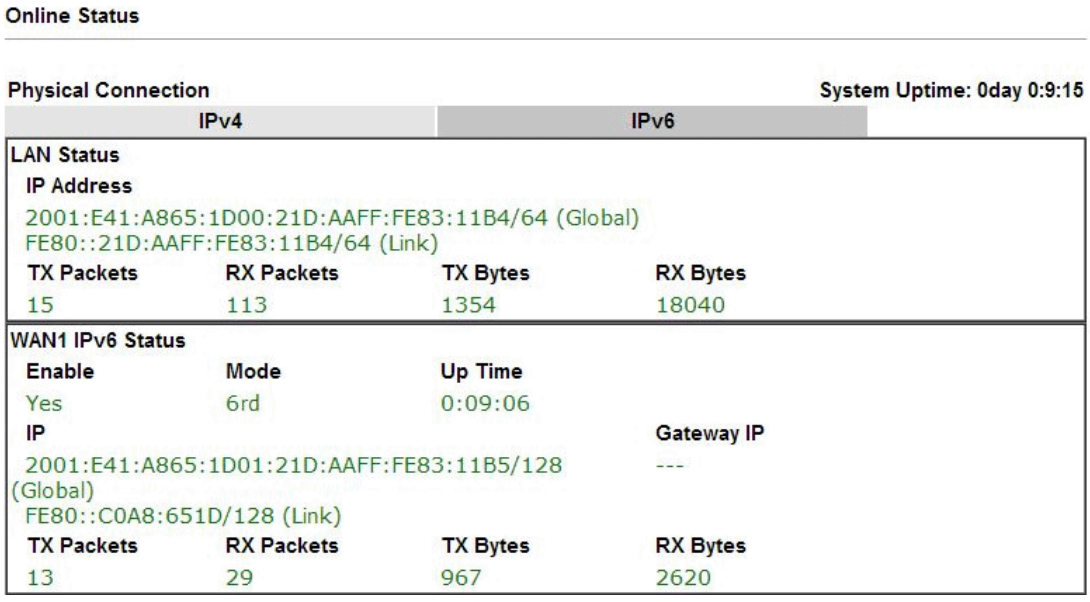
可用設定說明如下：

項目	說明
6rd 模式(6rd Mode)	**自動 6rd(Auto 6rd) -** 自 6rd 服務供應商自動取回 6rd 前置代碼資料。搭配的 IPv4 WAN 介面必須設定爲 DHCP 模式。 **固定 6rd(Static 6rd) -** 手動設定 6rd 選項。

IPv4 Border 中繼(IPv4 Border Relay)	選擇**固定 6rd** 模式之後，針對 6rd 網域提供 IPv4 位址作爲 6rd Border 的中繼。
IPv4 遮罩長度(IPv4 Mask Length)	選擇**固定 6rd** 模式之後，在 6rd 的網域中，輸入所有 CE 的 IPv4 位址需求的遮罩長度值。
6rd 前置代碼(6rd Prefix)	選擇**固定 6rd** 模式之後，輸入 6rd IPv6 位址。
6rd 前置代碼長度(6rd Prefix Length)	選擇**固定 6rd** 模式之後，輸入 6rd IPv6 前置代碼需求的長度數字。
WAN 連線檢測(WAN Connection Detection)	這個功能讓您檢查目前網路是否還在連線中。可透過 NS 檢測或是 Ping Detect 來完成。 **模式(Mode)** – 選擇**永遠連線(Alaways On)或 Ping 檢測(Ping Detect)**執行 WAN 檢測動作。**永遠連線(Alaways On)**表示無需進行任何檢測，網路永遠連線。 ● **Ping IP/主機(Ping IP/Hostname)** – 若您選擇了 **Ping 檢測(Ping Detect)** 作爲偵測模式，您必須在本區輸入 IP 位址或主機名稱。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。

完成上述設定之後，按下**確定(OK)**儲存設置內容。

下圖顯示以此模式爲基準，成功設定的 IPv6 連線範例。



II-1-3 多重 VLAN (Multi-VLAN)

多重 VLAN 可讓用戶針對 WAN 介面建立設定檔與橋接連線，以便用於需要高度網路流量的應用上。

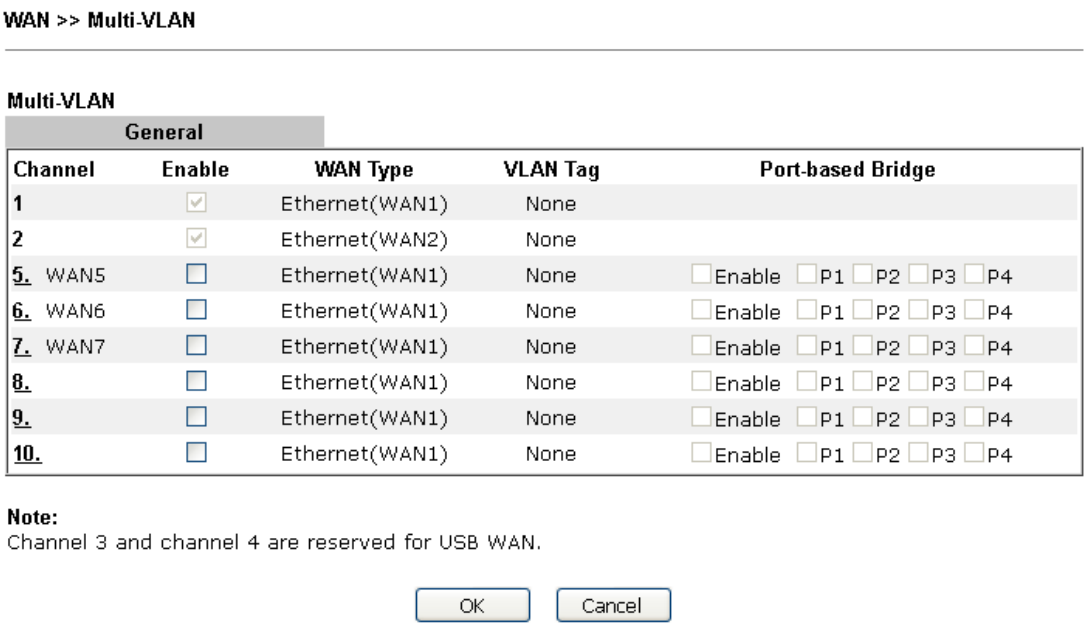
頻道 1 到 4 分別具有固定的用途：

- 頻道 1: WAN1(乙太網路)
- 頻道 2: WAN2 (光纖)/ WAN2 (乙太網路)，依照型號而定
- 頻道 3/4: USB1 (WAN3) 與 USB2 (WAN4)

頻道 5 到**頻道 10** 可橋接至 1 到 3 個以上的 LAN 埠口(P2 至 P4)，此外，**頻道 5** 至**頻道 7** 則可設定爲虛擬 WAN 介面(從 WAN5 到 WAN7)。

基本(General)

本頁顯示每個頻道的基本設定值。



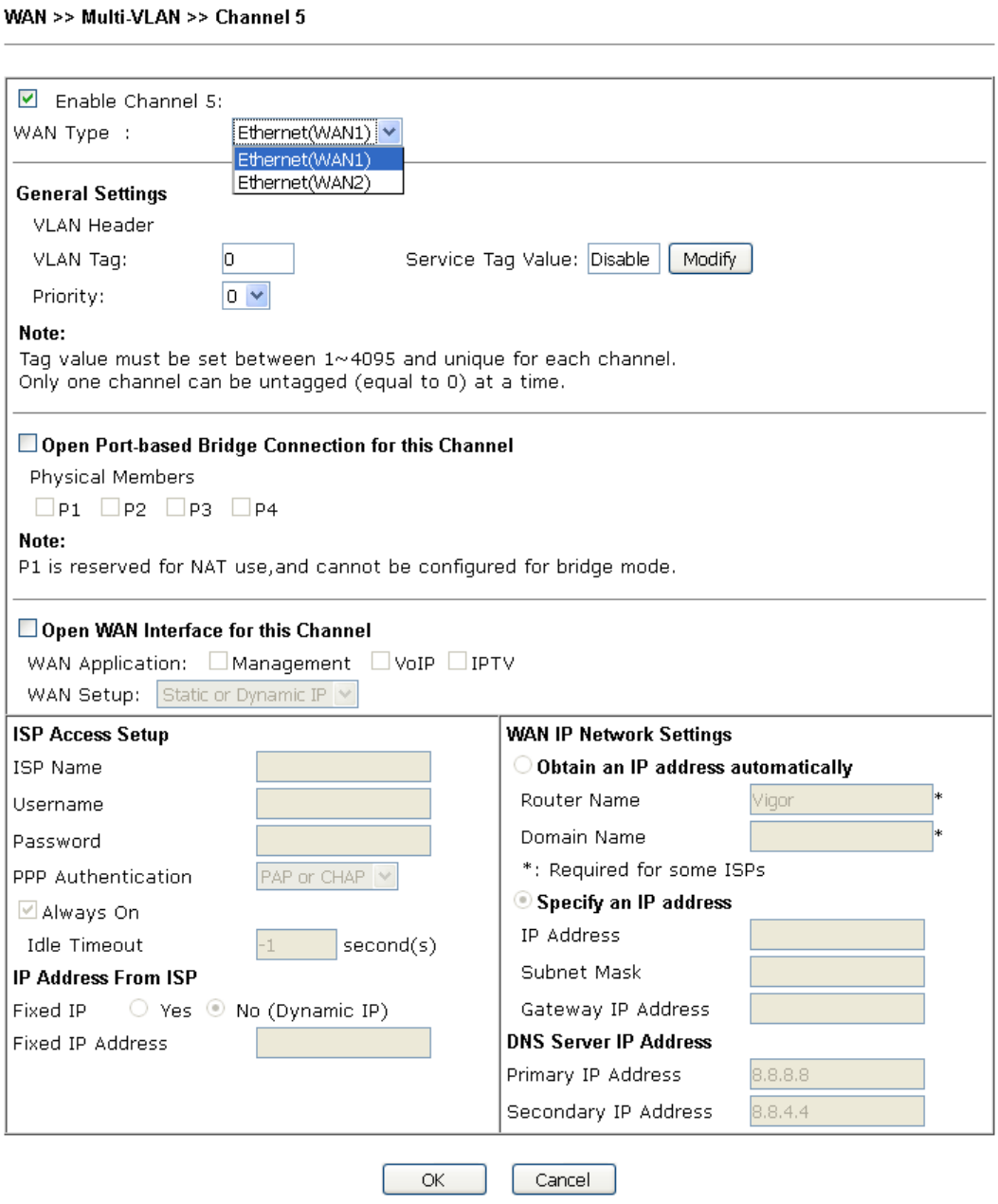
可用設定說明如下：

項目	說明
頻道(Channel)	顯示每個頻道的編號。 頻道 1 與 2 專屬於網際網路使用者介面，因此在此處是不可以修訂的。 頻道 5 ~ 10 是可以設定調整的。
啓用(Enable)	顯示此頻道的設定是啓用(是)還是停用(否)。
WAN 類型(WAN Type)	顯示頻道使用的實體介面類型。
VLAN 標籤(VLAN Tag)	顯示用於此頻道封包傳輸攜帶的 VLAN 標籤值。

埠號橋接 **(Port-based Bridge)**	系統可透過個別 VLAN 標籤值來辨識每個頻道網路流量，不同頻道即使利用相同 WAN 介面，也不可採用相同的 VLAN 標籤值。 **啓用(Enable)** - 勾選此方塊以便啓用該頻道的埠號橋接功能。 **P1 ~ P4** – 選需要的埠號以便建立區域網路端的橋接連線。

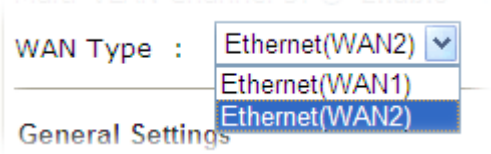
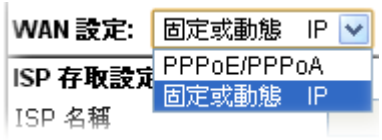
預設定一個 PVC 頻道，請按下頻道號碼連結。

頻道 5、6 與 7 的 WAN 連結主要用於路由器的應用，例如 **TR-069**。這邊的設定值必須取自 ISP 業者，且只能套用在該 ISP 業者。如果有特殊需要，請與您的 ISP 業者聯絡，然後再至此設定此三個頻道。



可用設定說明如下：

Item	Description
啓用頻道 5/6/7 **(Enable Channel 5/6/7)**	勾選此框啓用此頻道。

WAN 類型(WAN Type)	指定 PVC 頻道/VLAN 的 WAN 類型。 
基本設定 **(General Settings)**	**VLAN 標籤(VLAN Tag) -** 輸入 VLAN ID 號碼，可設定範圍自 1 到 4095，系統可透過 VLAN 標籤來辨識每個頻道，使用相同 WAN 類型的頻道不可設定相同的 VLAN 標籤值。 **優先權(Priority) -** 選擇一個號碼來決定此 VLAN 封包的優先權爲何，可設定範圍自 0 到 7。 **服務標籤值(Service Tag Value)** - 此數值依 **WAN>>基本設定(WAN>>General Setup)**內容而變更。必要時，請按**修正(Modify)** 開啓 **WAN>>基本設定(WAN>>General Setup)**。之後啓用 **VLAN 標籤插入(VLAN Tag insertion)**並設定服務(對外標籤)並指定 VLAN ID 號碼。或是停用。
開啓本頻道的埠號橋接連線 **(Open Port-based Bridge Connection for this Channel)**	此處設定將會在 LAN 埠口間與 WAN 口建立橋接連線，橋接連線建立在選定的 WAN 介面並使用 VLAN 標籤值。 **實體連線成員(Physical Members) -** 勾選您想要群組的埠號，使其套用橋接模式連線。 請注意，LAN 埠口 1 保留作爲 NAT 轉址之用，不可以選其做爲橋接介面。
針對此頻道開啓 WAN 介面 **(Open WAN Interface for this Channel)**	勾選選框啓用相關功能。 **路由器應用之 WAN 介面 - 管理(WAN Application - Management)**可指定爲一班管理之用(網頁設定/telnet/TR069)，如果您選擇此項，此 VLAN 設定將僅對網頁設定/telnet/TR069 產生作用。 **IPTV** - 允許 WAN 介面傳送 IGMP 封包到 IPTV 伺服器。 **WAN 設定(WAN Setup)** - 選擇 PPPoE/PPPoA 或是固定或動態 IP 設定，以便決定哪個 WAN 介面需要設定。 
ISP 存取設定(ISP Access Setup)	依照 ISP 提供的資訊，輸入使用者名稱、密碼與驗證參數。 **ISP 名稱(ISP Name)** - 指明 PPP 服務名稱，若您的 ISP 需要此設定值，請輸入名稱，否則此區可留空白。 **使用者名稱(Username)** - ISP 提供 PPPoE/PPPoA 驗證的名稱，最大長度爲 62 個字元。 **密碼(Password)** -SP 提供 PPPoE/PPPoA 驗證的密碼，最大長度爲 62 個字元。 **PPP 驗證(PPP Authentication)** - 指定 PPP 驗證需求的通訊協定。 ● **限用 PAP (PAP only)**- 僅能使用 PAP (Password Authentication Protocol)。 ● **PAP 或 CHAP(PAP or CHAP)**- PAP 與 CHAP (Challenge-Handshake Authentication Protocol)二種協定皆可用於 PPP 驗證。路由器與 PPTP 或是 L2TP 伺服器

	協商以決定要使用哪種協定。 **永遠連線(Always On)** – 勾選此項後，路由器將維持 PPPoE/PPPoA 連線且不斷線。 **閒置逾時(Idle Timeout)** – 指定連線斷線之前等待的時間(沒有流量)長度，單位爲秒。 **來自 ISP 的 IP 位址(IP Address From ISP)** – 指定頻道之 WAN IP 位址的設定方式。 ● **固定 IP (Fixed IP)** **是(Yes)** – 在固定 IP 位址欄位中輸入的 IP 位址將做爲虛擬 WAN 的 IP 位址。 **否(No)** – 虛擬 WAN IP 位址由 ISP 的 PPPoE/PPPoA 伺服器來分派。
WAN IP 網路設定 **(WAN IP Network Settings)**	**自動取得 IP 位址(Obtain an IP address automatically)** – 按此鈕以自動取得 IP 位址。 ● **路由器名稱(Router Name)** – 設定 DHCP Option 12 的名稱，某些 ISP 需要此設定內容。 ● **網域名稱(Domain Name)** – 設定 DHCP Option 15 的名稱，某些 ISP 需要此設定內容。 **指定 IP 位址(Specify an IP address)** – 按此鈕以指定 IP 位址。 ● **IP 位址(IP Address)** – 輸入 IP 位址。 ● **子網路遮罩(Subnet Mask)** – 輸入子網路遮罩。 ● **閘道 IP 位址(Gateway IP Address)** – 輸入閘道 IP 位址。 **DNS 伺服器 IP 位址(DNS Server IP Address) -** 如果要使用固定 IP 模式，請在此輸入路由器的主要 IP 位址；如有必要，亦可輸入次要 IP 位址以備將來之需。

在您完成上述的設定之後，請按**確定(OK)**按鈕回到上一頁。

按下索引編號(8，9 與 10)可以看到如下頁面：



可用設定說明如下：

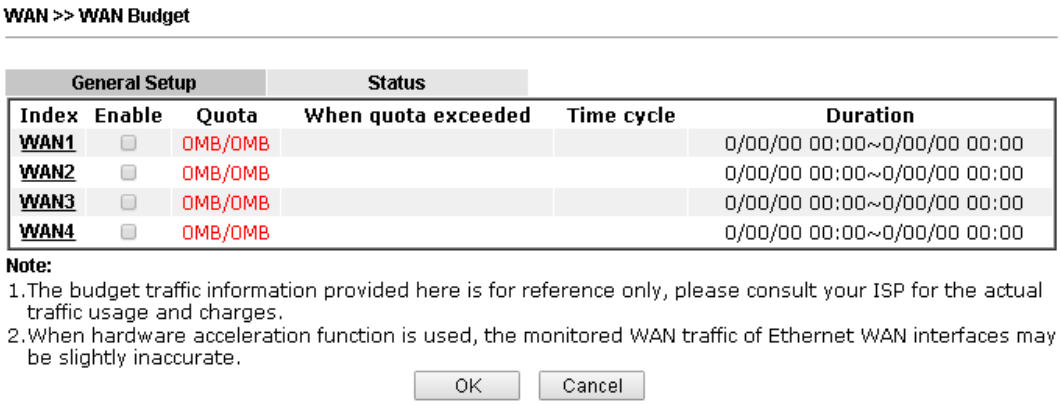
Item	Description
啓用頻道 8/9/10 (Enable Channel 8/9/10)	勾選此框啓用此頻道。
WAN 類型(WAN Type)	指定 PVC 頻道/VLAN 的 WAN 類型。 可選擇特定的 WAN 類型來建立每個頻道上的連線與介面。在多重 VLAN 應用中，只有乙太網路 WAN 類型是可用的。
基本設定 (General Settings)	**VLAN 標籤(VLAN Tag) –** 輸入 VLAN ID 號碼，可設定範圍自 1 到 4095，系統可透過 VLAN 標籤來辨識每個頻道，使用相同 WAN 類型的頻道不可設定相同的 VLAN 標籤值。 **優先權(Priority) –** 選擇一個號碼來決定此 VLAN 封包的優先權爲何，可設定範圍自 0 到 7。
橋接模式 (Bridge mode)	**啓用(Enable) –** 選擇此項啓用此頻道設定的橋接模式。 **實體連線成員(Physical Members) –** 勾選您想要群組的埠號，使其套用橋接模式連線。 請注意，LAN 埠口 1 保留作爲 NAT 轉址之用，不可以選其做爲橋接介面。

完成上述設定之後，按下**確定(OK)**儲存設置內容。

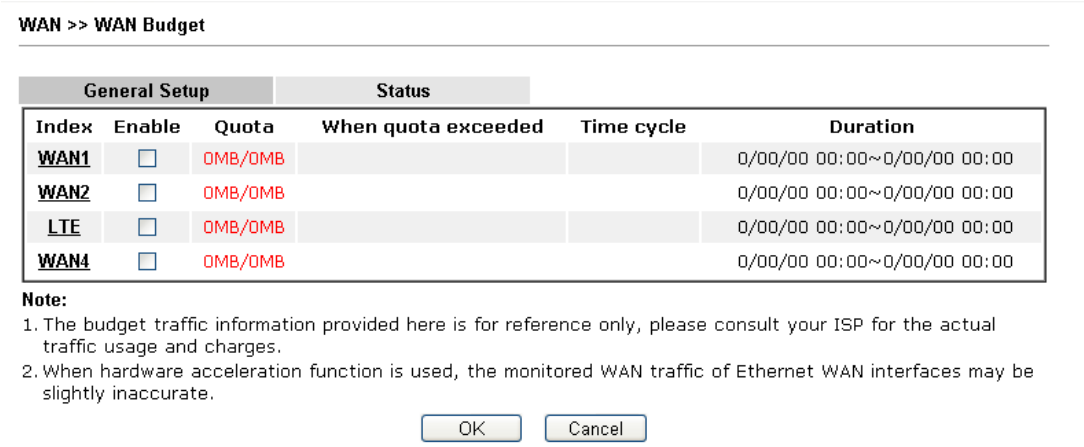
II-1-4 WAN 計量收費(WAN Budget)

本功能可用來分別測定每個 WAN 介面的資料流量，避免自 ISP 收到過多的數據傳輸。請注意額度限制與每月的 Billing cycle day 皆應設定正確，才能正確執行相關的計算。

II-1-4-1 基本設定(General Setup)

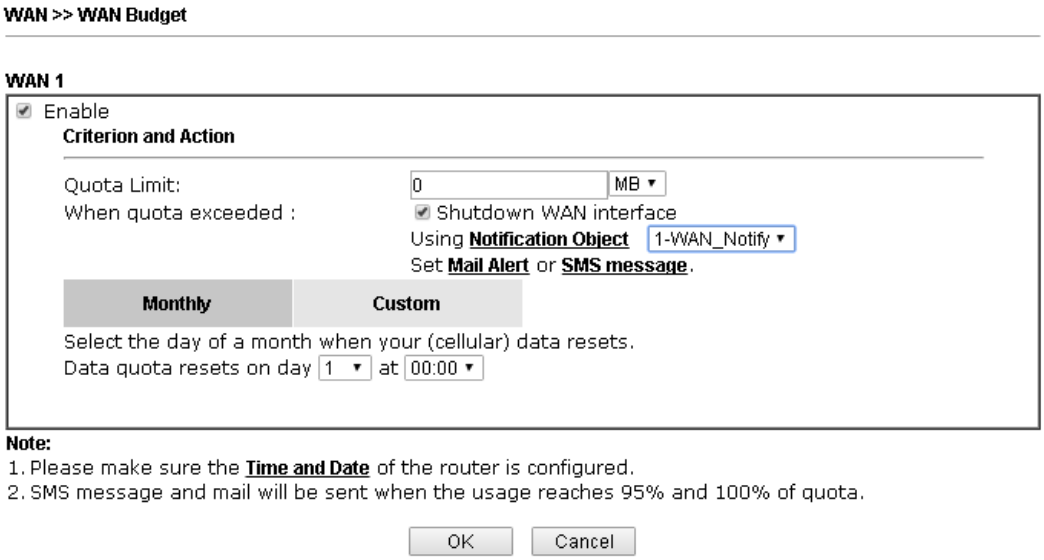


或是



項目	說明
索引編號(Index)	代表 WAN 埠口。 按編號設定 WAN 計量。
啓用(Enable)	**v -** 啓用此 WAN 介面的 WAN 計量收費。 **x -** 停用此 WAN 介面的 WAN 計量收費。
額度(Quota)	目前網際網路周期用量已 x/y 來表示，其中 x 爲累計用量而 y 爲上限值。例如 100MB/200MB 表示循環值是 100MB 上限值爲 200MB。
當額度超過(When quota exceeded)	一旦達到額度值時，系統會採取的行動。 **關閉(Shutdown)** – WAN 介面停用。 **郵件警示(Mail Alert)** – 警示郵件將會寄給管理者。
時間週期(Time cycle)	顯示重置資料用量的頻率。
期間(Duration)	顯示目前周期的開始與結束時間。

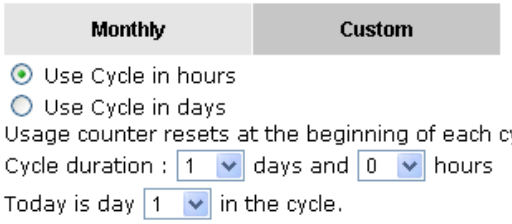
按下 WAN1/WAN2/WAN3 或是 LTE/WAN4 連結以便開啓如下頁面。



可用設定說明如下：

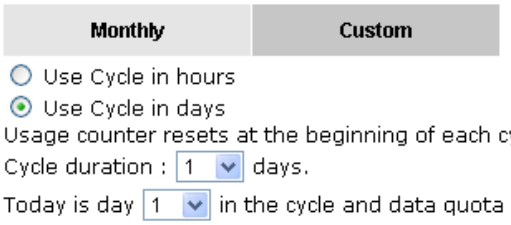
項目	說明
啓用(Enable)	勾選此框啓用此功能。
額度限制(Quota Limit)	請輸入此 WAN 介面最大的網路流量限制(單位是百萬位元或是 GB)。
當額度超過(When quota exceeded)	當超過額度限制時，系統可以依據選擇的方式來執行流量傳送。 **關閉 WAN 介面(Shutdown WAN interface)** – 所有透過此 WAN 介面的對外流量都將中止。 ● **使用通知物件(Using Notification Object)** – 系統將依照通知物件的內容發送通知訊息。 ● **設定郵件警示(Set Mail Alert)**– 當額度快要用完時，系統將發送警告訊息予管理者，不過連線費用仍然持續計算。 ● **設定簡訊(Set SMS message)** – 當額度快要用完時，系統將發送警告訊息予管理者。
每月(Monthly)	某些 ISP 業者可能想以每月流量限制來運用網路限制，這項設定可提供每月重新設定流量紀錄的機制以供 ISP 運用。  **結算週期起始於 ...(Data quota resets on day ...)** – 結算週期大約是一個月，您可以決定一個月當中的某日某時作爲結算週期的起始日。
使用者定義(Custom)	此設定可讓 ISP 業者依照實際的需要定義所需的結算週期。 WAN 計量收費可以經過一個週期間隔之後重新起算。 預設值是每個月，如果您需要一個更長或是更短的週期，請改設定**使用者定義**，結算週期介於 1 到 60 天，您可以指定日數與時數來決定週期的長短，此外您也可以指定目前週期內的天數爲幾天。

使用小時循環(Use Cycle in hours) –



- **結算週期(Cycle duration)**: 指定重設流量紀錄的期間(日、時)。例如數字 7 表示整個週期有 7 天；20 就表示有 20 天。當時間已到，路由器就會自動重置流量紀錄。
- **目前週期內的天數(Today is day)** – 指定結算週期內中的哪一天作爲結算的起始日，例如數字 3 就表示整個結算週期的第 3 日爲起始日。

使用日期循環(Use Cycle in days) -

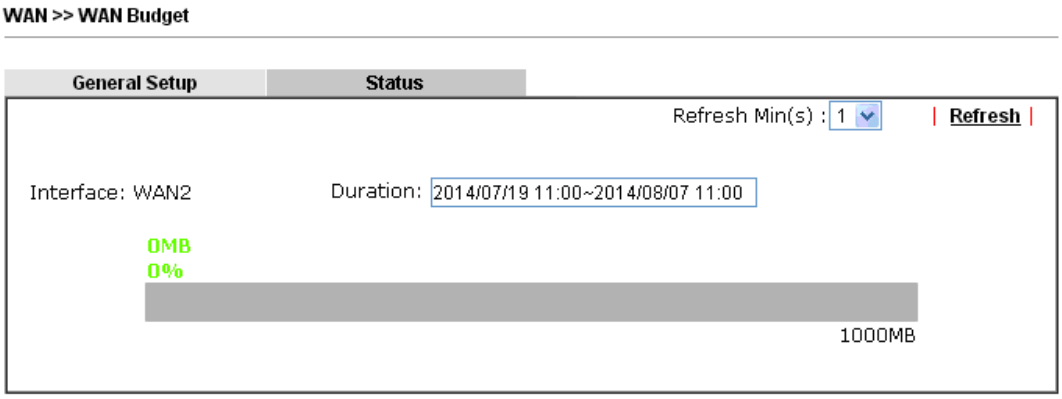


- **結算週期(Cycle duration)**: 指定重設流量紀錄的期間(日)。例如數字 7 表示整個週期有 7 天；20 就表示有 20 天。當時間已到，路由器就會自動重置流量紀錄。
- **目前週期內的天數(Today is day)** – 指定結算週期內中的哪一天作爲結算的起始日，例如數字 3 就表示整個結算週期的第 3 日爲起始日。

完成上述設定之後，按下**確定(OK)**儲存設置內容。

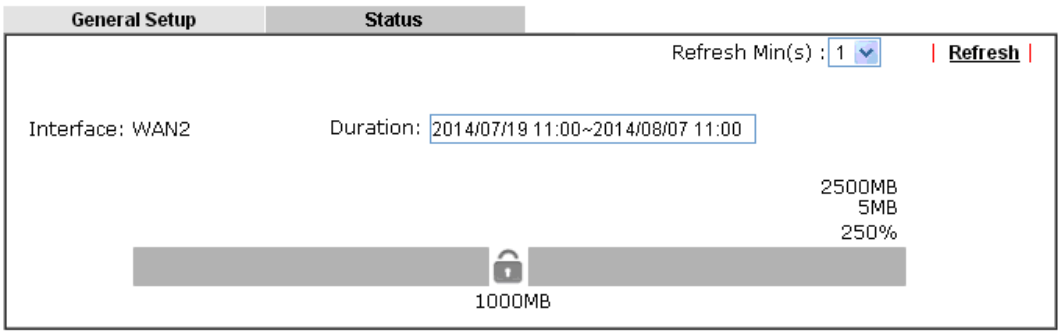
II-1-4-2 狀態(Status)

狀態頁面顯示 WAN 計量收費的目前狀態，包含持續時間與用量。



若 WAN 計量已耗盡且**關閉 WAN 介面(Shutdown WAN interface)**功能也被啓動，本頁會呈現一把鎖來表示，代表系統不會再處理任何資料傳輸。此外，若有指定郵件警示(Mail Alert)功能設定檔，系統也會發出警告訊息給予管理者；若有指定簡訊(SMS message)功能設定檔，則系統會傳送簡訊給予管理者。

WAN >> WAN Budget

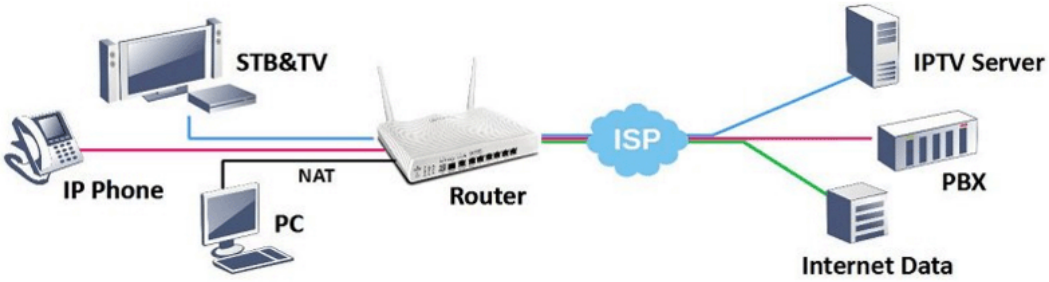


應用說明

A-1 如何設定多重 VLAN 以便因應三合一服務?

透過新增 VLAN 標籤來區分流量，服務供應商能經由單一連線，又稱爲三合一服務，傳送影像、聲音與資料予訂閱服務者。本文將展示如何設置多重 VLAN 功能以部署三合一服務。有二種設定類型，一個是埠號式橋接可透過指定 LAN 埠口，直接連接如 STB 等媒介至服務供應商；另一個設定則是開啓虛擬 WAN 介面並進行 NAT 轉址運用。

橋接虛擬 WAN 至 LAN 埠口



1. 開啓 **WAN>>多重 VLAN(WAN >> Multi-VLAN)**，點選頻道進行設定。

WAN >> Multi-VLAN

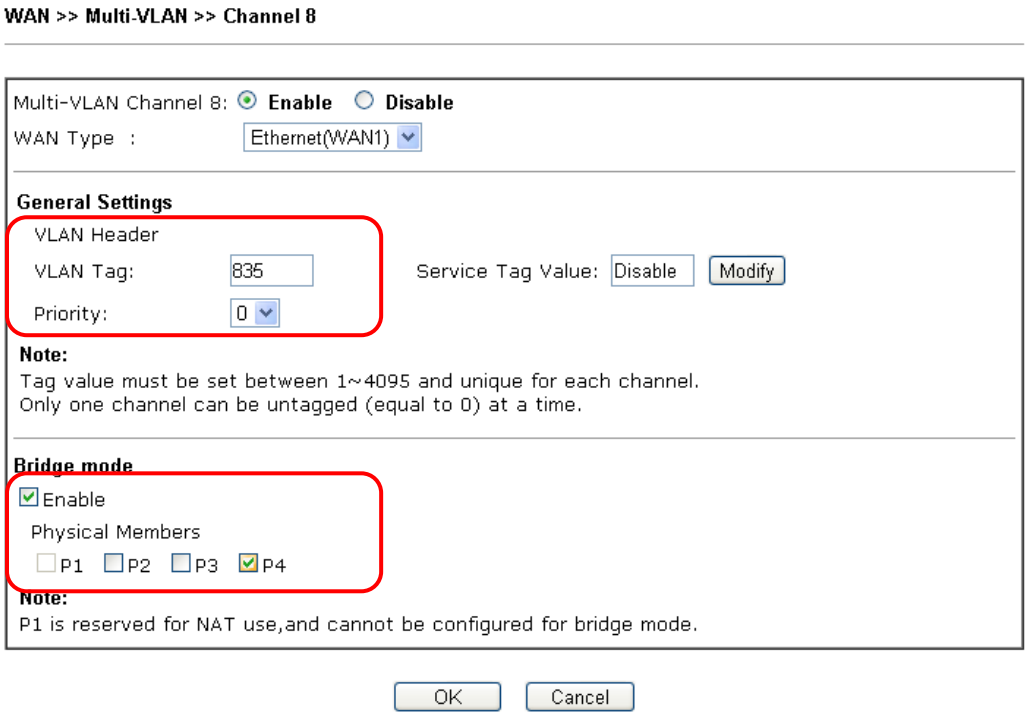
Multi-VLAN

General				
Channel	**Enable**	**WAN Type**	**VLAN Tag**	**Port-based Bridge**
1	☑	Ethernet(WAN1)	None	
2	☑	Ethernet(WAN2)	None	
5. WAN5	☐	Ethernet(WAN1)	None	☐Enable ☐P1 ☐P2 ☐P3 ☐P4
6. WAN6	☐	Ethernet(WAN1)	None	☐Enable ☐P1 ☐P2 ☐P3 ☐P4
7. WAN7	☐	Ethernet(WAN1)	None	☐Enable ☐P1 ☐P2 ☐P3 ☐P4
8.	☐	Ethernet(WAN1)	None	☐Enable ☐P1 ☐P2 ☐P3 ☐P4
9.	☐	Ethernet(WAN1)	None	☐Enable ☐P1 ☐P2 ☐P3 ☐P4
10.	☐	Ethernet(WAN1)	None	☐Enable ☐P1 ☐P2 ☐P3 ☐P4

Note:
Channel 3 and channel 4 are reserved for USB WAN.

OK Cancel

2. 頻道細部內容設定如下圖：



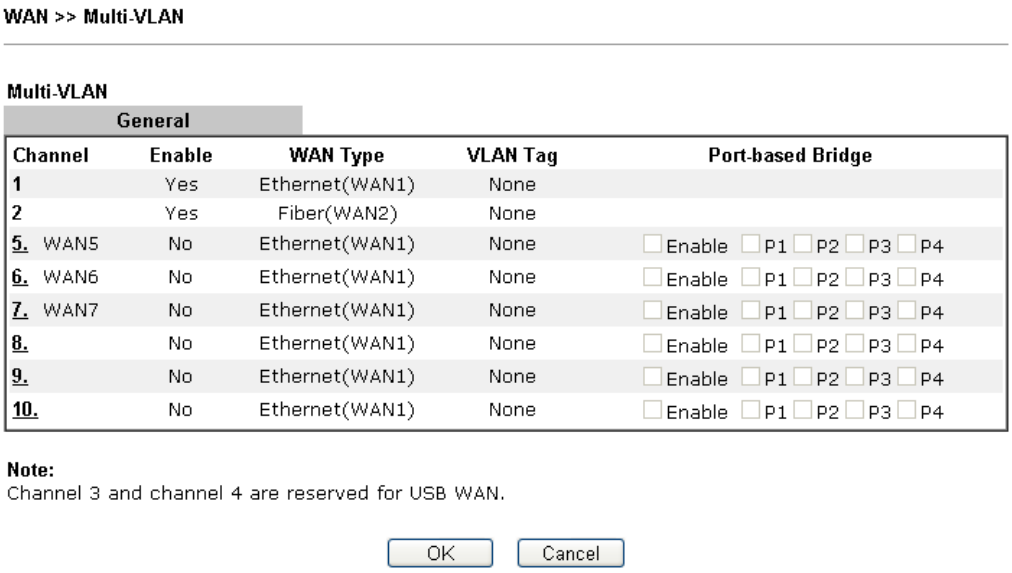
(a) 啓用此頻道

(b) 設定服務供應商準備使用的 WAN 類型(WAN Type)

(c) 輸入服務供應商需求的 VLAN 標籤與優先權

(d) 勾選橋接模式(Brdge Mode)的啓用(Enable)方框，並選擇連接至 STB 的實體埠號成員

3. 點選**確認(OK)**儲存設定，設定將會顯示在主頁面上，現在您可以連接 STB 至橋接埠口以便使用 IPTV 服務。



開啟虛擬 WAN 介面



1. 開啓 **WAN>>多重 VLAN(WAN >> Multi-VLAN)**，點選頻道 5, 6 或 7 進行設定。

WAN >> Multi-VLAN

Multi-VLAN

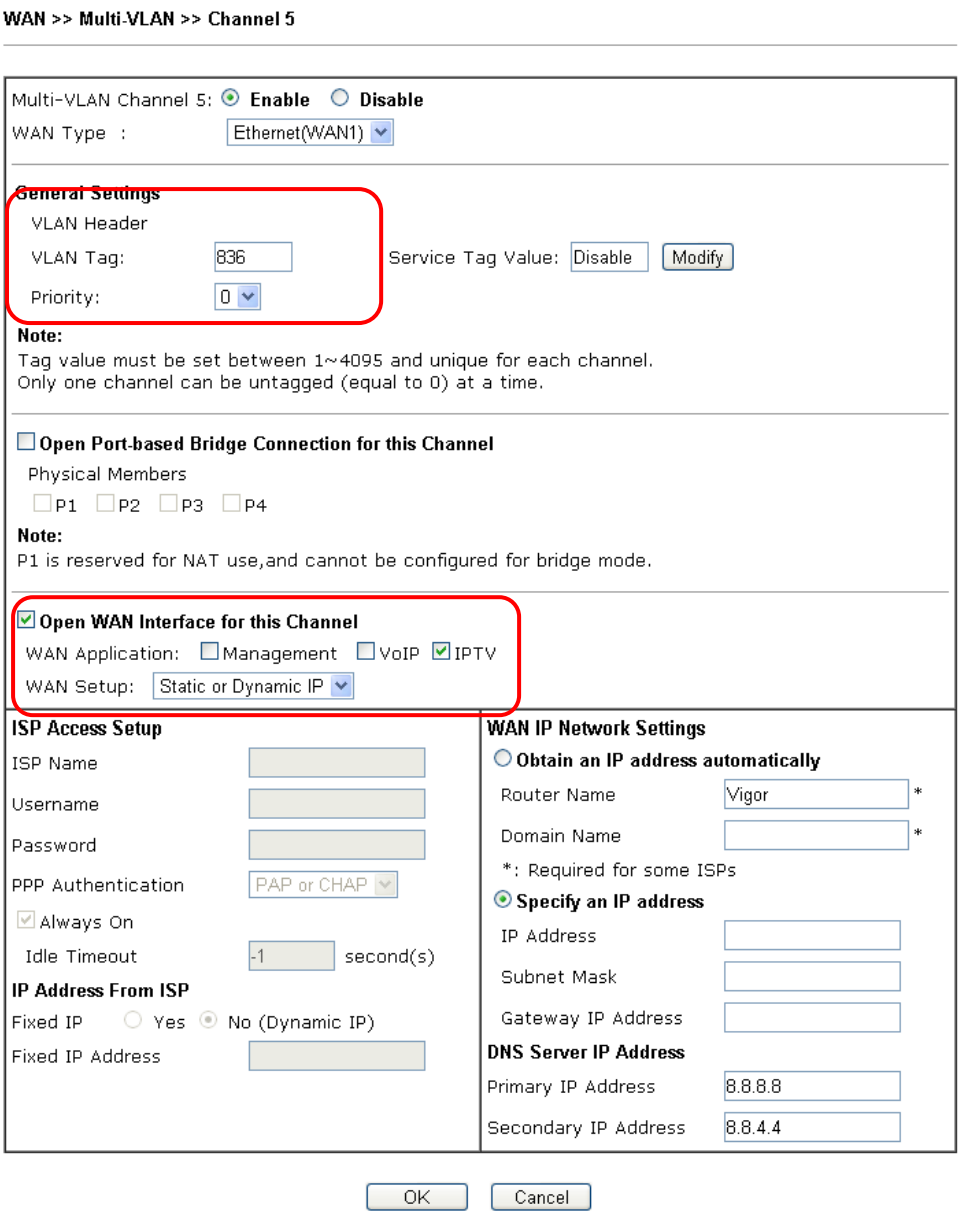
General

Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge
1	☑	Ethernet(WAN1)	None	
2	☑	Ethernet(WAN2)	None	
5. WAN5	☐	Ethernet(WAN1)	None	☐Enable ☐P1 ☐P2 ☐P3 ☐P4
6. WAN6	☐	Ethernet(WAN1)	None	☐Enable ☐P1 ☐P2 ☐P3 ☐P4
7. WAN7	☐	Ethernet(WAN1)	None	☐Enable ☐P1 ☐P2 ☐P3 ☐P4
8.	☐	Ethernet(WAN1)	None	☐Enable ☐P1 ☐P2 ☐P3 ☐P4
9.	☐	Ethernet(WAN1)	None	☐Enable ☐P1 ☐P2 ☐P3 ☐P4
10.	☐	Ethernet(WAN1)	None	☐Enable ☐P1 ☐P2 ☐P3 ☐P4

Note:
Channel 3 and channel 4 are reserved for USB WAN.

OK Cancel

2. 頻道細部內容設定如下圖：



(a) 啓用此頻道

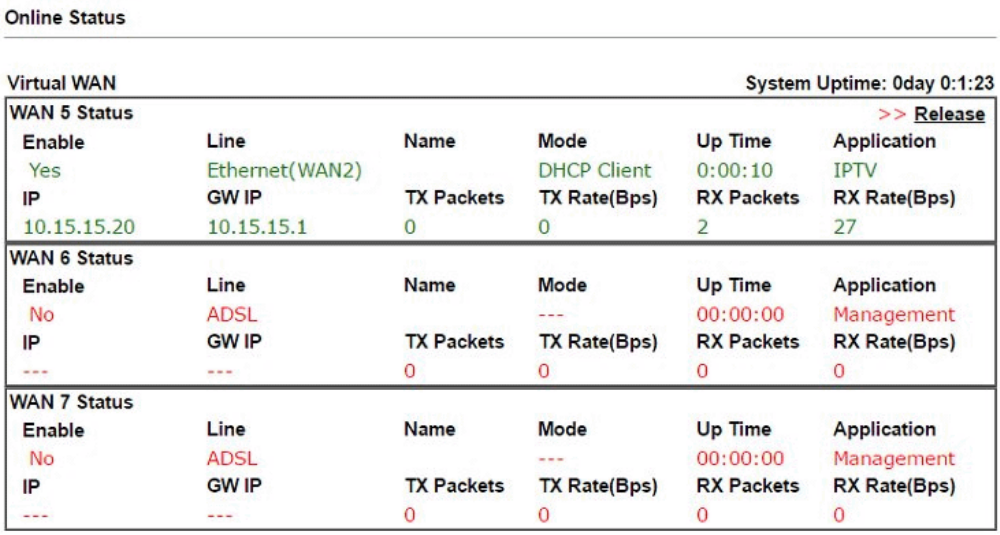
(b) 設定服務供應商準備使用的 WAN 類型(WAN Type)

(c) 輸入服務供應商需求的 VLAN 標籤與優先權

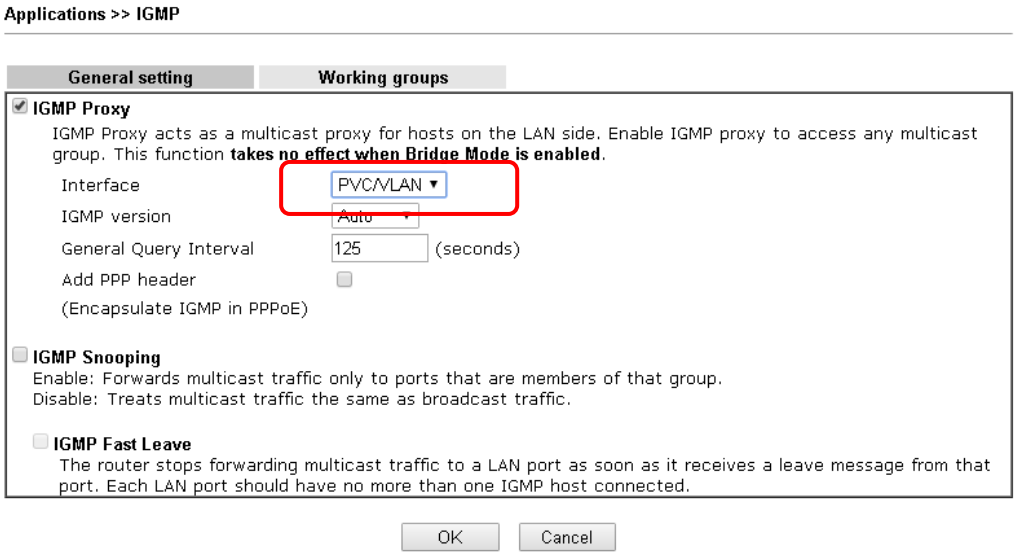
(d) 啓用 “針對此頻道開啓 WAN 介面(Open WAN Interface for this Channel)”，並選擇用於此頻道的應用類型。(註解：此選項僅在頻道 5-7 可用)

(e) 設定網際網路連線類型以應 ISP 之需要

3. 按下**確定(OK)**以儲存設定檔，並重新啓動路由器讓設定生效。路由器重新啓動之後，開啓**線上狀態>>虛擬 WAN(Online Status >> Virtual WAN)**確保 WAN 介面啓用且上線並已取得一組 IP 位址。



4. 現在，您可以使用虛擬 WAN 介面以應 IGMP 代理伺服器之用，只要選擇 PVC/VLAN 作爲 WAN 介面即可。



A-2 多重 WAN Vigor 路由器的負載平衡與備援

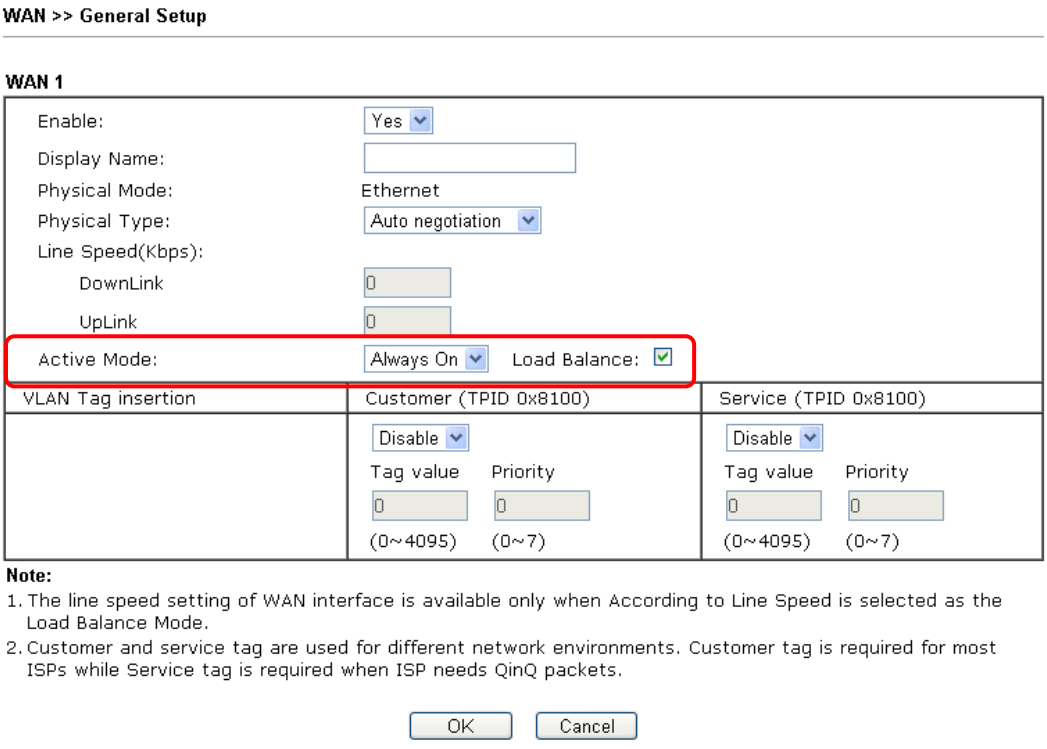
網路管理人員可以設定多條網際網路連線以分享流量負載或是新增一條可靠性較高的網路連線。

負載平衡 Load Balancing

預設情況下，所有運作中的連線的 WAN 介面皆可加入負載平衡運用，對外流量可使用運作中 WAN 作爲使用路徑，因爲所有的 WAN 介面皆共享流量負載。對於支援連線數式負載平衡的路由器，路由器也可以進行 WAN aggregation，表示 LAN 用戶端可以體驗的速度，將由所有運作中的 WAN 頻寬組合起來。



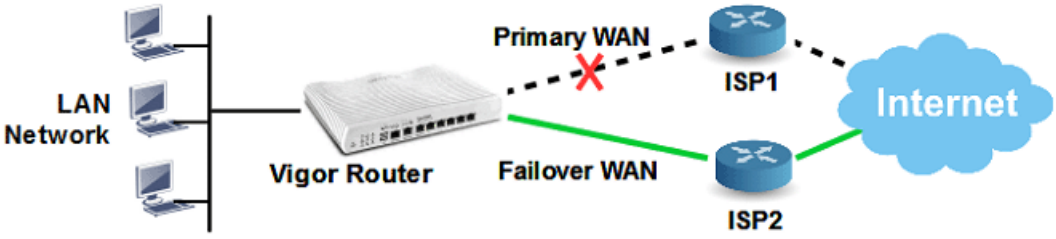
爲了確保某 WAN 介面必在負載平衡配置區中，開啓 **WAN>>基本設定(WAN>>General Setup)**頁面，按下該介面的索引連結編號，設定**使用中模式(Active Mode)**爲**永遠連線(Always On)**，確保啓用負載平衡。



預設負載平衡權重以每個 WAN 介面被偵測出的鋒值頻寬而定，但是網路管理者也可以使用**依照連線速度模式(According to Line Speed Mode)**來決定影響權重的最大頻寬。此外，當遇到多重 WAN 介面時，網路管理者可能想要指定對外路徑給予特定流量使用，解決方案可以透過使用路由策略。

備援

當設定爲備援模式時，WAN 介面僅在主要 WAN 介面斷線時才會啓用，並在主要 WAN 介面重新連線時再度下線。



在備援模式下設定 WAN 介面，開啓 **WAN>>基本設定(WAN>>General Setup)**，按下您想要設定成備援模式的 WAN 索引編號連結，設定**使用中模式(Active Mode)**爲**備援(Failover)**，並設定該介面何時可以啓用。

WAN >> General Setup

WAN 2

Enable:	Yes
Display Name:	
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Line Speed(Kbps):	
DownLink	0
UpLink	0
Active Mode:	Failover Load Balance:
	WAN Failure
	Traffic Threshold
	Upload User defined 0K ops (Default unit: K)
	Download User defined 0K ops (Default unit: K)
Active When:	Any of the selected WAN disconnect
	All of the selected WAN disconnect
	WAN 1 WAN 2 WAN 3 WAN 4

VLAN Tag insertion	Customer (TPID 0x8100)	Service (TPID 0x8100)
	Disable Tag value: 0 (0~4095) Priority: 0 (0~7)	Disable Tag value: 0 (0~4095) Priority: 0 (0~7)

Note:

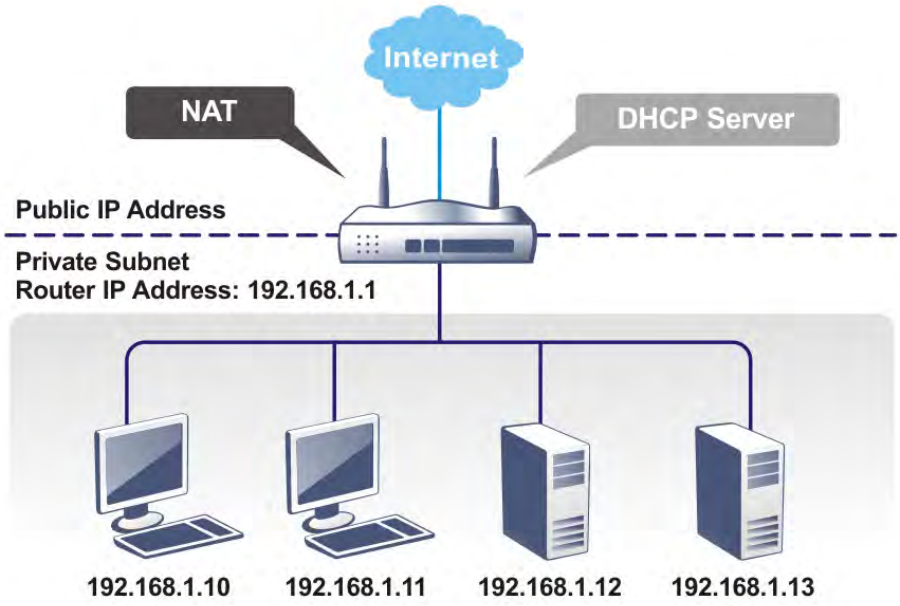
1. The line speed setting of WAN interface is available only when According to Line Speed is selected as the Load Balance Mode.
2. Customer and service tag are used for different network environments. Customer tag is required for most ISPs while Service tag is required when ISP needs QinQ packets.

資訊

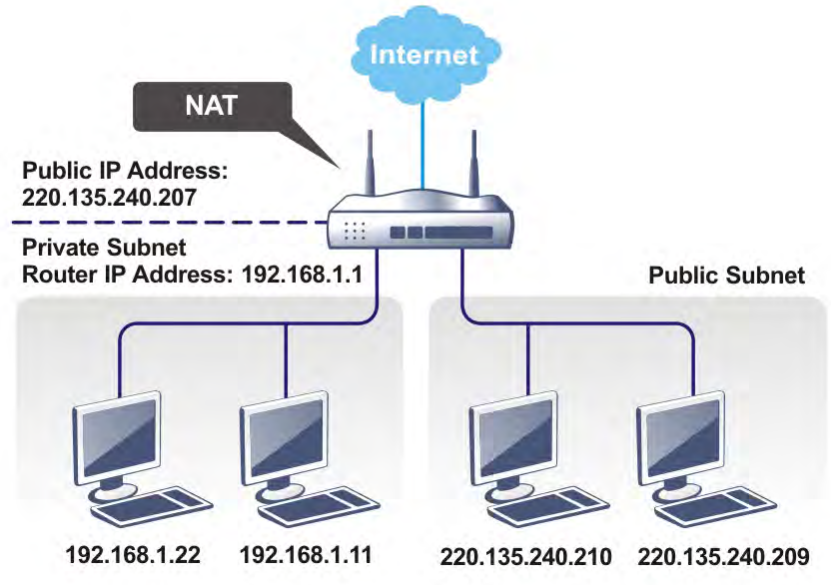
路由器可以依照 WAN>>網際網路連線(WAN>>Internet Access)中的 WAN 連線偵測(WAN Connection Detection)設定來決定某個 WAN 介面是否斷線

II-2 LAN

Vigor 路由器最基本的功能爲 NAT，可用來建立虛擬的子網路，如前所述，路由器利用真實 IP 位址與網際網路上其他的真實主機互相通訊，或是使用虛擬 IP 位址與區域網路上的主機連繫。NAT 要完成的事情就是轉換來自真實 IP 位址的封包到私有 IP 地址，以便將正確的封包傳送至正確的主機上，反之亦然。此外 Vigor 路由器還有內建的 DHCP 伺服器，可指定虛擬 IP 地址至每個區域主機上，請參考下麵的範例圖，即可獲得大略的瞭解。



在某些特殊的情形當中，您可能會有 ISP 提供給您的真實 IP 子網路像是 220.135.240.0/24，這表示您可以設定一個真實子網路，或是使用配備有真實 IP位址之主機的第二組子網路，作爲真實子網路的一部份，Vigor 路由器將會提供 IP 路由服務，幫助真實地區子網路上的主機能與其他真實主機/外部伺服器溝通連繫，因此路由器必須設定爲真實主機的通訊閘道才行。



什麼是 RIP(Routing Information Protocol)

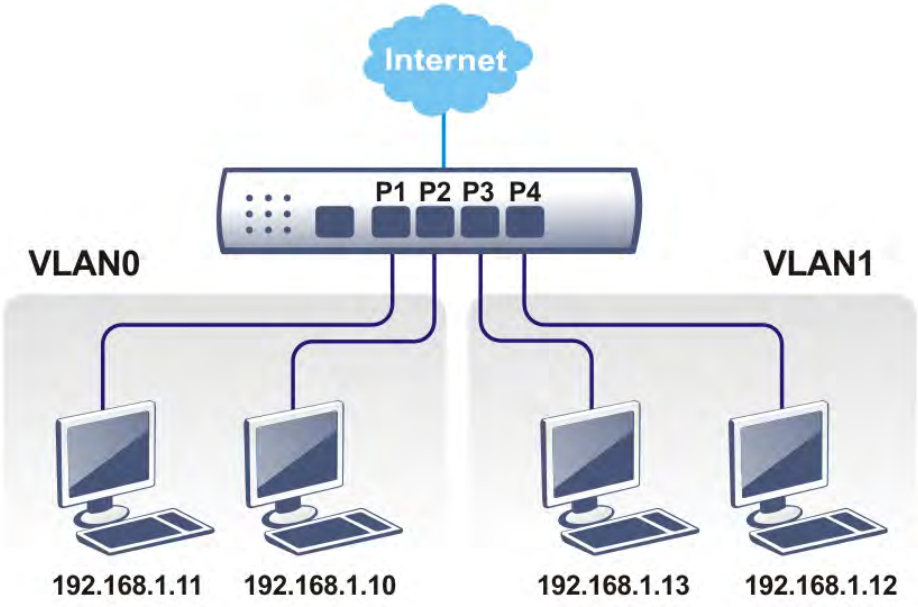
Vigor 路由器可利用 RIP 與鄰近路由器交換路由資訊，達到 IP 路由的目的。這樣可讓使用者變更路由器的資訊，例如 IP 地址，且路由器還會自動通知雙方此類訊息。

什麼是固定路由

當您的區域網路上有數個子網路時，比起其他的方法有時候對連線來說最有效也是最快速的方式就是固定路由功能，您可設定一些規則來傳送指定子網路上的資料到另一個指定的子網路上而不需要透過 RIP。

什麼是虛擬區域網路(VLAN)

您可以利用實體的連接埠將群組區域網路上的主機，然後建立虛擬區域網路，最多可達 4 個。爲了要管理不同群組間的通訊狀況，請再虛擬區域網路功能上設定一些規則，以及每個網路的傳送速率。



網頁使用者介面

區域網路(LAN)是由一群 LAN 用戶端亦即所在位置所有的網路裝置組合而成，LAN 用戶端可以是電腦、印表機、VoIP 電話、行動電話、遊戲機、IPTV 等等，可透過有線(使用乙太網路纜線)或是無線(使用 Wi-Fi)網路連線。

在相同區域網路下的用戶端一般可以直接與另一個設備溝通，只要他們是彼此的另一端即可。除非是透過某些方法如防火牆或是 VLAN 等功能限制了彼此的存取，例如，從 Windows XP 開始的微軟系統與 Apple OS X 系統都有內建的防火牆可以設定限制進出資料流量，另一方面，使用網路交換器或是路由器(例如本 Vigor 路由器)設定 VLAN 功能。

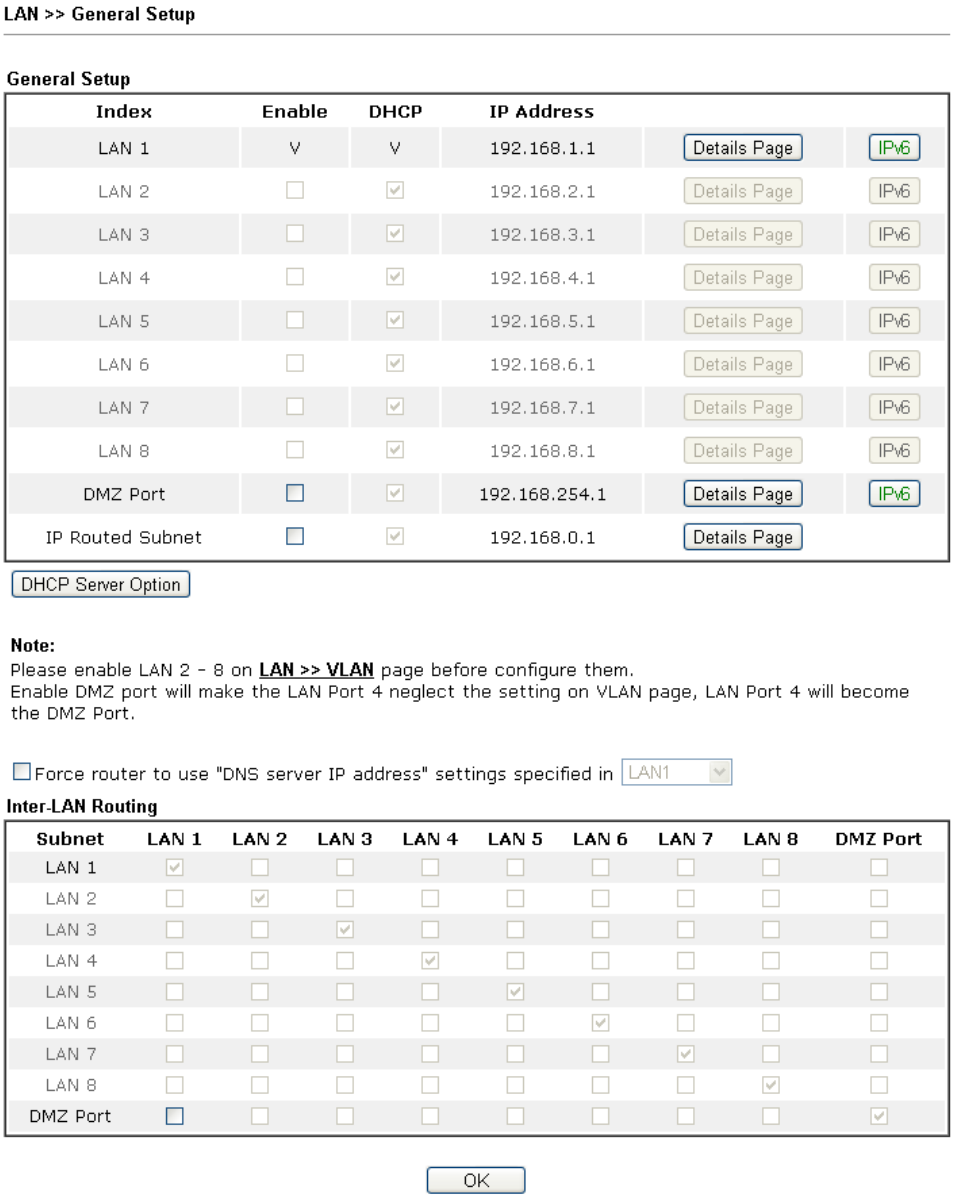
爲了能跟區域網路外部的主機溝通，區域網路用戶端必須通過網路閘道，在大部分的例子中，此閘道多半是位於區域網路與 ISP 網路(指的是 WAN 廣域網路)之間的路由器。路由器就像是一個指引器，可確保區域網路(LAN)與廣域網路(WAN)之間的流量達到預期的目的地。



II-2-1 基本設定(General Setup)

本頁提供您區域網路的基本設定。按**區域網路(LAN)**開啓區域網路設定並選擇**基本設定(General Setup)**。

路由器提供數個子網，讓使用者來區隔，此外，不同子網可透過 Inter-LAN 路由讓彼此互通。目前 LAN1 設定固定爲 NAT 模式專用，LAN2 至 LAN8 可用於 NAT 或是路由模式。IP 路由子網則可於路由模式下操作。



可用設定說明如下：

項目	說明
基本設定 (General Setup)	允許針對個別子網設定不同內容。 **索引編號(Index) -**.顯示全部的 LAN 項目。 **狀態(Status) -** 基本上 LAN1 狀態於預設時是啓用的，LAN2 之後與 IP 路由子網只有在狀態欄位已勾選時，始可查閱。 **DHCP-** 預設狀態下，LAN1 設定爲 DHCP 模式，如果有必要，請針對每個 LAN 勾選此方塊。 **IP 位址 -** 顯示每個 LAN 的 IP 位址。 **細節設定(Details Page) -** 按下此鈕可進入設定頁面，每條 LAN 都可以有不同的設定內容，也勾可以設定在不同的子網下。 **IPv6 –** 按下此鈕進入 IPv6 設定頁面。
DHCP 伺服器選項(DHCP Server Option)	DHCP 封包可以藉由新增 option 號碼以及資料資訊來處理。 詳情請參考後續章節說明。
強迫路由器使用...	強迫路由器使用 LAN1 / LAN2 / LAN3 / LAN4 / LAN5 / LAN6 /

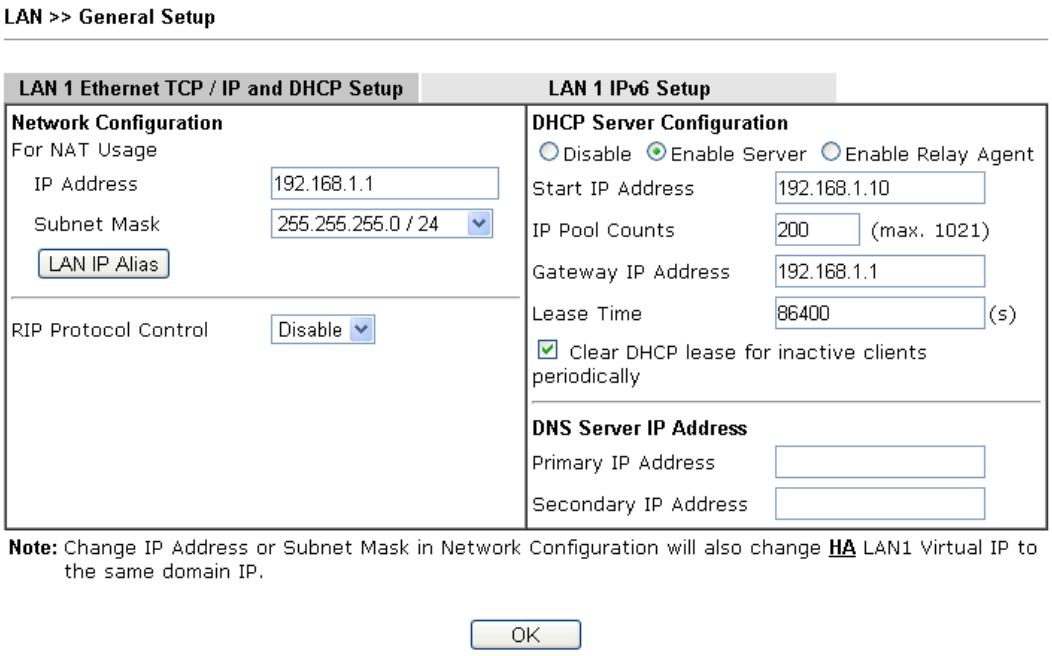
(Force router to use DNS server IP address ……)	LAN7 / LAN8 / DMZ Port 中設定的 DNS 伺服器而非網際網路存取伺服器((PPPoE, PPTP, L2TP 或 DHCP 伺服器)指定的 DNS 伺服器。
Inter-LAN 路由 **(Inter-LAN Routing)**	勾選方塊來連結二個或是多個不同的子網(LAN 與 LAN 間)。 Inter-LAN 路由允許不同的 LAN 子網彼此之間相連或是隔離。這個功能僅在 VLAN 功能已被啓用時可用。 在 Inter-LAN 路由矩陣時，選定的核取方框表示這二個互相交叉之區域網路可以彼此溝通。

當您完成上述設定之後，請按下**確定(OK)**儲存。

資訊	如欲設定子網，請選擇細節設定頁面，開啓設定頁面。

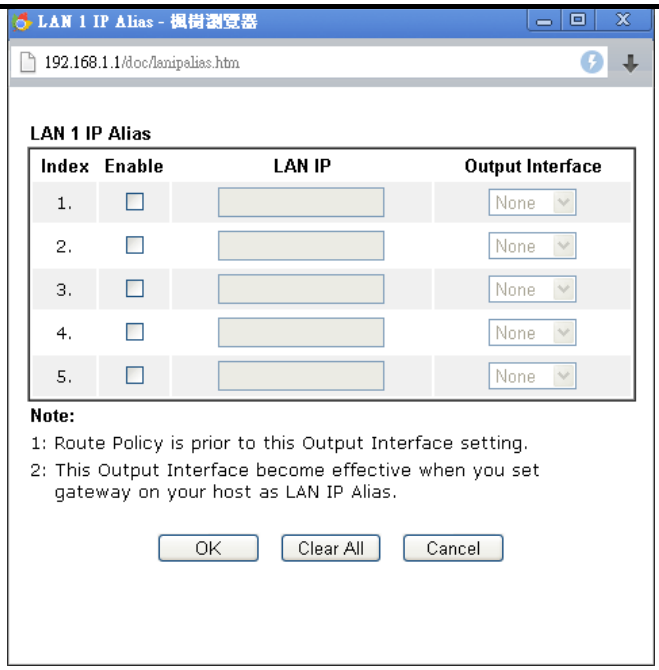
II-2-1-1 LAN1–乙太網路 TCP/IP 與 DHCP 設定之細節設定

LAN1 中有二種設定頁面，一個是乙太網路 TCP/IP 與 DHCP 設定(以 IPv4 爲基準)，另一個是 IPv6 設定。按下每個類型的標籤，並參考下述說明：



可用設定說明如下：

項目	說明
網路設定 **(Network Configuration)**	**針對 NAT 用途，** **IP 位址(IP Address)** - 請輸入虛擬 IP 位址以便連接區域虛擬網路(預設值爲 192.168.1.1)。 **子網路遮(Subnet Mask)** - 請輸入決定網路大小的位址代碼(預設值爲 255.255.255.0/ 24)。 **LAN IP 別名(LAN IP Alias)** – 此功能允許定多重閘道(在交換器下)，每個閘道有不同的 WAN 介面，以便透過路由器存取網際網路。



RIP 協定控制,

停用(Disable) - 關閉 RIP 協定，可讓不同路由器之間資訊交換暫停 (此爲預設值)。

啓用(Enable) - 啓動此協定。

DHCP 伺服器組態
(DHCP Server Configuration)

DHCP 是 Dynamic Host Configuration Protocol 的縮寫，路由器的出廠預設值可以作爲您的網路的 DHCP 伺服器，所以它可自動分派相關的 IP 設定給區域的使用者，將該使用者設定成爲 DHCP 的用戶端。如果您的網路上並沒有任何的 DHCP 伺服器存在，建議您讓路由器以 DHCP 伺服器的型態來運作。

如果您想要使用網路上另外的 DHCP 伺服器，而非路由器的伺服器，您可以利用中繼代理來幫您重新引導 DHCP 需求到指定的位置上。

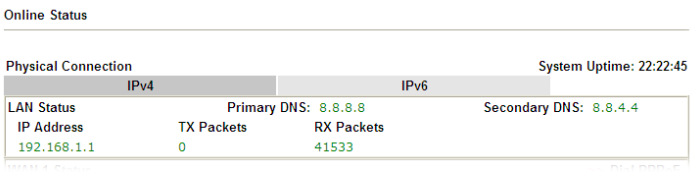
停用(Disable) - 讓您手動指定 IP 地址到區域網路上的每個主機上。

啓用伺服器(Enable Server) - 讓路由器指定 IP 地址到區域網路上的每個主機上。

- **起始 IP 位址(Start IP Address) -**輸入 DHCP 伺服器的 IP 位址配置的數值作爲指定 IP 位址的起始點。
- **IP 配置數量(IP Pool Counts) -** 輸入您想要 DHCP 伺服器指定 IP 地址的最大數量，預設值爲 200，最大值爲 1021。
- **閘道 IP 位址(Gateway IP Address) -**輸入 DHCP 伺服器所需的閘道 IP 位址，這項數值通常與路由器的第一組 IP 位址相同，表示路由器爲預設的閘道。
- **租約時間(Lease Time) -** 輸入 DHCP 伺服器可以使用來分派 IP 位址的時間長度。
- **定期從不再運作的用戶端取回 IP 位址(Clear DHCP lease for inactive clients periodically) -** 選擇此項後，路由器將發送 ARP 請求，以便回收早先分配給未活動 DHCP 客戶端的 IP 位址，防止 IP 位置耗竭殆盡。

  注意: 當啓用此功能時，路由器將會執行如下作業：

  ■ 當可用的 DHCP IP 配置數量低於 30 個的時候，透過

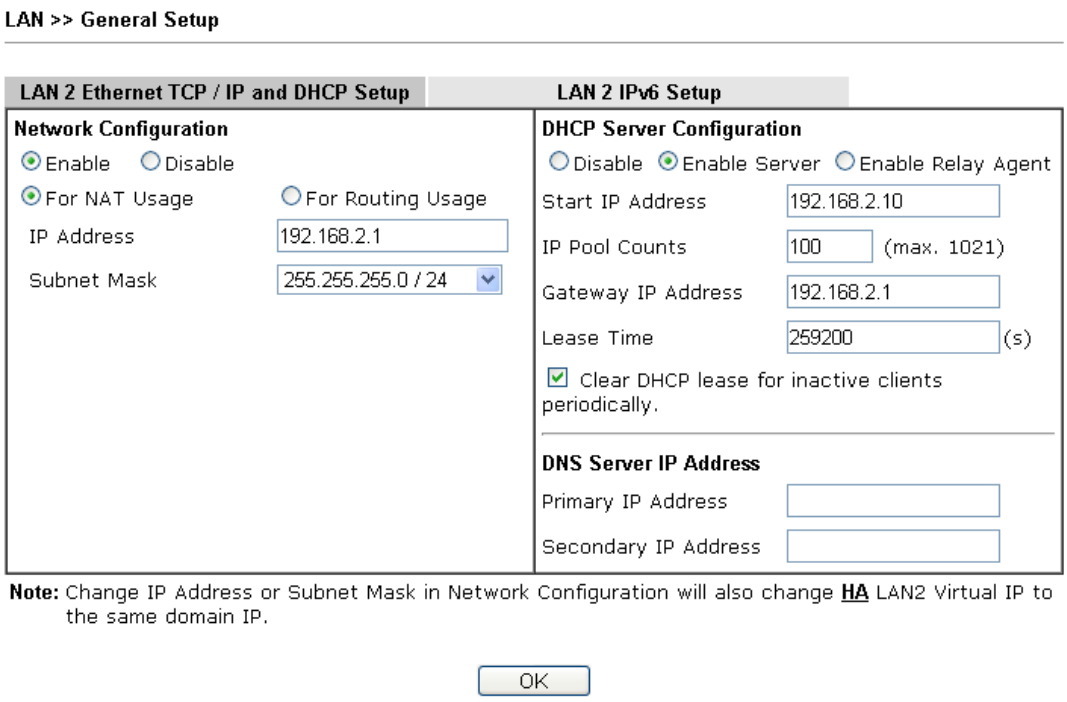
	每分鐘 ARP 請求，檢查 DHCP 用戶的活動狀況 ■ 當用戶端不回應 ARP 請求時，清除 DHCP 分派位址 **啓動中繼代理(Enable Relay Agent)** – 選擇此項後，所有的 DHCP 請求都會被轉發至 LAN 子網外的 DHCP 伺服器上，需求的 IP 位址就從 DHCP 伺服器 IP 位址欄位中指定。 ● **DHCP 伺服器 IP 位址(DHCP Server IP Address) -** 當您勾選了**啓動中繼代理**之後，即可見到此項目，設定您準備使用的伺服器 IP 位址讓中繼代理幫忙轉送 DHCP 需求至 DHCP 伺服器上。
DNS 伺服器組態 **(DNS Server IP Address)**	DNS 是 Domain Name System 的縮寫，每個網際網路的主機都必須擁有獨特的 IP 位址，也必須有人性化且容易記住的名稱諸如 www.yahoo.com 一般，DNS 伺服器可轉換此名稱至相對應的 IP 地址上。 **主要 IP 位址(Primary IP Address) -**您必須在此指定 DNS 伺服器的 IP 位址，因爲通常您的 ISP 應該會提供一個以上的 DNS 伺服器，如果您的 ISP 並未提供，路由器會自動採用預設的 DNS 伺服器 IP 地址 194.109.6.66，放在此區域。 **次要 IP 位址(Secondary IP Address) -** 您可以在此指定第二組 DNS 伺服器 IP 位址，因爲 ISP 業者會提供一個以上的 DNS 伺服器。如果您的 ISP 並未提供，路由器會自動採用預設的第二組 DNS 伺服器，其 IP 位址爲 194.98.0.1，放在此區域。 預設 DNS 伺服器 IP 位址可在線上狀態上查看:  如果主要和次要 IP 地址區都是空白的，路由器將會指定其本身的 IP 位址給予本地使用者作爲 DNS 代理伺服器並且仍保有 DNS 快速緩衝貯存區。 如果網域名稱的 IP 位址已經在 DNS 快速緩衝貯存區內，路由器將立即解析網域名稱。否則路由器會藉著建立 WAN (例如 DSL/Cable)連線時，傳送 DNS 疑問封包至外部 DNS 伺服器。

當您完成上述設定之後，請按下**確定(OK)**儲存。

系統可以透過 DHCP 自動分派虛擬 IP 位址給 LAN 端的用戶或是手動輸入給予。向 DHCP 客戶端分派 IP 位址的 DHCP 伺服器可以是路由器(最常見的例子)或是另一個伺服器。

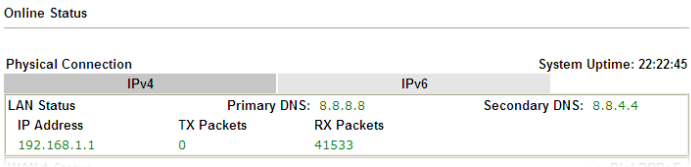
或者，可以手動輸入固定 IP 予 LAN 用戶，無論如何設定 IP 位址，沒有二個裝置會設定成相同的 IP 位址。若要在網路中同時使用 DHCP 與固定 IP 位址，請自 DHCP IP 配置中排除該固定 IP。例如，您的 LAN 使用 192.168.1.x 網段而您有 20 個 DHCP 用戶端以及 20 個固定 IP 用戶，您可以將 192.168.1.10 設定成起始 IP 位址，IP 配置數量設定爲 50，使用大於 192.168.1.100 的位址作爲固定 IP 分派用。

II-2-1-2 LAN2 ~ LAN8 與 DMZ 之細節設定



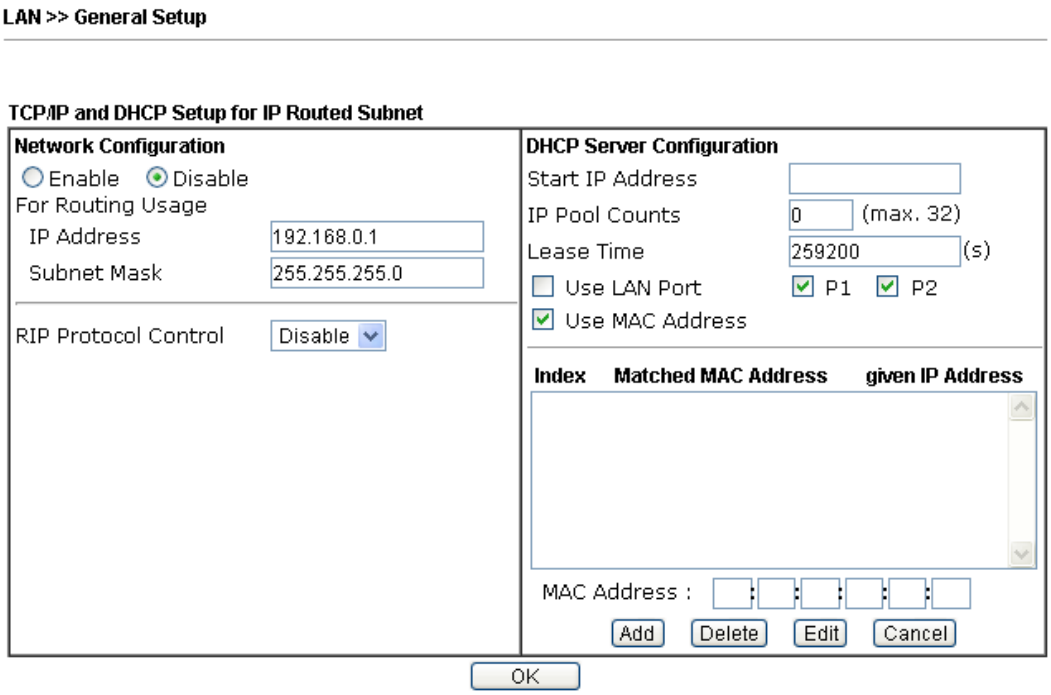
可用設定說明如下：

項目	說明
網路設定 (Network Configuration)	**啓用/停用(Enable/Disable) -** 選擇**啓用**來啓動此設定，按下**停用**則關閉此設定。 **供 NAT 用途(For NAT Usage)-** 選擇此鈕讓設定資料供 NAT 使用。 **用於路由(For Routing Usage)-** 選擇此鈕讓設定資料套用於路由。 **IP 位址(IP Address)** - 請輸入虛擬 IP 位址以便連接區域虛擬網路(預設值爲 192.168.1.1)。 **子網路遮罩(Subnet Mask) -** 請輸入決定網路大小的位址代碼(預設值爲 255.255.255.0/ 24)。
DHCP 伺服器組態 (DHCP Server Configuration)	**停用(Disable) -** 讓您手動指定 IP 地址到區域網路上的每個主機上。 **啓用伺服器(Enable Server) -** 讓路由器指定 IP 地址到區域網路上的每個主機上。 ● **起始 IP 位址(Start IP Address) -**輸入 DHCP 伺服器的 IP 位址配置的數值作爲指定 IP 位址的起始點。 ● **IP 配置數量(IP Pool Counts) -** 輸入您想要 DHCP 伺服器指定 IP 地址的最大數量，預設值爲 100，最大值爲 1021。 ● **閘道 IP 位址(Gateway IP Address) -**輸入 DHCP 伺服器所需的閘道 IP 位址，這項數值通常與路由器的第一組 IP 位址相同，表示路由器爲預設的閘道。 ● **租約時間(Lease Time)** - 輸入 DHCP 伺服器可以使用來分派 IP 位址的時間長度。 ● **定期從不再運作的用戶端取回 IP 位址(Clear DHCP lease for inactive clients periodically) -** 選擇此項後，路由器將發送 ARP 請求，以便回收早先分配給未活動 DHCP 客戶端的 IP 位址，防止 IP 位置耗竭殆盡。

	注意: 當啓用此功能時，路由器將會執行如下作業： ■ 當可用的 DHCP IP 配置數量低於 30 個的時候，透過每分鐘 ARP 請求，檢查 DHCP 用戶的活動狀況 ■ 當用戶端不回應 ARP 請求時，清除 DHCP 分派位址 **啓動中繼代理(Enable Relay Agent)** – 選擇此項後，所有的 DHCP 請求都會被轉發至 LAN 子網外的 DHCP 伺服器上，需求的 IP 位址就從 DHCP 伺服器 IP 位址欄位中指定。 ● **DHCP 伺服器 IP 位址(DHCP Server IP Address) -** 當您勾選了**啓動中繼代理**之後，即可見到此項目，設定您準備使用的伺服器 IP 位址讓中繼代理幫忙轉送 DHCP 需求至 DHCP 伺服器上。
DNS 伺服器組態 **(DNS Server IP Address)**	DNS 是 Domain Name System 的縮寫，每個網際網路的主機都必須擁有獨特的 IP 位址，也必須有人性化且容易記住的名稱諸如 www.yahoo.com 一般，DNS 伺服器可轉換此名稱至相對應的 IP 地址上。 **主要 IP 位址(Primary IP Address) -**您必須在此指定 DNS 伺服器的 IP 位址，因爲通常您的 ISP 應該會提供一個以上的 DNS 伺服器，如果您的 ISP 並未提供，路由器會自動採用預設的 DNS 伺服器 IP 地址 194.109.6.66，放在此區域。 **次要 IP 位址(Secondary IP Address) -** 您可以在此指定第二組 DNS 伺服器 IP 位址，因爲 ISP 業者會提供一個以上的 DNS 伺服器。如果您的 ISP 並未提供，路由器會自動採用預設的第二組 DNS 伺服器，其 IP 位址爲 194.98.0.1，放在此區域。 預設 DNS 伺服器 IP 位址可在線上狀態上查看:  如果主要和次要 IP 地址區都是空白的，路由器將會指定其本身的 IP 位址給予本地使用者作爲 DNS 代理伺服器並且仍保有 DNS 快速緩衝貯存區。 如果網域名稱的 IP 位址已經在 DNS 快速緩衝貯存區內，路由器將立即解析網域名稱。否則路由器會藉著建立 WAN (例如 DSL/Cable)連線時，傳送 DNS 疑問封包至外部 DNS 伺服器。

當您完成上述設定之後，請按下**確定(OK)**儲存。

II-2-1-3 IP 路由子網之細節設定



可用設定說明如下：

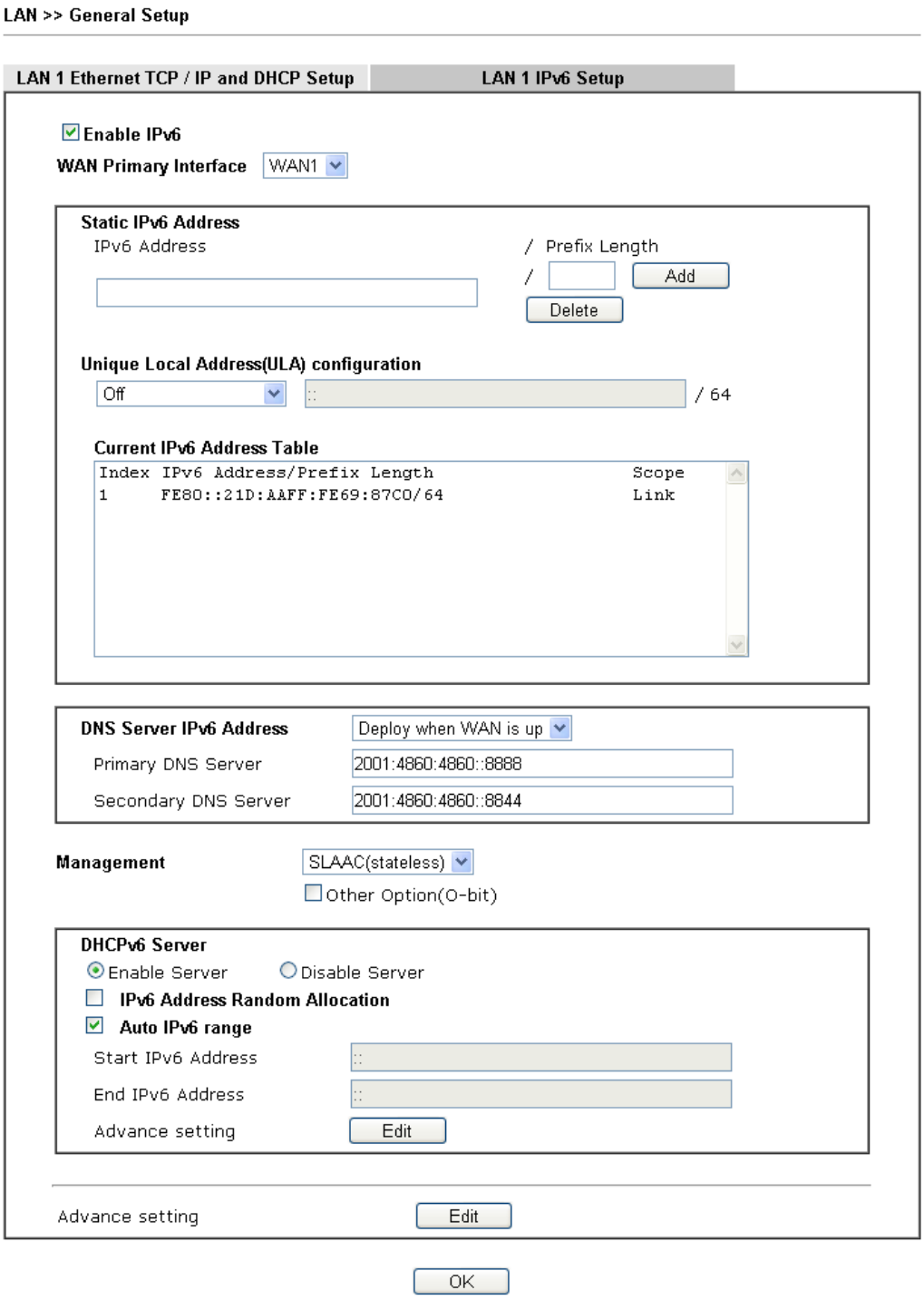
項目	說明
網路設定 (Network Configuration)	**啓用/停用(Enable/Disable) -** 選擇**啓用**來啓動此設定，按下**停用**則關閉此設定。 **針對路由用途,** **IP 位址(IP Address)** - 請輸入虛擬 IP 位址以便連接區域虛擬網路(預設值爲 192.168.1.1)。 **子網路遮(Subnet Mask) -** 請輸入決定網路大小的位址代碼(預設值爲 255.255.255.0/ 24)。 **RIP 協定控制,** **停用(Disable) -** 關閉 RIP 協定，可讓不同路由器之間資訊交換暫停 (此爲預設值)。 **啓用(Enable) -** 啓動此協定。路由器將會嘗試以相鄰路由器透過 RIP 協定進行路由資訊交換。
DHCP Server Configuration	DHCP 是 Dynamic Host Configuration Protocol 的縮寫，路由器的出廠預設值可以作爲您的網路的 DHCP 伺服器，所以它可自動分派相關的 IP 設定給區域的使用者，將該使用者設定成爲 DHCP 的用戶端。如果您的網路上並沒有任何的 DHCP 伺服器存在，建議您讓路由器以 DHCP 伺服器的型態來運作。 如果您想要使用網路上另外的 DHCP 伺服器，而非路由器的伺服器，您可以利用中繼代理來幫您重新引導 DHCP 需求到指定的位置上。 **起始 IP 位址(Start IP Address) -**輸入 DHCP 伺服器的 IP 位址配置的數值作爲指定 IP 位址的起始點。 **IP 配置數量(IP Pool Counts) -** 輸入您想要 DHCP 伺服器指定 IP 地址的最大數量。

	租約時間(Lease Time) - 輸入 DHCP 伺服器可以使用來分派 IP 位址的時間長度。 **使用 LAN 埠口(Use LAN Port) -** 指定一個 IP 位址供 IP 路由子網使用，如果啓用此埠，DHCP 伺服器將會自動指派一個 IP 位址給予 P1 與/或 P2 的用戶。請勾選準備使用的 LAN 埠口(P1 與/或 P2)。 **使用 MAC 位址(Use MAC Address) -**勾選此方框可指定 MAC 位址。 ● **MAC 位址(MAC Address)-**輸入輸入主機的 MAC 位址然後按下方的新增(Add)按鈕，建立伺服器分派位址的主機清單，也可以刪除或編輯清單內容。設定一群 MAC 位址以因應第二個 DHCP 伺服器使用可以幫助路由器分派給主機正確網段，正確的 IP 位址。如此一來再第二個網段下的主機就不會從第一個網段中取得任何 IP 位址。 **新增(Add) -** 在上方 MAC 位址框中輸入位址內容，按下此鈕之後即可新增。 **刪除(Delete)** – 刪除上方選定的 MAC 位址。 **編輯(Edit)** – 編輯上方選定的 MAC 位址。 **取消(Cancel)** – 取消新增、編輯以及刪除等運作。

當您完成上述設定之後，請按下**確定(OK)**儲存。

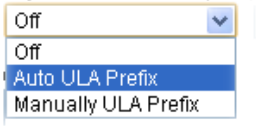
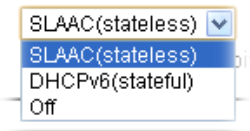
II-2-1-4 LAN IPv6 設定之細節設定

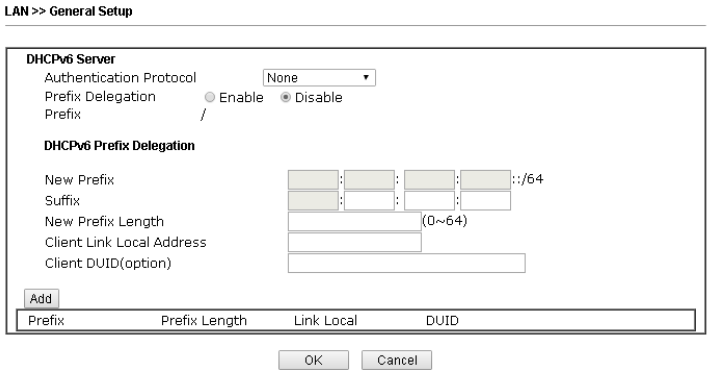
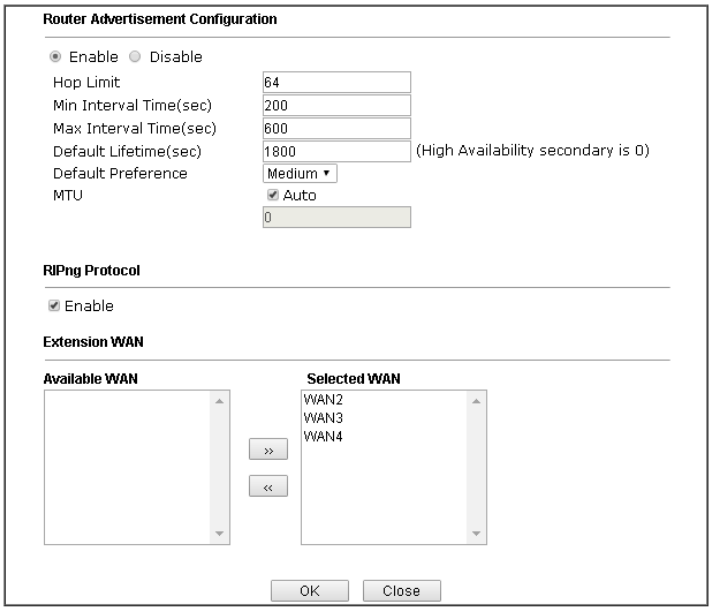
LAN1/LAN2/LAN3/LAN4/LAN5/LAN6/DMZ 埠口有二種設定頁面，一個是乙太網路 TCP/IP 與 DHCP 設定頁面(基於 IPv4)，另一個是 IPv6 設定頁面。按下每種類型的標籤並參考本節如下的說明。下圖爲 IPv6 設定頁面。



可用設定說明如下：

項目	說明
啓用 IPv6 (Enable IPv6)	勾選此框啓用 LAN 1 IPv6 設定。
WAN 主要介面(WAN Primary Interface)	使用下拉式清單指定一個 WAN 介面。
固定 IPv6 位址設定(Static IPv6 Address configuration)	**IPv6 位址(IPv6 Address)** – 輸入固定 IPv6 位址。 **前置碼長度(Prefix Length) –** 輸入一個固定值作爲前置碼長度。 **新增(Add) –** 按此新增一條新的位址。

	刪除(Delete) - 按此移除現有的位址。
ULA 設定 **(Unique Local Address (ULA) configuration)**	ULA 是分派給 LAN 用戶端的虛擬 IPv6 位址。 **停用(Off) -** 停用 ULA。 **手動輸入 ULA 前置碼(Manually ULA Prefix) -** LAN 用戶端取得之 ULA 將依照手動輸入的前置碼產生。 **自動取得 ULA 前置碼(Auto ULA Prefix) -** LAN 用戶端取得之 ULA 將依照系統自動決定的前置碼產生。 
目前 IPv6 位址表格 **(Current IPv6 Address Table)**	顯示目前使用的 IPv6 位址。
DNS 伺服器 IPv6 位址 **(DNS Server IPv6 Address)**	**當 WAN 上線時才配置(Deploy when WAN is up) -** 含 DNS 伺服器資訊的 RA (router advertisement) 封包僅在任何一個 WAN 介面連上網路時傳送至 LAN PC。 **啓用(Enable) -** 含 DNS 伺服器資訊的 RA (router advertisement) 封包將傳送至 LAN PC，不論 WAN 有無連線。 ● **主要 DNS 伺服器(Primary DNS Sever) -** 輸入主要 DNS 伺服器的 IPv6 位址。 ● **次要 DNS 伺服器(Secondary DNS Server) -** 輸入次要 DNS 伺服器的 IPv6 位址。 **停用(Disable) -** 不再使用 DNS 伺服器。
管理(Management)	設定在路由廣播下的 Managed Address Configuration flag (M-bit) 。 ● **關閉(Off) -** 無任何設定資訊會透過 RA 傳送出去。 ● **SLAAC(stateless) -** M-bit 未設定。 ● **DHCPv6(stateful) -** M-bit 已設定，表示 LAN 用戶端應該自 DHCPv6 伺服器獲得所有的 IPv6 設定資訊。DHCPv6 伺服器可以是路由器內建伺服器或是另外的 DHCPv6 伺服器。  **其他選項(Other Option (O-bit)) -** 勾選此框啓用 O-bit 以便從 DHCPv6 獲取額外的資訊(例如 DNS)。 選定此項時，其他設定旗標已設定完畢，表示除了 LAN IPv6 位址外的 IPv6 設定資訊皆可從 DHCPv6 伺服器取得。 設定 M-bit (參考上方的管理 **Management**)亦有同樣的效果，如同 O-bit 的 DHCPv6 提供所有的 IPv6 設定資訊。
DHCPv6 伺服器(DHCPv6 Server)	**啓用伺服器(Enable Server) -** 啓動 DHCPv6 伺服器，DHCPv6 伺服器可以依照起始/結束 IP 位址設定來分派 IPv6 位址至電腦上。 **停用伺服器(Disable Server) -** 停用 DHCPv6 伺服器的運作。 **自動 IPv6 範圍(Auto IPv6 range) -** 勾選此框後，路由器將會

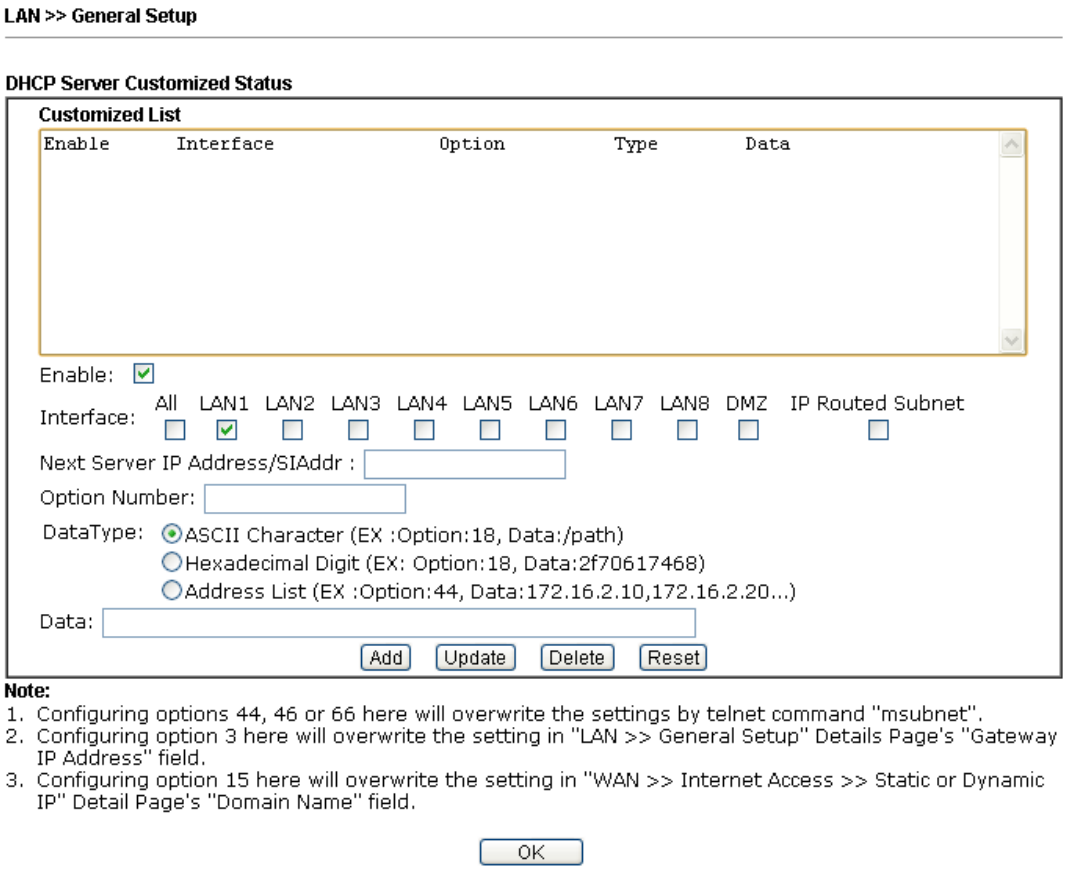
	自動指定 IPv6 範圍以分派位址。 **起始 IPv6 位址 / 結束 IPv6 位址(Start IPv6 Address / End IPv6 Address)** – 分別輸入起始以及結束的 IP 位址。 **進階設定(Advance setting)** – 按下編輯(Edit)按鈕以便設定 DHCPv6 伺服器進階的內容。 
進階設定(Advance setting)	進階設定頁面具有額外的路由器廣播功能設定，並可啓用多重 WAN 介面供 IPv6 流量使用。  **路由器廣播設定(Router Advertisement Configuration)** – 按下**啓用(Enable)** 以使用路由器廣播伺服器。當某個節點提出需求傳送路由器蒐集(Router Solicitation)訊息時，路由器廣播伺服器將定期傳送 RFC 2461 所指定的路由器廣播訊息至本機乙太網路 LAN 上。IPv6 stateless 自動配置需要這些訊息。 **停用(Disable)** – 按此停用路由器的 RA 伺服器。 **躍點限制(Hop Limt) –** 使用 IPv6 時，需要輸入此數值予位於路由器後方的裝置使用。 **最小/最大間隔時間(Min/Max Interval Time (sec)) –** 定義傳送 RA 封包的間隔(最小時間與最大時間二者之間)。 **預設有效時間(Default Lifetime (sec)) –** 在此期間，路由器可被視之爲預設的閘道器。 **預設優先(Default Preference) –** 當 RA 封包傳送時，決定路由器後方主機的優先權。 **MTU –** 封包的最大傳輸單位，若選擇**自動(Auto)**，路由器將自

	行決定 LAN 端的 MTU 數值。 **RIPng 通訊協定(RIPng Protocol)-**下一代 RIP(RIPng) 提供與 IPv4 RIP v2 相同的功用。 **延伸 WAN(Extension WAN) -** 除了在 LAN IPv6 設定頁面中於 WAN 主要介面，指定處理 IPv6 流量之預設 WAN 外，可以在延伸 WAN 處選擇其他的 WAN 介面來處理 IPv6 流量。 **可用 WAN(Available WAN)** – 其他可用但目前尚未被選定做爲處理 IPv6 流量的 WAN 介面。 **選定 WAN(Selected WAN)** – 用來處理 IPv6 流量的 WAN 介面。

完成進階頁面的設定變更之後，按**確定(OK)**按鈕儲存變更並回到 LAN IPv6 設定頁面。

II-2-1-5 進階 DHCP Options 設定

按下 LAN 基本設定中的 DHCP 伺服器選項(DHCP Server Option)按鈕可以設定 DHCP options。



可用設定說明如下：

項目	說明
客製化清單(Customized List)	顯示系統設定的所有 DHCP 選項設定。
啓用(Enable)	勾選此項啓用此頁設定。
介面(Interface)	指定套用此設定的 LAN 介面。
下一個伺服器 P 位址/SIA 位址(Next Server IP Address/SIAddr)	覆蓋 DHCP 伺服器所提供的 DHCP 下一個伺服器 IP 位址(DHCP Option 66)。

選項號碼(Option Number)	DHCP 選項號碼(例如 100)。
資料類型(DataType)	資料欄位中的資料類型。 **ASCII 字元(ASCII Character)** – 文字字串，範例: /path。 **十六進位數字(Hexadecimal Digit) -** 十六進位的字串，有效字元從 0 到 9，從 a 到 f，範例: 2f70617468。 **位址清單(Address List) –** 一個或多個 IPv4 位址，用逗號分隔。
資料(Data)	此 DHCP 選項的資料內容。

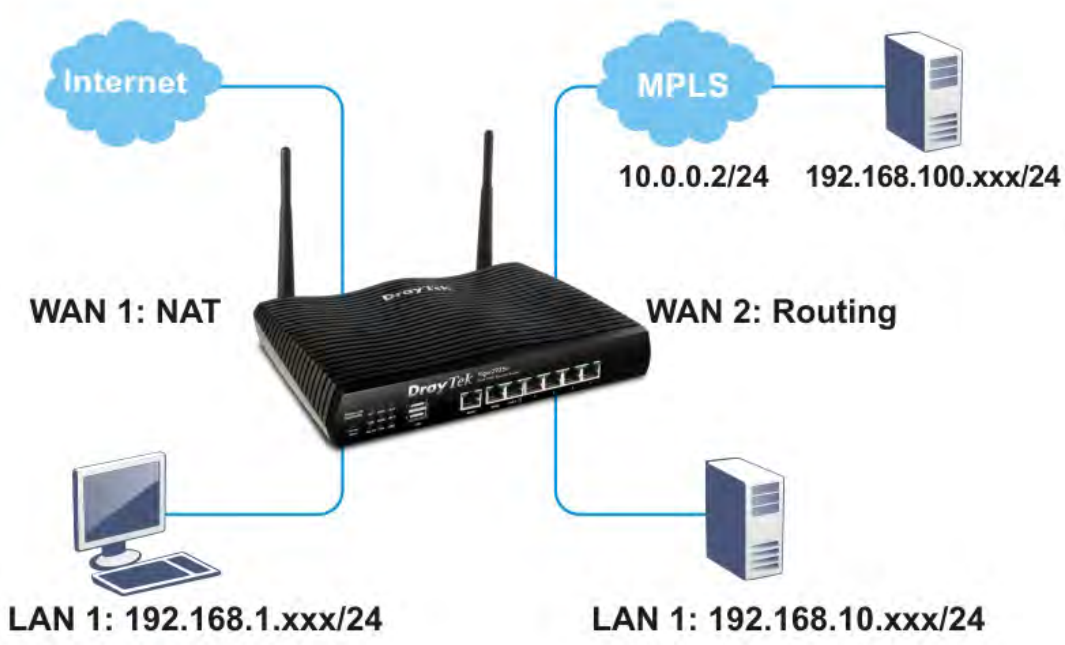
欲重頭開始新增 DHCP option，請先按下**重置(Reset)**按鈕清除資料欄位內所有的資訊，之後填入需求資訊(如啓用、介面、選項號碼、資料類型與資料內容等等)再按下**新增(Add)**，即可增加新的內容。

如要修改現有 DHCP 選項條目，請在**客製化清單(Customized List)**中按該條目，資料欄位將會以目前的數值顯示出來，完成必要的變更之後，按下**更新(Update)**儲存。

如要刪除某個 DHCP 選項條目，請在**客製化清單(Customized List)**中按該條目，然後按下**刪除(Delete)**即可。

應用說明

A-1 多網段應用-如何使用不做 NAT 的 Vigor 路由器?



1. 開啓 **LAN>>基本設定(LAN>>General Setup)**，再按 LAN1 中的**細節設定頁面(Details Page)** 。

LAN >> General Setup

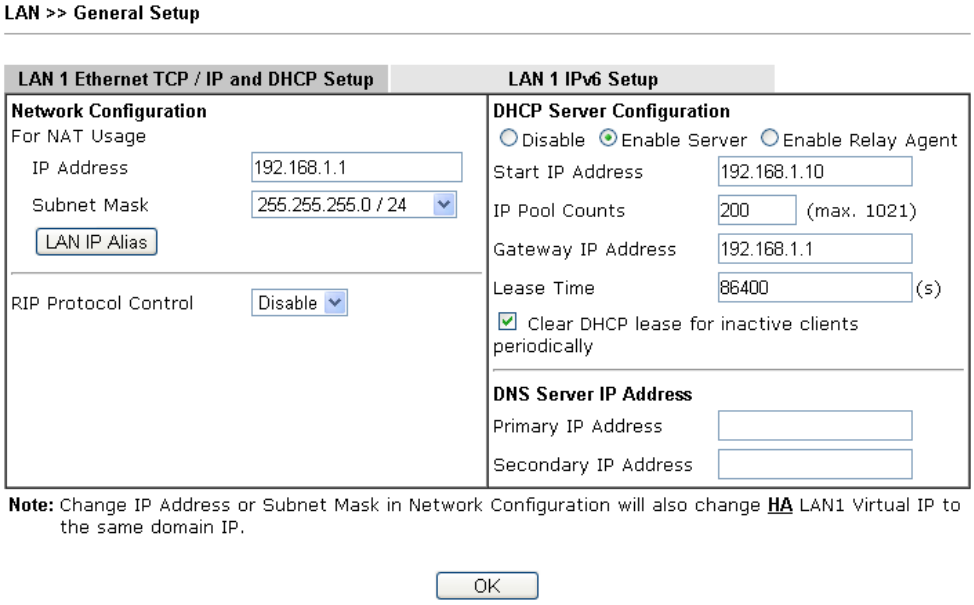
General Setup

Index	Enable	DHCP	IP Address		
LAN 1	V	V	192.168.1.1	Details Page	IPv6
LAN 2	☐	☐	192.168.2.1	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	

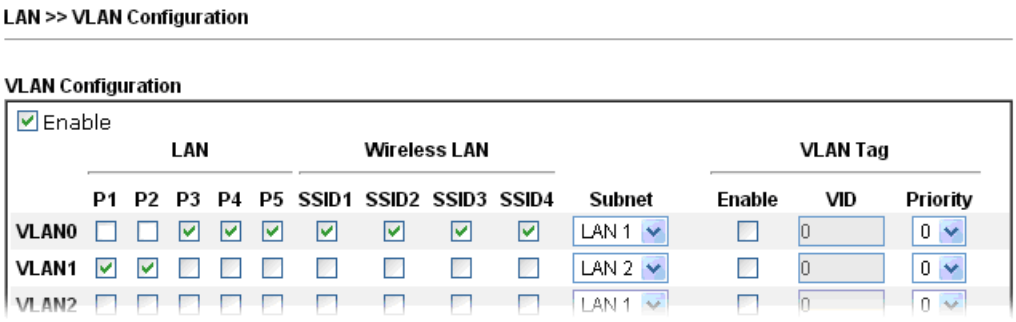
DHCP Server Option

Note:
Please enable LAN 2 - 8 on **LAN >> VLAN** page before configure them.
Enable DMZ port will make the LAN Port 4 neglect the setting on VLAN page, LAN Port 4 will become the DMZ Port.

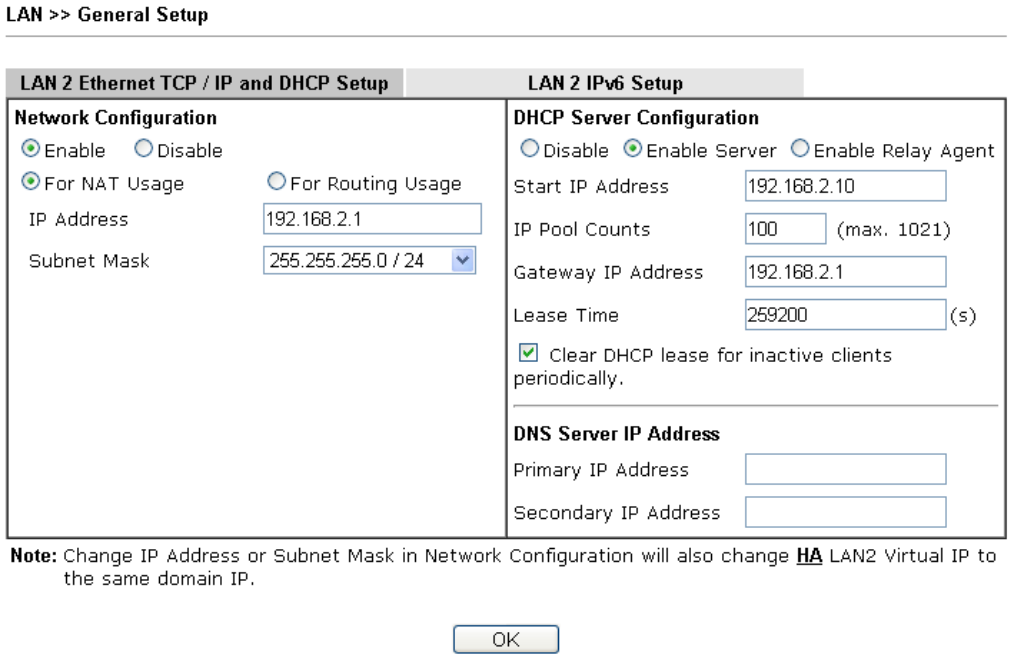
2. 在設定頁面上，依照下圖輸入設定內容，按下**確定(OK)**按鈕儲存設定，請注意 LAN1 永遠用於 NAT。



3. 在 **LAN>>VLAN 設定(LAN>>VLAN Configuration)**頁面中，依照下圖輸入設定內容，按下**確定(OK)**按鈕儲存設定。

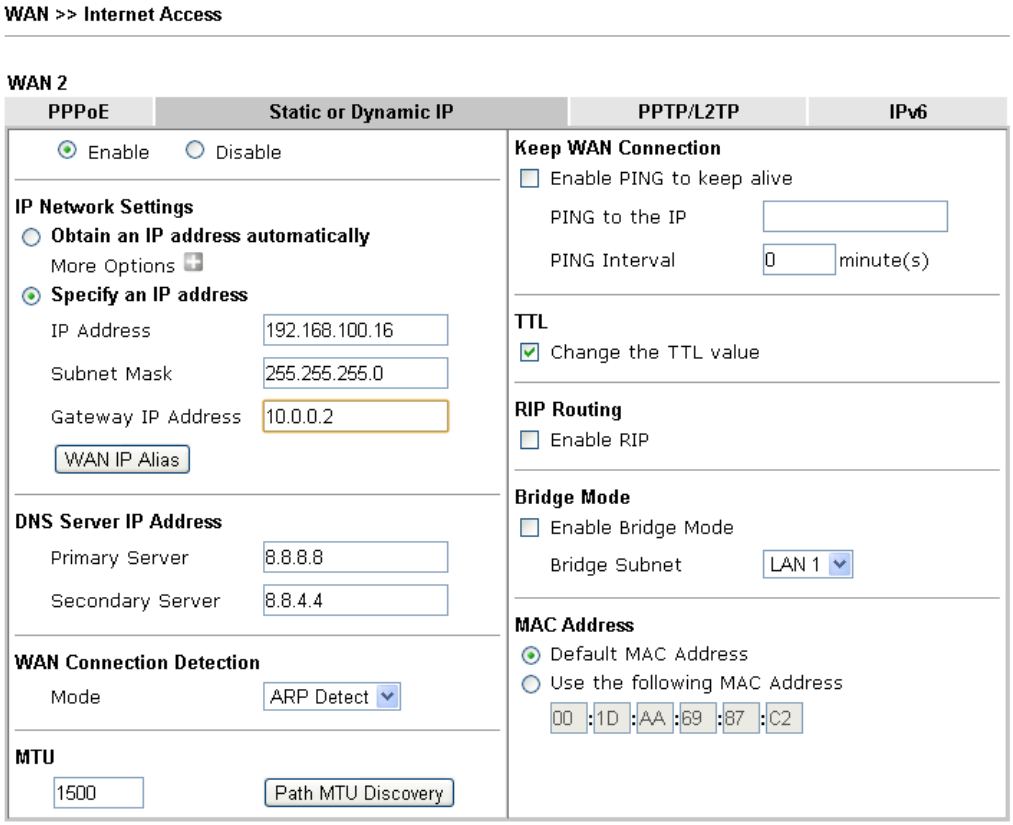


4. 回到 **LAN>>基本設定(LAN>>General Setup)**，LAN2 已經可以設定了，按 LAN2 上的細節設定按鈕開啓如下頁面，選擇**用於路由(For Routing Usage)**，依照下圖輸入相關資訊然後按下**確定(OK)**按鈕儲存。



5. 開啓 **WAN>>網際網路連線(WAN>>Internet Access)**，選擇**固定或動態 IP(Static or Dynamic IP)**作爲**連線模式(Access Mode)**，接著按下**細節設定(Details Page)**頁面。

6. 在設定網頁上，依照下圖輸入相關資訊然後按下**確定(OK)**按鈕儲存。



7. 現在，透過 LAN2 用戶與分公司用戶間的多協定標籤交換(MPLS)建構的網路連線已經成功建立，不再需要網際網路了。

II-2-2 虛擬區域網路(VLAN)

虛擬區域網路(VLAN)讓您細分區域網路以便管理或是改善網路的安全性。

選擇**區域網路>>VLAN(LAN>>VLAN)**開啓 VLAN 設定頁面。

以標籤為主的 VLAN(Tagged VLAN)

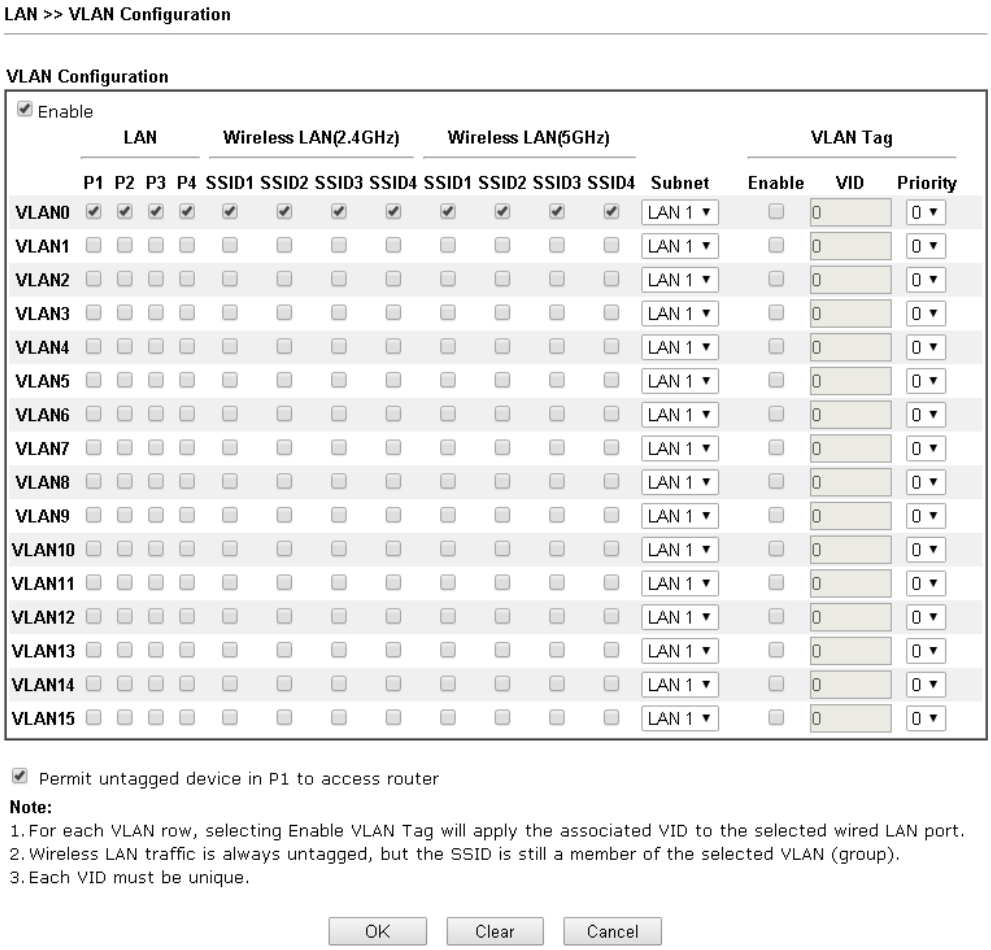
含標籤的 VLANs (802.1q)可將每筆資料標示 VLAN 識別碼，此一識別碼透過乙太網路交換器運送至指定的埠口，當資料傳送到區域網路時，指定的 VLAN 用戶即可以取得此識別碼。您可以設定 LAN 端 QoS 的優先權屬性，分派每個 VLAN 至不同的 IP 子網，讓路由器能操作提供更多不同的服務，這類的功能稱之爲含標籤的多重子網。

以埠口為主的 VLAN(Port-Based VLAN)

相對於以標籤(Tag)爲主的 VLAN 以標籤來群組用戶，以埠口爲主的 VLAN 使用的是實體的 LAN 埠口來區分用戶端至不同的 VLAN 群組上。

VLAN（虛擬區域網路）的功能提供您一個方便的方式，藉由群組實體通訊埠上的連結主機達到管理的目的。請開啓**區域網路>>VLAN**，可出現如下頁面，勾選**啓用(Enable)**方塊啓動 VLAN 功能。

對於具備 2.4GHz 與 5GHz 功能的路由器，網頁顯示如下:



資訊 本頁設定僅能套用於 LAN 埠口而非 WAN 埠口。

可用設定說明如下：

項目	說明
啓用(Enable)	勾選此框啓用 VLAN 設定。
LAN	**P1 - P4**–勾選準備納入此 VALN 群組下的 LAN 埠口。
無線區域網路(2.4GHz) (Wireless LAN (2.4GHz))	**SSID1 - SSID4 -**勾選準備納入此 VLAN 群組下的 SSID 方框。
無線區域網路(5GHz) (Wireless LAN (5GHz))	**SSID1 - SSID4 -**勾選準備納入此 VLAN 群組下的 SSID 方框。 這個選項限用於 Vigor2926ac / Vigor2926Vac / Vigor2926Lac 等型號。
子網(Subnet)	選擇其中一個埠口讓選定的 VLAN 僅對應至此。例如，LAN1 指定爲 VLAN0，就表示在 VLAN0 底下的電腦可透過此子網來取得 IP 位址。
VLAN 標籤 (VLAN Tag)	**啓用(Enable)** – 勾選此框啓用 VLAN 標籤功能。 區域網路中向外傳送的封包，路由器將指定 VLAN 號碼至全部

	封包上。 請輸入標籤值並指定其優先權。 **VID** – 輸入 VLAN ID 號碼值，範圍是 0 到 4095。 **優先權(Priority)** – 選擇此 VLAN 的優先權，範圍是 0 到 7。
允許 P1 中未加標籤的裝置存取路由器 **(Permit untagged device in P1 to access router)**	可讓使用者在設定了錯誤的 VLAN 標籤設定情形下，還能與路由器溝通。由於路由器僅有一個 LAN 實體埠口，建議啓用管理埠口(LAN1)以確保資料傳輸保持暢通。

資訊	至少保留一處未加標籤的 VLAN 以便在發生不預期錯誤時，還能連上路由器。

跨 LAN 路由(Inter-LAN Routing)

路由器支援最多可達 16 組 VLAN，每條 VLAN 可以設定成一個或多個乙太網路埠口與無線區域網路服務組別辨識符(SSID)，在 VLAN(水平行)與 LAN 介面(垂直欄)中，

- 相同 VLAN(水平行)下所有主機彼此可見
- 相同 LAN 或是 WLAN 介面(垂直欄)下所有主機彼此可見，假若
  - 他們皆屬於相同的 VLAN，或是
  - 他們屬於不同的 VLAN，但是有啓用跨 LAN 路由功能(LAN>>基本設定)，參考下圖

Inter-LAN Routing

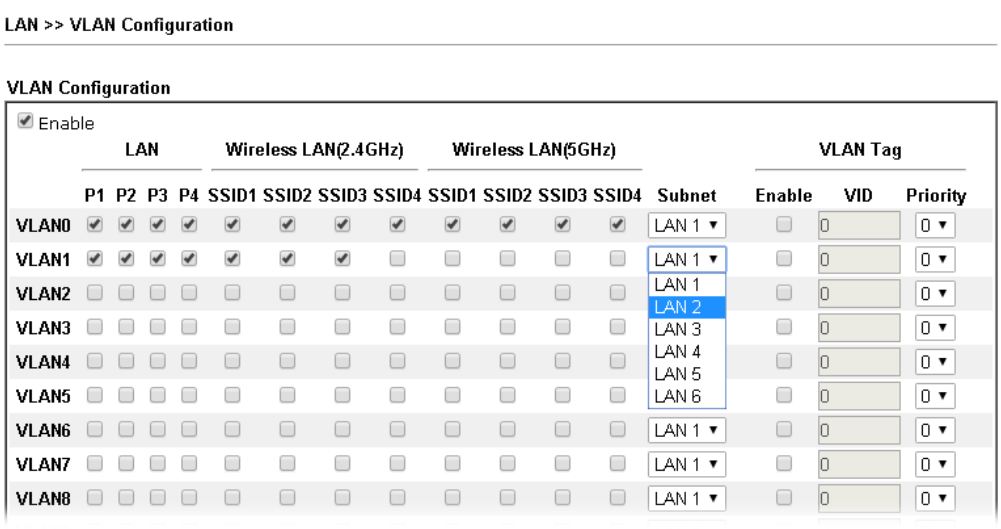
Subnet	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5	LAN 6	LAN 7	LAN 8	DMZ Port
LAN 1	☑	☐	☐	☐	☐	☐	☐	☐	☐
LAN 2	☐	☑	☐	☐	☐	☐	☐	☐	☐
LAN 3	☐	☐	☑	☐	☐	☐	☐	☐	☐
LAN 4	☐	☐	☐	☑	☐	☐	☐	☐	☐
LAN 5	☐	☐	☐	☐	☑	☐	☐	☐	☐
LAN 6	☐	☐	☐	☐	☐	☑	☐	☐	☐
LAN 7	☐	☐	☐	☐	☐	☐	☑	☐	☐
LAN 8	☐	☐	☐	☐	☐	☐	☐	☑	☐
DMZ Port	☐	☐	☐	☐	☐	☐	☐	☐	☑

跨 LAN 路由(Inter-LAN Routing)可讓不同的 LAN 網段能彼此相連或是彼此隔離，這個功能僅在 VLAN 功能也啓用的狀況下才可使用。在跨 LAN 路由(Inter-LAN Routing)矩陣中，選定的核取方框表示上、左方這二個 LAN 可以互相溝通。

Vigor2926 系列具有靈活的 VLAN 系統，在最簡單的形式中，每個 Gigabit LAN 埠口可以彼此隔離，例如提供不同的資訊給予不同的公司或部門，但與本機流量完全區隔開來。

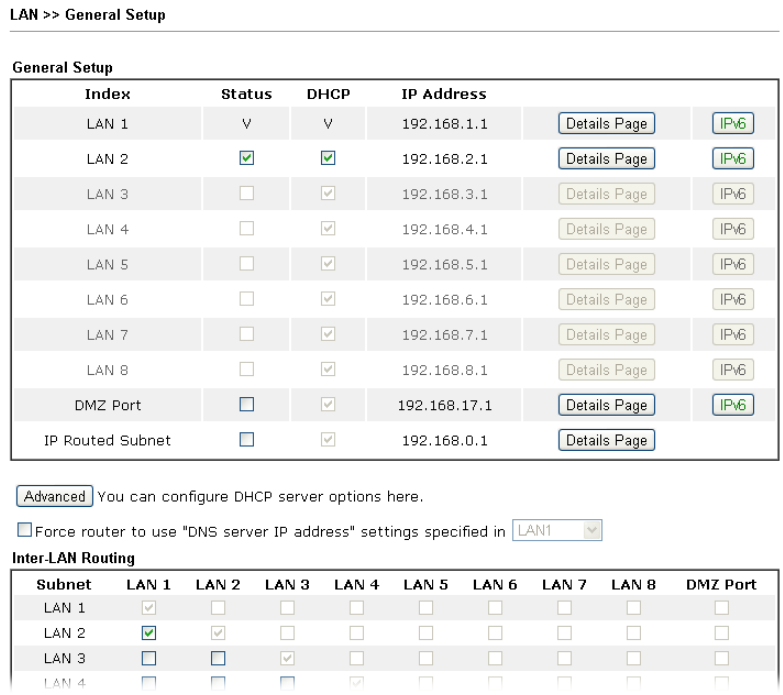
設定埠號式 VLAN 予無線與非無線用戶端

1. All the wire network clients are categorized to group VLAN0 in subnet 192.168.1.0/24 (LAN1).
   所有的有線網路用戶端分類至群組 VLAN0，網段爲 192.168.1.0/24(LAN1)之下。
2. 所有無線網路用戶端分類至群組 VLAN1，網段爲 192.168.2.0/24 (LAN2)之下。
3. 開啓 **LAN>>VLAN 設定(LAN>>VLAN Configuration)**，依照步驟 1 及 2 的說明勾選核取方框。



4. 按下**確定(OK)**。

5. 開啓 LAN>>基本設定**(LAN>>General Setup)**，如果您想要讓二個群組間的用戶能彼此溝通，可以勾選 **LAN1** 與 **LAN2** 間的方框。



路由器在 LAN 端最多可支援六組 IP 子網，每組子網都可以是獨立的或是彼此互連，對於部門或是需要多用途應用而言，是很理想的選擇。

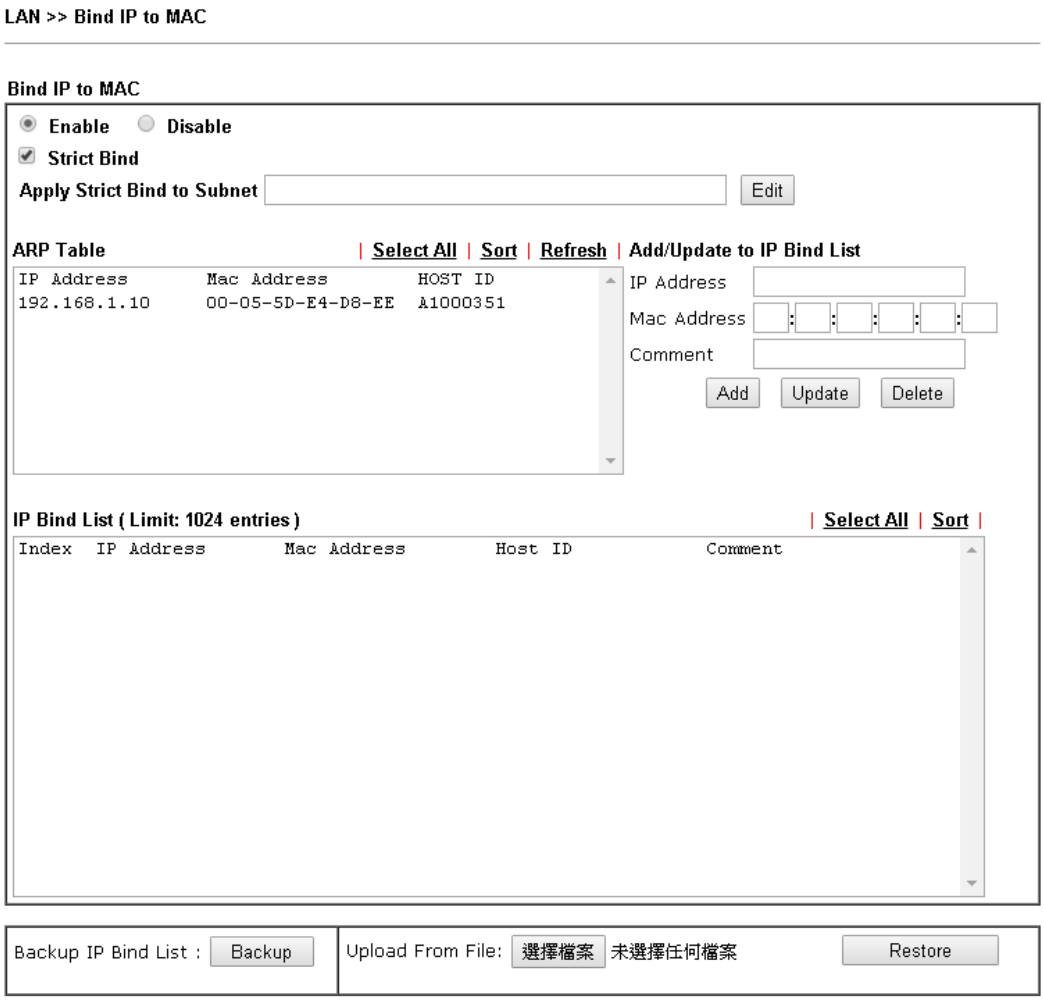
資訊

有關 VLAN 應用部分，請參考“附錄 I: 於 Vigor 路由器上的 VLAN 應用”取得更多細節資訊。

II-2-3 綁定 IP 與 MAC 位址(Bind IP to MAC)

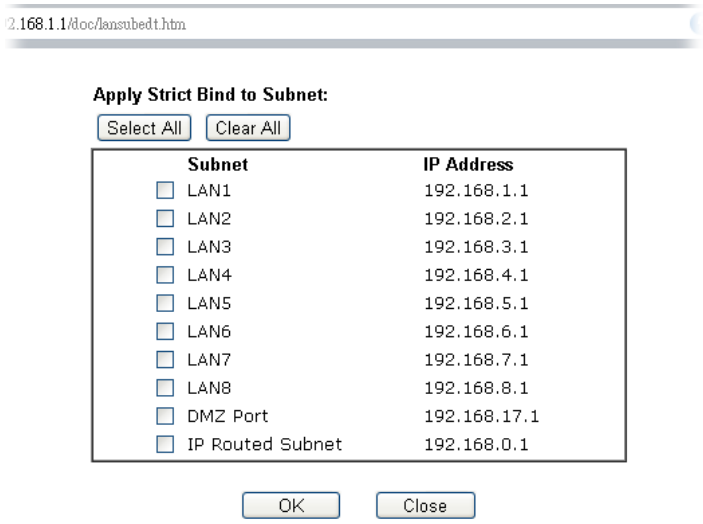
此功能用來綁定區域網路中的電腦之 IP 與 MAC 位址，如此一來可在網路上達到更有效的控制。當此一功能啓用時，所有被綁定的 IP 與 MAC 位址的電腦都不能在變更，如果您修改了綁定 IP 或 MAC 位址，可能會造成無法存取網際網路的窘態。

按**區域網路(LAN)**並選擇**綁定 IP 與 MAC 位址(Bind IP to MAC)**開啓設定網頁。



可用設定說明如下：

項目	說明
啓用(Enable)	按此鈕啓用此功能，不過未列在 IP 綁定清單中的 IP/MAC 位址以可以連上網際網路。
停用(Disable)	按此鈕關閉此功能，頁面上全部的設定都將會失效。
嚴格綁定(Strict Bind)	勾選此框以封鎖未列入 IP 綁定清單中的 IP/MAC 連線。 LAN 用戶端將依照 MAC 至 IP 位址組合由系統分派 IP 位址，MAC 位址尚未綁定 IP 位址者的 LAN 用戶端將無法進行網際網路連線。 **附註**：在選擇嚴格綁定**(Strict Bind)**之前，確保至少有一個有效的 MAC 位址有綁定一個 IP 位址，否則將會發生沒有任何一個 LAN 用戶端得以存取網際網路，也無法連上路由器進行設定變

	更。 **套用嚴格綁定至子網(Apply Strict Bind to Subnet)** – 選擇子網以便套用綁定 IP 至 MAC 的規則。 
ARP 表(ARP Table)	此表格爲路由器的區域網路 ARP 表，IP 和 MAC 資訊將顯示於本區。列於 ARP 表中的每組 IP 和 MAC 位址都可以爲使用者挑選並透過**新增(Add)**按鈕加到 IP 綁定清單上。
全選(Select All)	按此連結選擇表格內全部內容。
排序(Sort)	按此連結將表格內容按照 IP 位元址重新排序。
更新頁面(Refresh)	用來更新 ARP 表格，當新的電腦增加到區域網路上時，您可以按此連結取得最新的 ARP 表格資訊。
新增與更新至 IP 綁定清單(Add/Update to IP Bind List)	**IP 位址(IP Address)** – 輸入 IP 位址以作爲指定 MAC 位址之用。 **MAC 位址(Mac Address)** – 輸入 MAC 位址以便與指定的 IP 位址綁在一起。 **註解(Comment)** – 輸入簡易說明。
新增(Add)	允許您將 ARP 表格中所挑選的或是在新增和編輯上所輸入的 IP/MAC 位址新增至 **IP 綁定清單(IP Bind List)**上。
更新(Update)	允許您編輯或修正先前所建立的 IP 位址和 MAC 位址。
刪除(Delete)	您可以刪除 **IP 綁定清單**上任何一個項目，選擇您想刪除的項目然後按**刪除**按鈕，選定的項目將自 **IP 綁定清單(IP Bind List)**上刪除。
IP 綁定清單(IP Bind List)	顯示綁定 IP 至 MAC 資訊清單。
備份(Backup IP Bind List)	按**備份(Backup)**將設定檔儲存成檔案。
自檔案上傳(Upload From File)	按**瀏覽…(Browse…)** 選擇一個備份檔案，之後按**還原(Restore)** 將備份檔案取回覆蓋目前使用的清單。

資訊

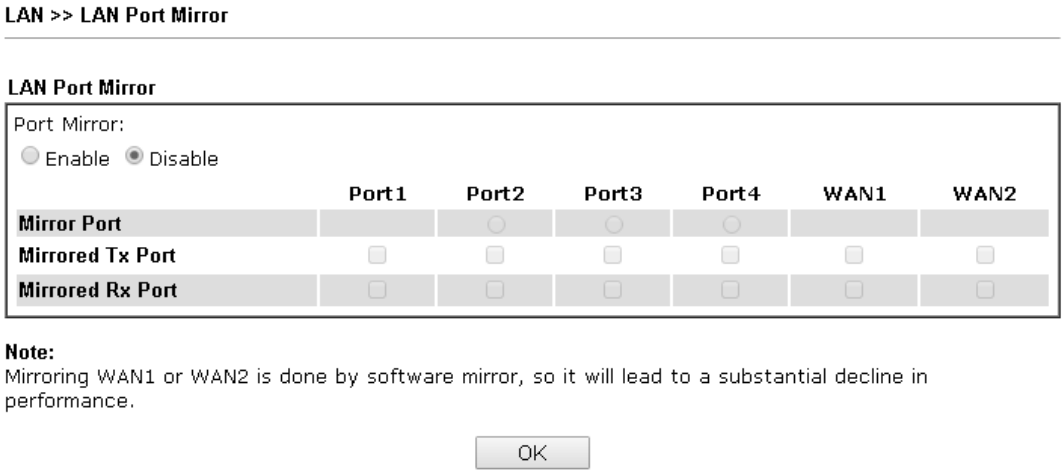
在您選擇**限制綁定(**Strict Bind**)**前，您必須爲一台電腦設定一組 IP/MAC 位址，若無設定的話，沒有一台電腦可以連上網際網路，路由器的網頁組態設定也無法進入了。

當您完成上述設定時，請按下**確定(OK)**按鈕儲存設定。

II-2-4 埠口監控(LAN Port Mirror)

LAN 埠口監控可以套用於區域網路上的所有使用者，此功能可從一個或是多個指定的埠口複製傳輸流量至目標埠口。這項機制可幫助追蹤網路錯誤或是不正常封包傳輸，但卻不會影響一般網路資料存取。也就是說，使用者可以套用此功能來監控需要監督之使用者所有的傳輸資料。

這項功能還有一些優點，首先對於沒有其他偵測設備的人來說，它是相當經濟實用的；其次，它可以同時檢視 VLAN 群組中一個以上埠口的資料傳輸；第三它可將監控的資料到監控埠口端的分析人員處；最後是它很方便也很容易設定。



可用設定說明如下：

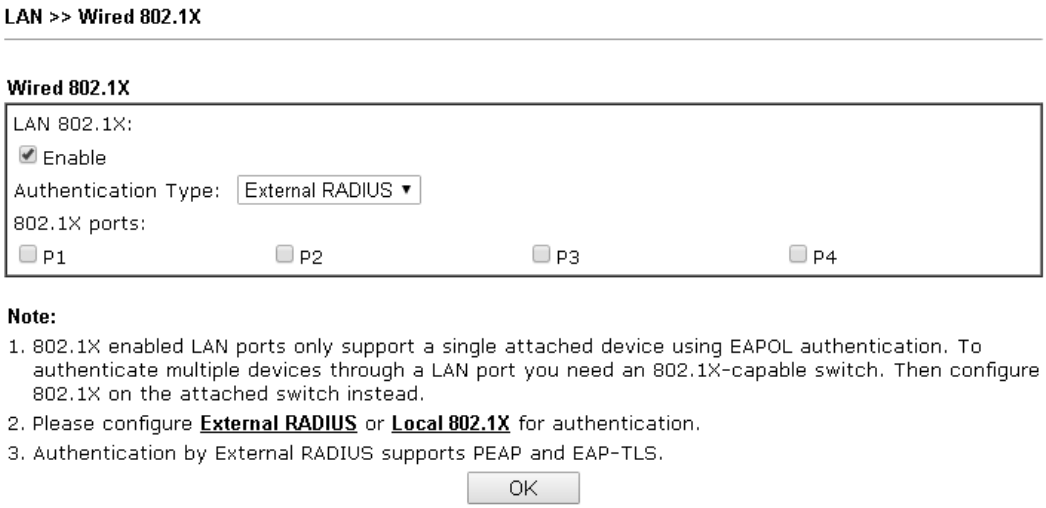
項目	說明
埠號監控(Port Mirror)	按下**啓用**可啓動此功能，或是按下**停用**停止此功能。
監控埠口(Mirror Port)	選擇任一埠口來檢視來自受控埠口的流量。
被監控傳輸埠口(Mirrored Tx Port)	選擇埠口作爲傳輸資訊用，須受到監控，可多選。
被監控接收埠口(Mirrored Rx Port)	選擇埠口作爲接收資訊用，須受到監控，可多選。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

II-2-5 有線 802.1x(Wired 802.1x)

IEEE 802.1x 是以 port-based Network Access Control (PNAC)爲基準的 IEEE 標準，提供驗證機制以便驗證 LAN 或是 WLAN 端的連接裝置。

有線 802.1x 可針對每個 LAN 埠口上的網路裝置進行驗證作業，RADIUS 伺服器設定必區在啓用此功能之前事先設定完畢，因爲 EAP (Extensible Authentication Protocol) 驗證機制仰賴 RADIUS 伺服器來進行，每個設定了有線 802.1x 的 LAN 埠口將僅轉送 802.1x 封包並阻擋其他的封包進入，直到驗證作業完成爲止。



可用設定說明如下：

項目	說明
啓用(Enable)	勾選此框啓用 LAN 802.1x 功能。
驗證類型(Authentication Type)	**外部 RADISU(External RADIUS) -** 外部 RADIUS 伺服器可用於 802.1X 驗證。前往**其他應用>>RADIUS/TACACS+>>外部 RADIUS(Applications >> RADIUS / TACACS+>>External RADIUS)** 以指定 RADIUS 伺服器。 **本機 802.1X(Local 802.1X)** – 使用路由器的使用者資料庫進行驗證，請前往使用者管理>>使用者設定檔(**User Management >> User Profile)** 設定使用者相關內容，如使用者名稱、密碼並確保設定檔內已經啓用本機 802.1X 服務
802.1x 埠號(802.1x ports)	啓用 LAN 802.1x 功能之後，請指定套用此功能的實體 LAN 埠口。

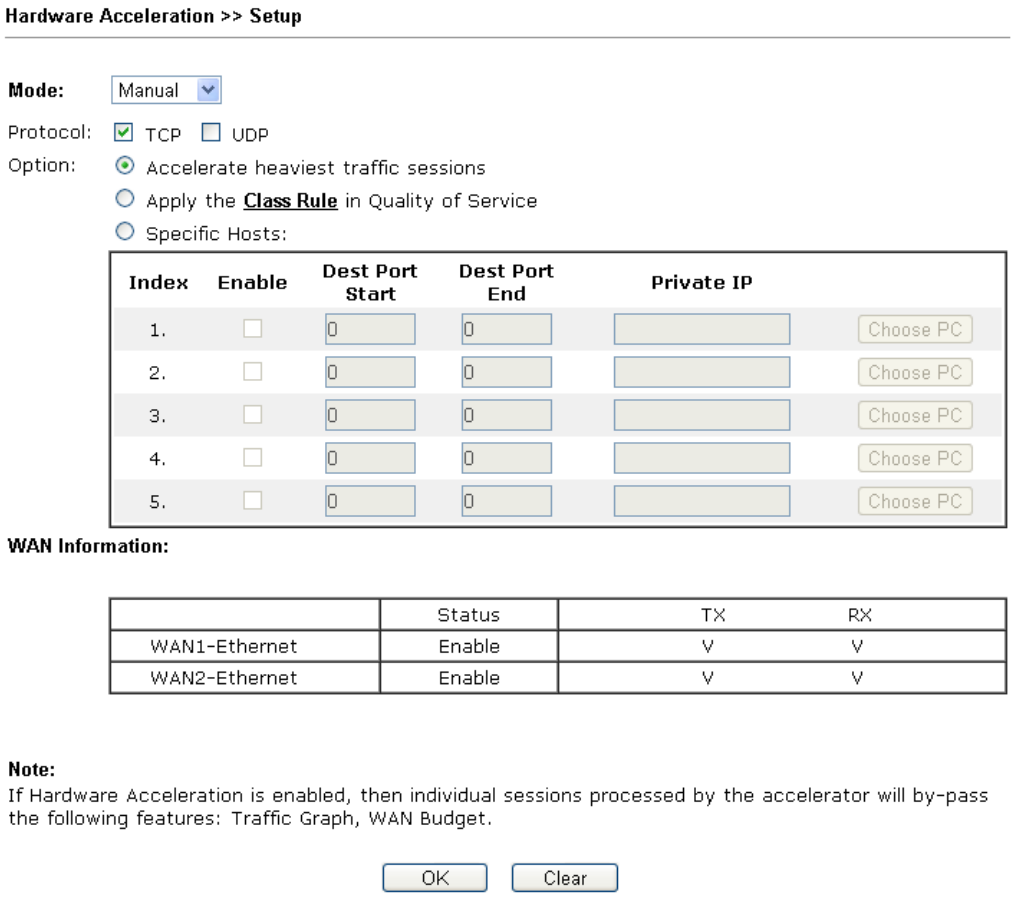
完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

II-3 硬體加速(Hardware Acceleration)

硬體加速在居易又稱爲 PPA，因爲是以 Infinion 的 PPE 爲基準設計的，此項功能只支援 128 條連線數的網路流量(進與出)，有三種模式可以選擇，停用、自動及手動。

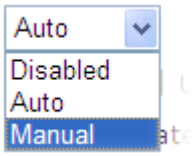
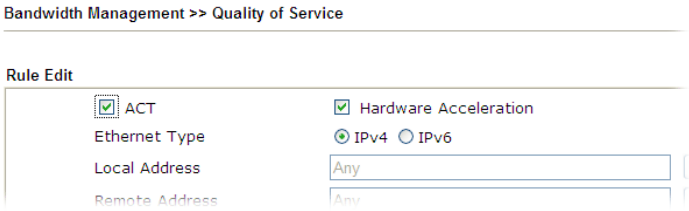
II-3-1 設定(Setup)

當您發現資料的流量過大且傳輸速度開始變得緩慢時，您可設定本頁透過硬體本身來加速資料流量。開啓**硬體加速>>設定(Hardware Acceleration>>Setup)**。



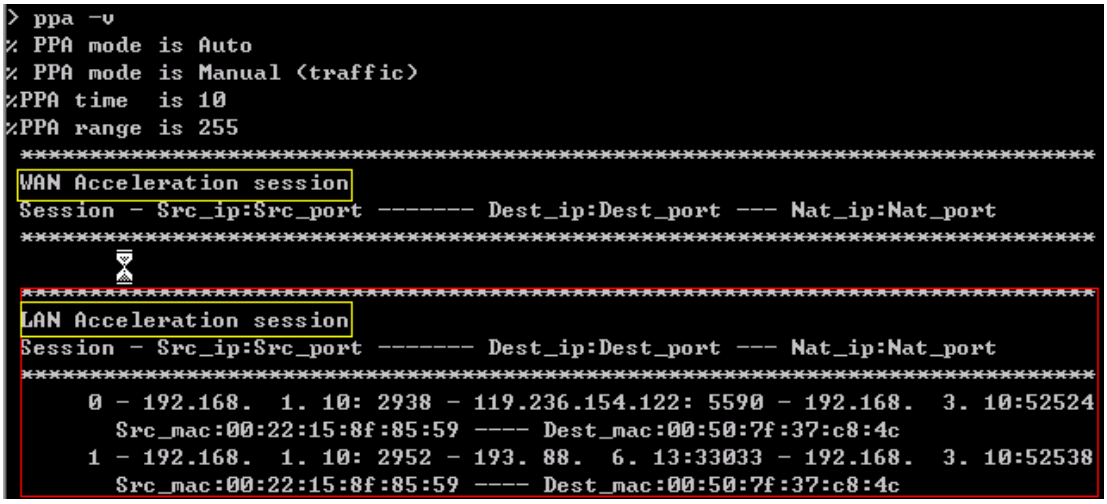
可用設定說明如下：

項目	說明
模式(Mode)	**停用(Disable) -** 預設值。 **自動(Auto) -** 硬體加速如果採用自動模式，就會加進最重承載連線數以及較低的延遲流量，不過，自動模式不支援 UDP 協定。 **手動(Manual) -** 手動模式會實施三個次要項目-*加速流量最大的連線數*、*應用類型規則（QoS）以及指定主機*，每個次項都支援 TCP 與 UDP 協定。

	
協定(Protocol)	有二種協定可以選擇，TCP 與 UDP。
選項(Option)	**加速流量最大的連線數(Accelerate most heavy traffic sessions)** – 此選項僅適用於自動模式，它也是 UDP 協定唯一支援的選項。 **應用類型規則(Apply the Class Rule in Quality of Service)** – 使用者可以套用 QoS 所提供的規則。 **注意:** 請造訪居易網站可以獲得更多 QoS 相關資訊。  **指定主機(Specific Hosts)** – 這個選項提供了 5 台主機以便加入 NAT 連線數。由於硬體加速僅支援 128 條連線數，這些主機全都得共享才行，因此，相關運作的成效會比單一主機要來的低。 選擇此項目來指定區域網路中特定電腦來套用硬體加速。 ● **啓用(Enable)** – 勾選方框讓指定電腦套用硬體加速功能。 ● **開始埠號(Start port)** – 輸入區域網路中的電腦起始埠號。 ● **結束埠號(End port)** – 輸入區域網路中的電腦結束埠號。 ● **虛擬 IP/選擇電腦(Private IP/Choose PC)** – 輸入選定主機的 IP 位址，或是按下選擇電腦按鈕，開啓小視窗選擇您想要指定的 IP 位址。

檢查 PPA 狀態

如果要檢查 PPA 是否運作中，使用者可以利用 telnet 指令檢視傳輸中的連線數有多少，請使用指令“**ppa –v**，參考下圖。


> ppa -v
% PPA mode is Auto
% PPA mode is Manual (traffic)
%PPA time is 10
%PPA range is 255
WAN Acceleration session
Session - Src_ip:Src_port ------- Dest_ip:Dest_port --- Nat_ip:Nat_port
LAN Acceleration session
Session - Src_ip:Src_port ------- Dest_ip:Dest_port --- Nat_ip:Nat_port
0 - 192.168. 1. 10: 2938 - 119.236.154.122: 5590 - 192.168. 3. 10:52524
Src_mac:00:22:15:8f:85:59 ---- Dest_mac:00:50:7f:37:c8:4c
1 - 192.168. 1. 10: 2952 - 193. 88. 6. 13:33033 - 192.168. 3. 10:52538
Src_mac:00:22:15:8f:85:59 ---- Dest_mac:00:50:7f:37:c8:4c

II-4 NAT

通常，路由器可以 NAT 路由器提供其相關服務，NAT 是一種機制，一個或多個虛擬 IP 位址可以對應到某個單一的真實 IP 位址。真實 IP 位址習慣上是由您的 ISP 所指定的，因此您必須爲此負擔費用，虛擬 IP 位址則只能在內部主機內辨識出來。

當封包之目的地位址爲網路上某個伺服器時，會先送到路由器，路由器即改變其來源位址，成爲真實 IP 位址，並透過真實通訊埠傳送出去。同時，路由器在連線數表格中列出清單，以記錄位址與通訊埠對應的相關資訊，當伺服器回應時，資料將直接傳回路由器的真實 IP 位址。

NAT 的好處如下：

- **於應用真實 IP 位址上節省花費以及有效利用 IP 位址** NAT 允許本機中的 IP 位址轉成真實 IP 位址，如此一來您可以一個 IP 位址來代表本機。
- **利用隱匿的 IP 位址強化內部網路的安全性** 有很多種攻擊行動都是基於 IP 位址而對受害者發動的，既然駭客並不知曉任何虛擬 IP 位址，那麼 NAT 功能就可以保護內部網路不受此類攻擊。

資訊

在 NAT 頁面中，您將可看見以 RFC-1918 定義的虛擬 IP 位址，通常我們會使用 192.168.1.0/24 子網路給予路由器使用。就如前所提及的一般，NAT 功能可以對應一或多個 IP 位址和/或服務通訊埠到不同的服務上，換句話說，NAT 功能可以利用通訊埠對應方式來達成。

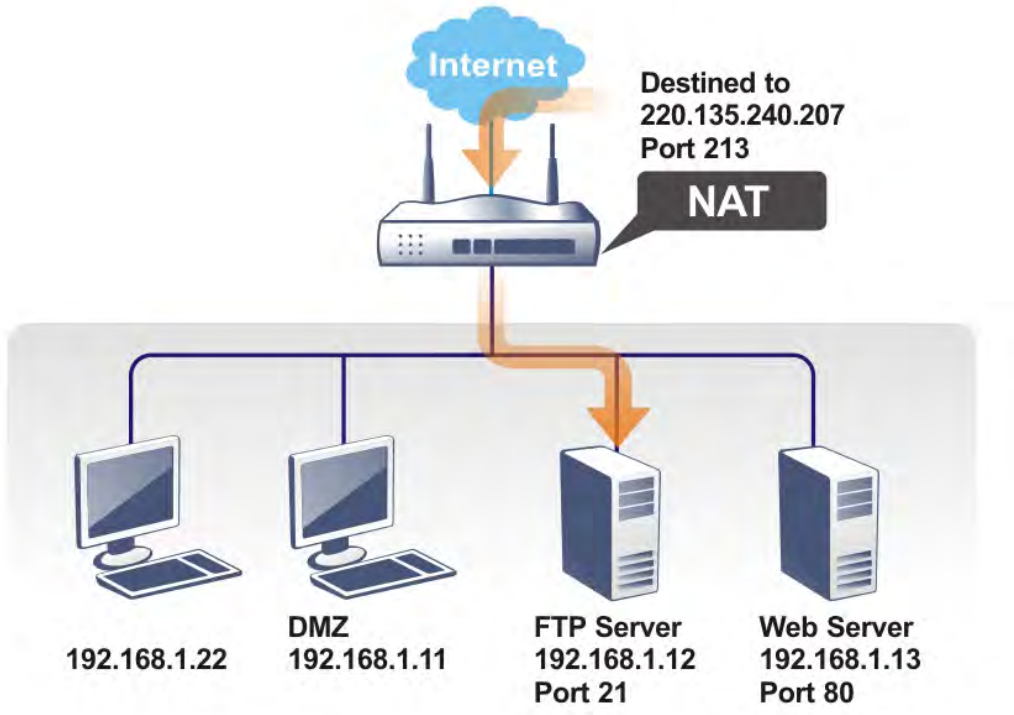
網頁使用者介面

下圖爲 NAT 功能項目：



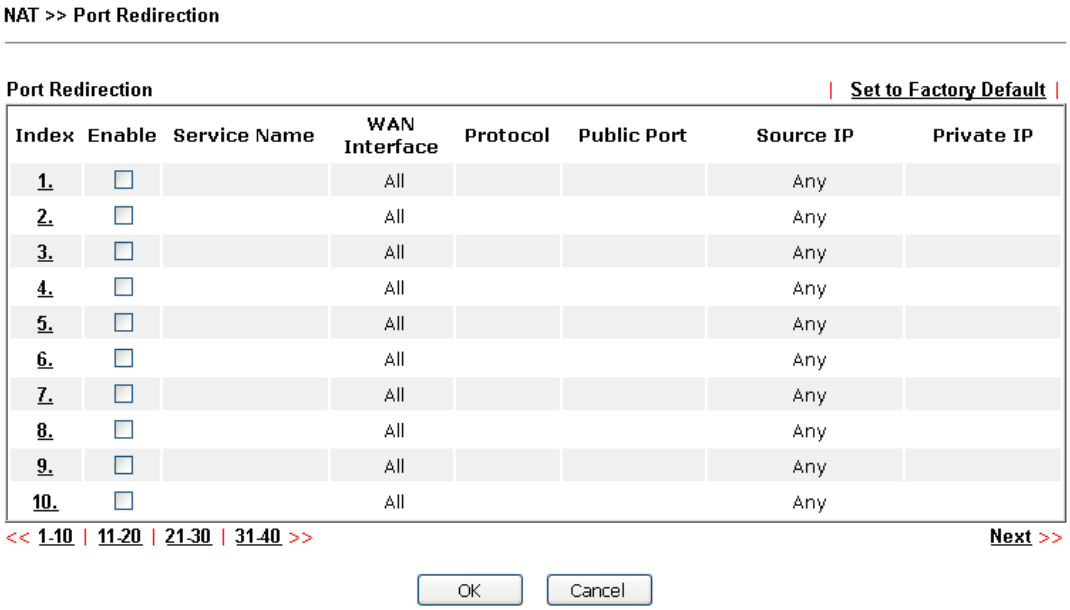
II-4-1 通訊埠重導向(Port Redirection)

通訊埠重導向通常是爲了本地區域網路中的網頁伺服器、FTP 伺服器、E-mail 伺服器等相關服務而設定，大部分的情形是您需要給每個伺服器一個真實 IP 位址，此一真實 IP 位址/網域名稱可以爲所有使用者所辨識。既然此伺服器實際坐落於區域網路內，因此網路可以受到路由器之 NAT 的詳密保護，且可由虛擬 IP 位址/通訊埠來辨認。通訊埠重導向表的功能是傳送所有來自外部使用者對真實 IP 位址之存取需求，以對應至伺服器的虛擬 IP 位址/通訊埠。



通訊埠重導向只能應用在流入的資料量上。

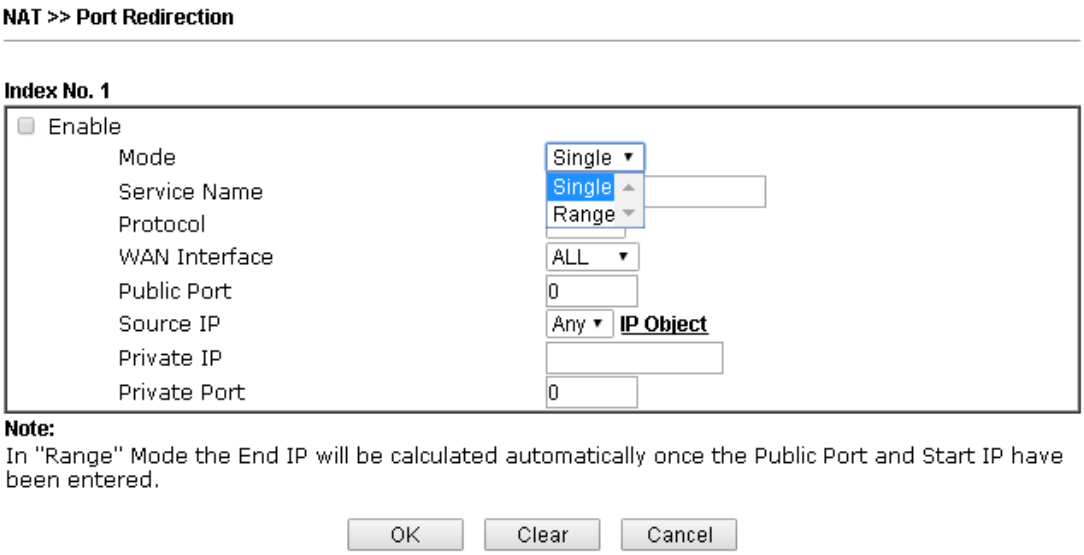
欲使用此項功能，請開啓 **NAT** 頁面然後選擇**通訊埠重導向(Port Redirection)**。**通訊埠重導向**提供 40 組通訊埠對應入口給予內部主機對應使用。



可用設定說明如下：

項目	說明
索引編號(Index)	顯示設定檔的編號。
啓用(Enable)	勾選此框啓用此設定檔。
服務名稱(Service Name)	顯示網路服務的說明。
WAN 介面(WAN Interface)	顯示設定檔使用的 WAN IP 位址。
協定(Protocol)	顯示使用的協定類別（TCP 或是 UDP）。
對外通訊埠(Public Port)	顯示將被導引至指定的內部主機的虛擬 IP 及埠口的埠號。
來源 IP(Source IP)	顯示來源 IP 的 IP 物件名稱。
虛擬 IP(Private IP)	顯示提供此服務之內部主機的 IP 位址。

按下索引編號下的號碼連結，進入次層之設定頁面。



可用設定說明如下：

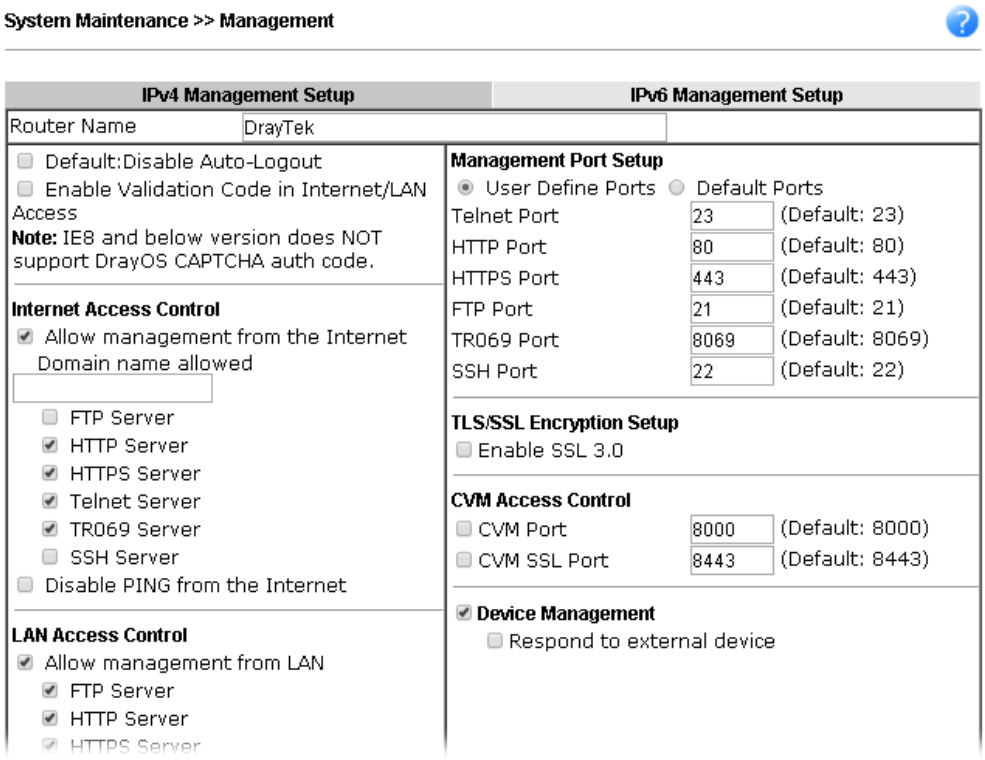
Item	Description
啓用(Enable)	勾選此方塊啓用此通訊埠重導向設定。
模式(Mode)	有二種模式可以供使用者選擇，如欲設定範圍給予指定服務，請選擇**範圍(Range)**。在"範圍" 模式下，若 IP 位元址與第一個對外通訊埠號皆填入之後，系統將自動計算並顯示第二個對外通訊埠值。
服務名稱(Service Name)	輸入特定網路服務的名稱。
通訊協定(Protocol)	選擇傳送層級的通訊協定(TCP 或 UDP)。
WAN Interface	選擇通訊埠重導向的 WAN IP 位址，有 8 組 WAN IP 別名可以選擇。 預設值是**全部(All)**，表示從任何一個通訊埠進入的資料都會重新導引至指定的 IP 位址及通訊埠。
對外通訊埠(Public Port)	指定哪一個通訊埠可以重新導向至內部主機特定的虛擬 IP 通訊埠上。如果您選擇**範圍(Range)**作爲重導向模式，您將會在此看見二個方塊，請在第一個方塊輸入需要的數值，系統將會自動指定數值予第二個方塊。
來源 IP(Source IP)	使用下拉式清單指定 IP 物件，或是按下 IP 物件連結建立另一個新的物件來使用。
虛擬 IP(Private IP)	指定提供服務的主機之 IP 位址，如果您選擇**範圍(Range)**作爲重導向模式，您將會在此看見二個方塊，請在第一個方塊輸入完整的 IP 位址 (作爲起點)，在第二個方塊輸入四位數字(作爲終點)。
虛擬通訊埠(Private Port)	指定內部主機提供服務之虛擬通訊埠號。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

注意路由器有其內建服務(伺服器)諸如 Telnet、HTTP 和 FTP，因爲這些服務(伺服器)的通訊埠號幾乎都相同，因此您可能需要重新啓動路由器以避免衝突發生。

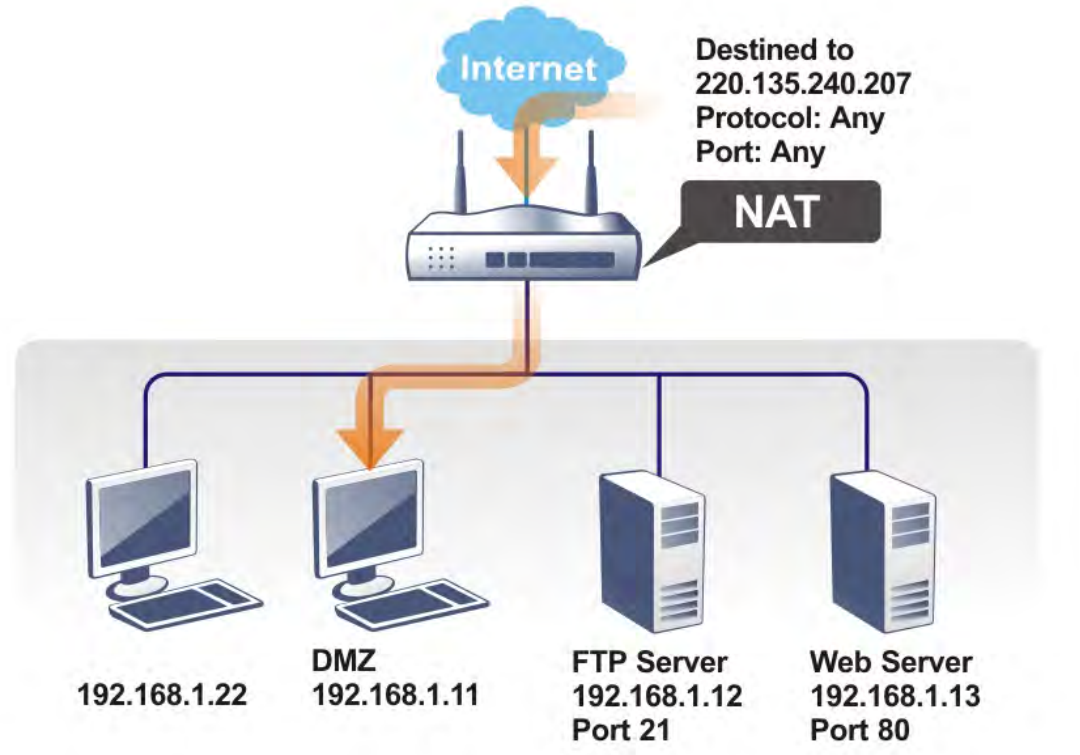
例如，路由器的內建網頁設定給予的設定值是埠號 80，它可能造成與本地網路中網頁伺服器 http://192.168.1.13:80 產生衝突，因此您需要改變路由器的 **http** 通訊埠號，除了 80 以外任何

一種都可以（例如 8080），來防止衝突發生。請改登入管理者模式並在系統維護群中的管理設定做調整，接著您可在 IP 位址尾端加入 8080 (如 http://192.168.1.1:8080 而非僅只通訊埠號 80) 來進入管理畫面。



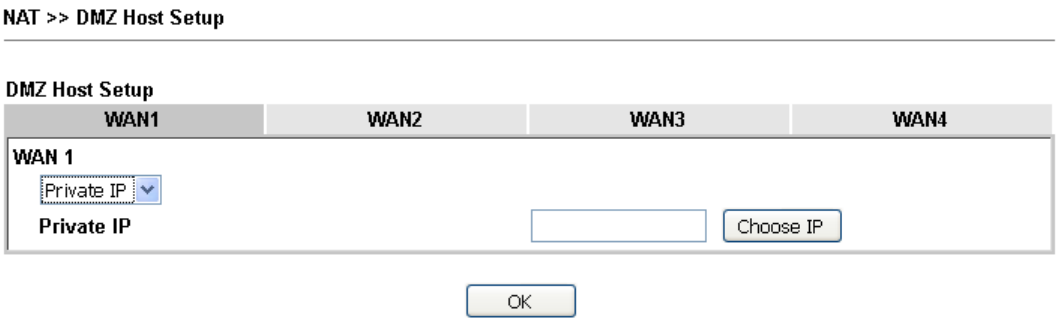
II-4-2 DMZ 主機(DMZ Host)

如同上面所提及的內容，通訊埠重導向可以將流入的 TCP/UDP 或是特定通訊埠中其他的流量，重新導向區域網路中特定主機之 IP 位址/通訊埠。不過其他的 IP 協定例如協定 50 (ESP)和 51(AH)是不會在固定通訊埠上行動的，Vigor 路由器提供一個很有效的工具 DMZ 主機，可以將任何協定上的需求資料對應到區域網路的單一主機上。來自用戶端的正常網頁搜尋和其他網際網路上的活動將可繼續進行，而不受到任何打擾。DMZ 主機允許內部被定義規範的使用者完全暴露在網際網路上，通常可促進某些特定應用程式如 Netmeeting 或是網路遊戲等等的進行。

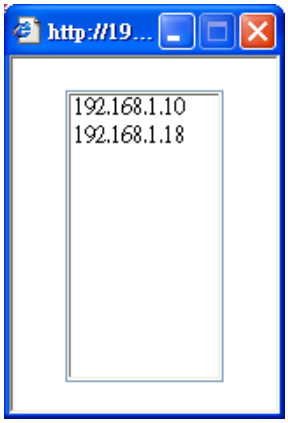
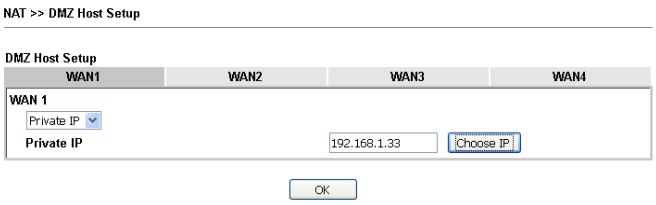


NAT 固有的安全性屬性在您設定 DMZ 主機時稍微被忽略了，建議您另外新增額外的過濾器規則或是第二組防火牆。

請按 **DMZ 主機(DMZ Host)**開啓下述頁面， WAN.您可以針對每個 WAN 界面設定不同的 DMZ 主機，按下 WAN 標籤即可切換到各個不同 WAN 設定頁面。

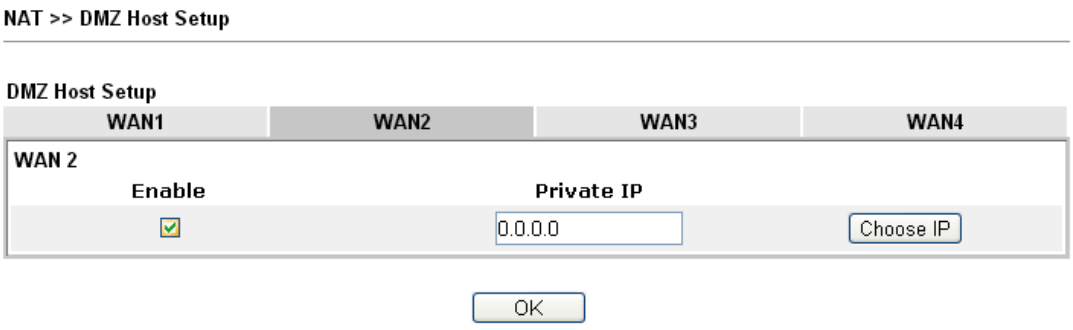


可用設定說明如下：

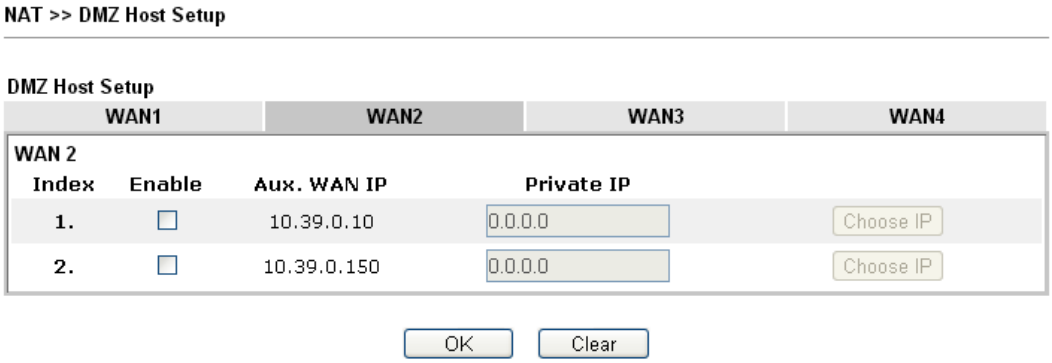
Item	Description
WAN1	請先選擇**虛擬 IP(Private IP)**或是**無(None)**。
虛擬 IP(Private IP)	輸入 DMZ 主機的虛擬 IP 位址，或是按**選擇 IP(Choose IP)**開啓另一頁面來選擇。
選擇 IP(Choose IP)	按下此鈕後，如下視窗立即跳出。此視窗包含您的區域網路中全部主機的虛擬 IP 位址清單，請自清單中選擇一個虛擬 IP 位址作爲 DMZ 主機。  當您已經從上面的視窗選好了虛擬 IP 位址時，該 IP 位址將會顯示在下面的螢幕上，請按**確定(OK)**儲存這些設定。 

當您已經從上面的視窗選好了虛擬 IP 位址時，該 IP 位址將會顯示在下面的螢幕上，請按**確定(OK)**儲存這些設定。

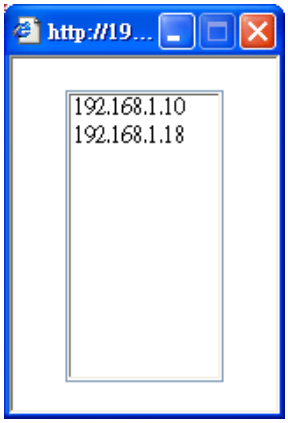
WAN2, WAN3 / LTE 或是 WAN4 的 DMZ 主機設定畫面與 WAN1 有些微不同，參考下圖：



如果您在 WAN2 介面的**網際網路連線設定**選擇 **PPPoE/固定 IP/PPTP**，並且設定 **WAN 別名，**您將可在此頁面發現**輔助 WAN IP** 項目。



可用設定說明如下：

項目	說明
啓用(Enable)	勾選此項以啓動 DMZ 主機功能。
虛擬 IP(Private IP)	輸入 DMZ 主機的虛擬 IP 位址，或是按**選擇 IP(Choose IP)**開啓另一頁面來選擇。
選擇 IP(Choose IP)	按下此鈕後，如下視窗立即跳出。此視窗包含您的區域網路中全部主機的虛擬 IP 位址清單，請自清單中選擇一個虛擬 IP 位址作爲 DMZ 主機。  當您已經從上面的視窗選好了虛擬 IP 位址時，該 IP 位址將會顯示在下面的螢幕上，請按**確定(OK)**儲存這些設定。

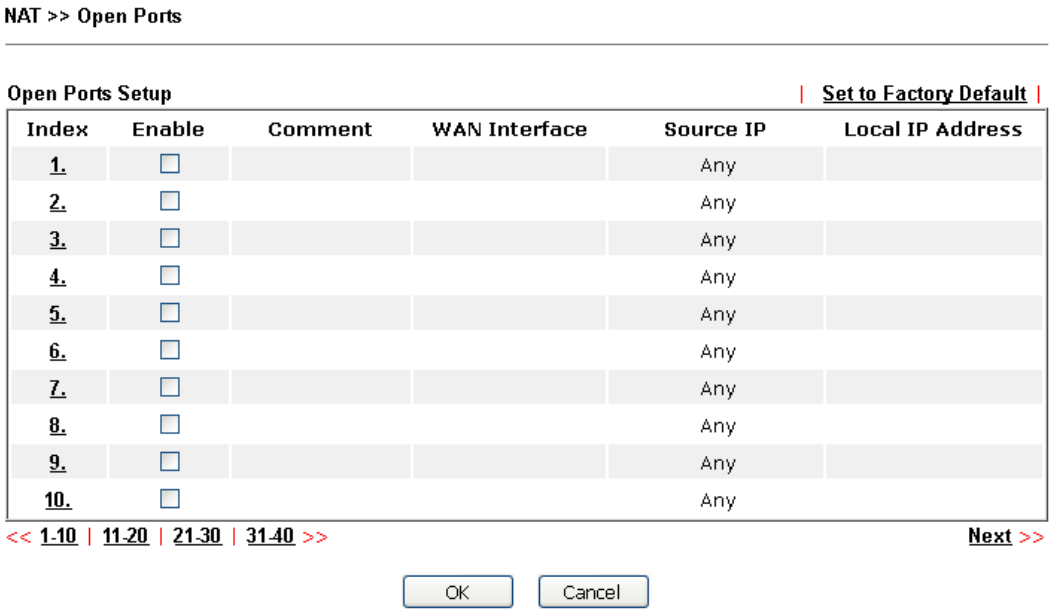
完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

II-4-3 開放通訊埠(Open Ports)

開放通訊埠允許您開啓一段範圍內的通訊埠，供特定應用程式使用。

常見的應用程式包含有 P2P 應用程式(如 BT、KaZaA、Gnutella、WinMX、eMule 和其他)、Internet Camera 等等，您需要先確定應用程式包含最新的資料，以免成爲安全事件的受害者。

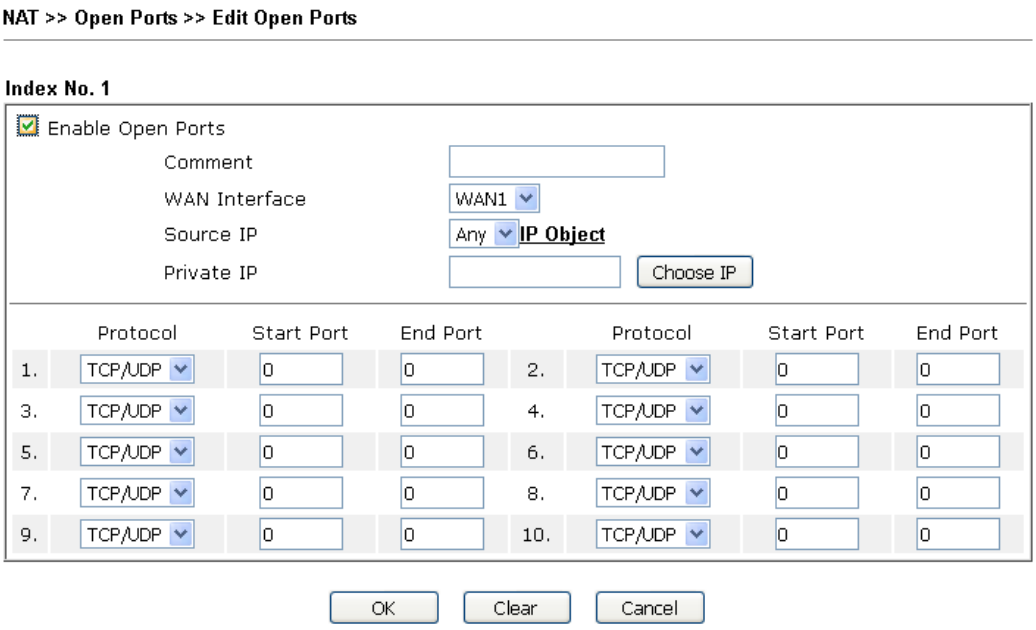
按**開放通訊埠(Open Ports)**結開啓下面的網頁。



可用設定說明如下：

項目	說明
索引(Index)	表示本地主機中您想要提供之服務，其特定內容網頁之相關號碼，您應該選擇適當的索引號碼以編輯或是清除相關的內容。
啓用(Enable)	勾選此框啓用此設定檔。
註解(Comment)	指定特定網路服務的名稱。
WAN 介面 (WAN Interface)	顯示此設定檔使用的 WAN 介面。
輔助 WAN IP (Aux. WAN IP)	顯示此設定檔使用的 IP 別名設定，若無任何別名存在，此區將不會顯示出來。
來源 IP(Source IP)	顯示來源 IP 的 IP 物件名稱。
內部 IP 位址(Local IP Address)	顯示提供此項服務之本地主機的 IP 位址。
狀態(Status)	顯示每項設定的狀態，X 或 V 表示關閉或是啓用狀態。

如果要新增或是編輯通訊埠設定，請按索引下方的號碼按鈕。該索引號碼入口設定頁面隨即出現，在每個輸入頁面中，您可以指定 10 組通訊埠範圍給予不同的服務。



可用設定說明如下：

項目	說明
啓用開放通訊埠 (Enable Open Ports)	勾選此項以啓動此功能。
說明(Comment)	請爲所定義的網路應用/服務命名。
WAN 介面 (WAN Interface)	指定該項設定之 WAN 介面。
來源 IP(Source IP)	使用下拉式清單指定 IP 物件，或是按下 IP 物件連結建立另一個新的物件來使用。
WAN IP	如果您在**網際網路連線設定**選擇 **PPPoE/固定 IP/PPTP**，並且設定 **WAN 別名，**您將可在此頁面發現 **WAN IP** 項目。請自下拉式選項中選擇需要的 IP 位址。
虛擬 IP(Private IP)	輸入本機的虛擬 IP 位址或是按**選擇 IP(Choose IP)**挑選另外一個。
通訊協定(Protocol)	指定傳送層級的通訊協定，有 **TCP**、**UDP** 和 **----- (none)**等幾種選擇。
起始通訊埠(Start Port)	指定本機所提供之服務的開始通訊埠號。
結束通訊埠(End Port)	指定本機所提供之服務的結束通訊埠號。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

NAT >> Open Ports

Open Ports Setup | Set to Factory Default |

Index	Comment	WAN Interface	Local IP Address	Status
1.	P2261	WAN1	192.168.1.49	v
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x

II-4-4 埠號觸發(Port Triggering)

埠號觸發式開放通訊埠的變更版。二者最主要的差異是：

- 一旦按下確定按鈕，設定檔即開始生效，開放通訊埠下的埠口永遠呈現開啓狀態。
- 一旦按下確定按鈕，設定檔即開始生效，埠號觸發會在觸發條件符合時嘗試開啓相關埠口。
- 所有埠口的持續開放的時間端賴使用的通訊協定而定，預設時間顯示如下，相關數據可以利用 telnet 指令進行變更。

  TCP: 86400 sec.

  UDP: 180 sec.

  IGMP: 10 sec.

  TCP WWW: 60 sec.

  TCP SYN: 60 sec.

NAT >> Port Triggering

Port Triggering | Set to Factory Default |

Index	Enable	Comment	Triggering Protocol	Source IP	Triggering Port	Incoming Protocol	Incoming Port
1.	☐						
2.	☐						
3.	☐						
4.	☐						
5.	☐						
6.	☐						
7.	☐						
8.	☐						
9.	☐						
10.	☐						

<< 1-10 | 11-20 >> Next >>

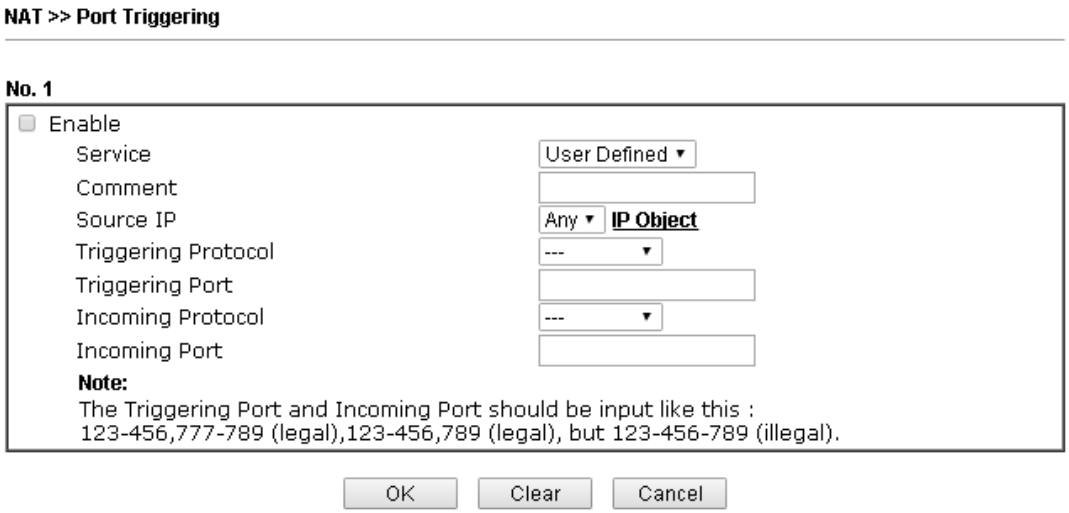
OK Cancel

可用設定說明如下：

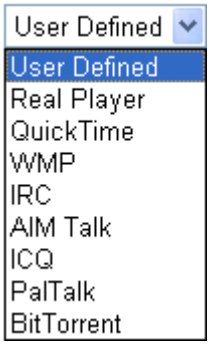
項目	說明
索引編號(Index)	表示埠號觸發設定檔的相應號碼，選擇適當的索引號碼以編輯

	或是清除相關的內容。
啓用(Enable)	勾選此框啓用此設定檔。
說明(Comment)	顯示與此規則相關的說明內容。
觸發協定 (Triggering Protocol)	顯示觸發封包使用的協定。
觸發通訊埠 (Triggering Port)	顯示觸發封包使用的埠號。
來源 IP(Source IP)	顯示 IP 物件的名稱。
輸入協定 (Incoming Protocol)	顯示觸發設定檔輸入資料使用的協定。
輸入通訊埠 (Incoming Port)	顯示觸發設定檔輸入資料使用的埠號。

按下任一索引連結開啓設定頁面：



可用設定說明如下：

項目	**說明**
啓用(Enable)	勾選方框啓用此設定檔。
服務(Service)	您可以選擇事先定義的服務套用到此觸發設定檔。 
說明(Comment)	輸入此設定檔需要特別說明的內容。
來源 IP(Source IP)	使用下拉式清單指定 IP 物件，或是按下 IP 物件連結建立另一個新的物件來使用。

觸發協定 (Triggering Protocol)	針對此觸發設定檔選擇適當的協定（如 TCP, UDP 或 TCP/UDP)。
觸發通訊埠 (Triggering Port)	輸入觸發設定檔的埠號或是埠號範圍。
輸入協定 (Incoming Protocol)	當收到觸發封包時，輸入封包將會利用此處所選擇的協定來處理。
輸入通訊埠 (Incoming Port)	輸入封包的埠號或是埠號範圍。

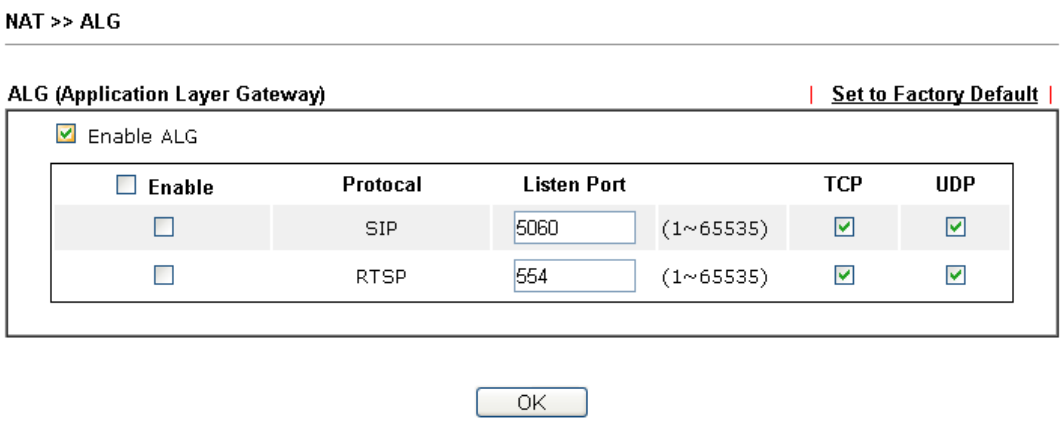
完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

II-4-5 應用層閘道(ALG)

ALG 代表應用層閘道(**Application Layer Gateway)**，路由器提供二種方式 RTSP (Real Time Streaming Protocol) ALG 以及 SIP (Session Initiation Protocol) ALG 來處理聲音與影音封包。

RTSP ALG 可透過路由器的 NAT 傳送並接收 RTSP 訊息、RTCP 訊息與 RTP 的聲音與影音封包。

而 SIP ALG 可透過路由器的 NAT 傳送並接收 SIP 訊息與 RTP 聲音封包。



可用設定說明如下：

項目	說明
啓用(Enable ALG)	勾選此框啓用此功能。
Listen Port	輸入 SIP 或是 RTSP 通訊協定需求之埠號。
TCP	勾選此框以便透過 NAT 從 TCP 傳輸與接收相應協定訊息封包。
UDP	勾選此框以便透過 NAT 從 UDP 傳輸與接收相應協定訊息封包。

II-5 其他應用(Applications)

動態 DNS(Dynamic DNS)

當您透過 ISP 業者嘗試連接到網際網路時，ISP 業者提供的經常是一個浮動 IP 位址，這表示指派給您的路由器使用之真實 IP 位址每次都會有所不同，DDNS 可讓您指派一個網域名稱給予浮動廣域網路 IP 位址。它允許路由器線上更新廣域網路 IP 位址，以便對應至特定的 DDNS 伺服器上。一旦路由器連上網路，您將能夠使用註冊的網域名稱，並利用網際網路存取路由器或是內部虛擬的伺服器資料。如果您的主機擁有網路伺服器、FTP 伺服器或是其他路由器後方提供的伺服器，這項設定就特別有幫助也有意義。

在您使用 DDNS 時，您必須先向 DDNS 服務供應商要求免費的 DDNS 服務，路由器提供分別來自不同 DDNS 服務供應商的三種帳號。基本上，Vigor 路由器和大多數的 DDNS 服務供應商 **www.dyndns.org, www.no-ip.com**、**www.dtdns.com**、**www.changeip.com**、**www.dynamic-nameserver.com** 像是都能相容，您應該先造訪其網站爲您的路由器註冊自己的網域名稱。

LAN DNS / DNS 轉送(LAN DNS / DNS Forwarding)

LAN DNS 讓網路管理者得以掌管具隱私與安全性的伺服器，當網管理者於 LAN 內端設定 FTP、郵件或是網頁伺服器，您可以指定特殊的虛擬 IP 予相應的伺服器上。如此一來，即使遠端 PC 採用真實 DNS 作爲 DNS 伺服器，路由器的 LAN DNS 解決方案將回應指定的虛擬 IP 位址。

排程(Schedule)

路由器具有內建時鐘，可以讓您手動或是透過網路時間協定(NTP)自動更新時間，因此您不只可以規劃路由器在特定時間撥號至網際網路，也能限制於特定時間內存取網際網路資料，如此一來使用者只能在限定時間(或說上班時間)上網，時間排程也可以和其他功能搭配使用。

RADIUS/TACACS+

撥接使用者遠端認證服務(RADIUS)是一種用戶端/伺服器端安全性驗證之通訊協定，支援驗證、授權和說明，通常爲網際網路服務供應商所廣泛應用，是用來作爲驗證和授權撥接網路使用者最常見的一種方法。

內建 RADIUS 用戶特徵設定，可以讓路由器協助遠端撥入用戶、無線工作站以及 RADIUS 伺服器能夠共同執行驗證的動作，它可集中遠端存取驗證工作以達成網路管理。

LDAP /Active Directory Setup

LDAP (Lightweight Directory Access Protocol)是運用 TCP/IP 網路的共用協定，它可定義用戶端存取分享目錄伺服器的方法，在目錄上工作以及共享目錄內的資訊。LDAP 標準是由國際網路工程研究團隊(IETF)所建立。

LDAP 的設計就是成爲一個存取目錄伺服器最有效的方式，而無其他目錄伺服器協定複雜特性。因爲 LDAP 被定義爲可在目錄內安全地執行、查詢及修改資訊，因此使用者可套用 LDAP 來搜尋或是條列目錄物件，查詢或是管理運作中的目錄。

UPnP

UPnP 協定爲網路連線裝置提供一個簡易安裝和設定介面，爲 Windows 隨插即用系統上的電腦週邊設備提供一個直接連線的方式。使用者不需要手動設定**通訊埠對應**或是 **DMZ**，**UPnP** 只在 Windows XP 系統下可以運作，路由器提供相關的支援服務給 MSN Messenger，允許完整使用聲音、影像和訊息特徵。

網路喚醒(Wake on LAN)

區域網路上的電腦可以透過所連結的路由器來喚醒，當使用者想要從路由器喚醒指定的電腦時，使用者必須在此頁面上輸入該電腦正確的 MAC 位址。

此外，此台電腦必須安裝有支援 WOL 功能的網卡，並在 BIOS 設定中開啓 WOL 功能。

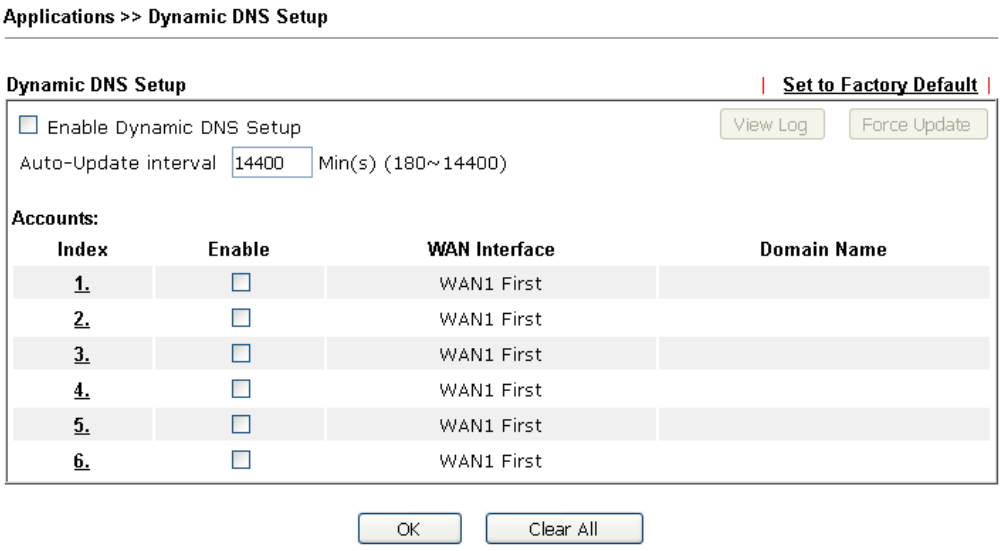
網頁使用者介面



II-5-1 動態 DNS(Dynamic DNS)

啟動此功能並增加一個動態 DNS 帳戶

1. 假設您已經從 DDNS 供應商註冊了一個網域名稱(例如 hostname.dyndns.org)，且獲得一個帳號，其使用者名稱爲 *test*；密碼爲: *test*。
2. 開啓**其他應用>>動態 DNS(Applications>>Dynamic DNS)**。
3. 勾選**啓用動態 DNS 設定(Enable Dynamic DNS Setup)**。

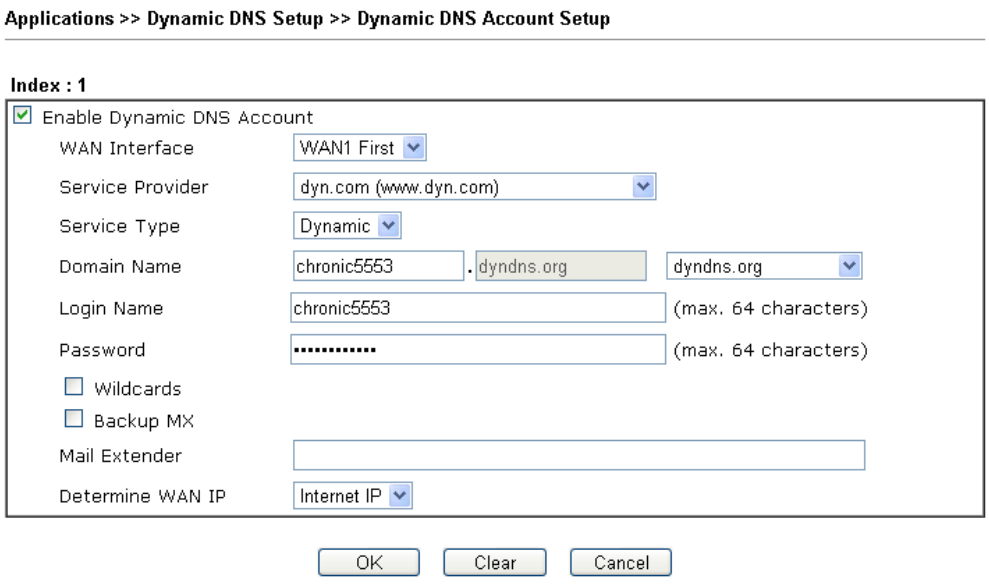


可用設定說明如下：

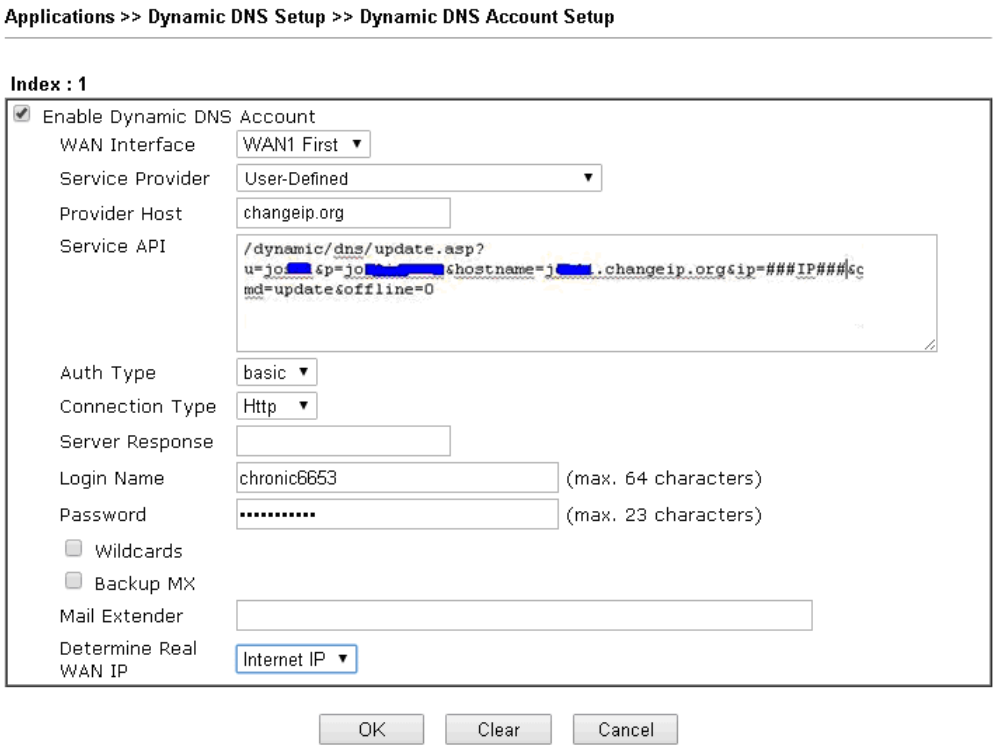
項目	說明
啓用動態 DNS 設定 (Enable Dynamic DNS Setup)	勾選此方塊啓用此功能。

回復出廠預設值(Set to Factory Default)	清除全部設定資料並回復到出廠的設定。
檢視記錄 (View Log)	可開啓另一個對話盒並顯示 DDNS 資訊紀錄。
強迫更新 (Force Update)	按此按鈕強迫路由器取得最新的 DNS 資訊。
自動更新間隔 (Auto-Update interval)	輸入動態 DNS 伺服器的自動更新的間隔時間。
索引(Index)	按下方的號碼連結進入 DDNS 設定頁面，以設定帳戶。
啓用(Enable)	勾選此框啓用此帳戶。
WAN 介面(WAN Interface)	顯示使用的 WAN 介面。
網域(Domain Name)	顯示您在 DDNS 設定頁面上所設定的網域名稱。

4. 選擇索引號碼 1，爲您的路由器新增一個帳號。勾選**啓用動態 DNS 帳號(Enable Dynamic DNS Account)**，然後選擇正確的服務供應商(例 dyndns.org)，輸入註冊的主機名稱(例 hostname)，並於網域名稱區塊中輸入網域的字尾名稱(例 dyndns.org)；接著輸入您的帳號登入名稱(例 dray)和密碼(例 test)。



若您選擇**使用者自定(User-Defined)**作爲服務供應商設定，網頁將會有些許不同：



可用設定說明如下：

項目	說明
啓用動態 DNS 帳號 (Enable Dynamic DNS Account)	勾選此方塊以啓用目前帳號，如果您勾選此方塊，您可在步驟 2 中的網頁上看到啓動欄位出現勾選標示。
WAN 介面(WAN Interface)	**WAN1/WAN2/WAN3 或LTE/WAN4 優先(WAN1/WAN2/WAN3 or LTE/WAN4 First)** - 連線時，路由器將會優先使用 WAN1/WAN2/WAN3 或 LTE /WAN4 作爲首選頻道，如果 WAN1/WAN2/WAN3 或 LTE /WAN4 連線失敗，路由器才會另外的 WAN 介面連線。 **限用 WAN1/WAN2/WAN3 或 LTE /WAN4 (WAN1/WAN2/WAN3 or LTE /WAN4 Only)** - 連線時，路由器僅會使用 WAN1/WAN2/WAN3 或 LTE /WAN4 作爲此帳號的唯一連線介面。
服務供應商 (Service Provider)	爲此 DDNS 帳號選擇適當的服務供應商。
服務類型 (Service Type)	選擇服務類型(動態、自訂、固定)。如果您選擇的是**自訂**，您可以修正網域名稱區域中所選定的網域資料。
網域名稱(Domain Name)	輸入您所申請的網域名稱。請使用下拉式選項選擇想要使用的一個名稱。 請注意當您選擇使用者自定作爲服務供應商設定時，這個選項將無法使用。
供應商主機(Provider Host)	輸入提供關服務的主機 IP 位址或是網域名稱。 請注意這個選項僅在您選擇使用者自定作爲服務供應商設定時，始可使用。
服務 API(Service API)	輸入字 DDNS 伺服器取得之 API 資訊。

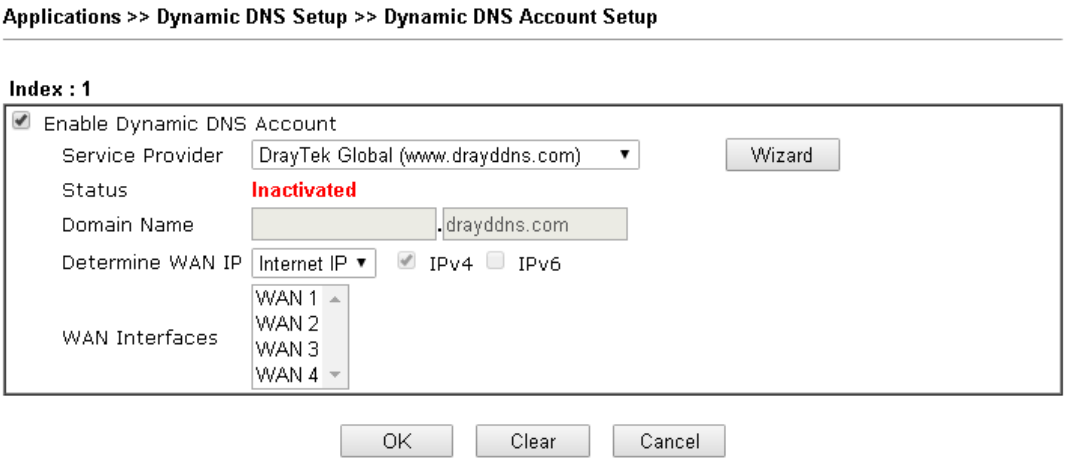
	請注意這個選項僅在您選擇使用者自定作爲服務供應商設定時，始可使用。 (e.g: /dynamic/dns/update.asp?u=jo***&p=jo********&hostname=j*****.changeip.org&ip=###IP### &cmd=update&offline=0)
驗證類型(Auth Type)	有二種方式可以用來驗證。 **基本(Basic)** – 定義的使用者名稱與密碼，之後可以從擷取的封包上顯示出來。 **URL** -定義的使用者名稱與密碼，之後可以從 URL 上顯示出來。(例如 http://ns1.vigorddns.com/ddns.php?username=xxxx&password=xxxx&domain=xxxx.vigorddns.com) 請注意這個選項僅在您選擇使用者自定作爲服務供應商設定時，始可使用。
連線類型 (Connection Type)	有二種(HTTP 與 HTTPs)連線類型可以指定，請注意這個選項僅在您選擇使用者自定作爲服務供應商設定時，始可使用。
伺服器回應(Server Response)	輸入您想要從 DDNS 伺服器接收的文字。 請注意這個選項僅在您選擇使用者自定作爲服務供應商設定時，始可使用。
登入名稱(Login Name)	輸入您在申請網域名稱時所設定之登入名稱。
密碼(Password)	輸入您在申請網域名稱時所設定之密碼。
萬用字元及備份 MX (Wildcard and Backup MX)	並非所有的動態 DNS 供應商都支援萬用字元與備份 MX(郵件交換)功能，您可以從其官網取的相關資訊。
郵件延伸程式(Mail Extender)	某些 DDNS 伺服器可能會要求提供額外的資訊，如電子郵件地址，請您在此輸入必要的電子郵件位址，以配合該 DDNS 伺服器之需要。
決定真實 WAN IP (Determine Real WAN IP)	如果路由器安裝在 NAT 路由器的後端，您可以啓用此功能來定位真實的 WAN IP 位址。 當 Vigor 路由器使用的真實 IP 其實爲虛擬 IP 時，此功能可以偵測出 NAT 路由器使用的真實 IP 並且利用偵測出來的 IP 位址來更新 DDNS。 有二種方法可以選擇: ● **WAN IP** - 如果選擇此項且路由器的 WAN IP 爲虛擬 IP，那麼 DDNS 更新時就會以偵測到的真實 IP 來替代。 ● **Internet IP** – 如果選擇此項且路由器的 WAN IP 爲虛擬 IP，在 DDNS 更新之前，它就會被轉換爲真實 IP。

5. 按**確定(OK)**按鈕啓動此設定，您將會看到所做的設定已被儲存。

DrayDDNS 設定

DrayDDNS是居易科技自行研發提供的DDNS服務,它可以記錄單一網域名稱內多個WAN IP (IPv4)位址。對使用者來說，方便使用且容易設定，每個 Vigor 路由器皆可註冊一個網域名稱。

選擇 **DrayTek Global** 作爲服務供應商，網頁將顯示如下：



可用設定說明如下：

項目	說明
啓用動態 DNS 帳號 (Enable Dynamic DNS Account)	勾選此框啓用目前的帳號。
服務供應商(Service Provider)	選擇 **DrayTek Global** 作爲服務供應商。 **設定精靈(Wizard)** – 此鈕僅在選定 **DrayTek Global** 爲服務供應商時可用，欲啓用居易科技的 DDNS 服務，按此進入**設定精靈>>服務啓用設定精靈(Wizards>>Service Activation Wizard)**網頁以啓用授權書。 可參考章節 **A-1 如何使用 DrayDDNS?** 查看詳細內容。
狀態(Status)	顯示授權書是否啓用。
決定 WANIP (Determine WAN IP)	如果路由器安裝在 NAT 路由器的後端，您可以啓用此功能來定位真實的 WAN IP 位址。 當 Vigor 路由器使用的真實 IP 其實爲虛擬 IP 時，此功能可以偵測出 NAT 路由器使用的真實 IP 並且利用偵測出來的 IP 位址來更新 DDNS。 有二種方法可以選擇: ● **WAN IP** - 如果選擇此項且路由器的 WAN IP 爲虛擬 IP，那麼 DDNS 更新時就會以偵測到的真實 IP 來替代。 ● **Internet IP** – 如果選擇此項且路由器的 WAN IP 爲虛擬 IP，在 DDNS 更新之前，它就會被轉換爲真實 IP。
WAN 介面(WAN Interface)	**WAN1/WAN2/WAN3 或 LTE/WAN4 優先(WAN1/WAN2/WAN3 or LTE/WAN4 First)** - 連線時，路由器將會優先使用 WAN1/WAN2/WAN3 或 LTE /WAN4 作爲首選頻道，如果 WAN1/WAN2/WAN3 或 LTE /WAN4 連線失敗，路由器才會另外的 WAN 介面連線。 **限用 WAN1/WAN2/WAN3 或 LTE /WAN4 (WAN1/WAN2/WAN3 or LTE /WAN4 Only)** - 連線時，路由器僅會使用 WAN1/WAN2/WAN3 或 LTE /WAN4 作爲此帳號的唯一連線介面。

停用此功能並清除全部動態 DNS 帳號

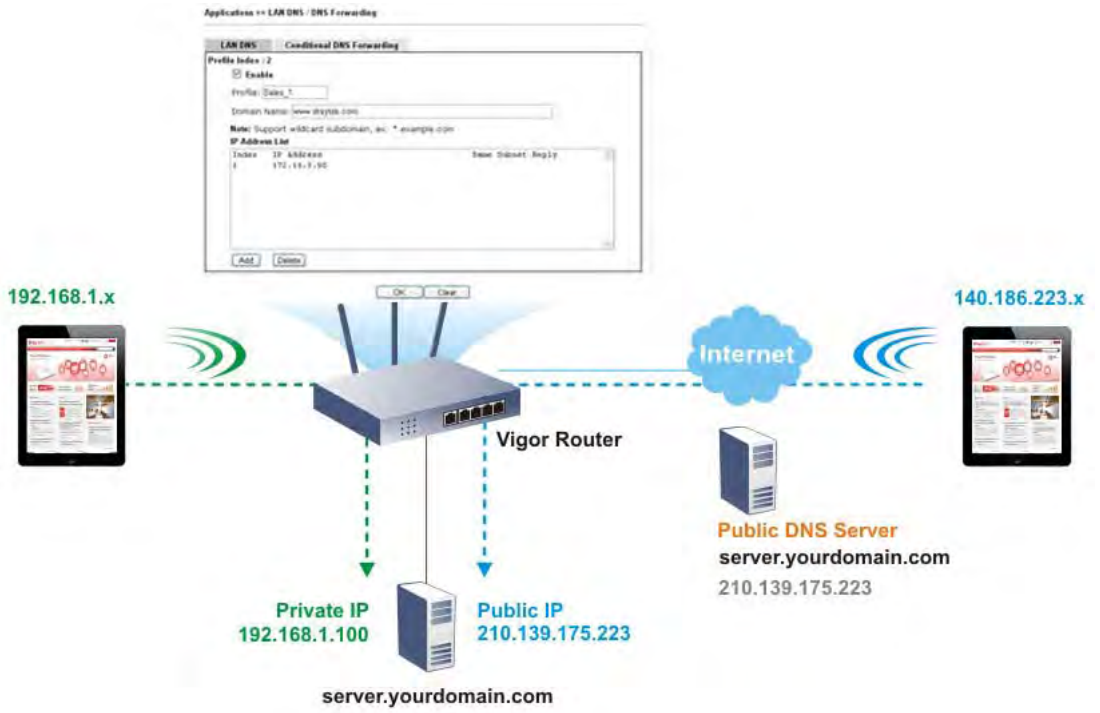
取消勾選**啓用動態 DNS 設定(Enable Dynamic DNS Setup)**，然後按下**清除全部(Clear All)**按鈕即可停用此功能並刪除所有的帳號。

刪除動態 DNS 帳號

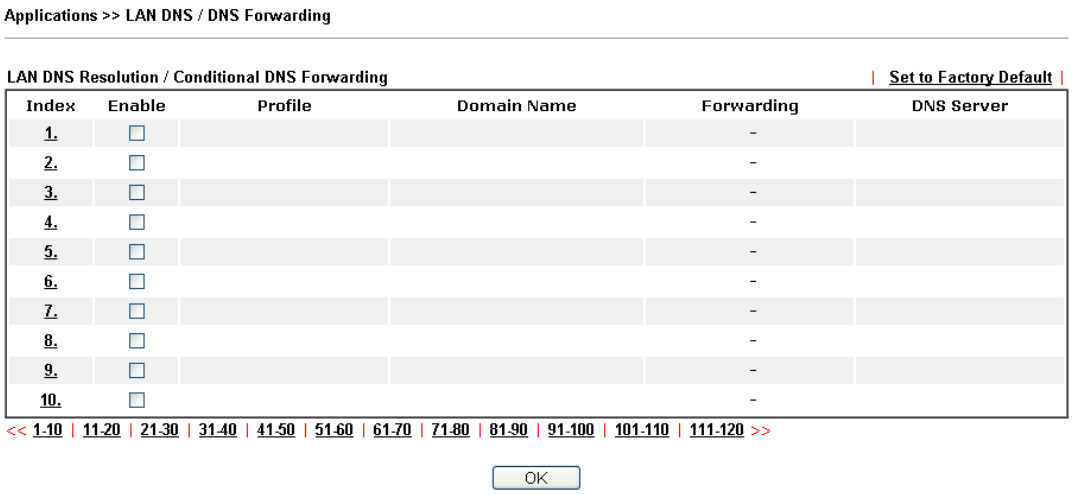
按下您想要刪除項目的索引編號連結，然後然後按下**清除全部(Clear All)**按鈕刪除所有的帳號。

II-5-2 LAN DNS / DNS 轉送(LAN DNS / DNS Forwarding)

LAN DNS 讓網路管理者得以掌管具隱私與安全性的伺服器，當網管理者於 LAN 內端設定 FTP、郵件或是網頁伺服器，您可以指定特殊的虛擬 IP 予相應的伺服器上。如此一來，即使遠端 PC 採用真實 DNS 作爲 DNS 伺服器，路由器的 LAN DNS 解決方案將回應指定的虛擬 IP 位址。



點選**其它應用>>LAN DNS / DNS 轉送(Application>>LAN DNS / DNS Forwarding)** 開啓如下頁面：



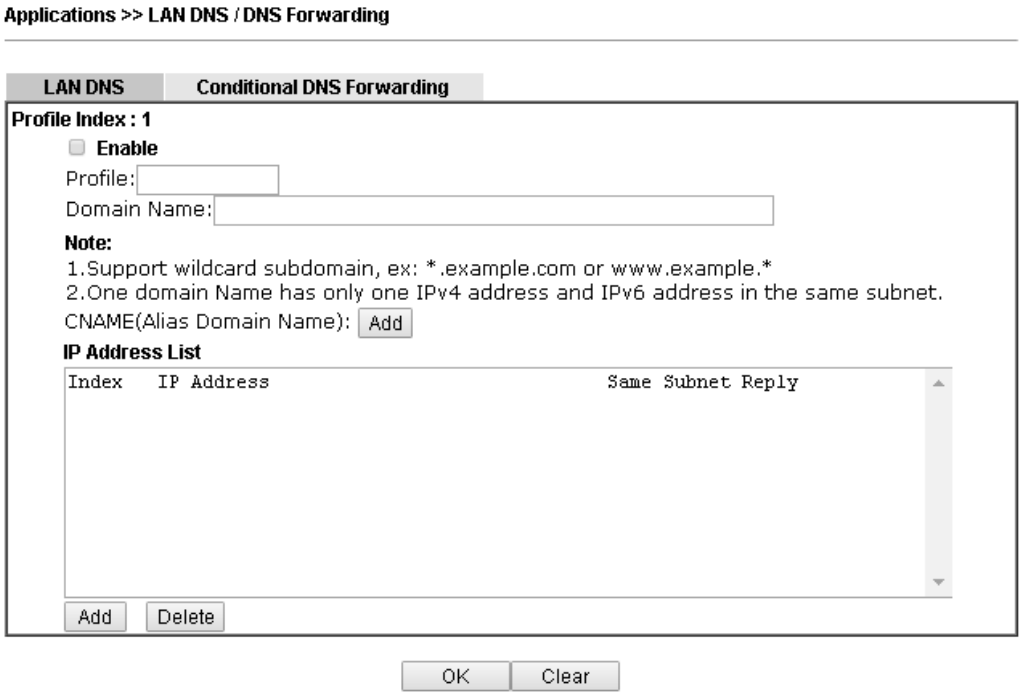
每個項目說明如下：

項目	說明
回復出廠預設值(Set to Factory Default)	清除所有的設定檔內容並回復出廠的預設值。
索引編號(Index)	按下索引編號下方的號碼連結可進入設定頁面。
啓用(Enable)	勾選此方框啓用選定的設定檔。
設定檔(Profile)	顯示 LAN DNS 設定檔的名稱。

網域名稱(Domain Name)	顯示 LAN DNS 設定檔的網域名稱。
轉送(Forwarding)	顯示此設定檔是否爲有條件式 DNS 轉送。
DNS 伺服器(DNS Server)	顯示 DNS 伺服器的 IP 位址。

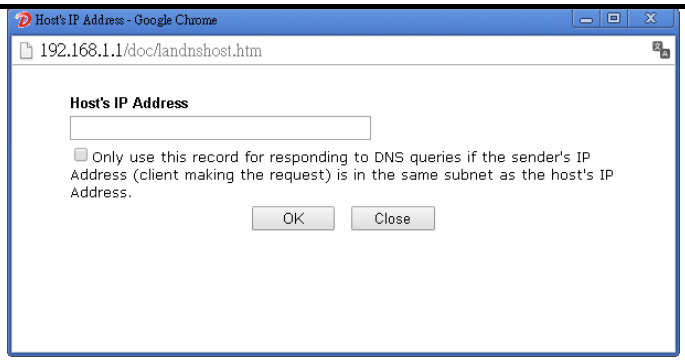
建立 LAN DNS 設定檔，請依下述步驟來進行：

1. 按下任何一個索引編號，本例採用 1。
2. 細部設定頁面呈現如下圖：



可用設定說明如下：

項目	說明
啓用(Enable)	勾選此方框啓用此功能。
設定檔(Profile)	輸入設定檔名。 **附註:** 若在此 LAN DNS 設定檔名，且按下**確定(OK)**儲存配置，相關名稱也會自動套用到條件式 DNS 轉送頁面。
網域名稱 (Domain Name)	輸入此設定檔的網域名稱。
IP 位址清單 (IP Address List)	IP 位址清單用來對照上述指定的網域名稱，一般來說，一個網域名稱對應一組 IP 位址，如有必要，您可以設定二組 IP 位址給予相同的網域名稱。 **新增(Add)** – 按下此按鈕後會出現如下對話方塊讓您輸入主機的 IP 位址。

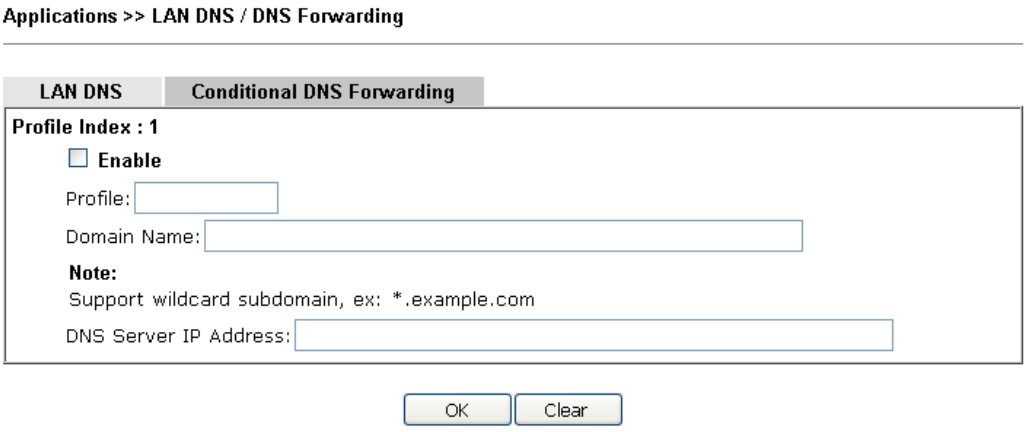


- **僅使用此紀錄....(Only use this record....)** – 不同區域網路端的電腦以共享相同的網域名稱，但是您必須勾選此方框讓路由器辨認並回應 IP 位址以因應來自區域網路端不同電腦 DNS 詢問要求。

刪除(Delete) – 按下此鈕刪除清單中選定的 IP 位址。

3. 按下**確定(OK)**按鈕儲存設定。

4. 如果您需要設定 LAN DNS 設定，請按下索引編號(例如#1)編輯剛剛完成的 LAN DNS 設定檔，或是，您可以按索引編號(#2)使用該設定檔做爲條件式 DNS 轉送設定檔。



可用設定說明如下：

項目	說明
啓用(Enable)	勾選此框啓用此功能。
設定檔(Profile)	輸入設定檔的檔名。 **附註:** 如果您在此輸入設定檔名並按下**確定(OK)**按鈕儲存，此處設定檔的名稱會自動套用到 LAN DNS 設定頁面(相同的索引編號)。
網域名稱 (Domain Name)	輸入設定檔需求的網域名稱。
DNS 伺服器 IP 位址 (DNS Server IP Address)	輸入 DNS 伺服器的 IP 位址，以便作爲 DNS 轉送功能之 DNS 伺服器。

5. 按下**確定(OK)**按鈕儲存設定。

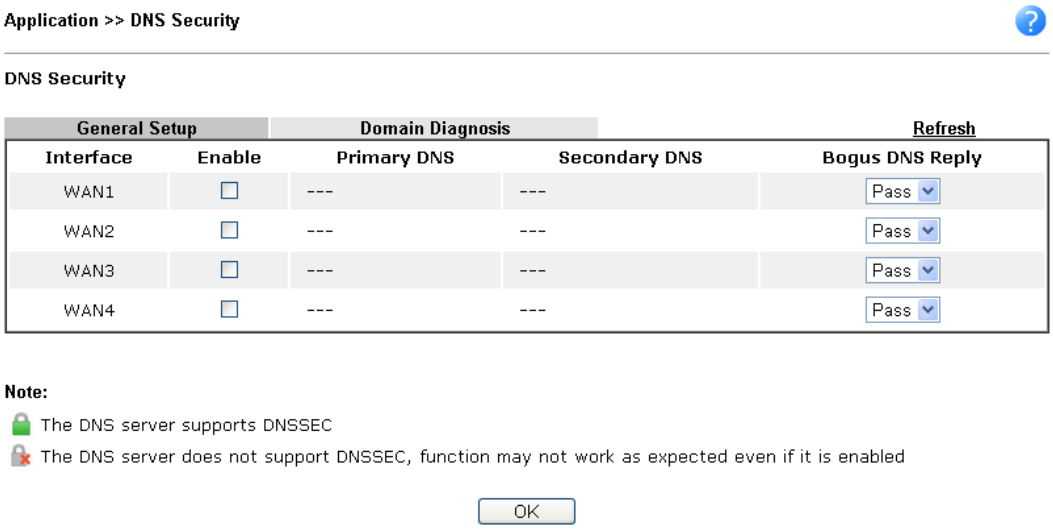
6. 新建立的 LAN DNS 設定檔完成如下。

II-5-3 DNS 安全性(DNS Security)

DSN 安全性(DNS security)能確保輸入的資料不是僞造的，且資料來源安全正確，防止受到外力發動的 DNS 攻擊。

II-5-3-1 基本設定(General Setup)

路由器所有的 WAN 介面都可以個別地啓用 DNS 安全性設定。

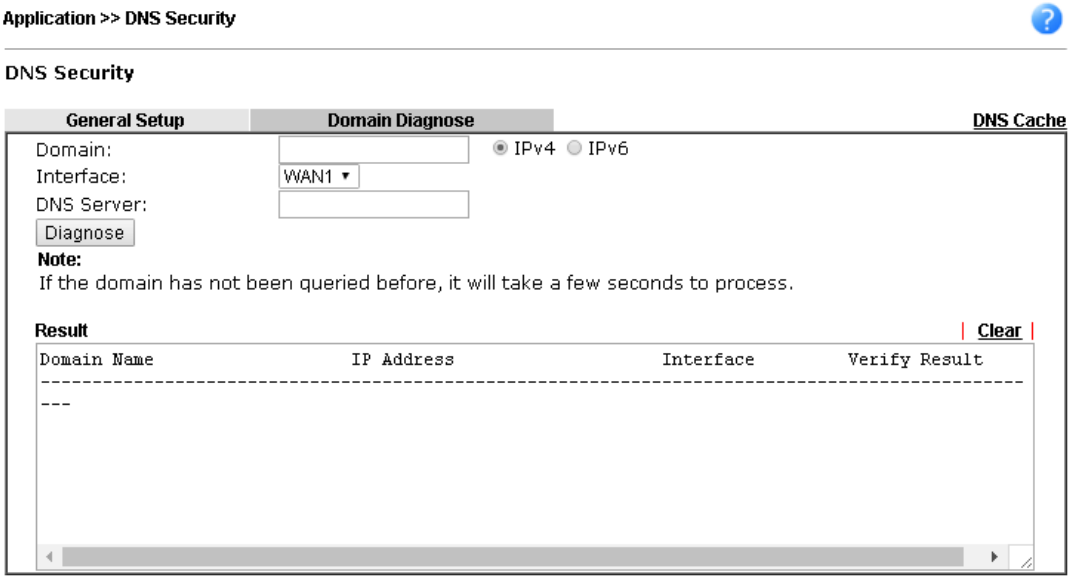


可用設定說明如下：

項目	說明
介面(Interface)	路由器的 WAN 介面都可以設定成啓用 DNS 安全性功能。
啓用(Enable)	勾選此框啓用 DNS 安全性管理。
主要 DNS(Primary DNS)	顯示自 DHCP 伺服器取得或是由固定 WAN 所指定的主要 DNS 的 IP 位址。
次要 DNS(Secondary DNS)	顯示自 DHCP 伺服器取得或是由固定 WAN 所指定的次要 DNS 的 IP 位址。
僞造 DNS 回覆(Bogus DNS Reply)	有時路由器可能會遇到僞造 DNS 查詢的封包，以下有二種方式可以回應這類的查詢： **捨棄(Drop)** – 直接丟棄該封包。 **放行(Pass)** – 接受該封包並讓其通過路由器。

II-5-3-2 網域自我診斷(Domain Diagnose)

本頁可利用手動設定來診斷特定網域是否安全。



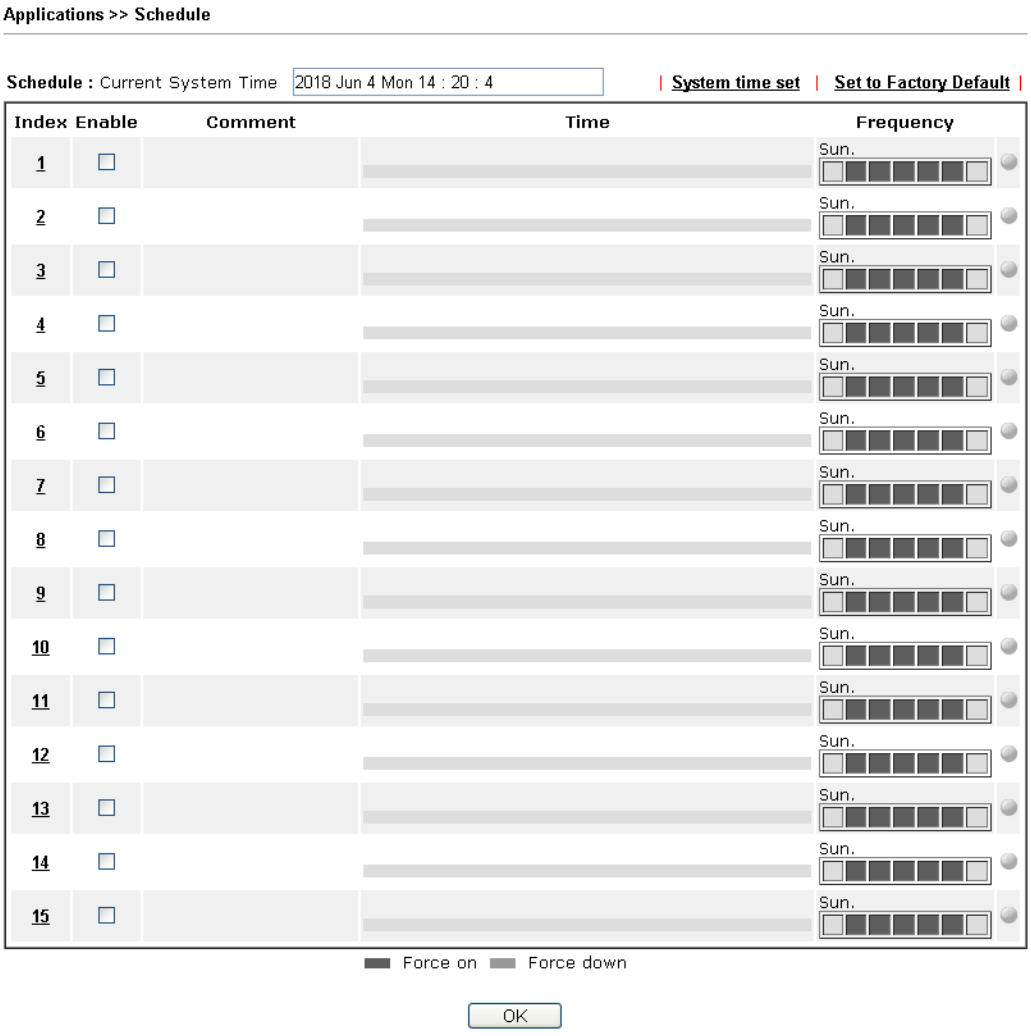
可用設定說明如下：

項目	說明
網域(Domain)	輸入您想要查詢的網域名稱或是 IP 位址(IPv4/IPv6)。
介面(Interface)	指定需要執行診斷的介面。
DNS 伺服器(DNS Server)	輸入用來診斷上述指定的網域名稱之 DNS 伺服器 IP 位址。
診斷(Diagnose)	按此執行網域診斷。
結果(Result)	診斷資訊將會顯示在本區。

II-5-4 排程(Schedule)

Vigor 路由器可允許您手動更新，或利用網路時間協定(NTP)更新時間，因此您不只可以規劃路由器在特定時間撥號至網際網路，也能限制於特定時間內存取網際網路資料，如此一來使用者只能在限定時間(或說上班時間)上網，時間排程也可以和其他功能搭配使用。

您必須在設定排程前先設定好時間，在**系統維護**群組中，選擇**時間和日期(System Maintenance>> Time and Date)**以開啓時間設定頁面，按**取得時間(Inquire Time)**按鈕取得與電腦(或網際網路)一致的時間，一旦您關閉或是重新啓動路由器，時鐘的時間也會重新啓動。還有另一種方法可以設定時間，您可以在網際網路上請求 NTP 伺服器(這是一個時間伺服器)以同步化路由器的時鐘，這個方法只能在廣域網路連線建立時才能使用。



可用設定說明如下：

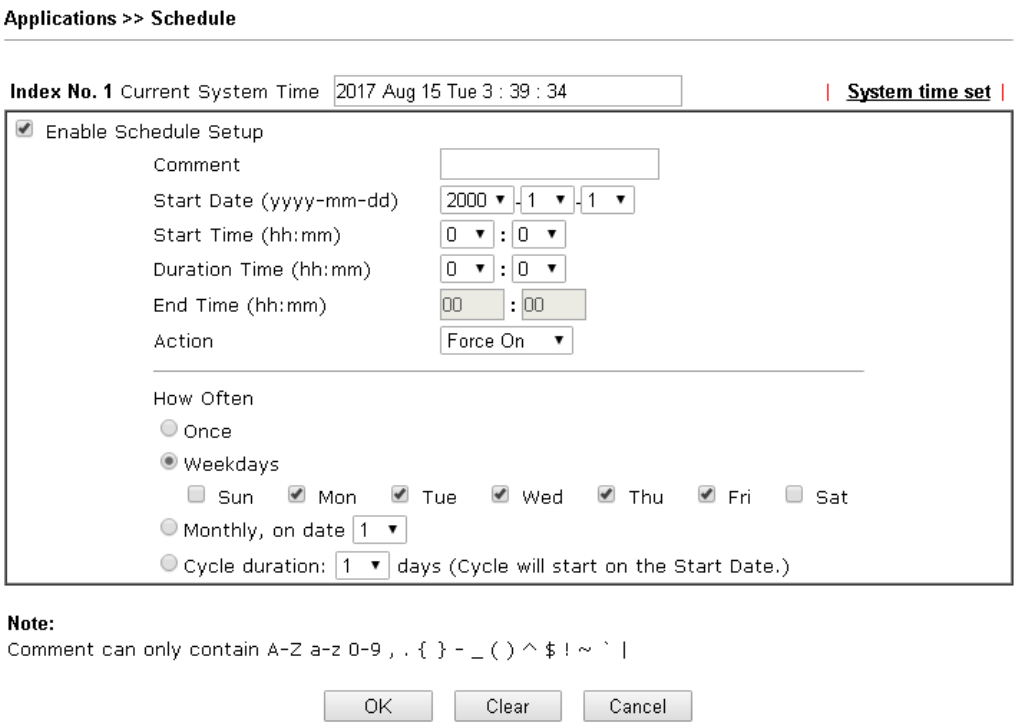
項目	說明
目前系統時間(Current System Time)	顯示路由器使用的時間。
系統時間設定(System time set)	按此連結開啓時間設定頁面(系統維護>>時間與日期)。
回復出廠預設值 (Set to Factory Default)	清除全部設定資料並回復到出廠的設定。

索引編號(Index)	按下方的號碼進入排程設定頁面。
啓用(Enable)	點選此框啓用此排程設定檔。
註解(Comment)	顯示時間排程的名稱。
時間(Time)	顯示有效的時程。
頻率(Frequency)	以色塊顯示排程設定檔內何日永遠連線，何日永遠下線。 - 如顯示綠燈，表示路由器正使用該排程中。

您最多可以設定 15 個排程，然後可以應用於**網際網路連線控制**或是 **VPN 與遠端存取控制 >>LAN-to-LAN** 設定上。

欲新增一個排程：

1. 請按任何一個索引號碼，這裡舉索引編號 1 爲例。
2. 開啓排程的細部設定顯示如下：



可用設定說明如下：

項目	說明
啓用排程設定 (Enable Schedule Setup)	勾選此項目以啓動此排程。
註解(Comment)	輸入此設定檔的簡短說明。
開始日期(Start Date (yyyy-mm-dd))	指定排程的開始日期。
開始時間(Start Time (hh:mm))	指定排程的開始時間。
持續時間(Duration Time (hh:mm))	指定排程的持續時間。

結束時間(End Time (hh:mm))	當開始時間與持續時間皆設定完畢之後，系統會自動計算結束時間。
動作(Action)	指定排程套用的方式： **強迫啓用(Force On) -** 強迫連線永遠存在。 **強迫停用(Force Down) -** 強迫連線永遠停止。
頻率(How Often)	指定套用的排程頻率。 ● **一次(Once) -** 此計劃的頻率只會應用一次。 ● **週期(Weekdays) -** 指定一週當中哪些日子需要執行此項排程作業。
週期(Cycle duration)	指定重設流量紀錄的期間(日、時)。例如數字 7 表示整個週期有 7 天；20 就表示有 20 天。當時間已到，路由器就會自動重置紀錄。

3. 按**確定(OK)**按鈕以儲存設定。

範例

假設您想要控制 PPPoE 網際網路存取連線能夠在每天的 9:00 到 18:00 都能保持開啓狀態(強迫啓用)，其他時間則中斷連線(強迫停用)。

Office Hour:

(Force On)





Mon - Sun **9:00 am** **to** **6:00 pm**

1. 確定 PPPoE 連線和**時間設定**都能正常運作。
2. 設定 PPPoE 每天早上 9:00 到下午 18:00 都保持連線狀態。
3. 設定每天晚上 18:00 到第二天早上 9:00 都是強迫停用狀態。
4. 在PPPoE網際網路存取設定檔中，指定此二個設定檔，現在PPPoE會依照時間排程，**強迫啓用**與**強迫停用**來計畫其網際網路連線。

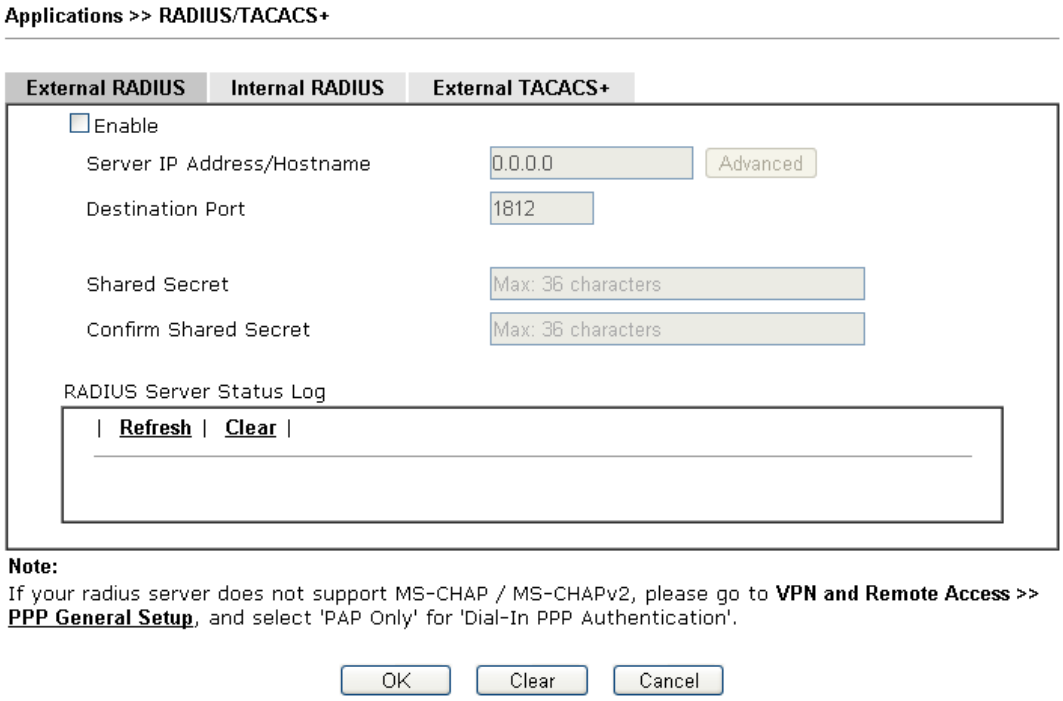
II-5-5 RADIUS/TACACS+

撥接使用者遠端認證服務(RADIUS)是一種用戶端/伺服器端安全性驗證之通訊協定，支援驗證、授權和說明，通常爲網際網路服務供應商所廣泛應用，是用來作爲驗證和授權撥接網路使用者最常見的一種方法。

II-5-5-1 外接 RADIUS(External RADIUS)

內建 RADIUS 用戶特徵設定，可以讓路由器協助遠端撥入用戶、無線工作站以及 RADIUS 伺服器能夠共同執行驗證的動作，它可集中遠端存取驗證工作以達成網路管理。

Vigor 路由器可以當成 RADIUS 用戶端使用，因此本頁可用來調整外接 RADIUS 伺服器的相關設定，之後路由器的 LAN 使用者將由此伺服器進行網路應用驗證。



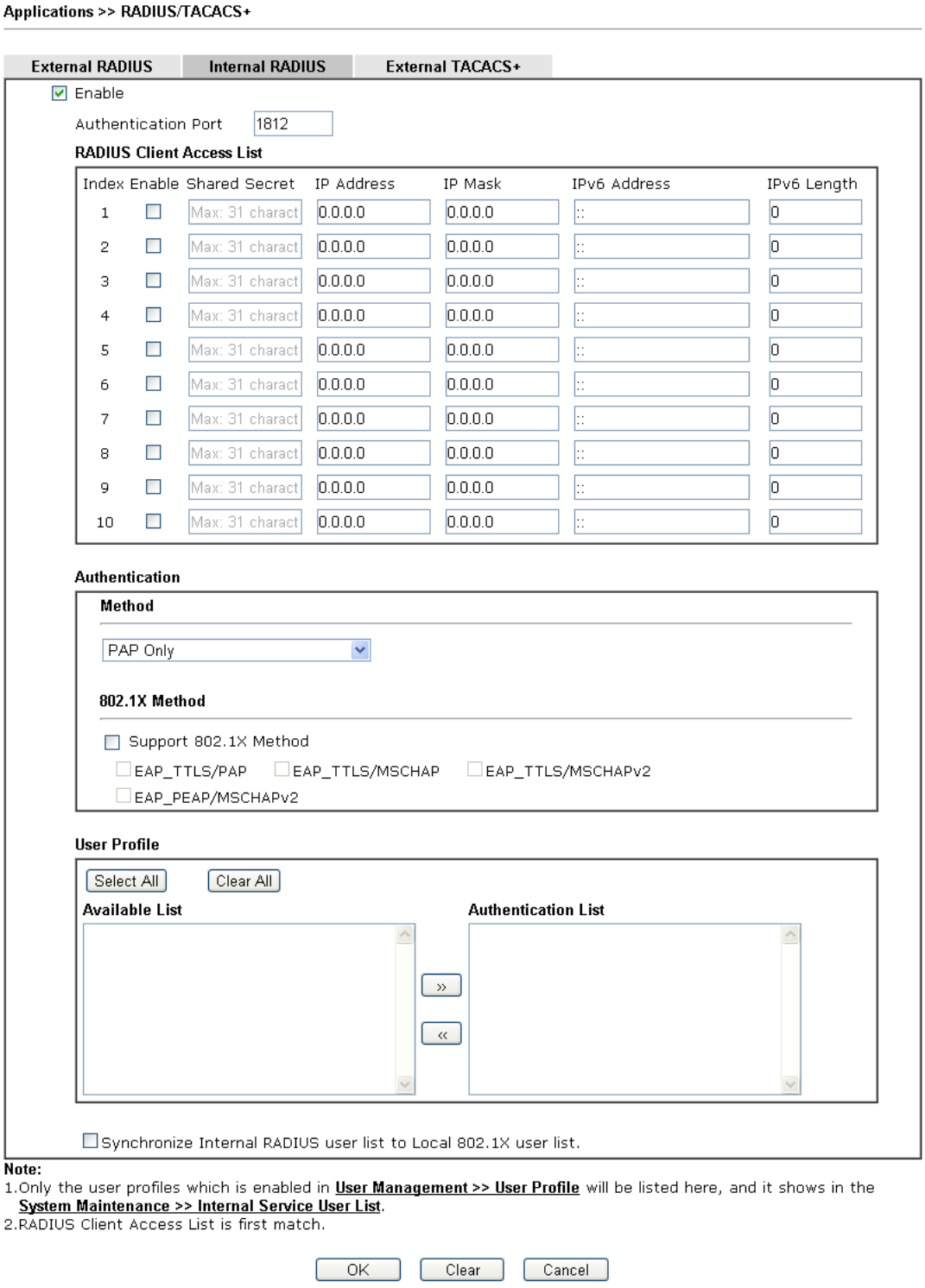
可用設定說明如下：

項目	說明
啓用(Enable)	勾選此項以啓動 RADIUS 設定。
伺服器 IP 位址/主機名稱 (Server IP Address/Hostname)	輸入 RADIUS 伺服器的 IP 位址。
通訊埠(Destination Port)	輸入 RADIUS 伺服器所使用的 UDP 通訊埠號，基於 RFC 2138，預設值爲 1812。
共用密鑰 (Shared Secret)	RADIUS 伺服器和用戶共用一個用來驗證二者之間傳遞訊息的密鑰，雙方都必須設定相同的共用密鑰。
確認共用密鑰 (Confirm Shared Secret)	請重新輸入共用密鑰以確認。

完成上述設定之後，請按下**確定(OK)**儲存。

II-5-5-2 內部 RADIUS(Internal RADIUS)

除了可作爲內建 RADIUS 用戶端以外，路由器也可以當成 RADIUS 伺服器，執行安全性驗證的工作。本頁用來配置內部 RADIUS 設定，之後路由器的 LAN 使用者將由此伺服器進行網路應用驗證。



可用設定說明如下：

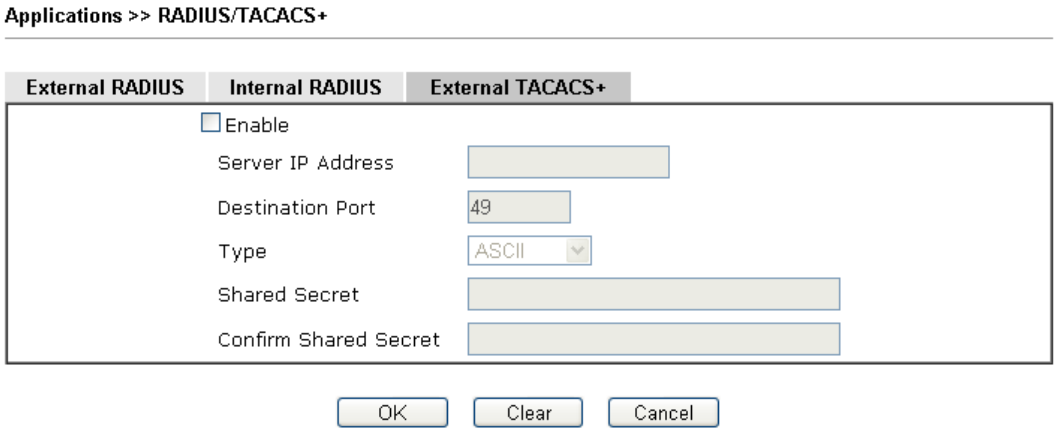
項目	說明
啓用(Enable)	勾選此項以啓動內部 RADIUS 設定。
驗證埠號(Authentication	設定內部 RADIUS 伺服器的埠號。

Port)	
RADIUS 用戶端存取清單 (RADIUS Client Access List)	允許設定指定網域(IPv4 and IPv6)下的用戶端必須以指定的密鑰進行驗證。 **啓用(Enable)** – 勾選此框啓用 RADIUS 用戶端功能。 **共用密鑰(Shared Secret)** - RADIUS 伺服器和用戶共用一個用來驗證二者之間傳遞訊息的密鑰，雙方都必須設定相同的共用密鑰。 **IP 位址(IP Address)** – 輸入有線/無線用戶端的 IP 位址。 **IP 遮罩(IP Mask)** – 輸入 IP 位址需求之子網遮罩 **IPv6 位址(IPv6 Address)** – 輸入有線/無線用戶端的 IPv6 位址。 **IPv6 Length** - 輸入 IPv6 位址需求之前置碼長度。
驗證(Authentication)	指定驗證無線用戶端的方式。 **PAP Only / PAP/CHAP/MS-CHAP/MS-CHAPv2** – 選擇限用 PAP，或是選擇支援 PAP, CHAP, MS-CHAP and MS-CHAPv2。 **支援 802.1x 方式(Support 802.1X Method)** – 路由器內建 RADIUS 伺服器可以當成 AAA 伺服器使用，請勾選方框啓用驗證機制。
使用者設定檔(User Profile)	在安全性驗證過程中，需要使用者帳號與使用者密碼進行身分驗證，在設定此頁前，請至少先在**使用者管理>>使用者設定檔(User Management>>User Profile)**網頁中設定一個使用者設定檔。 **選擇全部(Select All)** – 按下選擇可用清單內全部的使用者設定檔。 **清除全部(Clear All)**- 按下移除可用清單內全部的使用者設定檔。 **可用清單(Available List)** – 尚未加入驗證清單區的使用者設定檔。 **驗證清單(Authentication List)** –加入驗證清單的使用者設定檔，使用者可使用這些設定檔登入網頁以通過驗證。
同步內部 RADIUS 使用者清單至本機 802.1X 使用者清單(Synchronize Internal RADIUS user list to Local 802.1X user list)	使用者可以由RADIUS伺服器與802.1X驗證以便取得網路服務。 勾選此框，所有條列在驗證清單中的使用者設定檔(預備作爲 RADIUS 伺服器驗證)即可同步因應本機 802.1X 使用者驗證。

完成上述設定之後，請按下**確定(OK)**儲存。

II-5-5-3 外接 TACACS+(External TACACS+)

TACACS+的運作有如 RADIUS，按下**外接 TACACS+(External TACACS+)**開啓如下頁面：



可用設定說明如下：

項目	說明
啓用(Enable)	勾選此框啓用 TACACS+ 功能。
伺服器 IP 位址(Server IP Address)	輸入 TACACS+ 伺服器 IP 位址。
目的通訊埠(Destination Port)	TACACS+ 伺服器使用的 UDP 埠號。
共享密鑰 (Shared Secret)	TACACS+伺服器和用戶共用一個用來驗證二者之間傳遞訊息的密鑰，雙方都必須設定相同的共用密鑰。
確認共享密鑰 (Confirm Shared Secret)	請重新輸入共用密鑰以確認。

完成上述設定之後，請按下**確定(OK)**儲存。

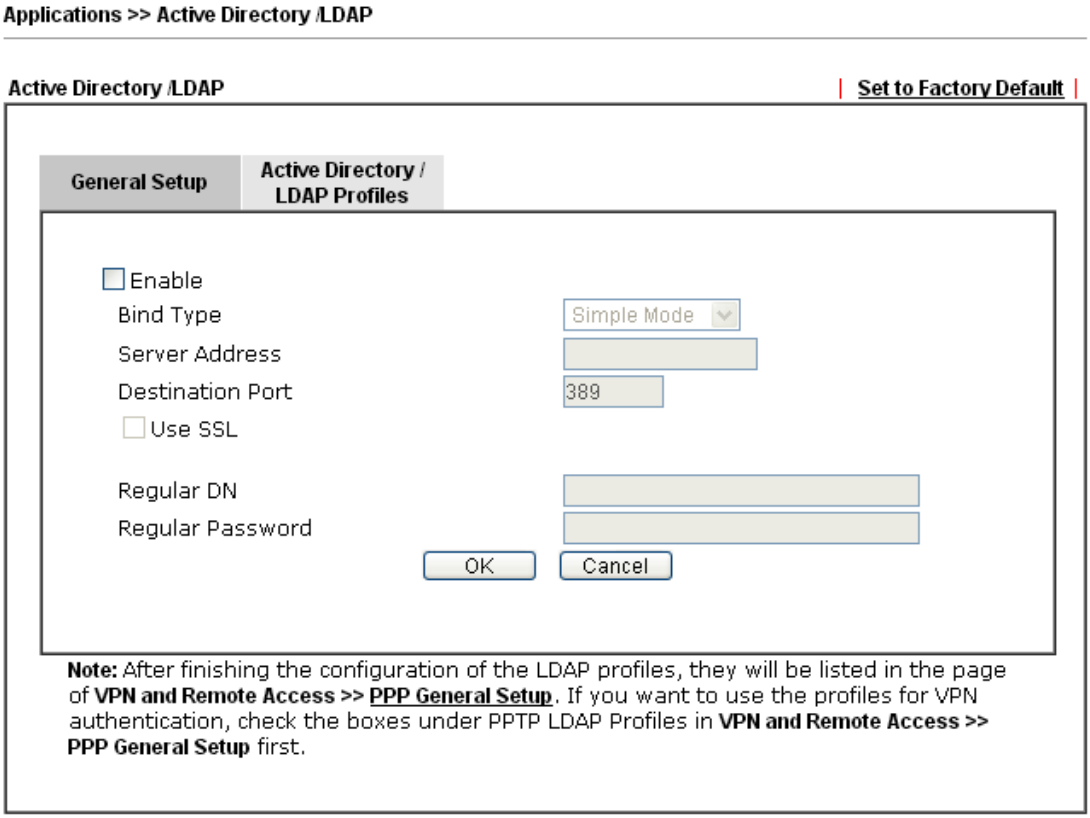
II-5-6 Active Directory/LDAP

LDAP (Lightweight Directory Access Protocol)是運用 TCP/IP 網路的共用協定，它可定義用戶端存取分享目錄伺服器的方法，在目錄上工作以及共享目錄內的資訊。LDAP 標準是由國際網路工程研究團隊(IETF)所建立。

LDAP 的設計就是成爲一個存取目錄伺服器最有效的方式，而無其他目錄伺服器協定複雜特性。因爲 LDAP 被定義爲可在目錄內安全地執行、查詢及修改資訊，因此使用者可套用 LDAP 來搜尋或是條列目錄物件，查詢或是管理運作中的目錄。

II-5-6-1 基本設定(General Setup)

本頁可讓您啓用功能並設定 LDAP 伺服器一般內容資訊。



可用設定說明如下：

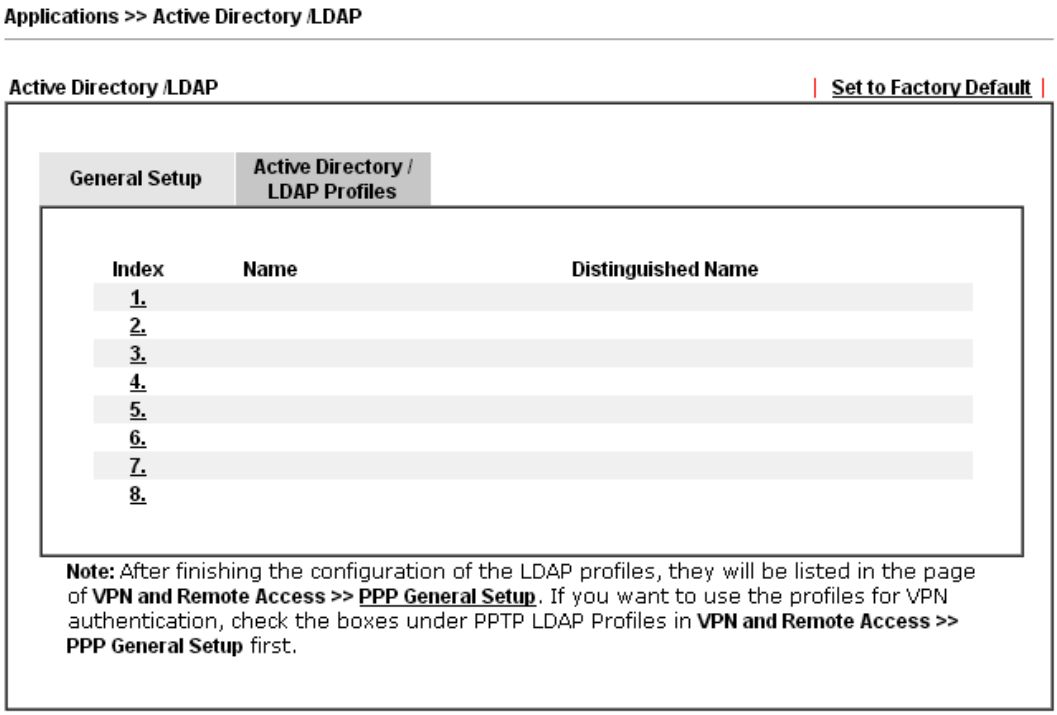
項目	說明
啓用(Enable)	勾選此框啓用此功能。
綁定類型(Bind Type)	有三種綁定類型可以選擇： ● **簡易模式(Simple Mode)** – 不用進行任何搜尋動作，直接綁定驗證。 ● **匿名(Anonymous)** – 先以匿名帳號執行搜尋動作，再進行綁定驗證。 ● **Regular 模式(Regular Mode)** – 大部分皆與匿名模式相同，不同之處再於伺服器將會先檢查是否具備搜尋權限。 對於 **Regular** 模式，您需要輸入 **Regular DN** 以及 **Regular 密碼。**
伺服器位址(Server	輸入 LDAP 伺服器的 IP 位址。

Address)	
目標通訊埠(Destination Port)	輸入 LDAP 伺服器之目的埠號。
使用 SSL(Use SSL)	勾選此方框使用 SSL 需求的埠號。
Regular DN	如果選擇 **Regular 模式爲綁定類型**，請在此輸入 **DN** 設定。
Regular Password (Regular 密碼)	如果選擇 **Regular 模式爲綁定類型**，請在此輸入密碼設定。

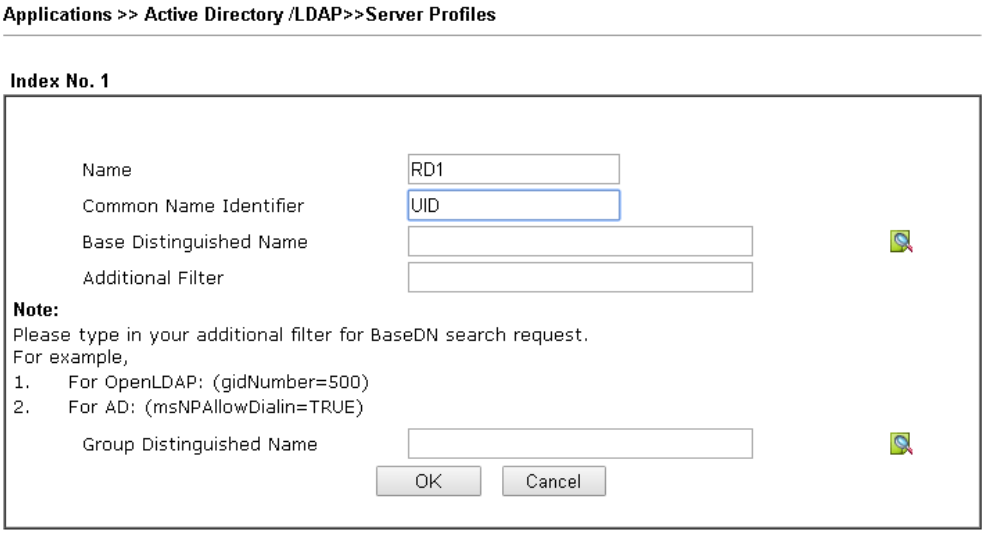
完成上述設定之後，請按下**確定(OK)**儲存。

II-5-6-2 Active Directory / LDAP 設定檔(Active Directory / LDAP Profiles)

您可以設定 8 組 AD/LDAP 設定檔，這些設定檔將用於使用者管理中以因應不同管理目的。



按下任一索引編號開啓下述頁面：



可用設定說明如下：

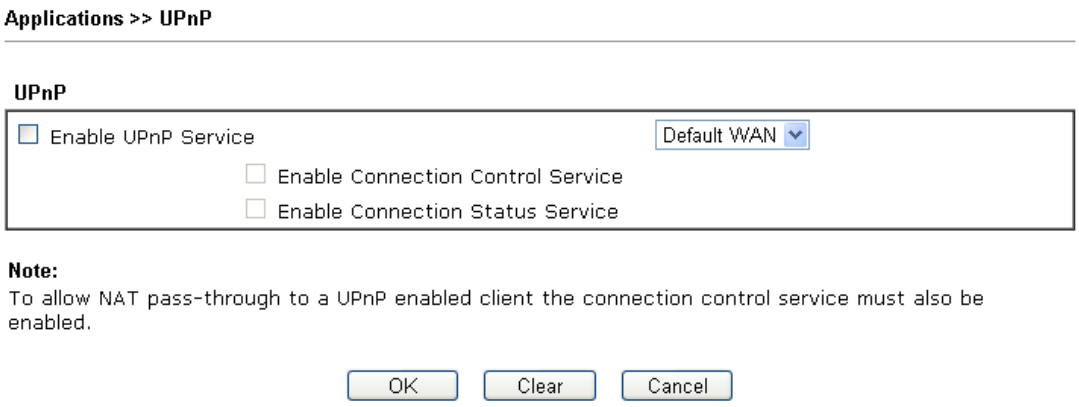
項目	說明
名稱(Name)	輸入設定檔的名稱。
共同名稱識別(CN ID)	輸入或是編輯 LDAP 伺服器的名稱識別碼，通用名稱爲 cn。
額外的過濾器(Additional Filter)	輸入額外過濾需求的條件。
基礎網域名稱(BaseDN) / 群組網域名稱(Group DN)	輸入或是編輯用於查詢 LDAP 伺服器中條目可分辨的名稱。 有時候，您可能會因爲名稱太長而忘記 Distinguished Name，那麼您可按下 按鈕列出 AD/LDAP 伺服器全部的帳號資訊，幫助您完成設定。

完成上述設定之後，請按下**確定(OK)**儲存，新的設定檔即可完成。

II-5-7 UPnP

UPnP 協定爲網路連線裝置提供一個簡易安裝和設定介面，爲 Windows 隨插即用系統上的電腦週邊設備提供一個直接連線的方式。對於 NAT 路由器來說，最主要的功能在於“NAT Traversal”，它可讓防火牆內的應用程式得以自動開放通過路由器的埠口。

資訊	某些應用程式需要 UPnP 來運作，像是 PPS, Skype, eMule…等等，如果您對 UPnP 不熟悉，建議您關閉此功能以確保安全。



可用設定說明如下：

項目	說明
啓用 UPnP 服務(Enable UPNP Service)	您可以視情況勾選**啓用連線控制服務(Connection Control Service)**或是**啓用連線狀態服務(Connection Status Service)**。
預設 WAN(Default WAN)	用來指定套用此功能的 WAN 介面。

有關防火牆與 UPnP 功能之提示:

無法與防火牆軟體配合 ftware

在您的電腦上啓用防火牆有可能造成 UPnP 不正常運作，這是因爲這些應用程式會擋掉某些網路通訊埠的存取能力。

安全考量

在您的網路上啓用 UPnP 功能可能會招致安全威脅，在您啓用 UPnP 功能之前您應該要小心考慮這些風險。

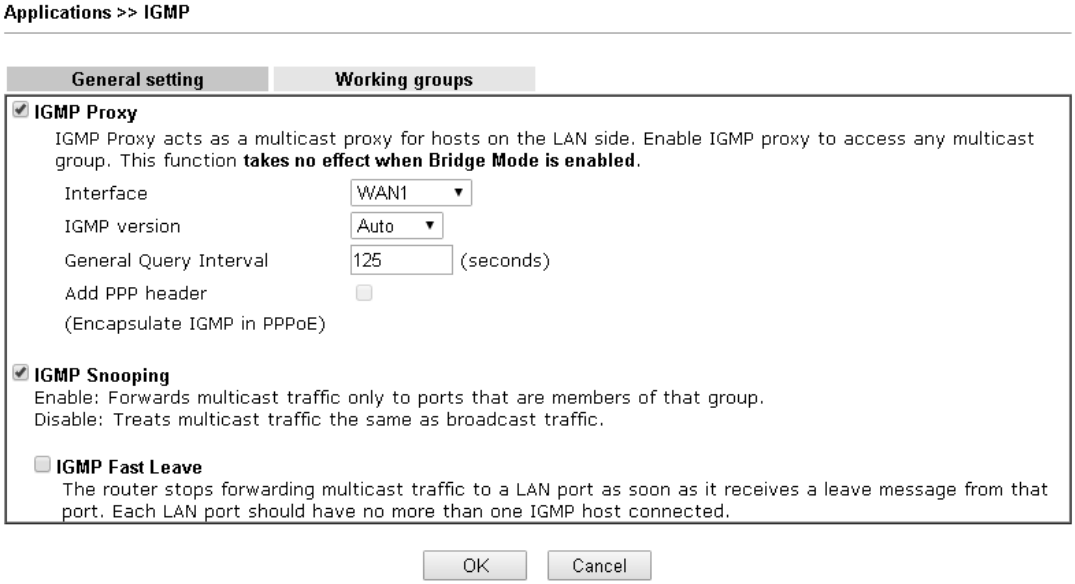
- 某些微軟操作系統已發現到 UPnP 的缺點，因此您需要確定已經應用最新的服務封包。
- 未享有特權的使用者可以控制某些路由器的功能，像是移除和新增通訊埠對應等。

UPnP 功能可不斷變化的新增通訊埠對應來表示一些察覺 UPnP 的應用程式，當這些應用程式不正常的運作中止時，這些對應可能無法移除。

II-5-8 IGMP

IGMP 爲 *Internet Group Management Protocol* 的縮寫，主要是用來管理網際網路協定多重播送群組會員數目的一種協定。

II-5-8-1 基本設定(General Setting)

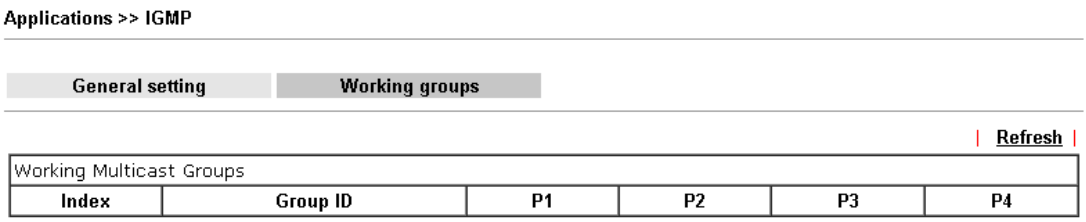


可用設定說明如下：

項目	說明
IGMP 伺服器(IGMP Proxy)	勾選此框啓用此功能。多重播送將透過 WAN/PVC/VLAN 埠口來執行。此外，此功能僅在 NAT 模式下可用。 **介面(Interface)** – 指定封包傳輸的介面。 **IGMP 版本(IGMP version)** – 目前路由器支援二個版本(v2 與 v3)，請依照您所訂購的 IPTV 服務選擇適合的版本。 **基本詢問間隔(General Query Interval)** – 透過發送詢問的方式，路由器會定期檢查從 IPTV 服務中獲取哪個 IP 位址，對用戶來說可能會造成些許不便，因此設定適合的時間(單位：秒)作爲詢問的間隔，以限制路由器發送詢問的頻率。 **新增 PPP header(Add PPP header)** – Check this box if the interface type for IGMP is PPPoE. It depends on the specifications regulated by each ISP. If you have no idea to enable or disable, simply contact your ISP providers.勾選
IGMP Snooping	勾選此方塊啓用此功能，多重播送流量將會轉送往具有該會員的群組之連接埠中。關閉此功能將會使多重播送流量被視爲一般的廣播播送流量。
IGMP 快速切換(IGMP Fast Leave)	勾選此框讓路由器一旦接收切換訊息時，即停止轉送多重播送流量至 LAN 埠口。每個 LAN 埠口都應連上一個 IGMP 主機。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

II-5-8-2 工作群組(Working Groups)



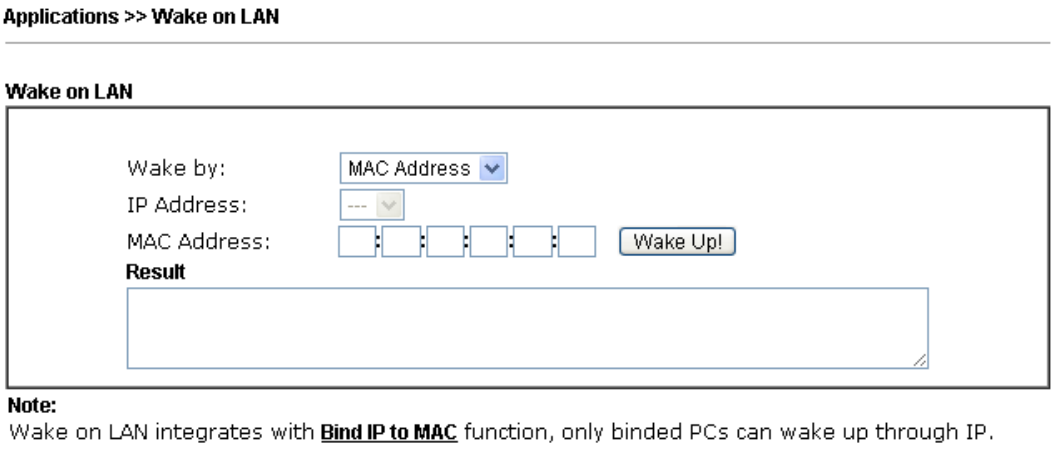
可用設定說明如下：

項目	說明
頁面更新(Refresh)	按下此連結更新多重播送群組狀態。
群組 ID(Group ID)	此區顯示多重播送群組的 ID 連接埠，可用範圍爲 224.0.0.0 至 239.255.255.254。
P1 到 P4	多重播送群組中所使用的 LAN 連接埠。

II-5-9 網路喚醒(Wake on LAN,WOL)

區域網路上的電腦可以透過所連結的路由器來喚醒，當使用者想要從路由器喚醒指定的電腦時，使用者必須在此頁面上輸入該電腦正確的 MAC 位址。

此外，此台電腦必須安裝有支援 WOL 功能的網卡，並在 BIOS 設定中開啓 WOL 功能。



可用設定說明如下：

項目	說明
喚醒方式 **(Wake by)**	有二種方式提供給使用者喚醒綁定 IP 的電腦： ● 如果您選擇由 MAC 位址來喚醒的話，您必須輸入該主機正確的 MAC 位址； ● 如果您選擇的是由 IP 位址來喚醒的話，您必須選擇正確的 IP 位址。
IP 位址 **(IP Address)**	已在**防火牆>>綁定 IP 至 MAC(Firewall>>Bind IP to MAC)**中設定完成的 IP 位址，將會出現在下拉式清單中，請自清單中選取您想要喚醒的電腦 IP。
MAC 位址 **(MAC Address)**	輸入被綁定之電腦的 MAC 位址。
網路喚醒(Wake Up)	按此鈕可以喚醒選定的電腦，喚醒結果將會顯示在方框內。

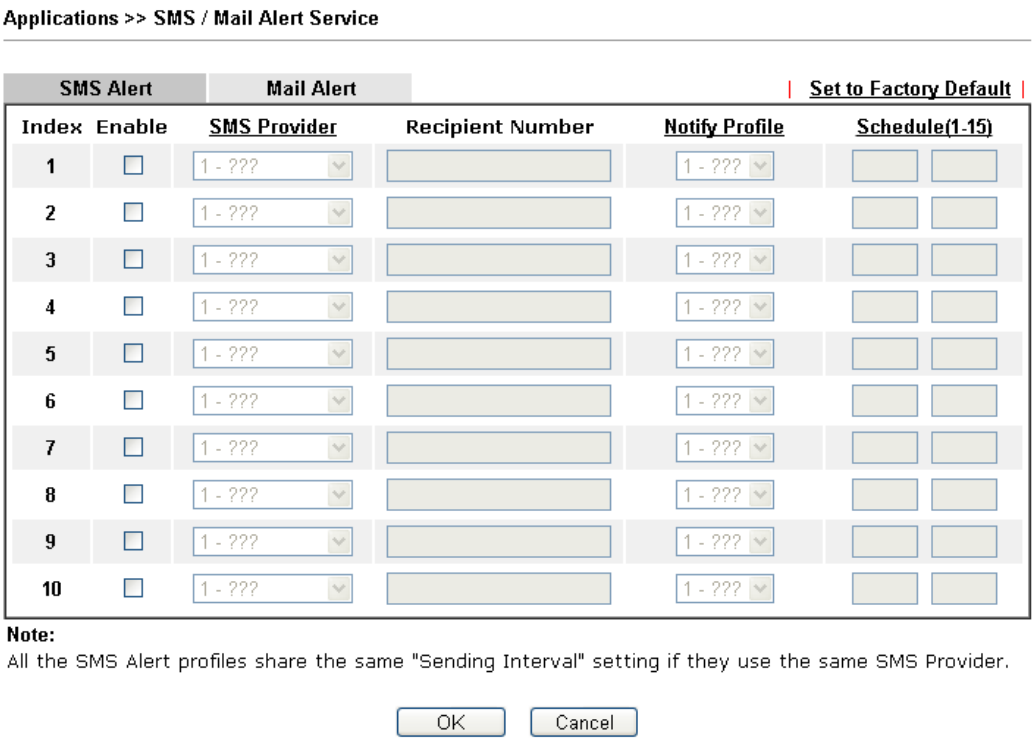
II-5-10 簡訊(SMS)/郵件警示服務(SMS / Mail Alert Service)

簡訊/郵件警示功能是路由器透過指定的服務供應商，傳送訊息至使用者行動電話或是電子郵件信箱，幫助使用者即時了解異常現象。

Vigor 路由器可讓您設定 10 組簡訊設定檔，可依據不同條件發送出去。

II-5-10-1 簡訊警示(SMS Alert)

本頁讓您指定簡訊服務供應商、收信人為何以及收信內容。



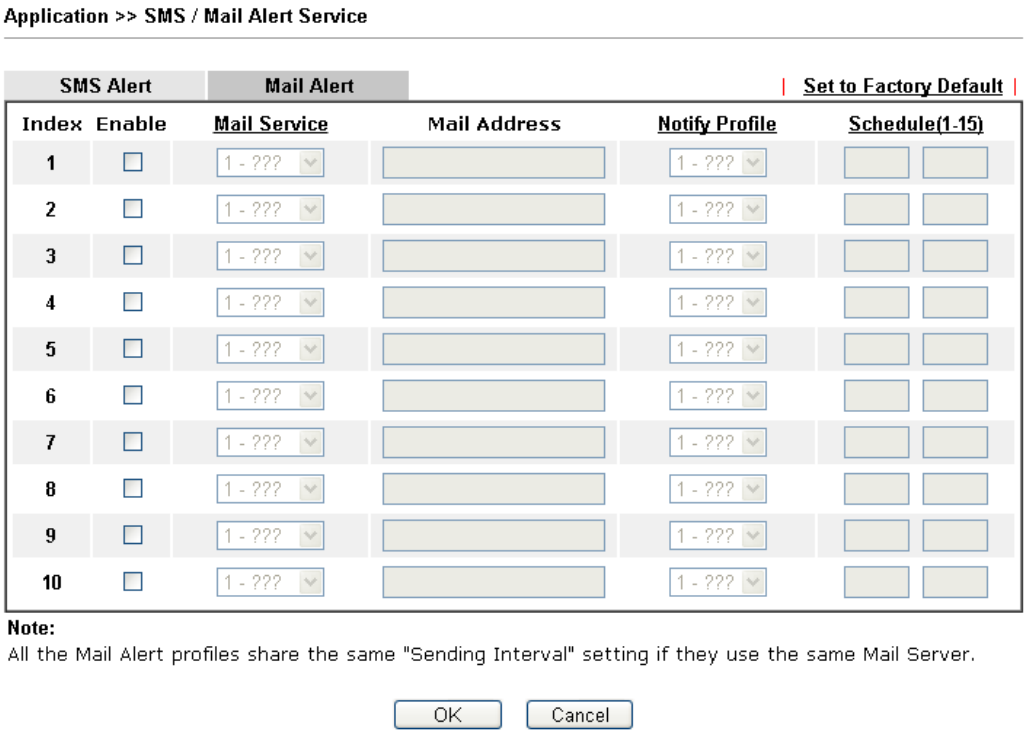
可用設定說明如下：

項目	說明
啓用(Enable)	勾選此方框啓用設定檔。
簡訊服務供應商(SMS Provider)	使用下拉式清單選則簡訊服務供應商。 您可以點**簡訊服務供應商**連結來定義 SMS 簡訊伺服器。
收信人號碼(Recipient Number)	輸入收信人的電話號碼。
通知設定檔 (Notify Profile)	使用下拉式清單選擇訊息設定檔。收信人將會收到通知設定檔內的訊息。 您可以點**通知設定檔**連結來定義簡訊的內容。
排程 (Schedule(1-15))	輸入簡訊發出的時間排程編號。 您可點**排程(1-15)**連結來定義排程內容。

完成設定之後，按下確定(OK)按鈕儲存相關設定。

II-5-10-2 郵件警示(Mail Alert)

本頁讓您指定郵件伺服器設定檔，收信人爲何以及收信內容。



可用設定說明如下：

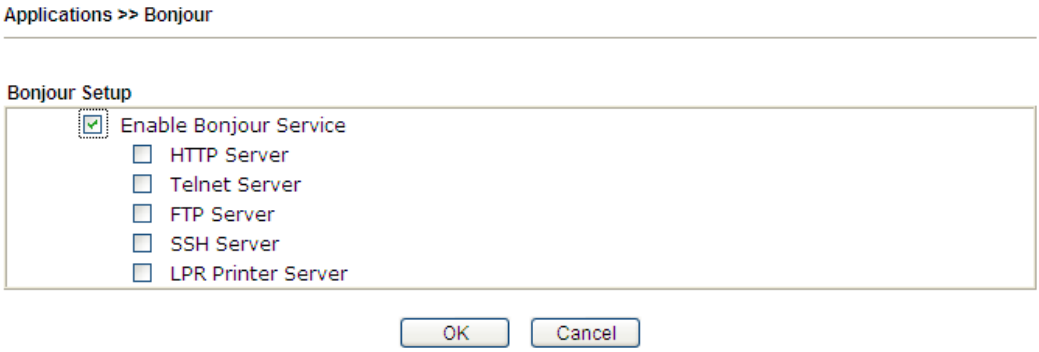
項目	說明
啓用(Enable)	勾選此方框啓用設定檔。
郵件服務(Mail Service)	使用下拉式清單選擇郵件服務物件。所有可用的物件皆可在**物件設定>>簡訊/郵件服務物件(Object Settings>>SMS/Mail Service Object)**建立。 您可以點**郵件服務(Mail Service)**連結來定義郵件伺服器。
郵件位址(Mail Address)	輸入收信人的電子郵件信箱。
通知設定檔 (Notify Profile)	使用下拉式清單選擇訊息設定檔。收信人將會收到通知設定檔內的訊息。 您可以點**通知設定檔**連結來定義簡訊的內容。
排程 (Schedule(1-15))	輸入簡訊發出的時間排程編號。 您可點**排程(1-15)**連結來定義排程內容。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

II-5-11 Bonjour

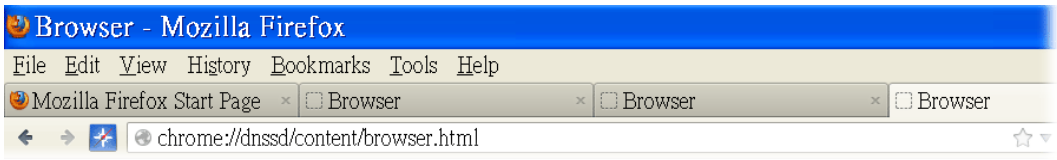
通常，使用者必須設定路由器或是個人電腦來使用各式各樣的服務，但有時候，設定很繁雜(出如 IP 設定、埠號設定等等)也不容易完成。這個功能的目的就是在降低設定的配置程度，如果主機與使用者的電腦安裝了 Bonjour 外掛驅動程式，它們就可透過點選路由器名稱圖示的方式來使用路由器提供的服務。簡單來說，用戶/使用者只要知道路由器的名稱就夠了。

要啓用 Bonjour 服務，請開啓**其他應用>>Bonjour(Application>>Bonjour)**，勾選您想要分享區域網路用戶的服務項目。

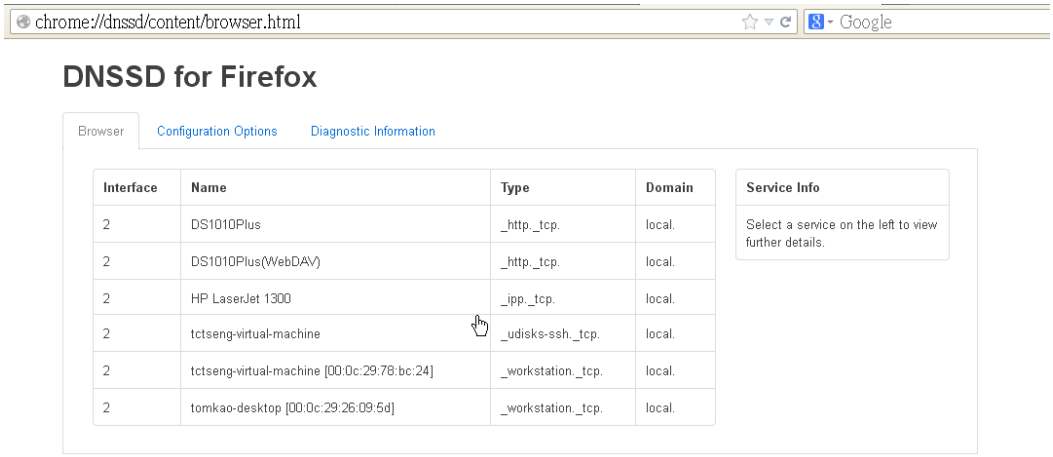


下面提供一個簡單的範例來應用 bonjour 功能：

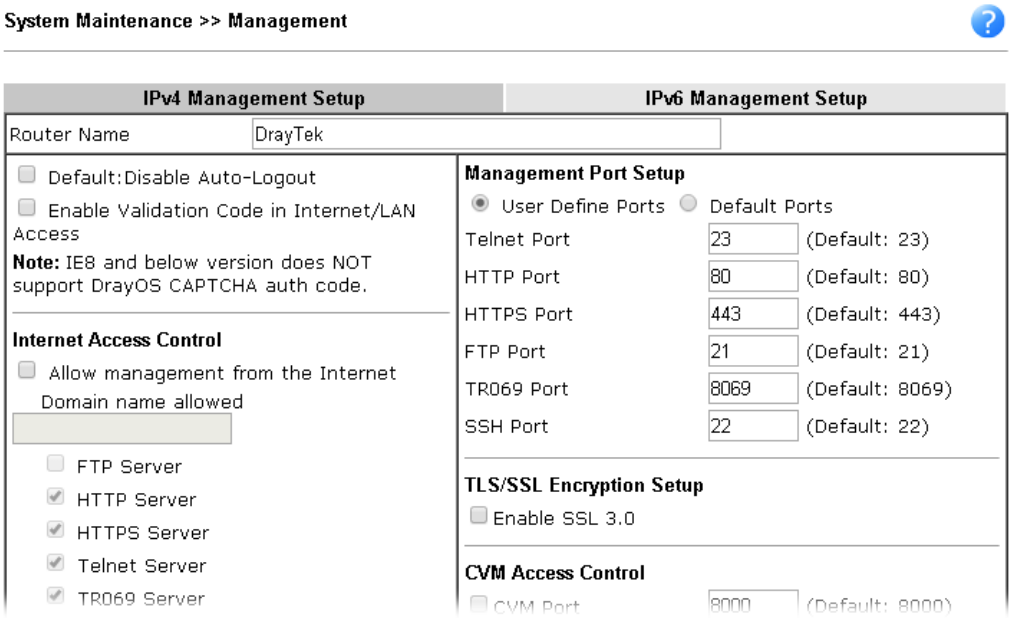
1. 此處我們使用 Firefox 與 DNSSD 來說明，請先確認 Bonjour 用戶端程式與 Firefox 的 DNSSD 已經安裝在電腦上。



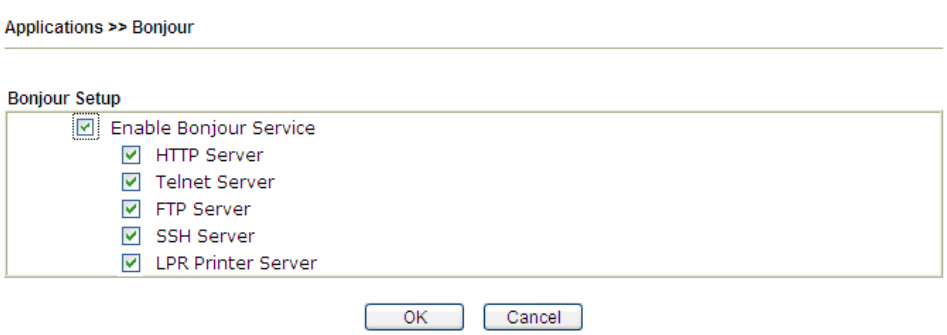
2. 在 Firefox 網頁瀏覽器上，如果 Bonjour 與 DNSSD 已經安裝完畢，您可以開啓相關網頁並看到如下的結果：



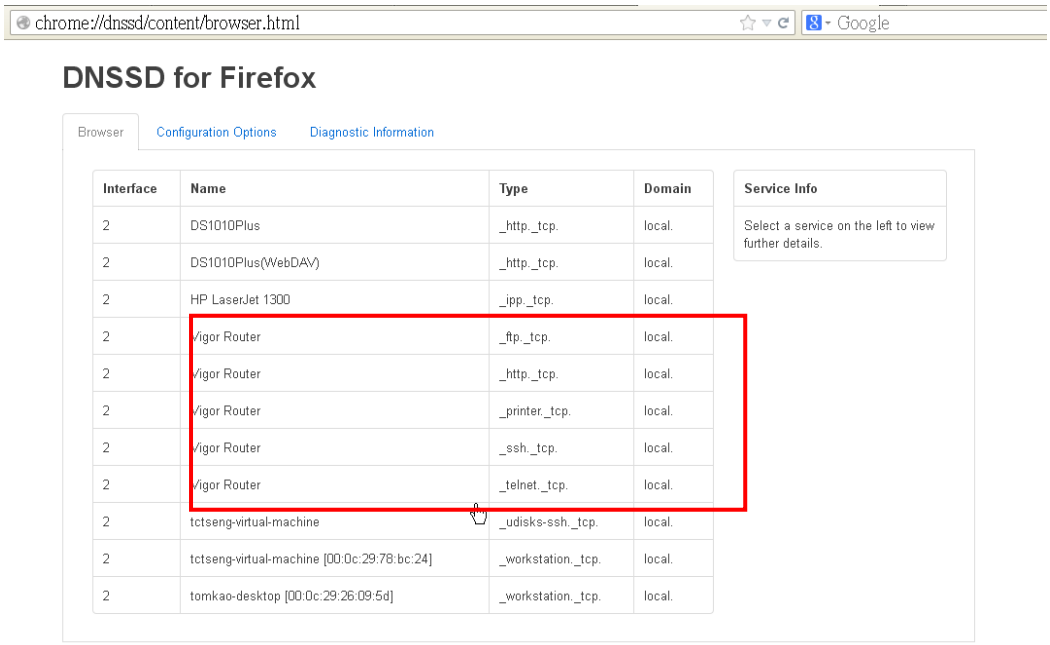
3. 開啓**系統維護>>管理(System Maintenance>>Management)**，輸入**路由器名稱**(例如 DrayTek)，然後按下**確定(OK)**儲存。



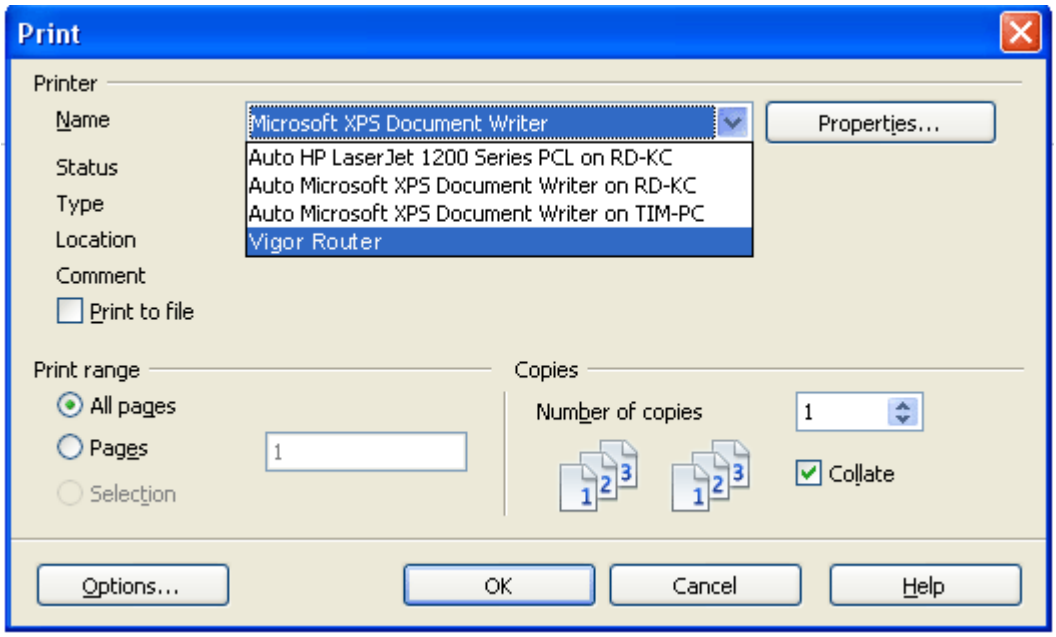
4. 接著，開啓**其他應用>>Bonjour(Applications>>Bonjour)**，勾選您想要透過 Bonjour 分享的服務。



5. 再次打開 DNSSD 頁面，可用的項目變更如下，表示 Vigor 路由器(以 Bonjour 協定爲基準)已經準備妥當可以作爲印表機伺服器、FTP 伺服器、SSH 伺服器、Telnet 伺服器以及 HTTP 伺服器。



6. 現在，任何頁面或是文件都可以透過 Vigor 路由器(配備有印表機)來列印輸出。



II-5-12 高可靠度(High Availability)

路由器的高可靠度功能提供網路資源冗餘，並在元件產生失誤時減少當機的時間。HA 是否複雜取決於系統中斷的可用性需求以及容忍程度。提供接近全時可用性的系統，通常都具有冗餘的硬體與軟體。

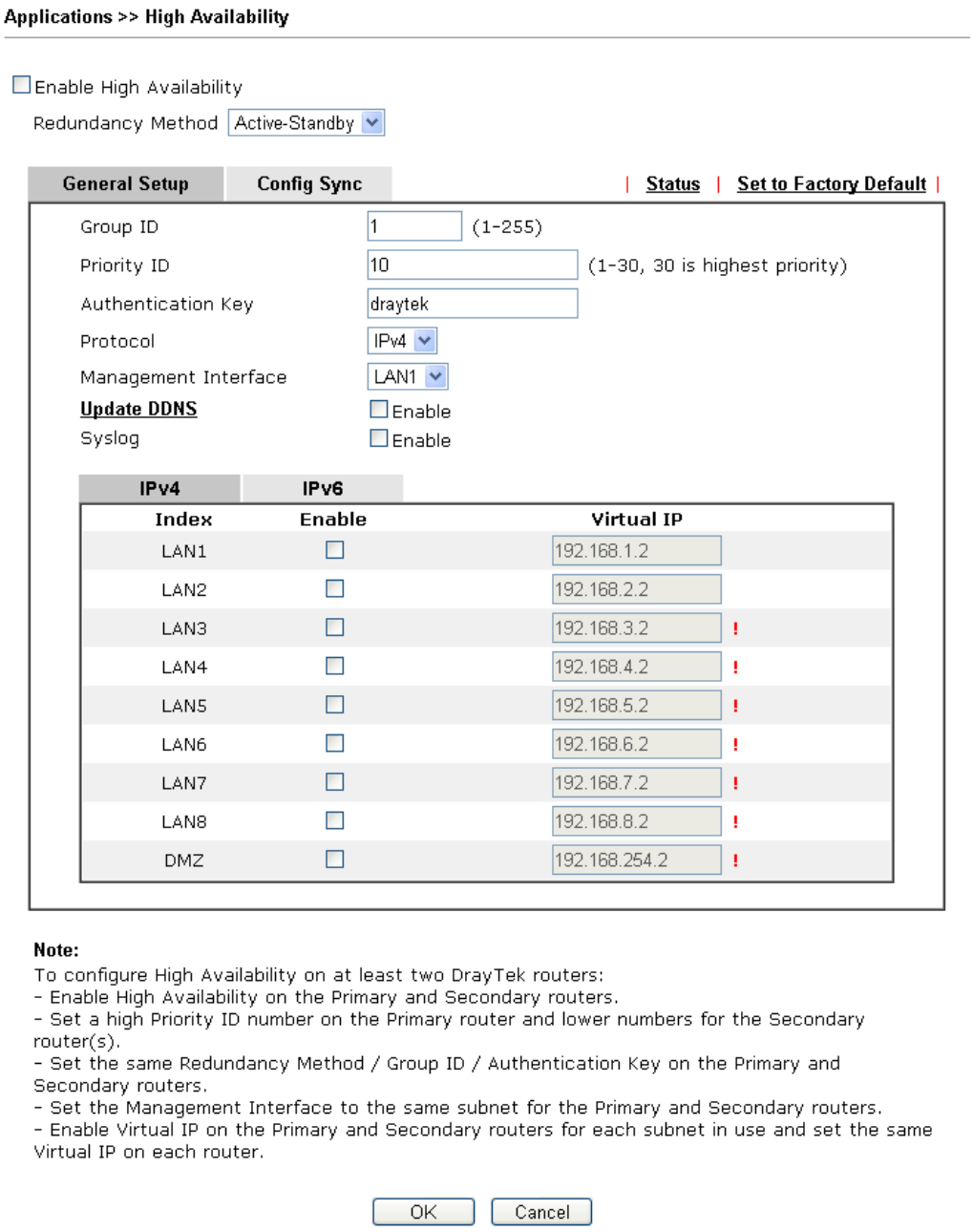
Vigor2926 的 HA 功能主要用意是避免單點故障，全部故障事件的發生。當發生故障時，故障轉移過程會將故障元件(主要路由器)所處理的網路負載移轉到被援元件(次要路由器)，即可保留網路資源的可用性，並且發生故障的部分亦可恢復。

欲設定高可靠度，至少要有 2 台路由器依如下內容設定：

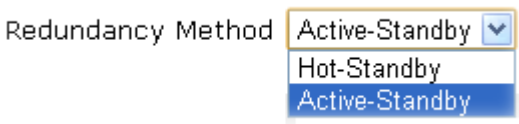
- 主要與次要路由器皆須啓用高可靠度功能
- 主要路由器設定高優先權 ID；而次要路由器設定較低的優先權 ID
- 2 台路由器皆設定一致的冗餘方式、群組 ID 與驗證密鑰
- 2 台路由器的管理介面皆設定在相同的網段上
- 在 2 台路由器上每個使用中的子網皆設定虛擬 IP，確保 2 台路由器的虛擬 IP 是相同的

II-5-12-1 基本設定(General Setup)

選擇**其他應用>>高可靠度(Applications>>High Availability)** 開啓如下頁面。



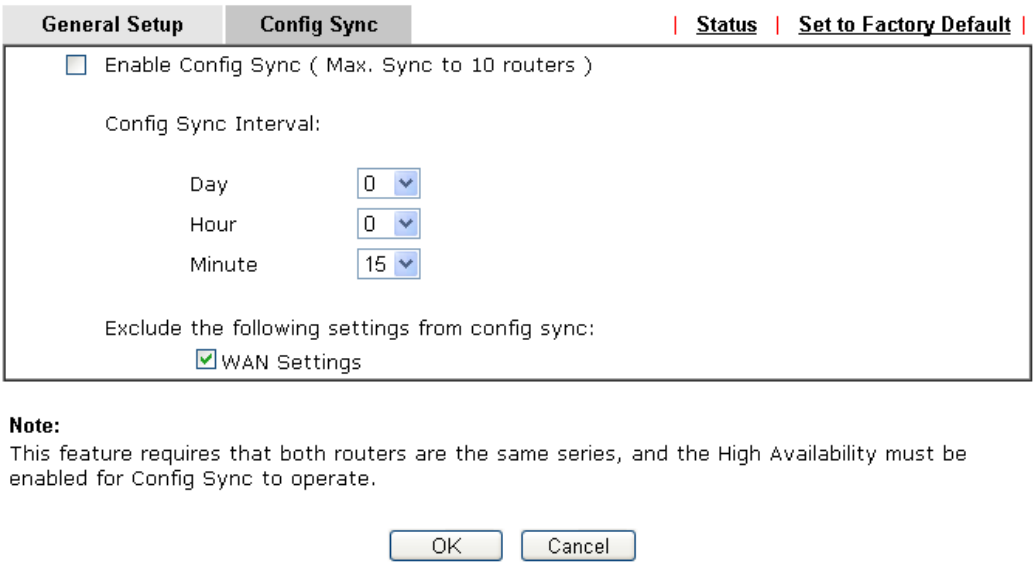
可用設定說明如下：

項目	說明
啓用高可靠度(Enable High Abailablity)	勾選此框啓用此功能。
Redundancy 方式 (Redundancy Method)	選擇冗餘方式。 

	熱備援(Hot-Standby) - 此方式非常適合僅有一組 ISP 帳號。當您選擇此方式時， ● 正常情況下，次要路由器會是閒置狀態，當主要路由器發生故障無法正常運作時，次要路由器將接管任務，進行運作 ● 主要和次要路由器的 WAN 設定必須一致 **附註**: 當系統使用熱備援時，於次要路由器的無線區域網路功能將直接被"停用"，用戶端無法隨時透過次要路由器上網。 **主動被援(Active-Standby) -** 當同時有數個 ISP 連線運作時，適合使用此一方式。當您選擇此方式時， ● 次要路由器上的 WAN 介面可以同時設定，在高可靠度下的區域網路用戶可以路由到次要路由器上 ● 主要和次要路由器上的 WAN 設定是分開設定的 ● 可以啓用設定同步化以便在主要和次要路由器間同步大多數的設定內容 ● 所有路由器必須設定相同的冗餘方式
群組 ID(Group ID)	輸入數值(1~255)。 在區域網路環境中，數個路由器可以區分成數個群組，每個群組都必須指定一個群組 ID 名稱。具有相同 ID 數值的不同的路由器可歸類到相同的群組中。 只有相同群組中的路由器可以被選定爲主要路由器。
優先權 ID(Priority ID)	輸入數值(1~30)。 不同的路由器必須設定不同的 ID。 在同一個群組中的路由器必須分派一個優先權 ID，在群組中，優先權 ID 最大的(例如最高優先權)將被視爲主要路由器。當群組中多個路由器被分派相同的優先權 ID 時，LAN IP 位址(於 LAN>>基本設定頁面)較低的路由器就會具有較高的優先權。
驗證密鑰(Authentication Key)	輸入驗證密鑰，最常可設定 31 個字元。這個密鑰可用來加密 DARP (DrayTek Address Redundancy Protocol)流量以防範惡意攻擊。
通訊協定(Protocol)	選擇用於 DARP 的 IP 通訊協定。
管理介面(Management Interface)	選擇在路由器間 DARP 協商使用的介面，只有 **LAN>>基本設定** 上啓用的介面可以選擇作爲管理介面。注意，LAN1 永遠啓用。
更新 DDNS (Update DDNS)	**啓用(Enable) -** 勾選此框以便在主要路由器發生故障時，得以更新次要裝置的 DDNS 伺服器。 如果主要裝置故障了，次要裝置必須接管資料傳輸與接收的工作。然後系統將會更新 DDNS 伺服器設定，讓使用者連接到指定的網域上。
Syslog	**啓用(Enable) -** 勾選此框紀錄必要的資訊於 Syslog 上。
LAN1 ~ LAN6, DMZ	**啓用(Enable) -** 勾選此框啓用此介面。 **虛擬 IP(Virtual IP) -** 輸入扮演主要裝置角色之路由器的 IP 位址。

II-5-12-2 設定同步化(Config Sync)

本頁用來指定此路由器的設定同步化時間，目前只有在高可靠度啓用且使用熱備援(Hot-Standby)時才能使用。



可用設定說明如下：

項目	說明
啓用設定同步化 (最多可同時進行 10 台路由器) (Enable Config Sync (Max. Sync to 10 routers))	勾選此框啓用設定同步化功能。 欲將主要路由器的設定同步化至次要路由器，二個路由器都需要啓用設定同步化(config sync)功能，並請注意目前只在 Redundancy 方式(Redundancy Method)選擇熱備援的情況下，得以使用同步化功能。
設定同步化間隔(Config Sync Interval)	**日/時/分(Day / Hour / Minute)** - 主要路由器將在指定的時間間隔，與次要路由器進行設定同步化。
自同步設定檔中排除下述設定(Exclude the following settings from config sync)	當執行設定同步化時，本區選擇的設定將排除在外。這個功能在 Redundancy 方式(Redundancy Method)設定爲熱備援(Hot Standby)時可用。

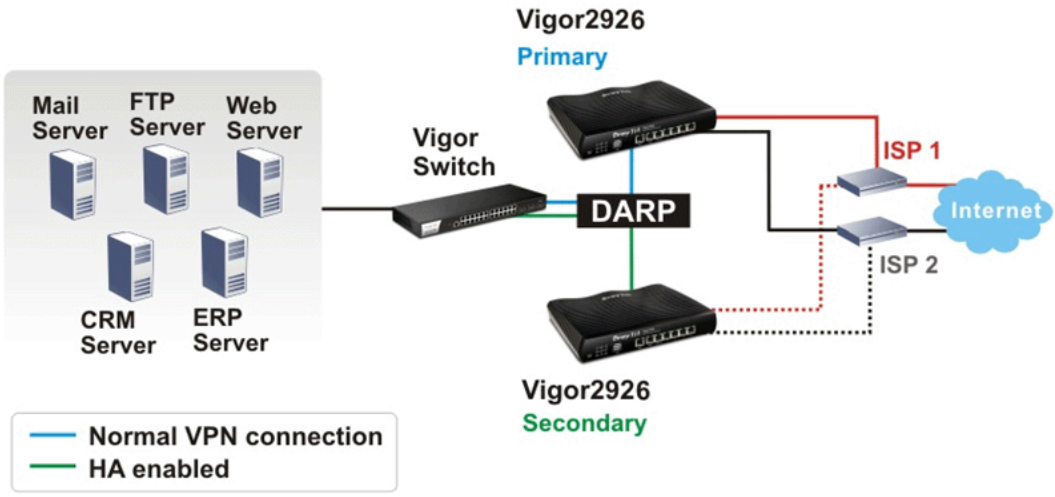
當您完成上述設定時，請按**確定(OK)**按鈕儲存設定。

當設定方式選擇熱備援(Hot Standy)時，下述設定也會同步處理：

- WAN (使用者可選擇)
- LAN
- LAN IPv6
- 路由器名稱
- 管理者與使用者密碼

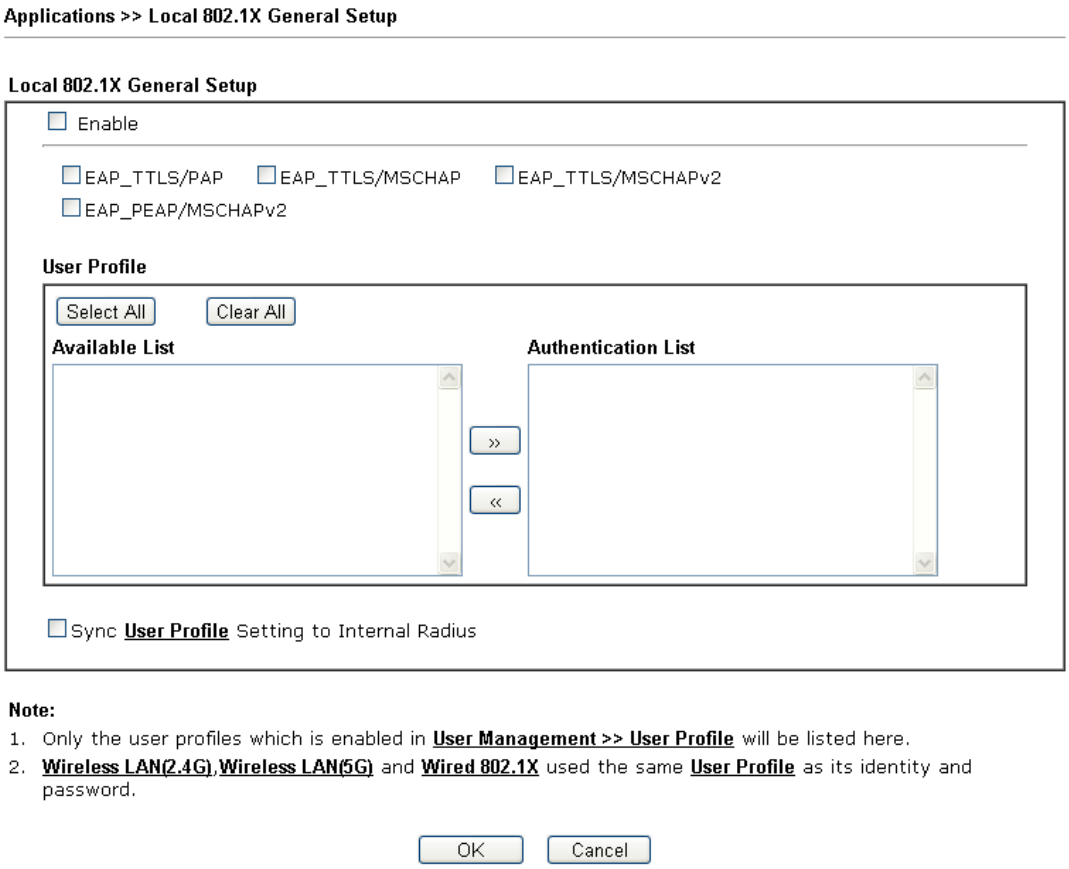
範例:

舉下圖爲例，上方的 Vigor2926 可視爲主要裝置，下方的 Vigor2926 則視爲次要裝置。當主要裝置斷線時，次要裝置會盡快替代主要裝置角色，執行全部的工作。不過，一旦主要裝置重新運作，次要裝置就會轉變爲原始備援的角色。



II-5-13 本機 802.1X 基本設定(Local 802.1X General Setup)

此頁允許您配置內建於路由器中本機 802.1X 伺服器的基本設定，本機 802.X 伺服器可用於驗證有線與無線區域網路用戶。



可用設定說明如下：

項目	說明
啓用(Enable)	勾選此框啓用內建 802.1X 伺服器。 目前此功能可用於無線與有線驗證。
使用者設定檔(User Profile)	**選擇全部(Select All)** – 按此將所有的使用者設定檔從可用清單(Available List)區移至驗證清單(Authentication List)區。 **清除全部(Clear All)** – 按此將所有的使用者設定檔從驗證清單(Authentication List)區移至可用清單(Available List)區。
同步使用者設定檔...(Sync User Profile ….)	這個功能可讓內部RADIUS與本機802.1X的啓用/停用設定同時套用到全部的使用者設定檔中。 例如，若本機 802.1X 設定爲啓用(勾選)，內部 RADIUS 功能也會被啓用。  若本機 802.1X 設定爲停用(未勾選)，內部 RADIUS 功能也會跟

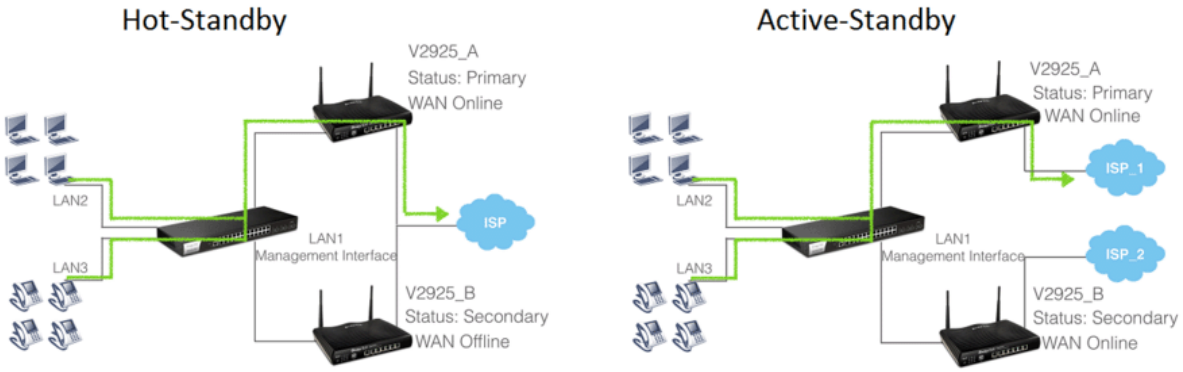
	著停用，即使其早先已被啓用。 
確定(OK)	按此儲存設定。
清除(Clear)	按此移除修改的設定內容。
取消(Cancel)	按此捨棄所有的設定內容。

當您完成上述設定之後，請按**確定(OK)**按鈕儲存。

應用說明

A-1 如何使用高可靠度(HA)?

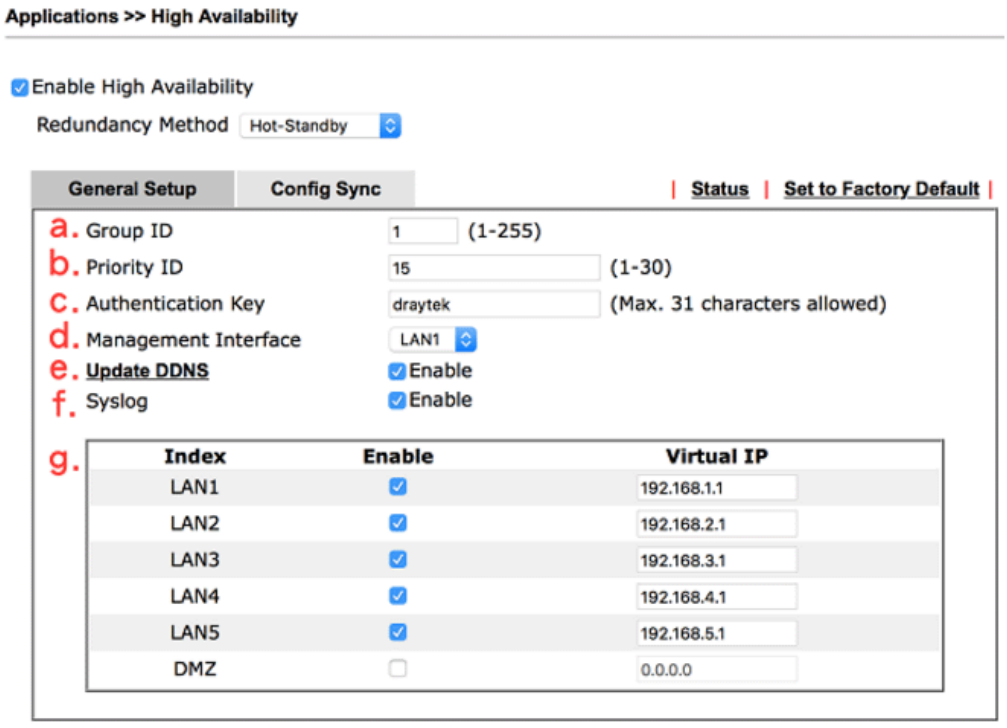
高可靠度提供硬體冗餘方式與區域網路用戶，居易路由器有二種模式可以使用:熱備援(Hot-Standby)與主動被援(Active-Standb)。



在熱備援模式中，主要與次要路由器共享相同的 WAN 資源，通常只有主要路由器會上線，當主要路由器斷線時，次要路由器便會啓用，使用相同的 WAN 線路撥號上線，繼續提供 LAN 用戶網際網路服務。

主動被援模式與熱備援模式幾乎是相同的，只有一個差異，亦即主動被援模式下，主要與次要路由器連接到不同的 WAN 來源，同時次要路由器隨時在上線等候。

1. 在主要路由器上，選擇您想要使用的冗餘模式，然後依照下圖設定頁面：



(a) 群組 ID 用來辨識群組成員有哪些，請對所有的成員輸入相同的 ID，預設值是 1，在此我們也可以直接使用預設值。

(b) 優先權 ID 用來決定哪個路由器被視爲主要路由器，其中數字 30 具有最高優先權。如果有二個或二個以上的路由器具有相同的優先權 ID 號碼，系統將會考量他們的 IP 位址(管理介面用)，例如 192.168.1.2 的優先權就高於 192.168.1.3。

(c) 驗證密鑰: 在所有的成員上輸入相同的驗證密鑰。

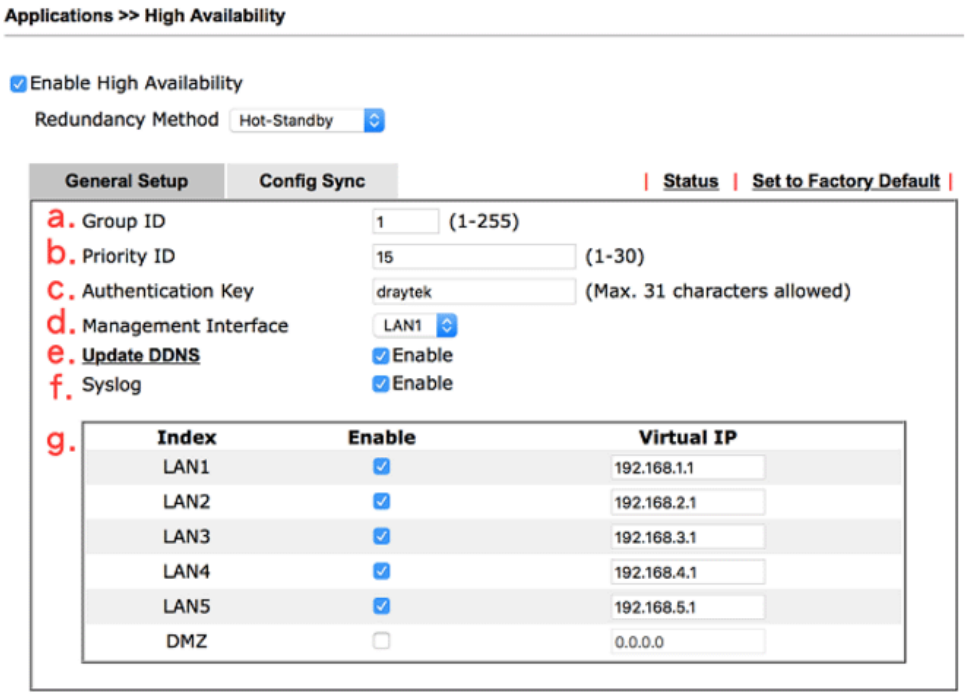
(d) 管理介面: 成員間的封包通訊(包含決定主要路由器、設定同步化、維護等等)會送進管理介面中，換言之，其他區域網路網段上的用戶就無法看見這些封包。爲了取得最佳的通訊內容以及爲了安全性考量，建議選擇一個比較不會受到通訊干擾(迴圈、廣播風暴等等)的介面。在我們設計場景中，我們保留 LAN1 以因應高可靠度使用，其他的 LAN 用戶則分別置於 LAN2~LAN5 中。

(e) 更新 DDNS: 對於動態 WAN IP 用戶，啓用此功能，如此一來，一旦次要路由器變成主要路由器並撥號連上 WAN，它同時也會更新 WAN IP 位址至相同的 DDNS 設定檔中，這樣您即可透過相同的 DDNS 網域存取網路。

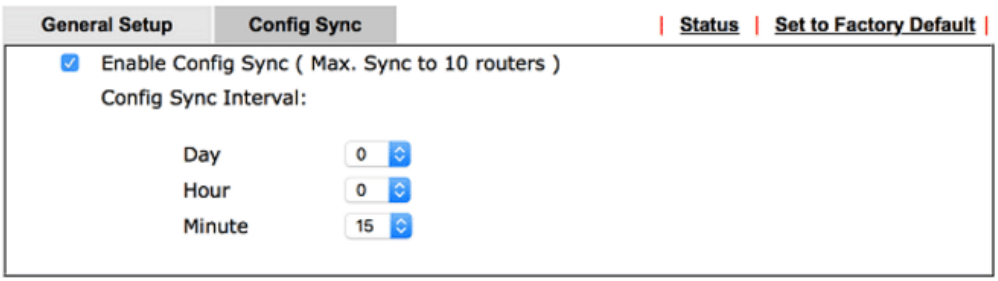
(f) Syslog:啓用此項以便在 Syslog 中顯示所有與高可靠度相關的日誌內容。

(g) 啓用 LAN 子網加入高可靠度，任何現存的區域網路若無加入高可度將無法受到硬體冗餘的服務。

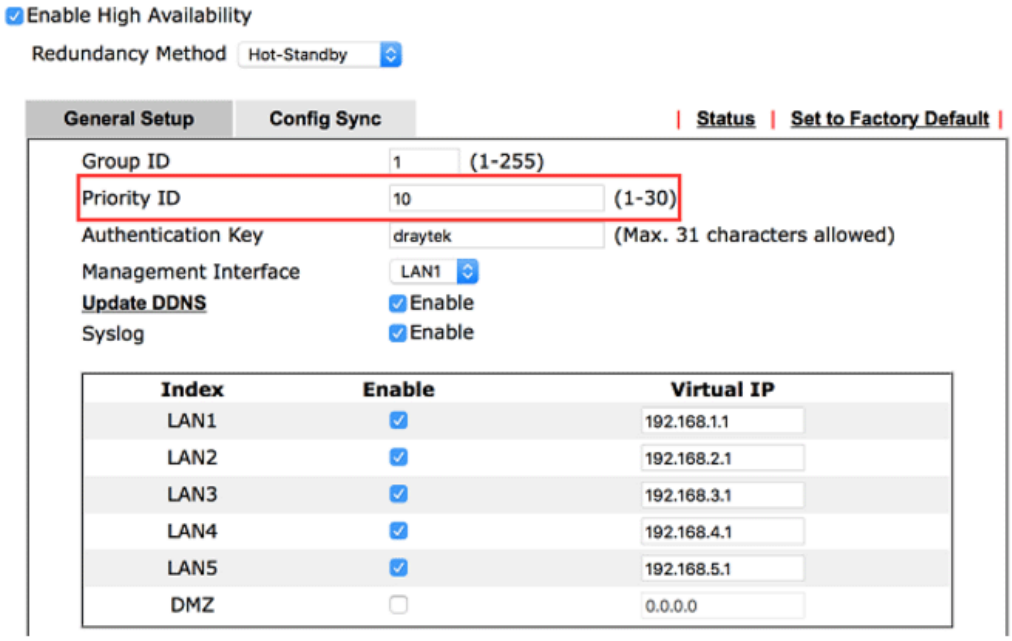
虛擬 IP: 輸入虛擬 IP，請注意這邊的虛擬 IP 不可與任何成員的 LAN IP 相同。



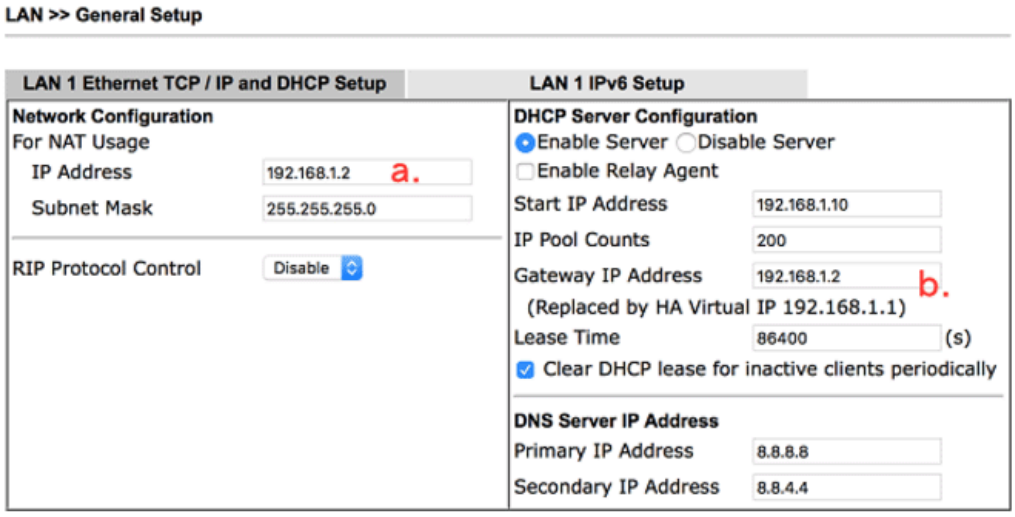
2. 啓用設定同步化與同步化間隔，預設值是 15 分鐘。



3. 設定次要路由器的高可靠度(High Availability)，注意優先權設定必需低於主要路由器的優先權設定，除了優先權以外，其他的設定必須相同。



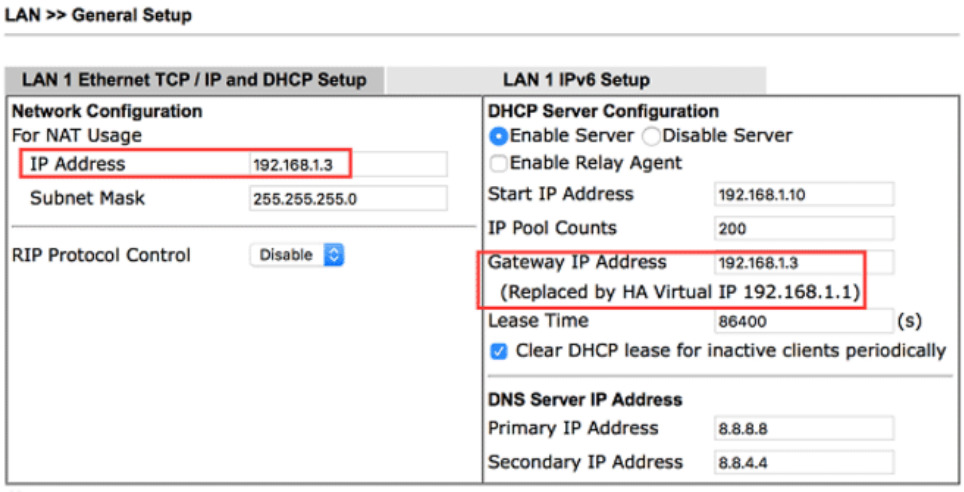
4. 設定主要路由器的 LAN 端設定。



(a) 設定 LAN IP 位址，這個位址必須與次要路由器上的虛擬 IP 及 LAN IP 不同。再者，具有相同優先權 ID 的路由器，其 IP 位址會受到比較，因此在主要路由器上建議使用號碼較低的 IP 位址。

(b) 閘道 IP 與 LAN IP 相同，在括號中的說明表示提供給 LAN 用戶端的閘道將被虛擬 IP 取代。

5. 設定次要路由器的 LAN 設定，請注意 IP 設定必須與主要路由器不同且必須較大。

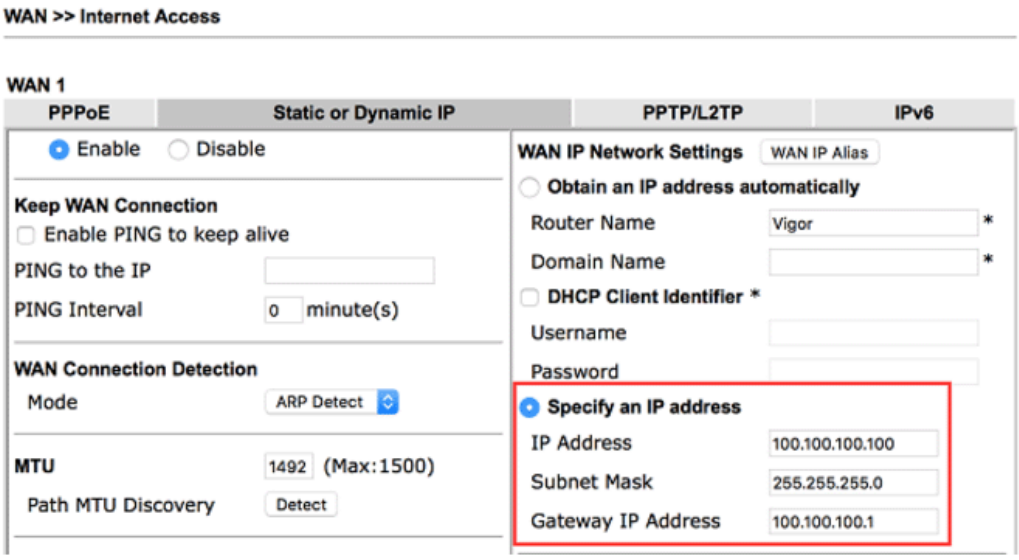


資訊

如果您有一個以上的 LAN，您應該將主要與次要路由器上的每個 LAN IP 設定不同的位址以避免 IP 衝突。舉下圖爲例，有數個 LAN，全部的區域網路都在硬體冗餘的保護下：

	Subnet	Primary Router	Secondary Router	Virtual IP
LAN1	192.168.1.0	192.168.1.2	192.168.1.3	192.168.1.1
LAN2	192.168.2.0	192.168.2.2	192.168.2.3	192.168.2.1
LAN3	192.168.3.0	192.168.3.2	192.168.3.3	192.168.3.1
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
LANx	192.168.x.0	192.168.x.2	192.168.x.3	192.168.x.1

6. 二邊路由器皆已設定高可靠度，在連結二台路由器之前，設定主要路由器上的其他功能，之後即可看到設定同步化。如果您的主要路由器已經設定妥當，請繼續進行下一個步驟。

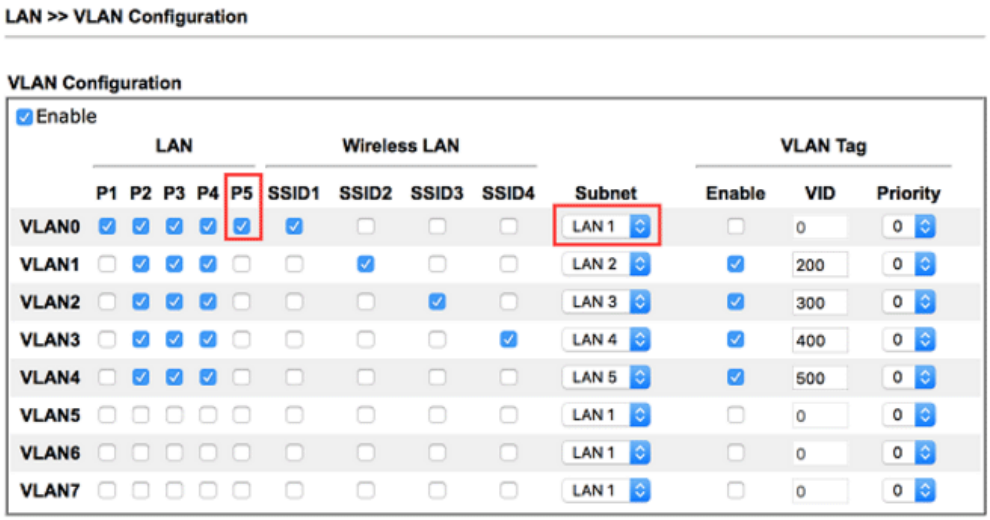


接著確認 WAN 設定內容。

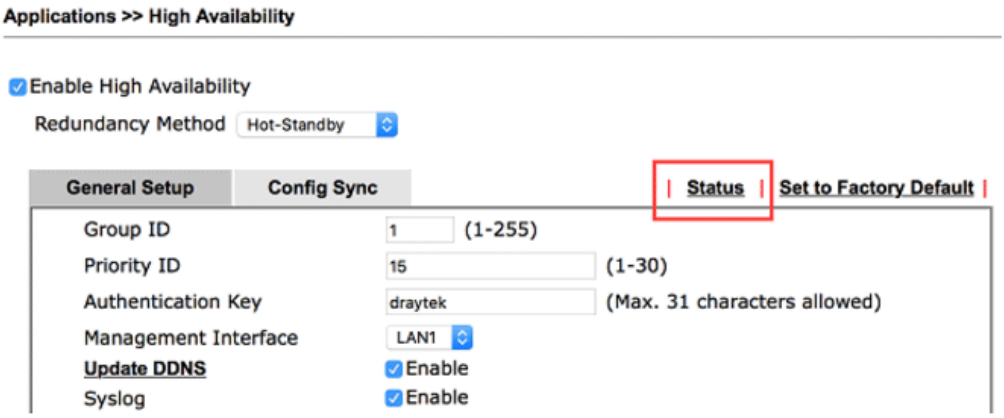
System Information			
Model Name	Vigor2862ac	System Up Time	100:23:32
Router Name	DrayTek	**Current Time**	Wed Jan 05 2000 04:23:26
Firmware Version	3.8.8_RC10_STD	Build Date/Time	Feb 6 2018 18:42:30
DSL Version	772801 HW: A	LAN MAC Address	00-1D-AA-5D-C9-E0

IPv4 LAN Information					
	IP Address	**DHCP**		**IP Address**	**DHCP**
LAN1	192.168.1.3/24	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	192.168.17.1/24	v	**IP Routed Subnet**	192.168.0.1/24	v

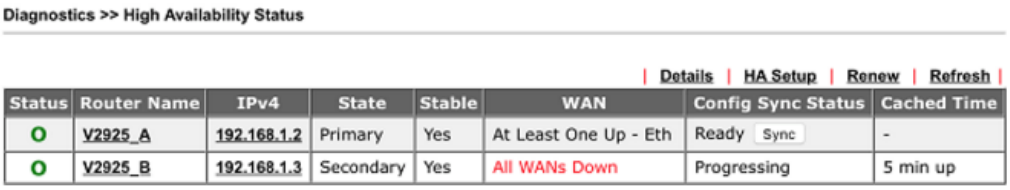
7. 在主要路由器上的功能全部都設定完善之後，我們連結 LAN 管理介面，讓雙邊路由器可以開始彼此偵測，決定哪一個作爲主要裝置並同步化彼此的設定。由於路由器會透過管理介面進行溝通，需要使用屬於的管理介面 LAN 埠口(本例使用 LAN1)，我們可以在 LAN>>VLAN 中檢查此項資訊，在本例中，我們使用埠口 5 供雙邊路由器使用，這樣我們就能使用一條乙太網路纜線連接雙邊路由器的 LAN5 埠口。



8. 按下狀態(Status)連結，檢查高可靠度(HA)狀態。



對於首次連結二台路由器，我們可以看見主要路由器的設定同步到次要路由器(顯示 Progressing)上。



Diagnostics >> High Availability Status

| Details | HA Setup | Renew | Refresh |

Status	Router Name	IPv4	State	Stable	WAN	Config Sync Status	Cached Time
O	V2925_A	192.168.1.2	Primary	Yes	At Least One Up - Eth	Ready Sync	-
O	V2925_B	192.168.1.3	Secondary	Yes	All WANs Down	Progressing	5 min up

注意: "暫存時間(Cached Time)" 指出路由器自其他路由器取得資訊的時間，按下"更新(Renew)"以更新遠端路由器的資訊，按下"頁面更新(Refresh)" 則可更新本機路由器的相關資訊。

完成同步化或是路由器已具有相同設定之後，畫面顯示結果"Equal"：



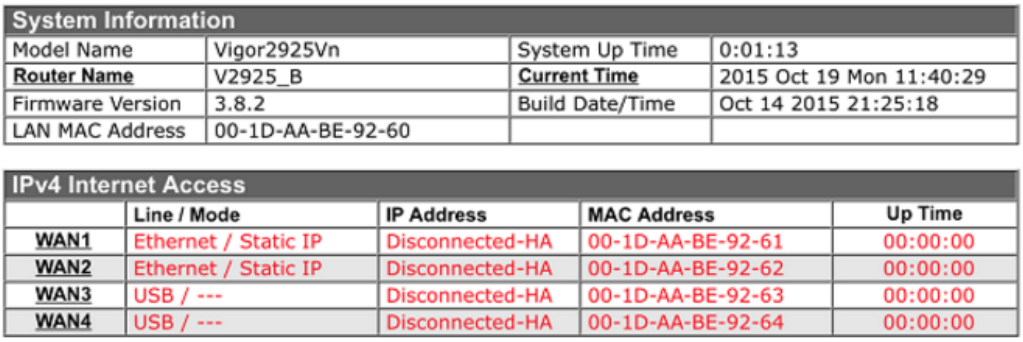
Diagnostics >> High Availability Status

| Details | HA Setup | Renew | Refresh |

Status	Router Name	IPv4	State	Stable	WAN	Config Sync Status	Cached Time
O	V2925_A	192.168.1.2	Primary	Yes	At Least One Up - Eth	Ready Sync	-
O	V2925_B	192.168.1.3	Secondary	Yes	All WANs Down	Equal	3 min 6 sec

注意路由器在達到設定的時間間隔時，將檢查是否有未同步化的修正，我們可以按下"同步化(Sync)"按鈕強迫同步化進行，次要路由器在同步化設定後即重新啓動。

9. 現在我們可以檢查次要路由器是否接收到來自主要路由器的設定，在此範例中，我們檢查次要路由器的線上狀態。



System Information

Model Name	Vigor2925Vn	System Up Time	0:01:13
Router Name	V2925_B	Current Time	2015 Oct 19 Mon 11:40:29
Firmware Version	3.8.2	Build Date/Time	Oct 14 2015 21:25:18
LAN MAC Address	00-1D-AA-BE-92-60		

IPv4 Internet Access

	Line / Mode	IP Address	MAC Address	Up Time
WAN1	Ethernet / Static IP	Disconnected-HA	00-1D-AA-BE-92-61	00:00:00
WAN2	Ethernet / Static IP	Disconnected-HA	00-1D-AA-BE-92-62	00:00:00
WAN3	USB / ---	Disconnected-HA	00-1D-AA-BE-92-63	00:00:00
WAN4	USB / ---	Disconnected-HA	00-1D-AA-BE-92-64	00:00:00

同步化之前，我們並未設定 WAN 介面，目前看到 WAN1 與 WAN2 都有固定 IP，表示其並未接收到相應設定內容。而 "中斷 HA(Disconnected-HA)"表示此路由器，因爲高可靠度群組的主要路由器正在運行之故並未撥打 WAN 連線，因此作爲次要路由器不需要連線。

10. 我們也可以檢查細節設定頁面。

Diagnostics >> High Availability Status >> Details

[Local Router] | Back | HA Setup | Renew | Refresh |

V2925_A				192.168.1.2
State	**Stable**	**WAN**	**Config Sync Status**	**Cached Time**
Primary	Yes	At Least One Up - Eth	Ready Sync	-
MAC		00:1d:aa:c6:4b:d8	**HTTPs Port**	4430
Model		Vigor2925Vn	**Firmware Version**	3.8.2
Enable High Availability		On	**Redundancy Method**	Hot-Standby
Group ID		1	**Priority ID**	15
Authentication Key		draytek	**Management Interface**	LAN1
Update DDNS		On		
Virtual IP		On	LAN1	192.168.1.1
			LAN2	192.168.2.1
			LAN3	192.168.3.1
			LAN4	192.168.4.1
			LAN5	192.168.5.1
Enable Config Sync		On	**Config Sync Interval**	0 Day 0 Hour 15 Minute

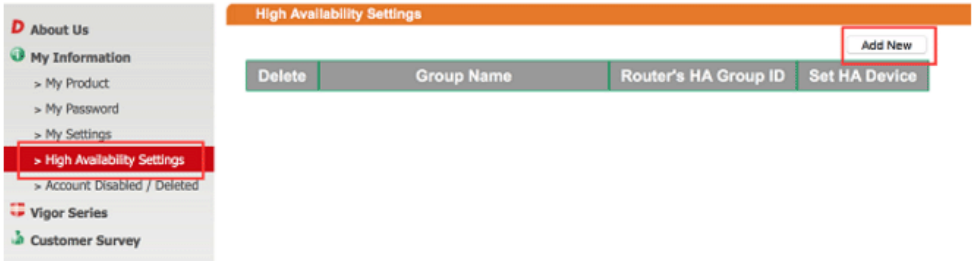
[Other Router]
Secondary

V2925_B				192.168.1.3
State	**Stable**	**WAN**	**Config Sync Status**	**Cached Time**
Secondary	Yes	All WANs Down !	Progressing	5 min up
MAC		00:1d:aa:be:92:60	**HTTPs Port**	4430
Model		Vigor2925Vn	**Firmware Version**	3.8.2
Enable High Availability		On	**Redundancy Method**	Hot-Standby
Group ID		1	**Priority ID**	10
Authentication Key		draytek	**Management Interface**	LAN1
Update DDNS		Off		
Virtual IP		On	LAN1	192.168.1.1
			LAN2	192.168.2.1
			LAN3	192.168.3.1
			LAN4	192.168.4.1
			LAN5	192.168.5.1
Enable Config Sync		On	**Config Sync Interval**	0 Day 0 Hour 15 Minute

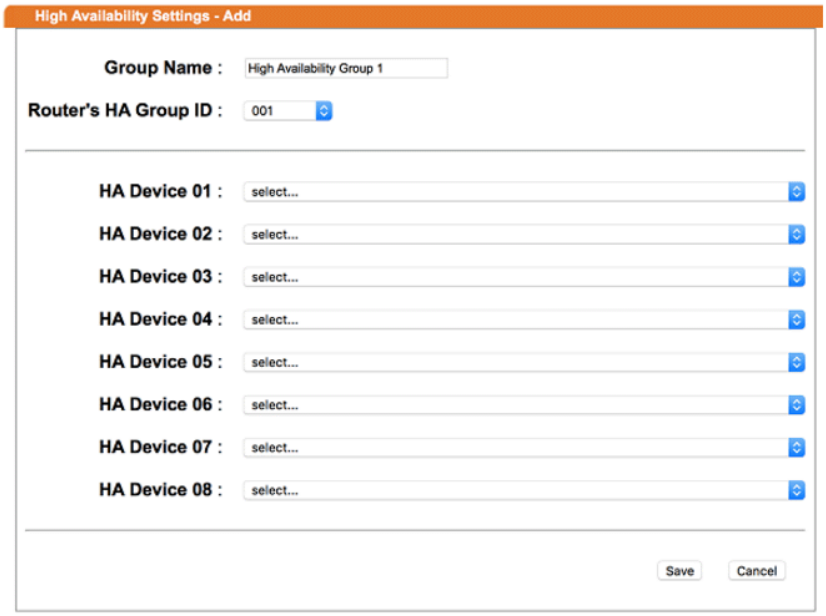
分享 WCF 授權書

11. 目前路由器已設定好，如果您擁有 WCF 授權書，您可以在 MyVigor 建立一個群組，讓這些路由器可以共享相同的授權書。

    (a) 首先，登入 myvigor.draytek.com，在右手邊找到高可靠度設定並按下新增(Add New)。

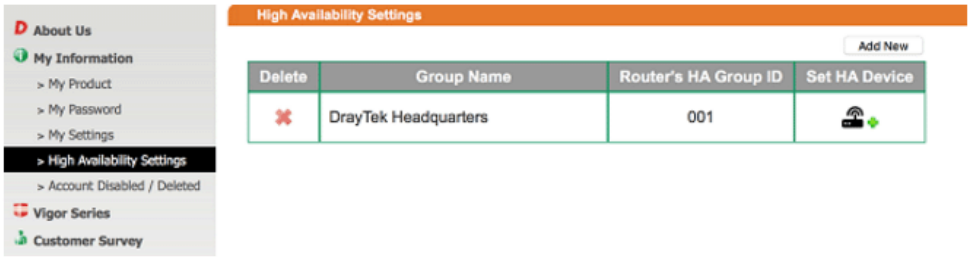


(b) 輸入群組名稱、選擇未使用的群組 ID 並從 HA 裝置下拉式清單中選擇會員路由器：



注意下拉式選單僅列出在 MyVigor 帳號下註冊的裝置，如果您未發現使用的路由器，請找出該裝置是註冊在哪個帳戶底下。

(c) 儲存設定檔，我們可以看見群組條目內容。



傳送通知至網路管理者

我們可以設定路由器在遇到如下事件時，可透過傳送電子郵件或是簡訊來通知網路管理者。

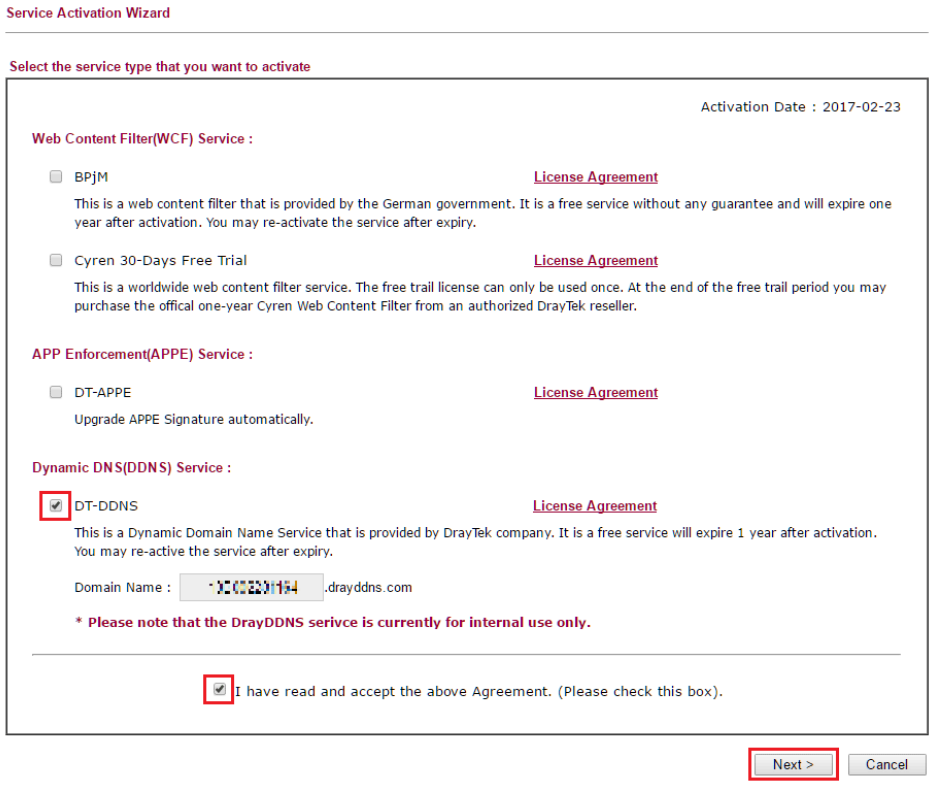
1. 故障發生：主要路由器的 WAN 斷線，次要路由器接管
2. 設定同步化失敗：主要與次要路由器之間的設定同步化失敗
3. 路由器不穩定：路由器的某一台變得不穩定

A-2 如何使用 DrayDDNS?

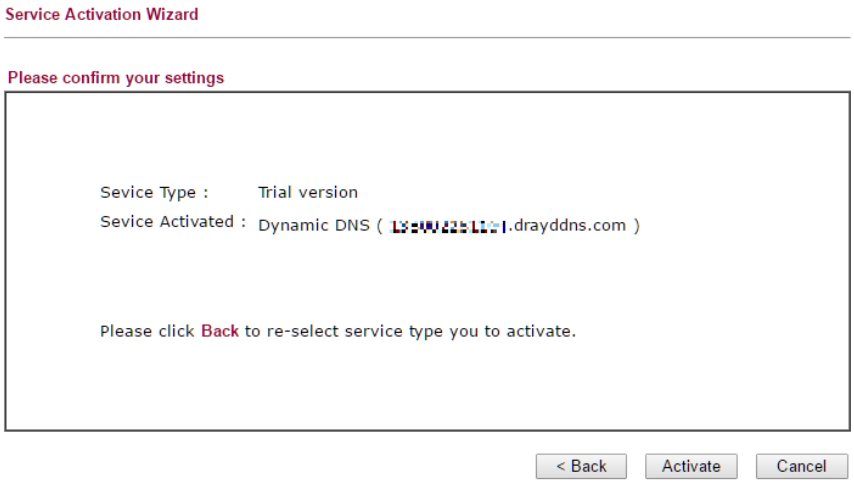
路由器支援不同的 DDNS 服務供應商，使用者可以設定使用者定義之設定檔來更新 DDNS，甚至該服務供應商不在清單上亦可處理。目前，居易開始支援自提的 DDNS 服務，稱爲 DrayDDNS，我們將針對每個居易路由器提供網域名稱，此個別的網域名稱可以記錄所有 WAN 介面的 IP 位址。

啟動 DrayDDNS 授權書

1. 開啓**設定精靈>>服務啓用設定精靈(Wizards >> Service Activation Wizard)**，等待路由器連線到 MyVigor 伺服器，然後勾選 **DT-DDNS** 與 **I have read and accept the above Agreement** 選框，接著按下一步**(Next)**。



2. 確認資訊，按下**啓動(Activate)**。



3. MyVigor 伺服器將回覆服務啓用資訊。

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Web Content filter	---	---	Not Activated
APP Enforcement	---	---	Not Activated
DDNS	2017-02-23	2018-02-23	DT-DDNS

Please check if the license fits with the service provider of your signature. To ensure normal operation for your router, update your signature again is recommended.

設定 DDNS 設定檔

1. 開啓**其他應用>>動態 DNS 設定(Applications >> Dynamic DNS Setup)**，

   a. 勾選**啓用動態 DNS 設定(Enable Dynamic DNS Setup)**

   b. 選擇可用的設定檔索引編號

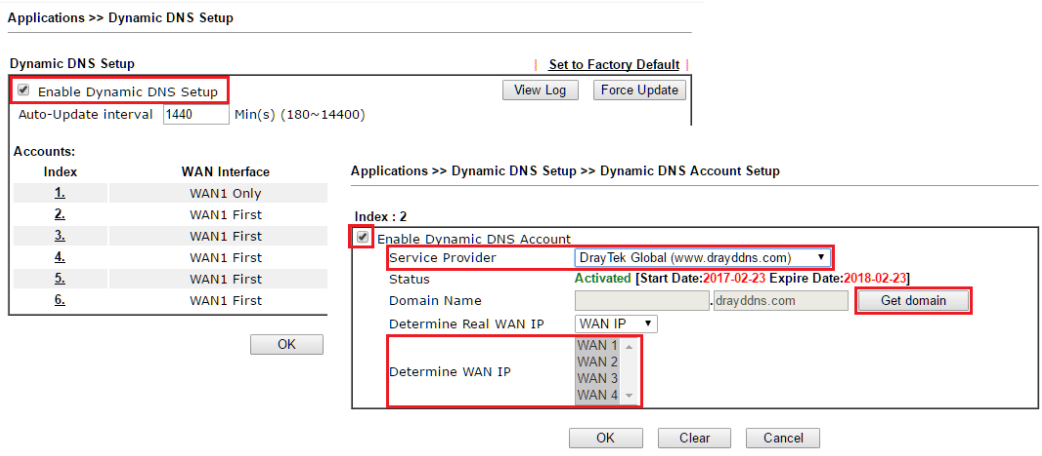
   c. 勾選**啓用動態 DNS 帳號(Enable Dynamic DNS Account)**

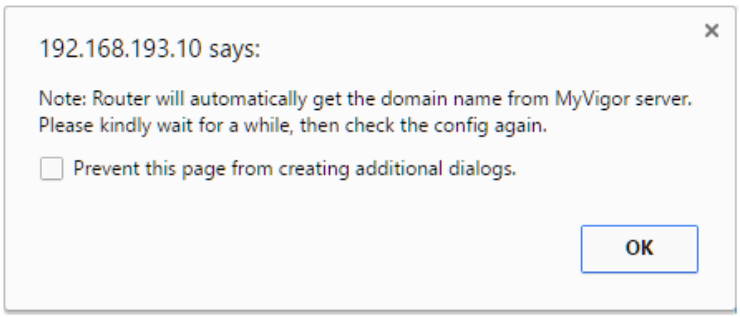
   d. 選擇 **DrayTek Global (www.drayddns.com)** 作爲**服務供應商(Service Provider)**

   e. 選擇想要的 WAN 介面以便上傳 IP 至 DDNS 伺服器

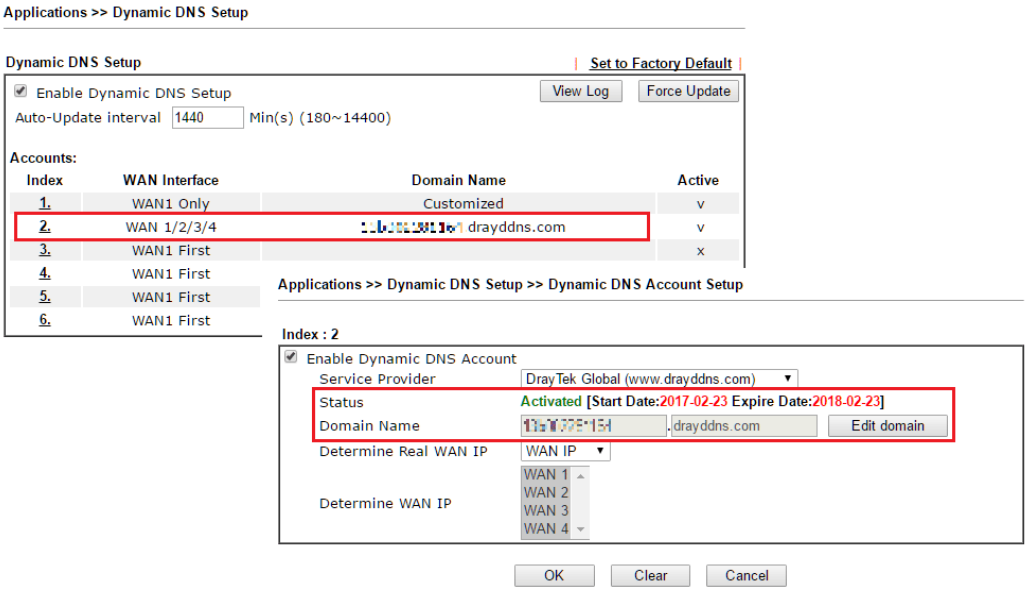
   f. 按下**取得網域(Get domain)**

   g. 在跳出的通知視窗上，按下**確定(OK)**





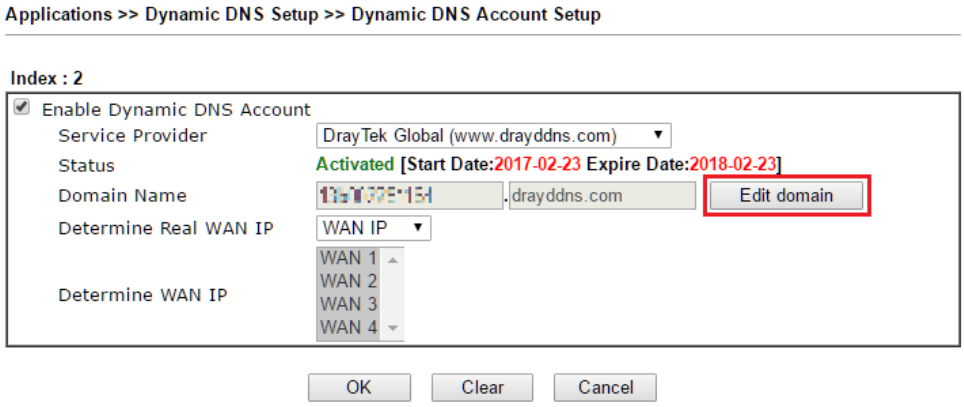
2. 等待數秒讓路由器取得網域名稱，接著我們可以選擇設定檔以便檢查授權書資訊以及網域名稱



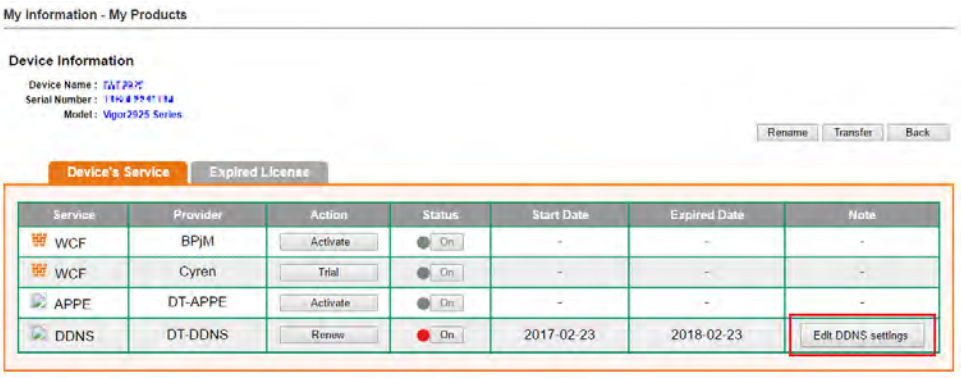
修改網域名稱

目前，只有網域名稱可以修改 MyVigor 網站，我們需要註冊路由器至 MyVigor 伺服器並且登入 MyVigor 網站修改名稱。

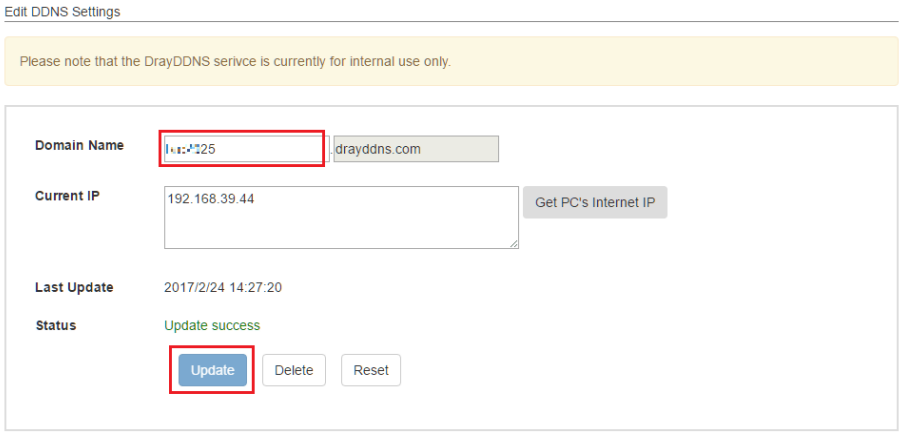
1. 請造訪 https://myvigor.draytek.com/ 或是**開啓其他應用>>動態 DNS 設定>>DrayDDNS 設定檔(Applications >> Dynamic DNS Setup >> DrayDDNS)**，再按下**編輯網域(Edit domain)**。



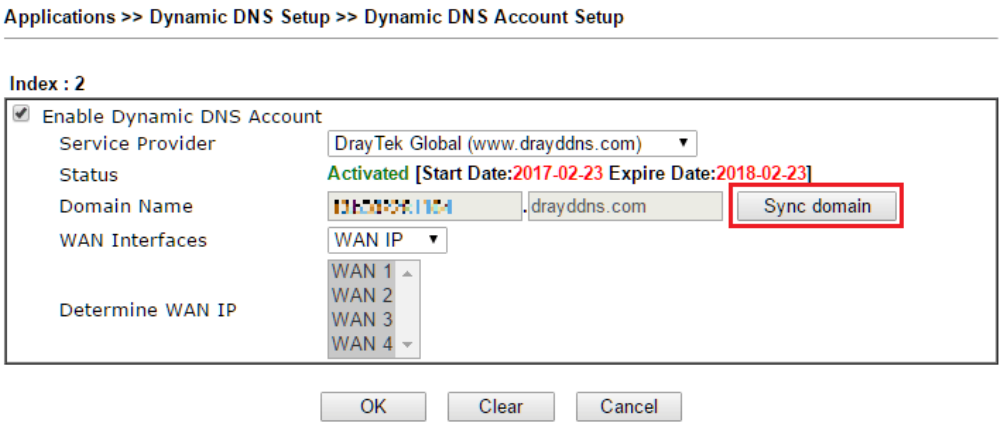
2. 登入 MyVigor 網站，選擇設定檔然後按下**編輯 DDNS 設定(Edit DDNS settings)**。



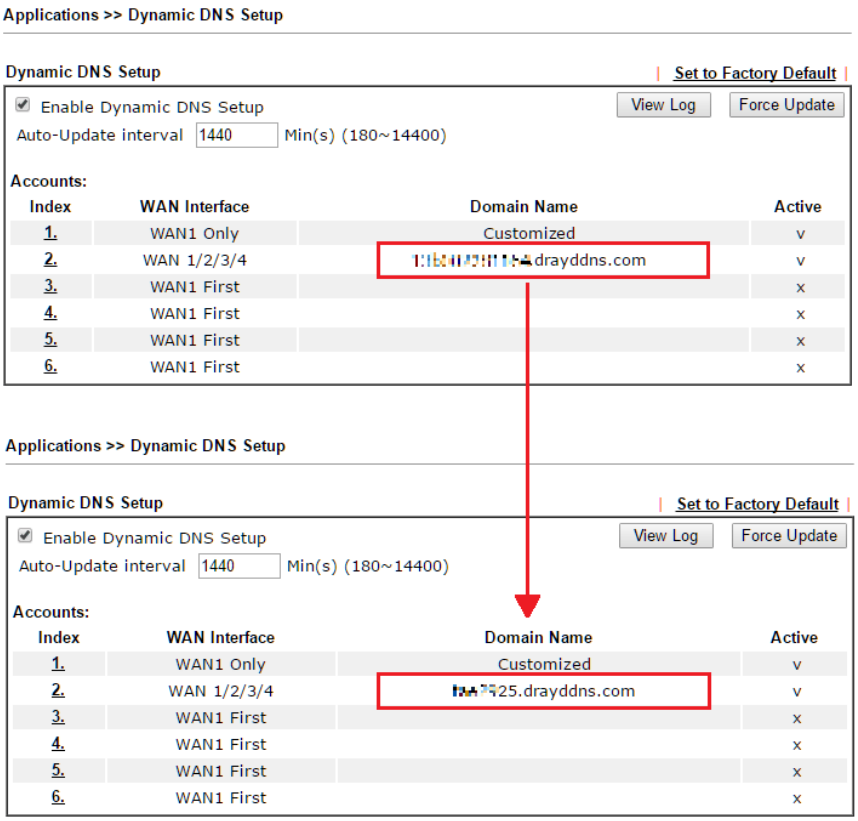
3. 輸入需要的網域名稱(例如 XXXX25)然後按下更新(**Update**)。



4. 當 Vigor 路由器執行下一個 DDNS 更新時，可以取得修正後的網域名稱，我們可以按下**同步網域(Sync domain)**加速處理流程。



數秒後，路由器將取得網域名稱並可顯示在設定檔清單上。


Applications >> Dynamic DNS Setup
Dynamic DNS Setup
Set to Factory Default
Enable Dynamic DNS Setup
View Log
Force Update
Auto-Update interval 1440 Min(s) (180~14400)
Accounts:
Index WAN Interface Domain Name Active
1. WAN1 Only Customized v
2. WAN 1/2/3/4 drayddns.com v
3. WAN1 First x
4. WAN1 First x
5. WAN1 First x
6. WAN1 First x
Applications >> Dynamic DNS Setup
Dynamic DNS Setup
Set to Factory Default
Enable Dynamic DNS Setup
View Log
Force Update
Auto-Update interval 1440 Min(s) (180~14400)
Accounts:
Index WAN Interface Domain Name Active
1. WAN1 Only Customized v
2. WAN 1/2/3/4 25.drayddns.com v
3. WAN1 First x
4. WAN1 First x
5. WAN1 First x
6. WAN1 First x

A-3 如何設定客製化 DDNS?

本文在說明如何在路由器上設定客製化 DDNS 以便更新您的 IP 位址至 DDNS 伺服器上，本文將舉“Changeip.org”與“3322.net”爲例，在設定之前，請確認 WAN 介面已正常連線。

A 部分: 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

請注意

Username: jo***

Password: jo********

Host name: j*****.changeip.org

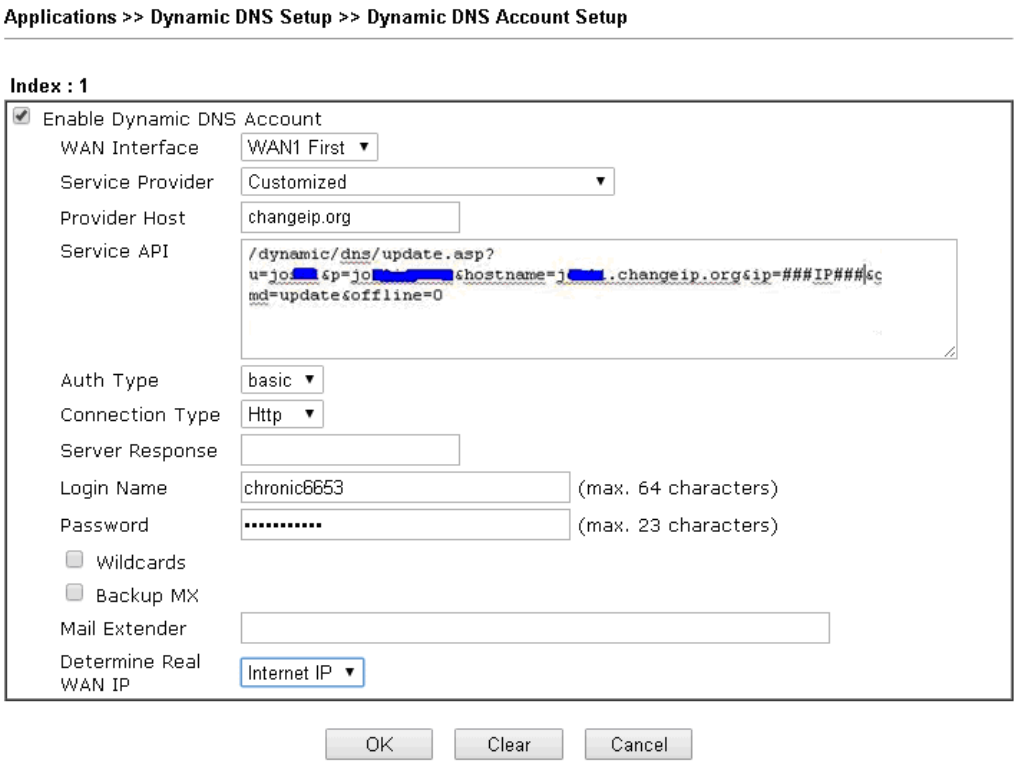
WAN IP address: 1.169.185.242

下圖是編輯瀏覽器上的 HTML 文字以更新 IP 位址至 DDNS 路由器的螢幕截圖



現在我們必須設定路由器讓其可以自動執行相同的工作。

1. 開啓**其他應用>>動態 DNS(Applications >> Dynamic DNS)** 以建立客製化 DDNS 用戶端之設定檔。



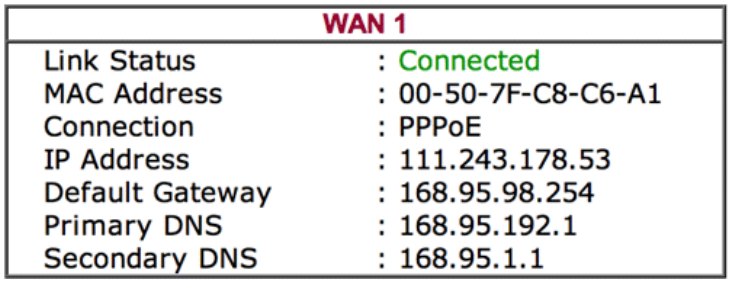
2. 設定服務供應商爲**客製化(Customized)**。

3. 設定服務 API 爲:
/dynamic/dns/update.asp?u=jo***&p=jo********&hostname=j****.changeip.org&ip=###IP### &cmd=update&offline=0

其中，當 DDNS 服務運作時，###IP### 是將來以當下的介面 IP 位址替換的內容，本例 IP 位址爲 1.169.185.242

4. 設定完後，客製化 DDNS 服務即可啓動上線，IP 位址也會更新至 DDNS 伺服器上。

B 部分: 3322.net



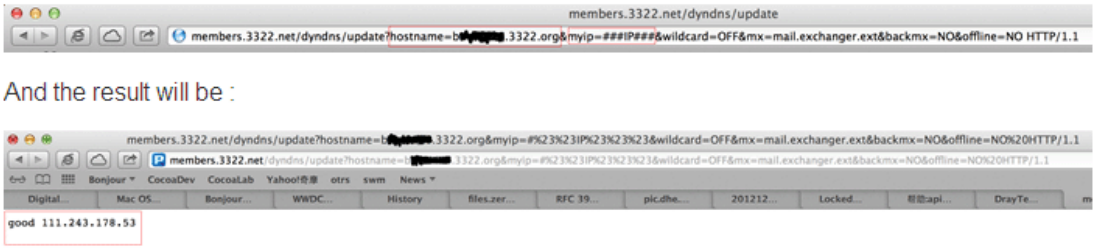
Username: bi*******

Password: 88********

Host name: bi*******.3322.org

WAN IP address: 111.243.178.53

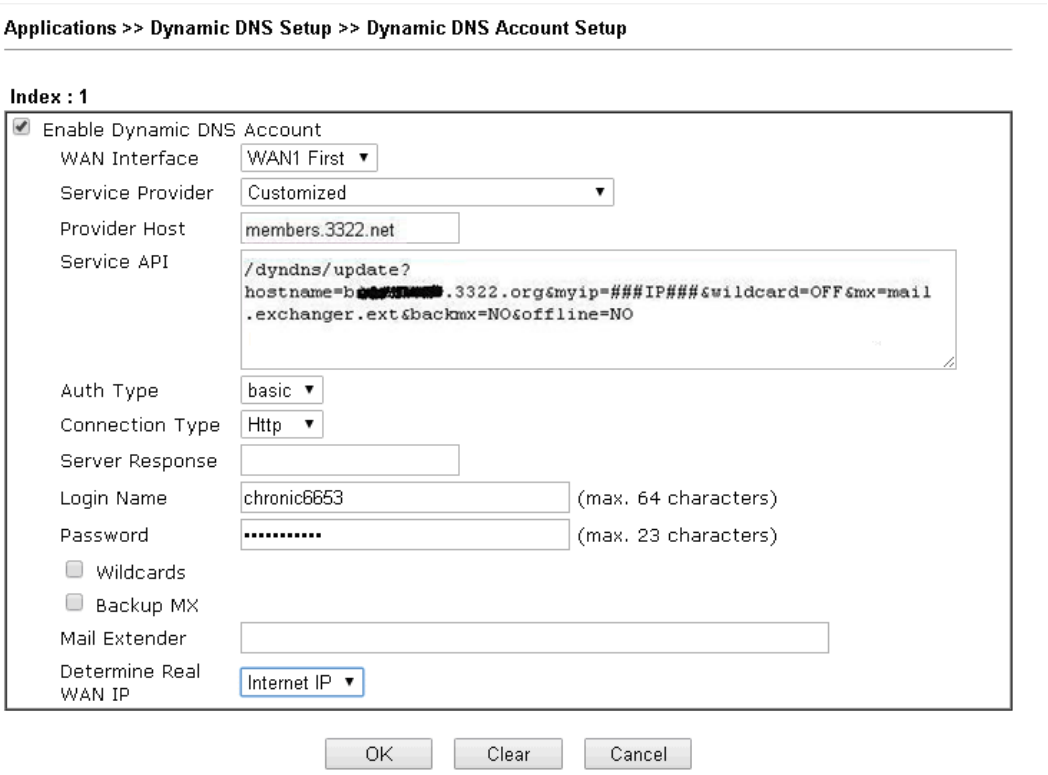
欲透過編輯 HTML 文字更新 IP 至 DDNS 伺服器，我們可以在瀏覽器上輸入如下的內容：



“good 111.243.178.53”表示我們的 IP 位址已經成功更新至伺服器上了。

現在，我們必須設定路由器讓其可以自動執行相同的工作。

1. 開啓**其他應用>>動態 DNS(Applications >> Dynamic DNS)** 以建立客製化 DDNS 用戶端之設定檔。



2. 設定服務供應商爲**客製化(Customized)**。

3. 設定服務供應商主機爲 **member.3322.net**。

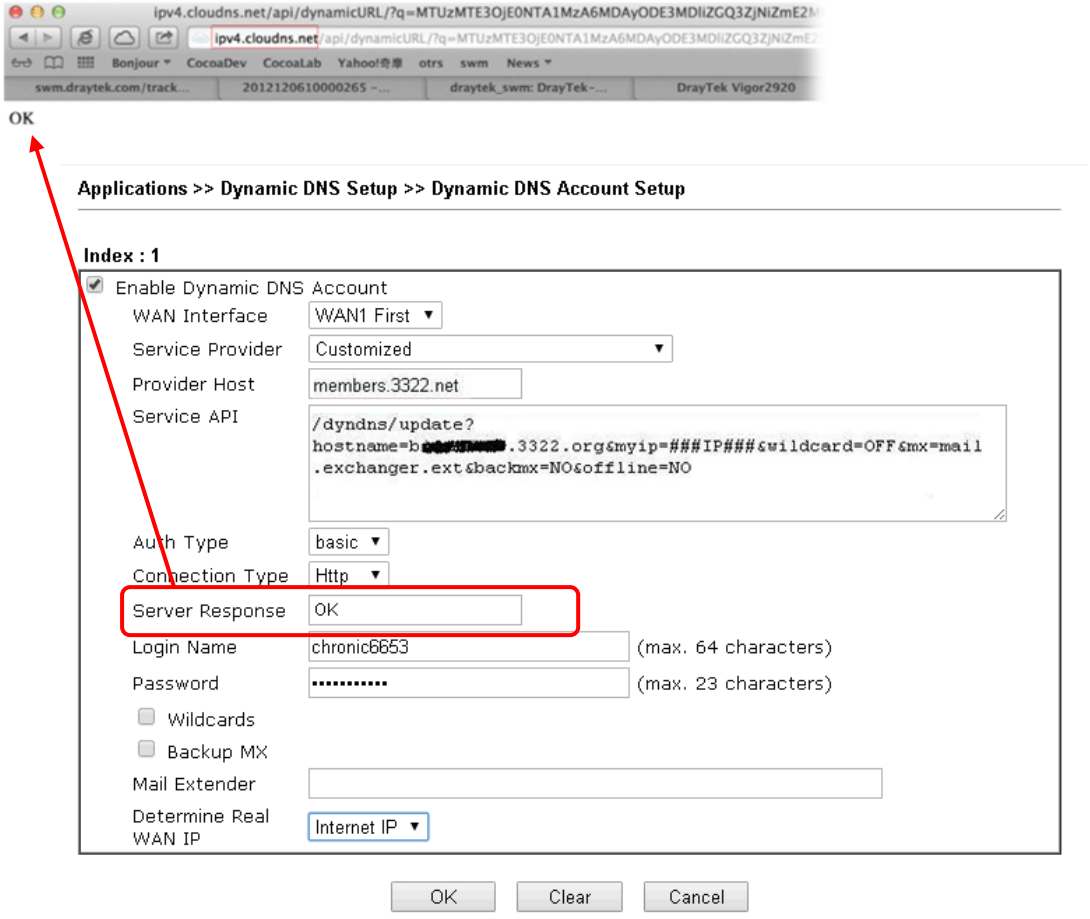
4. 設定服務 API 爲:
/dyndns/update?hostname=yourhost.3322.org&myip=###IP###&wildcard=OFF&mx=mail.exchanger.ext&backmx=NO&offline=NO

5. 輸入帳號與密碼。

6. 設定完後，客製化 DDNS 服務即可啓動上線，IP 位址也會更新至 DDNS 伺服器上。

C 部分: Extend Note

客製化服務供應商也能使用 ClouDNS.net。



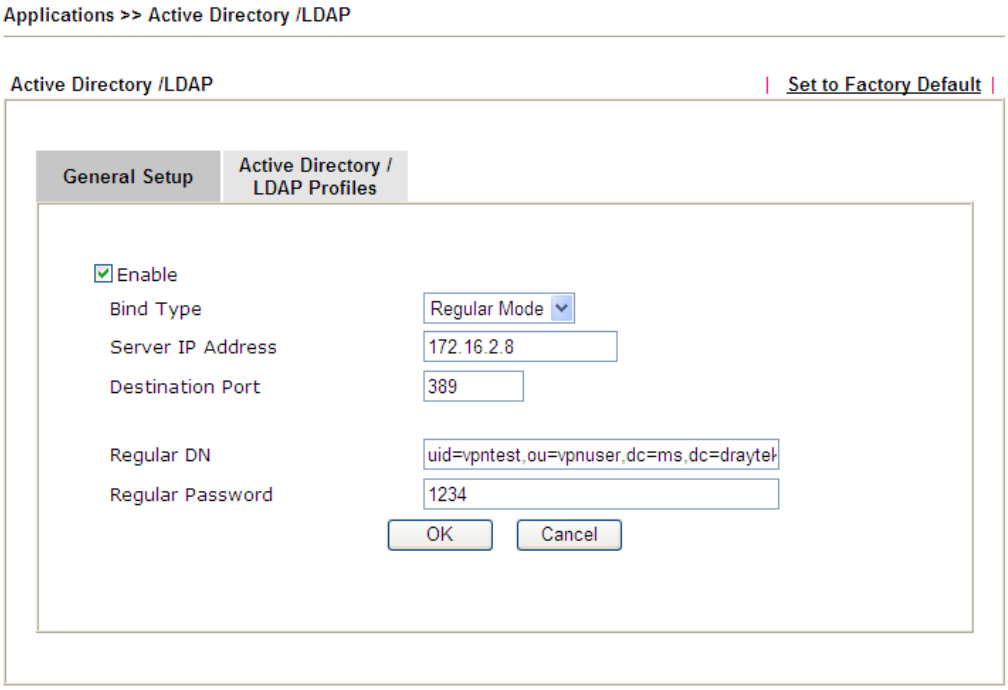
A-4 如何實施 LDAP/AD 驗證以應使用者管理?

爲了簡化 LDAP 驗證設定以利進行使用者登入管理，我們可以實施群組功能來達成目的。

無須針對路由器上的每個使用者，事先設定使用者設定檔，我們只要設定群組 DN，那麼路由器(例如本系列)就可以事先設定的群組路徑通過 LDAP 伺服器的驗證。

下圖顯示設定步驟：

1. 登入路由器的使用者設定介面。
2. 進入**其他應用>> Active Directory /LDAP (Applications>>Active Directory /LDAP)** 開啓下述頁面以利配置 LDAP 相關設定。

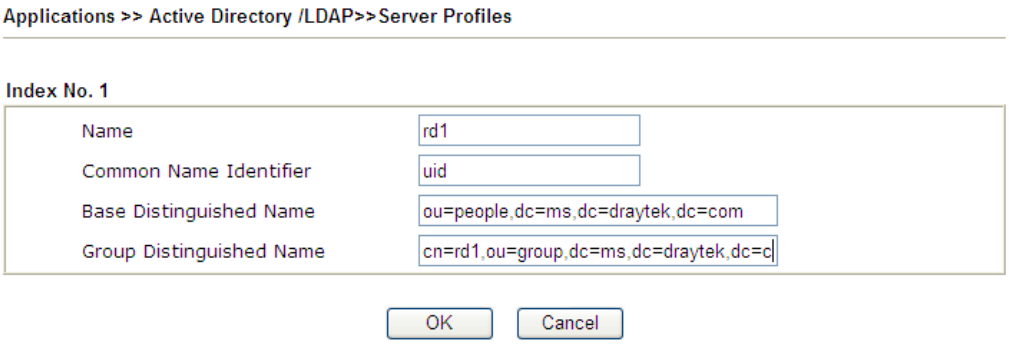


系統支援三種綁定類型：

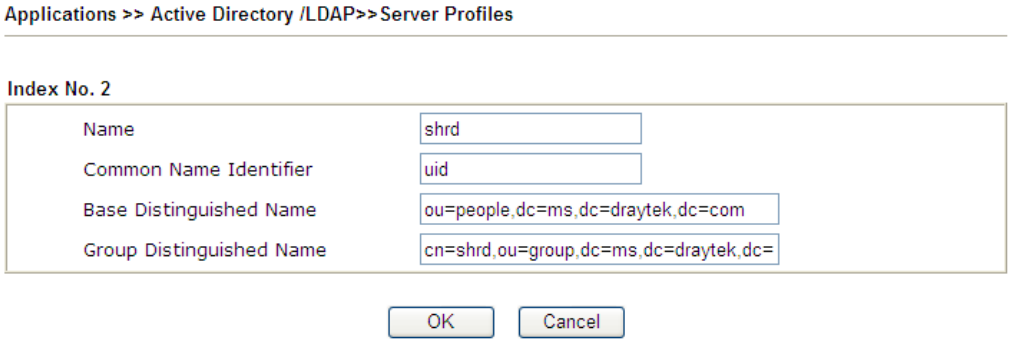
- **簡單模式(Simple Mode)** – 不需搜尋，只要進行綁定驗證即可
- **匿名(Anonymous)** – 先以匿名帳號執行搜尋動作，然後進行綁定驗證
- **常規模式(Regular Mode)**– 大部分與匿名模式相同，不同的地方在於伺服器會先檢查您是否有搜尋的權限。針對常規模式，您需要輸入常規 DN 與常規密碼(**Regular DN** and **Regular Password)**

3. 建立 LDAP 伺服器設定檔，按下 **Active Directory /LDAP** 標籤開啓設定檔網頁，按下任一個索引編號連結。

   如果在 LDAP 伺服器上我們有二個群組“**RD1**”與“**SHRD**”，我們可以將此 LDAP 伺服器設定檔給予不同的群組識別名稱(Group Distinguished Name)。

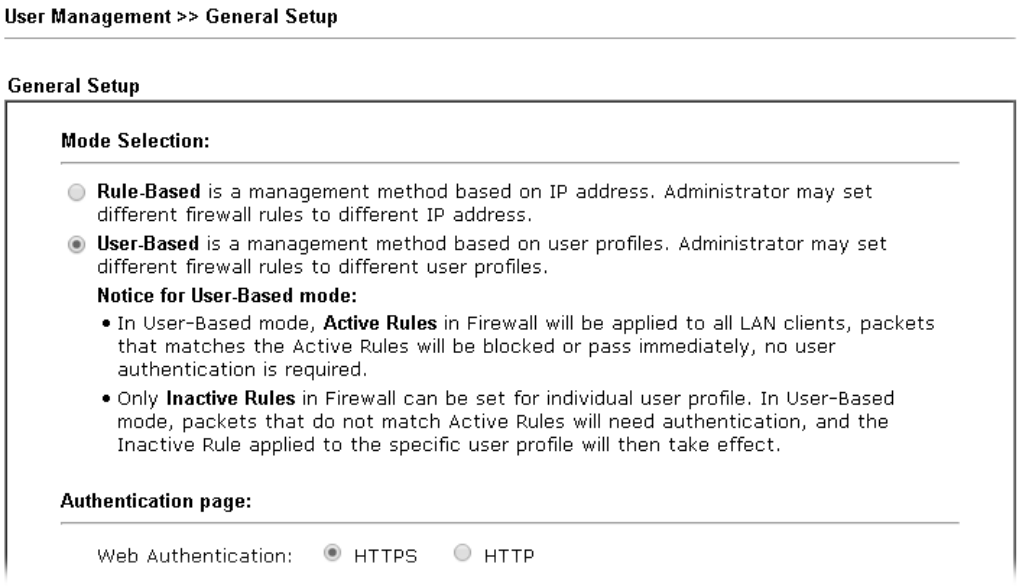


以及

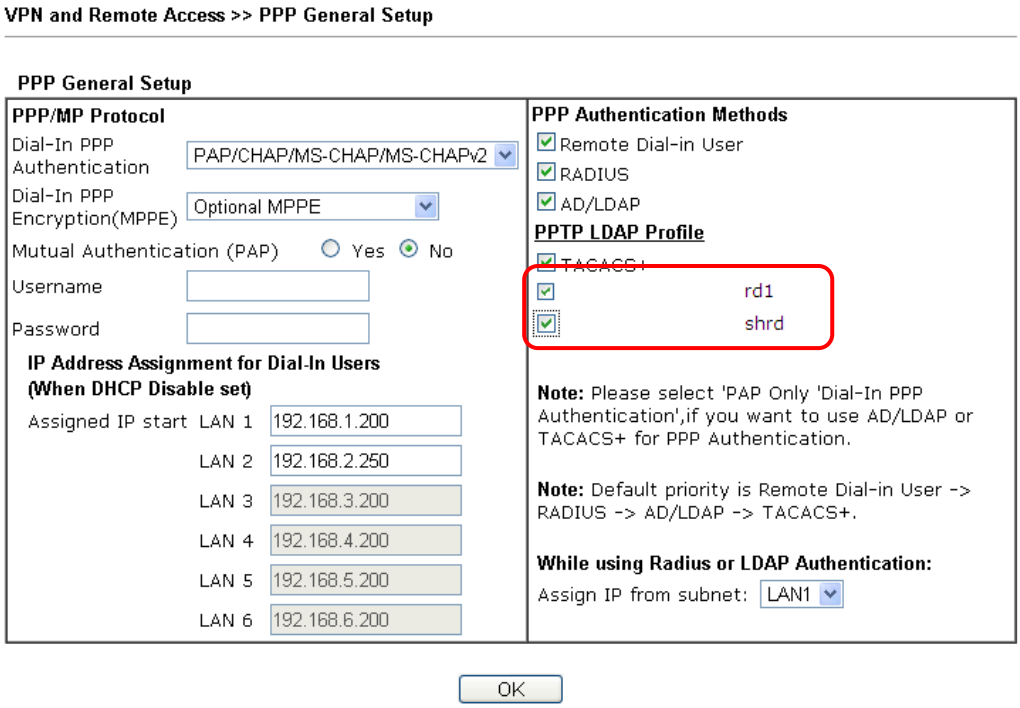


4. 按下**確定(OK)** 儲存上述設定。

5. 開啓**使用者管理>>基本設定(User Management>>General Setup)**，選擇**使用者模式(User-Based)**。



6. 接著開啓 **VPN 與遠端存取>>PPP 基本設定(VPN and Remote Access>>PPP General Setup)** 以勾選準備利用 LDAP 伺服器驗證的設定檔。



完成上述設定之後，在 LDAP 伺服器上輸入證書相關資訊後，屬於“rd1”或是“shrd”群組的使用者就可以存取網際網路。

II-6 路由(Routing)

策略路由(又稱爲 PBR，策略式路由) 功能允許您設定事先規則或是策略供後續使用，如果有某個封包符合任何一條策略的定義，該封包將會被導入指定的介面中。您可以爲了因應負載平衡、網路安全性、路由方針等各種不同的理由來設定策略。

透過通訊協定、IP 位址、埠號與介面設定，策略路由可以用來配置任何路由規則來符合實際的需要。一般來說，策略路由可以輕易達到如下的目的：

負載平衡(Load Balance)

您可以手動建立各種策略來平衡通過網路介面上的資訊流量。

指定介面

透過指定介面(WAN/LAN/VPN)，資料可以從來源 IP 傳送到目的 IP。

位址對應(Address Mapping)

允許您針對內部虛擬 IP 位址或是一定範圍的虛擬 IP 位址，指定對外 WAN IP 位址。

優先權

依據固定路由與策略路由的優先權設定，路由器可決定採用哪種策略來傳輸封包。

故障轉移/故障恢復(Failover to/Failback)

當原始介面斷線時(故障)，封包將透過其他介面或是依循策略規則傳送出去。一旦原始介面恢復運作(故障恢復)了，封包也會立刻回到原始介面傳輸。

其他路由

指定路由策略來決定資料傳輸的方向。

資訊	有關策略路由的詳細資訊，可以參考居易官網 www.draytek.com 的技術支援部份。

網頁使用者介面

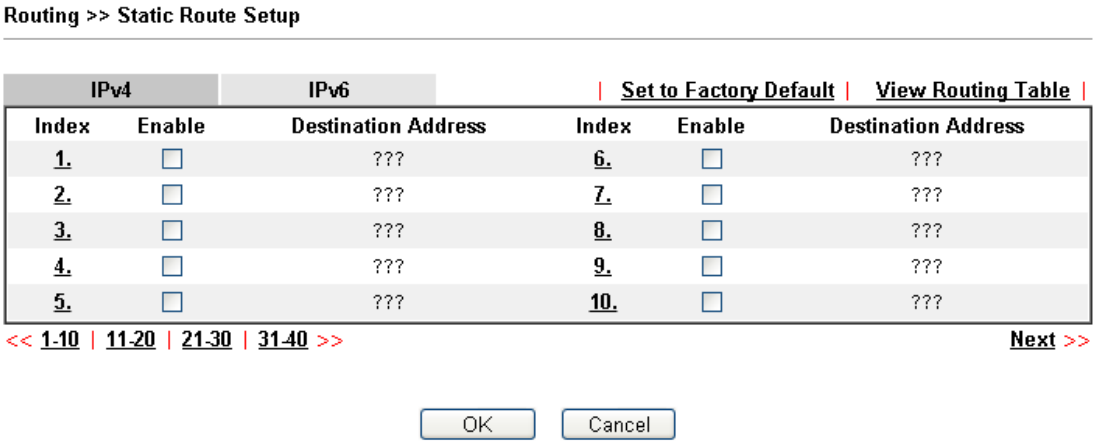


II-6-1 固定路由(Static Route)

固定路由是動態路由的另一種選擇，它是系統網路管理者透過設定路由器的必要資訊以利封包轉送的一種過程，

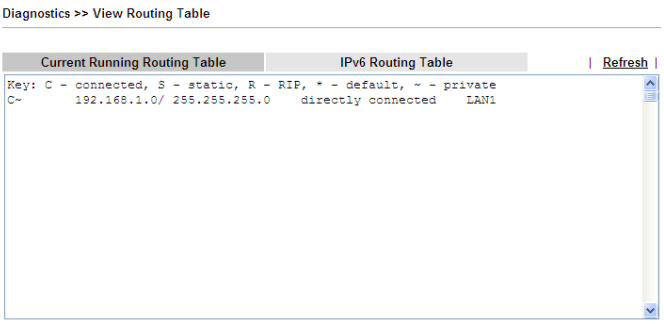
開啓**路由>>固定路由(Routing >> Static Route)**，路由器提供 IPv4 與 IPv6 頁面設定固定路由，二種協定會帶來不同的網頁設定內容。

固定路由(IPv4)



可用設定說明如下：

項目	說明
索引編號(Index)	索引編號下的號碼(1 到 40)可讓您開啓次頁面設定固定路由。
啓用(Enable)	勾選此框啓用此固定路由設定檔。
目的位址(Destination Address)	顯示固定路由的目的位址。
回復出廠預設值(Set to Factory Default)	清除所有設定並回到出廠的設定狀態。

檢視路由表(Viewing Routing Table)	開啓畫面檢視目前的路由狀況。 

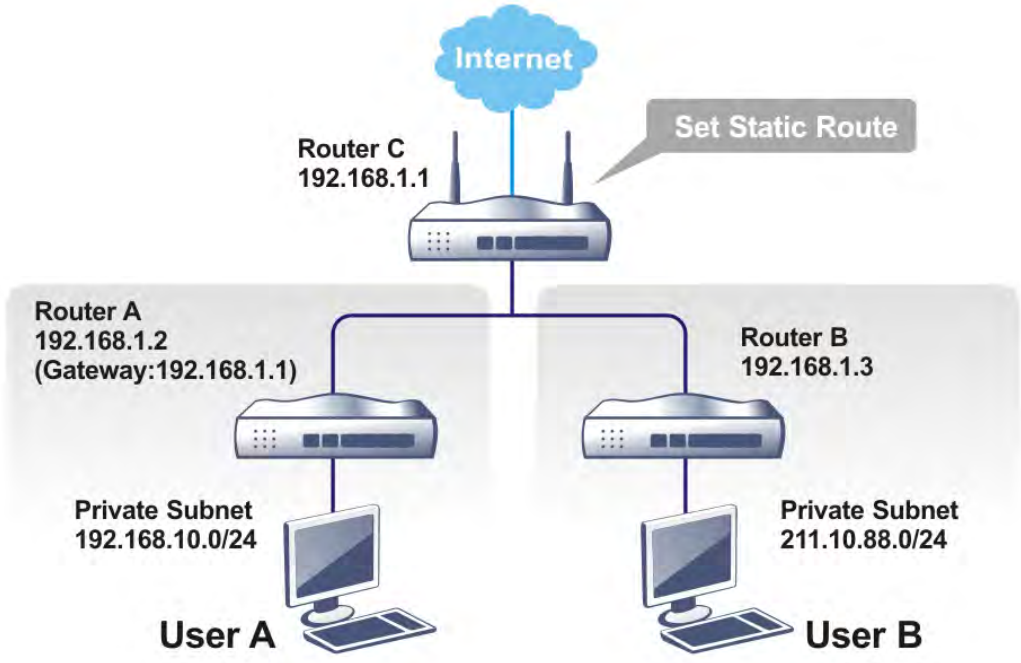
當您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

增加固定路由至虛擬或真實網路上(以 IPv4 為基準)

此處爲固定路由的範例，不同子網路上的使用者 A 與 B 可以透過路由器彼此溝通。假定網際網路的存取已設定完畢，路由器可以適當的運作。

- 使用主要路由器進入網際網路
- 利用內部的路由器 A(192.168.1.2)，建立虛擬子網路 192.168.10.0
- 透過內部的路由器 B(192.168.1.3)，建立真實子網路 211.100.88.0
- 已設定主要路由器 192.168.1.1 爲路由器 A (192.168.1.2) 的預設閘道

在設定固定路由之前，使用者 A 無法與使用者 B 溝通，因爲路由器 A 只會傳送辨認出的封包至主要路由器的預設閘道。

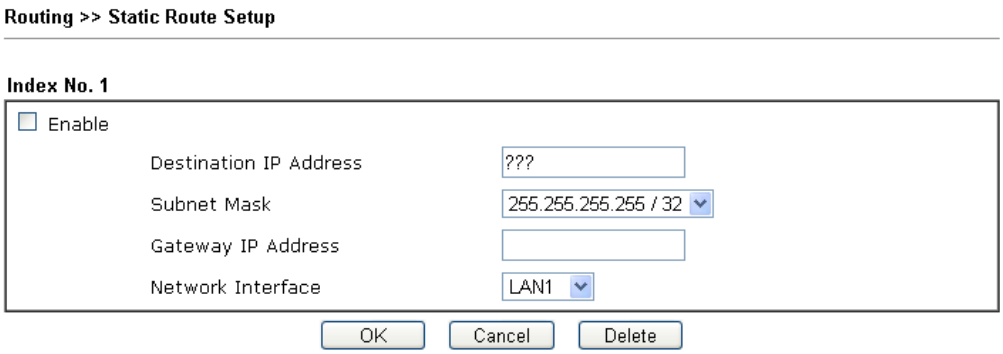


1. 在**區域網路(LAN)**群組中，選擇**一般設定(General Setup)**。再選擇第一子網路作爲 **RIP 協定控制**，然後點選**確定(OK)**按鈕。

資訊

有二個理由讓我們一定要在第一子網路上應用 RIP 通訊協定。第一個理由是區域網路介面可以透過第一子網路(192.168.1.0/24)與鄰近路由器作 RIP 封包交換，第二個，理由是網際網路虛擬子網路上(例如 192.168.10.0/24)的主機群可以藉此路由器存取網際網路資訊，並和不同子網路持續進行 IP 路由資訊交換。

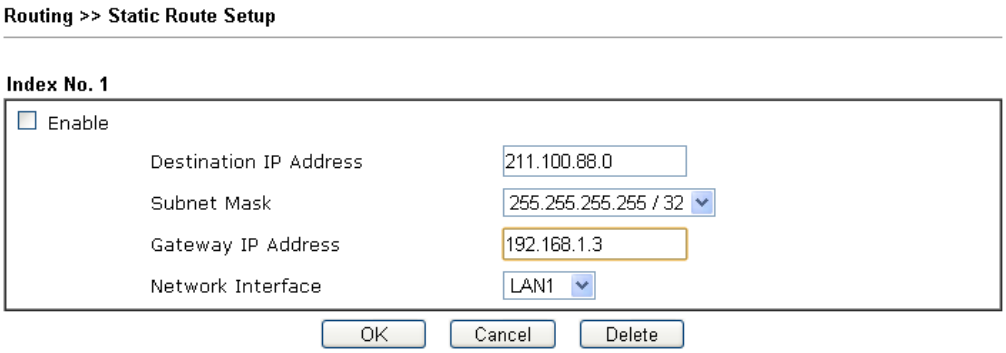
2. 在**路由>>固定路由(Routing >> Static Route)**，按索引編號 1 勾選**啓用(Enable)**方塊， 請以下列數字新增一個固定路由，讓所有應前往 192.168.10.0 的封包都能透過 192.168.1.2 來轉送，接著按**確定(OK)**。



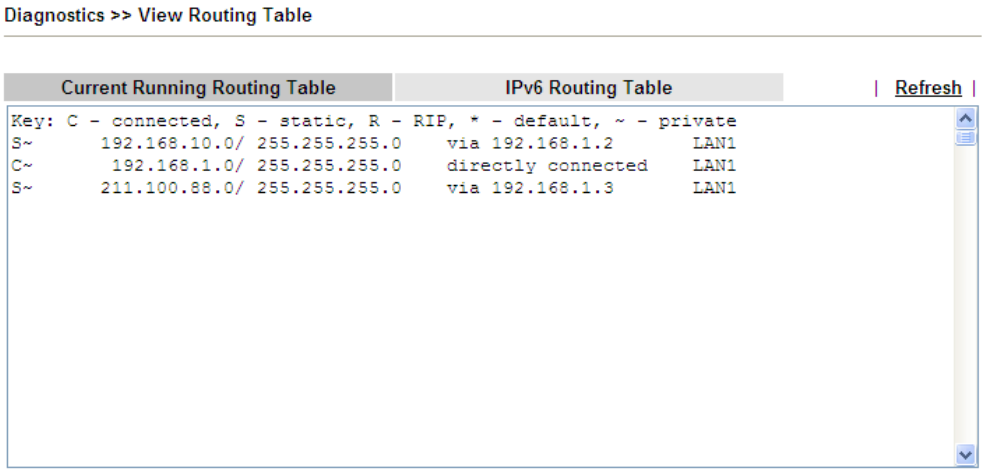
可用設定說明如下：

項目	說明
啓用(Enable)	勾選此框啓用此設定檔。
目的 IP 位址 (Destination IP Address)	輸入 IP 位址做爲固定路由的目的地。
子網遮罩(Subnet Mask)	輸入此固定路由的子網遮罩。
網路介面(Network Interface)	使用下拉式清單指定此固定路由的介面。

3. 回到**固定路由設定(Static Route Setup)**頁面，按另一個索引編號增加另一個固定路由，設定如下圖。它可將所有指定前往 211.100.88.0 的封包轉送至 192.168.1.3，然後按**確定(OK)**。

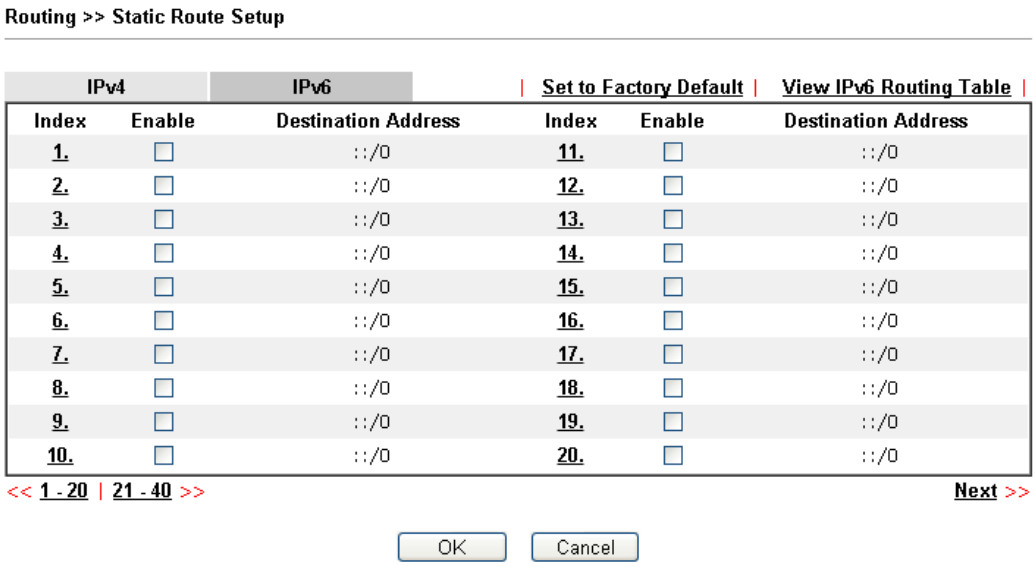


4. 按**自我診斷工具(Diagnostics)**中的**路由表(Routing Table)**檢查目前的路由表格。



固定路由(IPv6)

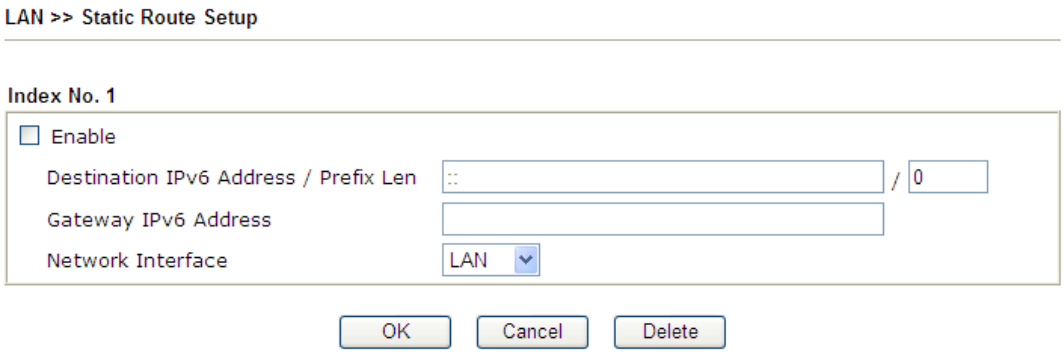
可以設定 40 組 IPv6 固定路由，按下 IPv6 標籤開啓設定頁面。



可用設定說明如下：

項目	說明
索引編號(Index)	索引編號下的號碼(1 到 40)可讓您開啓次頁面設定固定路由。
啓用(Enable)	勾選此框啓用此固定路由設定檔。
目的位址(Destination Address)	顯示固定路由的目的位址。
狀態(Status)	顯示固定路由的狀態。
回復出廠預設值(Set to Factory Default)	清除所有設定並回到出廠的設定狀態。
檢視 IPv6 路由表(Viewing IPv6Routing Table)	開啓畫面檢視目前的路由狀況。

按下任一索引編號連結開啓如下頁面。



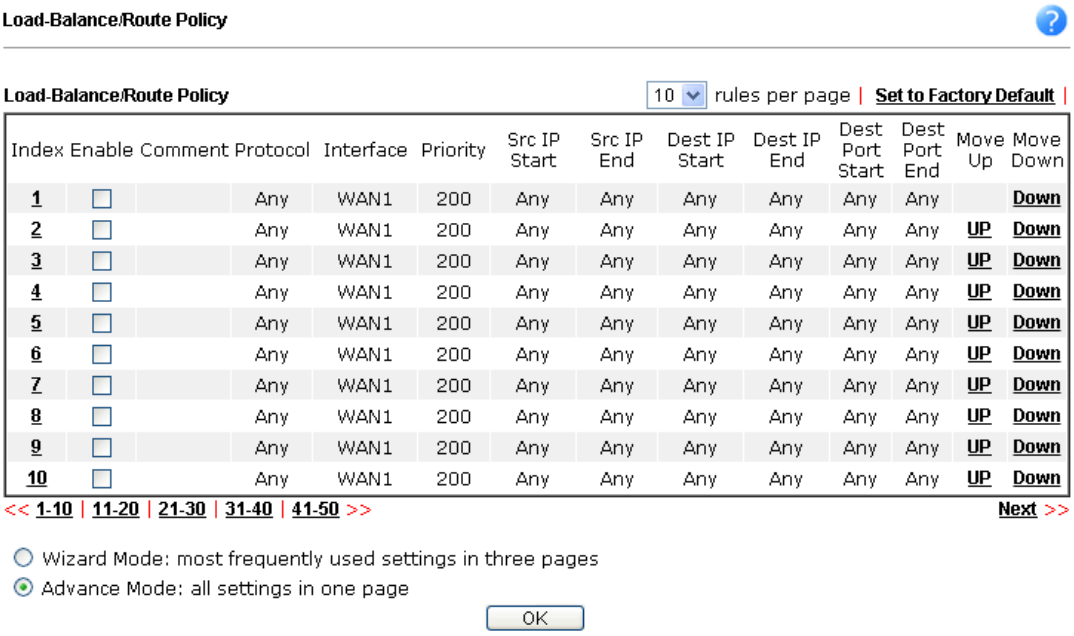
可用設定說明如下：

項目	說明
啓用(Enable)	按此啓用此設定檔。
目的 IPv6 位址/前置碼長度 (Destination IPv6 Address / Prefix Len)	輸入此設定檔的 IPv6 位址以及前置碼長度。
閘道 IPv6 位址(Gateway IPv6 Address)	輸入此設定檔的閘道位址。
網路介面(Network Interface)	使用下拉式清單指定此固定路由的介面。

當您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

II-6-2 負載平衡/策略路由(Load-Balance /Route Policy)

II-6-2-1 基本設定(General Setup)

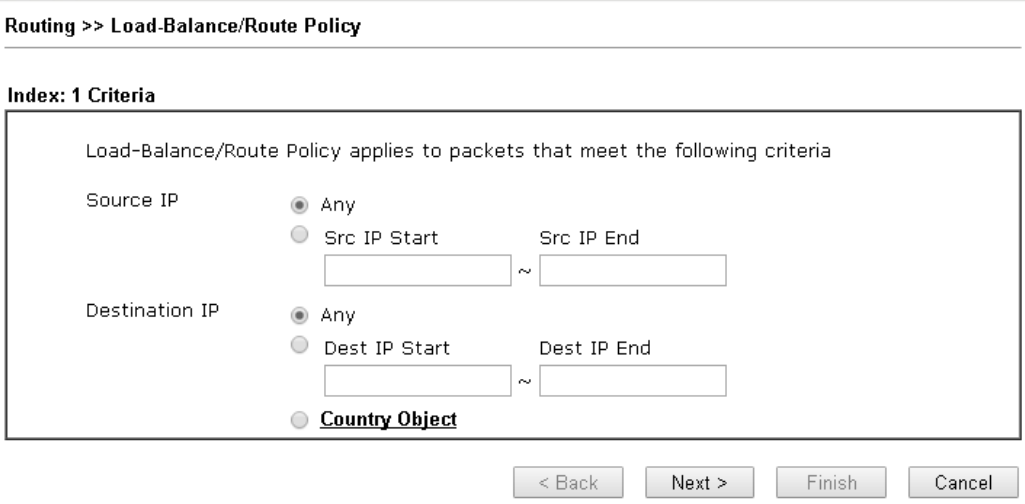


可用設定說明如下：

項目	說明
索引編號(Index)	點下號碼連結即可進入設定頁面。
啓用(Enable)	勾選此方框啓用此策略設定檔。
協定(Protocol)	顯示用於此路由策略設定檔的協定內容。
介面(Interface)	顯示此路由策略設定檔指定的封包傳送的介面。
優先權(Priority)	顯示此路由策略設定檔的優先權數值。
來源 IP 起點(Src IP Start)	顯示來源 IP 的起始 IP 位址。
來源 IP 終點(Src IP End)	顯示來源 IP 的結束 IP 位址。
目標 IP 起點(Dest IP Start)	顯示目標 IP 的起始 IP 位址。
目標 IP 終點(Dest IP End)	顯示目標 IP 的結束 IP 位址。
目標埠號起點(Dest Port Start)	顯示目標埠號的起始埠號。
目標埠號終點(Dest Port End)	顯示目標埠號的結束埠號。
上移/下移(Move UP/Move Down)	使用上移下移連結來移動策略路由的順序。
設定精靈模式(Wizard Mode)	允許透過三個頁面進行策略路由的常用設定。
進階模式(Advance Mode)	允許設定策略路由的細部設定。

欲使用設定精靈模式，參考如下的設定步驟：

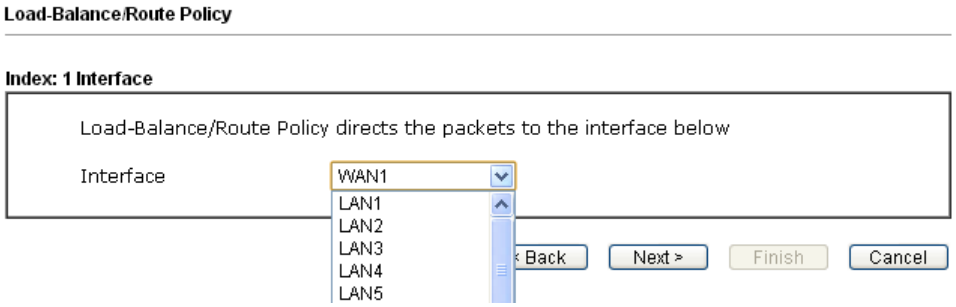
1. 按下**設定精靈模式(Wizard Mode)** 按鈕。
2. 點選**索引編號 1(Index 1)**連結，開啓如下頁面。



可用設定說明如下：

項目	說明
來源 IP(Source IP)	**任何(Any)** – 任何一個 IP 位址皆可視爲來源 IP。 **來源 IP 起點(Src IP Start) -** 輸入指定 WAN 介面的來源 IP 起始位址。 **來源 IP 終點(Src IP End) -** 輸入指定 WAN 介面的來源 IP 結束位址，如果此區留白，即表示所有區域網路內的來源 IP 皆可通過此 WAN 介面。
目標 IP(Destination IP)	**任何(Any)** – 任何一個 IP 位址皆可視爲目標 IP。 **目標 IP 起點(Dest IP Start)-** 輸入指定 WAN 介面的目標 IP 起始位址。 **目標 IP 終點(Dest IP End) -** 輸入指定 WAN 介面的目標 IP 結束位址，如果此區留白，即表示所有區域網路內的來源 IP 皆可通過此 WAN 介面。 **國家物件(Country Object)** – 指定一個國家物件，所有來自該國家的 IP 都可通過此 WAN 介面。

3. 按下**一步(Next)** 開啓下述頁面。

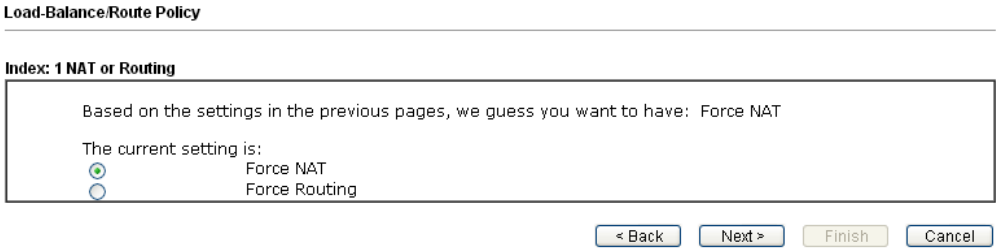


可用設定說明如下：

項目	說明

介面(Interface)	使用下拉式清單選擇一個 WAN 或是 LAN 介面或是 VPN 設定檔，符合此規定的封包就會透過此介面進行傳輸。

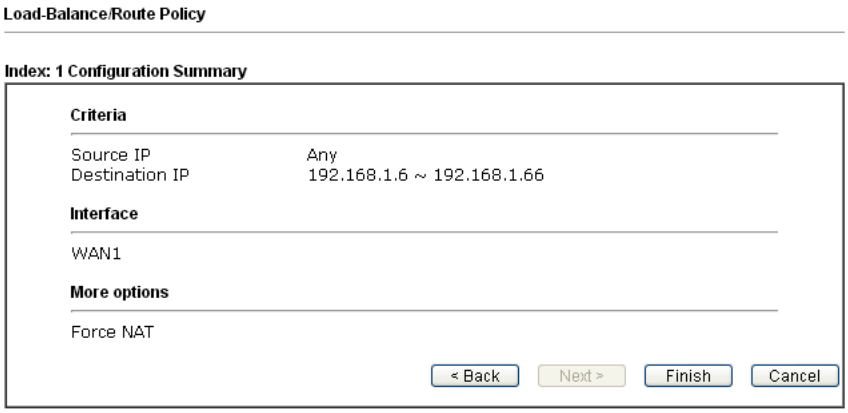
4. 指定完介面後，按**下一步(Next)** 進入次一個設定頁面。



可用設定說明如下：

項目	說明
強迫 NAT/強迫路由 (Force NAT /Force Routing)	決定路由器可以使用的機制來轉送 WAN 端的封包。

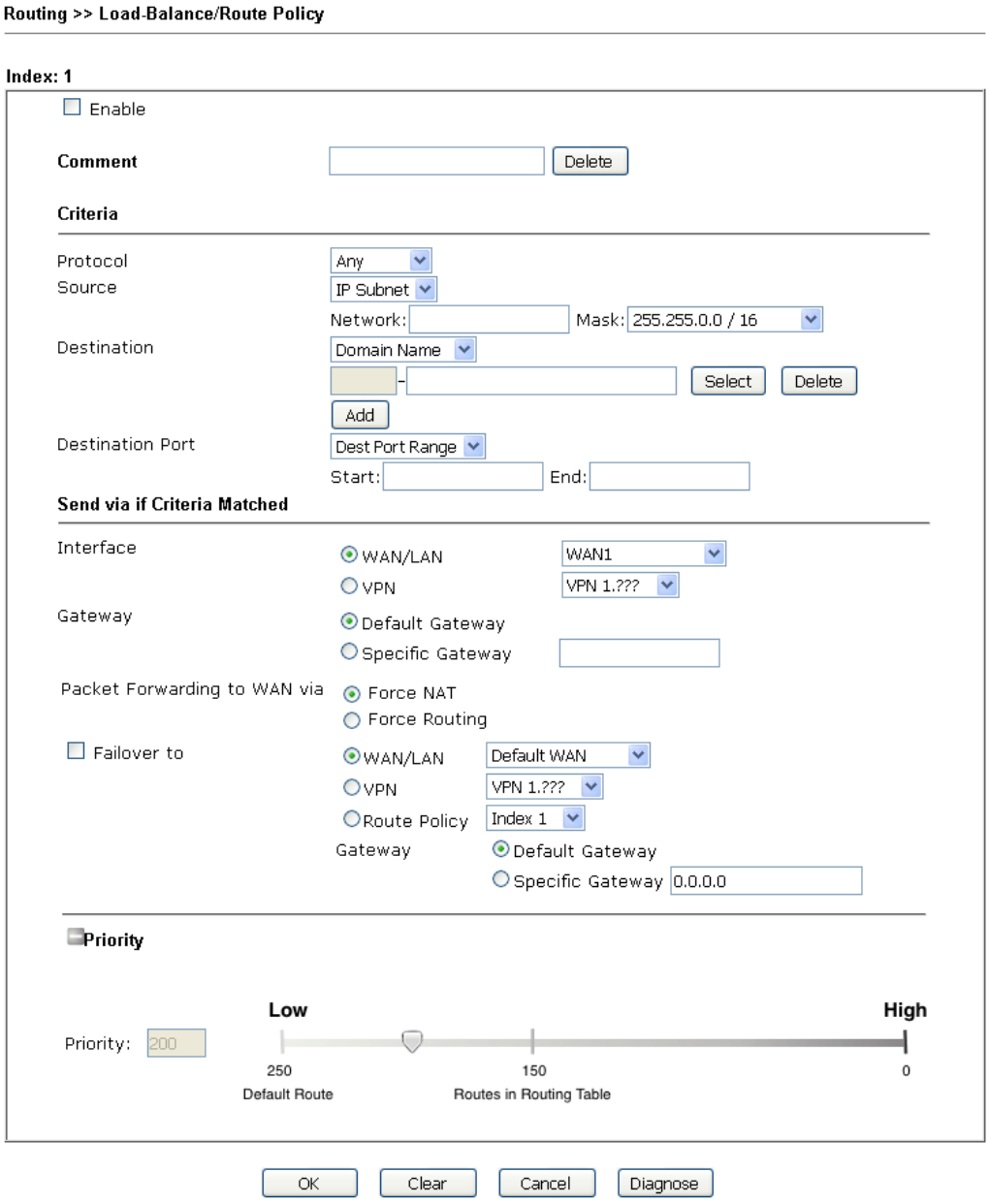
5. 機制選擇完畢之後，按**下一步(Next)** 查看設定總結內容。



6. 若無任何錯誤，請按**完成(Finish)** 結束設定精靈。

使用進階模式，參考如下的設定步驟：

1. 按下**進階模式(Advance Mode)** 按鈕。
2. 點選**索引編號 1(Index 1)**連結，開啓如下頁面。



Note:
Force NAT(Routing): NAT(Routing) will be performed on outgoing packets, regardless of which type of subnet (NAT or IP Routing) they originate from.

可用設定說明如下：

項目	說明
啓用(Enable)	勾選此框啓用此策略設定檔。
註解(Comment)	輸入與此設定檔有關的簡易說明。
通訊協定(Protocol)	使用下拉式清單選擇一個 WAN 或是 LAN 介面或是 VPN 設定檔，符合此規定的封包就會透過此介面進行傳輸。

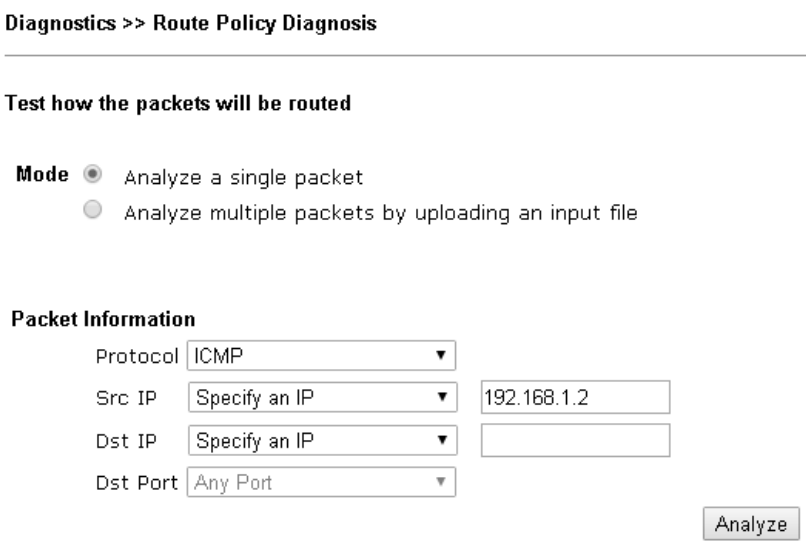
來源(Source)	**任何(Any)** – 任何一個 IP 位址皆可視爲來源 IP 位址。 **IP 範圍(IP Range)** – 定義一段 IP 範圍作爲來源 IP 位址。 ● **起點(Start) -** 輸入一個 IP 位址作爲此設定檔的來源 IP 的起始位址。 ● **終點(End) -** 輸入一個 IP 位址作爲此設定檔的來源 IP 的結束位址。 **IP 子網(IP Subnet)** – 定義子網，包含 IP 位址與遮罩位址。 ● **網路(Network)** – 輸入 IP 位址。 ● **遮罩(Mask)** – 使用下拉式清單選擇適當的網路遮罩。 **IP 物件/IP 群組(IP Object / IP Group)**– 使用下拉式清單選擇事先設定的 IP 物件/群組。
目標(Destination)	**任何(Any)** – 任何一個 IP 位址皆可視爲目標 IP 位址。 **IP 範圍(IP Range)** – 定義一段 IP 範圍作爲目標 IP 位址。 ● **起點(Start) -** 輸入一個 IP 位址作爲此設定檔的目標 IP 的起始位址。 ● **終點(End) -**輸入一個 IP 位址作爲此設定檔的目標 IP 的結束位址。 **IP 子網(IP Subnet)** -定義子網，包含 IP 位址與遮罩位址。 ● **網路(Network)** – 輸入 IP 位址。 ● **遮罩(Mask)** -使用下拉式清單選擇適當的網路遮罩。 **網域名稱(Domain Name)** – 指定目標網域名稱。 ● **選擇(Select)** – 按此選擇物件設定>>字串物件(Objects Setting>>String Object)中已經設定好的既有網域名稱。 ● **刪除(Delete)** – 移除目前使用的網域名稱。 ● **新增(Add)** – 建立新的網域名稱作爲目的地。 **IP 物件/IP 群組(IP Object / IP Group)**– 使用下拉式清單選擇事先設定的 IP 物件/群組。 **國家物件(Country Object)** – 使用下拉式清單選擇事先設定的物件，之後該國家內的所有 IP 全都會被視爲目標 IP。
目標埠號(Destination Port)	**任何(Any)** – 任何一個埠號皆可視之爲目標埠號。 **目標埠號範圍(Dest Port Range) -** ● **起點(Start) -** 輸入一個埠號爲此設定檔的目標 IP 的起始埠號。 ● **終點(End) -** 輸入一個埠號作爲此設定檔的目標 IP 之結束埠號。如果此區留白，即表示所有區域網路內的目標埠號可通過此 WAN 介面。
若符合上述原則，請轉往 **(Send to if criteria matched)**	**介面(Interface)** – 使用下拉式清單選擇 WAN 或是 LAN 介面或是 VPN 設定檔。符合上述原則的封包就會透過這裡所選的介面來傳輸。 **閘道 IP(Gateway IP)** –當您想轉送封包至需要的閘道上，請輸入指定閘道位址。通常預設閘道爲系統預設值。 **封包轉送至 WAN(Packet Forwarding to WAN via)** – 當您選擇 WAN 介面以應封包傳輸，您必須指定轉送的方式爲何，請選擇**強迫 NAT(Force NAT)**或是**強迫路由(Force Routing)**。 **自動備援至其它 WAN(Failover to)** – 勾選此框可在選擇的

	WAN 介面中斷連線時，將資料自動利用其它介面((WAN / LAN / VPN / 路由策略)來傳送。 ● **WAN/LAN –** 使用下拉式清單選擇自動備援介面。 ● **VPN –** 使用下拉式清單選擇 VPN 通道做爲備援通道。 ● **路由策略(Route Policy) –** 使用下拉式清單選擇既有的路由策略設定檔。 ● **閘道 IP(Gateway IP)** – 當您想要轉送封包至指定閘道時可在此輸入指定位址，通常系統會指定預設閘道位址。
優先權(Priority)	以全部路由或是路由策略爲基準傳送封包，路由器將依據固定路由或是路由策略的優先順序，決定採用哪種規則來傳送封包。 數值越大，優先權越低。預設值爲 200 代表具有比預設路由還高的優先權。 **故障恢復(Failback)**- 當啓用**自動備援至其它 WAN(Failover to)**選項時，管理者也可以啓用**故障恢復(Failback)**清除故障恢復介面上既有連線數並在原始介面恢復正常提供服務時，立刻回到原始介面上。當未啓用故障恢復(Failback)時，路由器僅會在既有連線數清除後，透過備援介面停止傳送封包，這可能會花費一些時間，因爲某些應用程式仍會持續傳送封包一陣子。因此，若管理者想要流量盡快經由主要介面傳送流量，建議使用此故障恢復選項。

3. 當您結束設定後，請按下**確定(OK)**儲存並離開此頁面。

II-6-2-2 自我診斷(Diagnose)

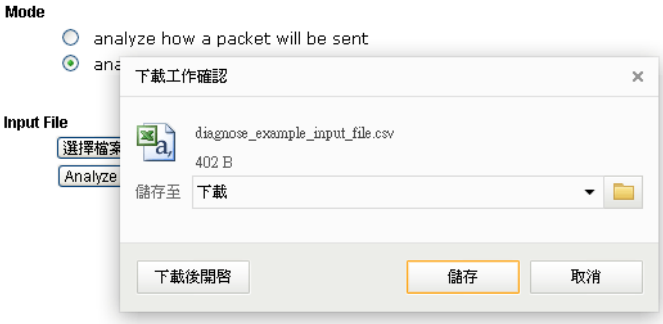
透過觀察此頁面完成的分析作業，管理人員可以追蹤封包傳輸的可能路徑(固定路由、路由表格或是策略路由等等)。

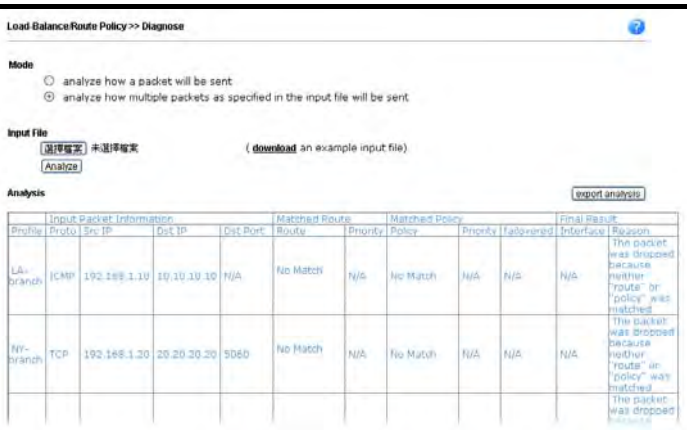


或是



可用設定說明如下：

項目	說明
模式(Mode)	**分析單一封包(Analyze a single packet)** – 選擇此模式以便路由器能針對單一封包進行分析，該封包會如何透過路由策略傳送出去。 **透過上傳輸入檔案以進行多重封包分析(Analyze multiple packets...)** - 選擇此模式以便路由器能針對指定檔案中的多重封包進行分析，這些封包會如何透過路由策略傳送出去。
封包資訊(Packet Information)	指定由路由器分析的封包性質。 **ICMP/UDP/TCP/ANY-** 指定一種協定以應診斷之需。 **來源 IP(Src IP)** – 輸入一個 IP 位址作爲來源 IP。 **目標 IP(Dst IP)** – 輸入一個 IP 位址作爲目標 IP。 **目標埠號(Dst Port)** – 使用下拉式清單指定一個目標埠號。 **分析(Analyze)** – 按此鈕執行分析工作。分析的結果將會顯示在本頁上，如有必要，可以按下輸出分析按鈕將結果以檔案的方式儲存起來。
輸入檔案(Input File)	**選擇(Select)** – 按下載連結取得空白範例檔案，接著按此鈕選擇該空白“.csv” 檔案以儲存分析的結果。  **分析(Analyze)** – 按此執行分析作業，分析的結果將會顯示在頁面上，如有必要可以按書出分析按鈕將結果以檔案輸出。



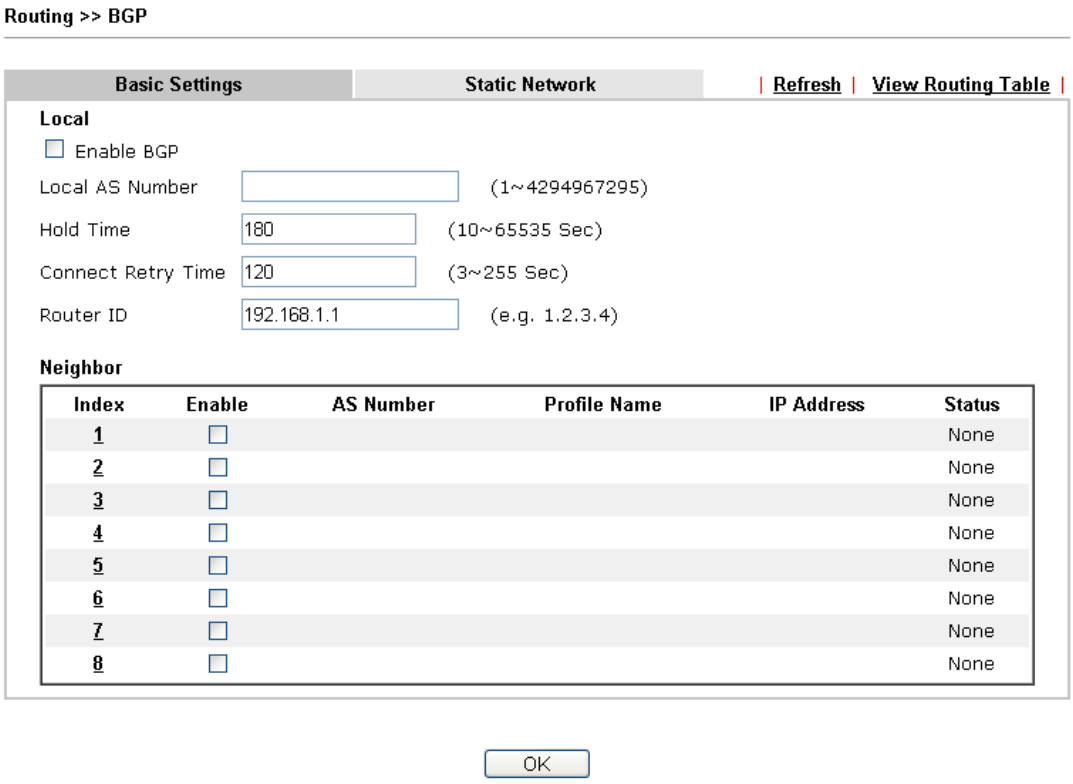
注意分析是以目前的負載平衡/策略路由設定爲基準，我們並不擔保能夠與真實例子百分百相同。

II-6-3 BGP

Border Gateway Protocol (BGP)是一種標準通訊協定，意欲在網際網路的自治系統(AS)之間進行路由與可達性資訊交換。

II-6-3-1 基本設定(Basic Settings)

本頁可配置本地路由器與相鄰路由器的基本設定。



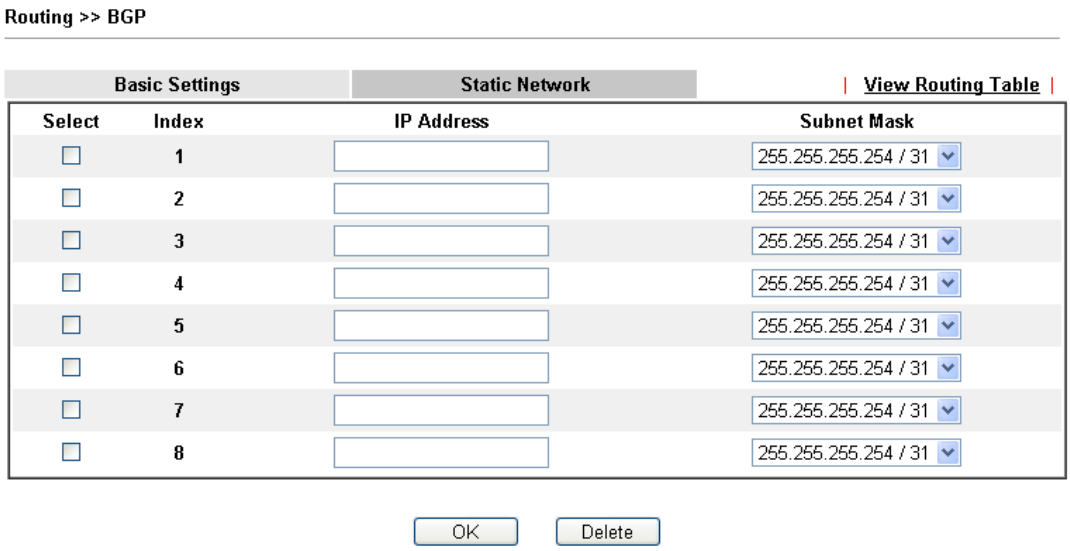
可用設定說明如下：

項目	說明
本地(Local)	
啓用 BGP(Enable BGP)	勾選此框啓用本機路由器基本的 BGP 功能。
本機自治系統編號(Local AS Number)	設定本機路由器的自治系統編號。
持續時間(Hold Time)	設定時間間隔(秒數)。當路由器無法接收來自對方的任何維持連線訊息時，這個時間可以用來確定對方是真的斷線了。
連接重試時間(Connect Retry Time)	如果路由器與相鄰路由器連接失敗，系統需要一段時間進行重新連接。 設定時間間隔來確定進行重新連接。
路由器 ID(Router ID)	輸入路由器的 LAN 子網位址。
鄰居(Neighbor)	
索引編號(Index)	按索引編號連結以配置相鄰設定檔。
啓用(Enable)	勾選此框以便啓動相鄰路由器的基本 BGP 功能。

自治系統編號(AS Number)	顯示相鄰路由器的自治系統編號(AS Number)。
設定檔名稱(Profile Name)	顯示相鄰設定檔的名稱。
IP 位址(IP Address)	顯示相鄰設定檔指定的 IP 位址。
狀態(Status)	顯示本地路由器與相鄰路由器的連線狀態。

II-6-3-1 固定網路(Static Network)

本頁允許您配置數個相鄰路由器以便進行與本機路由器的路由資訊交換。



可用設定說明如下：

項目	說明
選擇(Select)	勾選此框啓用選定之索引編號設定檔。
IP 位址(IP Address)	輸入路由器的 IP 位址。
子網遮罩(Subnet Mask)	使用下拉式清單指定 IP 位址所需的子網遮罩。

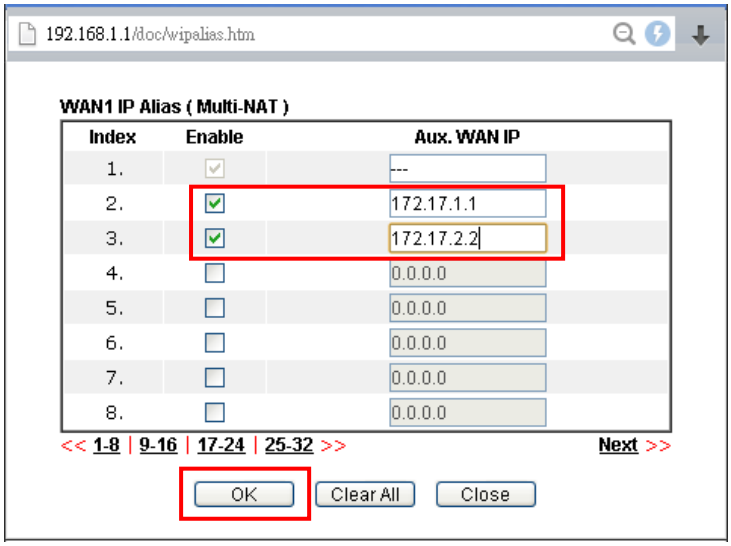
應用說明

A-1 如何利用路由策略設定位址對應(Address Mapping)?

位址對應(Address Mapping)可將 NAT 子網下特定虛擬 IP 或是一定範圍內的虛擬 IP 對應至特定的 WAN IP(或是 WAN IP 別名)。

此文介紹如何利用策略路由設定位址對應，當 WAN 介面具有多重真實 IP 位址時，管理者可以透過路由策略爲內部的 IP 位址，指定對外的 IP。

1. 設定 WAN IP 別名，開啓 **WAN>>網際網路連線>>細節設定(WAN >> Internet Access >> Details)** 頁面，並按下 **WAN IP 別名(WAN IP Alias)** 按鈕。



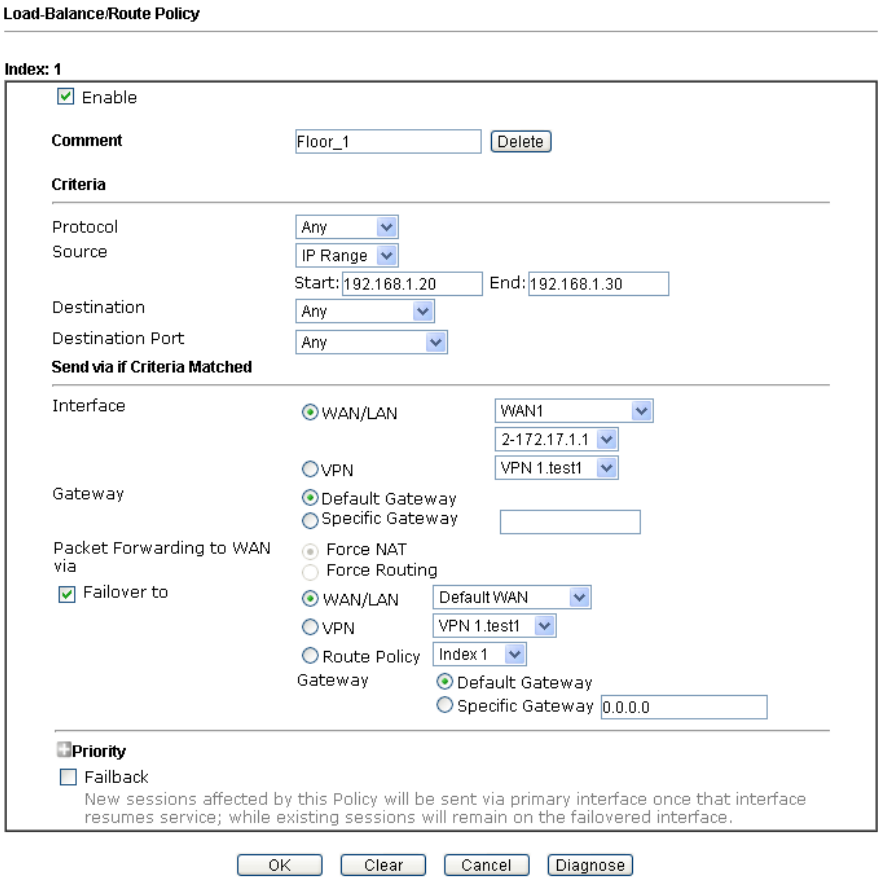
a. 勾選**啓用(Enable)**。

b. 輸入 WAN IP 位址。

c. 按下**確定(OK)**以儲存。

設定完 WAN IP 別名之後，這些 IP 位址會顯示在路由策略設定的介面下拉式清單中。

2. 開啓**路由>>負載平衡/路由策略(Routing>>Load Balance/Route policy)**，爲特定虛擬 IP 位址建立策略路由以便從特定 WAN IP 位址傳送。



a. 啓用此策略。

b. 輸入**來源 IP(Source IP)**範圍作爲虛擬 IP 位址。

c. 選擇任何(Any)作爲目標 IP(Destination IP)與埠號(Port)。

d. 介面(Interface)部分，選擇 WAN 並從下拉式清單中選擇適合的 WAN IP 位址。

e. 勾選 Failover to 其他的 WAN 介面，以便在指定路徑斷線時，讓流量可透過其他介面傳送。但是如果您想要流量僅使用特定的 IP 位址來傳送，請勿勾選啓用此選項。

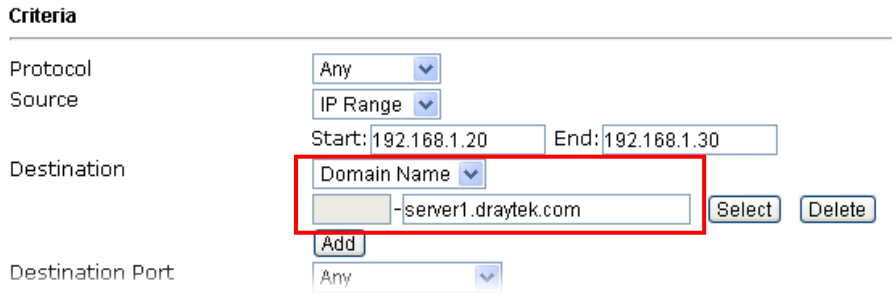
f. 按下**確定(OK)**儲存。

3. 完成上述設定之後，來自 192.168.1.20 與 192.168.1.30 之間並傳至網際網路的封包將使用真實 IP 172.17.1.1 來傳輸。

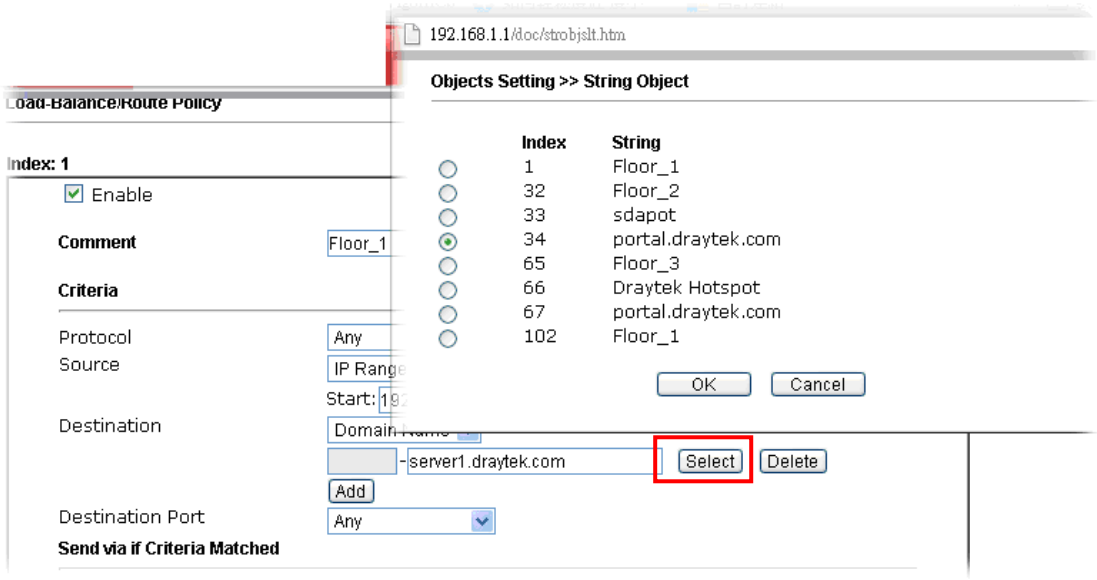
A-2 如何使用路由策略中的目標網域名稱?

路由策略支援使用網域名稱作爲目的標準，如果網路管理者嘗試指定發往某網站之流量的閘道，這個功能可以提供一個更直接的方式來進行路由策略設定。

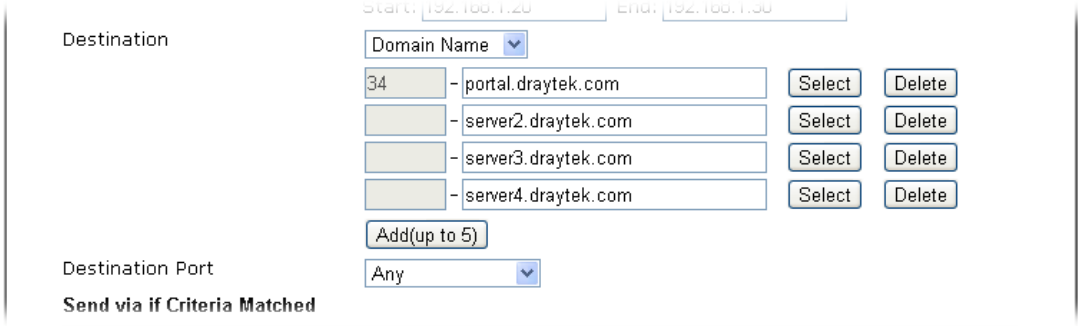
欲使用網域名稱，在**目標(Destination)**選項部分請選擇**網域名稱(Domain Name)**，然後在欄位中輸入網域的名稱。



或是，您可以按下**選擇(Select)**按鈕並使用於**物件設定>>字串物件(Objects Settings >> String Object)**頁面中事先定義的字串作爲網域名稱。

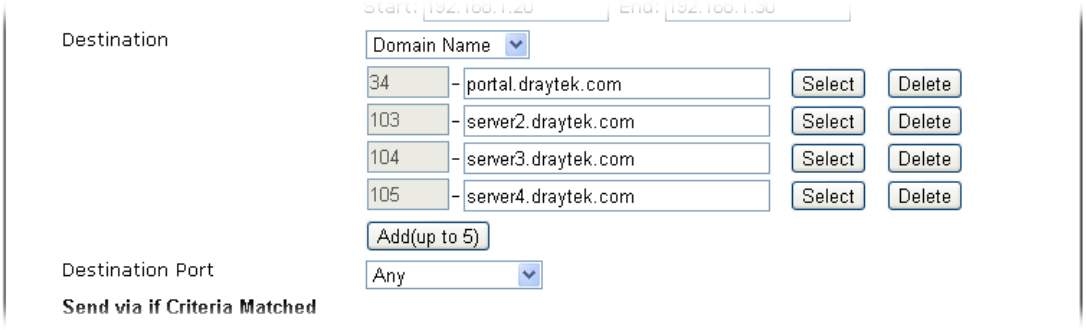


按**新增(Add)**建立更多的網域名稱，在路由策略中最多可以設定 5 個網域名稱。

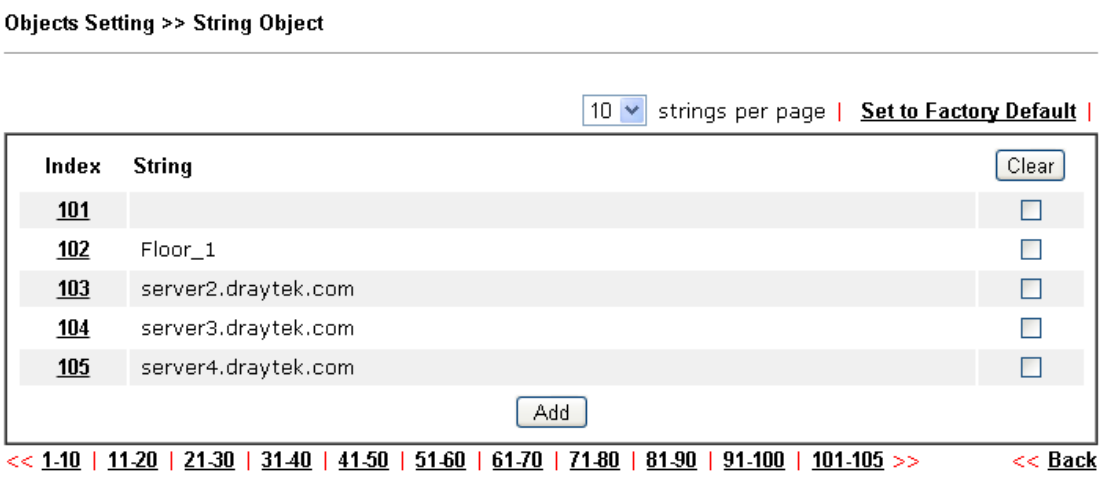


自動建立字串物件

如果您在路由策略中手動輸入網域名稱，在您按下**確定(OK)**按鈕套用路由策略之後，系統將自動給予特定的號碼予這些網域名稱。

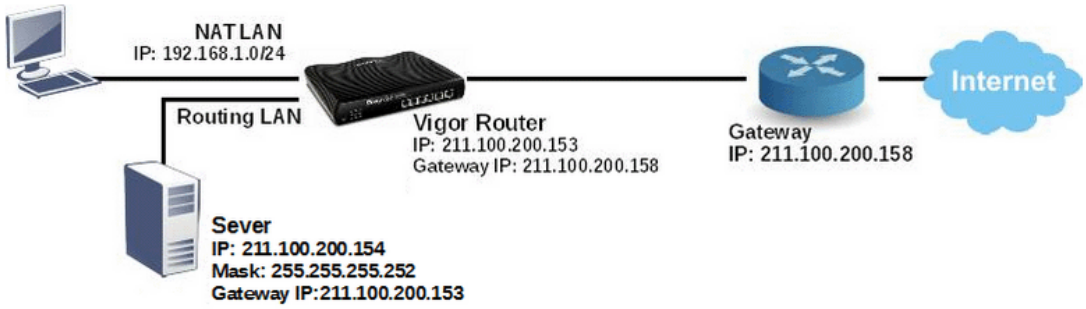


此表示路由器已經針對網域名稱自動建立字串物件，之後這些設定即可用於其他的路由策略和其他的功能。



A-3 如何使用區域網路(LAN)中的真實 IP?

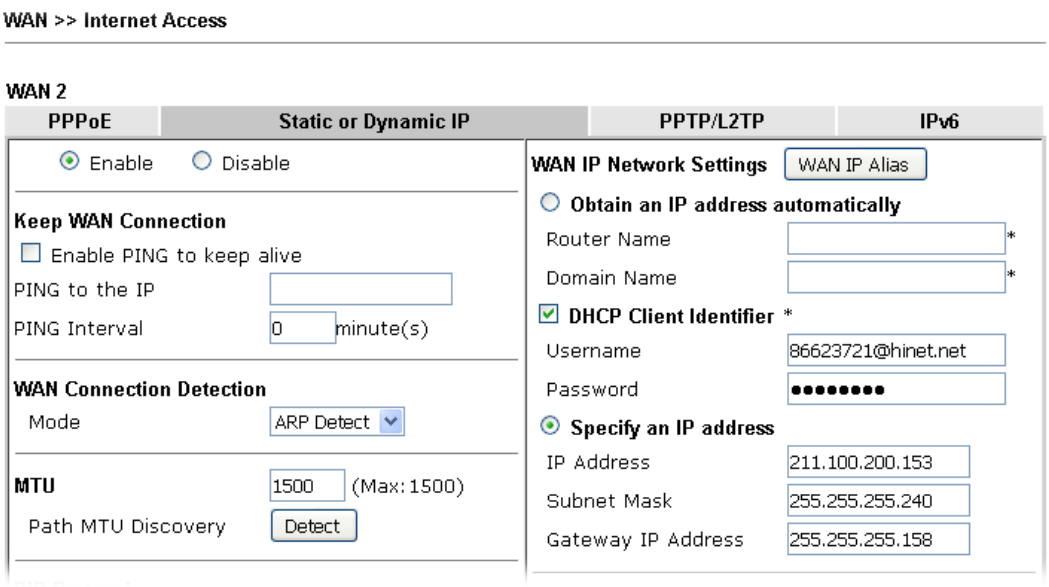
我們無法停用路由器的 NAT 功能，但是，我們可以使用路由器後方主機上的真實 IP 位址。如果 ISP 配給一個真實 IP 位址予我們使用，那麼我們可以利用這個真實 IP 來搭配 IP 路由子網。



設若 ISP 提供真實 IP 子網 211.100.200.152/255.255.255.248 而閘道 IP 爲 211.100.200.158。我們可以使用的真實 IP 位址即介於 211.100.200.153 到 211.100.200.157 之間，本文我們將說明如何設定一個非 NAT 子網讓路由器後方的伺服器能夠使用真實 IP(例如 211.100.200.154)。

WAN 設定

開啓 **WAN>>網際網路連線(WAN >> Internet Access)** 並依照 ISP 提供的內容設定 WAN 連線。(注意，若有必要指定一個 IP 位址，請記住 WAN 介面的子網遮罩必須大於 LAN 介面的遮罩設定。)

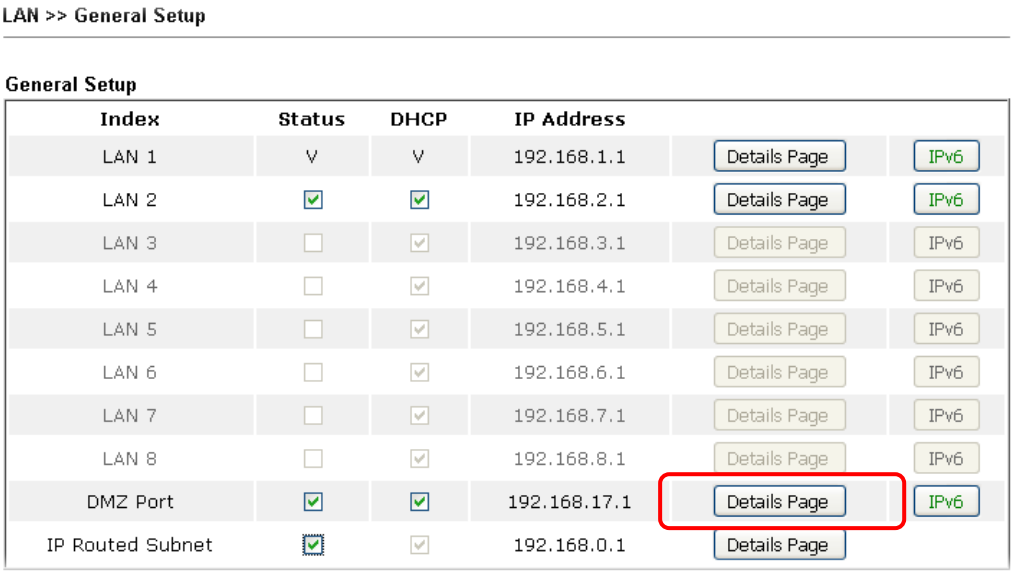


現在我們有二種方式可以運用：

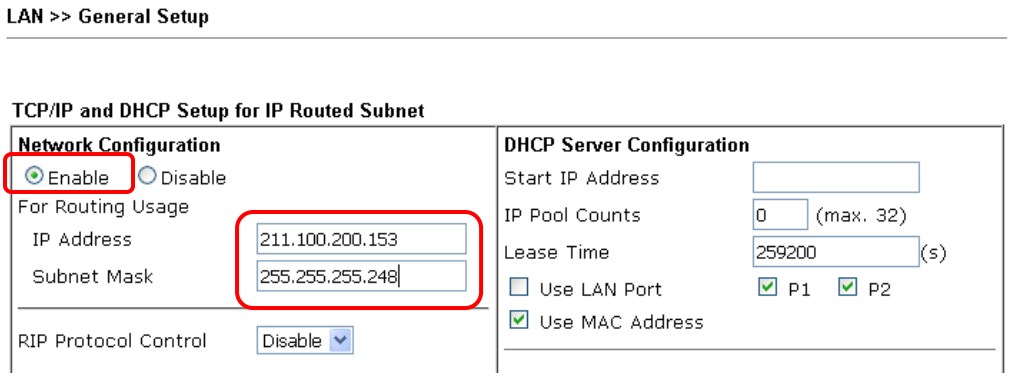
- IP 路由 LAN(IP Routed LAN)
- 用於路由(Routing Usage LAN)

IP 路由 LAN 設定(IP Routed LAN Setup)

1. 開啓 LAN>>基本設定(**LAN >> General Setup)**，按下 IP 路由子網的**細節設定(Details Page)**鈕。



2. 配置 TCP/IP 設定。



a. 啓用 IP 路由子網。

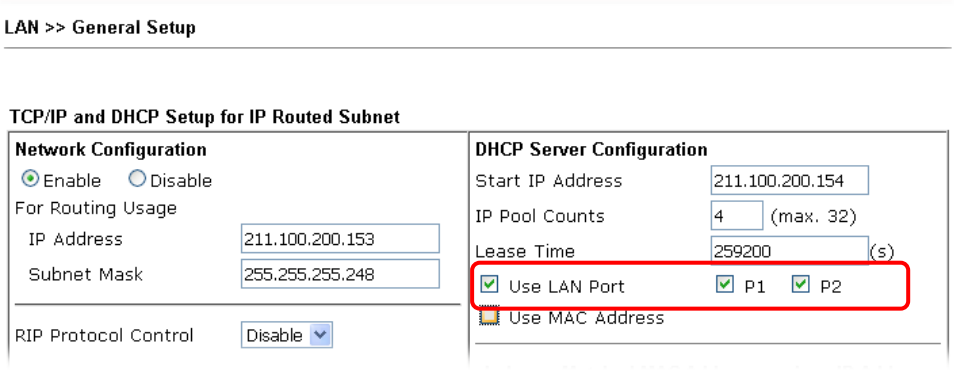
b. 輸入路由器的 IP 位址，請注意此位址可能與路由器的 WAN IP 位址相同。

c. 依照 ISP 提供的內容輸入子網遮罩。

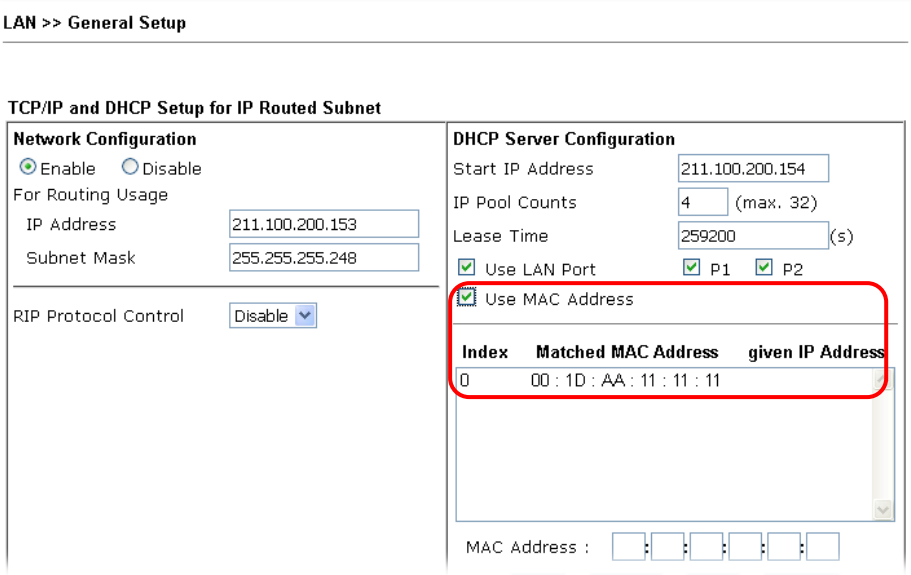
3. 欲使路由器後方的主機能取得真實 IP 位址，請

a. 在主機上設定固定 IP/子網遮罩。

b. 設定 DHCP IP Pool，勾選以啓用 Use LAN Port 並連接主機至指定 LAN 埠口的路由器上(本例是埠口 1 與埠口 2)。



c. 設定 DHCP IP pool，啓動使用 MAC 位址(Use MAC Address)，新增主機的 MAC 位址於表格中，然後自任何一個 LAN 埠口連接主機至路由器。

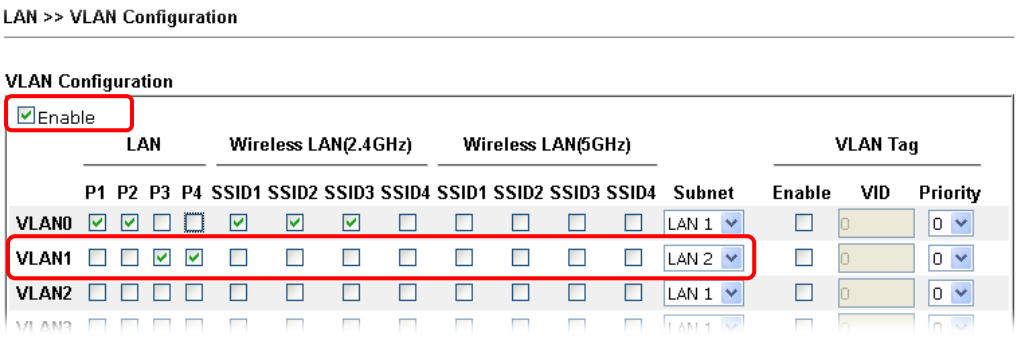


完成上述設定之後，具備真實 IP 211.100.200.154/ 遮罩 255.255.255.248/ 閘道 IP 211.100.200.153 的主機將能透過路由器存取網際網路。

用於路由(Routing Usage LAN)

我們也可以建立 LAN 子網以應路由用途，這裡舉 LAN2 爲例。

1. 開啓 **LAN >> VLAN**。

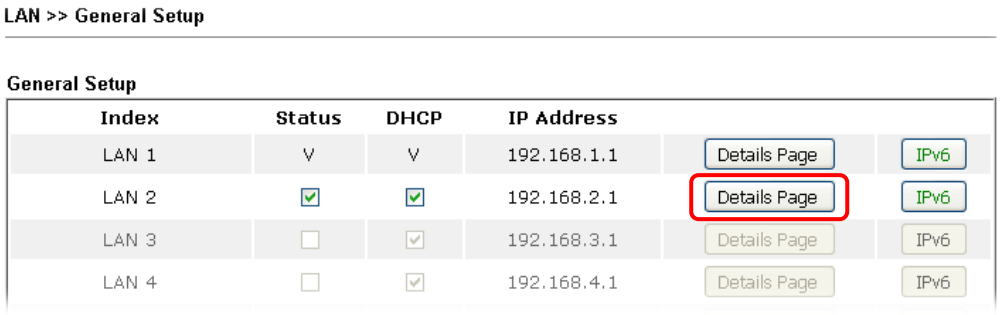


a. 啓用 VLAN 設定。

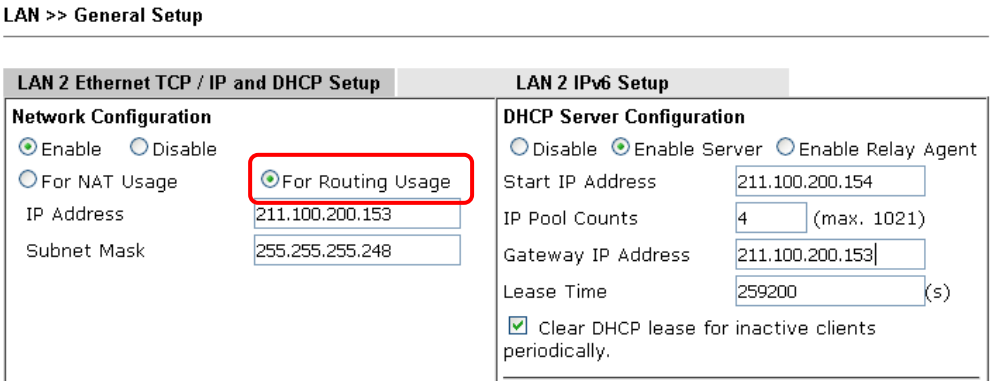
b. 針對 LAN2 子網設定一條 VLAN。

c. 指定屬於 LAN2 子網(本例指的是埠口 5 與 6)的 LAN 埠口，注意這些是主機應該連接的埠口。

2. 開啓 **LAN>>基本設定(LAN >> General Setup)**，按下 LAN 2 的**細節設定(Details Page)**。



3. 設定 LAN 2 的 TCP/IP 細節。



a. 啓用 LAN2。

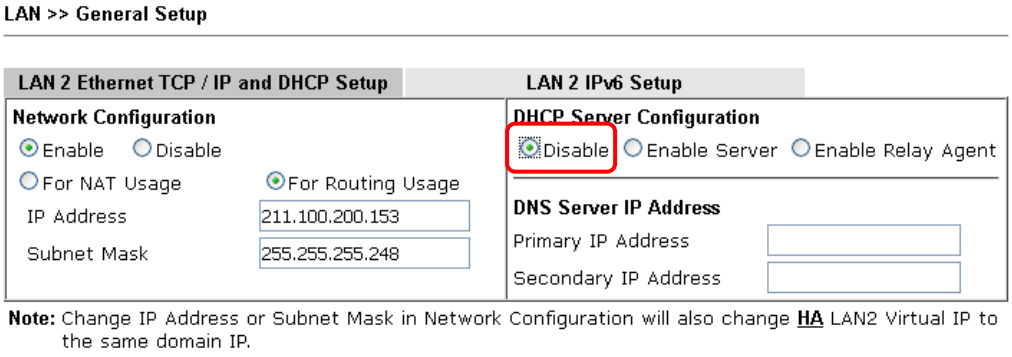
b. 選擇用於路由(For Routing Usage)。

c. 輸入路由器的 IP 位址，注意，這個設定可以跟路由器的 WAN IP 相同。

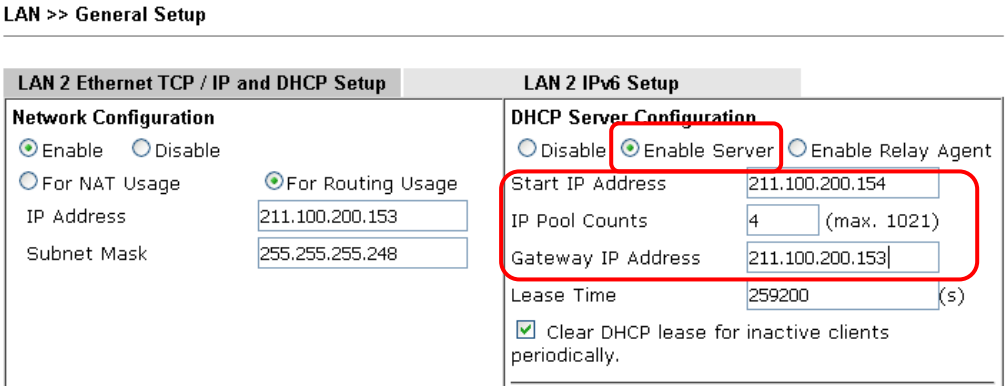
d. 依照 ISP 提供的內容輸入子網遮罩。

4. 針對 DHCP 伺服器設定，我們可以:

- 停用 DHCP 伺服器，在主機上設定固定 IP/子網遮罩。



- 啓用 DHCP 伺服器，並依照 ISP 提供的 IP 位址範圍設定 DHCP IP 配置量。



完成上述設定之後，連接至埠口 5 或是埠口 6，IP 設定爲真實 IP 211.100.200.154 / 遮罩 255.255.255.252 / 閘道 IP 211.100.200.153 的 PC 或是伺服器將能透過路由器存取網際網路。

故障排除

如果在上述設定之後，含真實 IP 位址的 PC 無法登入網際網路，請檢查：

- 是否真實 IP 位址正被其他裝置使用

- 是否路由器的 WAN 連線模式爲固定或動態 IP(Static or Dynamic IP)，確認 WAN 介面的子網遮罩必須大於 LAN 介面的遮罩設定。

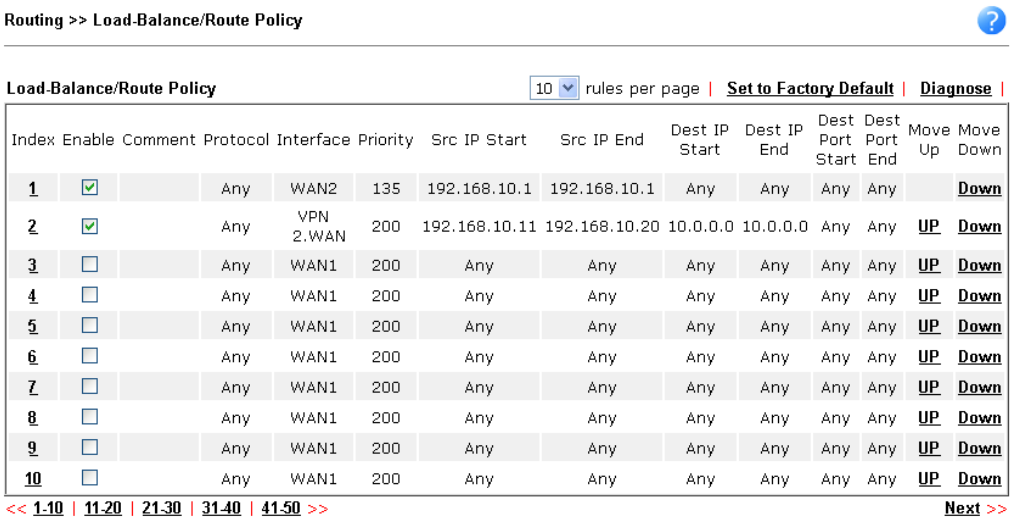
若上述資訊無法提供任何幫助，請變更主機的閘道 IP 位址，從路由器的 IP 211.100.200.153 改成 IP 閘道 211.100.200.158 並直接連接 PC 至 ISP 數據機，看看是否可以運作。

A-4 簡要說明負載平衡/策略路由(Load Balance/Route Policy)

本文主要針對負載平衡/策略路由提供簡易的說明，這個功能可以讓網路管理者能更具體的管理對外的流量。

負載平衡/路由策略設定的策略，其優先權設定，通常比 **WAN>>基本設定(WAN>>General Setup)** 中的預設路由與自動負載平衡要高，但比防火牆規則要低。管理者也可以對策略另外定義適合的優先權。

欲設定路由策略，請開啓**路由>>負載平衡/路由策略(Routing>>Load-Balance/Route Policy)**頁面，下圖提供網頁截圖範例，列出所有的策略並且顯示策略是否已被啓用，是否符合標準，透過哪個介面傳送流量以及優先權設定爲何。



Routing >> Load-Balance/Route Policy

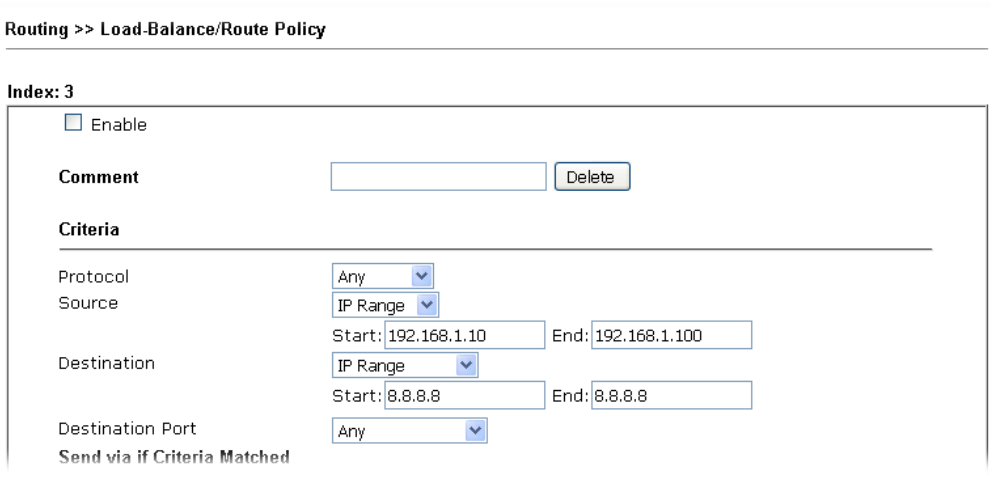
Load-Balance/Route Policy 10 rules per page | Set to Factory Default | Diagnose |

Index	Enable	Comment	Protocol	Interface	Priority	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	☑		Any	WAN2	135	192.168.10.1	192.168.10.1	Any	Any	Any	Any		Down
2	☑		Any	VPN 2.WAN	200	192.168.10.11	192.168.10.20	10.0.0.0	10.0.0.0	Any	Any	UP	Down
3	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
4	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
5	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
6	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
7	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
8	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
9	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
10	☐		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down

<< 1-10 | 11-20 | 21-30 | 31-40 | 41-50 >> Next >>

欲設定路由策略，請先點選一個索引編號，在頁面的底部，有二種設定的方式可以選擇：設定精靈模式提供簡單又基本的設定；進階模式提供較多的選項供用戶進行設定。

1. 首先，設定封包可套用的規則。



Routing >> Load-Balance/Route Policy

Index: 3

☐ Enable

Comment Delete

Criteria

Protocol: Any

Source: IP Range — Start: 192.168.1.10 End: 192.168.1.100

Destination: IP Range — Start: 8.8.8.8 End: 8.8.8.8

Destination Port: Any

Send via if Criteria Matched

a. 選擇一個通訊協定(Protocol)。

b. 輸入來源 IP 位址範圍，若是起點與終點是相同的，那麼來源 IP 就會是單一位址。

c. 輸入目標 IP 位址範圍。

d. 選擇目標埠號。

上述範例設定的情境是封包由 92.168.1.10~192.168.1.100 傳送至 8.8.8.8，不論通訊協定或是目標埠號設定爲何，系統都會遵循路由策略來處理封包的傳輸。

2. 接著我們可以選擇介面與閘道，若符合設定標準，那麼封包就可以透過該介面與指定之閘道傳送。

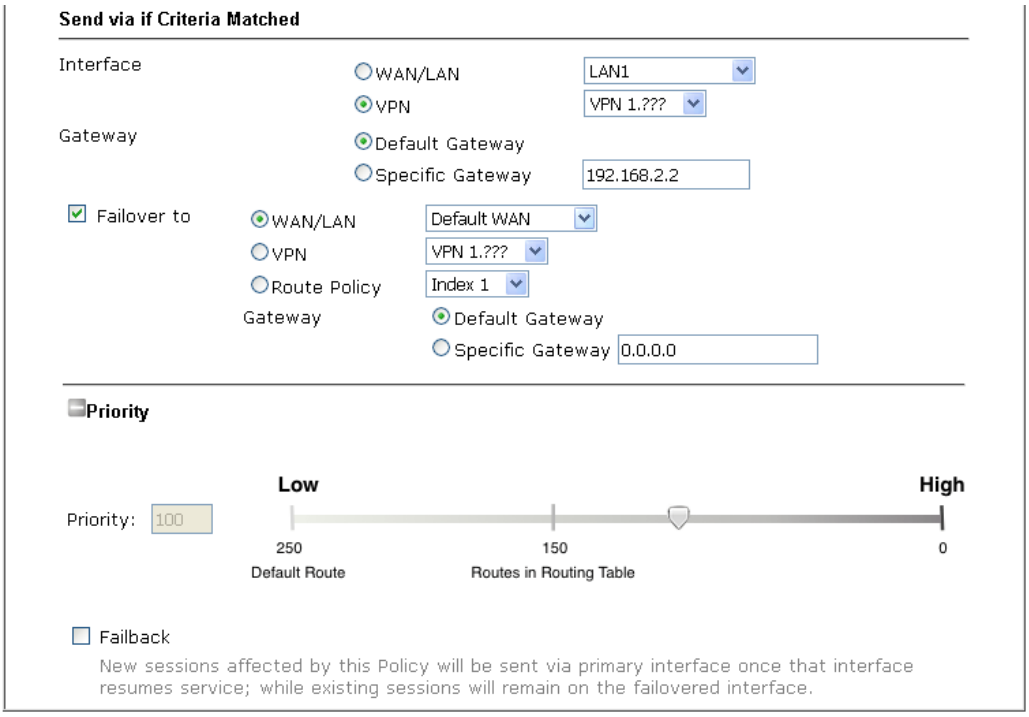


a. 選擇一個介面。

b. 選擇閘道 IP 位址，注意若是介面選擇爲 LAN，那就需要再指定特定的閘道位址。

上述範例設定的情境是如果封包符合此路由策略的規定，那麼它將被傳送至預設閘道，然後透過 VPN1 送往目的地。

3. 在**進階模式(Advance Mode)**中，如果介面選擇 WAN 或是 VPN，那麼還有更多的選項可以設定：



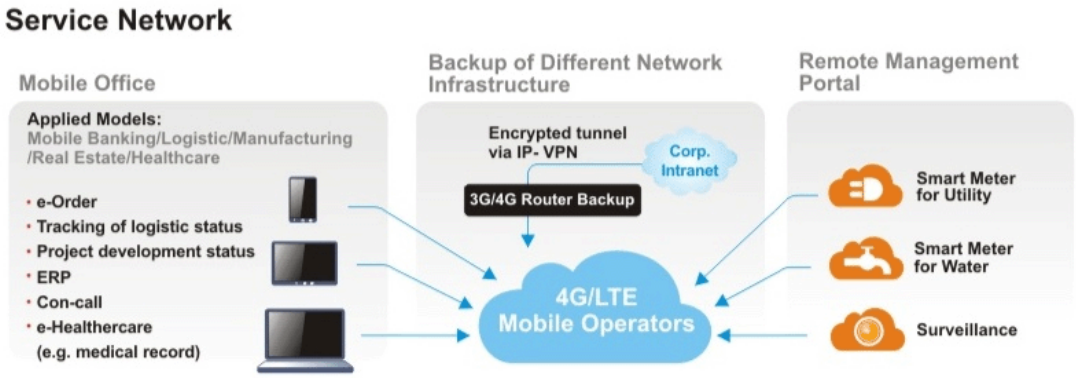
- **備援至(Failover to)**：啓用封包透過其他介面傳送或是遵循其他可以診斷出原始介面路徑中斷之策略來傳送，上述的設定指出當原始路由中斷連線了，封包可以透過 WAN2 來傳輸。
- **故障恢復(Failback)**：當啓用選項**備援至(Failover to)**時，管理者也可以啓用**故障恢復(Failback)**以便在原始介面恢復服務時，清除備援介面上既有連線數並立即返回原始介面。若未啓用**故障恢復(Failback)**，路由器僅會在既有連線數清除時，停止透過備援至介面傳送封包，而這個過程會花費較長的時間進行，因爲應用程式還會維持傳送封包一陣子之故。因此，若管理者想要儘快讓流量透過主要介面來傳送，建議使用**故障恢復(Failback)**選項。
- **優先權(Priority)**:管理者可以設定優先權範圍從 1 到 249 以應路由策略使用，其中數字越小代表優先權越高。當有二個策略具有相同的優先權時，則依照策略的索引編號順序，採用符合的策略。

II-7 LTE

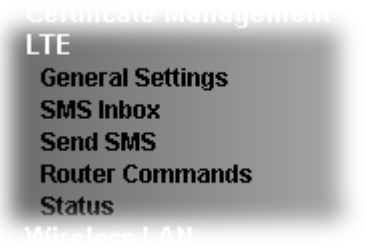
具備 SIM 卡的 LTE WAN 可以提供給路由器方便的網際網路存取方式，不過我們一直在想路由器是否還可以利用此 SIM 卡提供更多有用的功能呢？現在我們已經開發出一些有用的功能，可以提供給使用者運用，諸如從路由器傳送簡訊報告路由器的狀態，透過簡訊操作從遠端重新啓動路由器等等。

本節會引導您使用 LTE WAN 內的 SIM 卡，執行簡訊等相關操作。

資訊	此功能限用“L”型號。



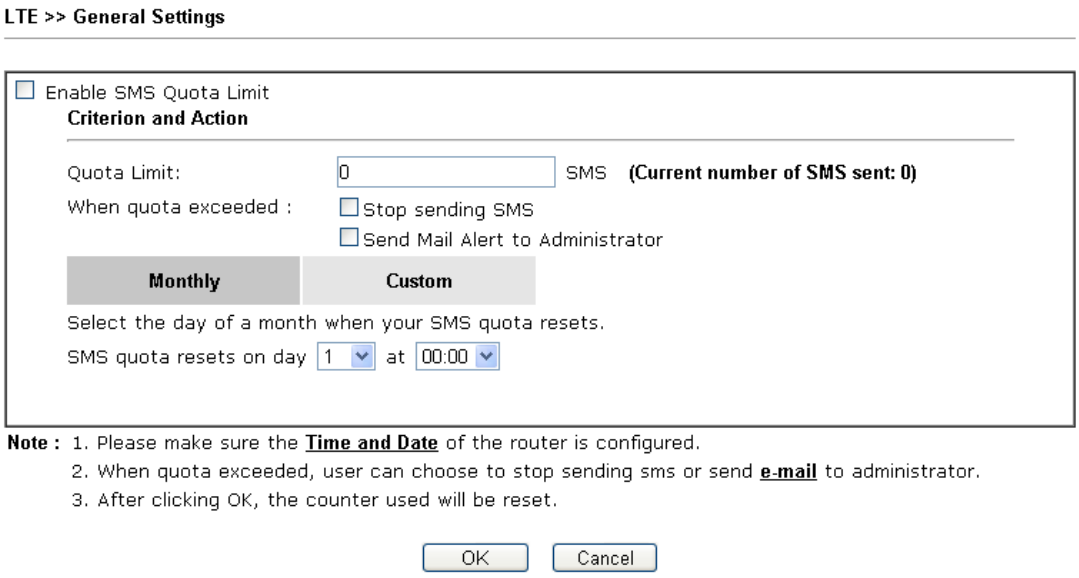
網頁使用者介面



II-7-1 基本設定(General Settings)

II-7-1- 1 簡訊額度(SMS Quota)

本頁讓您設定 LTE 基本設定，當您啓用了簡訊額度限制時，您可以指定簡訊額度的則數，超過額度時採取的行動以及重新設定簡訊額度等等。



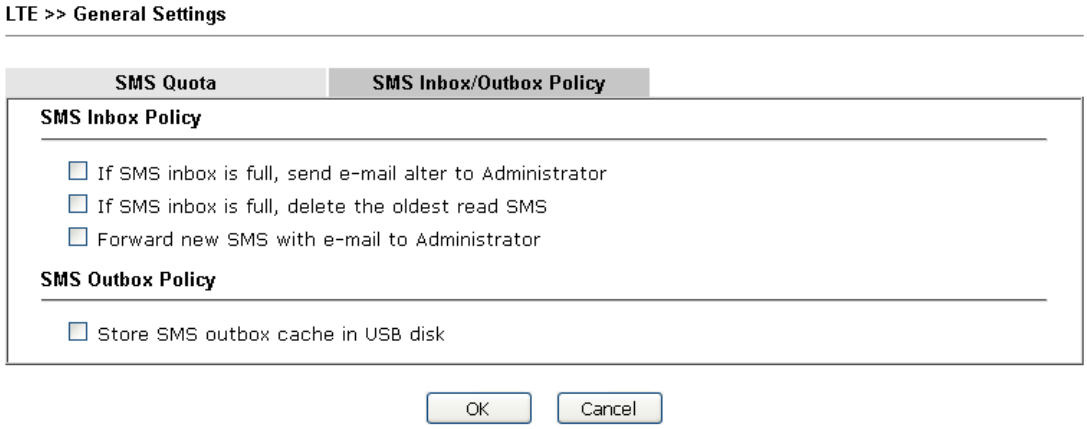
可用設定說明如下：

項目	說明
啓用簡訊額度限制(Enable SMS Quota Limit)	勾選此框啓用此功能。
額度限制(Quota Limit)	指定最多可以傳送簡訊的則數。
當額度超過時(When quota exceeded)	當超過額度限制時，有二種行動可以採取： **停止傳送簡訊(Stop sending SMS)** – 如果選擇此項，在額度超過時，沒有任何簡訊會傳送出去。 **傳送郵件警示給管理者(Send Mail Alert to Administrator)** – 如果選擇此項，在額度超過時，系統會寄發郵件警示予管理者。
每月(Monthly)	這個設定提供的機制可以重新設定每個月簡訊則數。 **簡訊額度每日重新起計(SMS quota resets on day XX at XX ...)** –您可以決定每個月的起始日期，屆時簡訊傳送的數量就會重置。

使用者定義(Custom)	這個設定可以依照需求讓使用者定義結算周期。 發送的簡訊數目在周期間隔重置。 **使用者定義(Custom)** – 預設值是每個月，如果您需要一個更長或是更短的週期，請改設定**使用者定義**，結算週期介於 1 到 60 天，您可以指定日數與時數來決定週期的長短，此外您也可以指定目前週期內的天數爲幾天。 ● **結算週期(Cycle duration)**: 指定重設簡訊則數的期間(日、時)。例如數字 7 表示整個週期有 7 天；20 就表示有 20 天。當時間已到，路由器就會自動重置檢訓則數紀錄。 ● **目前週期內的天數(Today is day XX in the cycle)** – 指定結算週期內中的哪一天作爲結算的起始日，例如數字 3 就表示整個結算週期的第 3 日爲起始日。

II-7-1-2 簡訊收件匣/寄件匣策略(SMS Inbox/Outbox Policy)

本頁列出簡訊收件匣與寄件匣可以使用的策略，請勾選需要的策略並按**確定(OK)**即可。



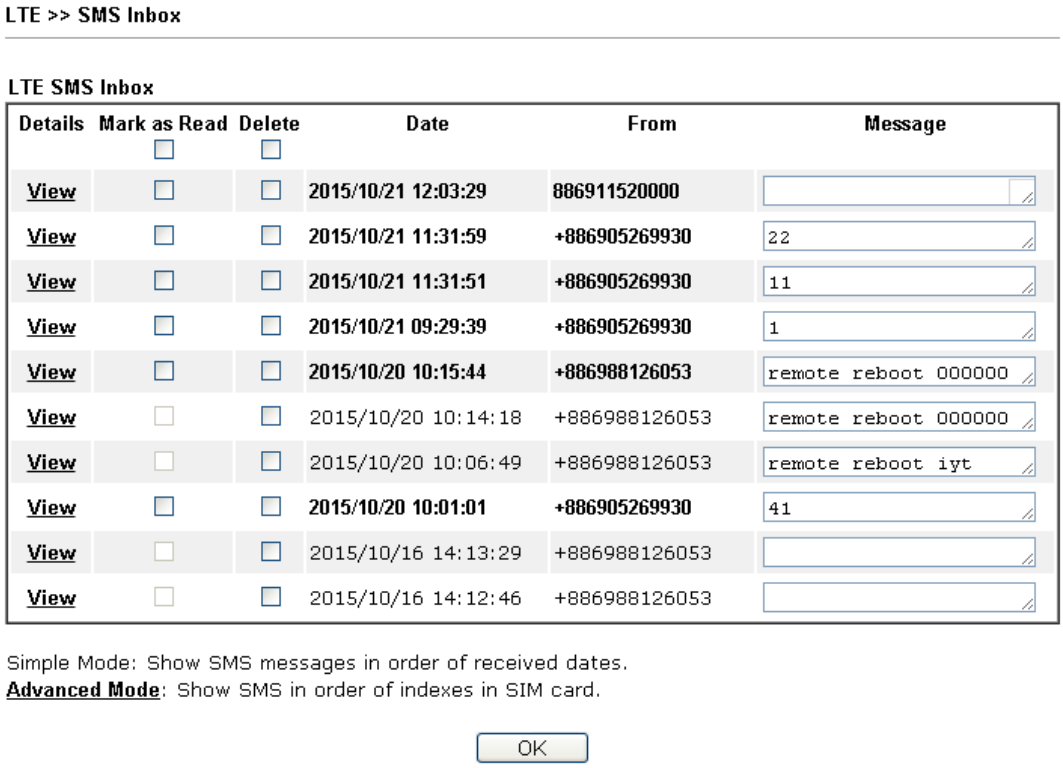
II-7-2 簡訊收件匣(SMS Inbox)

本頁列出 LTE SIM 卡接收到的簡訊。簡訊收件匣表顯示接收日期、電話號碼或是傳送者 ID 以及訊息的部分內容。

由於一封簡訊受到資料大小的限制，長訊息會以多封簡訊來寄送。爲了使用者的方便性，我們提供二種模式供選擇。**簡易模式(Simple Mode)**列出含接收時間的簡訊訊息；**進階模式(Advanced Mode)**列出 SIM 卡內實際索引編號呈現的簡訊，不同 SIM 卡有不同的功能，基本上，大約可以容納 30 到 40 封簡訊，請注意當所有的簡訊索引編號都滿額使用時，SIM 卡就無法再接收新的簡訊。

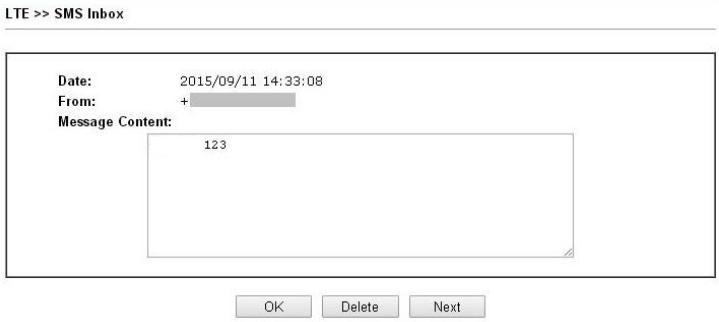
按網頁下方的簡易模式連結或是進階模式連結來切換這二種模式。

II-7-2-1 簡易模式(Simple Mode)



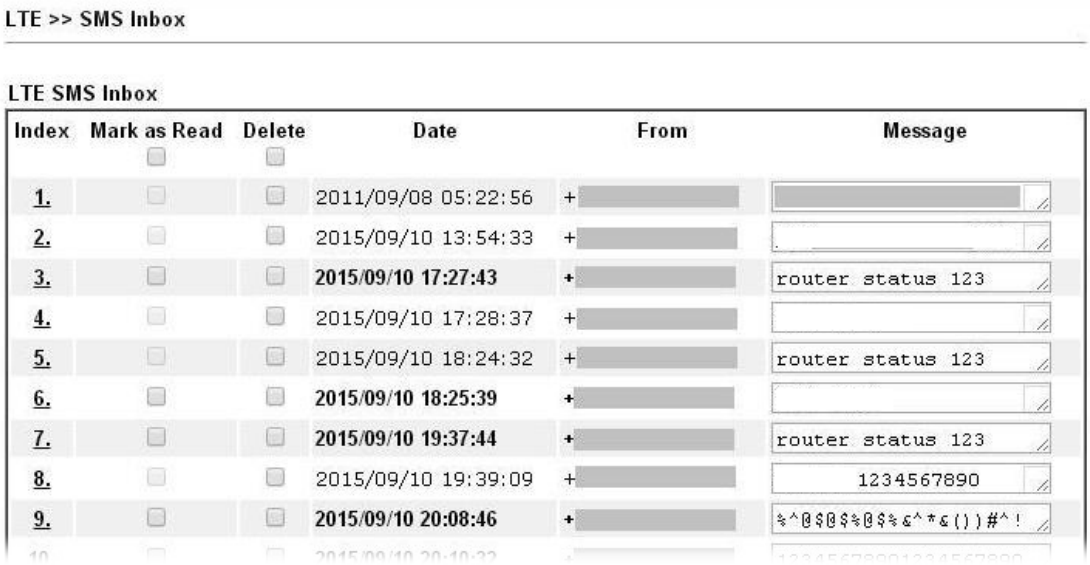
可用設定說明如下：

項目	說明
標示爲讀取(Mark as Read)	標示未讀取狀態的訊息以粗體字顯示，如果您想要變更訊息爲讀取狀態，選擇該訊息並按下確定(OK)按鈕。
刪除(Delete)	如果您想要刪除此訊息，請選擇該訊息並按下確定(OK)按鈕。
細節(Details)	顯示 SIM 卡目前接收到的簡訊則數。 如果您想要讀取訊息的全文，請按該訊息條列上的檢視(View)連結開啓如下的頁面。開啓之後，訊息的狀態就會變更爲“已讀取”。



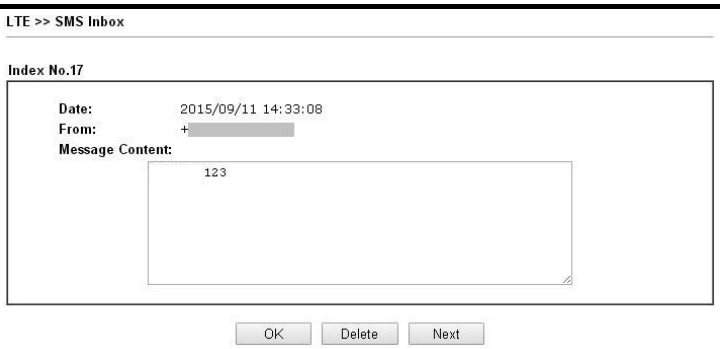
- **訊息內容(Message Content)** - 顯示訊息全文。
- **確定(OK)** – 回到前一個頁面。
- **刪除(Delete)** - 按此以刪除此訊息並回到前一個頁面。
- **下一頁(Next)** - 按此可以看下一篇訊息的內文。

II-7-2-1 進階模式(Advanced Mode)



可用設定說明如下：

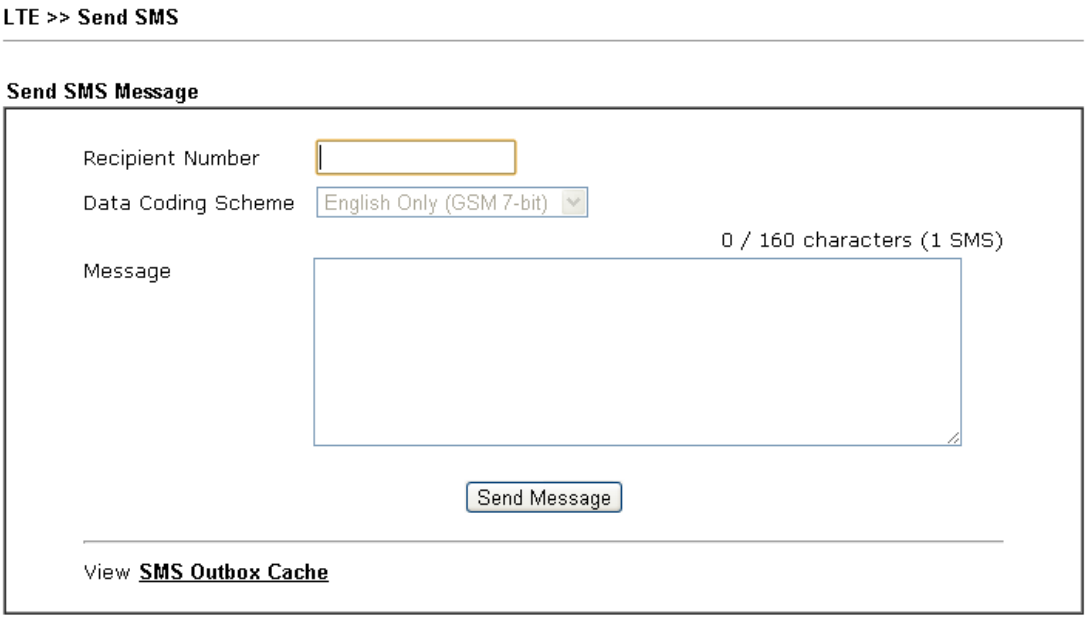
項目	說明
標示爲讀取(Mark as Read)	標示未讀取狀態的訊息以粗體字顯示，如果您想要變更訊息爲讀取狀態，選擇該訊息並按下確定(OK)按鈕。
刪除(Delete)	如果您想要刪除此訊息，請選擇該訊息並按下確定(OK)按鈕。
索引編號(Index)	顯示 SIM 卡可以接收的簡訊總數。 如果您想要讀取訊息的全文，請按該訊息條列上的索引編號連結開啓如下的頁面。開啓之後，訊息的狀態就會變更爲“已讀取”。



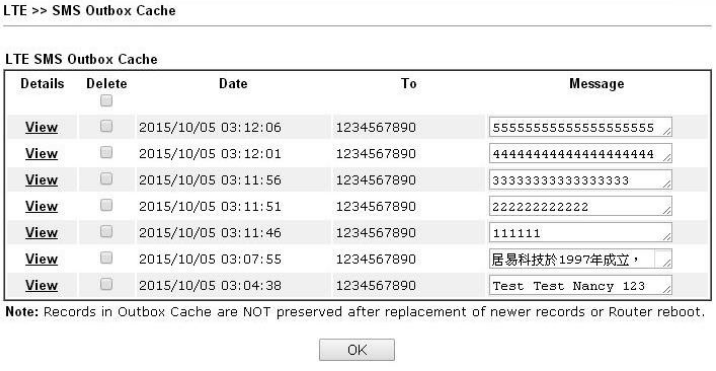
- **訊息內容(Message Content)** - 顯示訊息全文。
- **確定(OK)** – 回到前一個頁面。
- **刪除(Delete)** - 按此以刪除此訊息並回到前一個頁面。
- **下一頁(Next)** - 按此可以看下一篇訊息的內文。

II-7-3 傳送簡訊(Send SMS)

本頁用來配置透過 LTE SIM 卡傳送簡訊的設定，同時也顯示傳送訊息需要的簡訊則數。



可用設定說明如下：

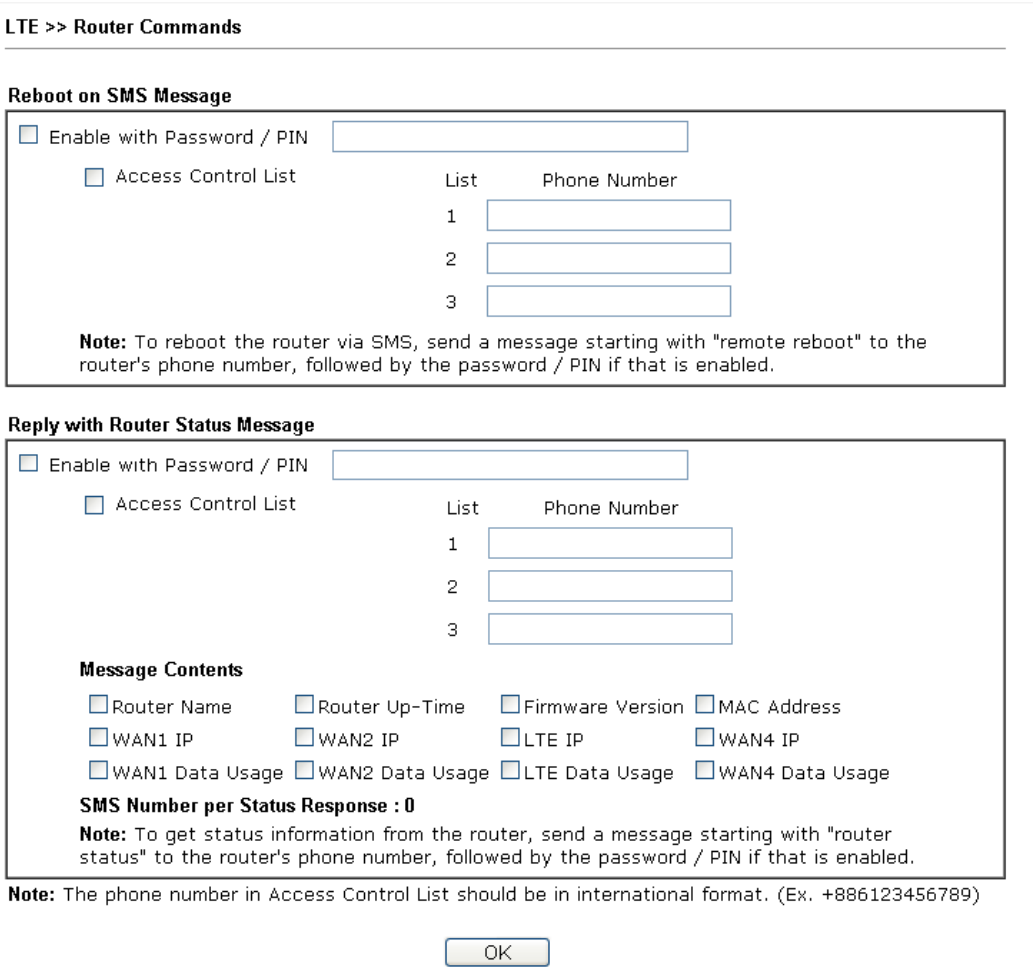
項目	說明
收件人號碼(Recipient Number)	輸入收件人的電話號碼。 格式可以是國際電話號碼(+8869123455678)或是一般電話號碼(0912345678)。
資料編碼方案(Data Coding Scheme)	路由器將依照目前的訊息內容，自動選擇適合的資料編碼方案。目前支援 GSM 7-bit 與 UCS-2。
訊息(Message)	輸入欲傳送出去的訊息內容。 文字總數爲 1024 個字元。
傳送訊息(Send Message)	按此立即傳送簡訊給指定的收件人。
檢視簡訊寄件匣暫存(View SMS Outbox Cache)	顯示從路由器發送的簡訊紀錄。 

II-7-4 路由器指令(Router Commands)

本頁可讓使用者設定遠端重新啓動路由器的功能並透過簡訊取得路由器的狀態資訊。



開啓 **LTE>>路由器指令(LTE>>Router Commands)**頁面。



可用設定說明如下：

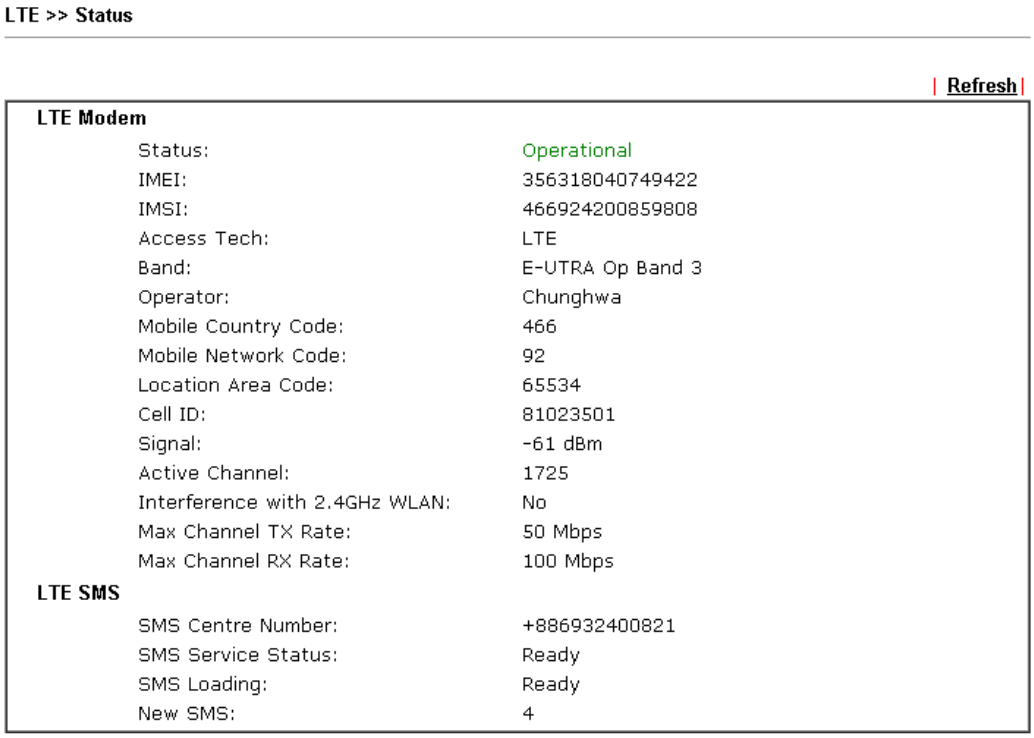
項目	說明
在簡訊的訊息上重新啓動(Reboot on SMS Message)	
以密碼/ PIN 碼啓用(Enable with Password / PIN)	欲透過簡訊從遠端重新啓動 Vigor 路由器，請勾選此框並輸入密碼/PIN 碼(以驗證行動電話)。

	密碼得包含字母、數字與底線。
存取控制清單(Access Control List)	勾選此框以便輸入或修正電話號碼(最多可設定 3 組)。 此處指定的電話號碼亦即有能力從遠端寄送簡訊以重新啓動 Vigor 路由器。 **注意**: 如果啓用了此功能，只有此處指定的行動電話能夠寄送簡訊以便重新啓動路由器；因此若停用此功能，只要輸入的密碼正確，任何行動電話都可以寄送簡訊重新啓動 Vigor 路由器。
回覆含路由器狀態訊息(Reply with Router Status Message)	
以密碼/ PIN 碼啓用(Enable with Password / PIN)	使用者可以透過行動電話，輸入此區的密碼或是 PIN 碼通過驗證，取得路由器的 WAN 資料運用以及基本資訊(如 IP 位址、MAC 位址等等) 密碼得包含字母、數字與底線。
存取控制清單(Access Control List)	勾選此框以便輸入或修正電話號碼(最多可設定 3 組)。 此處指定的電話號碼亦即有能力從遠端取得與 Vigor 路由器相關的資訊。 **注意**: 如果啓用了此功能，只有此處指定的行動電話能夠取得與路由器相關的資訊；因此若停用此功能，只要輸入的密碼正確，任何行動電話都可以取得與路由器相關的資訊。
訊息內容(Message Contents)	有數種訊息內容種類供使用者選擇，請選擇並勾選需要的項目，之後路由器將會發送簡訊提供與該項目相關的狀態回覆訊息。
每筆狀態回覆之簡訊訊息(SMS Number per status response)	顯示需要傳送狀態訊息的簡訊總數。

II-7-5 狀態(Status)

具備 LTE 功能的路由器存取網際網路，且能傳送簡訊給予指定的行動電話。

本頁顯示內嵌 LTE 模組的基本資訊以及目前 LTE 連線的狀態。



項目說明如下：

項目	說明
狀態(Status)	顯示 LTE WAN 狀態。
IMEI	顯示 LTE SIM 卡的國際移動設備辨識碼(IMEI) 。
IMSI	顯示 LTE SIM 卡的國際移動用戶識別碼(IMEI) 。
存取技術(Access Tech)	顯示 LTE 連線的類型(CDMA/GSM/WCDMA/LTE/TD-SCDMA)。
頻段(Band)	顯示 LTE 連線的頻段。
操作者(Operator)	顯示 LTE 連線的 ISP 名稱。
行動電話國碼、網路碼、區碼、電話 ID 等等(Mobile Country Code / Mobile Network Code / Location Area Code / Cell ID)	顯示基本站台資訊。
訊號(Signal)	顯示 LTE 連線的訊號強度。
使用中的頻道(Active Channel)	顯示 LTE 連線頻率。
2.4GHz WLAN 干擾值 (Interference with 2.4GHz	顯示目前 LTE 頻率有無造成 2.4G 無線干擾，若有發現，被干擾

WLAN)	的 2.4G 無線頻道會顯示出來。
最大頻道傳送/接收速率 (Max Channel TX Rate / Max Channel RX Rate)	顯示 LTE 連線的最高傳送/接收速率。
簡訊中心號碼(SMS Centre Number)	顯示 LTE SIM 卡的簡訊服務的電話號碼。
簡訊服務狀態(SMS Service status)	顯示 LTE SIM 卡的簡訊服務是否已經準備妥當。
簡訊載入(SMS Loading)	顯示在 LTE SIM 卡接收的簡訊是否已經載入路由器。
新簡訊(New SMS)	顯示簡訊收件匣內未讀取的簡訊則數。

第三篇 無線區域網路設定



無線區域網路可提供高移動性，因此無線區域網路的用戶能夠同時存取所有區域網路設備，如同有線區域網路以及網際網路一般。

III-1 無線區域網路設定(Wireless LAN (2.4GHz/5GHz))

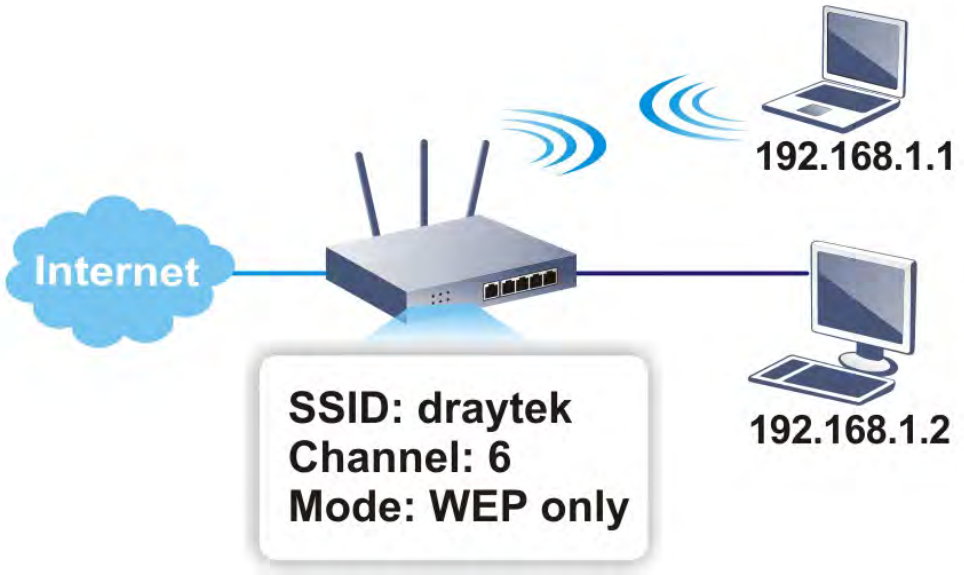
本節所提供的資訊僅針對 *n* 及 *ac* 系列機型。

在最近幾年無線通訊的市場有了極大的成長，無線技術線在到達了或說是有能力到達地球表面上的每一個點，數以百萬的人們每天透過無線通訊產品彼此交換資訊，Vigor G 系列路由器，又稱爲 Vigor 無線路由器，被設計成爲一個適合小型辦公室/家庭需要的路由器，擁有最大的彈性與效率，任何一個被授權的人，都可以攜帶內建的無線區域網路用戶端 PDA 或是筆記型電腦，進入會議室開會，因而不需擺放一堆亂七八糟的纜線或是到處鑽孔以便連線。無線區域網路機動性高，因此無線區域網路使用者可以同時存取所有區域網路中的工具，以及遨遊網際網路，好比是以有線網路連接的一樣。

Vigor 無線路由器皆配有與標準 802.11n draft 2 通訊協定相容之無線區域網路介面，爲了進一步提高其效能，Vigor 路由器也承載了進階無線技術以便將速率提升至 300 Mbps*，因此在最後您可以非常順利的享受流暢的音樂與影像。

資訊	資料的實際總處理能力會依照網路條件和環境因素而改變，如網路流量、網路費用以及建造材料。

在無線網路的基礎建設模式(Infrastructure Mode)中，Vigor 無線路由器扮演著無線網路基地台(AP)的角色，可連接很多的無線用戶端或是無線用戶站(STA)，所有的用戶站透過路由器，都可分享相同的網際網路連線。**基本設定(General Settings)**可讓您針對無線網路所需的訊息包含 SSID、頻道等項目做基本的配置。



多重 SSID

Vigor 路由器支援四組無線連線 SSID 設定，每個 SSID 都可以定義不同的名稱及上下載速率，方便遠端用戶於尋求無線連線時挑選使用。

即時硬體加密

Vigor 路由器配有 AES 加密引擎，因此可以採用最高級的保護措施，在不影響使用者的習慣之下，對資料達成保護效果。

完整的安全性標準選項

爲了確保無線通訊的安全性與私密性，提供數種市場上常見的無線安全標準。

有線對應隱私權(Wired Equivalent Privacy, WEP)是一種傳統的方法，使用 64-bit 或是 128-bit 金鑰透過無線收發裝置來加密每個資料訊框。通常無線基地台會事先配置一組含四個金鑰的設定，然後使用其中一個金鑰與每個無線用戶端通訊聯絡。

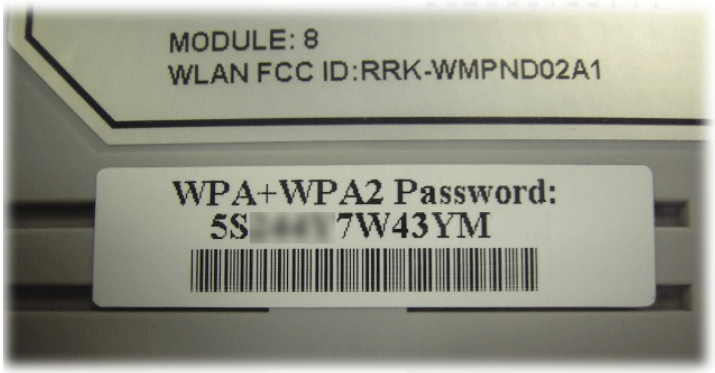
Wi-Fi 保護存取協定(Wi-Fi Protected Access, WPA)是工業上最佔優勢的安全機制，可分成二大類：WPA-personal 或稱爲 WPA Pre-Share Key (WPA/PSK)以及 WPA-Enterprise 又稱爲 WPA/802.1x。

在 WPA-Personal 機制中，會應用一個事先定義的金鑰來加密傳輸中的資料，WPA 採用 Temporal Key Integrity Protocol (TKIP) 加密資料而 WPA2 則是採用 AES，WPA-Enterprise 不只結合加密也還涵括驗證功能。

由於 WEP 已被證明是有弱點的，您可以考慮使用 WPA 作爲安全連線之用。您應該按照所需來選擇適當的安全機制，不論您選擇哪一種安全防護措施，它們都可以全方位的加強您無線網路上之資料保護以及/或是機密性。Vigor 無線路由器是相當具有彈性的，且能同時以 WEP 和 WPA 支援多種安全連線。

資訊

路由器提供預設安全性模式的密碼，在路由器底部的標籤中條列出來。對於想要透過此路由器登入網際網路的無線用戶，請於連線時記得輸入此預設的 PSK 號碼。



分隔無線與有線區域網路

可使您自有線區域網路中，分隔出無線區域網路以便隔離或是限制存取。隔離代表著雙方彼此都無法存取對方的資料，欲詳細說明商業用途之範例，您可以爲訪客設定一個無線區域網路，讓他們只能連接到網際網路而不必擔心洩露機密資訊。更彈性的作法是，您可以新增 MAC 位址的過濾器來區隔有線網路之單一使用者的存取行爲。

無線區域網路 - 無線用戶端列表

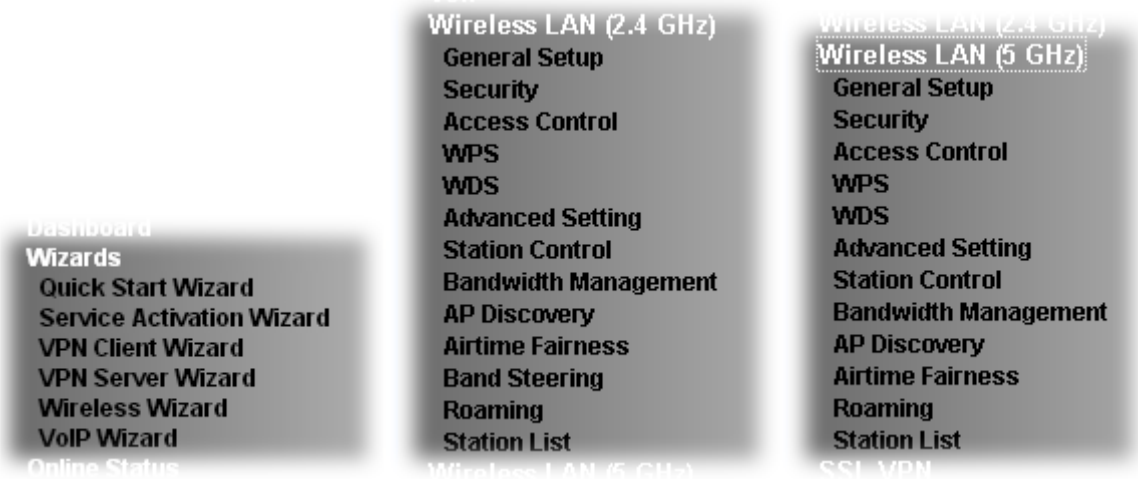
顯示無線網路中全部的無線用戶端以及連接狀態。

WPS

WPS (Wi-Fi Protected Setup) 提供簡易操作流程，讓無線用戶與無線基地台之間以 WPA 和 WPA2 之加密方式，成功完成網路連線。


AP Router
Connection via WPS
Wireless Client
Set SSID and Encryption (WPA/WPA2)
PBC
Pin Code
Wireless Card Installed

網頁使用者介面

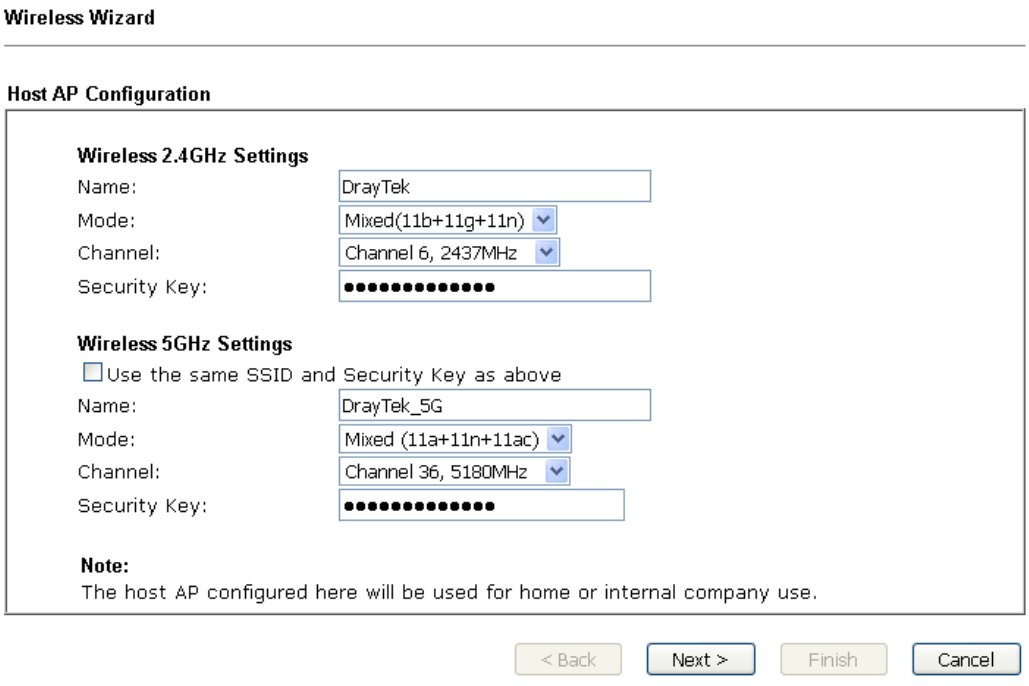


III-1-1 無線網路設定精靈(Wireless Wizard)

無線網路設定精靈允許您設定主機 AP(針對家庭用途或是公司內部運作)，以及指定客戶 AP(針對任何存取網際網路的無線用戶)之相關設定。

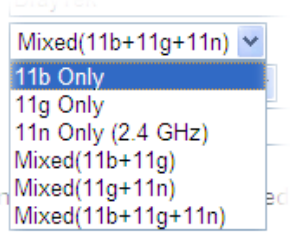
依照下列步驟進行：

1. 開啓**設定精靈>>無線設定精靈(Wizards>>Wireless Wizard)**。
2. 設定精靈頁面呈現如下，本頁針對公司或是家庭內部使用者而設定。此外細部設定內容會依照您所使用的路由器機種略有差異。本例是以 Vigor2926ac 爲範本。

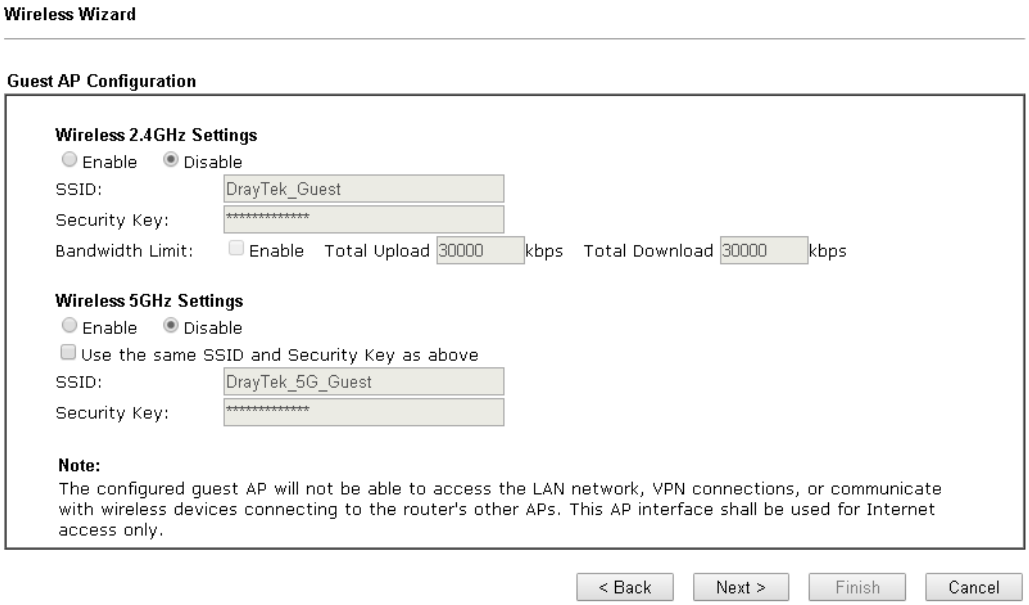


可用設定說明如下：

項目	說明

無線 2.4GHz 設定(Wireless 2.4GHz Settings)	
名稱(Name)	輸入路由器的 SSID 名稱(SSID1)。 預設名稱爲 DrayTek。
模式(Mode)	目前路由器提供的模式包含如圖各項，請選用綜合(11b+11g+11n)模式。 
頻道(Channel)	代表無線區域網路的頻率頻道，預設值爲 6，如果選定的頻道受到嚴重的干擾，您可以切換其他頻道，如果對於頻道選擇沒有特定的顧慮，請選擇自動即可。
密碼(Security Key	此精靈提供的無線網路密碼模式爲 WPA2/PSK。 WPA 利用密鑰針對傳輸的每個訊框進行加密作用，可利用手動輸入 PSK 或是透過 802.1x 驗證進行自動協商。 請輸入 8 至 63 個 ASCII 字元例如 012345678(或是 64 個十六進位數字且開頭爲 0x 的內容，如“0x321253abcde…”。
無線 5GHz 設定(Wireless 5GHz Settings) – 這個部份是當路由器支援無線網路 5GHz 時可用。	
使用相同 SSID 與密鑰 (Use the same SSID and Security Key as above)	勾選此方塊以使用上述相同之設定。
名稱(Name)	輸入路由器無線 5GHz 的 SSID 名稱(SSID2)。
模式(Mode)	目前路由器可以連接的模式。
頻道(Channel)	代表無線區域網路的頻率頻道，預設值爲 36，如果選定的頻道受到嚴重的干擾，您可以切換其他頻道，如果對於頻道選擇沒有特定的顧慮，請選擇自動即可。
密碼(Security Key)	此精靈提供的無線網路密碼模式爲 WPA2/PSK。 WPA 利用密鑰針對傳輸的每個訊框進行加密作用，可利用手動輸入 PSK 或是透過 802.1x 驗證進行自動協商。 請輸入 8 至 63 個 ASCII 字元例如 012345678(或是 64 個十六進位數字且開頭爲 0x 的內容，如“0x321253abcde…”。
下一步(Next)	按此進入下一個設定頁面。
取消(Cancel)	按此離開設定精靈，任何設定變更將無法儲存。

3. 輸入完畢必要資訊之後，按**下一步(Next)**。本頁的內容限制無線站台(即客戶端)登入網際網路，但無法分享區域網路(LAN)以及虛擬網路(VPN)的連線。



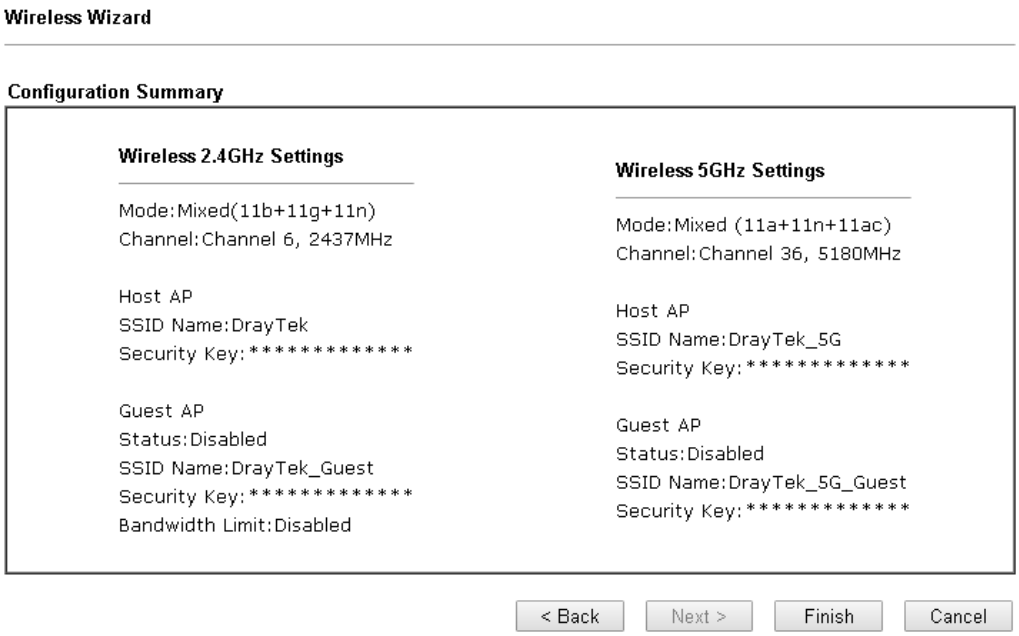
可用設定說明如下：

項目	說明
無線 2.4GHz 設定(Wireless 2.4GHz Settings)	
啓用/停用 (Enable/Disable)	啓用或是停用本頁的設定。
名稱(SSID)	輸入路由器的 SSID 名稱(SSID1) 。
密碼 (Security Key)	此精靈提供的無線網路密碼模式爲 WPA2/PSK。 WPA 利用密鑰針對傳輸的每個訊框進行加密作用，可利用手動輸入 PSK 或是透過 802.1x 驗證進行自動協商。 請輸入 8 至 63 個 ASCII 字元例如 012345678(或是 64 個十六進位數字且開頭爲 0x 的內容，如“0x321253abcde...”。
頻寬限制(Bandwidth Limit)	**啓用(Enable)** – 勾選此框以進行頻寬限制設定。控制透過無線連線的資料傳輸速度。 **上傳(Upload)** – 勾選啓用方塊之後，接著輸入資料上傳的速度，預設值爲 30,000 kbps。 **下載(Download)** – 勾選啓用方塊之後，接著輸入資料下載的速度，預設值爲 30,000 kbps。
無線 5GHz 設定(Wireless 5GHz Settings)	
啓用/停用 (Enable/Disable)	啓用或是停用本頁的設定。
使用上述相同的 SSID 與密鑰(Use the same SSID and Security Key as above)	勾選此方框使用上述相同的設定。
名稱(SSID)	輸入路由器的 SSID 名稱(SSID2) 。
密碼 (Security Key)	此精靈提供的無線網路密碼模式爲 WPA2/PSK。 WPA 利用密鑰針對傳輸的每個訊框進行加密作用，可利用手動輸入 PSK 或是透過 802.1x 驗證進行自動協商。

	請輸入 8 至 63 個 ASCII 字元例如 012345678(或是 64 個十六進位數字且開頭爲 0x 的內容，如“0x321253abcde...”。
下一步(Next)	按此進入下一個設定頁面。
取消(Cancel)	按此離開設定精靈，任何設定變更將無法儲存。

4. 輸入完上述資訊之後，按**下一步(Next)**。

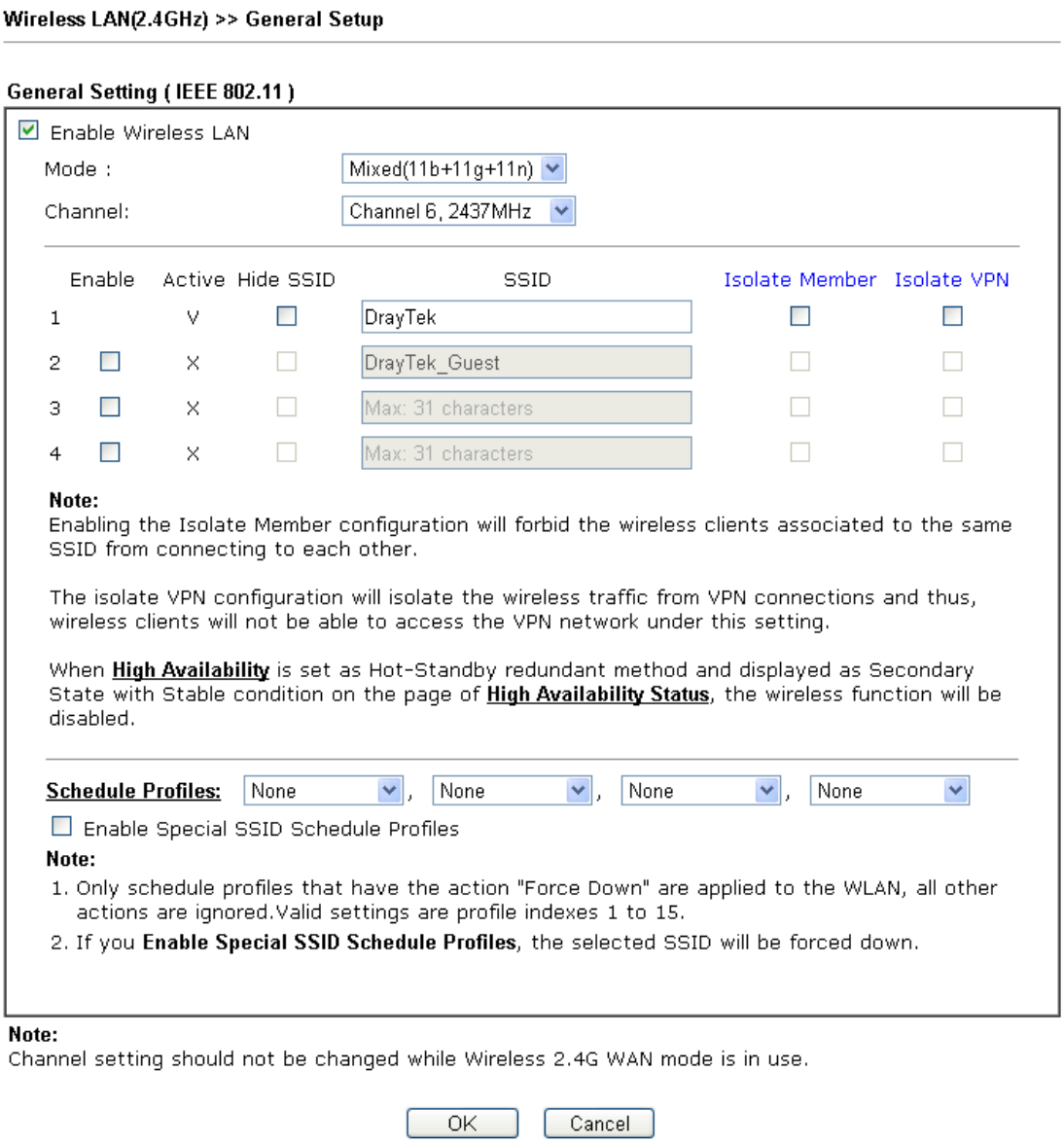
5. 接著螢幕會顯示無線設定的摘要內容。



6. 若無任何疑問，按下**完成(Finish)**按鈕來結束設定。

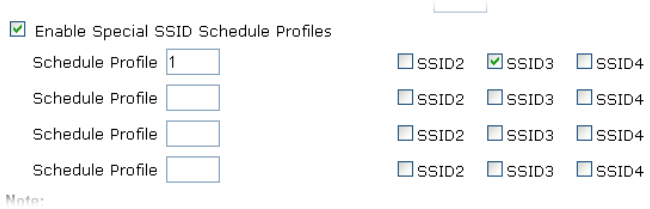
III-1-2 基本設定(General Setup)

按下**基本設定(Wireless LAN>>General Setup)**連結，新的網頁即會開啓，您可以設定 SSID 和無線頻道資訊，請參考下圖：



可用設定說明如下：

項目	說明
啓用(Enable Wireless LAN)	勾選此方塊啓動無線功能。
模式(Mode)	請選擇一個適當的無線模式。可選之無線模式依照所安裝之路由器機種而定。 **Note**: 802.11b/g 用於 2.4G 頻；802.11a 用於 5G 頻；802.11n 用於 2.4G 或是 5G 頻；802.11ac 用於 5G 頻
頻道(Channel)	無線區域網路的通道頻率，802.11n 與 802.11ac 的預設頻道是不同的，如果選定的頻道受到嚴重的干擾的話，您可自行切換爲其他頻道。

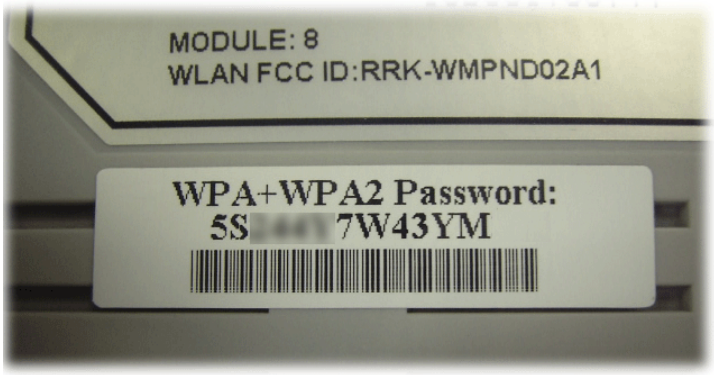
隱藏 SSID (Hide SSID)	勾選此方塊，防止他人得知 SSID 值，未知此路由器的 SSID 之無線用戶在搜尋網路時，看不到 Vigor 無線路由器的訊息。
SSID	預設的 SSID 值爲 **DrayTek**，建議您變更爲另一個特殊名稱。它是無線區域網路的身分辨識碼，SSID 可以是任何文字、數字或是各種特殊字元。
隔離(Isolate)	**VPN** – 勾選此方塊讓使用相同 VPN 的無線用戶無法存取彼此的電腦資料。 **成員(Member)**– 勾選此方塊讓使用相同 SSID 的無線用戶彼此無法存取對方資料。
排程設定檔(Schedule Profiles)	設定無線區域網路在特定的時間間隔中運作。您可以從**應用**的**排程設定(Applications >> Schedule)**頁面上，自 15 個排程中選擇 4 個，本區預設值是空白的，表示無線功能是永遠可以運作的狀態。
啓用特殊 SSID 排程設定檔 (Enable Special SSID Schedule Profiles)	選定的 SSID (2 /3 /4) 將在使用的排程設定檔安排下，強行上線/下線。 

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

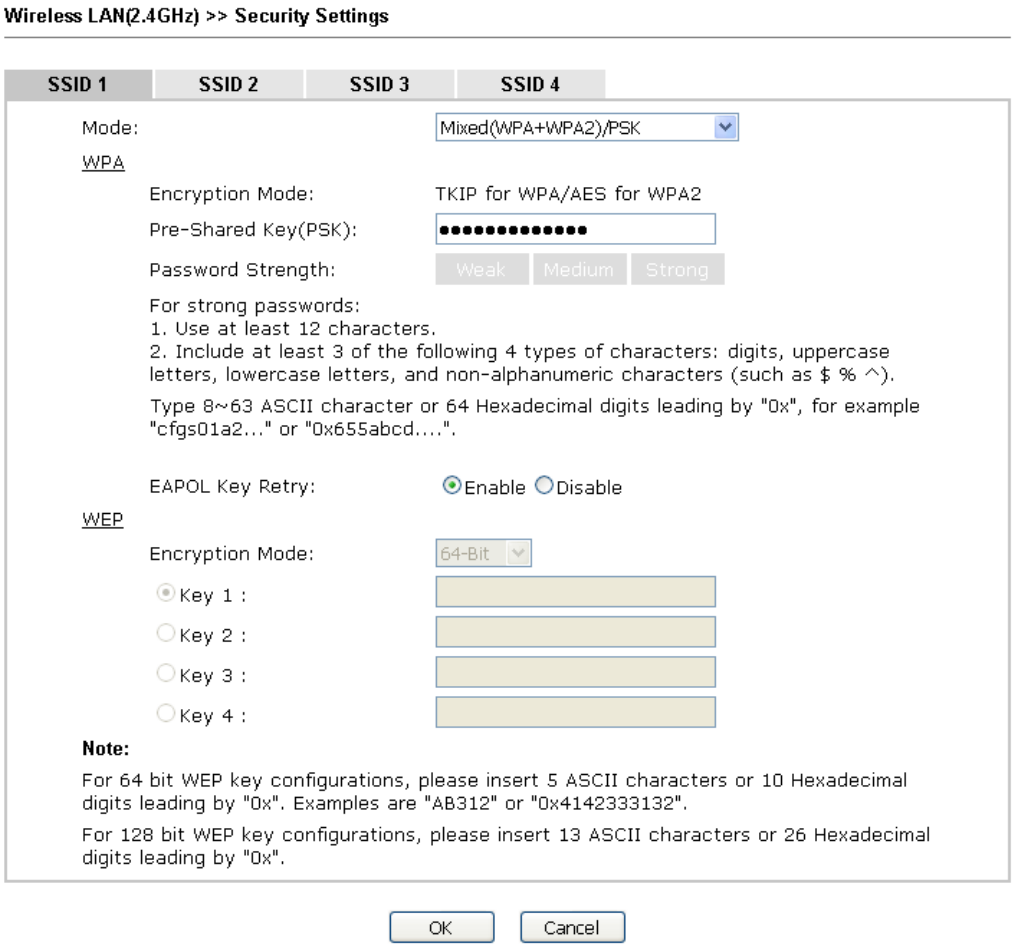
III-1-3 安全性設定(Security)

本頁讓使用者對 SSID 1,2,3 及 4 設定不同模式的安全性規則，設定完後，請按下**確定(OK)**按鈕儲存所有的變更。

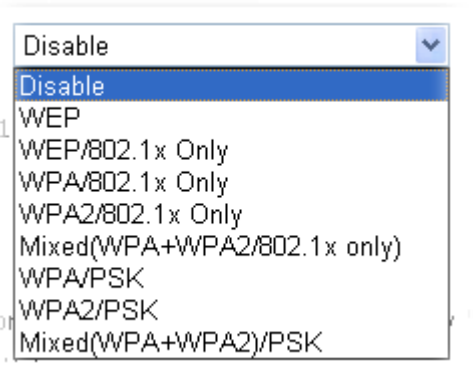
路由器提供預設安全性模式的密碼，在路由器底部的標籤中條列出來。對於想要透過此路由器登入網際網路的無線用戶，請於連線時記得輸入此預設的 PSK 號碼。

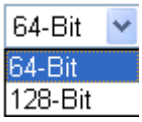


選擇**安全性設定(Security Settings)**後，新的網頁將會出現，您可以在此頁面上調整 WEP 和 WPA 設定。



可用設定說明如下：

項目	說明
模式(Mode)	此一設定有數種模式可供您選擇。  **資訊** 若有選擇了 802.1x 模式，那麼您也可以同時設定 **無線區域網路(2.4GHz) 802.1X 設定(Wireless LAN(2.4GHz) 802.1X Setting)**。 **停用(Disable)** - 關閉加密機制。 **WEP -** 只接受 WEP 用戶以及僅接受以 WEP 金鑰輸入的加密鑰匙。

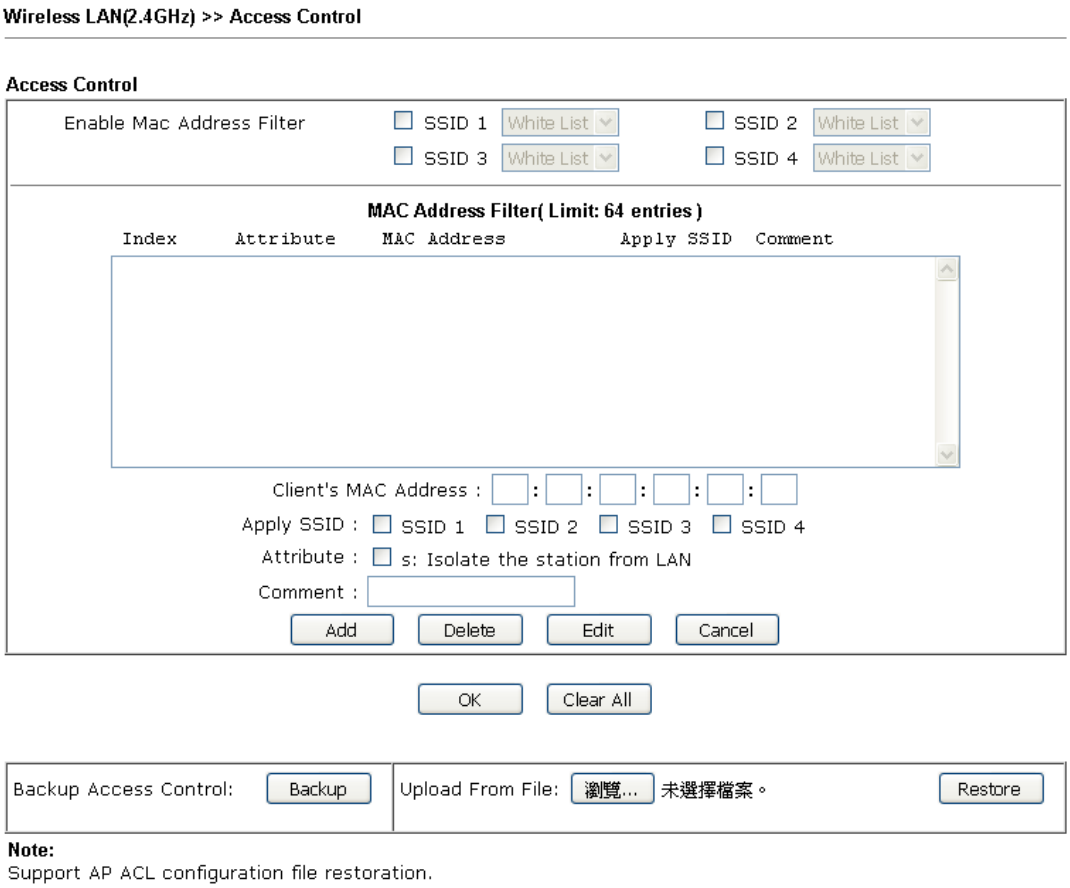
	器(含 802.1X 協定)動態分配之密鑰。 **WPA/802.1x Only -** 僅接受 WPA 用戶端以及得自 RADIUS 伺服器(含 802.1X 協定)動態分配之密鑰。 **WPA2/802.1x Only -** 僅接受 WPA2 用戶端以及得自 RADIUS 伺服器(含 802.1X 協定)動態分配之密鑰。 **Mixed (WPA+WPA2/802.1x only) -**.同時接受 WPA 與 WPA2 用戶端以及得自 RADIUS 伺服器(含 802.1X 協定)動態分配之密鑰。 **WPA/PSK -**接受 WPA 用戶，請在 PSK 中輸入加密金鑰。 **WPA2/PSK -**接受 WPA2 用戶，請在 PSK 中輸入加密金鑰。 **綜合(WPA+ WPA2)/PSK (Mixed(WPA+ WPA2)/PSK) -** 同時接受 WPA 與 WPA2 用戶，請在 PSK 中輸入加密金鑰。
WPA	WPA 可藉由金鑰加密每個來自無線網路的訊框，可在本區手動輸入 PSK，或是藉由 802.1x 驗證方式來自動加密。 **預先共用金鑰 (Pre-Shared Key (PSK))** - 輸入 **8~63** 個 ASCII 字元，像是 012345678(或是 64 個 16 進位數字，以 0x 開頭，如 0x321253abcde…等)。 **密碼強度**-系統將會顯示密碼強度(以極弱、中度、極強等文字來表示)。
WEP	**64-Bit** - 針對 64 位元的 WEP 金鑰，請輸入 5 個 ASCII 字元，像是 12345（或是 10 個 16 進位數字，以 0x 開頭，如 0x4142434445）。 **128-Bit** - 針對 128 位元的 WEP 金鑰，請輸入 13 個 ASCII 字元，像是 ABCDEFGHIJKLM（或是 16 個 16 進位數字，以 0x 開頭，如 0x4142434445）。  所有的無線裝置都必須支援相同的 WEP 加密位元大小，並擁有相同的金鑰。這裡可以輸入四組金鑰，但一次只能選擇一組號碼來使用，這些金鑰可以 ASCII 文字或是 16 進位元字元來輸入。請點選您想使用的金鑰組別。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

III-1-4 連線控制(Access Control)

爲了增加額外的無線存取安全性，連線控制頁面可讓您透過無線區域網路的用戶 MAC 位址來限制網路存取動作。

在連線控制頁面上，路由器可透過黑白名單的方式，進行封鎖 MAC 位址來限制無線用戶端存取無線網路。對於想封鎖的無線用戶，使用者可將其 MAC 位址放入黑名單中；或是讓用戶的 MAC 位址放入白名單，使無線用戶得以通行。



可用設定說明如下：

項目	說明
啓動 MAC 位址過濾器 (Enable Mac Address Filter)	請勾選任一 SSID 1 到 4 中以啓動無線 LAN 的 MAC 位址過濾器。下述方框中所有的無線用戶(以 MAC 位址表示)都可分別群組在不同的無線區域網路中，比方說假設您同時勾選了 SSID 1 及 SSID 2，那麼無線用戶將在 SSID 1 與 SSID 2 下群組起來。
MAC 位址過濾 (MAC Address Filter)	顯示之前編輯的全部 MAC 位元址。
客戶端的 MAC 位址 (Client's MAC Address)	請手動輸入無線用戶端的 MAC 位址。
套用 SSID (Apply SSID)	輸入用戶的 MAC 位址之後，勾選 SSID 的方框即可將其與 MAC 位址同時套入連線控制。
特性(Attribute)	**s -**勾選此項以便隔離無線用戶端之無線連線。
註解(Comment)	針對用戶端 MAC 位址輸入簡單的說明。

新增(Add)	新增新的 MAC 位址於清單上。
刪除(Delete)	刪除清單中選定的 MAC 位址。
編輯(Edit)	編輯清單中選定的 MAC 位址。
取消(Cancel)	放棄連線控制設定。
確定(OK)	按此鈕儲存連線控制清單。
全部清除(Clear All)	按此鈕儲存連線控制清單。
備份存取控制(Backup Access Control)	此頁面的設定可以儲存成一個檔案，後續可在此裝置還原使用或是套用至其他裝置使用。
自檔案上傳(Upload From File)	還原無線存取控制設定並套用到此裝置上。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

III-1-5 WPS

WPS (Wi-Fi Protected Setup) 提供簡易操作流程，讓無線用戶與無線基地台之間以 WPA 和 WPA2 之加密方式，成功完成網路連線。

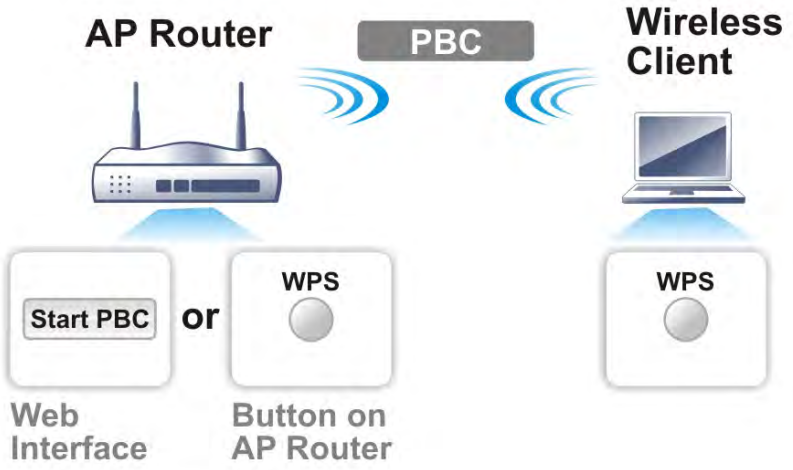


資訊	此功能僅在無線用戶端也支援 WPS 功能時可用。

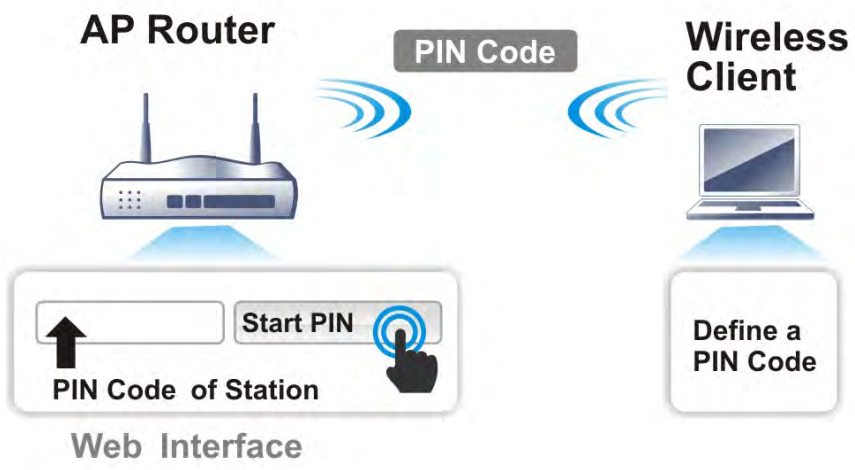
建立無線網路用戶與Vigor路由器之間的連線有個快速及簡單的方式，使用者不需要每次都必須選擇加密模式，或輸入任何長篇的資料以建立無線連線。使用者只要按下無線用戶端中的一個小小按鈕，WPS功能就會替他/她自動建立一個無線連線。

透過基地台與無線用戶之間的WPS來達成無線連線，有二個方式可以進行，一個是壓下*Start PBC*按鈕，一個是利用*PIN Code*來進行。

- Vigor 2926系列這一端，角色如同無線基地台，可按下路由器面板上的 **WPS** 按扭一次或是按網頁設定頁面上的 **Start PBC** 按鈕一次即可。而在無線用戶那一端，(確保網路卡已經安裝完畢)，則按下網路卡網頁畫面所提供的 **Start PBC** 按鈕。



- 保網路卡已經安裝完畢)，則按下網路卡網頁畫面所提供的 **Start PBC** 按鈕。

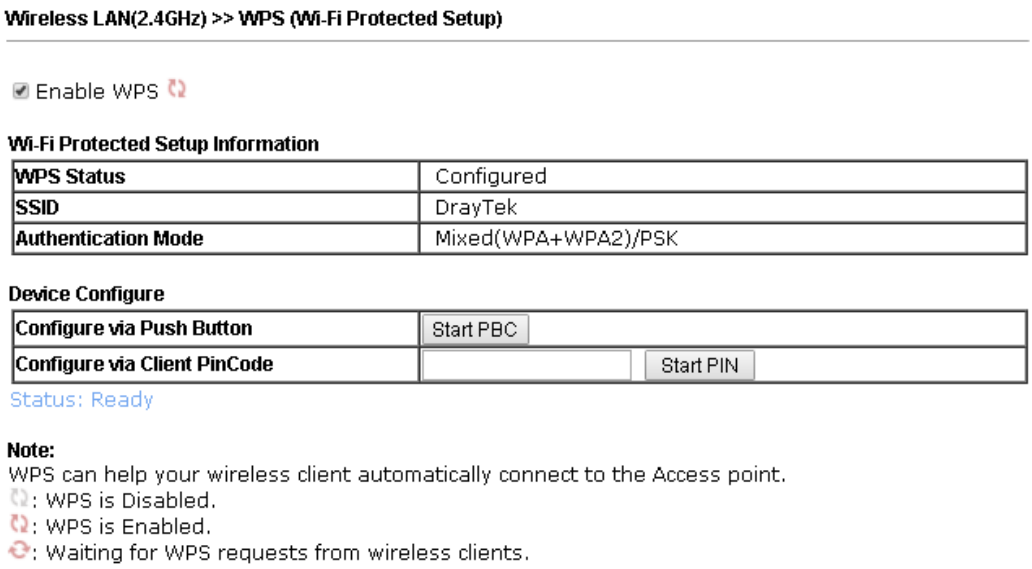


因爲 WPS 僅在 WPA-PSK 或 WPA2-PSK 模式下可用，如果您沒有在**無線區域網路>>安全性設定(Wireless LAN>>Security)**選擇此模式，您會看到如下的訊息。



請按下**確定(OK)**鈕，然後回到**無線區域網路>>安全性設定(Wireless LAN>>Security)**頁面，選擇 WPA-PSK 或 WPA2-PSK 模式，再進入 WPS 頁面。

下圖爲**線區域網路>>WPS(Wireless LAN>>WPS)**網頁畫面。



可用設定說明如下：

項目	說明
啓用 WPS (Enable WPS)	勾選此方塊啓動 WPS 設定。
WPS 狀態(WPS Status)	顯示 WPS 相關的系統訊息，如果無線安全性(加密)功能已設定，您可以在此看到"設定完畢"等訊息。
SSID	顯示路由器的 SSID1 名稱，WPS 僅在 SSID1 中可用。
驗證模式 (Authentication Mode)	顯示路由器目前的驗證模式，請注意僅有 WPA2/PSK 和 WPA/PSK 支援 WPS。
藉由 Push 按鈕來設定 (Configure via Push Button)	請按**啓動 PBC(Start PBC)** 啓用 Push-Button 式的 WPS 設定程式，路由器將會等待 2 分鐘取得無線用戶傳送過來的 WPS 需求，當 WPS 運作時，WLAN 燈號將會快速閃爍，2 分鐘後，路由器會回復一般的運作(您必須在 2 分鐘內設定 WPS)。
藉由用戶端 PinCode 來設定 (Configure via Client PinCode)	請輸入您想要連接的無線用戶所指定的 PIN 碼，在按**啓動 PIN(Start PIN)** 按鈕。當 WPS 運作時，WLAN 燈號將會快速閃爍，2 分鐘後，路由器會回復一般的運作(您必須在 2 分鐘內設定 WPS)。

III-1-6 WDS

WDS 表示無線分派系統，是一個連結二個無線基地台的通訊協定，通常可以下列二種方式來應用。

- 提供二個區域網路間空中交流的橋樑
- 延長無線區域網路的涵蓋範圍

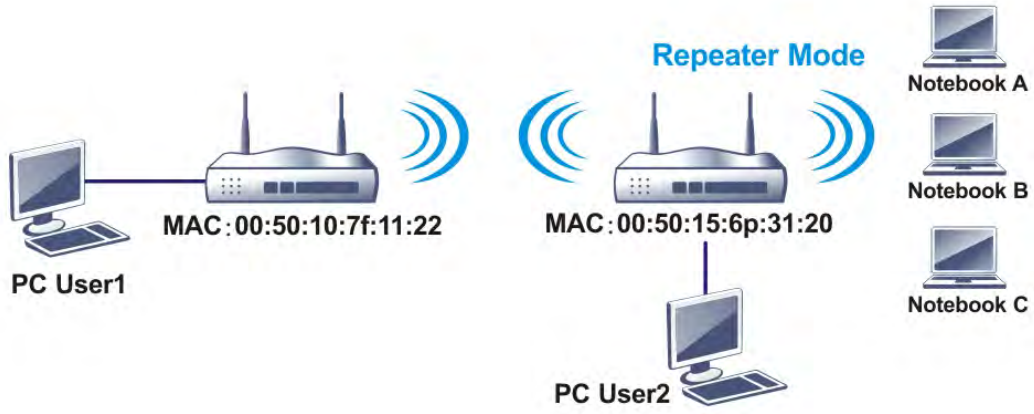
參考如下表格：

WDS 模式	無線訊號	差異比較
橋接 (Bridge)	受限	● 在無線訊號有效範圍內的無線站台(用戶端)可以透過路由器/AP 存取網際網路 ● 超出無線訊號有效範圍內的無線站台(用戶端)**無法**透過路由器/AP 的橋接(Bridge)模式存取網際網路 ● 來自 WDS 連結的封包僅能被轉發至本地有線或是無線主機
中繼 (Repeater)	延伸	● 在無線訊號有效範圍內的無線站台(用戶端)可以透過路由器/AP 存取網際網路 ● 超出無線訊號有效範圍內的無線站台(用戶端)**可以**透過路由器/AP 的中繼(Repeater)模式存取網際網路 ● 來自路由器的封包可以藉由 WDS 連結 repeat 到另一台 AP(遠端)上 ● 僅有中繼(Repeater)模式可以進行 WDS-to-WDS 封包轉發

迎合以上的需要，路由器可應用二種 WDS 模式，一爲**橋接(Bridge)**一爲**中繼(Repeater)**，下圖顯示 WDS 橋接介面的功能：

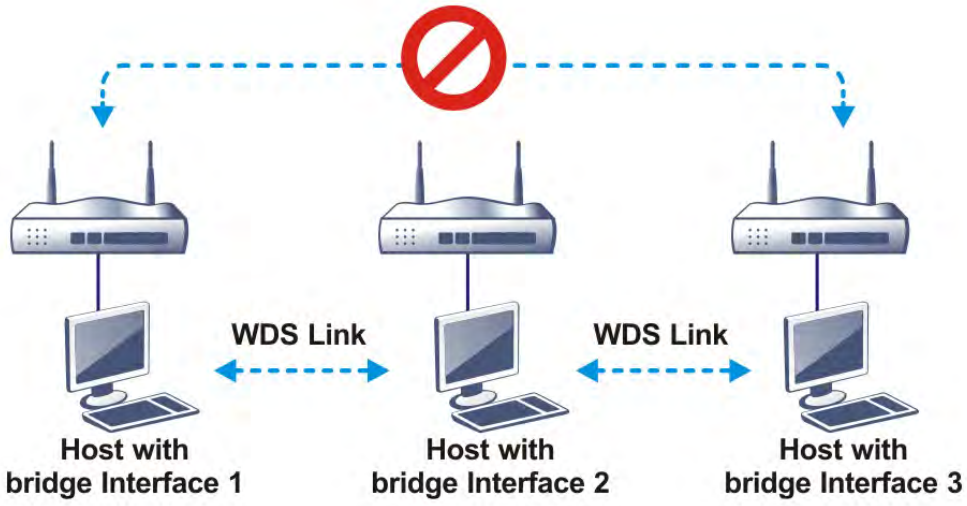


WDS-中繼模式的應用則描繪如下：

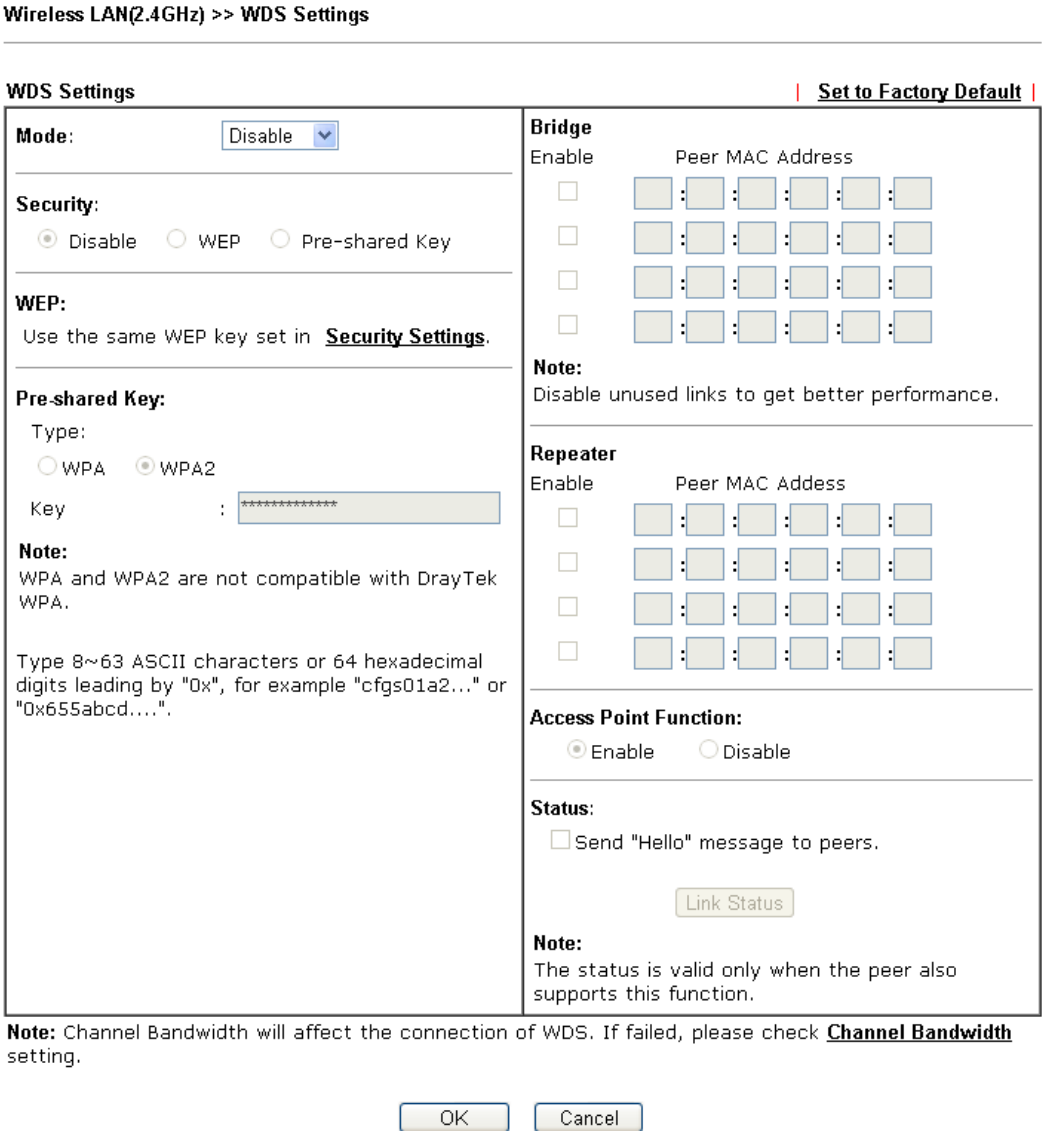


二種模式的主要不同點在於：**中繼(Repeater)**模式下，從一端 AP 過來的封包可以透過 WDS 連結再另一個 AP 上重複產生，WDS 連結傳送過來的封包只能轉送至本機有線或無線的主機。-而橋接(Bridge)模式，來自 WDS 連結的封包僅能轉發至本機有線或無線主機上。換言之，只有中繼模式能完成 WDS 到 WDS 封包轉送的工作

在下面這個例子當中，連接至橋接介面 1 或 3 的主機可以透過 WDS 連結與橋接介面 2 相連。不過連接至橋接 1 的主機無法透過橋接介面 2 與橋接介面 3 的主機相通。



按**無線區域網路(Wireless LAN)**中的 **WDS** 功能以出現如下畫面：



可用設定說明如下：

項目	說明
模式(Mode)	選擇 WDS 設定模式，**停用(Disable)**將無法啓用任何 WDS 設定；**橋接(Bridge)**模式乃是設計用來符合第一種實際之應用；**中繼(Repeater)**模式則是設計用來符合第二種實際之應用。 
安全性(Security)	有三種安全性類型可選擇，**停用(Disable)**、**WEP** 和預設共用金鑰**(Pre-shared key)**。您在此處所選擇的設定將會使得 WEP 或是預設共用金鑰有效或是無效。請自三種中挑選出一種。
WEP	當選擇 **WEP** 爲安全性模式時，路由器將會使用於**無限區域網路>>安全性設定(Wireless LAN>>Security Settings)**中設定的 WEP 金鑰內容。 請務必確認 WEP 模式與 WEP 金鑰設定都已經在**無限區域網路>>安全性設定(Wireless LAN>>Security Settings)**頁面中設定完畢。

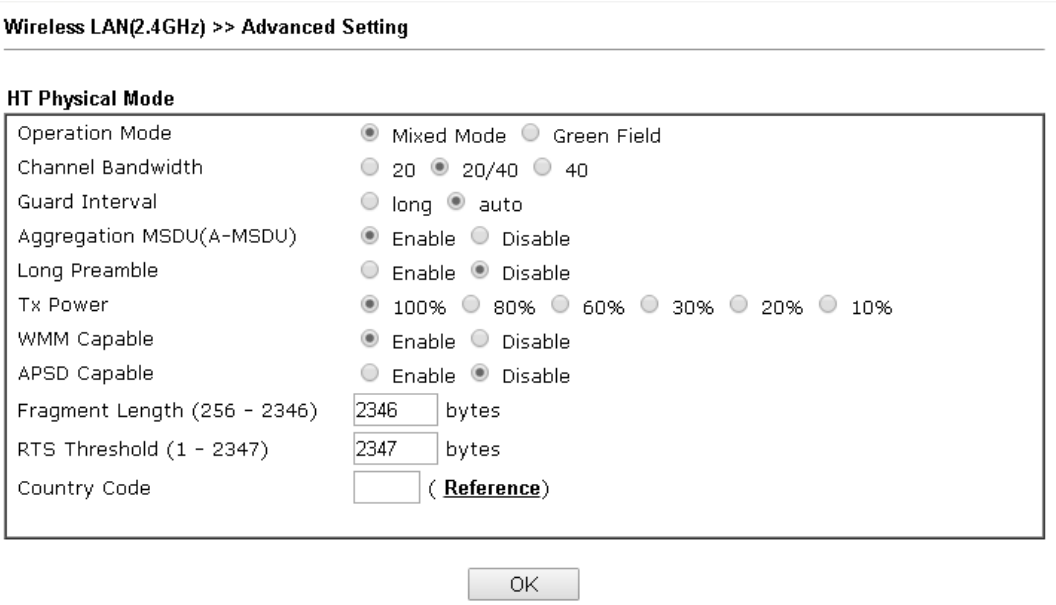
	附註: 若在**無限區域網路>>安全性設定(Wireless LAN>>Security Settings)**頁面中設定的安全性模式與此處設定的模式不同，系統會發出警告訊息，提醒您並要求您務必確保雙邊的設定一致。
預設共用金鑰 (Pre-shared Key)	當選擇**預設共用金鑰(Pre-shared Key)**爲安全性模式時，視需要設定如下項目： **類型(Type) –** 有數種類型可以選擇，您可以設定 WPA 或是 WPA2 爲加密模式，建立 AP 與路由器之間的 WDS 系統。 **金鑰(Key) –** 請在此區設定加密金鑰，輸入開頭爲"0x"之 8 ~ 63 個 ASCII 字元或是 64 的 16 進位的數字。
橋接 (Bridge)	如果您選擇橋接做爲通訊模式，請在此區輸入對方的 MAC 位址，本頁可讓您一次輸入六個對方 MAC 位址。停用不使用的連結可以取得較好的執行效果，如果您想要啓動對方的 MAC 位址，記得輸入完成後勾選**啓用(Enable)**方塊。
中繼(Repeater)	如果您選擇**中繼(Repeater)**做爲通訊模式，請在此區輸入對方的 MAC 位址，本頁可讓您一次輸入二個對方 MAC 位址。同樣的，如果您想要啓動對方的 MAC 位址，記得輸入完成後勾選**啓用(Enable)**方塊。
無線基地台功能 (Access Point Function)	當選擇中繼作爲 WDS 模式時，按**啓用(Enable)**讓路由器提供無線基地台的服務；若是選擇橋接作爲 WDS 模式，則請按**停用(Disable)**取消此功能。
狀態(Status)	允許使用者傳送招呼訊息給對方，然而則此功能僅在對方也支援時才有效用。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

III-1-7 進階設定(Advanced Setting)

本頁允許用戶設定進階項目，例如操作模式、頻道頻寬、防護間隔以及 aggregation MSDU 等無線資料傳輸設定。

對於“n, ac”等機型 ---



可用設定說明如下：

項目	說明
操作模式 (Operation Mode)	**混合模式(Mixed Mode)** – 路由器可以 802.11a/b/g 和 802.11n 標準所支援的方式來傳送資料，但是若 802.11g 或 802.11b 無線用戶連接上此路由器的話，整個網路傳輸速率將會降低。 **Green Field** – 爲了取得較高的處理能力，請選擇此項模式。此模式僅讓資料在 11n 系統中傳輸。另外，此模式也沒有防護機制好避免與相鄰採用 802.11a/b/g 的裝置產生衝突。
頻道頻寬 (Channel Bandwidth)	**20-** 路由器使用 20Mhz 作爲基地台與無線用戶之間傳輸的資料速度。 **40-** 路由器使用 40Mhz 作爲基地台與無線用戶之間傳輸的資料速度。 **20/40 -** 路由器使用 20Mhz 或 40Mhz 作爲基地台與無線用戶之間傳輸的資料速度。此選項可以增加資料傳輸的成效。
防護間隔 (Guard Interval)	確保宣傳延遲的安全性以及敏感數位資訊的反映，如果您選擇**自動(auto)**的話，基地台路由器將依照無線用戶的能力，選擇較短的間隔(增加無線性能-)或是較長的間隔來傳輸資料。
Aggregation MSDU	Aggregation MSDU 可整合不同大小的選框，用來改善某些品牌用戶的 MAC 層級成效，預設值爲**啓用(Enable)**。
長封包標頭(Long Preamble)	此選項用來定義 802.11 封包中同步區塊的長度，最新的無線網路以 56 bit 同步區來使用短封包標頭，而不是以 128 bit 同步區來使用長封包標頭。不過，一些原始 11b 無線網路裝置只有支援長封包標頭而已，因此如果您需要和此種裝置通訊溝通的話，請勾選此方塊。

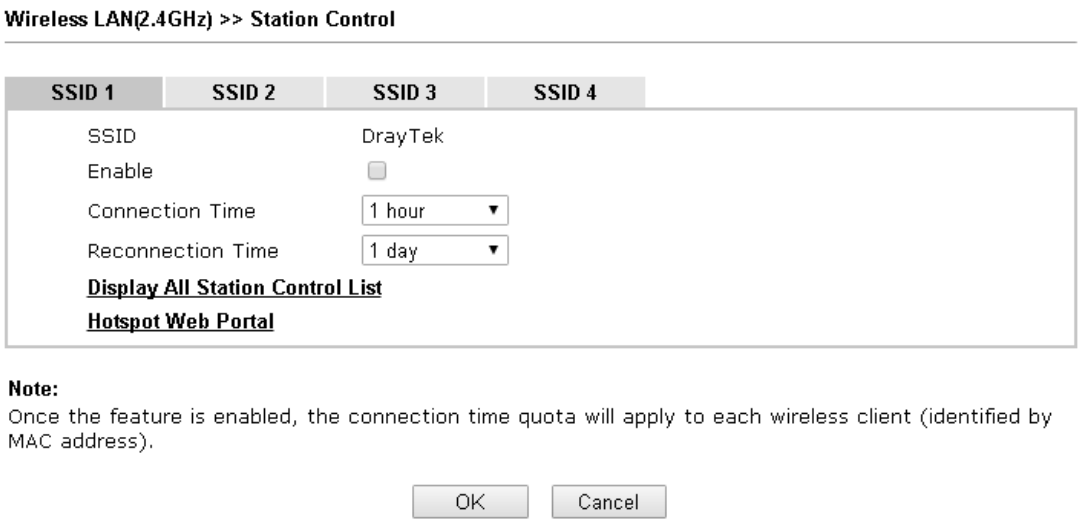
傳輸電力(Tx Power)	設定裝置的傳輸訊號的電力百分比，數值越大，訊號密度越高。
WMM Capable	WMM 爲 Wi-Fi Multimedia 的縮寫，定義從 802.1d 衍生的四種存取類型錄的優先層級，這些類型都是針對流量、聲音、影像特別設計的，此四種類型分別是 - AC_BE , AC_BK, AC_VI and AC_VO。 在無線資料傳輸中應用 WMM 參數，請按**啓用(Enable)**鈕。
APSD Capable	自動省電模式(APSD, automatic power-save delivery)是 Wi-Fi 網路支援的強化省電機制，允許裝置花較多時間休眠，並透過縮小傳輸延遲時間，花費少許電力來改善成效。 預設值爲**停用(Disable)**。
訊框長度(256 – 2346) **(Fragment Length (256 – 2346))**	設定無線信號的訊框門檻值，如果不清楚此功能作用，則毋須變更預設值，預設值爲 2346。
RTS 門檻值(1 – 2347) **(RTS Threshold (1 – 2347))**	縮減隱藏用戶端間的碰撞數以改善無線的成效。 設定無線訊號的 RTS 門檻值，如果不清楚此功能作用，則毋須變更預設值，預設值爲 2347。
國家代碼(Country Code)	Vigor 路由器依循 802.11d 標準廣播國家代碼，然而某些無線站台會偵測/掃描國家代碼以避免衝突的發生，若是偵測到衝突，無線站台將會收到警告且無法進行網路連線，因此改變國碼可以確保特定用戶時刻皆擁有成功的網路連線。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

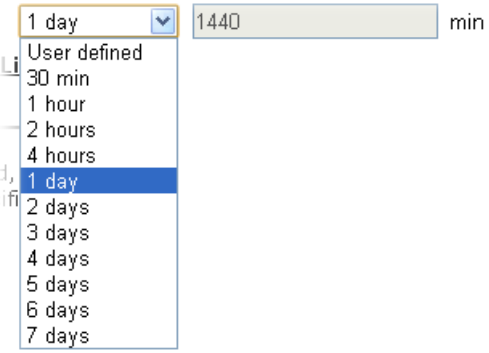
III-1-8 無線用戶控制(Station Control)

無線用戶控制(Station Control)用於指定無線用戶連接與重新連接 Vigor 路由器的時間，如果沒有啓用此功能，無線用戶可以一直連線路由器，直到路由器關機爲止。

對免費 Wi-Fi 服務而言，此功能相當有用，比方說咖啡車每日提供免費一小時無線服務給予顧客，那麼連線時間可以設定爲 1 小時，重新連線可以設定爲 1 日，如此顧客可以在一小時內完成工作，不會長期佔據無線網路。



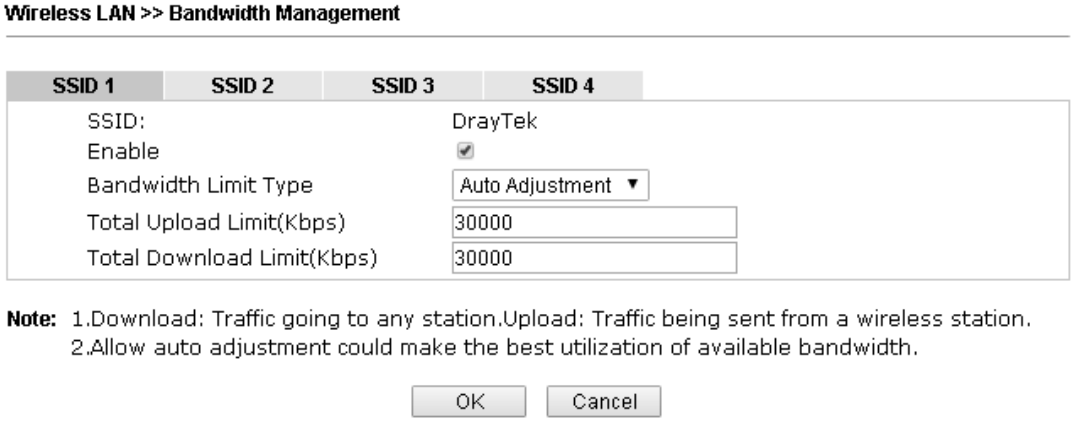
可用設定說明如下：

項目	說明
SSID	顯示無線用戶連接 Vigor 路由器使用的 SSID。
啓用(Enable)	勾選此框啓用此功能。
連線時間/重新連線時間 (Connection Time / Reconnection Time)	使用下拉式清單選擇連線/重新連線 Vigor 路由器的時間，如果選擇**使用者設定(User defined)**，請手動輸入連線時間。 
顯示所有的無線用戶清單 (Display All Station Control List)	顯示所有透過此 SSID 連線至 Vigor 路由器的無線用戶清單。
客製化入口網站(Hotspot Web Portal)	按此連結可開啓**客製化入口網站(Hotspot Web Portal)**設定頁面進行修改。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

III-1-9 頻寬管理(Bandwidth Management)

來自 FTP, HTTP 或是某些 P2P 應用程式的上傳或是下載都會佔據大量的頻寬，且影響其他應用程式的運作。請使用頻寬管理功能讓頻寬的運用更有效率。



可用設定說明如下：

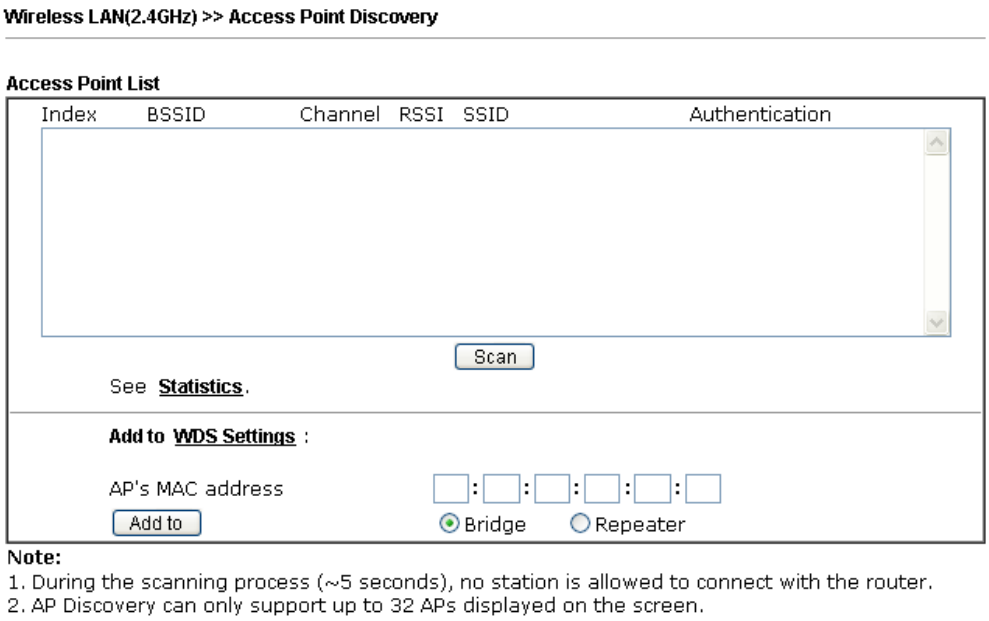
項目	說明
SSID	顯示 SSID 名稱。
啓用(Enable)	勾選此框以啓用用戶端的頻寬管理機制。
頻寬限制類型(Bandwidth Limit Type)	**自動調整(Auto Adjustment) -** 系統自動決定頻寬限制。 **每台無線站台限制(Per Station Limit)** – 依照無線用戶決定頻寬的限制。
全部上傳限制(Total Upload Limit)	當選擇自動調整(Auto Adjustment)爲頻寬限制類型，可設定此項目。 輸入用來限制全部無線用戶連接至路由器的最大資料流量(上傳)之數值。
全部下載限制(Total Download Limit)	當選擇自動調整(Auto Adjustment)爲頻寬限制類型，可設定此項目。 輸入用來限制全部無線用戶連接至路由器的最大資料流量(下載)之數值。
上傳限制(Upload Limit)	當選擇每台無線站台限制(Per Station Limit)爲頻寬限制類型，可設定此項目。 輸入用來限制單一無線用戶連接至路由器的最大資料流量(上傳)之數值。
下載限制(Download Limit)	當選擇每台無線站台限制(Per Station Limit)爲頻寬限制類型，可設定此項目。 輸入用來限制單一無線用戶連接至路由器的最大資料流量(下載)之數值。

完成設定之後，按下確定(OK)按鈕儲存相關設定。

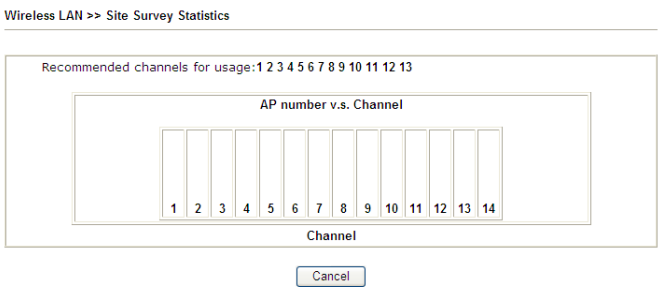
III-1-10 搜尋無線基地台(AP Discovery)

路由器可以掃描全部的頻道以及發現鄰近地區運作中的無線基地台，基於掃描的結果，使用者將會知道哪個頻道是可用的，此外它也可以用來發現 WDS 連結中的無線基地台，注意在掃描過程中(約 5 秒)，任何一台無線用戶都不可以連接上路由器。

本頁可用來掃描無線區域網路中的無線基地台的存在，不過只有與路由器相同頻道的無線基地台可以被發現，請按**掃描(Scan)**按鈕尋找所有相連的無線基地台。



可用設定說明如下：

項目	說明
掃描(Scan)	用來尋找所有相連的無線基地台，搜尋結果將會顯示在按鈕上方的方框中。
統計(Statistics)	顯示基地台所使用的頻道統計資料。 
新增(Add to)	您想要找到套用 WDS 設定的無線基地台，請在本頁底部輸入該 AP 的 MAC 位址，並點選橋接(Bridge)或是中繼(Repeater)模式，然後按**新增(Add to)**，稍後該 MAC 位址即會加入 WDS 設定頁面中。

III-1-11 無線頻寬均化(Airtime Fairness)

無線頻寬均化在那些必須支援關鍵企業應用程式的無線網路運用中是相當重要的。

大部分的應用不是同步進行就是須要更多的下載連結能力(非上傳能力)，電話與電子郵件在每個方向都會傳送相同數額的資料，而比起其他方式，影音串流和網頁瀏覽涉及到更多來自基地台的流量。這個功能可確保預測的成效與服務品質，允許使用 802.11n 及後續無線用戶都能同時共存在相同的網路下。若無無線頻寬均化，使用綜合模式的辦公室就會冒著讓傳統客戶拖慢整個網路的風險，或是讓速度較快的用戶排擠到其他用戶。

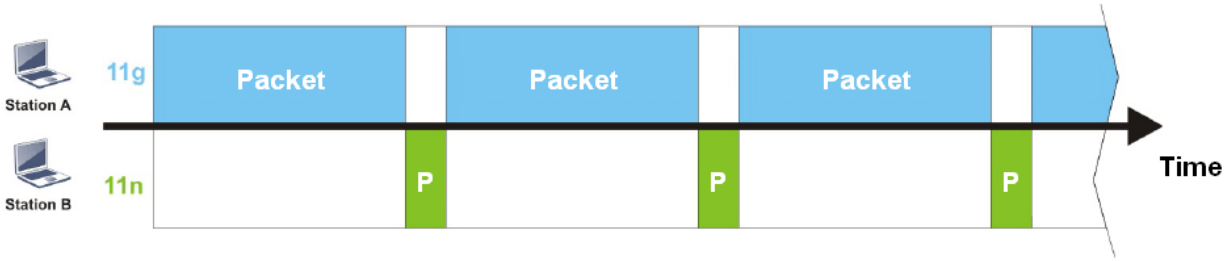
透過此功能，每個用戶在給定的 QoS 層級下能擁有平等機會存取空中無線網路。

同一時間僅容許一個無線站台存取特定無線頻道。

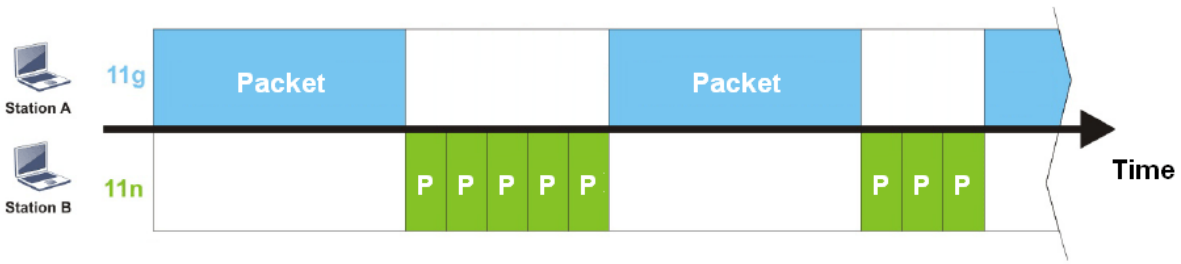
IEEE802.11 頻道存取機制的原理在於每個站台都具有同等的概率使用無線頻道。當無線站台們都有相同的資料傳輸速率時，這個原理可引導一個較爲公平的結果，在這種情況下，無線站台們都可以取得相同的頻道存取時間。

不過，當無線站台具有不同的傳輸速率時(例如 11g, 11n)，使用結果將會不大公平。慢速的站台(11g)以緩慢的資料傳輸運行，佔據太多的傳輸時間，相對來看，快速的站台(11n)就變得慢了許多。

以下圖爲例，站台 A(11g)和 B(11n)皆透過路由器傳輸資料封包，雖然他們都有同等的概率存取無線頻道，站台 B(11n)僅能用到一點點時間，卻得等待很久讓站台 A(11g)花很長的時間傳輸一個封包。換言之，站台 B 被站台 A 給阻塞了。



爲改善這樣的現象，使用此功能可透過控制傳輸流量的方式讓站台 A/B 使用相同的存取時間，藉由這種方式站台 B(速度快)具有較高的可能性傳送比站台 A(速度慢)更多的資料封包出去。



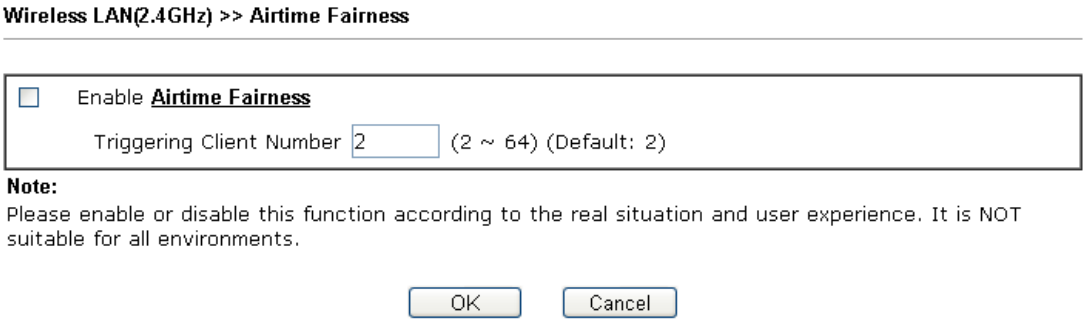
這有點類似自動頻寬限制，每個無線站台的動態的頻寬限制，乃視即時活動的無線站台數目與頻寬均化分派結果而定。請注意 2.4GHz 和 5GHz 的無線頻寬均化是獨立的。但是具有不同 SSID 功能的無線站台會一起運作，因爲他們都是使用相同的無線頻道，在特定的環境中，此功能可以減少慢速的無線設備造成的不良影響，且改善整體的無線成效。

適合的環境如下：

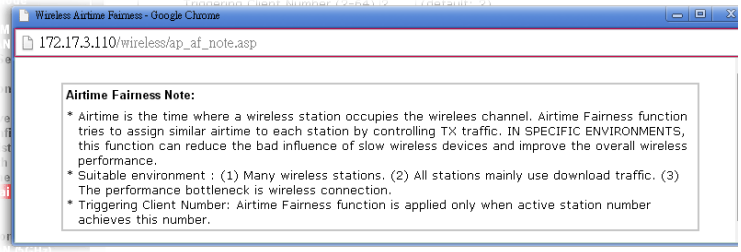
(1) 多個無線站台

(2) 所有的無線站台主要用途在下載

(3) 成效瓶頸在無線連線上



可用設定說明如下：

項目	說明
啓用無線頻寬均化(Enable Airtime Fairness)	藉由控制傳輸流量，分派相同的無線頻寬給予每一個無線站台。 **無線頻寬均化(Airtime Fairness)** – 按此連結可以開啓視窗顯示無線頻寬均化的注意事項。  **觸發用戶數目(Triggering Client Number) -**無線頻寬均化功能僅在運作的無線站台達到此設定數目時才套用。

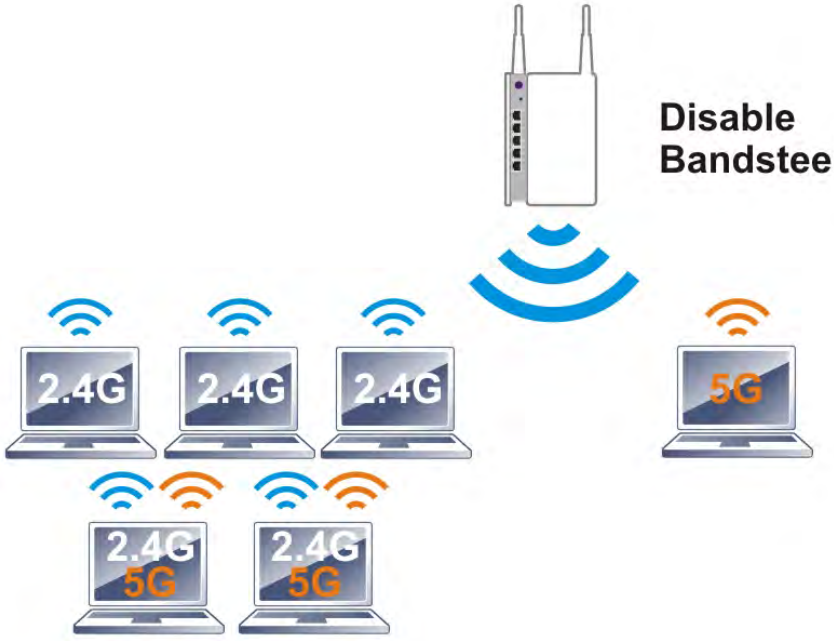
完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

Info

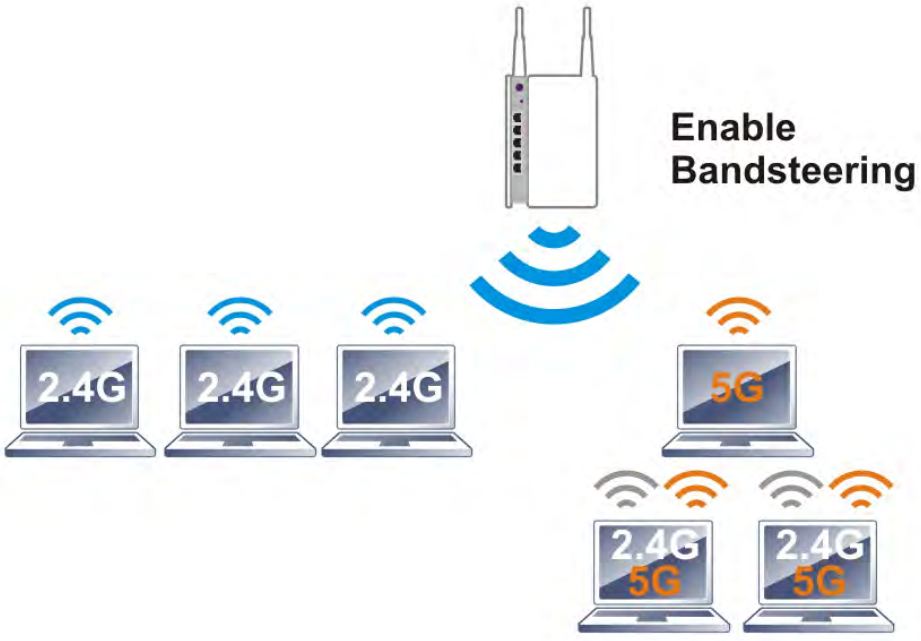
無線頻寬均化功能與頻寬限制功能是互斥的，因此其個別網頁上皆有額外的動作確保二個功能不會同時啓用。

III-1-12 頻段操控(Band Steering)

頻段操控(Band Steering)偵測無線用戶是否具有 5GHz 操作能力，並可引導用戶使用該頻率，這個功能可以協助傳統用戶離開 2.4GHz 頻，降低頻道利用率以改善用戶使用經驗。



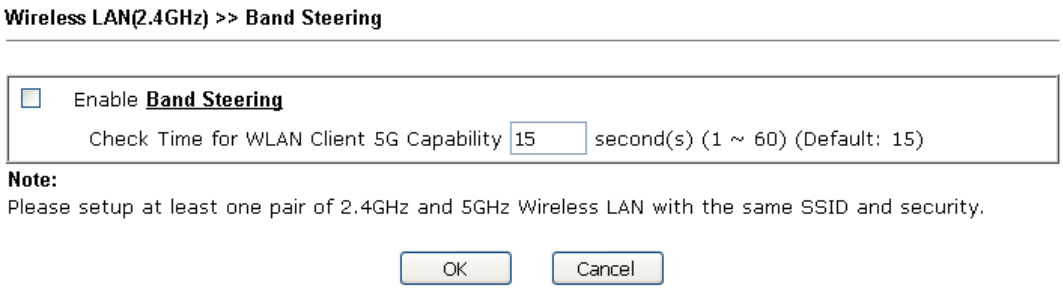
若是偵測出雙頻功能，基地台將讓無線用戶連接到較不擁擠的無線區域網路，諸如 5GHz 等以避免網路塞車。



資訊

欲成功運作頻段操控，於 2.4GHz 上的 SSID 與安全性也必須同時廣播至 5GHz。

開啓**無線區域網路>>頻段操控(Wireless LAN (2.4GHz)>>Band Steering)**：

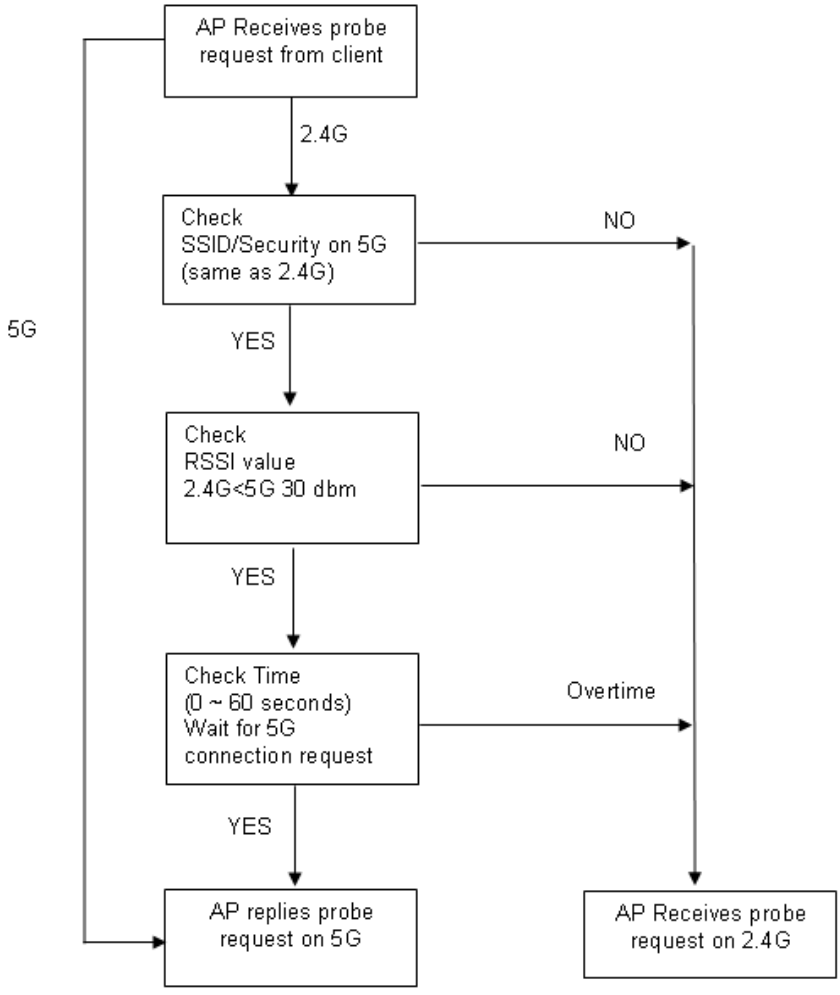


可用設定說明如下：

項目	說明
啓用頻段操控(Enable Band Steering)	若啓用了此功能，路由器將會在限定時間內偵測無線用戶是否具有雙頻能力。 **檢查時間...(Check Time....)** – 如果無線站台不具備 5GHz 網路連線能力，系統得等待並檢查數秒(預設值等 15 秒)以進行 2.4GHz 網路連線。請設定時間限制秒數以利路由器偵測無線用戶。

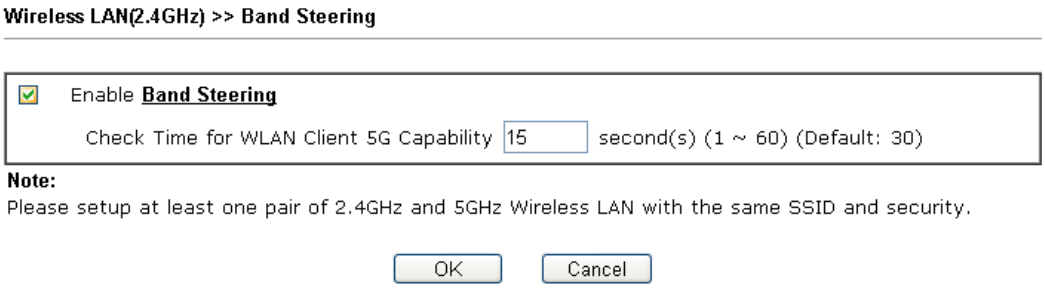
完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

下圖顯示頻段操控的運作方式。

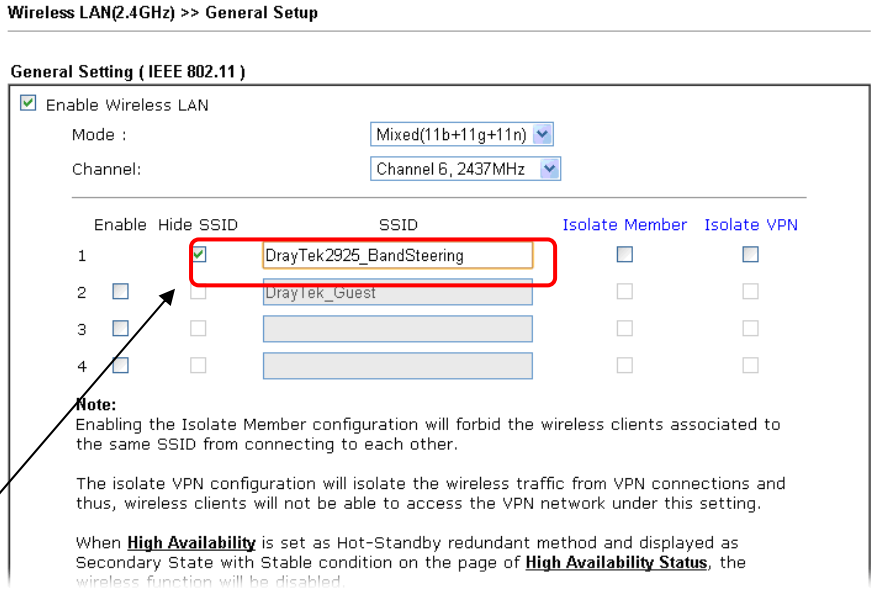


如何使用頻段操控(Band Steering)?

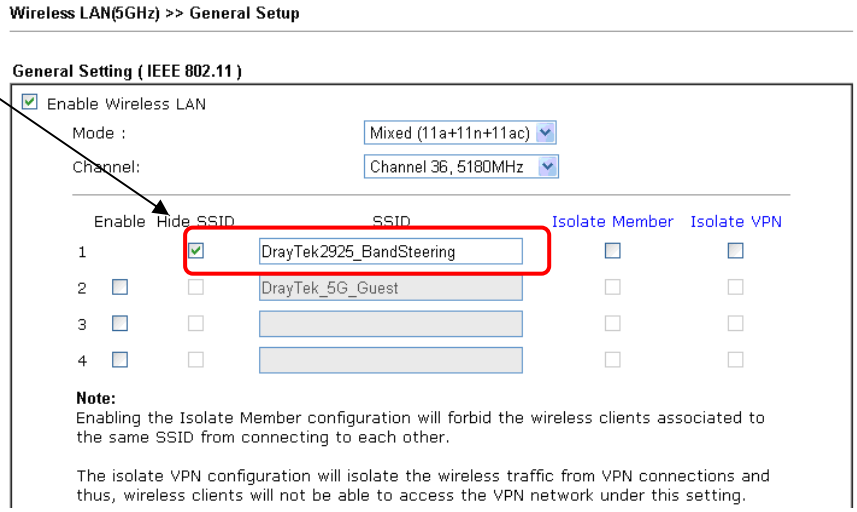
1. 開啓**無線區與網路(2.4GHz)>>頻段操控(Wireless LAN(2.4GHz)>>Band Steering**)。
2. 勾選**啓用頻段操控(Enable Band Steering)**並使用預設值(15)作爲檢查時間之設定。



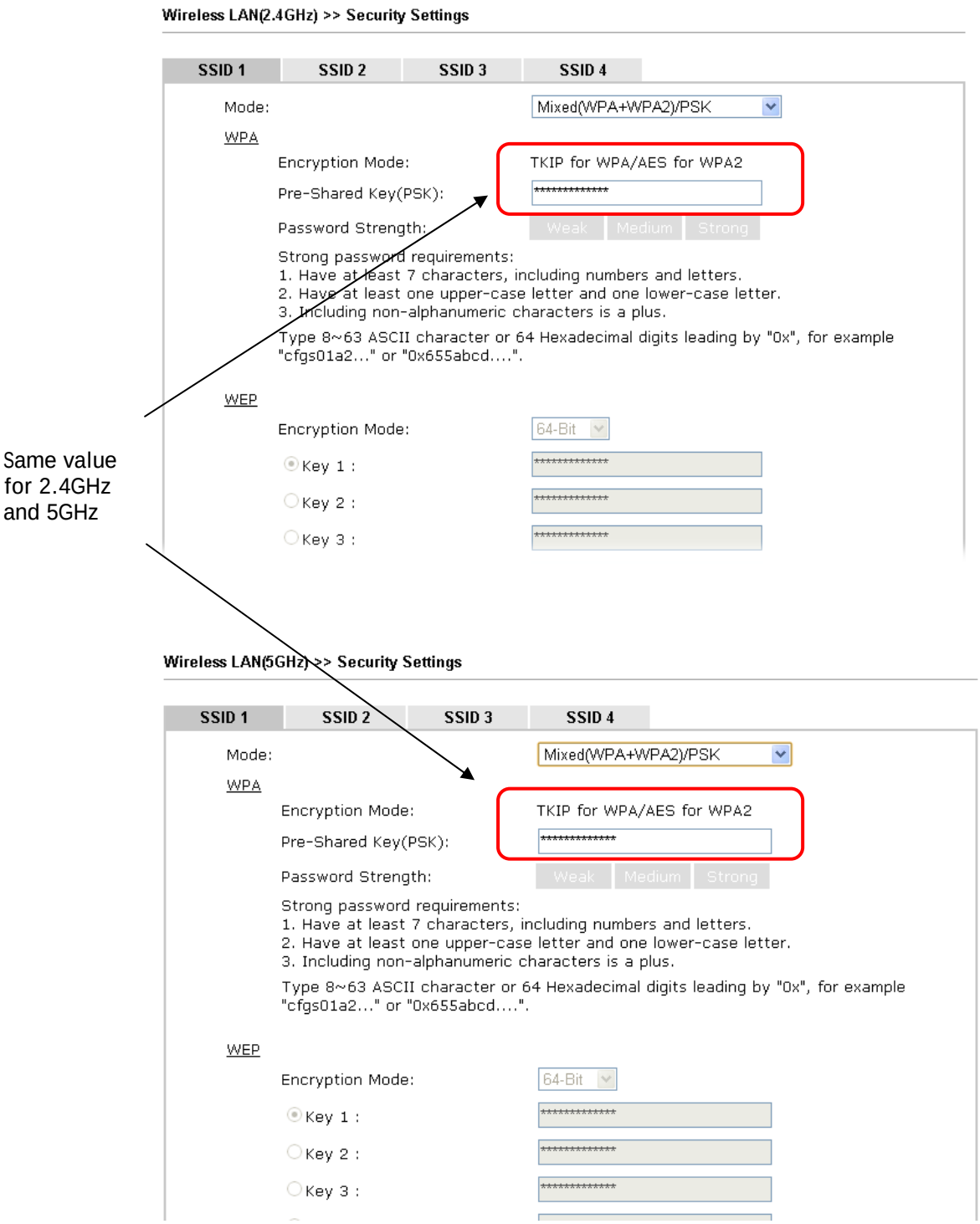
3. 按下**確定(OK)** 儲存設定。
4. 開啓**無線區與網路(2.4GHz)>>基本設定(Wireless LAN (2.4GHz)>>General Setup)** 以及**無線區與網路(5GHz)>>基本設定(Wireless LAN (5GHz)>>General Setup)**，二邊的頁面皆設定 SSID 爲 *DrayTek2925_BandSteering*。按下**確定(OK)** 儲存設定。



Same value for 2.4GHz and 5GHz



5. 開啓**無線區與網路(2.4GHz)>>安全性設定(Wireless LAN (2.4GHz)>> Security)** 以及**無線區與網路(5GHz)>> 安全性設定(Wireless LAN (5GHz)>> Security)**，二邊的頁面皆將安全性設定爲 *12345678*。按下**確定(OK)** 儲存設定。

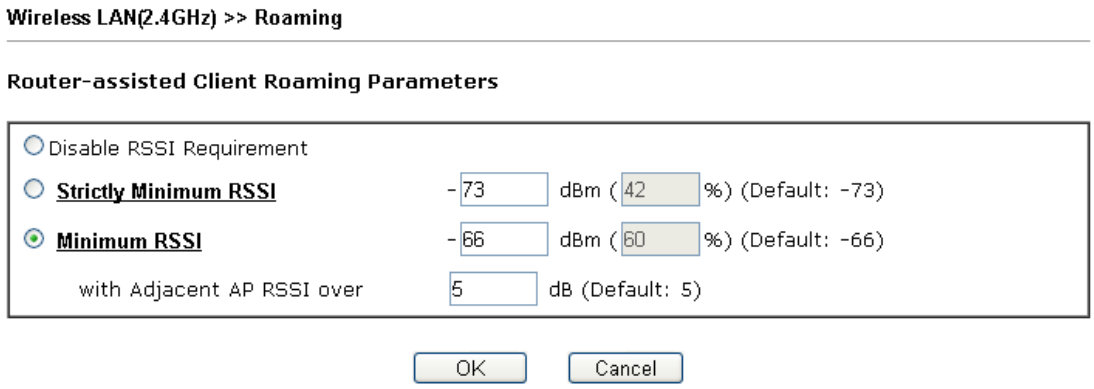


6. 現在，路由器將可讓無線用戶連接至較不擁擠的無線區域網路像是 5GHz 好避免網路壅塞的情形。

III-1-13 漫遊(Roaming)

單一無線網路基地台的網路訊號會受到其涵蓋範圍的限制，因此若您想要以快速的方式在大型的展示區域擴展無線網路，您可以安裝多個基地台，啓用每台基地台的漫遊功能，就可以達成無縫擴展無線訊號的目的了。

這些彼此相連的基地台可以利用預先認證的方式來驗證，本頁面可讓您啓用漫遊以及預先認證功能。



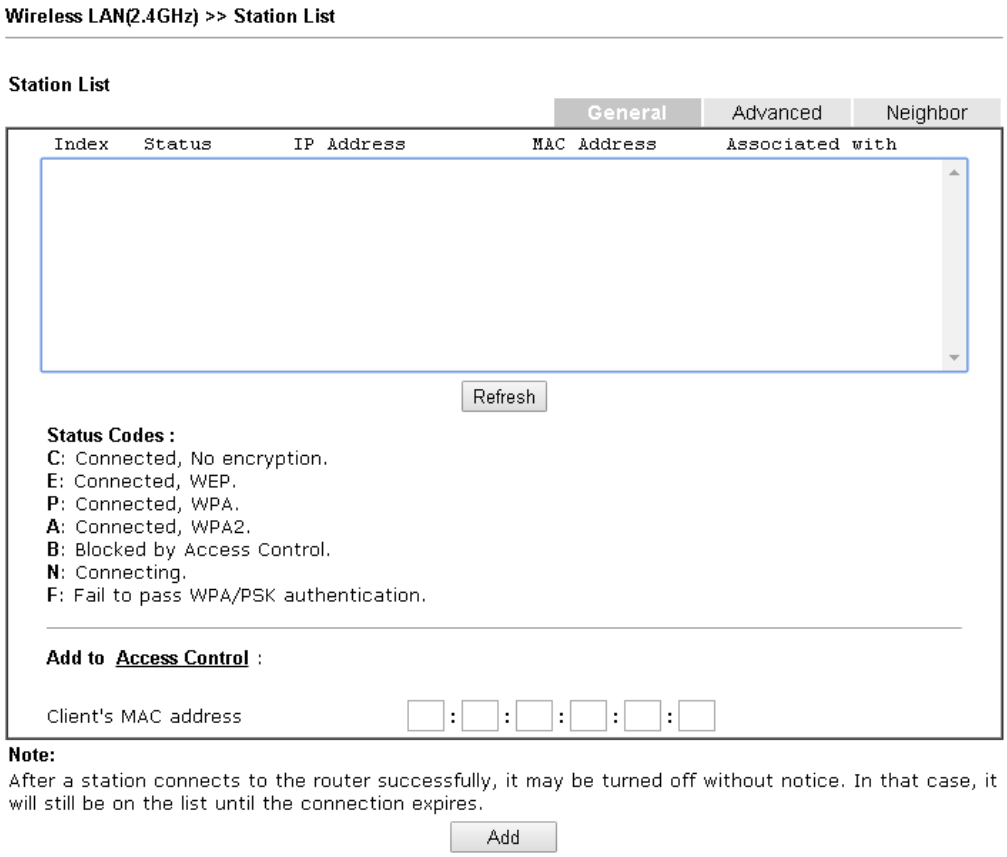
可用設定說明如下：

項目	說明
停用 RSSI 需求 (Disable RSSI Requirement)	當無線站台的連結速率過慢或是接收的訊號太差，路由器將會自動偵測（依照連線速率以及 RSSI 需求）並切斷網路連線，幫助該站台連線至其他無線基地台取得更好的無線訊號。 此選項可停止漫遊機制。
嚴格最小 RSSI (Strictly Minimum RSSI)	路由器使用 RSSI（接收訊號強度指示器）來決定中止無線站台的網路連線。 當訊號強度低於此處的設定值時，路由器將立刻中止網路連線。
最小 RSSI (Minimum RSSI)	**最小 RSSI (Minimum RSSI) -**當訊號強度低於此處的設定值時，而路由器偵測出的相鄰基地台(必須是居易 AP 且也支援此功能)具有較高的訊號強度(數值定義在此)，那麼 Vigor 路由器將中止該無線站台的網路連線，稍後該無線站台即可連線至相鄰的無線基地台(訊號較佳)。 ● **相鄰 AP 的 RSSI 值超過(With Adjacent AP RSSI over) -** S 指定一個數值作爲門檻。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

III-1-14 無線用戶端列表(Station List)

無線用戶端列表(Station List)提供您目前相連之無線用戶的狀態碼，下圖針對狀態碼提供了詳盡的解說，爲了能有更方便的連線控制，您可以選擇一台 WLAN 用戶站然後選擇**新增至連線控制(Add to Access Control)**，這樣就可以了。



可用設定說明如下：

項目	說明
更新頁面(Refresh)	按此鈕更新用戶端的 MAC 位址列表。
新增(Add)	按此鈕新增選定之 MAC 位址至**連線控制(Access Control)**。

本頁留白

第四篇 VoIP 語音設定



網際網路通訊協定語音(VoIP – Voice over Internet Protocol) 可讓用戶使用寬頻網際網路連線，進行高音質語音通話。

IV-1 VoIP

Voice over IP network (VoIP)可讓您使用寬頻網際網路連線撥打網路電話。



資訊	此功能僅適用“V”機型。

有很多種不同的電話信號協定、方法可讓 VoIP 裝置使用以便與對方溝通聯繫，最普遍的協定有 SIP、MGCP、Megaco 和 H.323，這些協定彼此都不完全相容(除非是透過軟體伺服器的掌控)。

Vigor V 系列機種支援 SIP 協定，因爲此種協定對 ITSP (Internet Telephony Service Provider)而言是很理想也很方便，支援也最廣。SIP 是一種端對端信號協定，可建立使用者於 VoIP 結構中之出席情形和機動性。每個想要使用 SIP 相同資源辨識器之用戶都可使用標準的 SIP URI 格式

sip: user:password @ host: port

某些區域可能有不同的使用方式，一般來說主機指的是網域，使用者資訊包含有使用者名稱區、密碼區，@符號則緊跟在後，這種格式和 URL 很相似，所以有些人以 SIP URL 來稱呼它。SIP 支援點對點直接撥號，同時也可透過 SIP 代理伺服器(角色雷同 H.323 Gatekeeper)來撥號，而 MGCP 協定則是使用用戶-伺服器結構，撥號方式和目前 PSTN 網路是相同的。

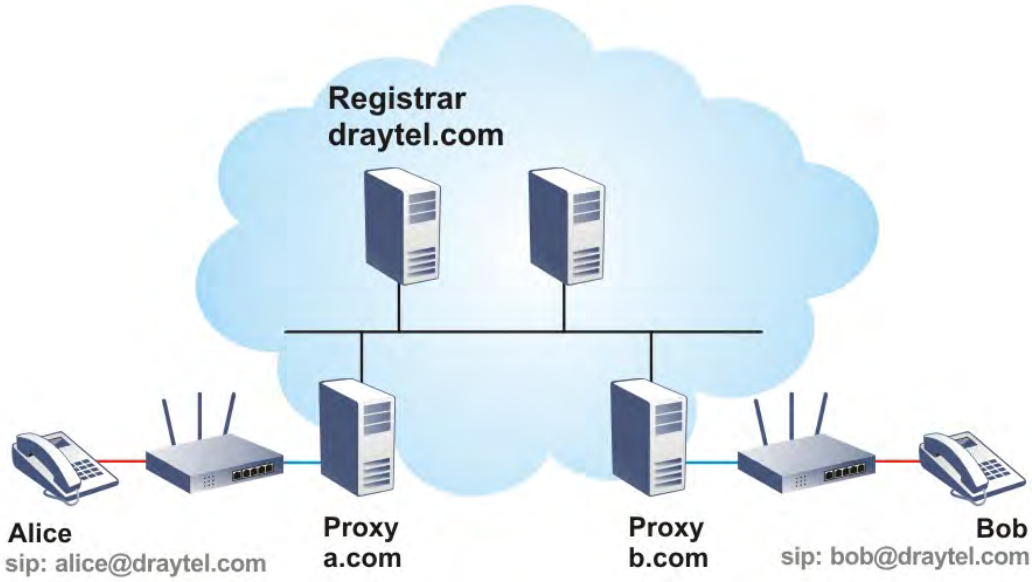
在撥號設定之後，聲音是透過 RTP (Real-Time Transport Protocol)來傳送的，不同的 codecs(用來壓縮和解壓縮聲音)可以包覆於 RTP 封包中，Vigor V 機種提供不同的 codecs 包括 G.711 A/μ-law, G.723, G.726 和 G.729 A & B，每個 codecs 都使用不同頻寬，因此可以提供不同等級的聲音品質。Codec 使用的頻寬越多，聲音品質越好，雖然如此還是應該配合您的網際網路頻寬選擇適宜的 codec 才恰當。

通常有二種撥號類型，說明如下：

透過 SIP 伺服器撥號

首先 Vigor V 機種必須先向 SIP 註冊，傳送註冊訊息才可生效，然後雙方的 SIP 代理商將轉送一系列訊息給與撥號者，以便建立完整的連線數。

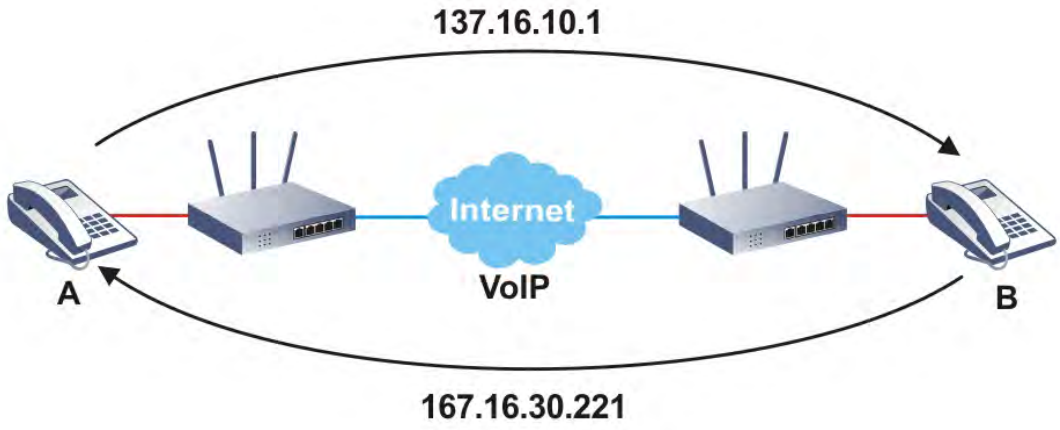
如果雙方都向相同 ISP 業者註冊，那麼我們可以下圖來做簡單說明：



這種模式最主要的好處是您不必去記朋友的 IP 位址(因爲它可能常常會改變，如果該位址是浮動的位址的話)，相反的您只要使用撥號對應表或是直接撥朋友的帳號名稱就可以了。

點對點

在撥打電話之前，您必須知道朋友的 IP 位址，Vigor VoIP 路由器會建立雙方間的連線。



我們的 Vigor V 機種首先採用有效之 codecs，但同時也擔保自動 QoS 的功能，QoS 擔保可以協助指定聲音流量較高之優先權，您對聲音所需求之 inbound 和 outbound 頻寬永遠擁有優先處理權，但是您的資料處理就會有些慢，不過還在忍受範圍內。

網頁使用者介面

下圖爲 VoIP 的功能項目：

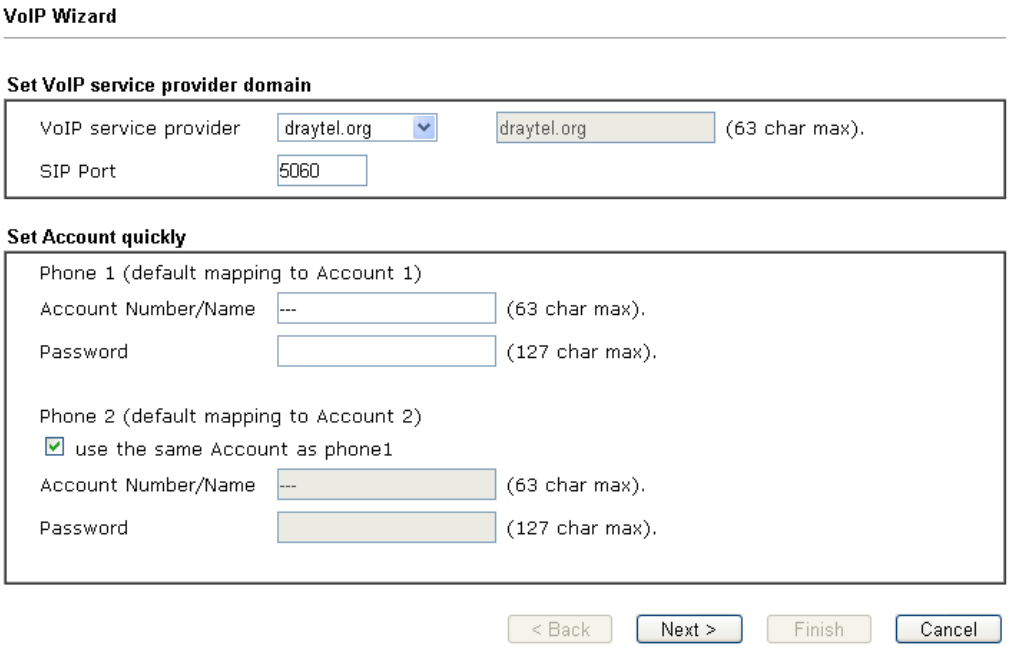


IV-1-1 VoIP 設定精靈(VoIP Wizard)

Vigor 路由器提供可以快速設定 VoIP 運用的設定精靈。

資訊	此設定精靈僅適用“V”系列機型。

1. 開啓**設定精靈>>VoIP 設定精靈(Wizards>>VoIP Wizard)**。
2. **VoIP** 設定精靈出現如下：

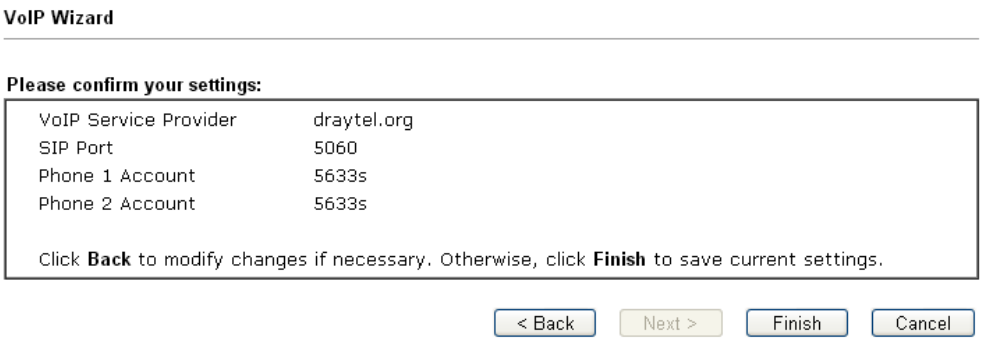


可用設定說明如下：

項目	說明
設定 VoIP 服務供應商網域 (Set VoIP service provider domain)	**VoIP 服務供應商(VoIP service provider)** – 使用下拉式清單列出可以選擇的 VoIP 服務供應商選項。 **SIP 埠號(SIP Port)** – 使用預設埠號設定 (5060)。
快速設定帳號(Set	**帳號/名稱(Account Number/Name)** – 輸入於 ISP 註冊的帳

Account quickly)	號與名稱。 **密碼(Password)** – 輸入於 ISP 註冊的密碼。 **使用電話 1 相同帳號(Use the same Account as phone 1)** – 如果不需要設定 Phone 2 的內容，請勾選此方框。
下一頁(Next)	按此進入下一個設定頁面。
取消(Cancel)	按此取消設定並離開此設定精靈。

3. 完成設定之後，按**下一頁(Next)**檢視連線的設定總結內容。

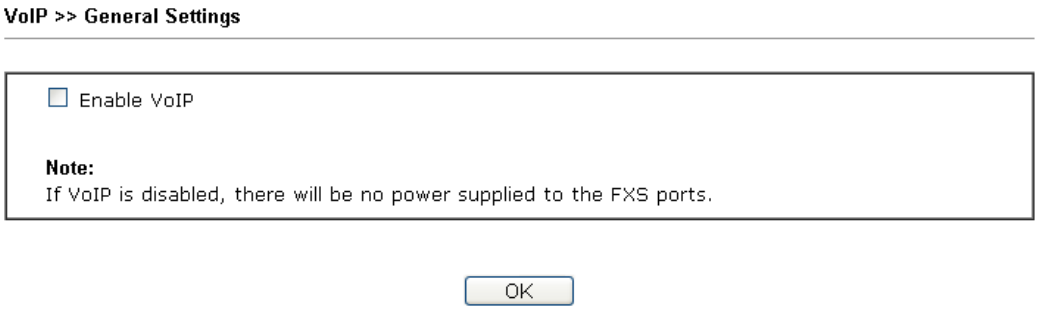


4. 按**完成(Finish)**，**VoIP Wizard Setup OK!!!** 頁面即可顯示於畫面上。

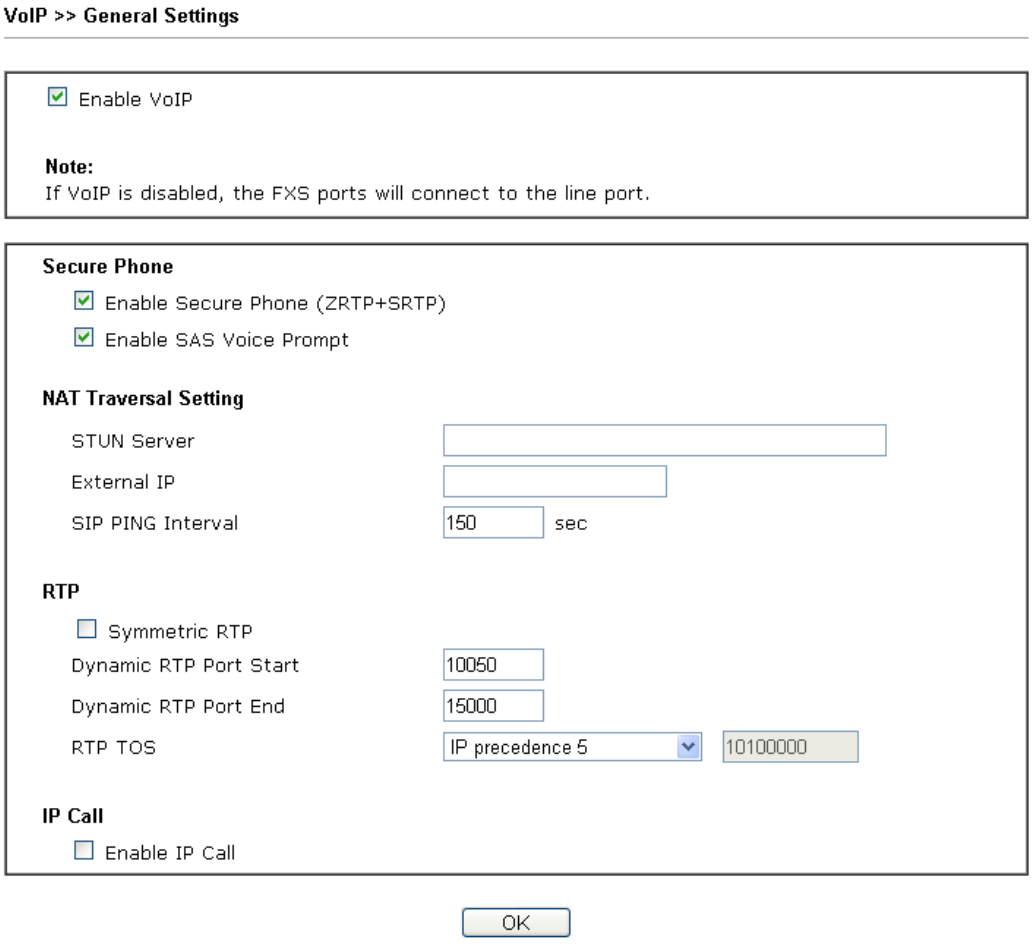


IV-1-2 基本設定(General Settings)

按下 **VoIP>>基本設定(VoIP>>General Settings)**開啓如下頁面，勾選**啓用 VoIP (Enable VoIP)**並按下**確認(OK)**按鈕即可開啓細部的設定頁面，若未勾選此方框，則無法設定任何 VoIP 功能。

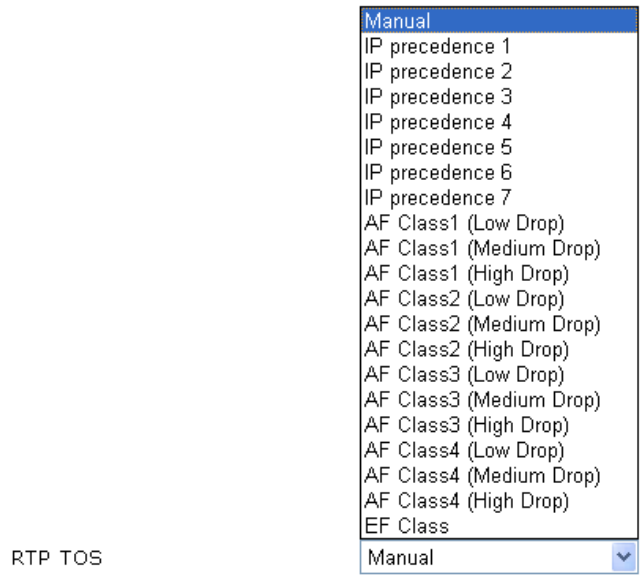


在勾選方框並按下**確認(OK)**後，即可取得如下頁面，您可設定安全電話、IP 電話、NAT 轉址設定、RTP 設定等等。



可用設定說明如下：

項目	說明
安全電話(Secure Phone)	**啓用安全電話(Enable Secure Phone)** -利用相同的通訊協定(ZRTP+SRTP)讓使用者能有加密的 RTP stream 與遠端通訊，請勾選此方塊啓動此安全電話功能。 **啓用 SAS 聲音提示(Enable SAS Voice Prompt)** -若啓動此項目，每一次雙邊都會聽見 SAS 提示音，若沒有啓動，就再也不

	會聽到提示音。
NAT 轉址設定(NAT Traversal Setting)	**STUN 伺服器(STUN Server) -** 輸入 STUN 伺服器的 IP 位址或是網域名稱。 **外部 IP(External IP) -** 輸入閘道器 IP 位址。 **SIP PING 間隔(SIP PING interval) -** 預設值爲 150 秒，對 Nortel 伺服器而言這項設定是相當有用的。
RTP	**對稱 RTP(Symmetric RTP) -** 勾選此框啓用此功能。爲了讓資料能夠在本機路由器與遠端路由器之間傳輸，不至於因爲 IP 漏失(如傳送來自遠端路由器的真實 IP 至本機路由器的虛擬 IP)而誤導，您可以勾選此框以解決此問題。 **RTP 通訊埠起點(Dynamic RTP Port Start) -** 指定 RTP 之通訊埠起點，預設值爲 10050。 **RTP 通訊埠終點(Dynamic RTP Port End) -** 指定 RTP 之通訊埠終點，預設值爲 15000。 **RTP TOS -**此項可決定 VoIP 封包的等級，請使用下拉式選項選擇其中一種。 
IP 電話(IP Call)	**啓用 IP 電話(Enable IP Call) -** 可讓使用者撥出對外 IP 電話，路由器則接收 IP 來電。

安全電話的應用

啓用 SAS 聲音提示，例如路由器 A **啓用安全電話(nable Secure Phone)**與**啓用 SAS 聲音提示(Enable SAS Voice Prompt)**並打電話給路由器 B：

1. 在連線建立後，路由器 A 將會傳送 SAS 聲音提示訊息給予 A，路由器 B 傳送 SAS 聲音提示訊息給予 B。
2. 此時，RTP 流量是受到安全保護的，直到電話通訊結束。
3. 如果路由器 A 想要下次再打給路由器 B，即使在網頁上已經勾選了**啓用 SAS 聲音提示**，這次不會再聽到任何聲音提示了，亦即只有第一通電話才會有聲音提示的功能。

啓用 SAS 聲音提示，例如路由器 A **啓用安全電話**，但未**啓用 SAS 聲音提示**並打電話給路由器 B：

1. 在連線建立後，路由器 A 將**不會**傳送 SAS 聲音提示訊息給予 A，路由器 B **也不會**傳送 SAS 聲音提示訊息給予 B。
2. 即使沒有聲音提示，RTP 流量仍然受到安全保護，直到電話通訊結束。

資訊

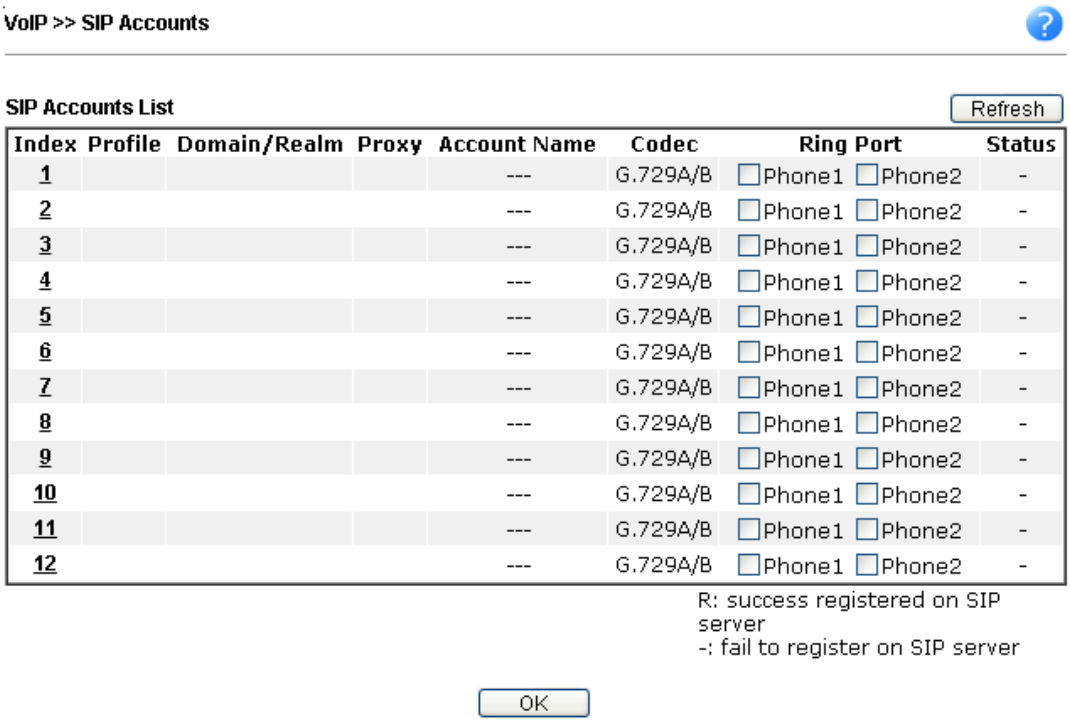
如果來電或去電並不符電話簿上的任何一個設定，路由器將會嘗試讓該通電話先具備一定的保護，但是如果該通電話是以未受保護的情況下結束（例如對方並不支援 ZRTP+SRTP 功能），路由器將不會播放任何警告訊息。

IV-1-3 SIP 帳號(SIP Accounts)

在此頁面中，您可以調整自己的 SIP 設定，當您申請一個帳號時，您的 ISP 服務供應商會給您一個帳號名稱或是使用者名稱、SIP 登錄者、代理人和網功能變數名稱稱(最後三種在某些條件下，有可能是完全相同的)，您可以告訴您的成員有關您的 SIP 位址，表示法爲**帳號名稱@網功能變數名稱**。

當路由器打開時，將以使用帳號名稱@網功能變數名稱稱來登錄，之後，您的電話將由 SIP 代理者以帳號名稱@網功能變數名稱稱傳送至目的地作爲辨識之用。

資訊	**振鈴通訊埠(Ring Port)**的項目會依照您所使用的路由器而有所差異。

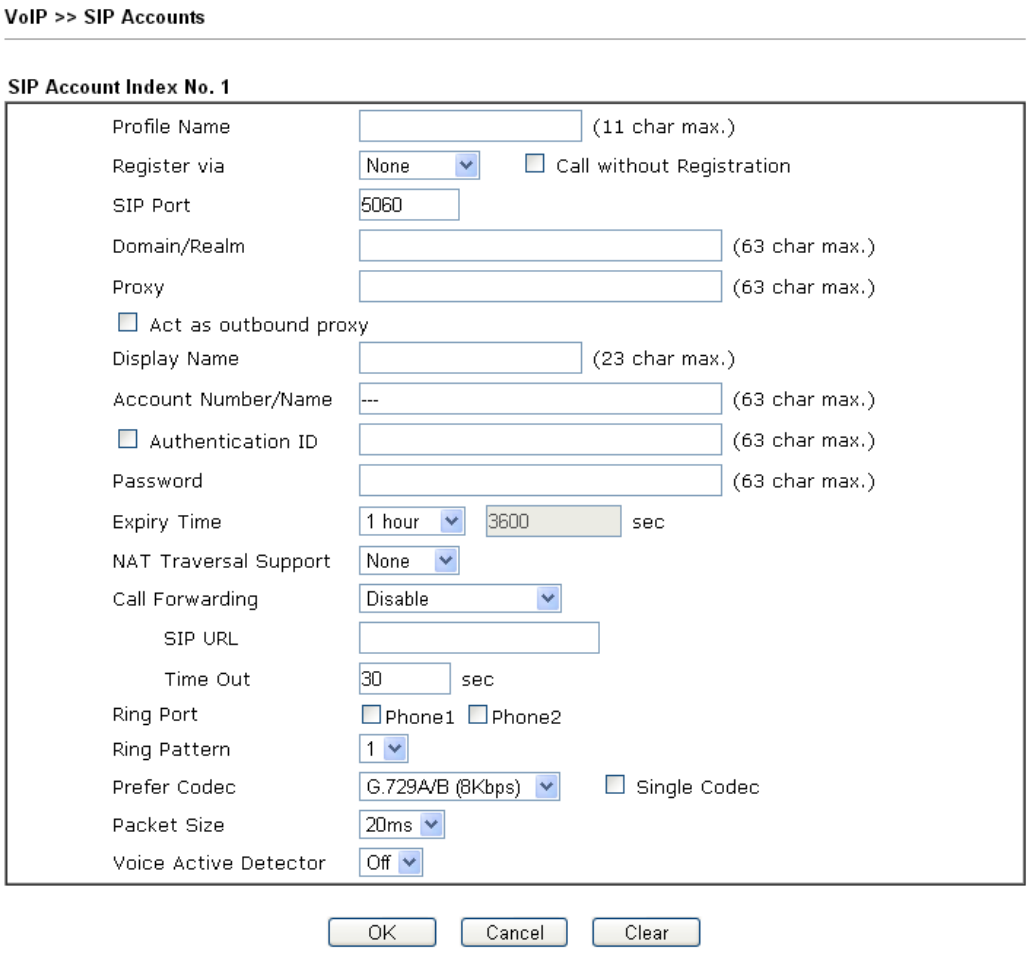


可用設定說明如下：

項目	設定
索引(Index)	按此鈕進入下一層設定頁面設定 SIP 帳號。
設定檔(Profile)	顯示帳號的設定檔名稱。
網域(Domain/Realm)	顯示 SIP 註冊伺服器的網功能變數名稱稱或是 IP 位址。
伺服器(Proxy)	顯示 SIP 伺服器的網功能變數名稱稱或是 IP 位址。
帳號名 (Account Name)	顯示@前面的 SIP 位址帳號名稱。
Codec	每個通訊埠的預設 Codec 設定都會顯示在本區，您可以按索引號碼變更每個電話通訊埠的設定。
振鈴通訊埠 (Ring Port)	指定接收電話時由哪一個通訊埠響鈴。

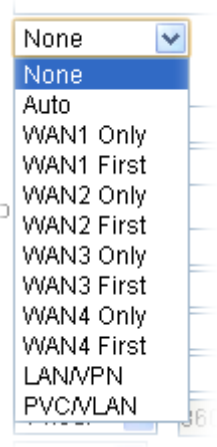
狀態(Status)	顯示相關 SIP 帳號的狀態，**R** 表示此帳號已註冊成功，**-** 表示尚未成功註冊。

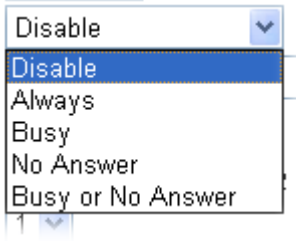
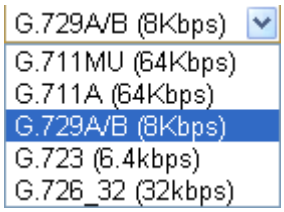
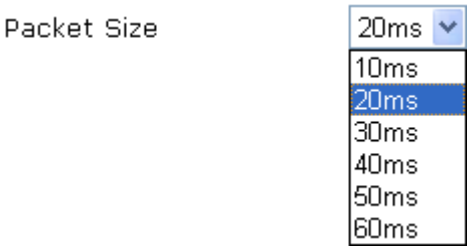
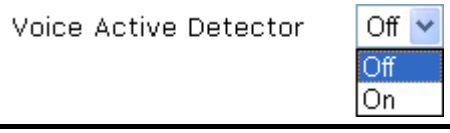
按任何一個索引連結開啓如下頁面：



可用設定說明如下：

項目	設定
設定檔名稱 (Profile Name)	指定一個名稱作爲辨識之用，您可以使用與網域類似的名稱，例如網功能變數名稱稱爲 *draytel.org*,您就可以在本區中設定 *draytel-1*。
由此註冊 (Register via)	指定您申請註冊時所透過的介面爲何，如果您不想註冊個人資料而直接使用 VoIP 撥號功能，請選擇**無(None)**。某些 SIP 伺服器允許使用者不須登錄即可使用 VoIP 功能，針對這類伺服器，請勾選**無需登錄即撥出(Call without Registration)**。其它則選擇**自動(Auto)**，系統將爲您選擇最佳方式作爲 VoIP 撥號之用。

	
SIP 埠號(SIP Port)	設定傳送/接收 SIP 訊息的埠號以建立連線。預設值爲 5060，對方必須於其註冊登錄服務商設定相同的數值。
網域(Domain/Realm)	設定 SIP 註冊伺服器的網域或是 IP 位址。
伺服器(Proxy)	設定 SIP 伺服器的網域或是 IP 位址，您可以在網域名稱後方輸入號碼，指定該埠號作爲資料傳輸的埠號(例如 nat.draytel.org:5065)。
以對外伺服器之身份來運作 (Act as Outbound Proxy)	勾選此方塊以啓用伺服器成爲對外伺服器。
顯示名稱(Display Name)	您想要在朋友的電話顯示螢幕上出現的名稱。
帳號名稱/號碼 (Account Number/Name)	輸入 SIP 位址的帳號名稱，例如@之前的文字。
驗證 ID 身分 (Authentication ID)	勾選此方塊啓用此功能並輸入名稱或號碼供 SIP 驗證，如果設定值與帳戶名稱相同，您就不必勾選此方塊另設數值。
密碼(Password)	當您以 SIP 服務註冊時所需提供的密碼。
有效時間 (Expiry Time)	爲 SIP 伺服器提保存使用者註冊帳號的有效時間。在到期之前，路由器將會再次傳送另一個註冊需求給予 SIP 登錄伺服器。
NAT 穿透 (NAT Traversal Support)	如果路由器(寬頻路由器)是透過其他裝置連接上網際網路，您就必須設定此功能。 NAT Traversal Support None (None / Stun / Manual / Nortel) **無(None) -**.關閉此功能。 **Stun** –若路由器支援 Stun 伺服器，請選擇此項目。 **手動(Manual)** –若您想要指定外部 IP 位址作爲 NAT transversal 支援，請選擇此項目。 **Nortel** – 如果軟體支援 nortel 方案，您可以選擇此項目。
指定轉接(Call Forwarding)	共有四種選項可以選擇，**停用(Disable)**可關閉此功能，**永遠(Always)**則表示來電會一直轉接到 SIP URL 上，**忙線(Busy)**則表示來電只在本機忙碌時轉接到 SIP URL，**沒回應(No Answer)**則表示來電若未收到任何回應，電話都會在切斷時轉接到 SIP URL 上。

	 **SIP URL** – 請輸入 SIP URL (例如 aaa@draytel.org 或 abc@iptel.org) 做爲轉送電話的終點。 **逾時(Time Out)**– 設定電話轉接的逾時現制，預設值爲 30 秒。
振鈴通訊埠(Ring Port)	設定 Phone 1, Phone 2 作爲 SIP 帳號的預設振鈴通訊埠。
振鈴樣式(Ring Pattern)	選擇 VoIP 電話的振鈴樣式。 
偏好 Code (Prefer Codec)	選擇任何一種偏好 Codec，每通電話的 Codec 在每次連線時可以與對方交涉，預設值爲 G.729A/B，它會佔據少許頻寬以維護良好的聲音品質。 如果上傳速度僅有 64Kbps，請勿使用 G.711 codec。如果想要使用 G.711，那麼上傳速度至少要有 256Kbps。  **單一 Codec(Single Codec)** – 如果勾選此方塊，只有選定的 Codec 會被路由器套用。
語音資料長度(Packet Size)	資料總數包含單一封包(10, 20, 30, 40, 50 和 60)，預設值爲 20ms，表示資料封包含 20ms 聲音資訊。 
聲音活動檢測(Voice Active Detector)	選擇**開啓**(On)啓動此項功能，以檢測使用者是否正在交談。如果安靜無聲，路由器將採取行動節省頻寬的使用。選擇開(On)啓用此功能，關(Off)停用此功能。 

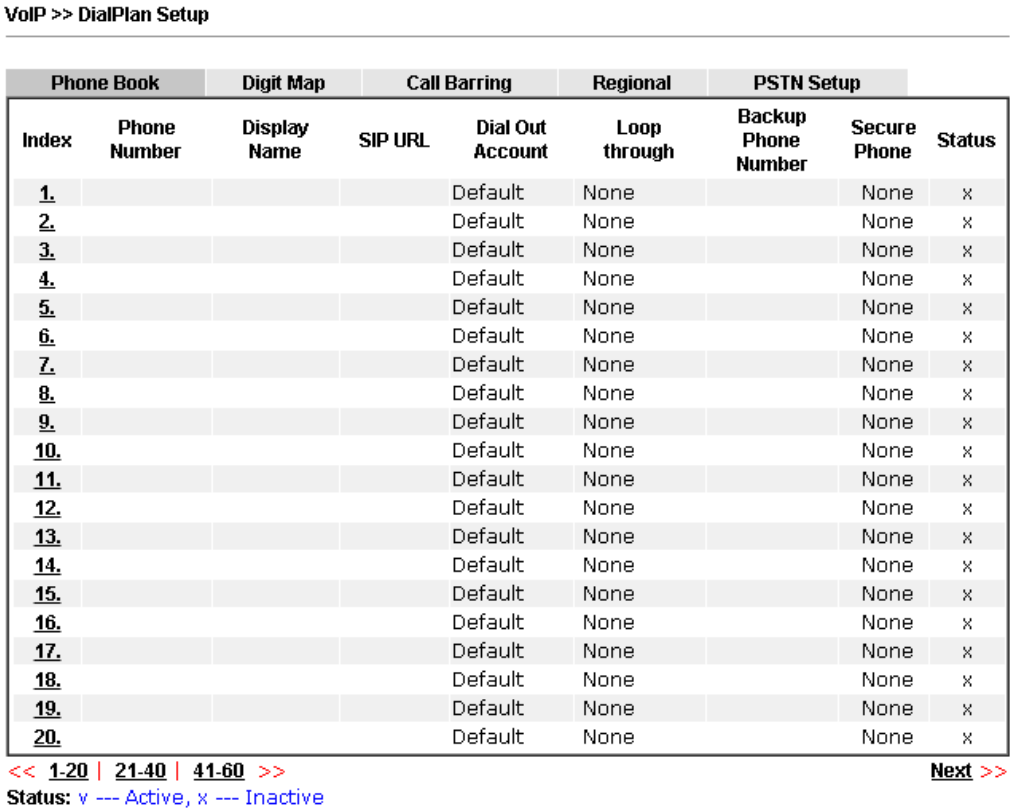
完成設定之後，按下確定(OK)按鈕儲存相關設定。

IV-1-4 撥號對應表(DialPlan)

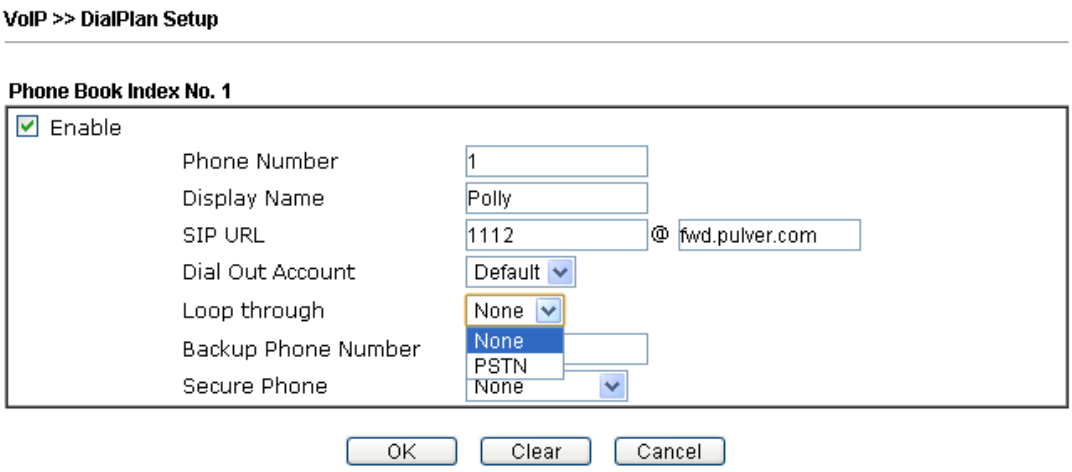
本頁讓使用者設定 VoIP 功能所需的電話簿及數字對應設定。請按頁面上的連結進入下一層設定頁面。

IV-1-4-1 電話簿(Phone Book)

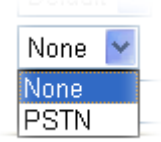
在本節中，您可以設定 VOIP 電話，這個設定可以幫助用戶以最快且最簡單的方式撥出電話號碼。本頁總共提供 60 組號碼給用戶儲存朋友以及家人的 SIP 位址。



按任何一個索引標號進入下一個設定頁面。



可用設定說明如下：

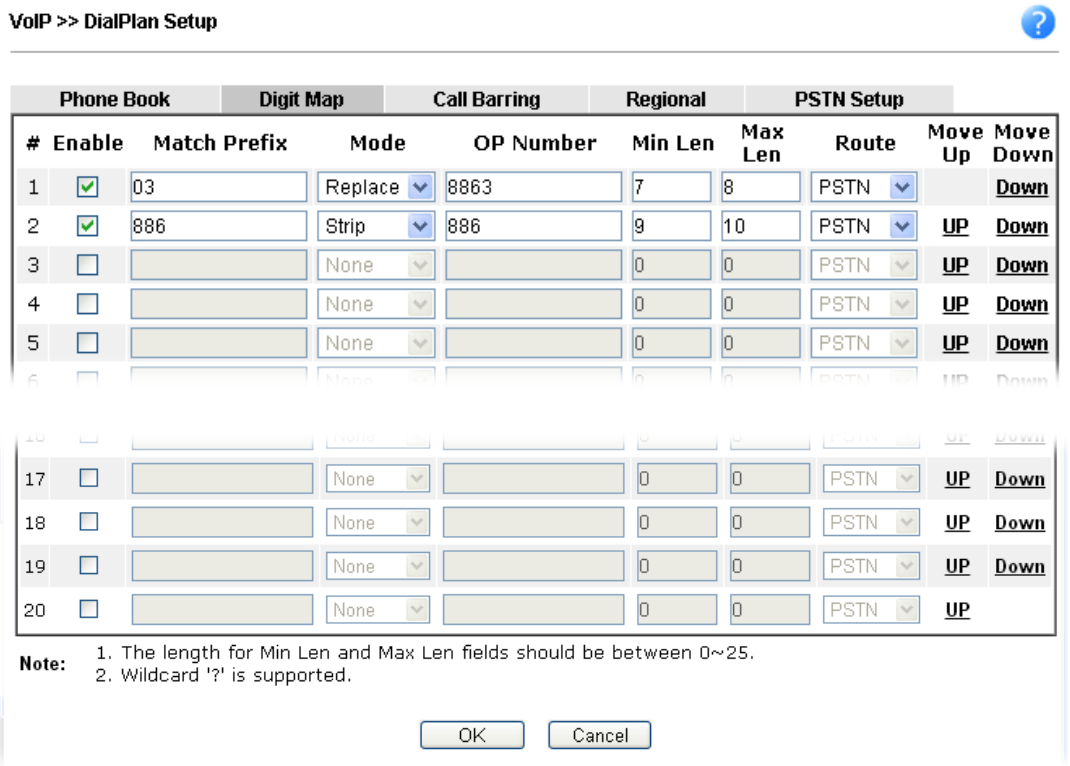
項目	設定
啓用(Enable)	勾選此方塊啓用此號碼。
電話號碼(Phone Number)	此索引編號的快速撥號號碼，任何號碼都可以使用，範圍是數字 **0-9** 以及*****。
顯示名稱(Display Name)	您想要在朋友的電話螢幕上顯示出來的名稱，可讓您的朋友容易知道是誰打的電話。
SIP URL	請輸入朋友的 SIP 位址。
撥出帳號 (Dial Out Account)	選擇 SIP 帳號供此設定檔使用，對在不同 SIP 伺服器註冊的雙方，此設定相當有用。如果撥號者與接號者沒有使用相同的 SIP 伺服器，有時候 VoIP 電話連線可能不會成功，但使用指定的撥號帳號，就可確保網路電話得以成功連線。
電話介接 (Loop through)	請選擇 PSTN 以便啓用此功能。 
備援電話號碼 (Backup Phone Number)	當 VoIP 電話受到幹擾或是網際網路因爲某種原因而中斷，備援電話將可撥出以替代 VoIP 網路電話。此時，電話會依照所選擇的電話介接方向從 VoIP 電話轉變成爲 PSTN 電話。請注意，在電話交換期間，電話的嘟嘟聲響也會短暫出現，當 VoIP 電話切換成 PSTN 電話後，電信公司就會向您收取連線的費用。請在此輸入備援電話號碼(PSTN)。
安全電話(Secure Phone)	**ZRTP+SRTP** -透過相同協定(ZRTP+SRTP) 加密 RTP 字串讓使用者與對方交談時達到安全效果。勾選此框取得安全電話。
取消(Cancel)	回到前一個頁面。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

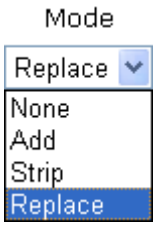
資訊	如果來電或去電不符合電話簿上任何規則，路由器將嘗試保護該通電話，但是若該通電話到結束時都處於"未保護"狀態(例如對方並未支援 ZRTP+SRTP)，路由器將無法發出警告訊息。

IV-1-4-2 數字對應設定(Digit Map)

爲了使用者的方便，本頁允許使用者以新號碼來編輯 SIP 帳號的前置號碼，或是取代該號碼等等，這個設定可以提供用戶一個透過 VoIP 介面快速且簡單的撥號方式。



可用設定說明如下：

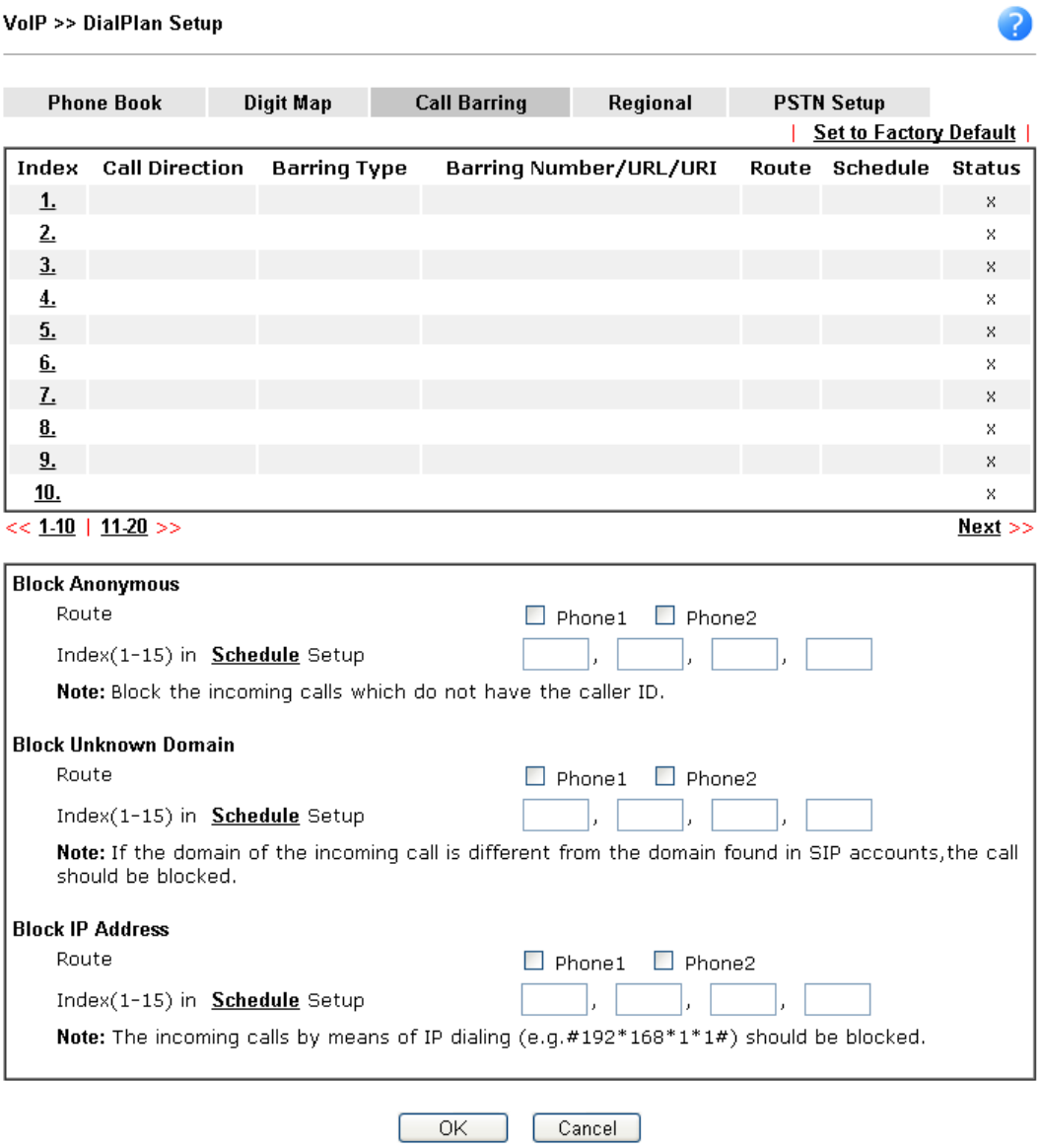
項目	設定
啓用(Enable)	按此方塊啓動此功能。
前置號碼(Match Prefix)	此處所設定的號碼可用來新增，取代變更之號碼。
Mode	**無(None)** – 無動作。 **新增(Add)** -當您選擇此模式時，變更號碼將會增加前置號碼於前面，並藉由選定的 VoIP 介面撥出。 **卸除(Strip)** -當您選擇此模式時，變更號碼將會被刪除。參考上圖所示，變更號碼 886 將被完全刪除。 **取代(Replace)**- 當您選擇此模式時，透過指定的 VoIP 介面之變更號碼將會被前置號碼所取代，當您選擇此模式時，透過指定的 VoIP 介面之變更號碼將會被前置號碼所取代，參考上圖所示，號碼 *03* 將被變更號碼 *8863* 取代。例如號碼爲“031111111”就會被改爲“88631111111”並傳送至 SIP 伺服器。 
變更號碼(OP Number)	您在此處所輸入的號碼是您想要執行特殊功用的帳號前半部

	份(依據選擇的模式而定)。
最小長度(Min Len)	設定撥號的最小長度以套用前置號碼之設定，參考上圖所示，如果號碼介於 7 和 9，那麼該號碼可以就能套用此處所設定的前置號碼設定。
最大長度(Max Len)	設定撥號的最大長度以套用前置號碼之設定。
介面(Route)	請自預設的 SIP 帳號中選擇一個您想要啓動前置號碼設定的介面。
上移/下移(Move UP /Move Down)	按下連結移動選定項目(上/下)。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

IV-1-4-3 限撥等級(Call Barring)

限撥等級用來封鎖不受歡迎的來電。



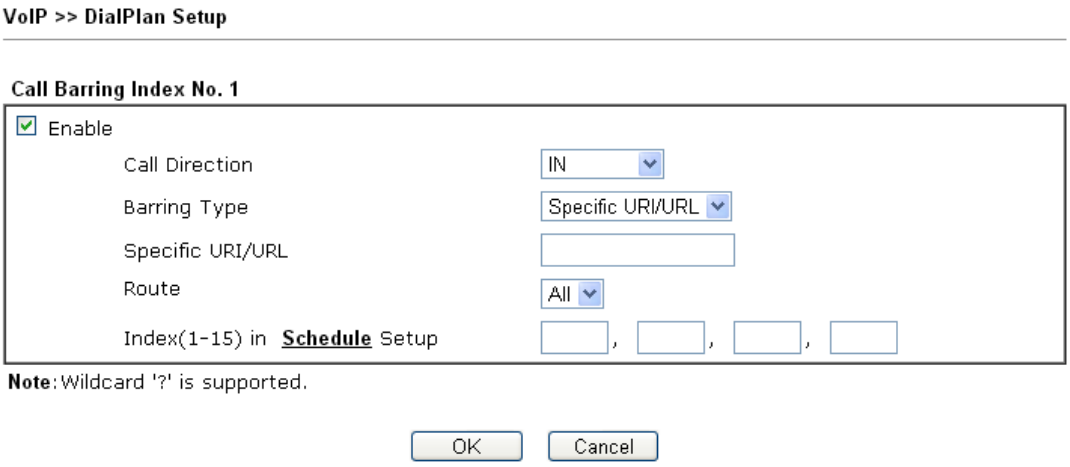
此外，您也可以將限撥等級做進一步的設定諸如**匿名封鎖(Block Anonymous)**、**未知網域封鎖(Block Anonymous)**或是**封鎖 IP 位址(Block IP Address)**等等。按下相關連結即可開啓網頁。

針對**封鎖匿名(Block Anonymous)**部分 – 此功能可封鎖沒有顯示身分的任何來電，此項設定也可依照事先設定的排程來控制。

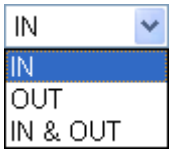
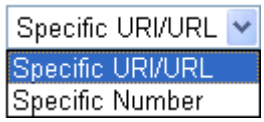
針對**封鎖未知網域(Block Unknown Domain)**部分 - 此功能可封鎖未在 SIP 帳號中指定的網域之來電，此項設定也可依照事先設定的排程來控制。

針對**封鎖 IP 位址(Block IP Address)**部分 - 此功能可封鎖來自 IP 位址之來電，此項設定也可依照事先設定的排程來控制。

按任一索引編號，開啓下述頁面。

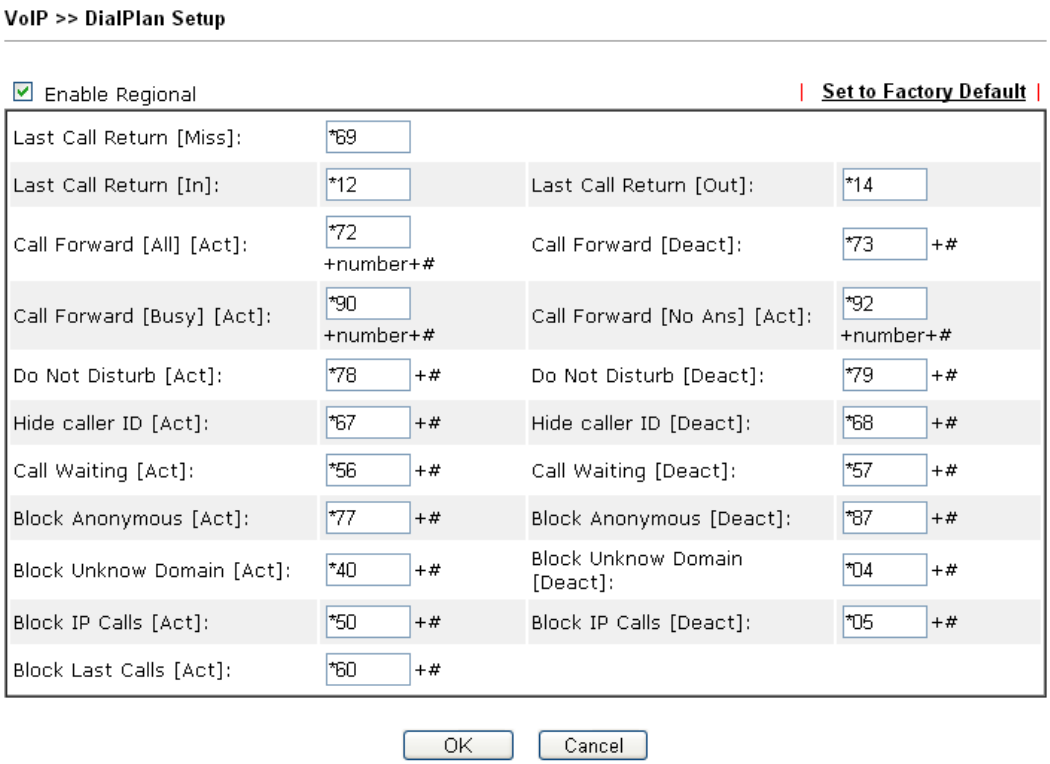


可用設定說明如下：

項目	設定
啓用(Enable)	按此方塊啓動此功能。
撥號方向 (Call Direction)	決定電話的撥打方向。撥入- 來電，撥出-去電，撥出及撥出-來電與去電。 
限定類型 (Barring Type)	決定 VoIP 電話的類型，URI/URL 或號碼。 
指定 URI/URL 或指定號碼 (Specific URI/URL or Specific Number)	本區依照您在限撥等級類型中所選擇的內容而有所不同。
介面(Route)	**全部(All)**表示全部的電話都會被此機制阻擋。
索引 (1-15) 於排程設定...(Index (1-15) in Schedule)	依照事先設定完成之排程，在此輸入排程計畫的索引編號以控制勿打擾模式。詳細設定請參考**應用>>排程 (Applications>>Schedule)**一節。

IV-1-4-4 區域設定(Regional)

本頁可讓您處理某些區域的來電與去電，預設值(大部分地區的常用值)顯示在網頁上，您可以依照路由器放置的地點，視需要去改變相關號碼。



可用設定說明如下：

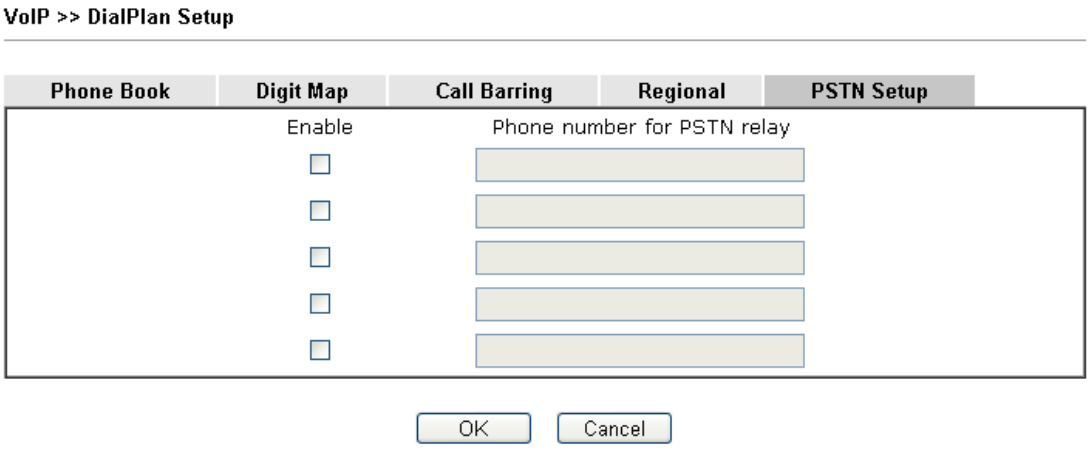
項目	設定
啓用區域設定(Enable Regional)	勾選此框啓用區域設定功能。
回撥最後來電 [漏接] (Last Call Return [Miss])	有時候，人們會漏接某些電話，您可撥打此區所設定的號碼，查看最後的來電是誰打的，然後撥打回去。
回撥最後來電 [撥入] (Last Call Return [In])	您剛完成來電通話，但爲了某些原因你需要再通話一次，請撥打此區所設定的號碼，即可撥打給剛剛通話的人員。
回撥最後來電 [撥出] (Last Call Return [Out])	請撥打此區所設定的號碼，再次撥打剛剛去電的人員。
來電跟隨 [全部][執行] (Call Forward [All][Act])	請撥打此區所設定的號碼，轉送全部來電給指定的位置。
來電跟隨 [解除] (Call Forward [Deact])	請撥打此區所設定的號碼，解除來電跟隨功能。
來電跟隨 [忙線][執行] (Call Forward [Busy][Act])	電話忙線時，請撥打此區所設定的號碼，轉送來電給指定的位置。
來電跟隨 [無回應][執行] (Call Forward [No Ans][Act])	來電欲連接的電話沒有回應時，請撥打此區所設定的號碼，轉送所有來電至指定位址。
勿打擾 [執行]	請撥打此區所設定的號碼，執行請勿打擾功能。

(Do Not Disturb [Act])	
勿打擾 [解除] **(Do Not Distrub [Deact])**	請撥打此區所設定的號碼，解除請勿打擾功能。
隱藏撥出號碼 [執行] **(Hide caller ID [Act])**	請撥打此區所設定的號碼，讓您的電話號碼不會顯示在對方的顯示面板上。
隱藏撥出號碼 [解除] **(Hide caller ID [Deact])**	請撥打此區所設定的號碼，解除此項功能。
來電待接 [執行] **(Call Waiting [Act])**	請撥打此區所設定的號碼，讓所有的來電等待您的回應。
來電待接 [解除] **(Call Waiting [Deact])**	請撥打此區所設定的號碼，解除此項功能。
封鎖匿名 [執行] **(Block Anonymous[Act])**	請撥打此區所設定的號碼，封鎖所有未之身分的來電。
封鎖匿名 [解除] **(Block Anonymous[Deact])**	請撥打此區所設定的號碼，解除此項功能。
封鎖不明網域 [執行] **(Block Unknown Domain [Act]**	請撥打此區所設定的號碼，封鎖所有未知網域的來電。
封鎖不明網域 [解除] **(Block Unknown Domain [Deact])**	請撥打此區所設定的號碼，解除此項功能。
封鎖 IP 來電 [執行] **(Block IP Calls [Act])**	請撥打此區所設定的號碼，封鎖所有自 IP 位址的來電。
封鎖 IP 來電 [解除] **(Block IP Calls [Deact])**	請撥打此區所設定的號碼，解除此項功能。
封鎖最後來電 [執行] **(Block Last Calls [Act])**	請撥打此區所設定的號碼，封鎖最後的來電。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

IV-1-4-5 PSTN 設定(PSTN Setup)

某些緊急電話(例如 119)或是特殊電話，可能無法使用 VoIP 功能撥出，只能透過 PSTN 線路來撥打，爲了解決這類的問題，本頁可讓您設定 5 個 PSTN 號碼，無須透過網際網路即可撥打。請勾選**啓用(Enable)**方框，接著可在 **PSTN 中繼電話號碼(Phone number for PSTN relay)**欄位輸入 PSTN 號碼，之後即可在需要時隨時得以撥出。



完成設定之後，按下確定(OK)按鈕儲存相關設定。

IV-1-5 電話設定(Phone Settings)

本頁讓使用者得以個別設定 Phone 1 和 Phone 2 。

VoIP >> Phone Settings

Index	Port	Call Feature	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay
1	Phone1	CW,CT,	User Defined	5/5		OutBand
2	Phone2	CW,CT,	User Defined	5/5		OutBand

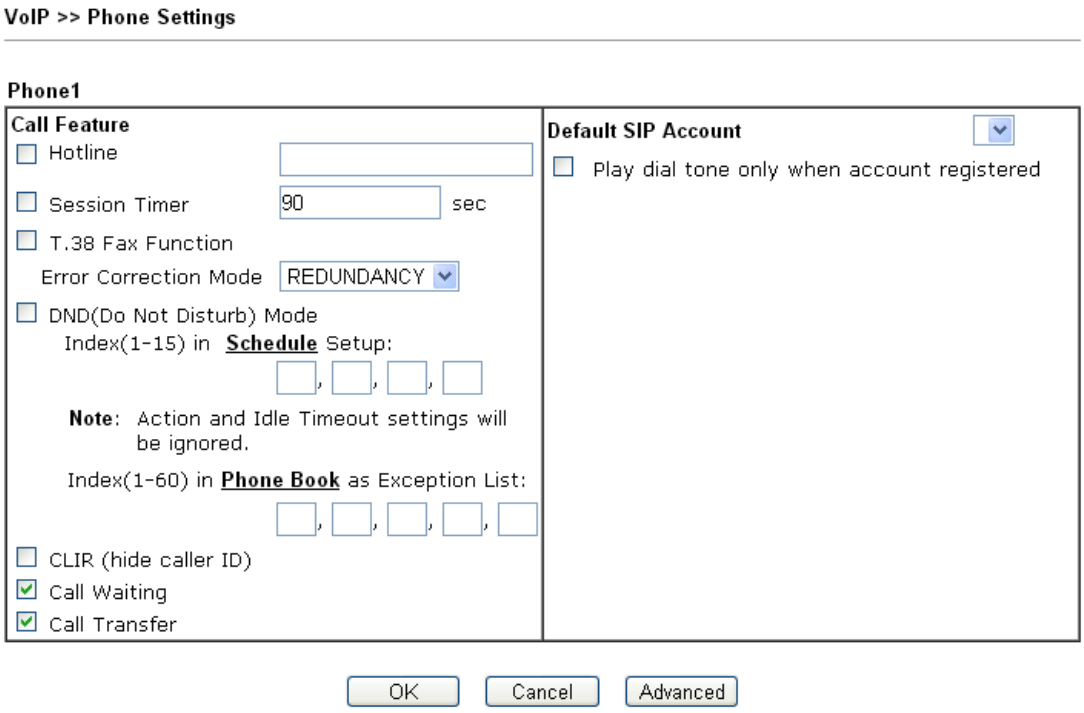
可用設定說明如下：

項目	說明
電話設定(Phone Setting)	**通訊埠(Port) –** 有種通訊埠類型提供給您選擇。 **通話功能(Call Feature)** – 這個欄位簡單描述此通電話的功能供使用者參考。 **音調(Tone)** – 顯示進階頁面所設定的音調值。 **音量(Gain)** – 顯示進階頁面中 Mic/Speaker 的音量設定。 **預設 SIP 帳號(Default SIP Account)** – “draytel_1” 是預設的 SIP 帳號，您可按索引下方的編號變更 SIP 帳號設定。 **DTMF 中繼(DTMF Relay)** – 顯示進階頁面中所設定的 DTMF 模式。

完成設定之後，按下確定(OK)按鈕儲存相關設定。

電話埠口的細節設定

請按電話埠口下方的 1 或 2 連結進入下面的設定頁面。

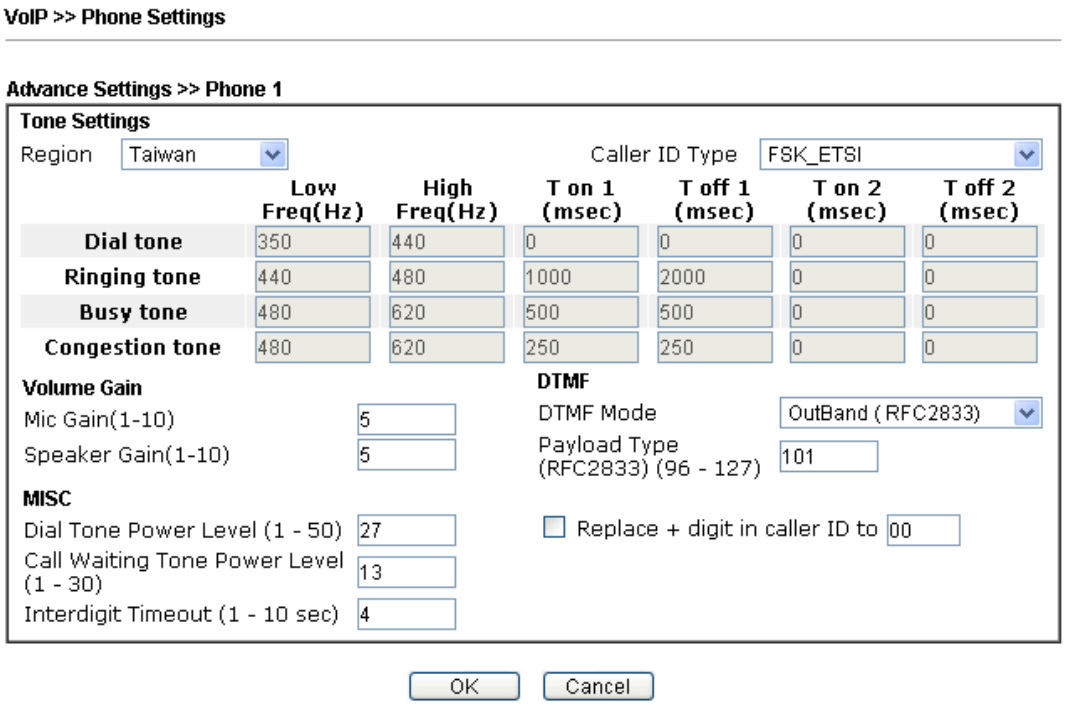


可用設定說明如下：

項目	說明
熱線(Hotline)	勾選此方塊啓用此功能，請在本區輸入 SIP URL 讓系統在您拿起話機後自動撥號。
連線數計時器 (Session Timer)	勾選此方塊啓用此功能，您在本區所設定的限制時間內如果沒有任何回應，連線電話將會自動關閉。
T.38 傳真功能 (T.38 Fax Function)	勾選此框啓用 T.38 傳真功能。 **錯誤校正模式(Error Correction Mode)** – 選擇一種錯誤校正的模式類型。
DND (勿干擾)	設定一段和平時間不受任何 VoIP 來電的幹擾。在此期間，撥號進來的人會聽到忙線的聲音，而本機用戶則聽不到任何電話鈴聲。 **索引(1-15) 於排程(Index (1-15) in Schedule) -** 輸入排程設定檔之索引編號以便控制電話何時響鈴何時靜音。 **索引(1-60) 於電話簿(Index (1-60) in Phone) -** 輸入例外電話於此方塊內，列於此之電話不受勿幹擾的限制。詳細設定請參考**電話簿**一節。
CLIR (隱藏撥號者身分)	勾選此方塊讓撥號者身分不會顯示在話機的顯示面板上。
話中插接(Call Waiting)	勾選此方塊啓用此功能，提示聲音將會出現以告知使用者有電話在等待。
電話轉接(Call Transfer)	勾選此方塊啓用此功能，按轉接鍵轉接另一通電話，當電話連線成功時，掛上電話。此時另外二方就可直接溝通。
預設 SIP 帳號	您可以設定 SIP 帳號(最多 6 組)，請使用下拉式清單選擇其中一組作爲預設帳號。

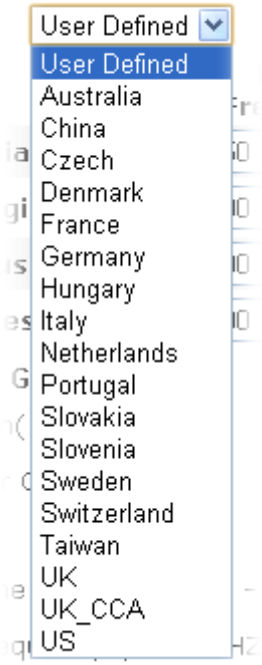
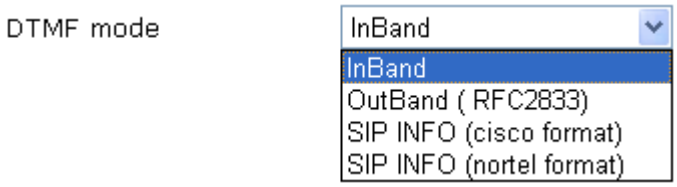
(Default SIP Account)	**當帳號已經註冊時請使用撥號音(Play dial tone only when account registered) -** 勾選此方塊啓用此功能。

此外，您也可以按**進階(Advanced)**按鈕進入深一層的設定。此項設定是爲了符合路由器安裝所在地區的電信習慣而提供，錯誤音調設定可能會造成使用者的不便。關於設定話機的聲音型態，方法很簡單，只要選擇適當的區域讓系統自動尋找事先設定的音調設定和呼叫 ID 類型，或是您也可選擇使用者自訂，然後以手動方式調整音調，TOn1, TOff1, TOn2 和 TOff2 表示音調型態的韻律，TOn1 和 TOn2 表示開啓聲音；TOff1 和 TOff2 則表示關閉聲音。



可用設定說明如下：

項目	說明
地區(Region)	選擇您目前所處地區，**來電顯示類型(Caller ID Type)**、**撥號(Dial tone)**、**響鈴音(Ringing tone)**、**忙線音(Busy tone)**和**系統擁塞音(Congestion tone)**都會自動顯示在本頁面上。如果您無法找到適合的地區，請您選擇**使用者自訂(User Defined)**，再自行輸入頁面所需的各式資料。

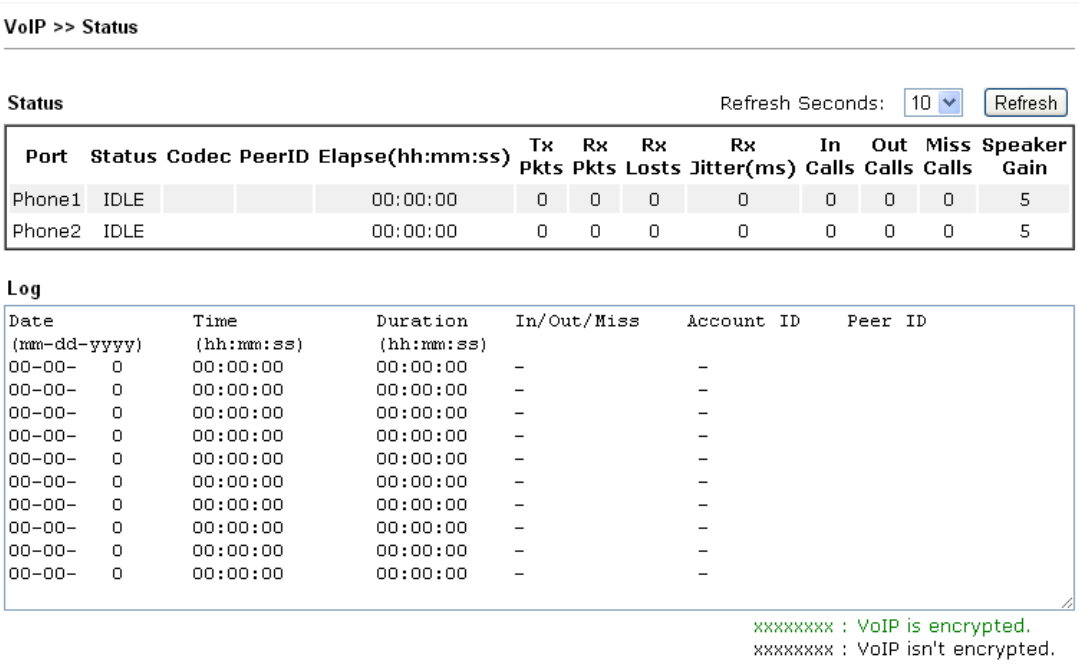
	 您也可以是個人需要指定各個區域內容，建議您採用預設值作爲 VoIP 通訊之用。
來電顯示類型 (Caller ID Type)	此處提供數種標準，以便在電話機面板上顯示來電者的身分，請依照路由器安裝所在地區選擇適合的類型，如果您不知道話機究竟支援哪種標準，請直接採用預設值。
音量控制(Volume Gain)	**麥克風音量/喇叭音量(Mic Gain (1-10)/Speaker Gain (1-10))**- 請輸入 1- 10 以設定麥克風的音量，數字越大聲音越大。
雜項(MISC)	**撥號音量控制(Dial Tone Power Level)** -此項設定用來調整撥號的音量大小，數字越小音量越大，建議使用預設值。 **振鈴聲頻率(Call Waiting Tone Power Level)-** 此項設定用來驅動鈴聲的頻率，建議使用預設值。 **Interdigit 逾時(Interdigit Timeout)** – 輸入數值以指定限制時間限制。
DTMF	**DTMF 模式(DTMF Mode) –** 有四種類型可選擇。  ● *InBand* **-**當您按壓電話上的鍵盤時，路由器將會直接以聲音模式傳送 DTMF 音調。 ● *OutBand* **-**路由器將會抓取您所按壓的鍵盤號碼然後以數位格式傳送至另一端；接收者將會依照所接收的數位格式來產生音調。這個功能在網路擁塞的情形下是很有用處的，因爲它仍可保持 DTMF 音調的準確度。 ● *SIP 資訊(SIP INFO)*- 路由器將抓取 DTMF 音調然後以 SIP 訊息轉送給遠端用戶。 **Payload 類型 (rfc2833)** - 請自 96 至 127 中選擇一個數字，預設值爲 101，此項設定只對 OutBand (RFC2833)模式有效。

	更換來電者 ID 的+符號至(Replace + digit in caller ID to) - 對於國際電話，電話號碼可以加上+符號，例如+8865972727。不過來電者 ID(特別是 DTMF 類型)是無法顯示+符號的。 因此，可以啓用此功能以便指定另一個號碼，來更換+符號。例如，可用 00 來表示 “+” 符號。之後上述電話號碼就會成爲 008865972727。當來電者接收到此號碼，他可以使用重撥號功能撥打回電。

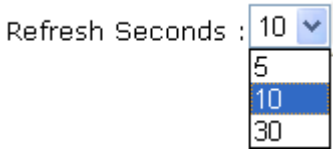
完成上述設定後，按下**確定(OK)**儲存設定。

IV-1-6 狀態(Status)

在 VoIP 撥號狀態下，您可以看見 VoIP 1 和 VoIP 2 的 codec、連線情形和其他重要的撥號狀態資料。



可用設定說明如下：

項目	說明
更新間隔秒數 (Refresh Seconds)	指定更新的間隔秒數以取得最新的 VoIP 撥號資訊，當按下**更新頁面**按鈕時，頁面資訊將會立即更新。 
通訊埠(Port)	顯示目前 VoIP 電話的連線通訊埠。
狀態(Status)	顯示 VoIP 連線狀態。 **IDLE -**表示 VoIP 功能正處於閒置狀態。 **HANG_UP -**表示連線並未建立(忙線音調)。 **CONNECTING -**表示用戶正撥出號碼中。 **WAIT_ANS -**表示已連線並等待遠端用戶的回答。 **ALERTING -**表示有來電。

	ACTIVE-表示 VoIP 連線啓動。
Codec	表示目前頻道所利用的聲音 codec。
對方 ID (PeerID)	撥進或撥出之對方 ID (格式可以是 IP 位址或是網功能變數名稱稱)。
經過時間 (Elapse(hh:mm:ss))	通話時間以秒數計算，格式爲時：分：秒 (hours:minutes:seconds)。
傳送封包數(Tx Pkts)	在連線中全部的傳送封包數量。
接收封包數(Rx Pkts)	在連線中全部的接收封包數量。
漏失接收封包(Rx Losts)	在連線中漏失的全部封包。
接收抖動(Rx Jitter)	接收聲音封包抖動狀態。
來電(In Calls)	已接來電總數。
撥出電話(Out Calls)	撥出電話總數。
漏接電話(Miss Calls)	未接到之電話總數。
接聽音量(Speaker Gain)	電話音量大小。
記錄(Log)	顯示 VoIP 電話紀錄。

IV-1-7 自我診斷(Diagnostics)

VoIP 自我診斷用於診斷 VoIP 電話撥通失敗是否是因爲音調不同還是來電者 ID 不同而造成。

VoIP >> Diagnostics

VoIP Diagnostics

Caller ID
Tone

IV-1-7-1 來電者 ID (Caller ID)

VoIP >> VOIP Diagnostics

Send Caller ID

FXS 1 | FXS 2

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 音調(Tone)

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

第五篇 VPN 連線設定



VPN

VPN是虛擬網路的延伸，包含共享或公共網路(如網際網路)，簡而言之，透過VPN技術，您可以透過模擬點對點虛擬連結的方式，在二台電腦之間傳送資料。



SSL VPN

爲一種可用於標準的網頁瀏覽器的VPN形式。



Certificate Management

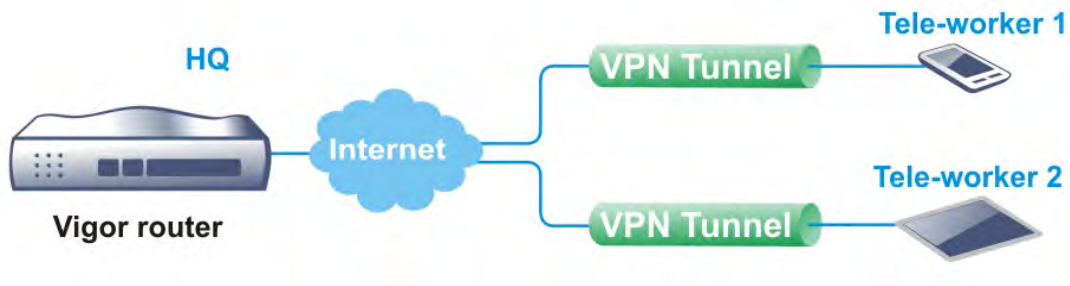
數位憑證的作用就像是電子ID，是由憑證中心(CA)所發行的，包含的內容資訊有名稱、序號、到期日期以及憑證單位發行的數位簽章，讓收取者可以驗證憑證是否真實，Vigor路由器支援符合標準X.509的數位憑證。

V-1 VPN 與遠端存取(VPN and Remote Access)

VPN 是 Virtual Private Network (虛擬私有網路) 的縮寫，是一種利用公眾網路建立一個虛擬的、安全的、方便的通道。企業可透過這個安全通道讓兩個不同地方的辦公室互通內部資料或讓出差在外的辦公人員可以遠端撥入 VPN 通道擷取公司內部的資料。

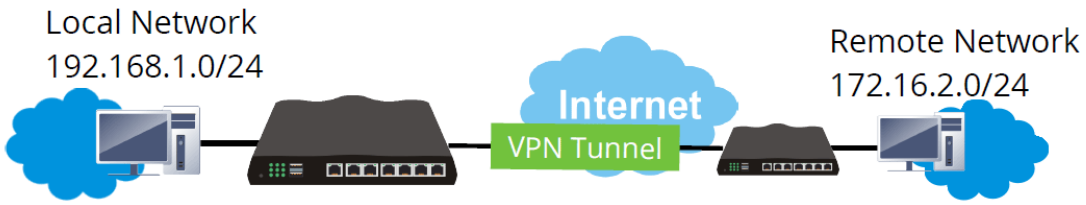
VPN 建構適合用於：

- 家用辦公室與客戶間的聯繫
- 遠距工作人員、出差人員與主辦公室之間的安全連線
- 遠端辦公室與主辦公室之間交換資料
- 分公司與總公司間的 POS 銷售情報系統



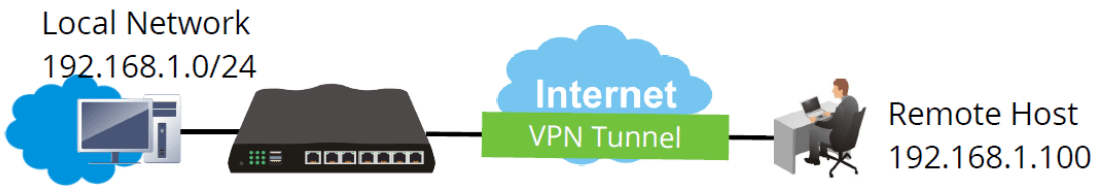
站對站(LAN-to-LAN)

- 二台路由器 LAN 網路間的連線
- 允許分支機構雇員和總公司分享相同的網路資源



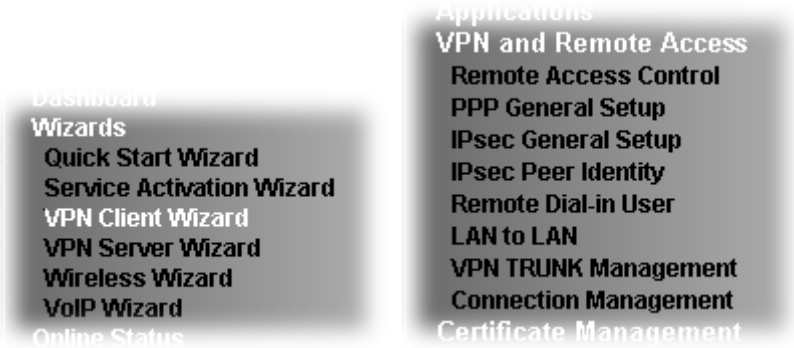
遠端存取(遠端撥入)

- 遠端主機與路由器 LAN 網路之間的連線，主機將使用本機子網中的 IP 位址
- 允許雇員在外商旅時存取公司內部資源



網頁使用者介面

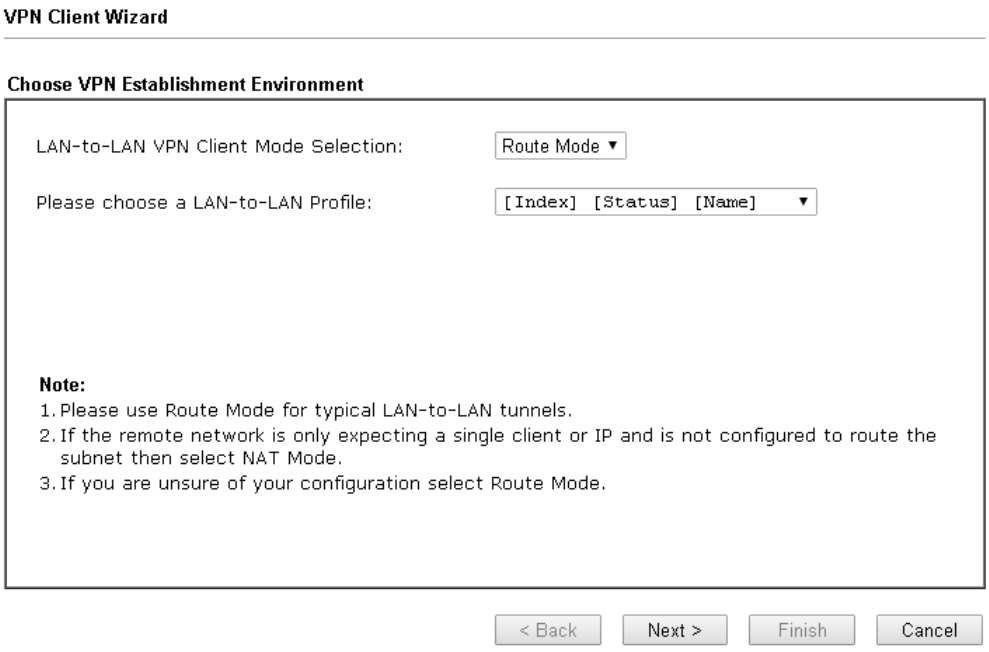
下圖爲 VPN 與遠端存取的主要功能項目：



V-1-1 VPN 用戶端設定精靈(VPN Client Wizard)

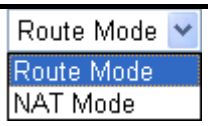
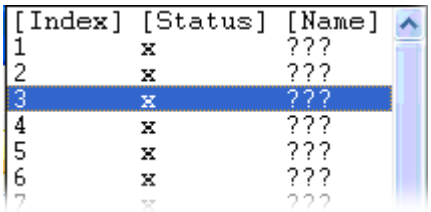
此精靈用來設定 VPN 用戶端所需的 VPN 設定，精靈將引導您一步步建立 VPN 撥出方向的 LAN-to-LAN 設定檔(從伺服器到用戶端)。

1. 開啓**設定精靈>VPN 用戶端設定精靈(Wizards >>VPN Client Wizard)**，設定頁面如下所示：

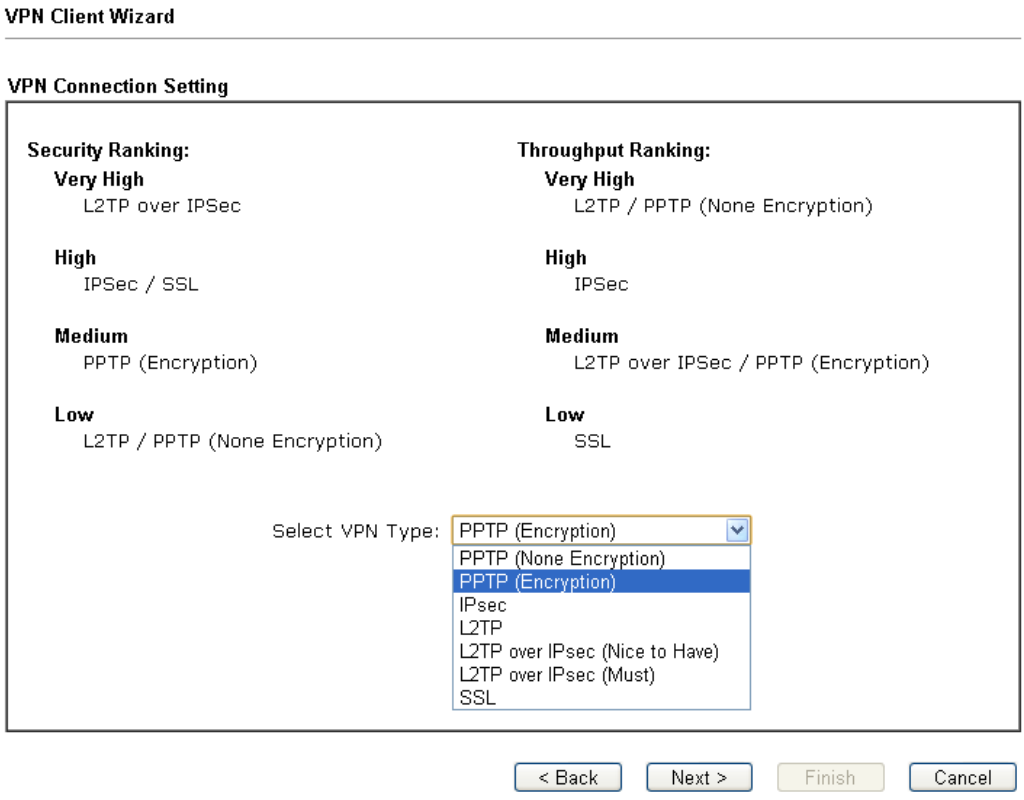


可用設定說明如下：

項目	說明
LAN-to-LAN 用戶端模式選項 (LAN-to-LAN Client Mode Selection)	選擇用戶端模式。 **路由模式/NAT 模式(Route Mode/NAT Mode)** – 如果遠端網路只允許您以單一 IP 撥入，請選擇此一模式，否則請選擇路由模式。

	
請選擇 LAN-to-LAN 設定檔 **(Please choose a LAN-to-LAN Profile)**	共有 32 個 VPN 設定檔可以供使用者選擇來設定。 

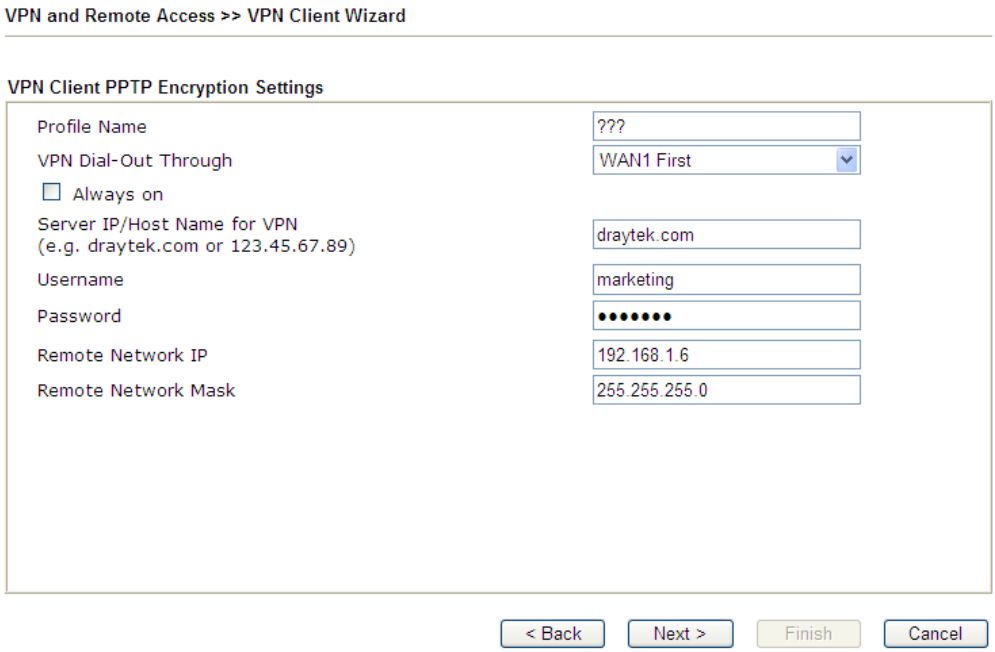
2. 選擇好模式與設定檔選項之後，請按**下一頁(Next)**開啓下一個頁面。



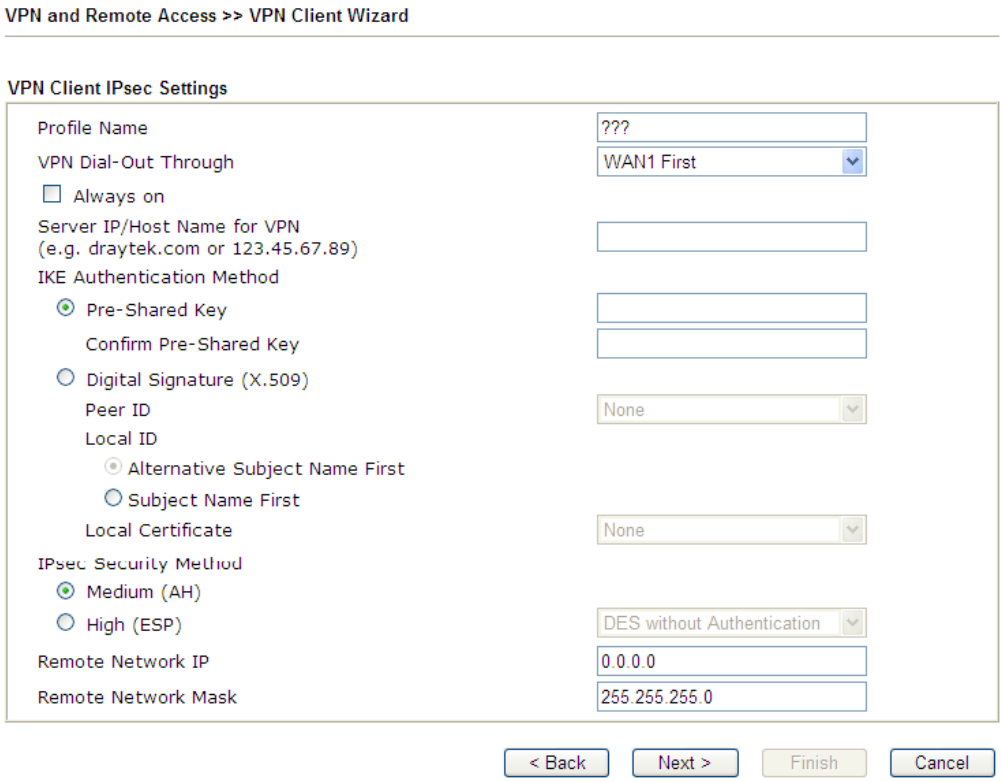
在本頁中，您必須針對 VPN 用戶設定檔選擇適當的 VPN 類型，總共有 6 個類型可以選擇，不同的類型會導引出不同的配置頁面，在選擇完畢後，請按**下一頁(Next)**，根據您所選擇的條件，您將會看到不同的配置畫面：

資訊	以下提供的 VPN 類型說明以**路由模式**爲基準。

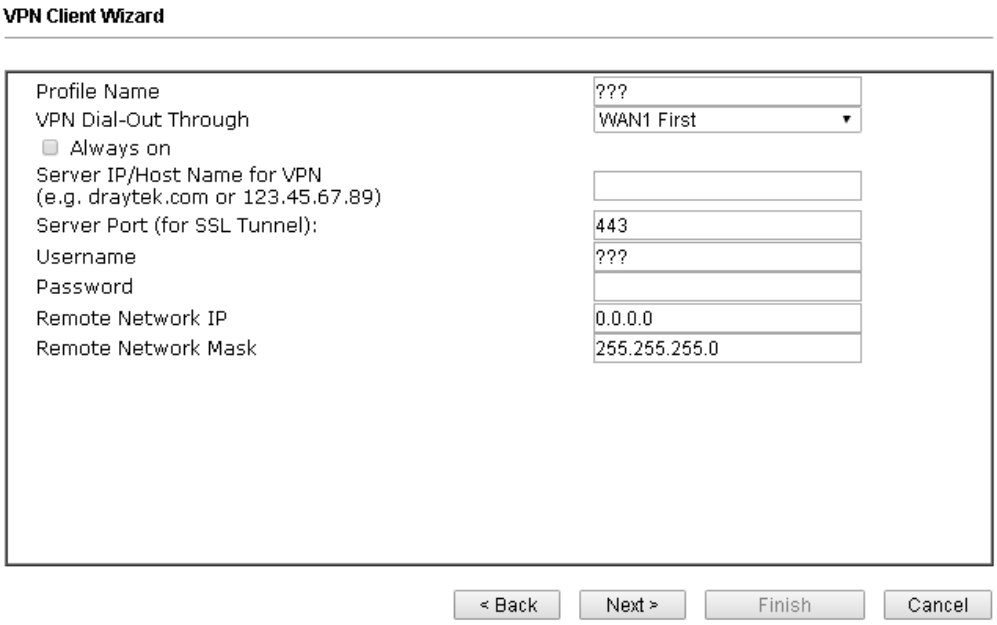
當您選擇 **PPTP (None Encryption)** 或 **PPTP (Encryption)**時，您會看到如下頁面：



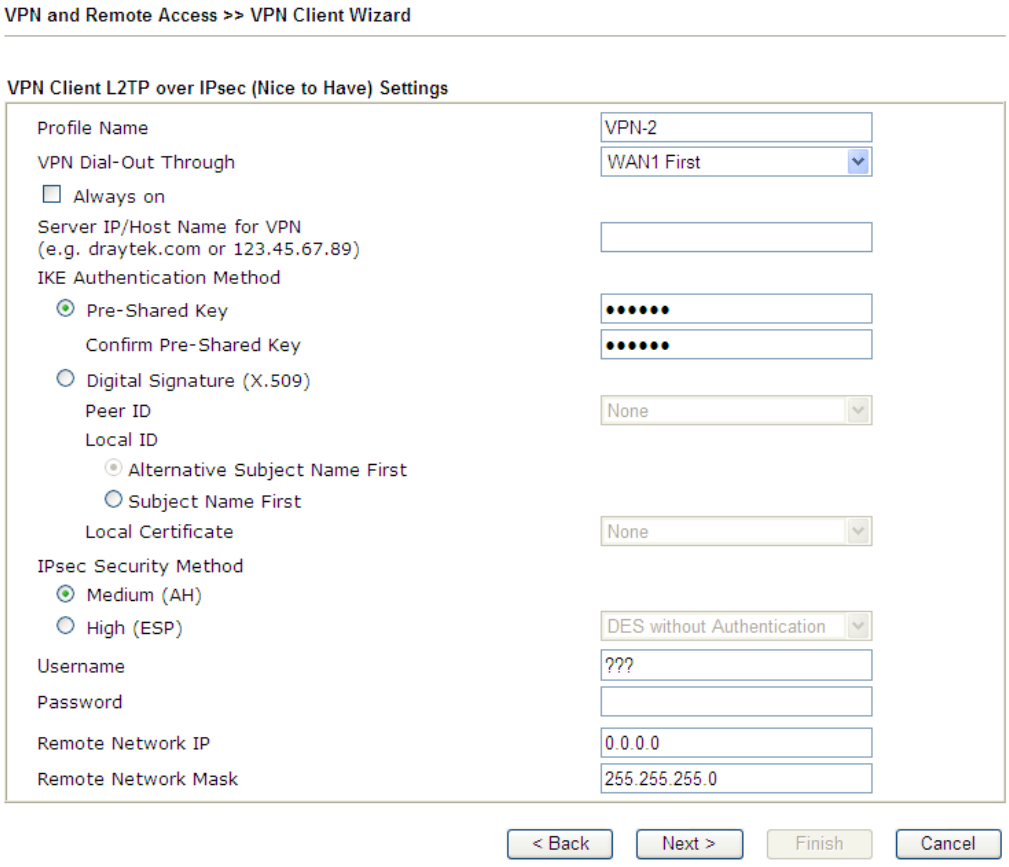
當您選擇 **IPSec** 您看到的頁面如下：



當您選擇 **SSL** 您看到的頁面如下：

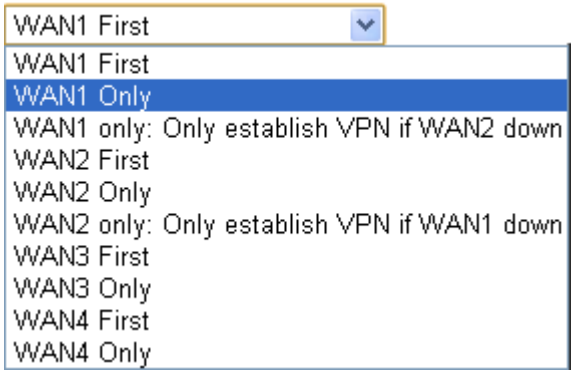
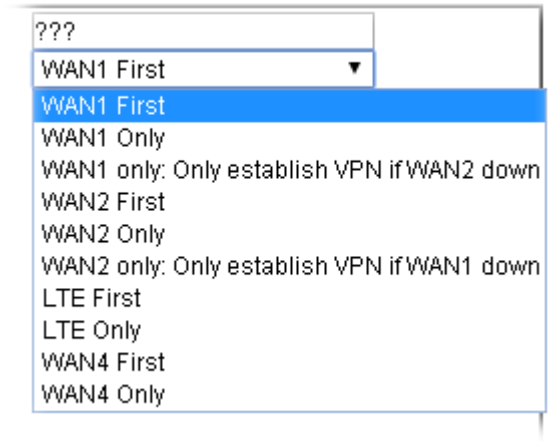


當您選擇 **L2TP over IPSec (Nice to Have)** 或是 **L2TP over IPSec (Must)**，您看到的頁面如下：



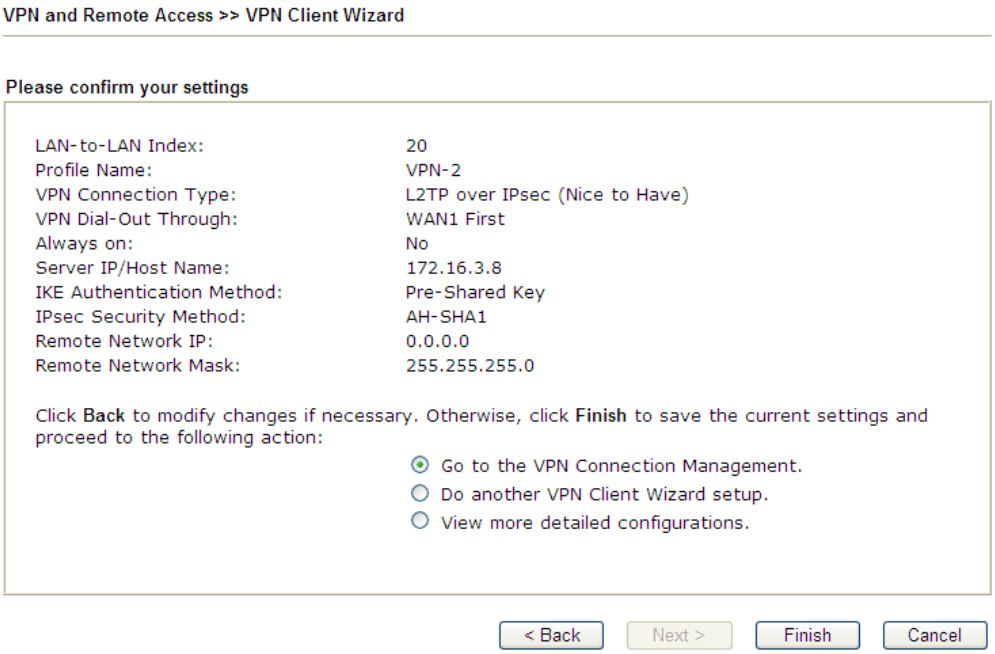
可用設定說明如下：

項目	說明
設定檔名稱	請輸入設定檔的檔名，檔案的長度限制在 10 的字元間。

(Profile Name)	
VPN 連線經由介面(VPN Dial-Out Through)	使用下拉式選項選擇適合的 WAN 介面，此設定僅適合撥出時使用。  或是，  **WAN1 優先/ WAN2 優先/ WAN3 優先(或 LTE 優先)/WAN4 優先-** 連線時，路由器會將 WAN1 視爲 VPN 連線的首要選擇，如果 WAN1/WAN2/WAN3(或 LTE)/WAN4 連線失敗，路由器將使用其他 WAN 介面來取代。 **限用 WAN1/限用 WAN2/限用 WAN3(或限用 LTE)/限用 WAN4-** 連線時，路由器會將 WAN1/WAN2/ WAN3(或 LTE)/WAN4 視爲 VPN 連線的唯一選擇。 **限用 WAN1:如果 WAN2 斷線了** – 當 WAN2 斷線時，此 VPN 通道會經由 WAN1 連線撥打出去，亦即 WAN1 爲 WAN2 的備援介面。 **限用 WAN2: 如果 WAN1 斷線了**-當 WAN1 斷線時，此 VPN 通道會經由 WAN2 連線撥打出去，亦即 WAN2 爲 WAN1 的備援介面。
永遠連線 (Always On)	勾選此方塊讓路由器永遠保持 VPN 連線。
伺服器 IP/ VPN 的主機名稱 (Server IP/Host Name for VPN)	輸入伺服器的 IP 位址或是輸入此 VPN 設定檔的主機名稱。
IKE 驗證方式(IKE Authentication Method)	IKE 驗證方式通常套用在使用動態 IP 位址與 IPsec 相關的 VPN 連線如 L2TP over IPsec 與 IPsec 通道之遠端撥入使用者或是節點(LAN to LAN)。

	預先共用金鑰- 勾選此方塊啓用此功能並按 **IKE 預先共用金鑰**按鈕輸入金鑰及確認金鑰。 **確認預先共用金鑰-** 再度輸入金鑰內容。
數位簽章 (X.509) **Digital Signature (X.509)**	點選**數位簽章(Digital Signature)**啓用此功能。 **對方 ID (Peer ID)**–自下拉式清單中選擇對方的 ID。 **本機 ID(Local ID)** – 選擇**替代主體名稱優先**或是**主體名稱優先**。 **本地憑證(Local Certificate)** –自下拉式清單中選擇一種憑證，您必須事先在**憑證管理>>本機憑證(Certificate Management >> Local Certificate)**中設定至少一組的憑證，否則無憑證可以使用。
IPSec 安全防護方式 **(IPsec Security Method)**	對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區爲必要設定。 **中級 (AH)** 表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。 **高級 (ESP-Encapsulating Security Payload)** 表示資料將被加密及驗證，請自下拉式清單中選取適合項目： *DES **無驗證*** - 使用 DES 加密演算式，但不採用任何驗證計畫。 *DES **有驗證*** **-** 使用 DES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。 *3DES **無驗證*** - 使用三重 DES 加密演算式，但不採用任何驗證計畫。 *3DES **有驗證*** **-**使用三重 DES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。 *AES **無驗證*** - 使用 AES 加密演算式，但不採用任何驗證計畫。 *AES **有驗證*** **-**使用 AES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。
使用者名稱(User Name)	輸入字元作爲使用者名稱。當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區資料可用來驗證連線。
密碼(Password)	輸入密碼資料。當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區資料可用來驗證連線。
遠端網路 IP (Remote Network IP)	請輸入區域網路 IP 位址（依照遠端主機實際位置）建立 VPN 連線。
遠端網路遮罩 **(Remote Network Mask)**	請輸入區域網路遮罩（依照遠端主機實際位置）建立 VPN 連線。

3. 完成配置後，請按**下一頁(Next)**，確定頁面將顯示如下，如果沒有任何問題的話，您可以按下面可至不同設定頁面的按鈕，然後按**完成(Finish)**進行另一個 VPN 設定。



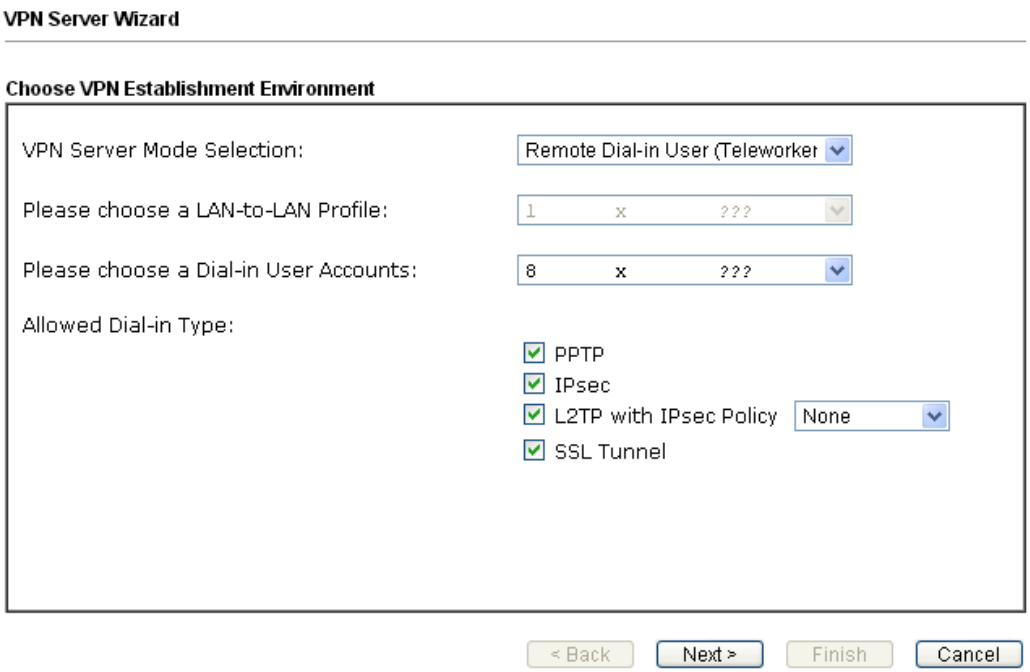
可用設定說明如下：

項目	說明
進入 VPN 連線管理 (Go to the VPN Connection Management)	按此鈕進入 **VPN 及遠端存取>>連線管理(VPN and Remote Access>>Connection Management)**頁面檢視 VPN 連線狀態。
執行另一個 VPN 伺服器精靈設定 (Do another VPN Server Wizard Setup)	按此鈕以便利用 VPN 伺服器設定精靈設定另一個 VPN 伺服器設定檔。
檢視設定詳細內容 (View more detailed configuration)	按此鈕進入 **VPN 及遠端存取>> LAN to LAN(VPN and Remote Access>>LAN to LAN)**以檢視細節內容。

V-1-2 VPN 伺服器端精靈(VPN Server Wizard)

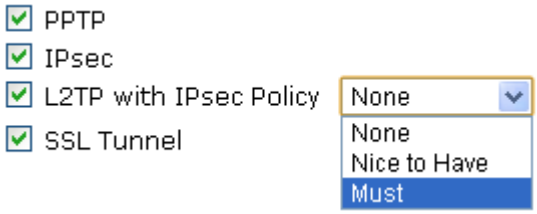
此精靈用來設定 VPN 伺服器端所需的 VPN 設定，精靈將引導您一步步建立 VPN 撥入方向的 LAN-to-LAN 設定檔(從用戶端到伺服器)。

1. 開啓**設定精靈>VPN 伺服器設定精靈(Wizards>>VPN Server Wizard)**，設定頁面如下所示：



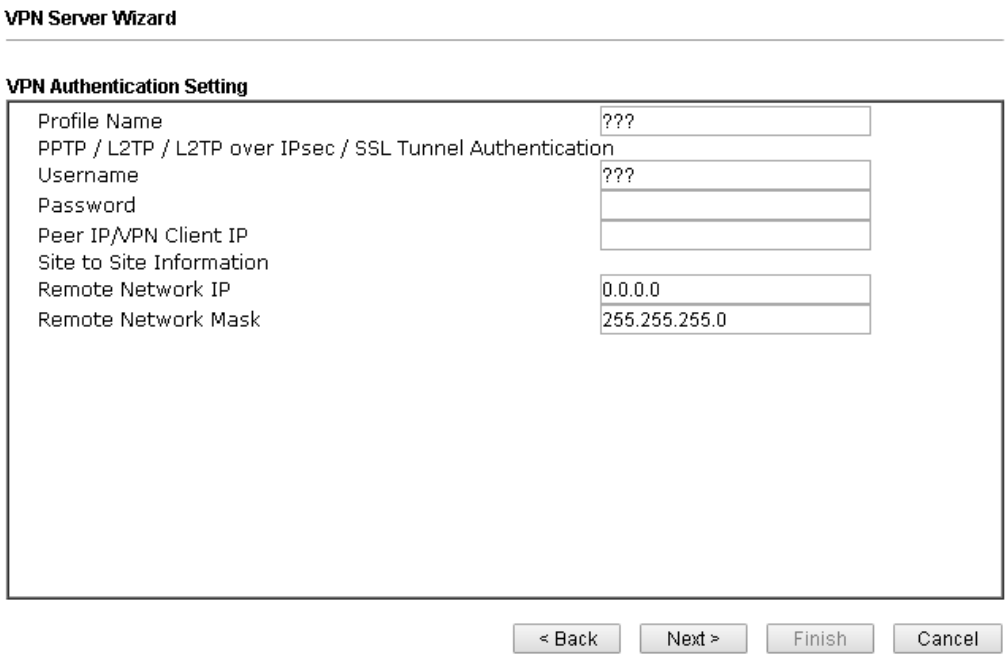
可用設定說明如下：

項目	說明
VPN 伺服器模式選項 **(VPN Server Mode Selection)**	請選擇 VPN 伺服器的方向。 **點對點 VPN (Site to Site VPN)** – 想要自動設定 LAN-to-LAN 設定檔，請選擇**點對點 VPN**。 **遠端撥入使用者(Remote Dial-in User)**– 管理遠端使用者設定檔表格來管理遠端用戶的存取狀態，使用者透過 VPN 連線存取網路時，必須接受驗證過程。 **注意**: VPN 伺服器設定精靈畫面會依據所選擇的 VPN 伺服器模式而有所不同。
請選擇 LAN-to-LAN 設定檔 **(Please choose a LAN-to-LAN Profile)**	當您選擇的是點對點 VPN（LAN-to-LAN）作爲 VPN 伺服器模式時，即可使用此設定檔，共有 32 個 VPN 設定檔可以供使用者選擇並設定。
請選擇撥入使用者帳號 **(Please choose a Dial-in User Accounts)**	當您選擇了遠端撥入使用者作爲 VPN 伺服器模式時，即可使用此項目，總共有 32 個不同的 VPN 通道供用戶設定使用。
允許的撥入類型	當您選擇了任何一個撥入使用者帳號設定檔，即可使用此類型

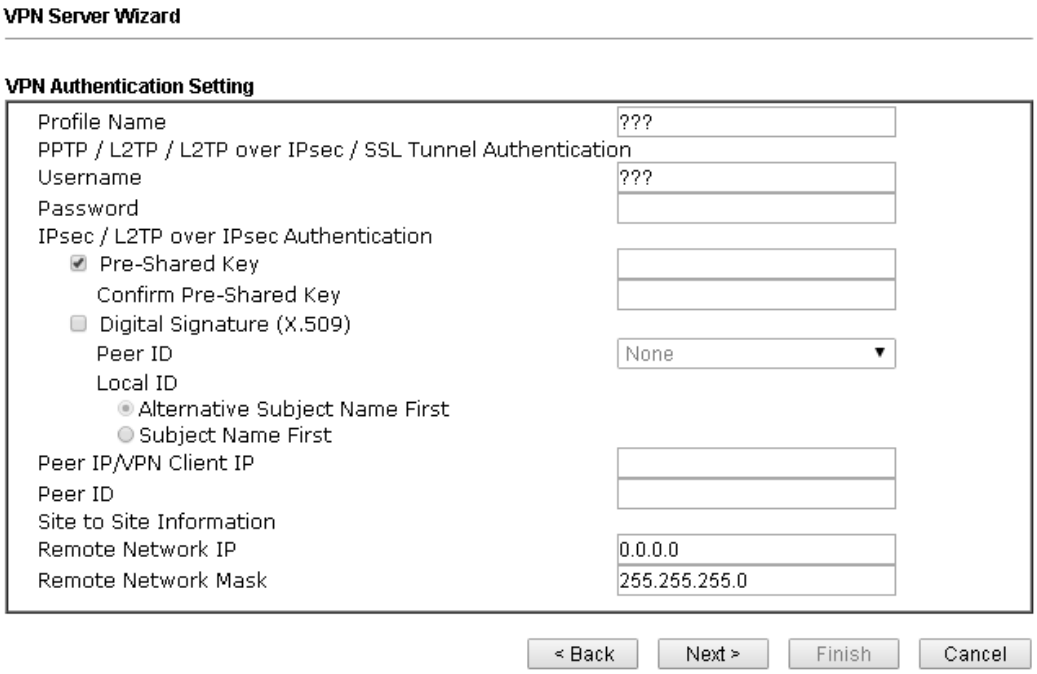
(Allowed Dial-in Type)	設定，您必須針對 VPN 伺服器設定檔選擇適當的撥入類型，此處提供數種可以選擇的項目（類似 VPN 用戶端精靈）。  不同的撥入類型所帶出的設定頁面也會有些許的差異。此外，依照選擇的 VPN 伺服器模式(**Site to Site VPN** 與 **Remote Dial-in User**)，每種撥入類型的設定項目也會隨之改變。

2. 在選擇完畢後，請按**下一步(Next)**，根據您所選擇的條件，您將會看到不同的配置畫面。此處所舉的範例是**以點對點 VPN(Site-to-Site VPN)**作爲 **VPN 伺服器模式選項(VPN Server Mode)**。

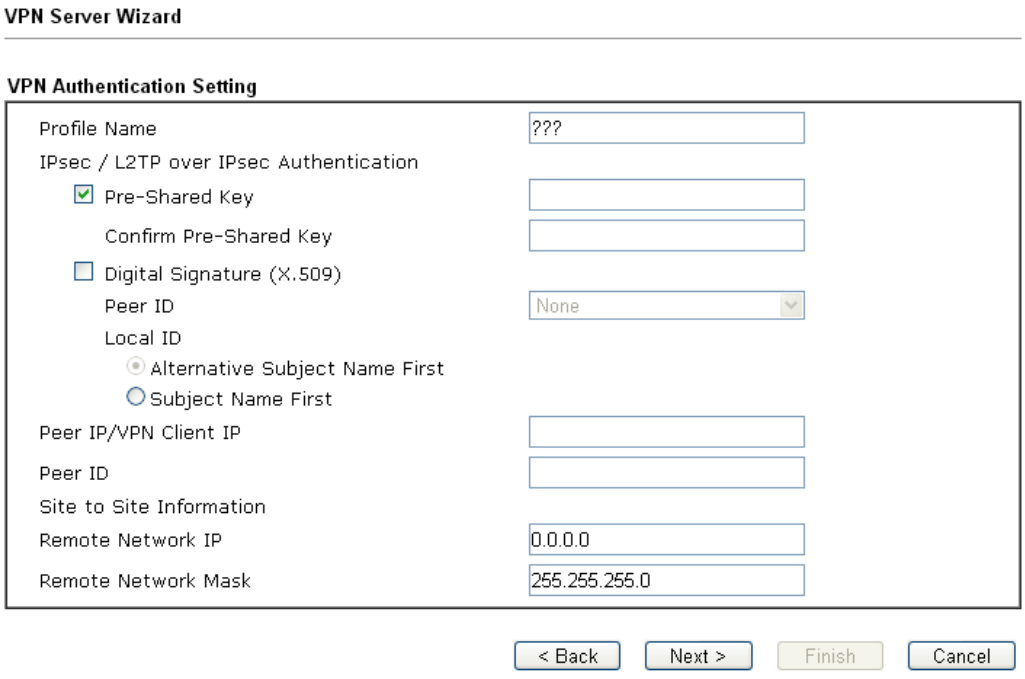
   當您勾選了 **PPTP/SSL** 之後，您會看到如下頁面：

   當您選擇 **PPTP, IPSec, L2TP** 或 **PPTP, IPSec** 或 **L2TP with Policy (建議選填/必須)**，您會看到如下頁面：



當您選擇 **IPSec**，您看到的頁面如下：

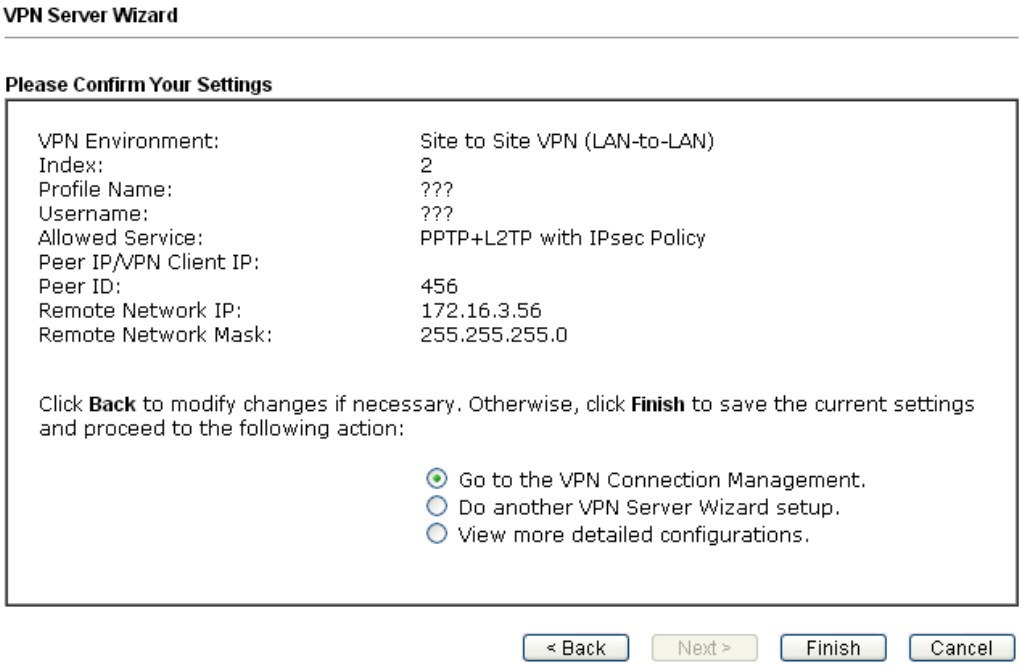


可用設定說明如下：

項目	說明
設定檔名稱 (Profile Name)	請輸入設定檔的檔名，檔案的長度限制在 10 的字元間。
使用者名稱 (User Name)	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區資料可用來驗證連線。
密碼 (Password)	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區資料可用來驗證連線。

預先共用金鑰 (Pre-Shared Key)	爲了驗證 IPSec/L2TP IPSec，請輸入金鑰內容。
確認預先共用金鑰 (Confirm Pre-Shared Key)	再輸入一次金鑰內容確認。
數位簽章 (X.509) (Digital Signature (X.509))	勾選此方塊啓用此功能並選擇一組事先定義的簽章內容 (在 **VPN 和遠端存取>>IPSec 端點辨識**中設定)。 **Peer ID** – 自下拉式清單中選擇一組對方 ID。 **Local ID** – 選擇 **Alternative Subject Name First** 或是 **Subject Name First**.
對方 IP/VPN 用戶端 IP (Peer IP/VPN Client IP)	請輸入遠端用戶的 WAN IP 位址或是 VPN 用戶端 IP 位址。
對方 ID (Peer ID)	請輸入遠端用戶的 ID 名稱。
遠端網路 IP (Remote Network IP)	請輸入區域網路 IP 位址（依照遠端主機實際位置）建立 VPN 連線。
遠端網路遮罩 (Remote Network Mask)	請輸入區域網路遮罩（依照遠端主機實際位置）建立 VPN 連線。

3. 完成配置後，請按**下一步(Next)**，確定頁面將顯示如下，如果沒有任何問題的話，您可以按下面可至不同設定頁面的按鈕，然後按**完成(Finish)**進行另一個 VPN 設定。



可用設定說明如下：

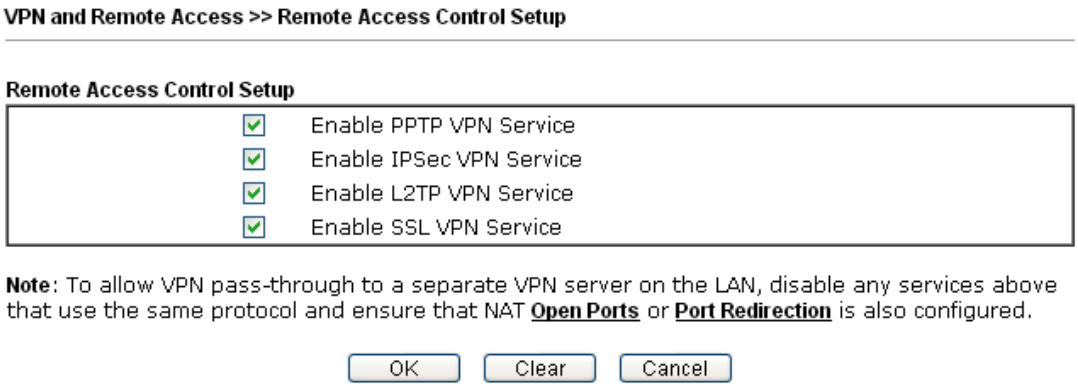
項目	說明

進入 VPN 連線管理 (Go to the VPN Connection Management)	按此鈕進入 VPN 及**遠端存取>>連線管理(VPN and Remote Access>>Connection Management)**頁面檢視 VPN 連線狀態。
執行另一個 VPN 伺服器精靈設定 (Do another VPN Server Wizard Setup)	按此鈕以便利用 VPN 伺服器設定精靈設定另一個 VPN 伺服器設定檔。
檢視設定詳細內容 (View more detailed configuration)	按此鈕進入 **VPN 及遠端存取>> LAN to LAN(VPN and Remote Access>>LAN to LAN)**以檢視細節內容。

V-1-3 遠端存取控制(Remote Access Control)

這個設定可以啓動必要的 VPN 服務，如果您想要在區域網路中執行 VPN 伺服器功能，您一定要適度關閉路由器的 VPN 服務，讓 VPN 通道暢通，並關閉類似 DMZ 或是開放埠等 NAT 設定。

開啓 **VPN 與遠端存取>>遠端存取控制(VPN and Remote Access>>Remote Access Control)**。



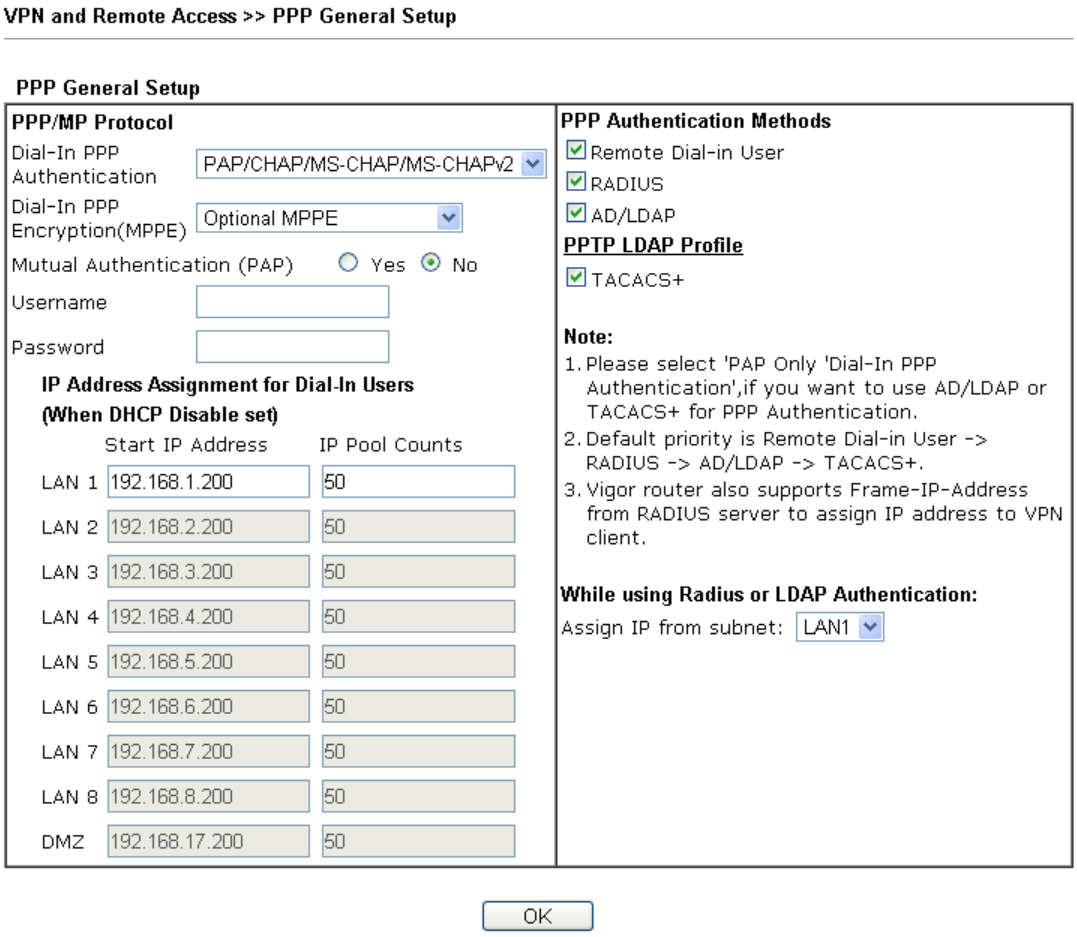
可用設定說明如下：

項目	說明
啓用 PPTP VPN 服務	勾選此方塊啓動經由 PPTP 通訊協定之 VPN 服務。
啓用 IPSec VPN 服務	勾選此方塊啓動經由 IPSec 通訊協定之 VPN 服務。
啓用 L2TP VPN 服務	勾選此方塊啓動經由 L2TP 通訊協定之 VPN 服務。
啓用 SSL VPN 服務	勾選此方塊啓動經由 SSL 通訊協定之 VPN 服務。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

V-1-4 PPP 基本設定(PPP General Setup)

這項功能可以應用在 PPP 相關的 VPN 連線中，諸如 PPTP、L2TP、L2TP over IPSec 等。



可用設定說明如下：

項目	說明
撥入 PPP 驗證 **(Dial-In PPP Authentication)**	**PAP Only -** 選擇此項目強迫路由器以PAP協定來驗證撥入使用者。 **PAP/CHAP/MS-CHAP/MS-CHAPv2 -** 選擇此項目表示路由器會嘗試先以 CHAP 協定驗證撥入使用者，如果撥入使用者沒有支援此項協定，系統會改用 PAP 協定來驗證使用者。
撥入 PPP 加密(MPPE) **(Dial-In PPP Encryption (MPPE))**	**Optional MPPE** - 此選項代表 MPPE 加密方式是由路由器針對遠端撥入使用者選擇性採用的方法，如果遠端撥入使用者沒有支援 MPPE 加密演算式，路由器將會傳送無 MPPE 加密封包出去，否則 MPPE 加密將直接用於資料加密處理。 ● **Require MPPE (40/128bits) -**選擇此項目可以強迫路由器利用 MPPE 加密演算式加密資料封包，此外遠端撥入使用者在使用 128-bit 之前可先使用 40-bit 執行加密動作，換言之，如果沒有支援 128-bit 加密法，系統將會自動使用 40-bit 加密方式於資料加密上。 ● **Maximum MPPE -**此選項指出路由器將會使用 MPPE 最大

	值(128 bits)來加密資料。
雙方共同驗證 (PAP) **(Mutual Authentication (PAP))**	共同驗證功能主要應用於和其他路由器或是需要雙向驗證的用戶連絡，以便取得更佳安全性能，因此當您的對點路由器需要共同驗證時，您就應該啓動此功能，並進一步指定使用者名稱和密碼。
指派 IP 位址 **(IP Address Assignment for Dial-In Users (when DHCP Disable set))**	輸入撥入 PPP 連線的 IP 位址(LAN1) 。 LAN2 ~ LAN6 若有啓用則亦可設定 IP 位址，可前往 **LAN>>基本設定(LAN>>General Setup)**開啓需要的 LAN 介面。
PPP 驗證方法(PPP Authentication Methods)	勾選您想要用來進行 PPP 連線驗證的方式。 **PPP Authentication Methods** ☑ Remote Dial-in User ☑ RADIUS ☑ AD/LDAP
PPTP LDAP 設定檔(PPTP LDAP Profile)	設定完成的 LDAP 設定檔將列於此處下方，選擇您想要用來進行 PPP 驗證的 LDAP 設定檔即可。 不過，若是無任何設定檔條列於此，請按此連結建立新的設定檔。
在使用 RADIUS 或 LDAP 驗證時(While using Radius or LDAP Authentication)	如果 PPP 連線將透過 RADIUS 伺服器或是 LDAP 設定檔進行驗證，您有必要指定一個 LAN 設定檔給予撥入使用者，以取得 IP 位址。

完成上述設定之後，請按下**確定(OK)**儲存。

V-1-5 IPSec IPSec 基本設定(IPsec General Setup)

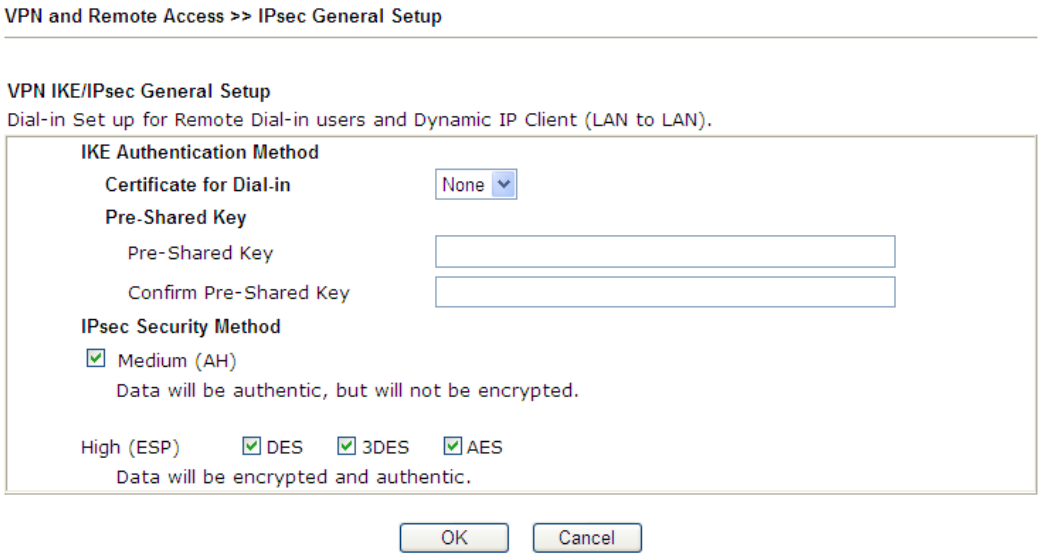
在 **IPSec 基本設定(**(IPsec General Setup))中，有二種主要的配置方式。

- 第一階段：IKE 參數的協商作業包含加密、重述、Diffie-Hellman 參數值和壽命，以保護後續 IKE 交換、使用預先共同金鑰或是數位簽章(x.509)之對等驗證。協商程式起始方提出所有的原則給遠端的另一方，遠端一方嘗試尋找符合其政策之最高優先權，最後建立一個 IKE 階段 2 的安全通道。
- 第二階段：IPSec 安全協商包含驗證封包頭(AH)或是 ESP，供後續 IKE 交換和雙邊安全通道設立之檢測之用。

在 IPSec 中有二種加密方式 – 傳送與通道，傳送模式將會增加 AH/ESP 承載量並使用原始 IP 標頭來加密承載的資料，此模式只應用於本地封包上如 L2TP over IPSec，通道模式不只增加 AH/ESP 承載量也會使用新的 IP 封包頭來加密整個原始 IP 封包。

驗證封包頭(AH) 提供 VPN 雙方的 IP 封包資料驗證和整合，可以單方重述功能來達成建立訊息摘要的動作，這些摘要隨著封包傳送將放置於封包頭。接收方將會在封包上執行同樣的動作，並與所接收到的數值比較。

封裝式安全酬載(ESP)提供選擇性驗證方法，對資料機密化和防護的安全協定，可重新進行檢測。



可用設定說明如下：

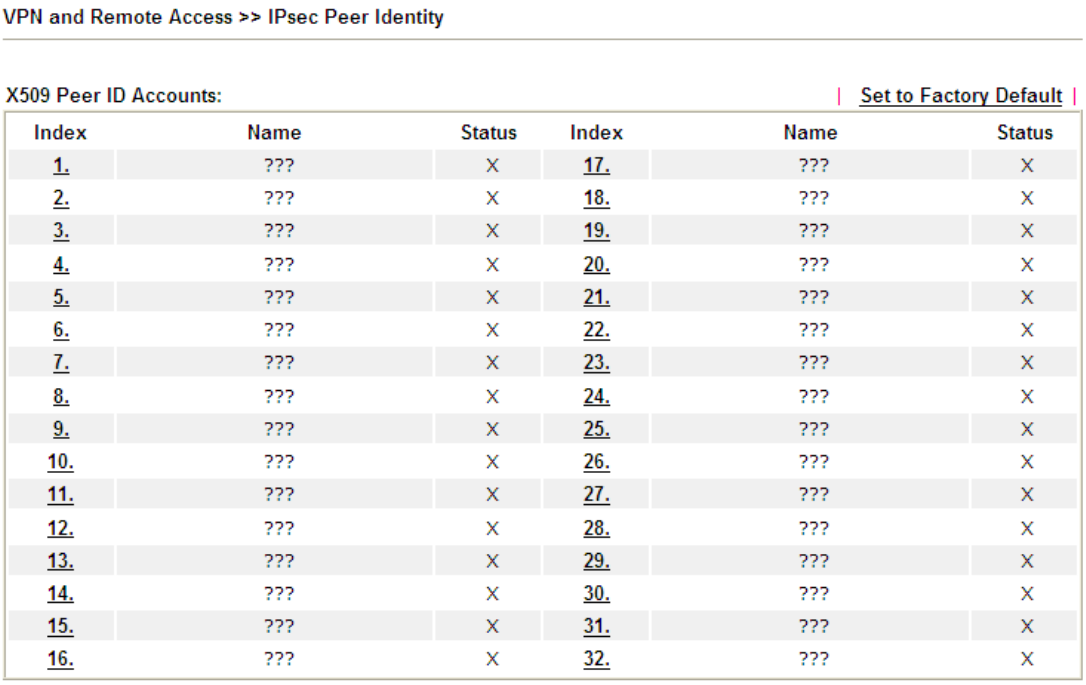
項目	說明
IKE 認證方式	通常應用在遠端撥入使用者或是使用動態 IP 位址的節點(LAN-to-LAN)以及 IPSec 相關之 VPN 連線上，像是 L2TP over IPSec 和 IPSec 通道。有二種方式可用來驗證來自遠端撥入用戶的資料 - **憑證(Certificate (X.509))** 以及**預先共用金鑰(Pre-Shared Key)**。 **撥入憑證(Certificate for Dial-in)** – 可自下拉式清單中選擇一個本機憑證。 **預先共用金鑰(Pre-Shared Key) -** 只有支援預先共用金鑰，請指定一個金鑰作爲 IKE 驗證之用。 **確認預先共用金鑰(Confirm Pre-Shared Key)-** 確認您所輸入的共用金鑰。

	注意：來自遠端撥入使用者的任何一個封包，若不符合 **VPN 與遠端存取>>遠端撥入使用者(VPN and Remote Access>>Remote Dial-In User)**定義的規則，即會套用此處選擇的方式。
IPSec 安全防護方式	**中級 (AH)** - 表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。 **高級 (ESP)** - 表示資料將被加密及驗證，請自下 DES、3DES 或 AES 中選取適合項目。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

V-1-6 IPSec 端點辨識(IPsec Peer Identity)

如果在 LAN-to-LAN 連線或是遠端撥入使用者連線上，想要使用數位認證作爲遠端驗證工具，您可以編輯對方認證表格供後續選擇使用。路由器提供 32 種 IPSec 端點辨識設定檔：



VPN and Remote Access >> IPsec Peer Identity

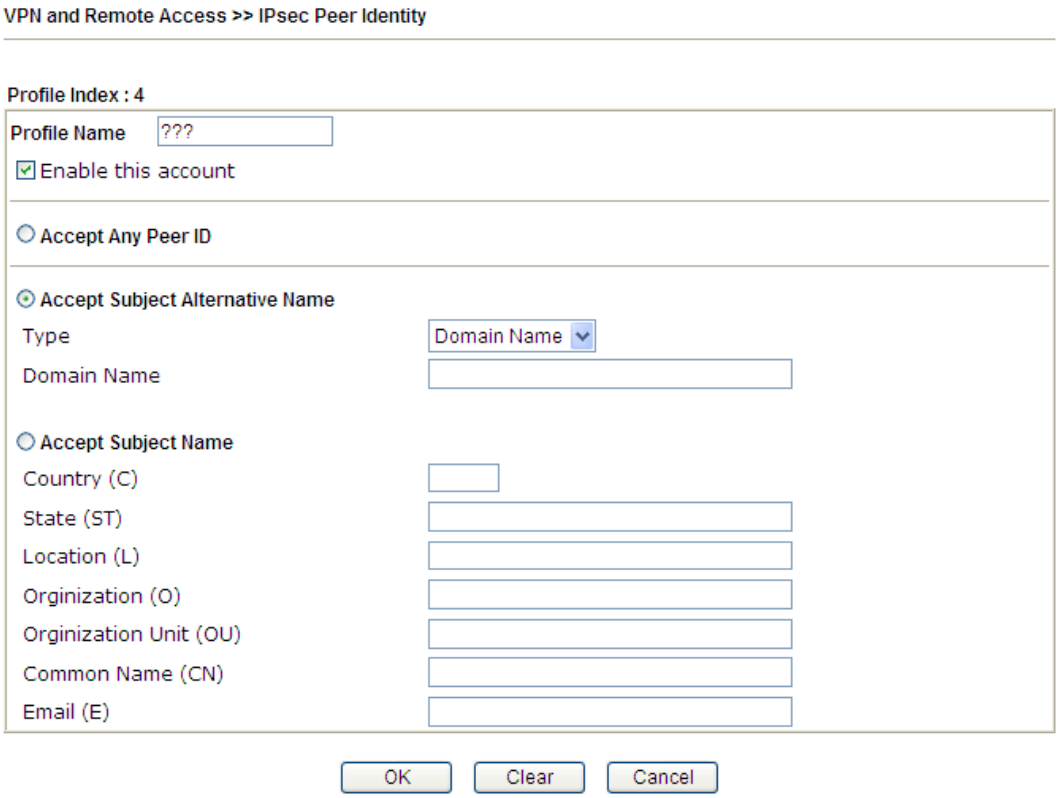
X509 Peer ID Accounts: | Set to Factory Default |

Index	Name	Status	Index	Name	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	按此鈕清除全部設定。
索引編號(Index)	請按索引下方的號碼以進入設定頁面。
名稱(Name)	顯示 LAN-to-LAN 設定檔案中特定撥入使用者的使用者名稱，符號**???**代表該設定檔是空的，未做任何設定。

點選每個索引號碼以便編輯遠端使用者設定檔，每個撥入類型需要您在右邊填入不同資訊，如果該區域是灰色的，即表示您無法在該項目做任何設定，下面的說明可以引導您於各個設定區填入相關資訊。



可用設定說明如下：

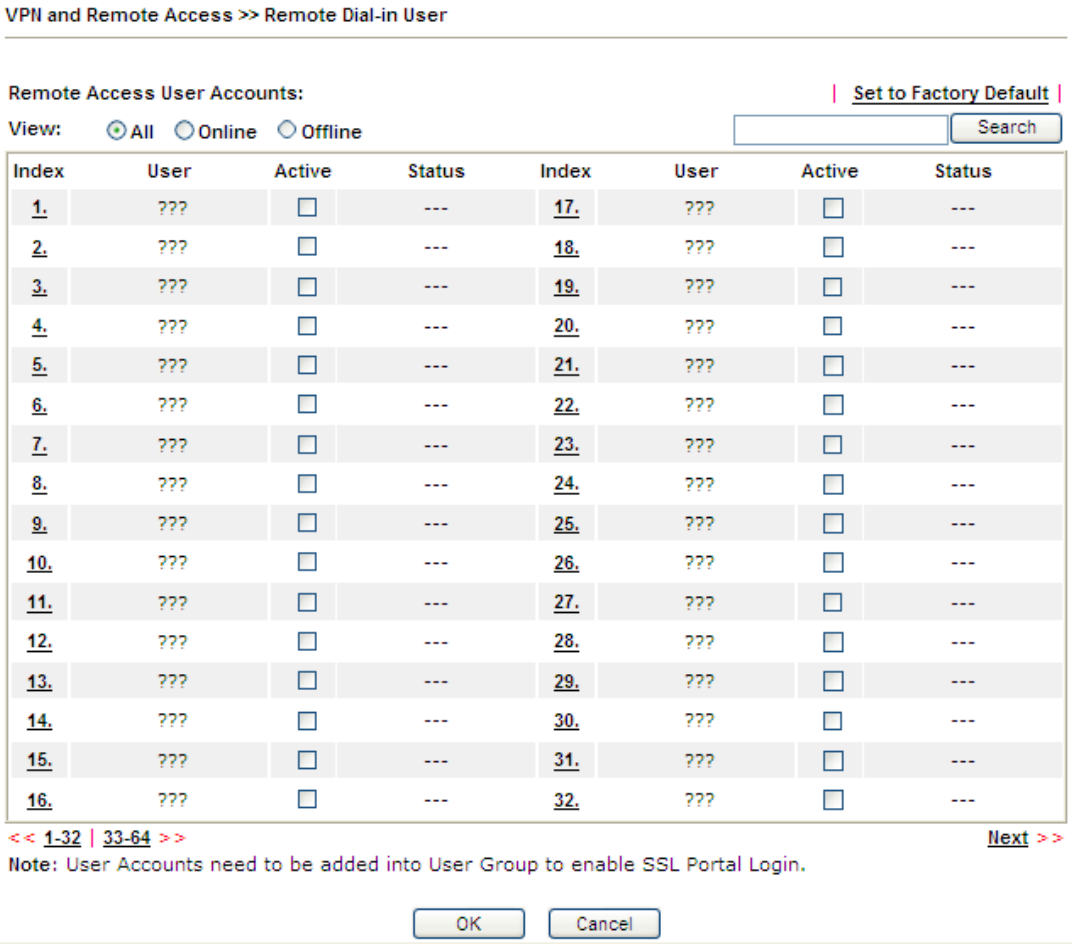
項目	說明
設定檔名稱 (Profile Name)	請輸入此設定檔的檔名。
啓動這個帳號 (Enable this account)	勾選方框啓用帳號設定檔。
接收任何對方 ID (Accept Any Peer ID)	按此鈕可以接受任何一個電腦的連線而不理會它是誰。
接受主體替代名稱 (Accept Subject Alternative Name)	按此鈕以決定特定之數位簽章接受符合要求的對手，本區可以是 IP 位址、網域或是電子郵件，類型下方區域方塊依據您所選的類型而有所不同，請按照實際需要填入必要資訊。
接受主體名稱 (Accept Subject Alternative Name)	按此鈕讓特定區域的數位簽章能接受符合要求的對手，本區包含有國家、狀態、居住地區、組織、單位、常用名稱及電子郵件等等。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

V-1-7 遠端撥入使用者(Remote Dial-in User)

藉由維護遠端使用者設定檔表格，您可以管理遠端存取狀況，這樣使用者可以經由驗證得以撥入或是建立 VPN 連線。您可以設定包含指定連線對點 ID、連線 ID (PPTP、IPSec Tunnel 以及 L2TP 和 L2TP over IPSec)等參數，和相關安全防護方式。

路由器提供 **64** 種存取使用者號碼予撥入用戶，此外經由內建 RADIUS 用戶端功能，您可以將帳號延伸至 RADIUS 伺服器。下圖顯示帳號總表格：

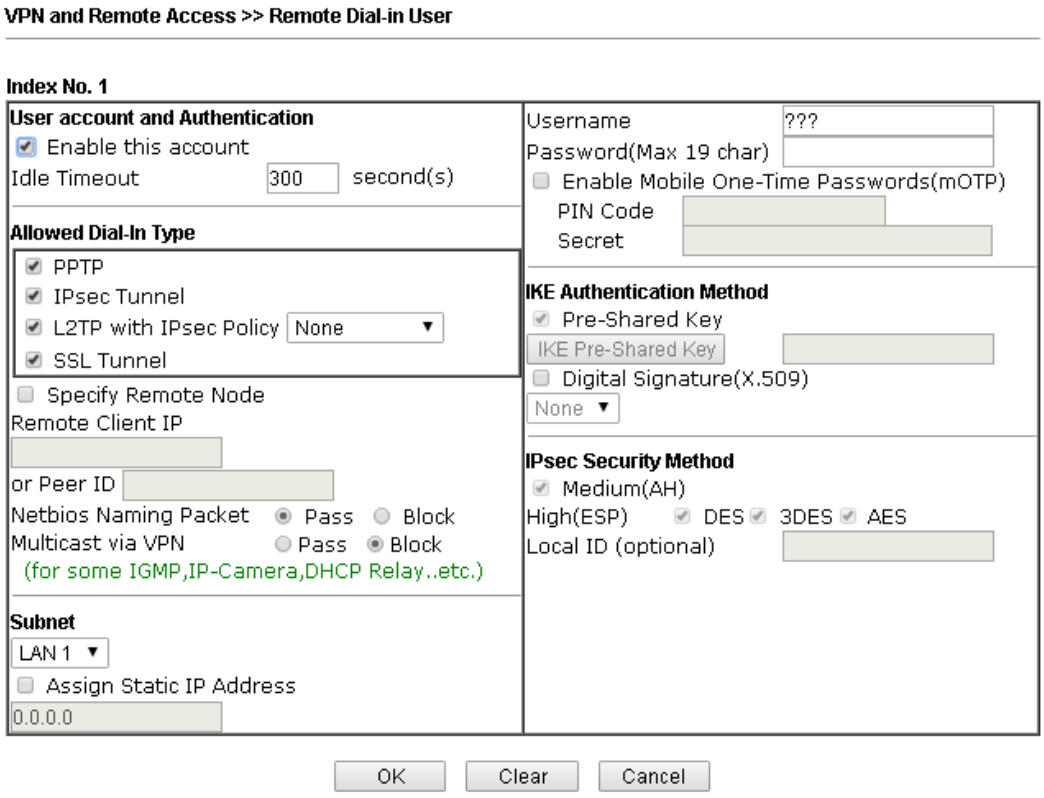


可用設定說明如下：

項目	說明
回復出廠預設值(Set to Factory Default)	按此鈕清除全部設定。
檢視	**全部(All) -** 按此顯示全部使用者帳號。 **上線(Online) -** 按此顯示上線使用者帳號。 **下線(Offline) -** 按此顯示下線使用者帳號。
索引編號(Index)	請按索引下方的號碼以進入遠端撥入使用者之設定頁面。
用戶(User)	顯示 LAN-to-LAN 設定檔案中特定撥入使用者的使用者名稱，符號**???**代表該設定檔是空的，未做任何設定。
使用中(Active)	勾選此框啓用該設定檔。

狀態(Status)	顯示特定撥入使用者的存取狀態，符號 V 和 X 分別代表活動中與不活動的檔案。

點選每個索引號碼以便編輯遠端使用者設定檔，每個撥入類型需要您在右邊填入不同資訊，如果該區域是灰色的，即表示您無法在該項目做任何設定，下面的說明可以引導您於各個設定區填入相關資訊。



可用設定說明如下：

項目	說明
使用者帳號與驗證 (User account and Authentication)	**開啓這個帳號(Enable this account) -**勾選此方塊以啓用此功能。 **閒置逾時(Idle Timeou) -** 如果撥入使用者閒置超過所設定的時間，路由器將會自動中斷連線，預設閒置逾時爲 300 秒。
允許撥入類型 (Allowed Dial-In Type)	**PPTP-**爲伺服器建立一個透過網際網路的 PPTP VPN 連線，您必須設定連線類型和身分辨識像是使用者名稱與密碼等，以便驗證遠端伺服器。 **IPSec 通道(IPSec Tunnel)-**允許遠端撥入使用者透過網際網路觸發 IPSec VPN 連線。 **具有 IPSec 原則的 L2TP(L2TP with IPSec Policy)-**爲伺服器建立一個透過網際網路的 L2TP VPN 連線。您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取： ● **無(None) -** 此選項完全不會應用 IPSec 原則，VPN 連線採用不帶有 IPSec 原則的 L2TP，可以在完全 L2TP 連線中檢視內容。 ● **建議選填(Nice to Have) -**如果在整個連線過程中完全可以運用，此選項會先應用 IPSec 原則。否則撥入

	VPN 連線會成爲一種完全的 L2TP 連線。 ● **必須(Must) -** 此選項可在L2TP連線中明確指定所要運用的 IPSec 原則。 **SSL 通道(SSL Tunnel) -** 允許遠端撥入用戶透過網際網路進行 SSL VPN 連線。 **指定遠端節點(Specify Remote Node)-**您可以指定遠端撥入使用者或是對方 ID (應用於 IKE 主動模式中)的 IP 位址。若您不勾選此項，即表示您所選擇的連線類型，將會應用**基本設定**中所設定的驗證方式和安全防護方式。 **Netbios 命名封包(Netbios Naming Packet) -** ● **通過(Pass)** – 按此鈕讓資料能在二台主機之間所建立的 VPN 通道上傳輸。 ● **封鎖(Block)** –當雙方所建立的 VPN 通道連線產生衝突時，此功能可以封鎖此通道。 **經由 VPN 執行多重播送(Multicast via VPN) -**某些程式可透過 VPN 連線進行多重播送封包。 ● **通過(Pass)** –點選此鈕讓多重播送封包通過路由器。 ● **封鎖(Block)** – 此爲預設值。點選此鈕之後，路由器將會封鎖多重播送封包。 **使用者名稱(User Name)-**當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。 **密碼(Password)-**當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。 **啓動行動動態密碼系統 (mOTP)(Enable Mobile One-Time Passwords (mOTP)) -** 勾選此框以便利用 mOTP 功能進行驗證。 **PIN 碼(PIN Code)** – 輸入驗證專用碼（例如 1234）。 **密碼(Secret)** – 使用行動電話中由 mOTP 產生的 32 個數字密碼(例如 e759bb6f0e94c7ab4fe6)。
子網路(Subnet)	選擇此 VPN 設定檔所需的子網。 **指定固定 IP 位址(Assign Static IP Address) -** 請輸入固定 IP 位址。
IKE 認證方式 **(IKE Authentication Method)**	當您指定遠端節點的 IP 位址時，本區僅適用於 **IPsec 通道**與**具有 IPSec 原則的 L2TP** 類型，唯一例外的是當您選擇 **IPsec 通道**時，不論有無指定 IP 位址，您還可以設定數位簽章(X.509)。 **預先共同金鑰(Pre-Shared Key)-** 勾選此方塊啓用此功能並輸入 1-63 文字做爲預先共同金鑰。 **數位簽章 (X.509) (Digital Signature (X.509))-**勾選此方塊啓用此功能並選擇一組事先定義的簽章內容 (在 **VPN 和遠端存取 >>IPSec 端點辨識(VPN and Remote Access >>IPSec Peer Identity)**中設定)。
IPSec 安全防護方式 **(IPSec Security Method)**	對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區爲必要設定。請勾選中級或是高級設定作爲安全防護方式。 **中級 -Authentication Header (AH)**表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。 **高級 -Encapsulating Security Payload (ESP)**表示資料將被加密及驗證，請自下拉式清單中選取適合項目。 **本機 ID(視需要填入) (Local ID (Optional))-**指定一個本地 ID 以

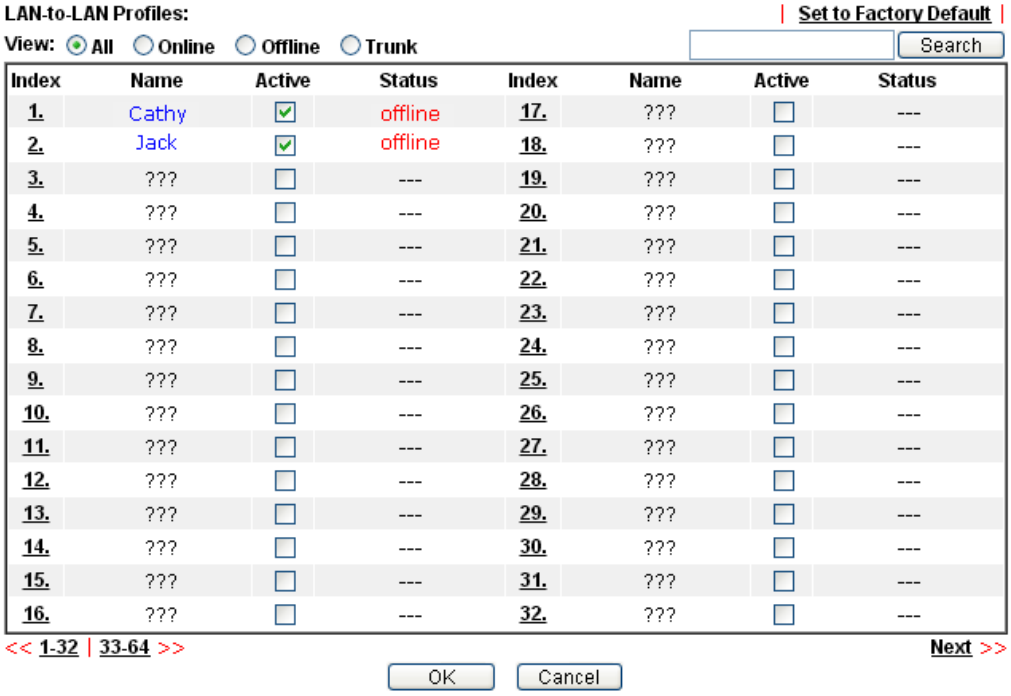
	便作爲 LAN-to-LAN 的撥入設定，此項是選擇項目且只能應用在 IKE 主動模式上。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

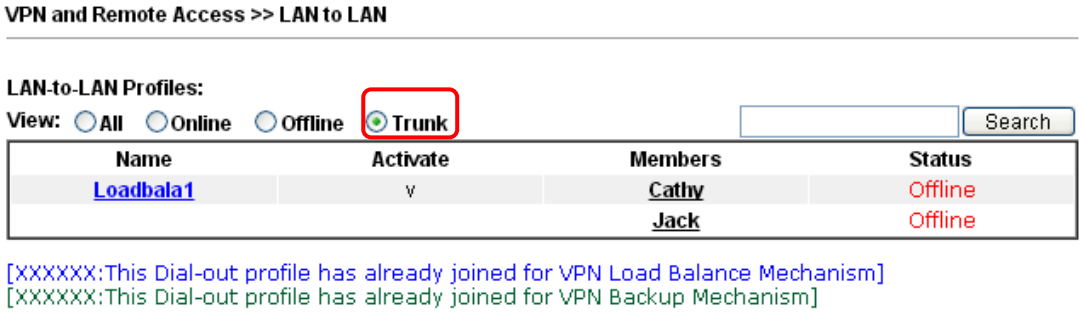
V-1-8 LAN to LAN

您可以透過維護連線檔案的表格來管理 LAN-to-LAN 連線，您可設定包含指定連線方向(撥進或是撥出)的參數、連線對方的 ID、連線型態(VPN 含 PPTP, IPSec Tunnel 和 L2TP 或是其他)以及相關的安全防護方法等等。

路由器提供 64 個設定檔，下圖顯示設定檔案的簡易清單。



下圖顯示參與 VPN 負載平衡與 VPN 備援機制之設定檔。



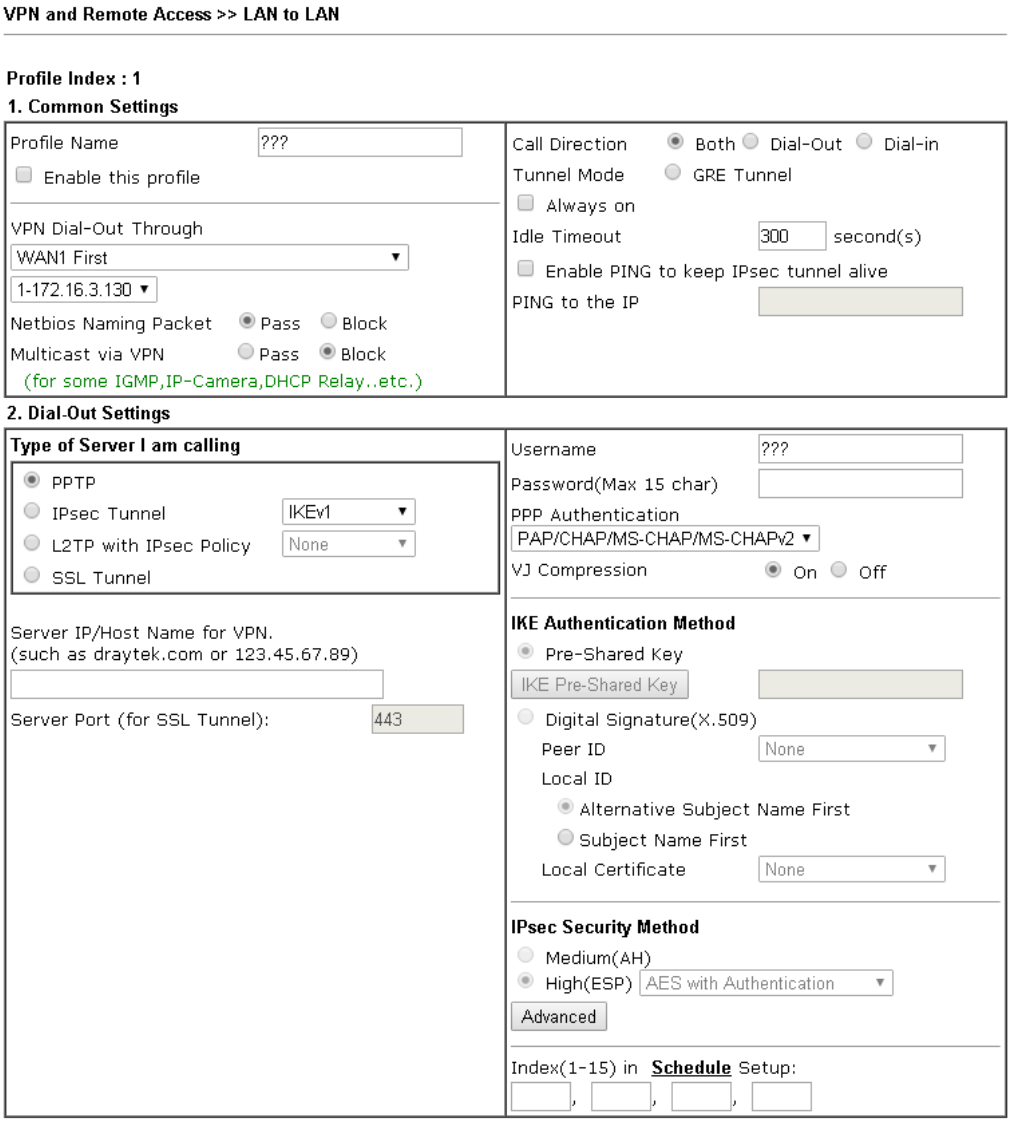
可用設定說明如下：

項目	說明

檢視(View)	**全部(All) –** 按此顯示全部 LAN to LAN 設定檔。 **上線(Online)** – 按此顯示上線 LAN to LAN 設定檔。 **下線(Offline)** – 按此顯示下線 LAN to LAN 設定檔。 **Trunk –** 按此顯示 Trunk 設定檔。
回復出廠預設值(Set to Factory Default)	按此鈕清除全部設定。
索引編號(Name)	請按索引下方的號碼以進入設定頁面。
名稱(Name)	意即 LAN-to-LAN 檔案名稱，**???**符號代表該檔案目前是空的。
啓動(Active)	表示個別檔案的狀態，符號 V 和 X 分別代表使用中與未使用的檔案。
狀態(Status)	Online – 表示此 LAN to LAN 設定檔目前運作中。 Offline – 表示此 LAN to LAN 設定檔目前並未運作，即使已經啓動。

如欲編輯設定檔，請：

1. 請按索引編號連結以編輯個別設定檔，按下後可看到如下的頁面，每個 LAN-to-LAN 檔案包含有四個子群組，如果該區域是灰色的，即表示您無法在該項目做任何設定，下面的說明可以引導您於各個設定區塡入相關資訊。由於網頁太長，我們將之切成數個段落來說明。



可用設定說明如下：

項目	說明
共同設定 (Common Settings)	**設定檔名稱(Profile Name) -** 針對此 LAN-to-LAN 連線，請指定一個設定檔案名稱。 **啓用此設定檔(Enable this profile) -** 按此方塊啓用此設定檔。 **VPN 連線經由介面(VPN 連線經由介面-**使用下拉式選項選擇適合的 WAN 介面，此設定僅適合撥出時使用。**)-**使用下拉式選項選擇適合的 WAN 介面，此設定僅適合撥出時使用。 ● **WAN1 優先/WAN2 優先/WAN3 優先或 LTE 優先/WAN4 優先(WAN1 First/ WAN2 First/ WAN3 First or LTE First/WAN4 First)**- 連線時，路由器會將 WAN1/WAN2/WAN3 或 LTE/WAN4 視爲 VPN 連線的首要選擇，如果 WAN1/WAN2/WAN3 或 LTE/WAN4 連線失敗，路由器將使用其他 WAN 介面來取代。 ● **限用 WAN1/限用 WAN2/限用 WAN3 或限用 LTE/限用 WAN4 (WAN1 Only /WAN2 Only/WAN 3 Only or LTE Only /WAN 4 Only)**- 連線時，路由器會將 WAN1/WAN2/WAN3 或是 LTE /WAN4 視爲 VPN 連線的唯

	一選擇。 ● **限用 WAN1:備援 WAN2 (WAN1 Only: Only establish VPN if WAN2 down)**– 當 WAN2 斷線時，此 VPN 通道會經由 WAN1 連線撥打出去，亦即 WAN1 爲 WAN2 的備援介面。 ● **限用 WAN2:備援 WAN1(WAN2 Only: Only establish VPN if WAN1 down)** -當 WAN1 斷線時，此 VPN 通道會經由 WAN2 連線撥打出去，亦即 WAN2 爲 WAN1 的備援介面。 **Netbios 命名封包(Netbios Naming Packet)** ● **通過(Pass)** – 按此鈕讓資料能在二台主機之間所建立的 VPN 通道上傳輸。 ● **封鎖(Block)** – 當雙方所建立的 VPN 通道連線產生衝突時，此功能可以封鎖此通道。 **經由 VPN 執行多重播送(Multicast via VPN) -**某些程式可透過 VPN 連線進行多重播送封包。 ● **通過(Pass)** –點選此鈕讓多重播送封包通過路由器。 ● **封鎖(Block)** – 此爲預設值。點選此鈕之後，路由器將會封鎖多重播送封包。 **撥號方向(Call Direction) -**針對此 LAN-to-LAN 連線，請指定允許的撥號方向。 ● **雙向(Both)** – 發話方/接話方 ● **撥出(Dial-Out)** - 發話方 ● **撥入(Dial-In) -** 接話方 **永遠連線(Always On) -** 勾選此方塊讓路由器永遠保持 VPN 連線。 **閒置逾時(Idle Timeout) -** 預設值爲 300 秒，若連線閒置時間超過此數值，路由器將自動中斷連線。 **啓用 PING 以維持連線(Enable PING to keep alive) -**此功能可協助路由器決定 IPSec VPN 連線狀態，對不正常的 IPSec VPN 通道中斷尤其有用。詳細內容請參考下面的註解，請勾選此方塊啓動 PING 封包傳輸至指定的 IP 位址。 **啓用 PING 以維持連線(Enable PING to keep alive)** 用於管理異常的 IPsec VPN 中斷。它可幫忙讓路由器重撥來判斷 VPN 連線狀態，正常來看如果 VPN 任何一方想中斷 VPN 連線，它必須依循一系列的封包交換過程以便通知對方。然而若是遠端用戶沒有通知便中斷連線，路由器將無由得知實際狀況。爲了解決此難題，藉由持續傳送 PING 封包至遠端主機，路由器可以得知此 VPN 的真實存在，並據而做出回應。 **指定 IP 位址(PING to the IP) -** 輸入 VPN 通道另一端的主機 IP 位址。
撥出設定 **(Dial-Out Settings)**	**我撥出的伺服器類型(Type of Server I am calling) -** **PPTP-**爲伺服器建立一個透過網際網路的 PPTP VPN 連線，您必須設定連線類型和身分辨識像是使用者名稱與密碼等，以便驗證遠端伺服器。 **IPSec 通道(IPSec Tunnel)-**爲伺服器建立一個透過網際網路的 IPSec VPN 連線。 **具有 IPSec 原則的 L2TP(L2TP with IPSec Policy)**-爲伺服器建立一個透過網際網路的 L2TP VPN 連線。您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取： ● **無(None) -** 此選項完全不會應用 IPSec 原則，VPN 連線採

用不帶有 IPSec 原則的 L2TP，可以在完全 L2TP 連線中檢視內容。

- **建議選填(Nice to Have) -**如果在整個連線過程中是可以運用的情形下，此選項會先應用 IPSec 原則。否則撥出 VPN 連線會成爲一種完全的 L2TP 連線。
- **必須(Must) -** 此選項可在 L2TP 連線中明確指定所要運用的 IPSec 原則。

SSL 通道(SSL Tunnel) - 透過網際網路建立 SSL VPN 連線。

使用者名稱(User Name)-當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。

密碼(Password)-當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。

PPP 認證(PPP Authentication)-當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。PAP/CHAP 是最平常的選項。

VJ 壓縮(VJ compression)-當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。VJ 壓縮可作爲 TCP/IP 協定標頭壓縮之用，通常設定選擇**開啓**以改善頻寬利用的狀況。

IKE 驗證方式(IKE Authentication Method) - 這個功能適用 **IPsec 通道**與**具有 IPSec 原則的 L2TP**。

- **Pre-Shared Key** - Input 1-63 characters as pre-shared key. 點選此項啓用此功能並按 **IKE 預先共用金鑰(IKE Pre-Shared Key)**按鈕輸入金鑰及確認金鑰。
- **數位簽章(X.509) -** 點選此項啓用此功能並選擇一組事先定義的簽章內容 (在 **VPN 和遠端存取>>IPSec 端點辨識**中設定)。

  對方 ID(Peer ID) - 自下拉式清單中(設定於 **VPN 與遠端存取>>IPsec 端點辨識**)選擇對方的 ID。

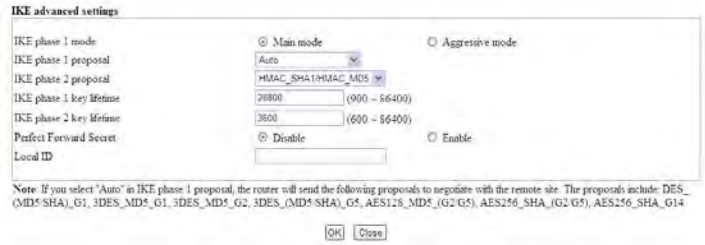
  本機 ID(Local ID) - 指定一個本機 ID(**替代主體名稱優先(Iternative Subject Name First)**或是**主體名稱優先(Subject Name First))**，用於撥入設定，這個項目是選填項目。
- **本機憑證(Local Certificate) -** 自下拉式清單中選擇一種憑證，您必須事先在**憑證管理>>本機憑證(Certificate Management>>Local Certificate)**中設定至少一組的憑證，否則無憑證正可以使用。

IPSec 安全防護方式(IPSec Security Method) -對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區爲必要設定。

- **中級(AH)(Medium AH (Authentication Header))** 表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。
- **高級(ESP-Encapsulating Security Payload)(High (ESP-Encapsulating Security Payload))** 表示資料將被加密及驗證，請自下拉式清單中選取適合項目：
- *DES 無驗證*(**DES without Authentication**) - 使用 DES 加密演算式，但不採用任何驗證計畫。
- *DES 有驗證*(**DES with Authentication**) **-** 使用 DES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。
- *3DES 無驗證*(**3DES without Authentication**) - 使用三重 DES 加密演算式，但不採用任何驗證計畫。

- *3DES 有驗證*(**3DES with Authentication)-**使用三重 DES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。
- *AES 無驗證*(**AES without Authentication**) - 使用 AES 加密演算式，但不採用任何驗證計畫。
- *AES 有驗證*(**AES with Authentication**) **-**使用 AES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。

進階(Advanced)-指定模式、建議和 IKE 階段金鑰有效時間等設定，可按**進階**按鈕進入進階設定，視窗顯示如下：

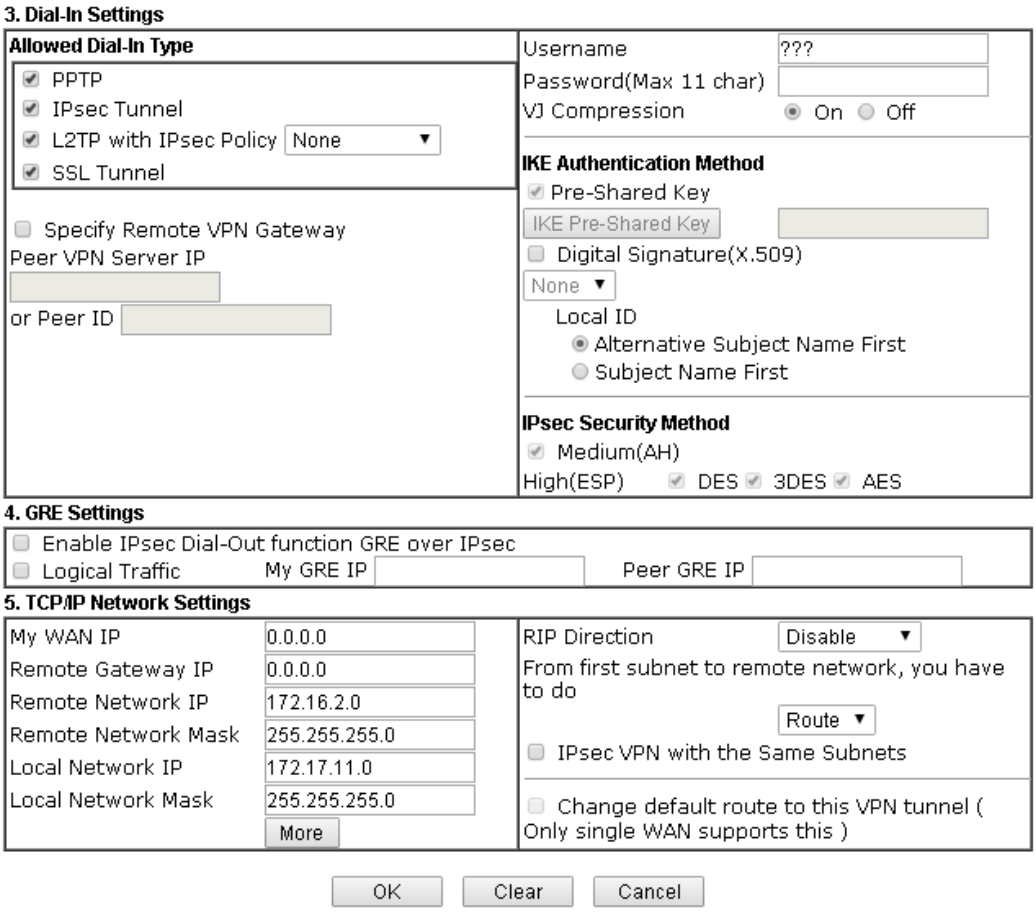


IKE 階段 1 模式(IKE phase 1 mode) - 選擇 **Main 模式**或是 **Aggressive 模式**。比起 **Aggressive 模式**，**Main 模式**顯得更加安全，因爲在安全通道中有更多的交換動作於此完成，不過，**Aggressive 模式**是比較快速的模式。路由器的預設值爲 **Main 模式**。

- **IKE phase 1 proposal-** 針對 VPN 通道另一方可提供本地有效的驗證計畫及加密演算式，並取得回覆訊息以找出符合的結果。對 **Aggressive 模式**來說有二種有效的組合方式，對 **Main 模式**來說有九種有效的組合方式，建議您選擇能涵蓋多數計畫的組合方式。
- **IKE phase 2 proposal-** 針對 VPN 通道另一方可提供本地有效的驗證計畫及加密演算式，並取得回覆訊息以找出符合的結果。**Aggressive 模式**與 **Main 模式**皆有三種有效的組合方式，建議您選擇能涵蓋多數計畫的組合方式。
- **IKE 階段 1 金鑰有效時間(IKE phase 1 key lifetime)-** 考慮到安全之故，使用者必須訂定有效時間，預設值爲 28800 秒，您可以在 900 與 86400 秒之間指定所需的時間值。
- **IKE 階段 2 金鑰有效時間(IKE phase 2 key lifetime)-** 考慮到安全之故，使用者必須訂定有效時間，預設值爲 3600 秒，您可以在 600 與 86400 秒之間指定所需的時間值。
- **Perfect Forward Secret (PFS)-** IKE Phase 1 密鑰可再次使用以便防止 phase 2 產生計算複雜的問題。預設狀況是不啓用此功能。

  本機 ID(Local ID) - 在 **Aggressive 模式**中，當鑑定遠端 VPN 伺服器身分時，本機 ID 代表 IP 位址，ID 長度限制於 47 個字元。

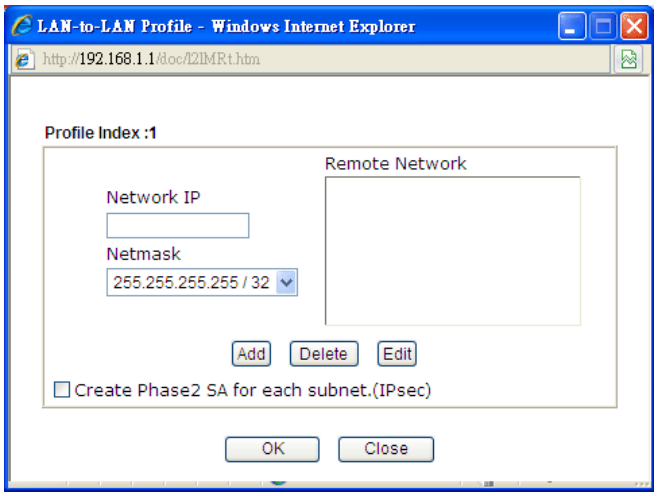
索引號碼(1-15) 於排程設定(Index(1-15)) -可以輸入四組時間排程，全部的排程都是在**其他應用>>排程(Applications >> Schedule)**網頁中事先設定完畢，您可在此輸入該排程的索引編號。



可用設定說明如下：

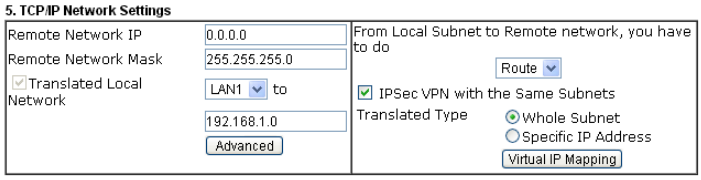
項目	說明
撥入設定 (Dial-In Settings)	**允許的撥入類型(Allowed Dial-In Type)-**以不同類型來決定撥入連線。 ● **PPTP-**允許遠端撥入用戶透過網際網路達成 PPTP VPN 連線，請設定遠端撥入用戶的使用者名稱和密碼。 ● **IPSec 通道(IPSec Tunnel)-**允許遠端撥入用戶透過網際網觸發 IPSec VPN 連線。 ● **具有 IPSec 原則的 L2TP(L2TP with IPSec Policy)-**允許遠端撥入用戶透過網際網路製造 L2TP VPN 連線，您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取： ■ **無(None) -** 此選項完全不會應用 IPSec 原則，VPN 連線採用不帶有 IPSec 原則的 L2TP 可以在完全 L2TP 連線中檢視內容。 ■ **建議選填(Nice to Have)-**如果在整個連線過程中是可以運用的情形下，此選項會先應用 IPSec 原則。否則撥出 VPN 連線會成爲一種完全的 L2TP 連線。 ■ **必須(Must) -** 此選項可在 L2TP 連線中明確指定所要運用的 IPSec 原則。 ● **SSL 通道(SSL Tunnel) -** 讓遠端撥入使用者透過網際網路觸發 SSL VPN 連線。 **指定遠端 VPN 閘道(Specify Remote VPN Gateway) -**您可勾

	選此項，並指定遠端撥入用戶的真實 IP 位址或 ID (必須與撥入類型中所設定的 ID 相同)。此外針對 VPN 功能，您應該進一步指定右邊相關安全設定。 如果您不勾選此方框，您上述選定的連線類型將會套用基本設定中所選用的驗證方式及安全性方法。 **使用者名稱(User Name)-**當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。 **密碼(Password)-**當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。 **VJ 壓縮(VJ Compression)-**當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。VJ 壓縮可作爲 TCP/IP 協定標頭壓縮之用。 **IKE 驗證方式(IKE Authentication Method) -**當您指定遠端節點的 IP 位址時，IKE 驗證可套用在 IPSec 通道和含 IPSec 原則之 L2TP 上。不過，不管有沒有指定遠端節點的 IP 位址予 IPSec 通道使用，您仍然可以設定數位簽章(X.509)。 ● **預先共用金鑰(Pre-Shared Key)-** 勾選此方塊啓用此功能並按 **IKE 預先共用金鑰**按鈕輸入金鑰及確認金鑰。 ● **數位簽章 (X.509) (Digital Signature (X.509))-**勾選此方塊啓用此功能並自下拉式清單中選擇 **VPN 遠端存取控制>>IPSec 端點辨識(VPN and Remote Access >>IPSec Peer Identity)**中所預先定義的設定檔。 ■ **本機 ID(Local ID)**–指定先檢測下方哪一種類型。 ■ **替代主體名稱優先(Alternative Subject Name First)** – 先檢測替代主體名稱(於**憑證管理>>本機憑證**中定義)。 ■ **主體名稱優先(Subject Name First)** – 先檢測主體名稱(於**憑證管理>>本機憑證**中定義)。 **IPSec 安全防護方式(IPSec Security Method)**-當您指定遠端模式時，對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區爲必要設定。 ● **中級(AH)(Medium)** 表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。 ● **高級(ESP-Encapsulating Security Payload)(High)-** 表示資料將被加密及驗證，請自下拉式清單中選取適合項目。
GRE over IPsec 設定 (GRE over IPsec Settings)	**啓用 IPsec 撥出功能 GRE over IPSec(Enable IPsec Dial-Out function GRE over IPsec)** - 設定完畢 IPsec 撥出設定之後，勾選此框驗證資料並透過 GRE over IPSec 封包加密技術傳輸資料。雙邊的虛擬 IP 位址必須符合才能溝通。 **合理流量(Logical Traffic)** - 此項技術得自 RFC2890，透過 GRE 的特性定義 VPN 通道雙邊的資料傳輸的合理流量，即使駭客可以解開 IPSec 加密內容，也無法要求區域網路站點進行資料傳輸。此功能可確保資料在 VPN 通道中傳輸時，能真正傳達至彼此雙方。這個功能是選填內容，可以設定也可以省略，不過如果有一方想要使用，另一方也必須啓用此功能才能運作。 **我的 GRE IP(My GRE IP)** - 輸入路由器本身的虛擬 IP 位址以便讓對方驗證。 **對方 GRE IP(Peer GRE IP)** – 輸入對方主機的虛擬 IP 位址以便

	讓路由器驗證。
TCP/IP 網路設定 **(TCP/IP Network Settings)**	**我的 WAN IP (My WAN IP)-**本區只在您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時有效。預設值爲 0.0.0.0，表示 Vigor 路由器在 IPCP 協商階段期間，將從遠端路由器取得您所指定的 IP 位址。如果 PPP IP 位址由遠端鎖定，那麼請在此輸入該鎖定的 IP 位址。不過若您並未選擇 PPTP 或是 L2TP，請維持預設 IP 值。 **遠端閘道 IP(Remote Gateway IP) -** 本區只在您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時有效。預設值爲 0.0.0.0，表示 Vigor 路由器在 IPCP 協商階段期間，將發予對方的 IP 位址，請在此輸入發予對方之 IP 位址。如果 PPP IP 位址由遠端鎖定，那麼請在此輸入該鎖定的 IP 位址。不過若您並未選擇 PPTP 或是 L2TP，請維持預設 IP 值。 **遠端網路 IP/遠端網路遮罩(Remote Network IP/ Remote Network Mask) -** 新增一個靜態路由以便透過網際網路，引導遠端網路 IP 位址/遠端網路遮罩預定之全部傳輸流量。對 IPSec 而言，這項設定是第二階段快速模式的目的用戶端之身分。 **本機網路 IP 位址/ 本機網路遮罩(Local Network IP / Local Network Mask) -** 顯示 TCP / IP 設定中的本機網路 IP 位址與遮罩，如有必要，您可以修改設定。 **更多(More)-**新增一個靜態路由，並藉由網際網路引導更多的遠端網路 IP 位址/遠端網路遮罩預定之全部傳輸流量。通常在您發現遠端 VPN 路由器有數個子網路存在時，您會使用此按鈕設定更多的路由。  **RIP 方向(RIP Direction)-**此選項指定 RIP (路由資訊協定) 封包的方向，您可以啓用也可以停用 RIP 方向，於此，我們提供您四種選擇：TX/RX 二者均有、TX、RX 以及停用。 **從第一個子網路到遠端網路，您必須要作(From first subnet to remote network, you have to do) -**如果遠端網路只允許您以單一 IP 撥號，請選擇 **NAT** 否則請選擇**路由**。 **變更預設路由此 VPN 通道(Change default route to this VPN tunnel) -**勾選此方塊變更此 VPN 通道的預設路由。
具備相同子網的 IPsec VPN (IPSec VPN with the Same subnet)	由於雙方(例如同一公司不同部門)皆在相同的子網內，這個功能可讓您在雙邊建立虛擬 IP 對應。如此一來，當 VPN 連線建立完畢，路由器將會依照此處設定改變 IP 位址，並封鎖非由此處定

義的 IP 位址傳送過來的連線數。

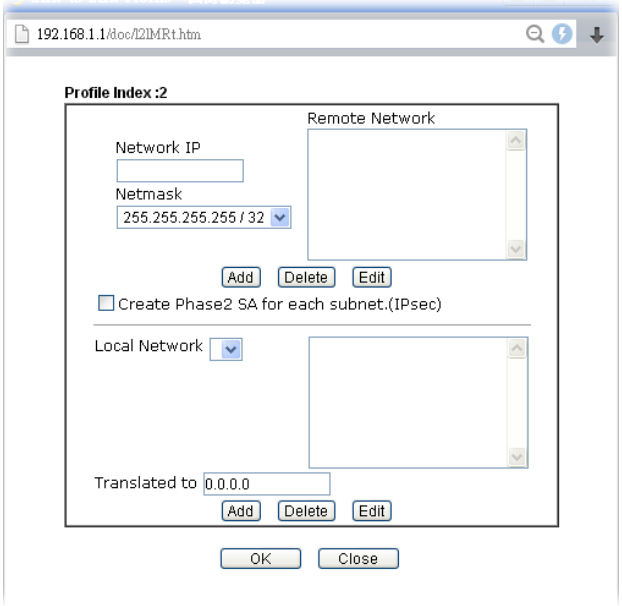
勾選**具備相同子網的 IPsec VPN (IPSec VPN with the Same subnet)**核取方框後，位於 **TCP/IP 網路設定(TCP/IP Network Settings)**下方的項目也會跟著變動，參考下圖：



遠端網路 IP/遠端網路遮罩(Remote Network IP/ Remote Network Mask) - 新增固定路由透過 VPN 連線導引所有的流量至此處所設定的遠端網路 IP 位址/遠端網路遮罩。對 IPsec 來說，這是階段 2 快速模式下的目標客戶。

轉譯本機網路(Translated Local Network) -此功能預設是開啓的，請使用下拉式選單中指定一個 LAN 埠口作爲轉發方向，然後指定一個 IP 位址，若有需要請按下**進階(Advanced)**按鈕設定細節內容。

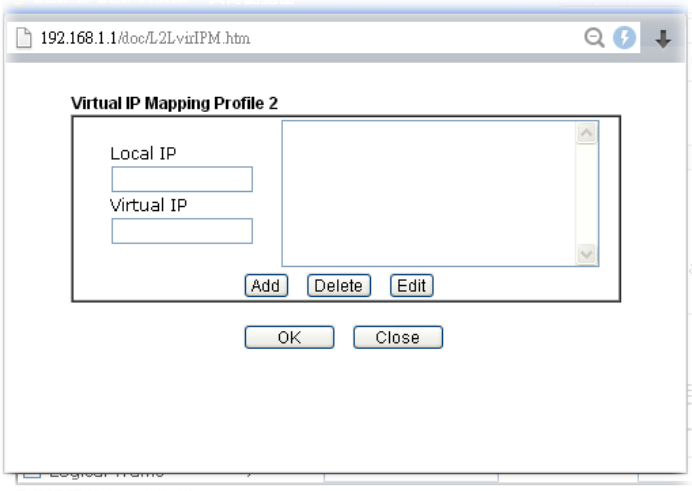
進階(Advanced) - 新增固定路由透過 VPN 連線導引所有流量至更多的遠端網路 IP 位址/遠端網路遮罩，通常在您發現遠端 VPN 路由器擁有數個子網時，可透過進階功能進行細部設定。



轉譯類型(Translated Type) - 共有 2 種可以選擇

- **全部子網(Whole Subnet)**
- **指定 IP 位址(Specific IP Address)**

虛擬 IP 對應(Virtual IP Mapping) - 系統跳出視窗讓您指定本機 IP 位址以及對映的虛擬 IP 位址。



2. 完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

V-1-9 VPN TRUNK 管理(VPN Trunk Management)

VPN TRUNK 包含數種功能如 VPN 備援、VPN 負載平衡、GRE over IPSec 以及綁定通道策略等等。

VPN TRUNK 功能 — VPN 備援機制

VPN TRUNK 管理可以是備援機制，可讓您設定數種 VPN 通道做爲備援通道。這項特性可讓網路不至於因爲網路環境受到任何理由的封鎖而中斷連線。

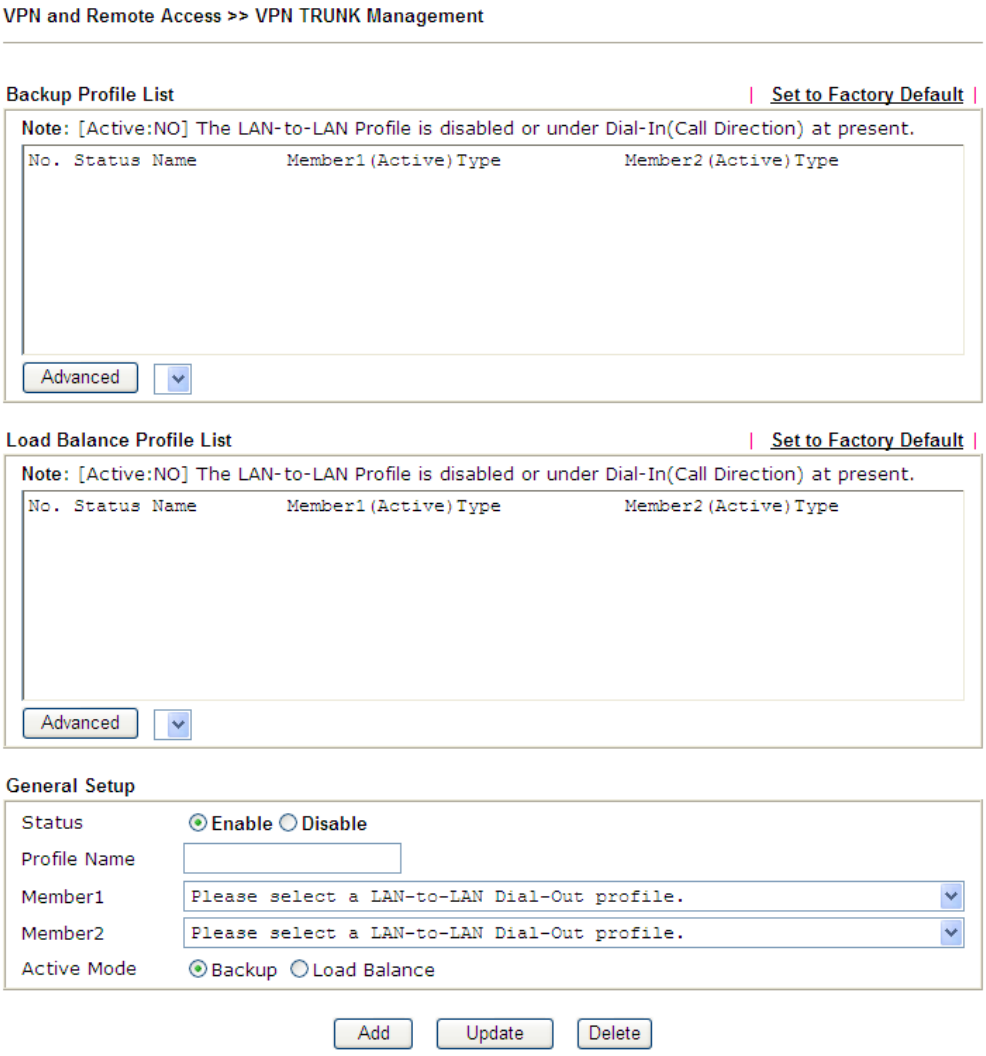
- VPN TRUNK-VPN 備援機制可判斷 VPN 伺服器環境的異常現象並修正以便及時完成 VPN 通道的備援任務
- VPN TRUNK-VPN 備援機制可相容所有 WAN 模式(單一/多重)
- 撥出連線類型包含 IPSec、PPTP、L2TP、L2TP over IPSec(依照硬體規格而定)
- 網頁設定易於了解且容易設定
- 與 VPN 伺服器 LAN 單一站點/多重網路完全相容
- 郵件警示支援部份，請參考**系統維護>> SysLog/郵件警示(System Maintenance >> SysLog / Mail Alert)**
- Syslog 支援部份，請參考**系統維護>>SysLog /郵件警示(System Maintenance >> SysLog / Mail Alert)**
- 特定的 ERD(Environment Recovery Detection 環境回復監測)機制可利用 Telnet 指令來操作

當初始連線的單一 VPN 通道斷線時，VPN TRUNK-VPN 備援機制設定檔立即啓動，在設定 VPN TRUNK -VPN 備援機制設定檔之前，請至少先完成二組 LAN-to-LAN 設定檔 (必須包含完整的撥出設定)，否則您將無任何選項可供成員 1 與會員 2 選擇。

VPN TRUNK 功能 —VPN 負載平衡機制

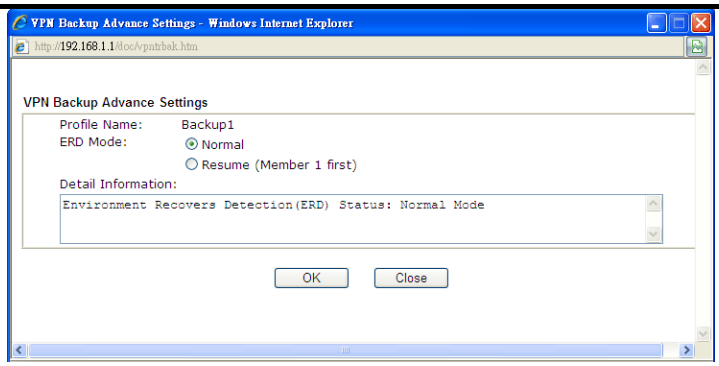
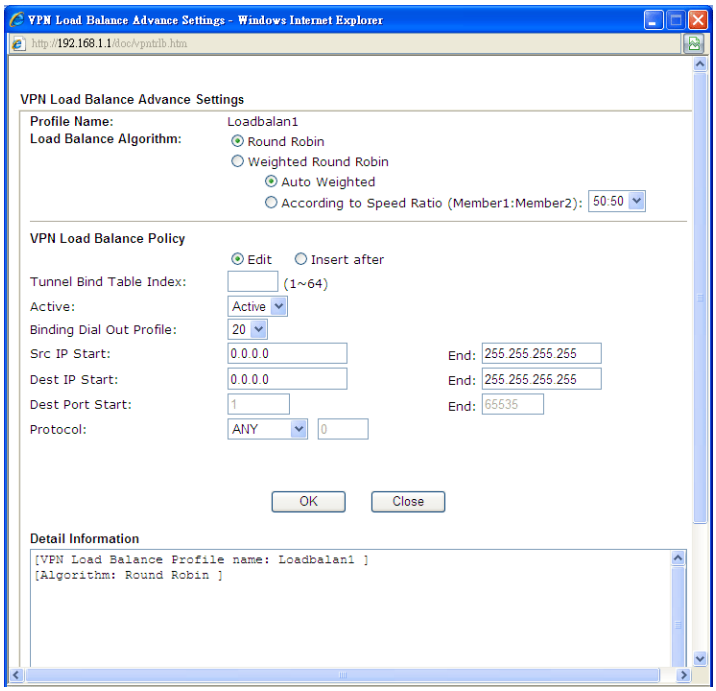
VPN 負載平衡機制可以設定多重 VPN 通道，作爲流量負載平衡通道之用。它可依照實際的頻寬，幫助使用者確保多重 VPN 通道可以進行有效率的負載分享。另外，它還可提供三種不同的演算方式來運作負載平衡以及綁定通道策略機制，讓管理者管理網路更有彈性。

- 提供三種負載分享演算方式包含循環(Round Robin)、權重循環(Weighted Round Robin)以及速率
- 綁定通道策略機制允許使用者於傳輸時加密資料，或是指定服務功能並可定義 VPN 通道以便進行有效的頻寬管理
- 撥出連線類型包含 IPSec、PPTP、L2TP、L2TP over IPSec 以及 GRE over IPSec
- 網頁設定易於了解且容易設定
- 利用 VPN TRUNK-VPN 負載平衡機制運作的 TCP 連線數不會因爲某條 VPN 通道中斷而丟失，使用者不需要重新設定 TCP/UDP 埠號來重新連線，VPN 負載平衡功能可以讓資料在通道當中維持穩定傳輸



可用設定說明如下：

項目	說明
備援設定檔清單(Backup Profile List)	**回復出廠預設值(Set to Factory Default) -** 按下此連結清除全部的備援機制設定檔。 **編號(No) -** 備援機制設定檔的流水編號。 **狀態(Status)** - “v” 表示該設定檔已經啓用；“x”表示該設定檔已被停用。 **名稱(Name) -** 顯示備援機制設定檔的檔名。 **成員 1(Member1) -**顯示自成員 1 下拉式清單中選取出來的撥出設定檔。 **啓用(Active) -** “是” 表示正常，”否” 表示停用或是該 LAN to LAN 設定檔目前的撥號方向爲撥入模式。 **類型(Type) -** 顯示設定檔的連線類型諸如 IPSec、PPTP、L2TP、L2TP over IPSec (NICE)、L2TP over IPSec(MUST) 等等。 **成員 2(Member2) -**顯示自成員 2 下拉式清單中選取出來的撥出設定檔。 **進階(Advanced)** – 此按鈕僅在清單中已建立備援設定檔時始有作用。

	 此對話盒的詳細資訊，請參考稍後的章節。
負載平衡設定檔清單(Load Balance Profile List)	**回復出廠預設值(Set to Factory Default) -** 按下此連結清除全部的負載平衡機制設定檔。 **編號(No) -**負載平衡機制設定檔的流水編號。 **狀態(Status)** - “v” 表示該設定檔已經啓用；“x”表示該設定檔已被停用。 **名稱(Name) -** 顯示負載平衡機制設定檔的檔名。 **成員 1(Member1) -**顯示自成員 1 下拉式清單中選取出來的撥出設定檔。 **啓用(Active) -** “是” 表示正常，”否” 表示停用或是該 LAN to LAN 設定檔目前的撥號方向爲撥入模式。 **類型(Type) -** 顯示設定檔的連線類型諸如 IPSec、PPTP、L2TP、L2TP over IPSec (NICE)、L2TP over IPSec(MUST) 等等。 **成員 2(Member2) -**顯示自成員 2 下拉式清單中選取出來的撥出設定檔。 **進階(Advanced)** – 此按鈕僅在清單中已建立負載平衡設定檔時始有作用。 此對話盒的詳細資訊，請參考稍後的章節。 
基本設定(General Setup)	**狀態(Status)** – 選擇**啓用**啓動上述完成的設定檔，如果您按下**停用**，選定的或是目前使用的 VPN TRUNK 備援/負載平衡機制設

	定檔就不會產生任何作用。 **設定檔名稱(Profile Name)-** 輸入 VPN TRUNK 設定檔名稱，每個設定檔可以群組二個 LAN-to-LAN 連線設定檔，在成員 1 與成員 2 下拉式清單中可以見到已經設定完畢的 LAN-to-LAN 設定檔。 **成員 1/成員 2 (Member 1/Member2)**– 顯示 LAN-to-LAN 撥出設定檔選項 (於 **VPN 與遠端存取 >> LAN-to-LAN** 中設定)，您可於此二區域選擇放在 VPN TRUNK-VPN 備援/負載平衡機制設定檔中群組下的內容。 ● **號碼(No)** - LAN-to-LAN 撥出設定檔的索引編號。 ● **名稱(Name)** - LAN-to-LAN 撥出設定檔的檔名。 ● **連線類型(Connection Type)** - LAN-to-LAN 撥出設定檔的連線類型。 ● **VPN 伺服器 IP (虛擬網路)(VPN ServerIP (Private Network))** - AN-to-LAN 撥出設定檔的 VPN 伺服器 IP。 **運作模式(Active Mode)** - 顯示可用的運作模式（備援或是負載平衡）供您選擇。 **新增(Add) -** 新增並儲存新的設定檔至備援設定檔清單或是負載平衡設定檔清單，在新的 VPN TRUNK – VPN 備援機制中的成員就此被鎖定，而在 LAN-to-LAN 中將以紅色字體來顯示；VPN TRUNK – VPN 負載平衡機制中的成員也會被鎖定，且在 LAN-to-LAN 中以藍色字體顯示。 **更新(Update)-** 按下此鈕儲存狀態（啓用或停用）、設定檔名稱、成員 1 或是成員 2 的變更。 **刪除(Delete) -** 按下此鈕刪除選定的 VPN TRUNK 設定檔，群組內相關的成員(LAN-to-LAN 設定檔)都將釋放，在 LAN-to-LAN 設定頁面中改成以黑色字體呈現。

啓動 VPN TRUNK – VPN 備援機制設定檔的時機

VPN TRUNK – VPN 備援機制在單一 VPN 通道初始連線因故中斷之後會自動啓動，在 VPN TRUNK – VPN 備援機制設定檔內成員 1/2 的內容與 LAN-to-LAN 頁面中撥出設定檔是相同的；一旦啓動，除非是斷線，VPN TRUNK – VPN 備援機制的備援設定檔會處理所有大小事情。

啓動 VPN TRUNK – VPN 負載平衡機制設定檔的時機

在完成一條通道連線之後，另一條通道將會在二秒內自動撥出，因此，您可以在 VPN 負載平衡設定檔中選擇任何一個成員。

當 VPN 負載平衡中斷連線時啓動 VPN TRUNK -撥出的時機

由於只有一條通道建立並成功連線，爲了維持二條通道之間負載平衡效果，二秒內系統就會自動撥出。

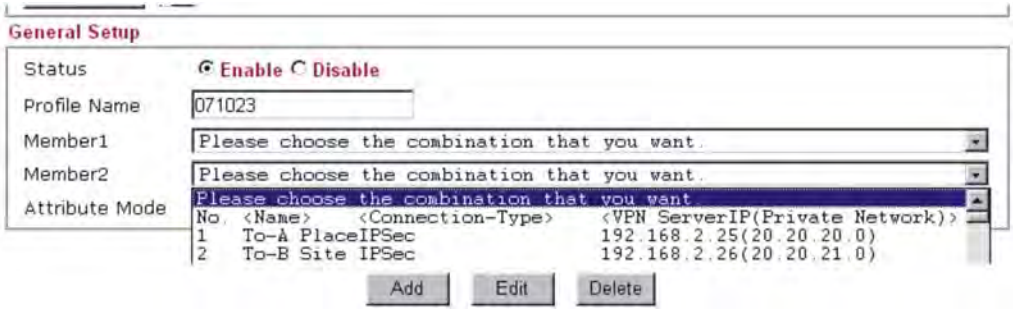
在負載平衡連線後如要關閉二條通道，請於**基本設定(General Setup)**區域的**狀態(Status)**項目選擇**停用(Disable)**。

如何設定 VPN TRUNK-VPN 備援/負載平衡機制設定檔?

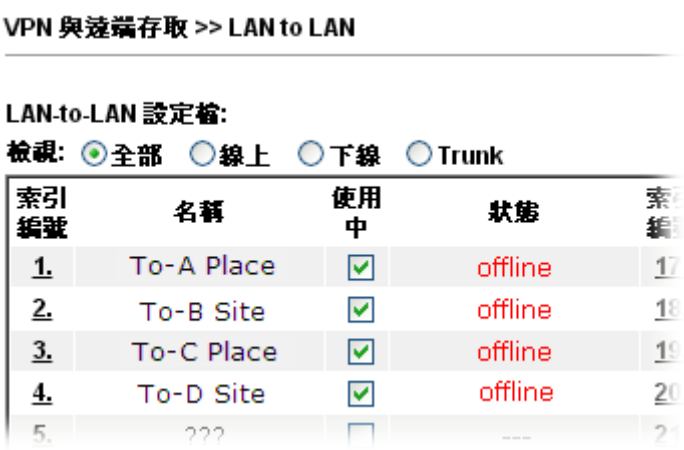
1. 首先，前往 **VPN 與遠端存取>> LAN-to-LAN(VPN and Remote Access>>LAN-to-LAN)**，先設定準備成員 1 與成員 2 可以選擇的 LAN-to-LAN 設定檔（二個或是多個），如果您沒有設定足夠的 LAN-to-LAN 設定檔，您就無法操作 VPN TRUNK – VPN 備援/負載平衡機制。

2. 登入 **VPN 與遠端存取>>VPN TRUNK 管理(VPN and Remote Access>>VPN TRUNK Management)**。

3. 按下**啓用(Enable)**按鈕來設定一組 VPN TRUNK – VPN 備援/負載平衡設定檔；輸入設定檔名稱（例如 071023)；自成員 1 清單中選擇一組 LAN-to-LAN 設定檔；自成員 2 清單中也選擇一組 LAN-to-LAN 設定檔，最後按下**新增(Add)**。



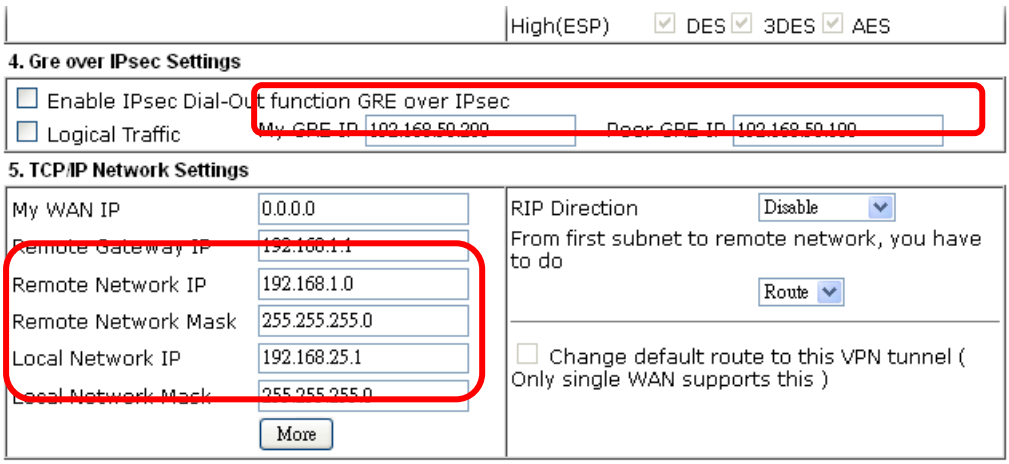
4. 先看看 LAN-to-LAN 設定檔，索引編號 1 選擇爲成員 1；索引編號 2 選擇爲成員 2，因此 LAN-to-LAN 設定檔 1 與 2 都會以紅色表示該檔案已被鎖定。如果您刪除 VPN TRUNK – VPN 備援/負載平衡機制設定檔，選定的 LAN-to-LAN 設定檔就會被釋放出來，並以黑字呈現。



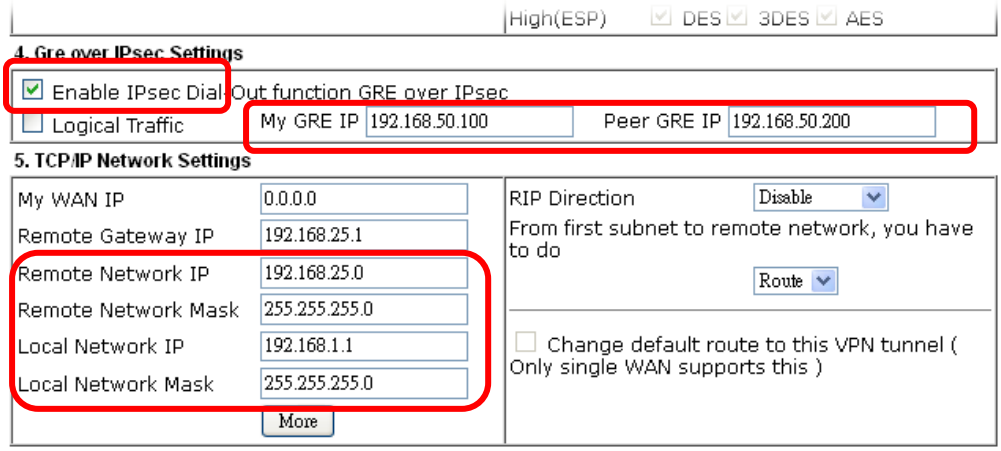
如何設定 GRE over IPSec 設定檔?

1. 先至 LAN to LAN 頁面設定 IPsec 設定檔。

2. 如果路由器將被視爲 VPN 伺服器(虛擬位址爲 192.168.50.200)，請在我的 GRE IP 欄位輸入 192.168.50.200，在對方 GRE IP 欄位輸入用戶端位址 192.168.50.100，參考下圖：



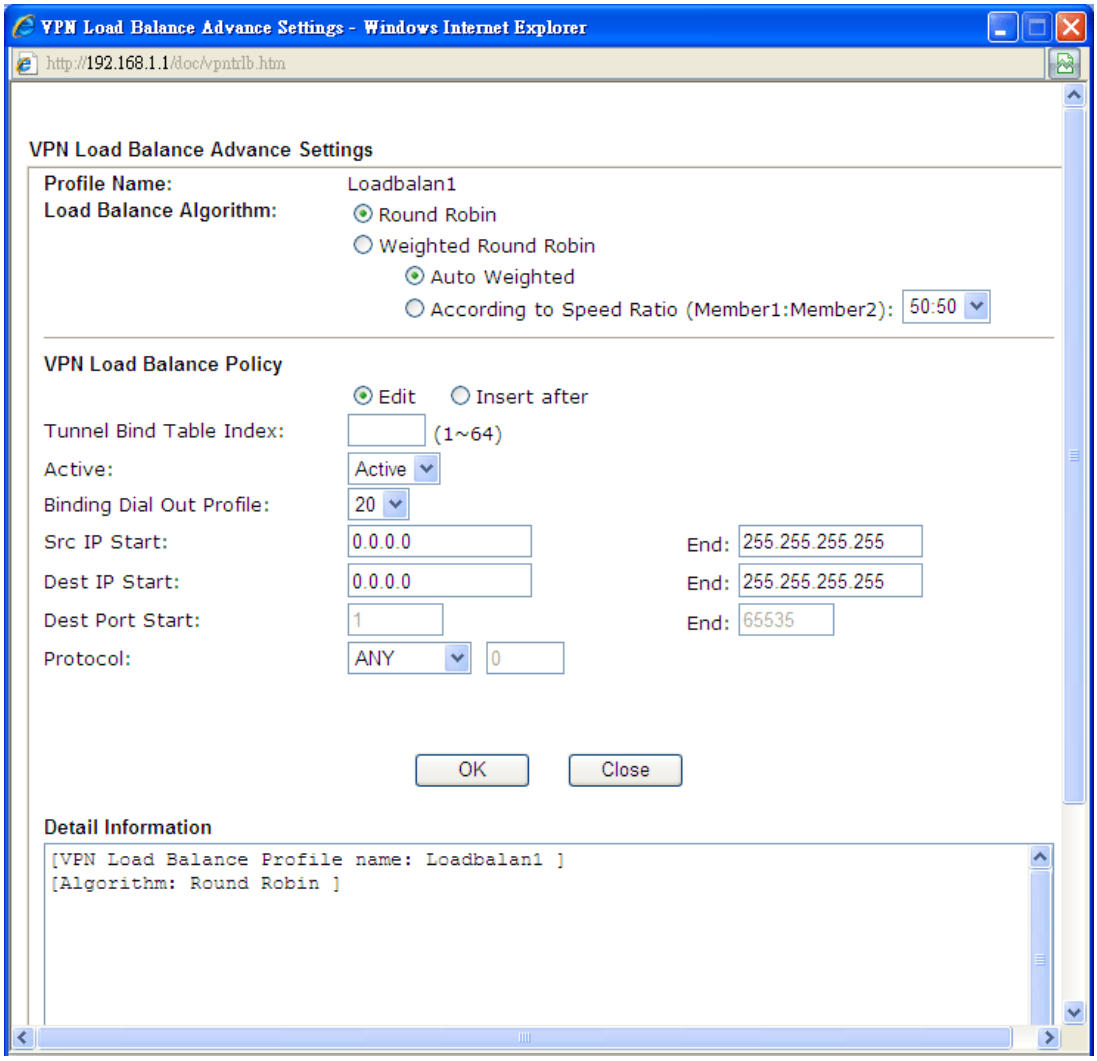
3. 稍後，在對方電腦上(作爲 VPN 用戶端)，在我的 GRE IP 欄位中輸入 192.168.50.100，在對方 GRE IP 欄位中則輸入 192.168.50.200。



負載平衡與備援的進階頁面(Advanced Load Balance and Backup)

負載平衡設定完畢之後，您可以選擇其中一組設定檔，接著按下**進階**進行更細部的設定。**負載平衡(Load Balance)**與**備援(Backup)**之**進階**設定視窗有所不同，請參考下述說明。

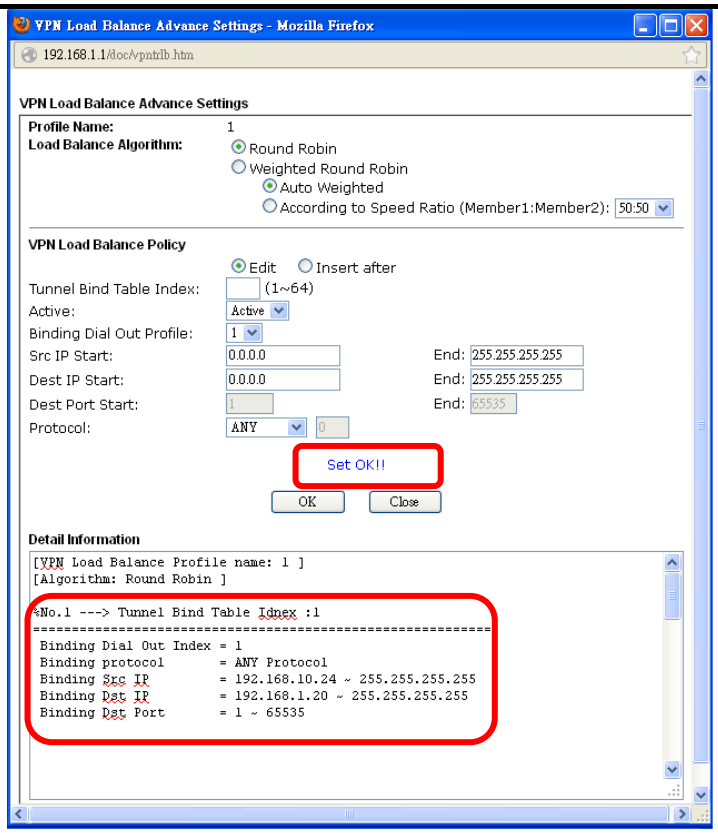
進階負載平衡(Advanced Load Balance)



可用設定說明如下：

項目	說明
設定檔名稱(Profile Name)	顯示設定檔的檔名。
VPN 負載平衡原則(Load Balance Algorithm)	**循環(Round Robin)** – 依照封包的大小而定，二條通道將交替遞送封包，此法可以固定的速率達成平衡傳輸封包。 **權重循環(Weighted Round Robin)** – 此法可以利用彈性速率達成平衡傳輸封包，可分爲**自動權重(Auto Weighted)**與**依照速率(According to Speed Ratio)**。**自動權重**可以固定的比值(3:7)偵測裝置速度(10Mbps/100Mbps)及交換器來進行封包傳輸，如果通道雙邊的速度是相同的，自動權重比值就應該是 5.5。**依照速率**讓使用者調整適當的速度，成員 1:成員 2 適用的比率有 100 組(範圍從 1:99 到 99:1)。
VPN 負載平衡原則(VPN Load Balance Policy)	**編輯(Edit)** – 按下此鈕即可設定綁定通道。 **於此後插入(Insert after)** – 按下此鈕即可新增一條綁定通道表格。 **通道綁定表格編號(Tunnel Bind Table Index)** - 此裝置提供 128 個綁定通道表格，請予負載平衡設定檔指定通道號碼。 **啓動(Active)** – 啓動/清除可刪除此綁定通道表格，啓動則是用

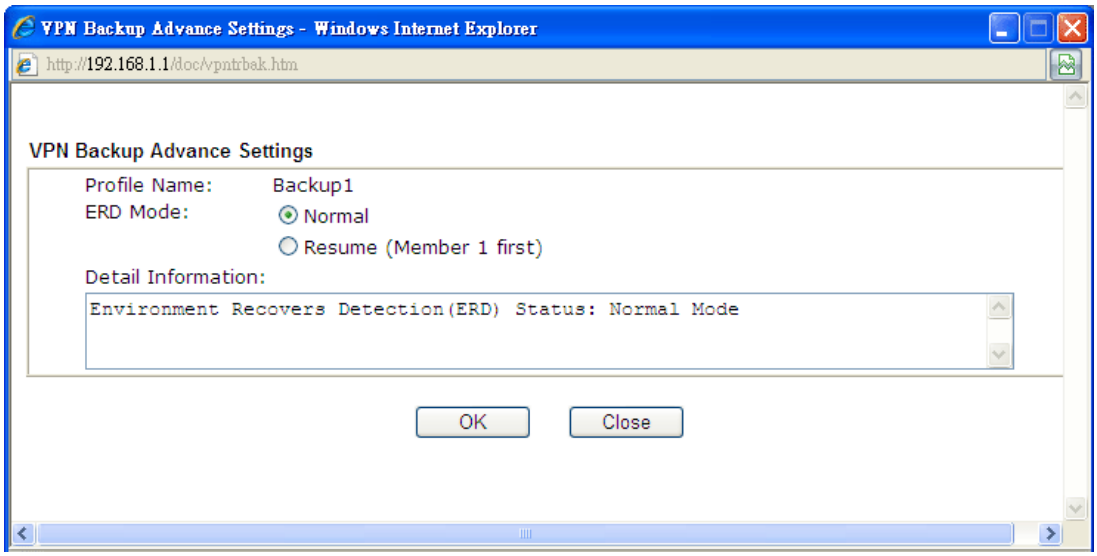
	來啓用此通道表格。 **綁定撥出設定檔(Binding Dial Out Index)** – 選擇 LAN to LAN 設定檔索引編號來指定傳輸連線類型。 **來源 IP 起點/結束(Scr IP Start /End)**– 指定來源 IP 起點與終點。 **目標 IP 起點/結束(Dest IP Start/End)**– 指定目標 IP 起點與終點。 **目標通訊埠起點/結束(Dest Port Start /End)**–指定目標通訊服務埠號起點與終點。 **協定(Protocol)** – **任何(Any)**表示當來源 IP、目標 IP、目標通訊埠以及訊框條件符合此處指定的設定時，可依照此處的 TCP Service Port/UDP Service Port/ICMP/IGMP 設定建立綁定通道表格。 **TCP** 表示當來源 IP、目標 IP、目標通訊埠以及訊框條件符合此處的設定時，且 TCP 服務埠號也符合此處設定，系統將會建立綁定通道表格。 **UDP** 表示當來源 IP、目標 IP、目標通訊埠以及訊框條件符合此處的設定時，且 UDP 服務埠號也符合此處設定，系統將會建立綁定通道表格。**TCP/UPD** 表示當來源 IP、目標 IP、目標通訊埠以及訊框條件符合此處的設定時，且 TCP/UPD 服務埠號也符合此處設定，系統將會建立綁定通道表格。 **ICMP** 表示當來源 IP、目標 IP、目標通訊埠以及訊框條件符合此處的設定時，且 **ICMP** 服務埠號也符合此處設定，系統將會建立綁定通道表格。**IGMP** 表示當來源 IP、目標 IP、目標通訊埠以及訊框條件符合此處的設定時，且 **IGMP** 服務埠號也符合此處設定，系統將會建立綁定通道表格。 **其他**表示當來源 IP、目標 IP、目標通訊埠以及訊框條件符合此處的設定，但卻具有不同的 TCP Service Port/UDP Service Port/ICMP/IGMP 埠號，系統將依此建立綁定通道表格。
細節資訊(Detail Information)	本區將顯示綁定通道策略之細節資訊，下圖顯示的是成功的負載平衡綁定通道策略。



欲成功設定綁定通道，您必須:

輸入綁定來源 IP 範圍(起始與結束)以及綁定目標 IP 範圍(起始與結束)，選擇 TCP/UDP, IGMP/ICMP 或是其他作爲綁定協定。

進階備援(Advanced Backup)



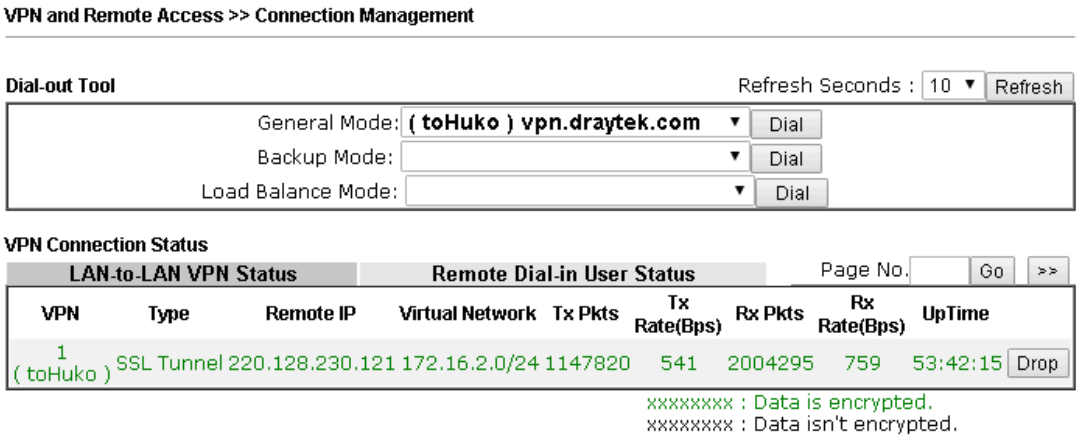
可用設定說明如下：

項目	說明
設定檔名稱(Profile Name)	顯示設定檔的檔名。
ERD 模式(ERD Mode)	ERD 代表環境回復偵測(Environment Recovers Detection)。 **正常(Normal)** – 所有的撥出 VPN TRUNK 備援設定檔會輪流被

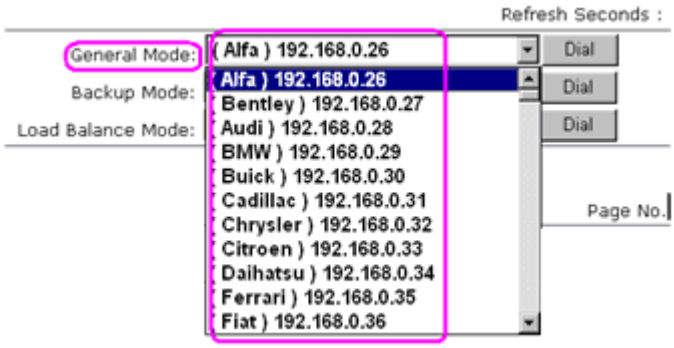
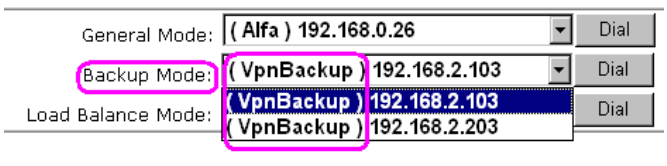
	系統用來重新連線 VPN。 **重新取回(Resume)** – 當 VPN 連線中斷連線時，成員 1 被系統視爲最高優先進行 VPN 重新連線。
細節資訊(Detail Information)	顯示環境回復偵測的細節內容。

V-1-10 連線管理(Connection Management)

您可以查看全部 VPN 連線的總結清單，您可中斷任何一個 VPN 連線，只要輕輕按下**中斷(Drop)**按鈕即可。您也可以使用撥出工具並按**撥號(Dial)**按鈕主動撥出任何的電話。



可用設定說明如下：

項目	說明
撥號工具 (Dial-out Tool)	**基本模式(General Mode)-**本區顯示在 LAN-to-LAN 設定的檔案(含索引編號以及 VPN 伺服器 IP 位址)，基本模式所建立的 VPN 連線不支援 VPN 備援功能。  **備援模式(Backup Mode) -** 本區顯示儲存在VPN TRUNK下的設定檔名(含索引編號以及 VPN 伺服器 IP 位址)，備份模式所建立的 VPN 連線支援 VPN 備援功能。  **撥號(Dial) -** 按此鈕執行撥號功能。 **更新間隔秒數(Refresh Seconds)-**選擇重新顯示狀態的間隔秒

	數，有 5、10、30 秒等三種選擇。 **更新頁面(Refresh)-**按此鈕以重新顯示整個連線狀態。

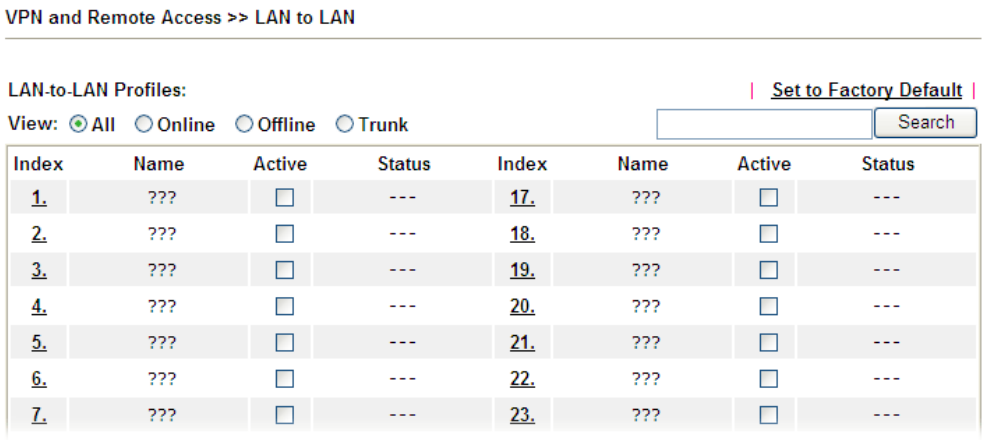
應用說明

A-1 如何在總公司與遠端分公司建立 LAN-to-LAN VPN 連線通道(透過 Main 模式)

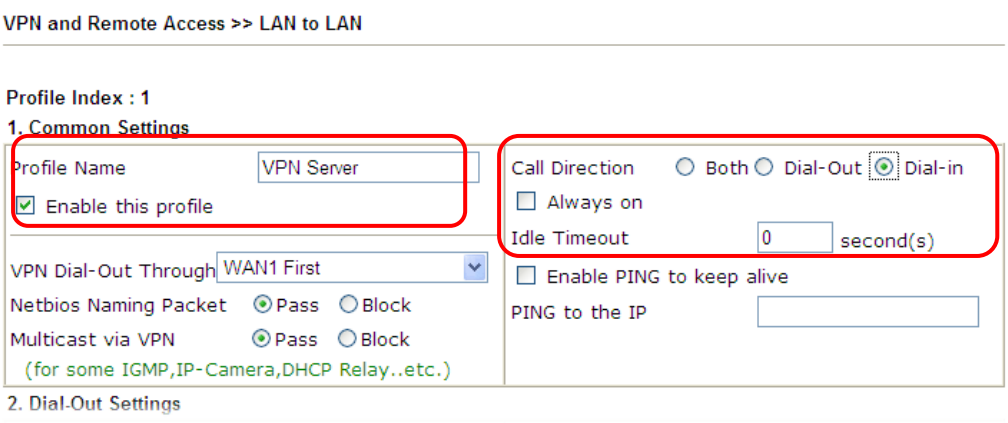


總公司的 Vigor 路由器設定

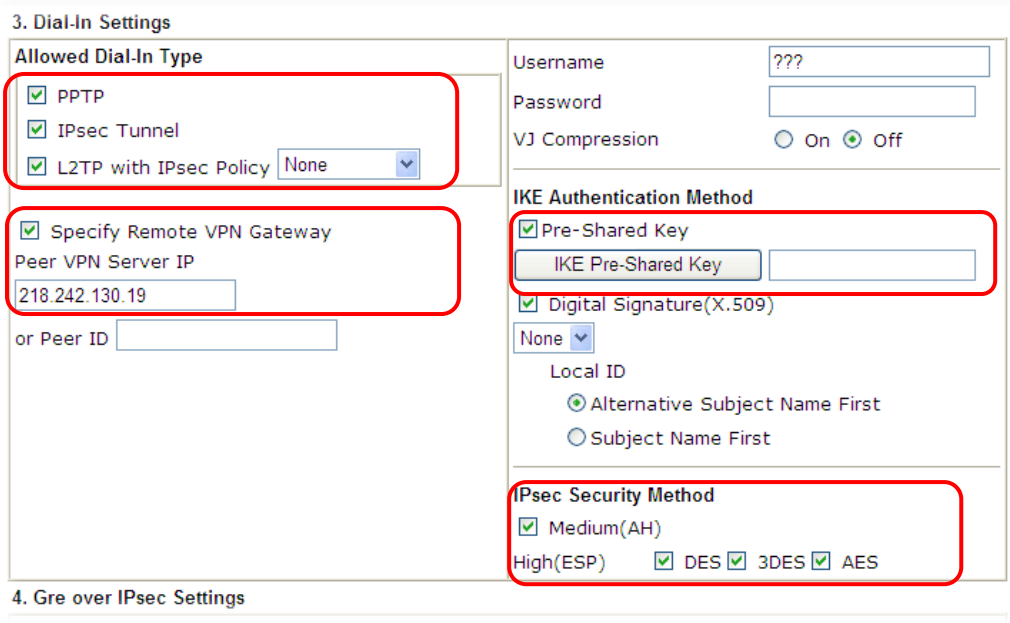
1. 登入路由器的使用者介面。
2. 開啓 **VPN 與遠端存取>>LAN to LAN(VPN and Remote Access>>LAN to LAN)** 建立一個設定檔。



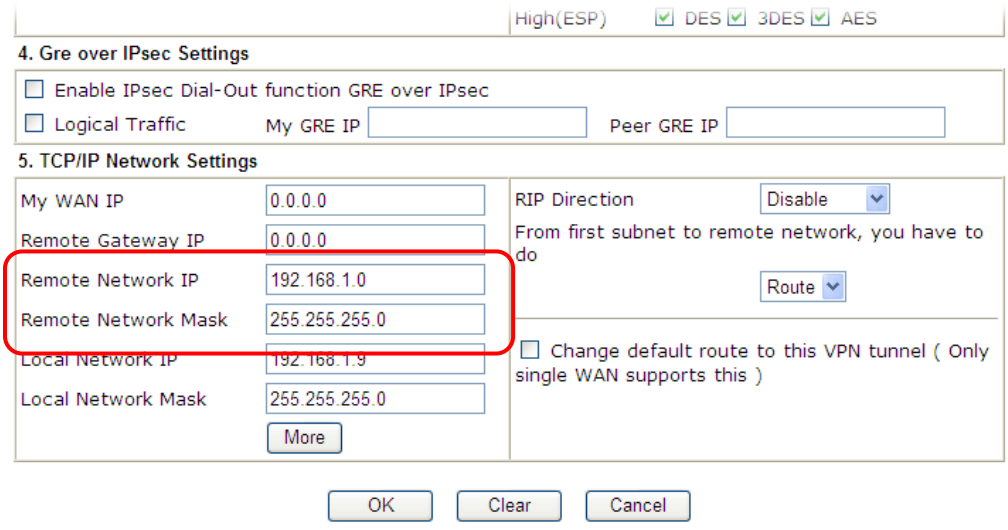
3. 按下任何一個索引編號開啓設定頁面。輸入容易辨識的檔案名稱(本例我們使用 VPN Server)然後勾選**啓用此設定檔(Enable This Profile)**方塊。由於路由器準備被視爲伺服器，因此撥號方向應設定爲**撥入(Dial-in)**且**閒置逾時(Idle Timeou)**設定爲 0。



4. 現在往下瀏覽設定頁面，在**撥入設定(Dial-In Settings)**中，勾選 PPTP、IPsec 通道以及 L2TP，勾選**指定遠端 VPN 閘道(Specify Remote...)**，然後輸入對方 VPN 伺服器 IP 位址(例如本例使用的 218.242.130.19)，按下 **IKE 預先共用金鑰(IKE Pre-Shared Key)**按鈕設定金鑰 PSK 再勾選**中級(AH)**或是**高級(ESP)**安全防護方式。

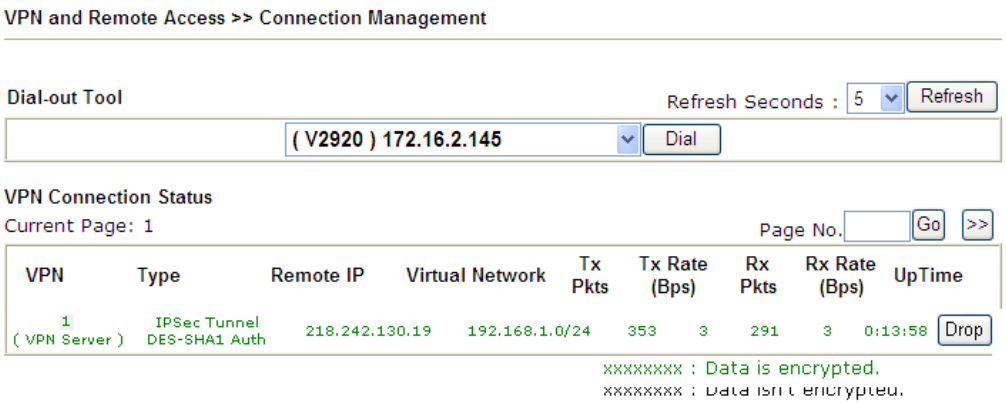


5. 繼續往下瀏覽設定頁面至 TCP/IP 網路設定區域，設定遠端的 LAN IP 位址。



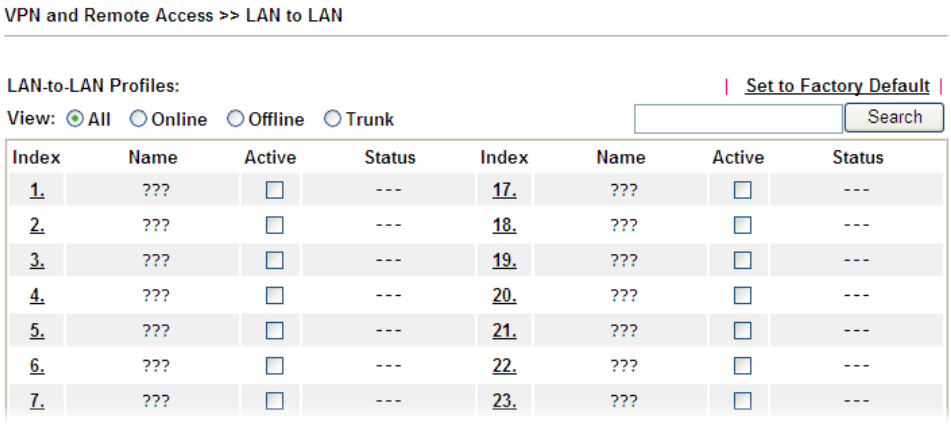
6. 按下**確定(OK)**儲存。

7. 開啓 **VPN 與遠端存取>>連線管理(VPN and Remote Access>>Connection Management)** 檢查撥入連線的狀態(資料來自分公司)。

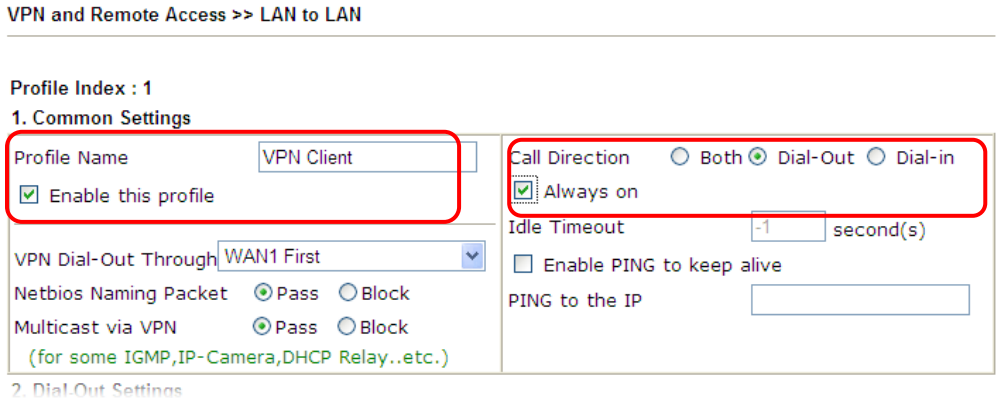


分公司的 Vigor 路由器設定

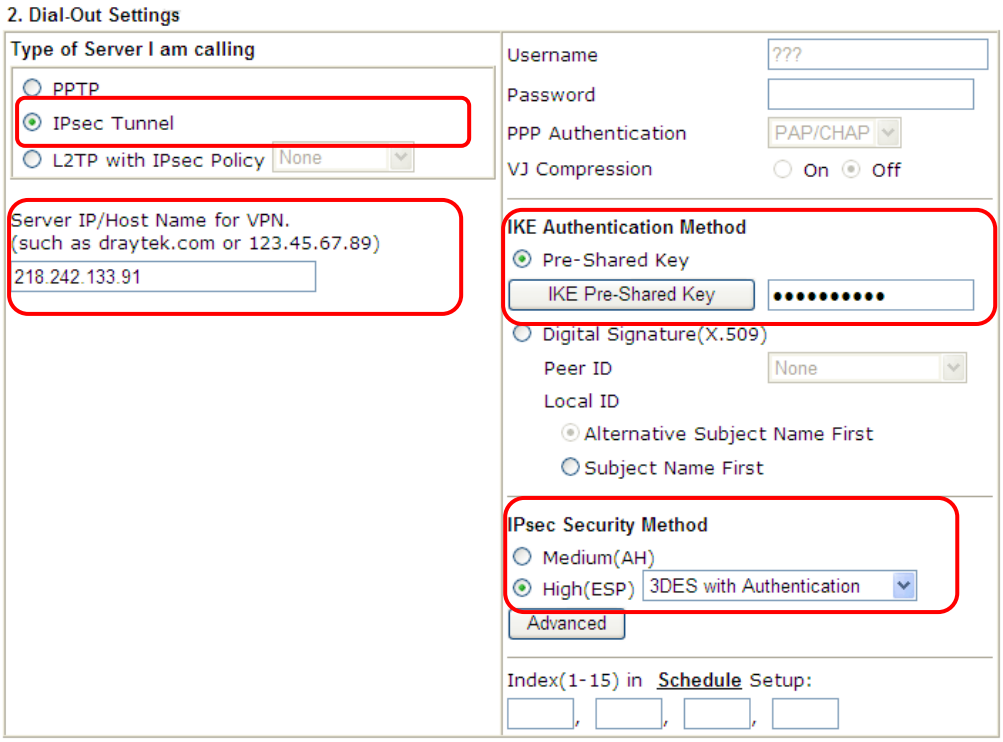
1. 登入路由器的使用者介面。
2. 開啓 **VPN 與遠端存取>>LAN to LAN (VPN and Remote Access>> LAN to LAN)**建立一個設定檔。



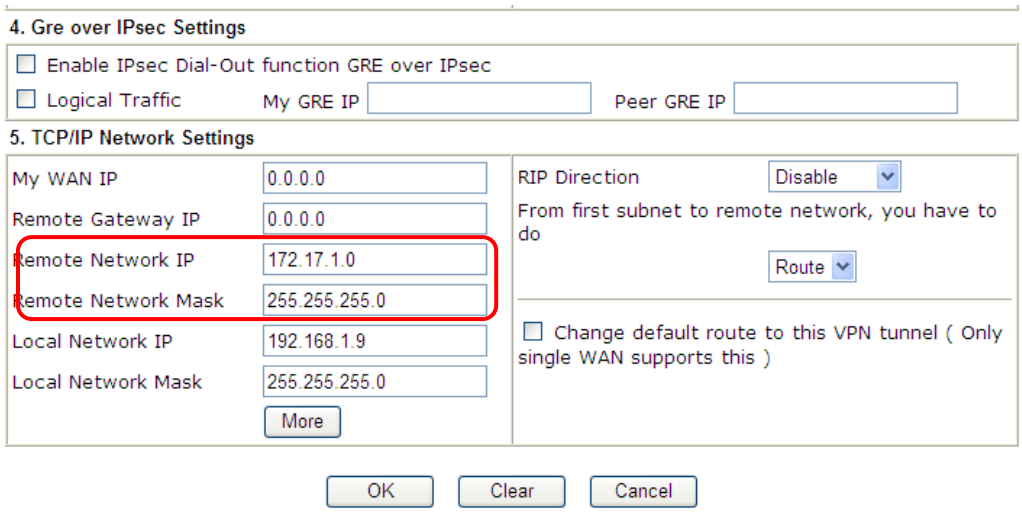
3. 按下任何一個索引編號開啓設定頁面。輸入容易辨識的檔案名稱(本例我們使用 VPN Client)然後勾選**啓用此設定檔(Enable This Profile)**方塊。由於路由器準備被視爲用戶端，因此撥號方向應設定爲**撥出**並勾選**永遠連線(Always on)**。



4. 現在往下瀏覽設定頁面，在**撥出設定(Dial-Out Settings)**中，勾選 **IPsec 通道**，然後輸入遠端伺服器主機名稱/IP 位址(例如本例使用的 218.242.133.91)，按下 **IKE 預先共用金鑰(IKE Pre-Shared Key)**按鈕設定金鑰 PSK 再勾選**中級(AH)**或是**高級(ESP)**安全防護方式。

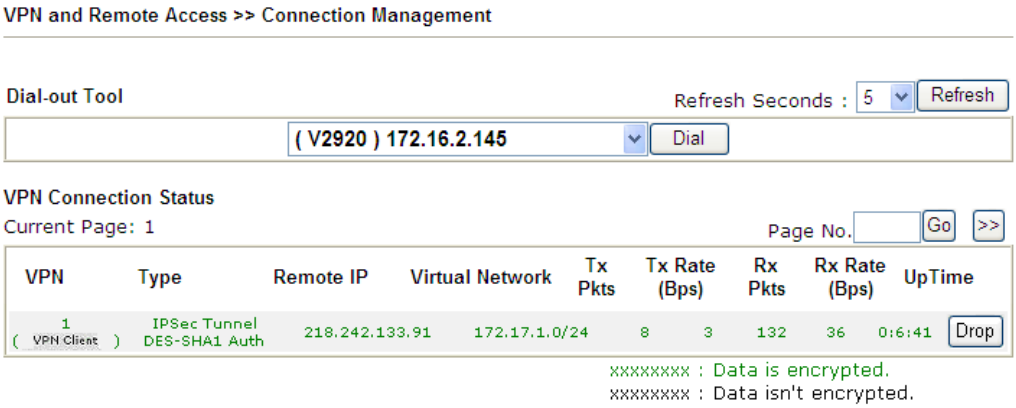


5. 繼續往下瀏覽設定頁面至 TCP/IP 網路設定區域，設定遠端的 LAN IP 位址。



6. 按下**確定(OK)**儲存。

7. 開啓 **VPN 與遠端存取>>連線管理(VPN and Remote Access>>Connection Management)** 檢查撥入連線的狀態(資料來自總公司)。



V-2 SSL VPN

SSL VPN (Secure Sockets Layer virtual private network) 是 VPN 形式的一種，它可與標準的網頁瀏覽器搭配使用。

SSL VPN 提供的好處有二：

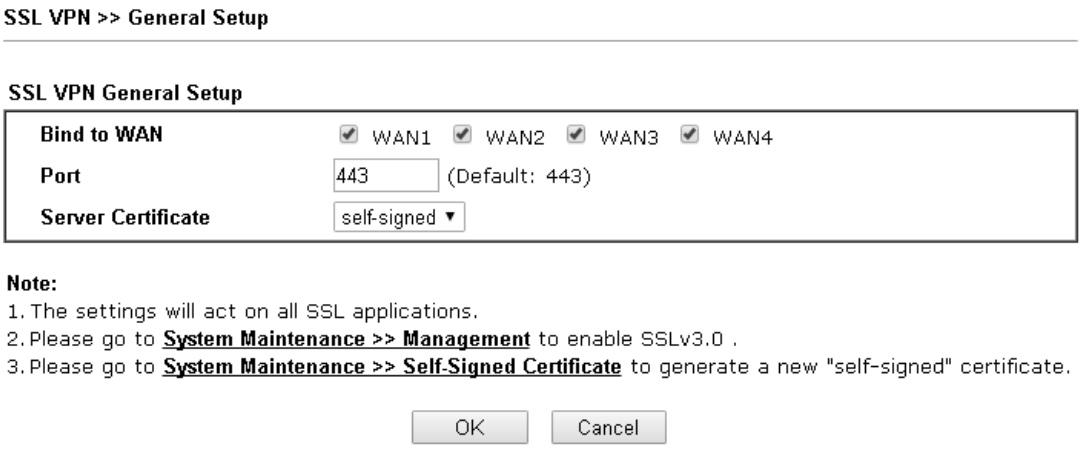
- 使用者不需事先安裝 VPN 用戶端軟體以便進行 SSL VPN 連線
- 比起傳統 VPN，透過 SSL VPN 的資料加密限制較少

網頁使用者介面



V-2-1 基本設定(General Setup)

本頁決定 SSL VPN 以及 SSL Tunnel 的基本設定內容。



可用設定說明如下：

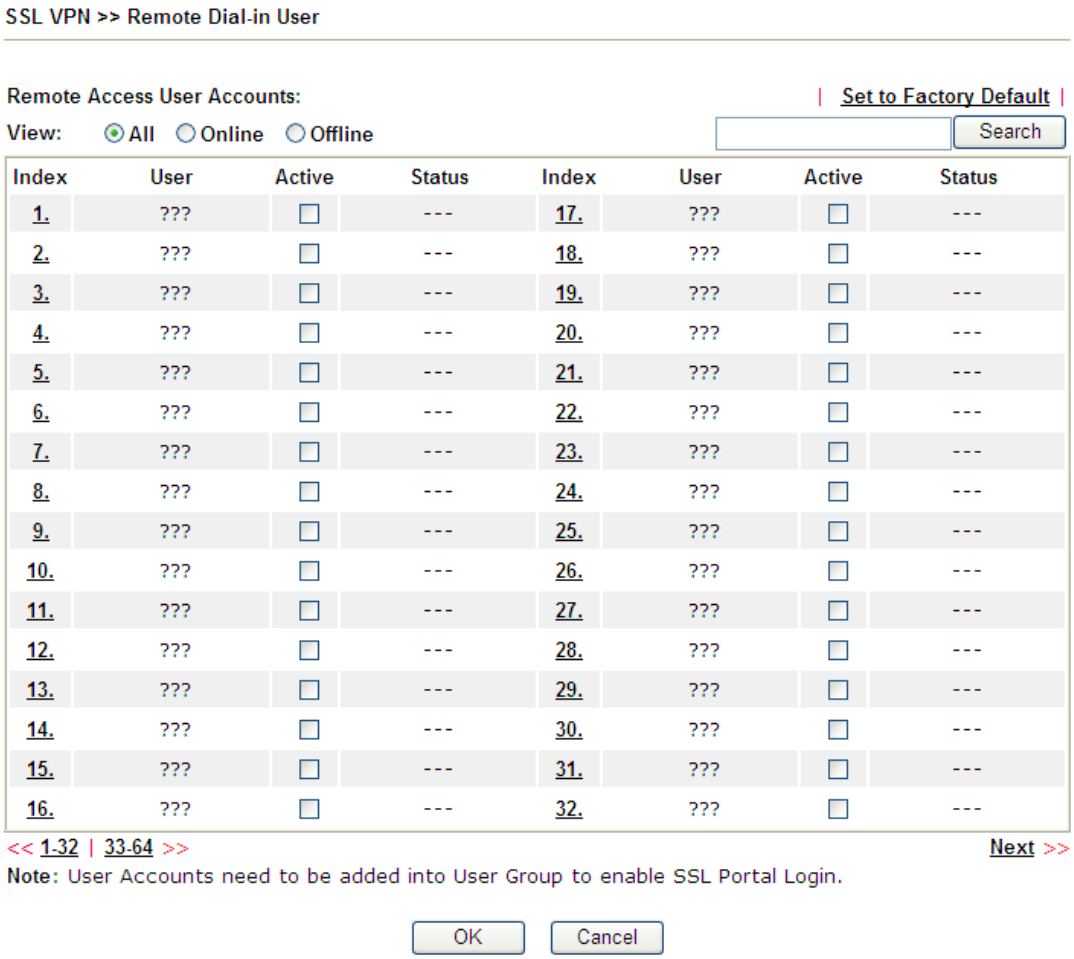
項目	說明
綁定至 WAN (Bind to WAN)	勾選您需要的 WAN 介面以便進行 SSL VPN 通道設立。
埠號(Port)	此埠號設定乃提供與 SSL VPN 伺服器之用，不會影響**系統維護>>管理(System Maintenance>>Management)**中的 HTTPS 埠號設定。基本上，預設值是 443。
伺服器憑證(Server Certificate)	若先前已經建立了數項憑證，可透過下拉式清單選擇任何一個使用者定義的憑證，否則請用**自行簽核(Self-signed)**讓路由器使用內建的預設憑證。預設憑證可用於 SSL VPN 伺服器以及 HTTPS 網頁代理伺服器。 但當用戶端未設定任何憑證時，預設憑證將用於 HTTPS 以及 SSL VPN 伺服器。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

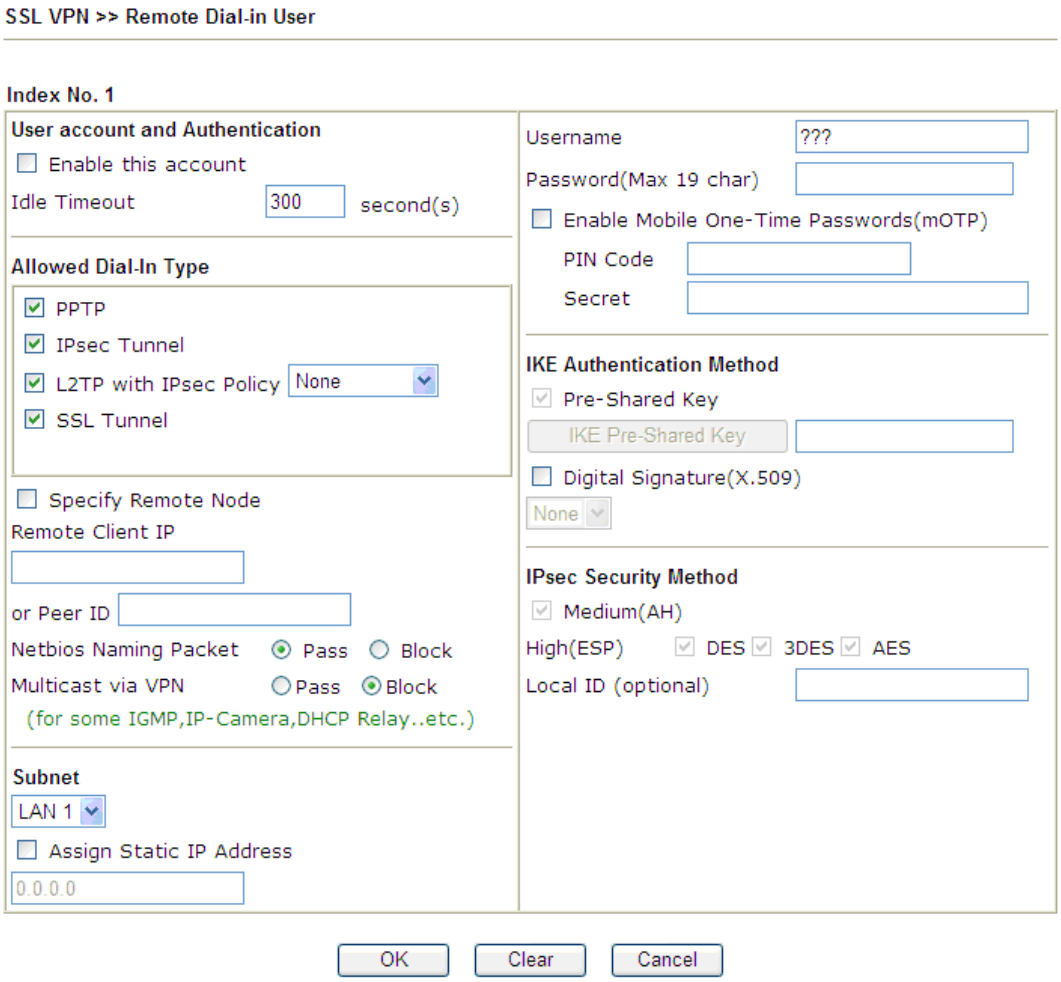
V-2-2 使用者帳號(User Account)

透過 SSL VPN，路由器可讓遠端工作人員方便且容易存取中心站點 VPN。遠端工作人員不需要安裝任何 VPN 軟體，只要使用一般的網頁瀏覽器，不論是客戶的網路或是網吧，您就可以建立 VPN 連線連回主要辦公室。SSL 技術與您用於安全網站例如線上銀行使用的加密技術是類同的，此外，SSL VPN 可以全通道模式或是代理伺服器模式，目前路由器允許設置 16 個使用者帳號。

對於 SSL VPN 而言，辨識驗證與管理都是透過使用者帳號來進行，因此 SSL VPN 使用者帳號必須與遠端撥入使用者的設定頁面相同。

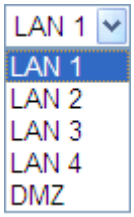


按下任一索引編號編輯遠端使用者設定檔。



可用設定說明如下：

項目	說明
使用者帳號與認證(User account and Authentication)	**開啓這個帳號(Enable this account) -**勾選此方塊以啓用此功能。 **閒置逾時(Idle Timeout) -** 如果撥入使用者閒置超過所設定的時間，路由器將會自動中斷連線，預設閒置逾時爲 300 秒。 **使用者名稱(User Name)** - 當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。請輸入名稱。 **密碼(Password)** -當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。請輸入密碼。 **啓動行動動態密碼系統 (mOTP)(Enable Mobile One-Time Passwords (mOTP))-** 勾選此框以便利用 mOTP 功能進行驗證。 **PIN 碼(PIN Code)** – 輸入驗證專用碼（例如 1234）。 **密鑰(Secret)** – 使用行動電話中由 mOTP 產生的 32 個數字密碼(例如 e759bb6f0e94c7ab4fe6）。
允許的撥入模式(Allowed Dial-In Type)	**PPTP** -爲伺服器建立一個透過網際網路的 PPTP VPN 連線，您必須設定連線類型和身分辨識像是使用者名稱與密碼等，以便驗證遠端伺服器。 **IPSec 通道(PSec Tunnel)-**允許遠端撥入使用者透過網際網路觸發 IPSec VPN 連線。 **具有 IPSec 原則的 L2TP(L2TP with IPSec Policy)-**爲伺服器建立

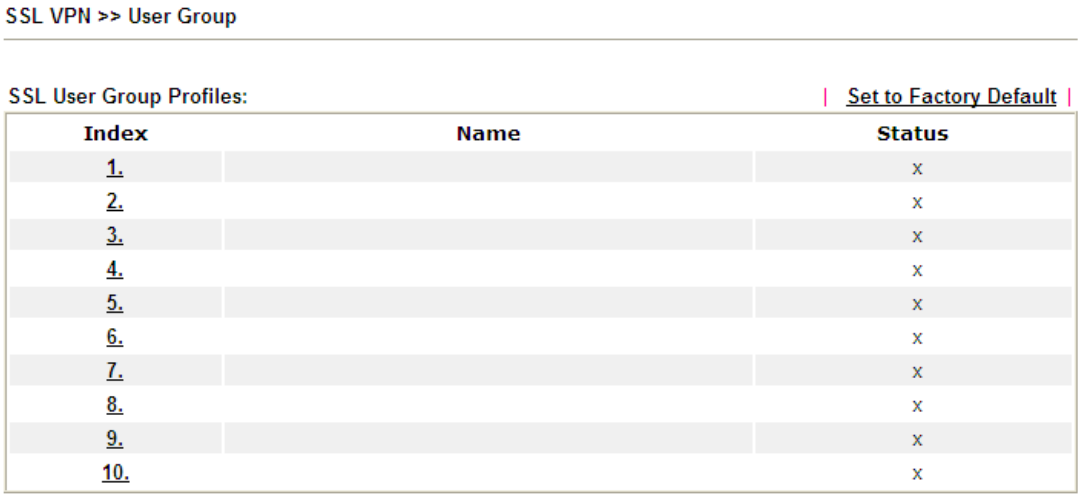
項目	說明
	一個透過網際網路的 L2TP VPN 連線。您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取： ● **無(None) -** 此選項完全不會應用 IPSec 原則，VPN 連線採用不帶有 IPSec 原則的 L2TP，可以在完全 L2TP 連線中檢視內容。 ● **建議選填(Nice to Have) -**如果在整個連線過程中完全可以運用，此選項會先應用 IPSec 原則。否則撥入 VPN 連線會成爲一種完全的 L2TP 連線。 ● **必須(Must) -** 此選項可在 L2TP 連線中明確指定所要運用的 IPSec 原則。 **SSL 通道(SSL Tunnel)-**允許遠端撥入用戶透過網際網路進行 SSL VPN 連線。如果您勾選此框，專屬此帳號的 SSL 通道就會立即啓動。 **指定遠端節點(Specify Remote Node)-**您可以指定遠端撥入使用者或是對方 ID (應用於 IKE 主動模式中)的 IP 位址。若您不勾選此項，即表示您所選擇的連線類型，將會應用**基本設定**中所設定的驗證方式和安全防護方式。 **Netbios 命名封包(Netbios Naming Packet)** ● **通過(Pass)** – 按此鈕讓資料能在二台主機之間所建立的 VPN 通道上傳輸。 ● **封鎖(Block)** – 當雙方所建立的 VPN 通道連線產生衝突時，此功能可以此通道。 **經由 VPN 執行多重播送(Multicast via VPN) -**某些程式可透過 VPN 連線進行多重播送封包。 ● **通過(Pass)** -點選此鈕讓多重播送封包通過路由器。 ● **封鎖(Block)** – 此爲預設值。點選此鈕之後，路由器將會封鎖多重播送封包。
子網路遮罩(Subnet)	選擇此 VPN 設定檔所需的子網。  **指定固定 IP 位址(Assign Static IP Address) -** 請輸入固定 IP 位址。
IKE 認證方式(IKE Authentication Method)	當您指定遠端節點的 IP 位址時，本區僅適用於 **IPsec 通道**與**具有 IPSec 原則的 L2TP** 類型，唯一例外的是當您選擇 **IPsec 通道**時，不論有無指定 IP 位址，您還可以設定數位簽章(X.509)。 **預先共同金鑰(Pre-Shared Key)-** 勾選此方塊啓用此功能並輸入 1-63 文字做爲預先共同金鑰。 **數位簽章(X.509) (Digital Signature (X.509)) -**勾選此方塊啓用此功能並選擇一組事先定義的簽章內容(在 **VPN 和遠端存取 >>IPSec 端點辨識(VPN and Remote Access >>IPSec Peer Identity)**中設定。
IPSec 安全性模式(IPSec Security Method)	對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區爲必要設定。請勾選中級或是高級設定作爲安全防護方式。

項目	說明
	中級 -Authentication Header (AH)表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。 **高級 -Encapsulating Security Payload (ESP)**表示資料將被加密及驗證，請自下拉式清單中選取適合項目。 **本機 ID(Local ID)-**指定一個本地 ID 以便作爲 LAN-to-LAN 的撥入設定，此項是選擇項目且只能應用在 IKE 主動模式上。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

V-2-3 使用者群組(User Group)

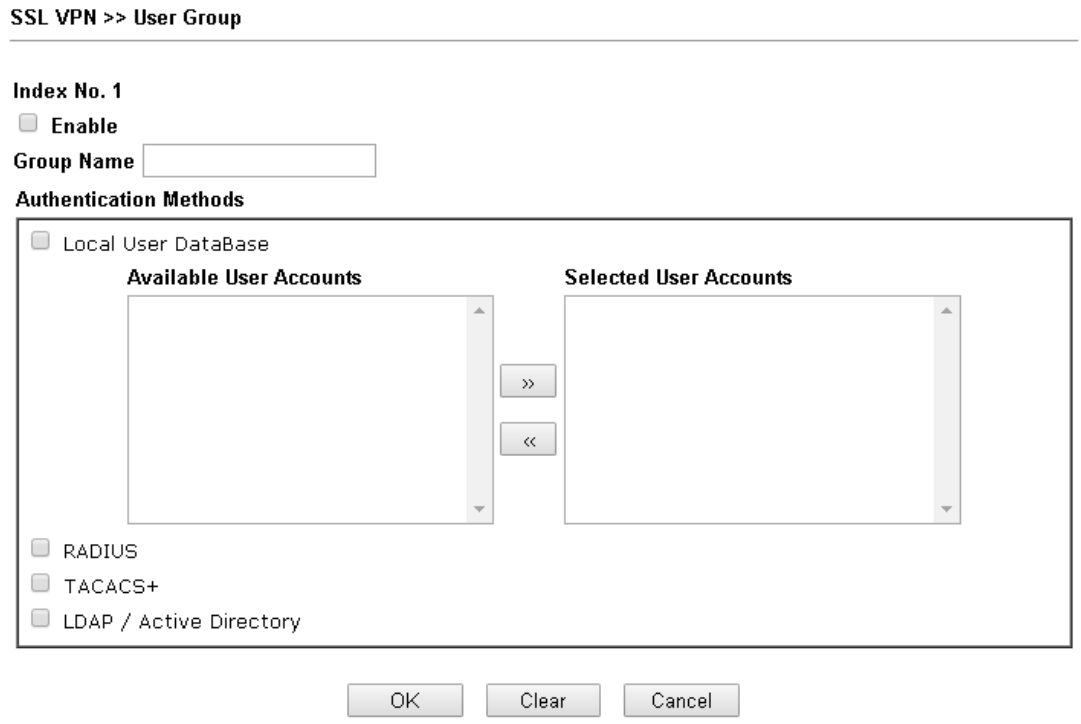
有 10 組使用者群組設定檔可以用來設定，並可運用在使用者管理、VPN 等地方。



可用設定說明如下：

項目	說明
回復出廠預設值(Set to Factory Default)	按下此連結清除全部設定檔內容。
索引編號(Index)	顯示設定檔連結之編號。
名稱(Name)	顯示物件設定檔的檔名。

按下任一索引編號編輯遠端使用者設定檔。



可用設定說明如下：

項目	說明
啓用(Enable)	勾選此方塊啓用此設定檔。
群組名稱(Group Name)	輸入此群組設定檔名稱。
驗證方式(Authentication Methods)	決定設定檔的驗證方法。 **本地使用者資料庫(Local User DataBase) -** 系統利用使用者定義的設定檔(在 **VPN 與遠端存取>>遠端撥入使用者(VPN and Remote Access>>Remote Dial-In User)**頁面)進行驗證，啓用的設定檔將條列在**可用的使用者帳號(Available User Account)**區，如要新增設定檔至群組當中，只要選擇該設定檔名然後按下**>>**鈕，該選定檔將顯示在**選定的使用者帳號(Selected User Account)**區中。 **RADIUS -** RADIUS 伺服器利用使用者名稱和密碼進行驗證。 **TACACS+** - TACACS+ 將利用使用者名稱與密碼進行相關驗證。 **LDAP / Active Directory -** 如果勾選的是此項， LDAP / AD 伺服器會利用選擇的設定檔內容以及帳號密碼來進行驗證。 若上述三種選項都啓用時，系統將據此按照順序執行驗證。

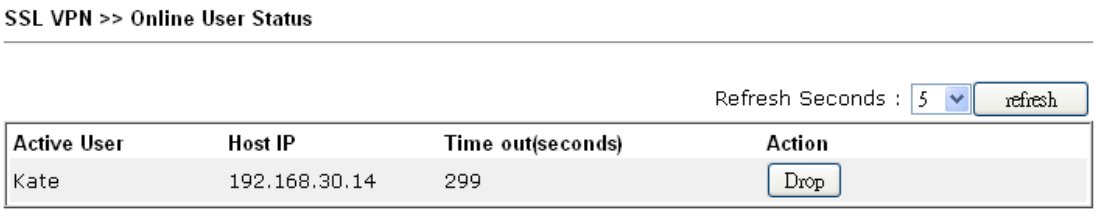
完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

V-2-4 線上使用者狀態(Online User Status)

如果您已經完成 SSL 網頁伺服器的設定，使用者即可登入 DrayTek SSL VPN 入口網站查看相關設定。



接著，使用者可以開啓 **SSL VPN>> 線上使用者狀態(SSL VPN>> Online Status)**檢視 SSL VPN 登入狀態。



可用設定說明如下：

項目	說明
目前使用者(Active User)	顯示目前運用 SSL VPN 伺服器的使用者。
主機 IP(Host IP)	顯示主機的 IP 位址。
閒置逾時(Time out)	顯示強迫登出的剩餘時間。
動作(Action)	您可按下 Drop 按鈕中斷利用路由器 SSL 入口網站登入的特定使用者。

V-3 憑證管理(Certificate Management)

數位憑證就像是一個電子 ID，此 ID 可以由憑證授權中心註冊取得。它包含有您的名字、序號、到期日、憑證授權的數位簽章，這樣一來，接收者可以確認該憑證是否是真實的。本路由器支援遵守標準 X.509 的數位憑證。

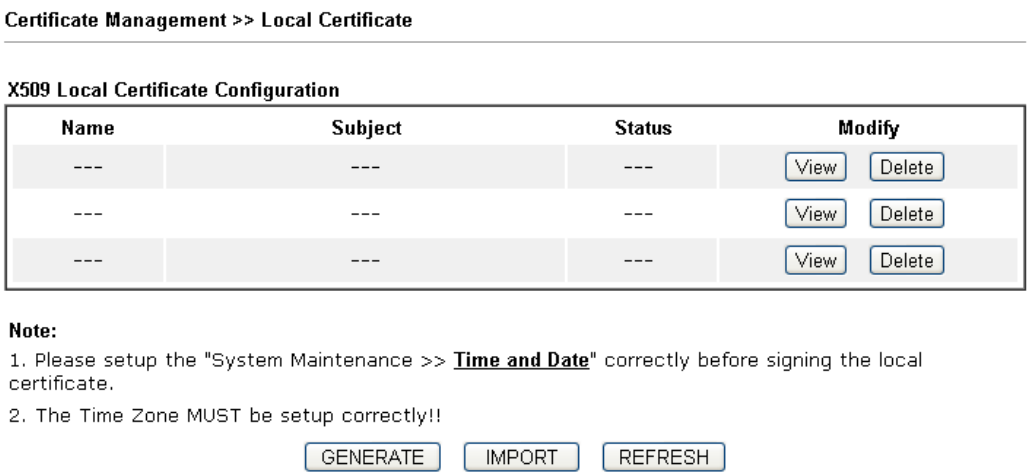
任何想要使用數位憑證的人都應該先有 CA 伺服器註冊的憑證，此憑證也可從其他具公信力的 CA 伺服器取得，如此還可以驗證其他從公信力的 CA 伺服器取得憑證的另一方。

此處您可以管理產生本機的數位憑證，並設定具公信力之 CA 憑證，使用憑證前，請記得調整路由器的時間，這樣才可取得正確的憑證有效期。

網頁使用者介面



V-3-1 本機憑證(Local Certificate)

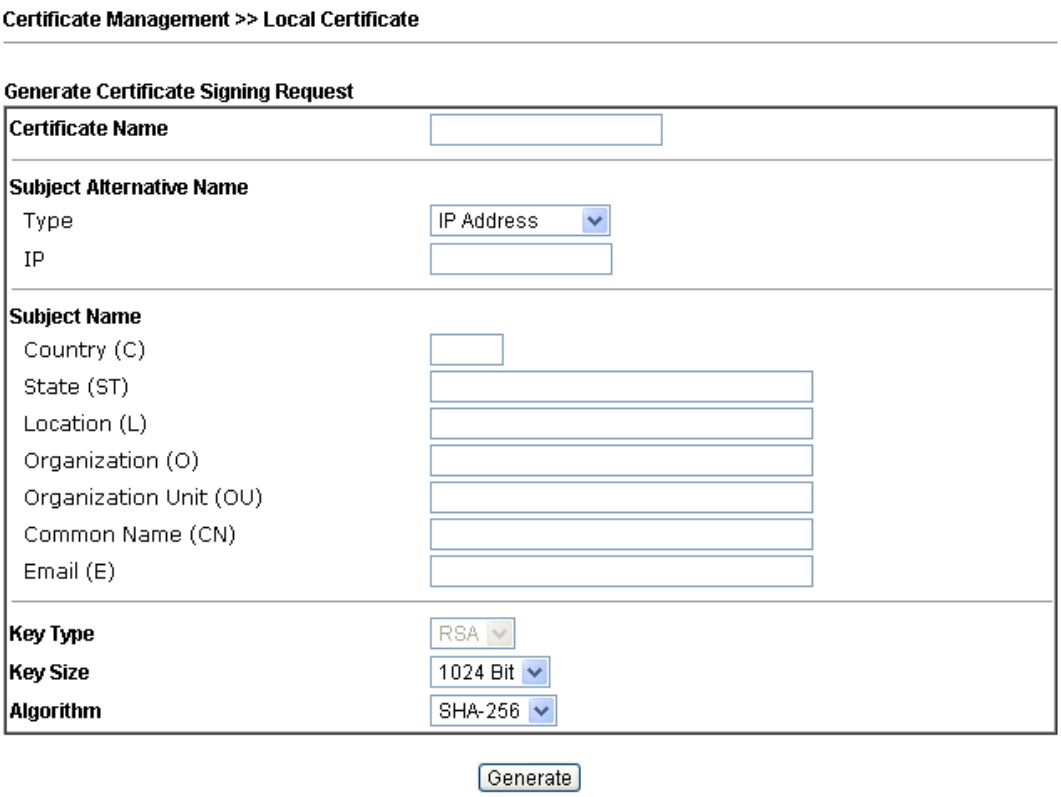


可用設定說明如下：

項目	說明
產生(Generate)	按此鈕以開啓**產生憑證需求(Generate Certificate Request)**視窗。 輸入全部的資訊，然後再按一次**產生(Generate)**按鈕。
匯入(Import)	按此鈕以匯入儲存的檔案作爲憑證資訊。
更新頁面(Refresh)	按此鈕以更新資訊。
檢視(View)	按此鈕以檢視憑證詳細的設定。
刪除(Delete)	按此鈕刪除選定的憑證及其相關資訊。

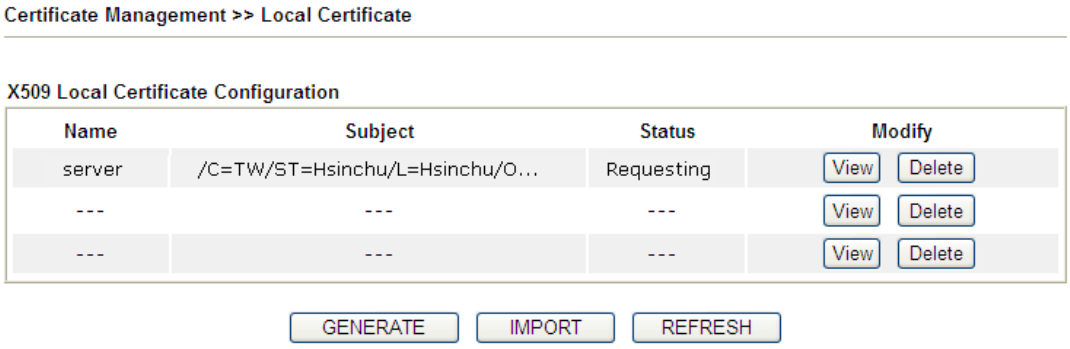
產生(GENERATE)

按下此鈕開啓**產生本機憑證需求(Generate Certificate Signing Request)**視窗，輸入所有必要資訊，例如檔名(用來分辨憑證)、主體替代名稱類型以及相關的設定內容，然後按最下方的**產生(GENERATE)**按鈕。



資訊 請注意常用名稱必須設定爲路由器的 WAN IP 位址或是網址。

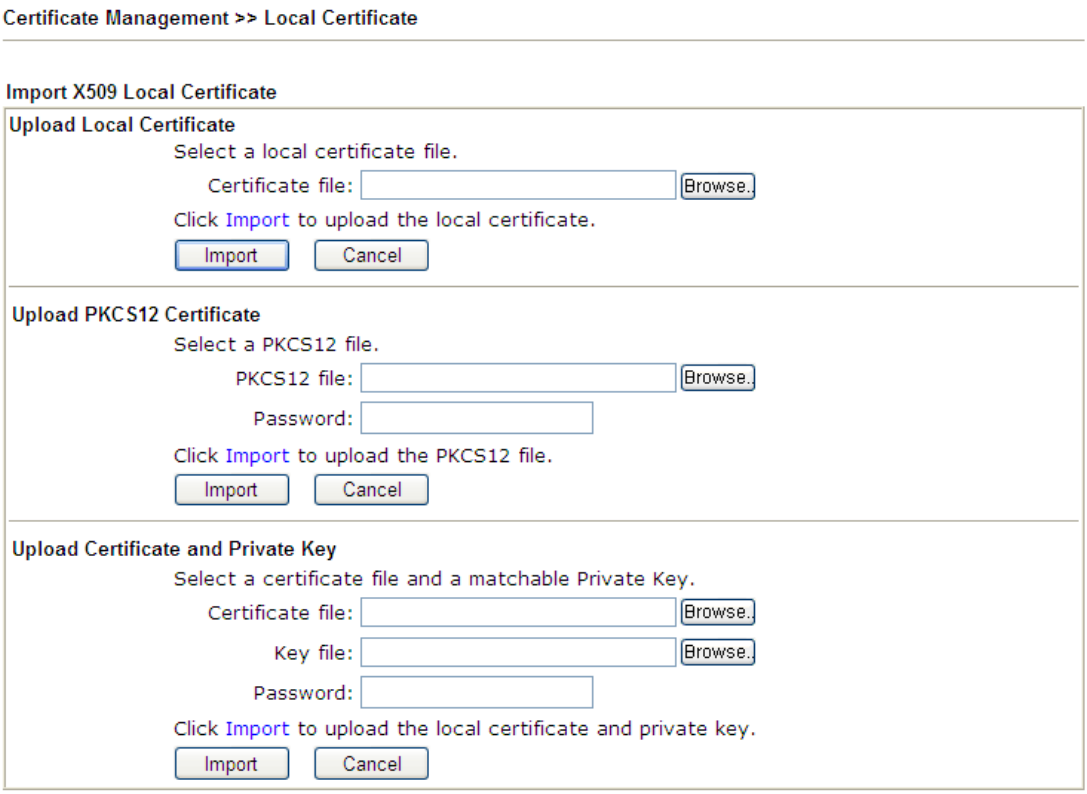
按下**產生(Generate)**按鈕之後，憑證產生的資訊就會顯示在畫面上：



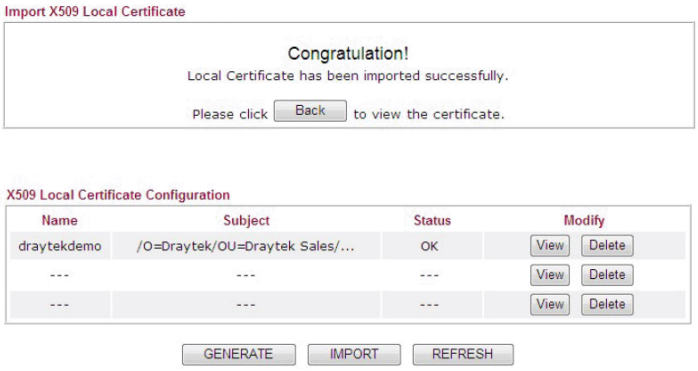
匯入(IMPORT)

路由器可讓您產生憑證需求並提交至 CA 伺服器，後續讓您匯入作爲本機憑證。如果您已經從第三方取得了憑證，您也可以直接採用。支援的類型爲 PKCS12 憑證以及含有密鑰的憑證。

按下此鈕後可以匯入檔案作爲憑證資訊，有三種本機憑證類型可以運用。



可用設定說明如下：

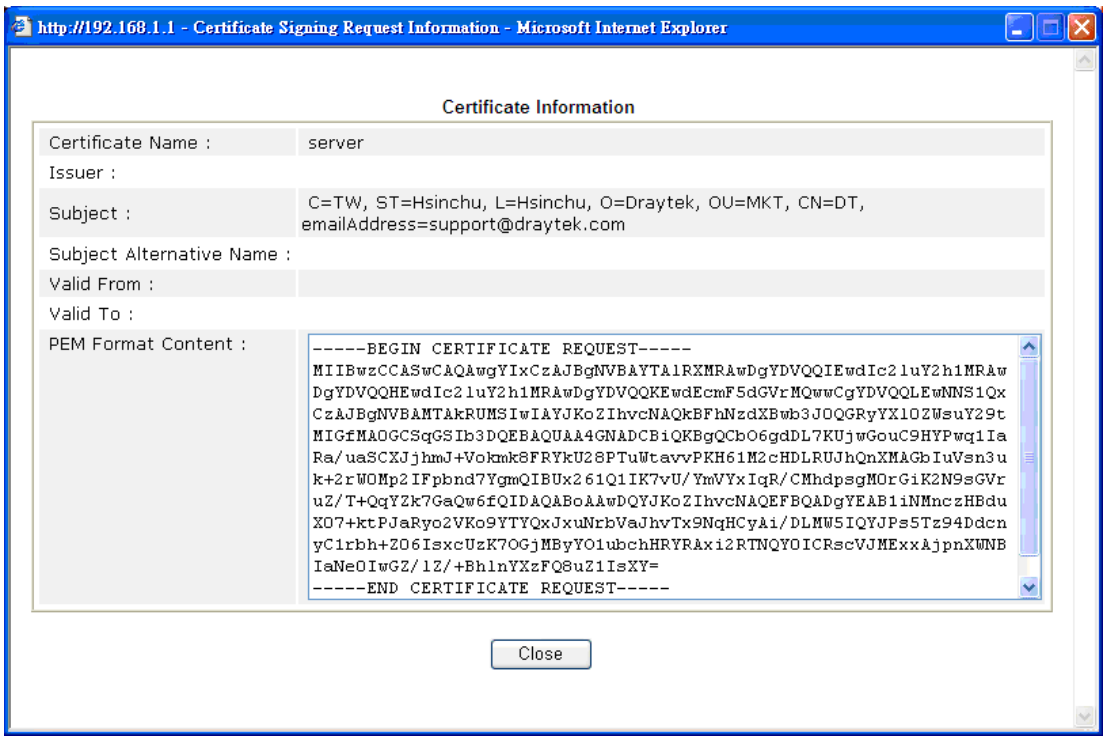
項目	說明
上傳本機憑證(Upload Local Certificate)	可讓使用者輸入路由器產生的且由 CA 伺服器簽署之憑證。 如果您已完成憑證產生作業，憑證的狀態欄會顯示確定**(OK)**。 
上傳 PKCS12 憑證(Upload PKCS12 Certificate)	可讓使用者輸入副檔名爲.pfx 或 .p122 的憑證，這些憑證通常需要密碼驗證。 請注意 PKCS12 爲安全儲存虛擬密鑰與憑證的一種標準，主要用於 Netscape 與微軟 IE 上。
上傳憑證與虛擬密鑰(Upload Certificate and Private Key)	這個功能在使用者有不同的憑證與虛擬密鑰時特別有用，若密鑰本身需要加密，那麼請輸入密碼內容。

頁面更新(REFRESH)

按下此鈕可以更新資訊頁面。

檢視(View)

按下此鈕查看細部內容。



資訊	請自上述視窗複製憑證需求資訊，接著登入您的 CA 伺服器然後進入憑證需求頁面，複製憑證需求資訊至該頁面上並提交要求，CA 伺服器將依據此點發行憑證，您即可將該憑證儲存備用。

刪除(Delete)

按此紐移除選定的憑證。

V-3-2 具公信力之 CA 憑證(Trusted CA Certificate)

具公信力 CA 憑證列出三組憑證，若有必要，您也可以建立一個 RootCA 憑證。

當本機用戶與遠端用戶都需要進行憑證驗證(例如 IPsec X.509)以便讓資料通過 SSL 通道並且防止來自 MITM 攻擊時，可使用具公信力之憑證(Root CA)可用來驗證雙邊提供的數位憑證。

然而，套用來自具公信力數位憑證的數位憑證是相當複雜且花時間，因此路由器提供一種機制讓您可以產生根 CA 節省時間並提供一般使用者更多的便利性。之後此根 CA 可以進行本機憑證之發行事宜。

資訊

根 CA(Root CA)可以刪除但無法編輯改寫，如果您想要修改根 CA 設定，請刪除該憑證，重新再建立一個。

Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Root CA	---	---	Create
Trusted CA-1	---	---	View Delete
Trusted CA-2	---	---	View Delete
Trusted CA-3	---	---	View Delete

Note:

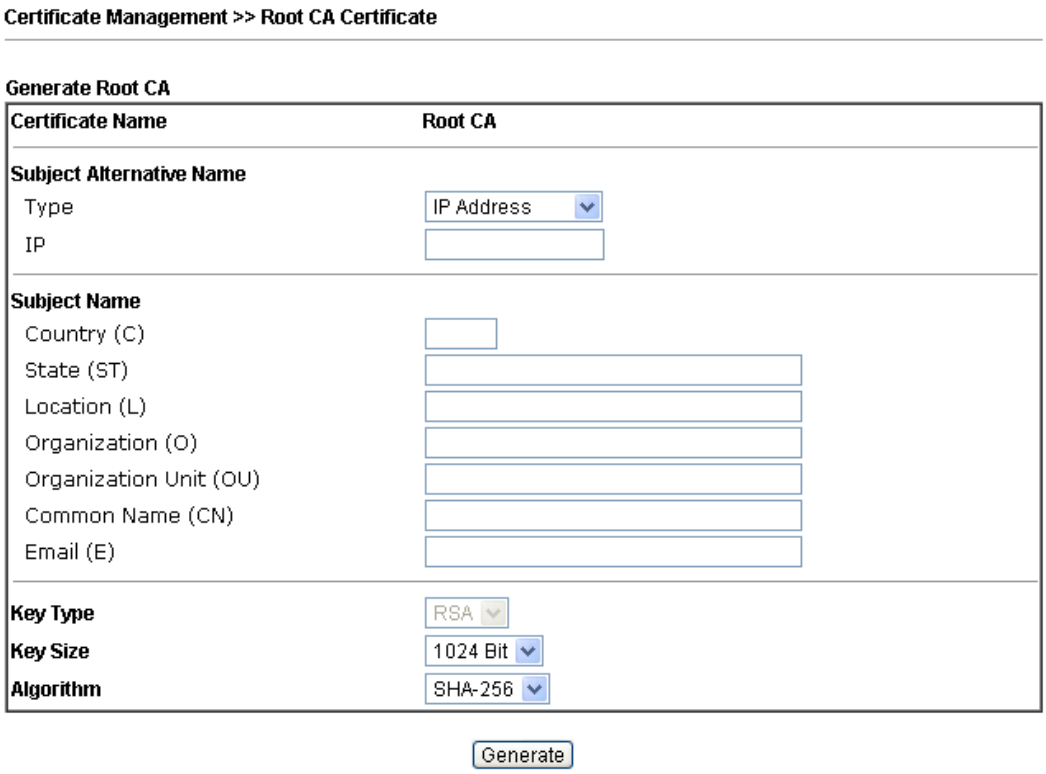
1.Please setup the "System Maintenance >> **Time and Date**" correctly before you try to generate a RootCA!!

2.The Time Zone MUST be setup correctly!!

IMPORT REFRESH

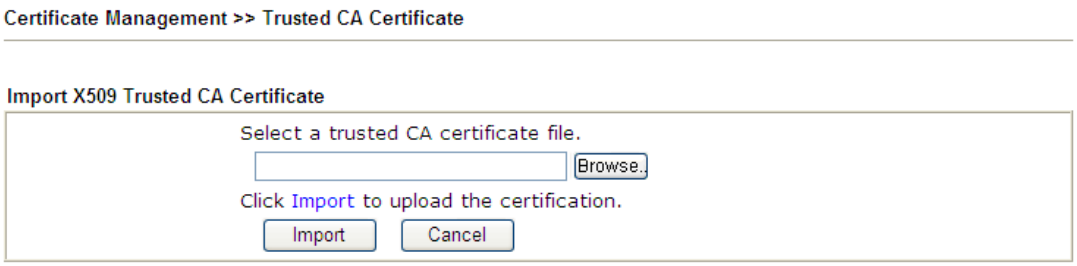
建立根 CA 憑證(Root CA)

按下建立**(Create)** 開啓如下頁面。輸入頁面要求的所有資訊，例如憑證名稱(用於辨識不同的憑證用)、主體替代名稱類型與其他相關的設定，接著再按下產生**(Generate)**。

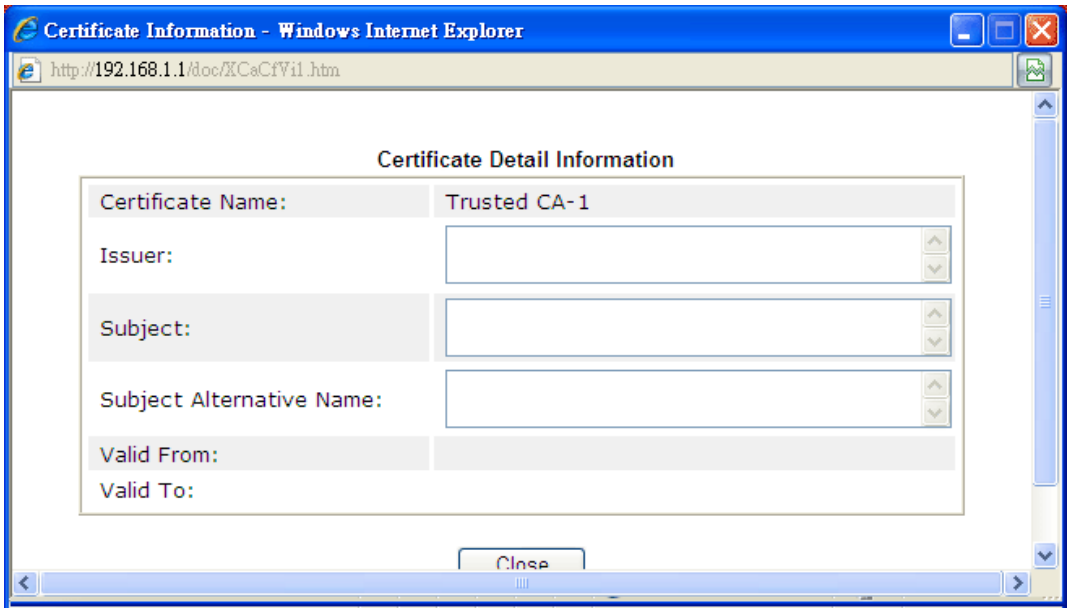


輸入具公信力的 CA 憑證 (Trusted CA)

若要輸入事先儲存的具公信力之 CA 憑證，請按**匯入(IMPORT)**鈕開啓如下的視窗，並使用**選擇檔案(Browse...)**找到儲存的文字檔案，接著按下**匯入(IMPORT)**鈕，您所要匯入的檔案將會列在視窗上。



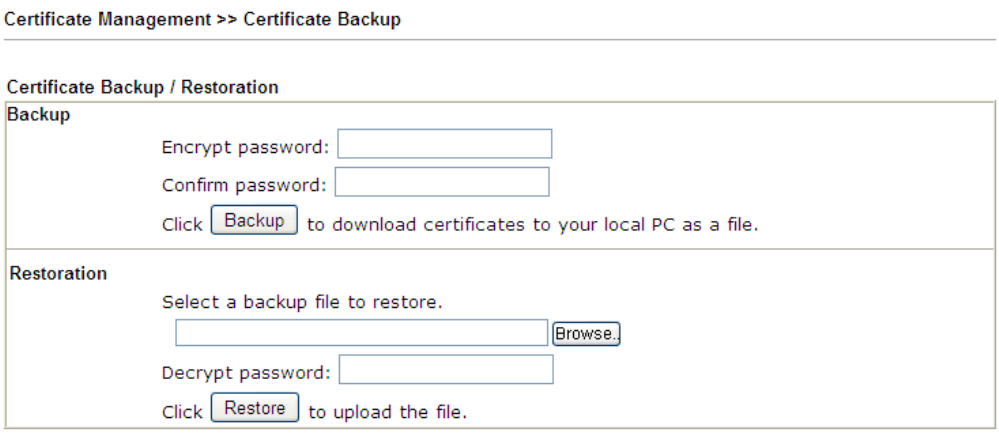
如要檢視每個具公信力之 CA 憑證，請按**檢視(View)**按鈕開啓憑證的詳細資訊視窗，如果您想要刪除 CA 憑證，選擇該憑證並按下**刪除(Delete)**按鈕，所有相關的憑證資訊即可刪除。



V-3-3 憑證備份(Certificate Backup)

路由器的本機憑證與具公信力之 CA 憑證可以儲存爲一個檔案，請按下述畫面的備份按鈕來儲存，如果您想要設定加密的密碼，請在**加密密碼(Encrypt password)**與**確認密碼(Confirm password)**二欄中輸入所需的字元。

同時，您也可以隨時使用**還原(Restore)**功能取回設定內容。



第六篇 安全性設定



Firewall

當使用者需要更多的頻寬以便用於多媒體、交互運用或是遠距學習時，最關心的莫過於網路安全性議題。路由器的防火牆功能可保護您的區域網路，免受未經授權之外來者的攻擊，同時也可限制區域網路中的使用者登入網際網路。



CSM

CSM是中央安全性管理的簡稱，用來控制IM/P2P運用，過濾網頁內容以及URL內容，已達成安全性管理的目標。

VI-1 防火牆(Firewall)

當寬頻使用者需要更多的頻寬以便用於多媒體、應用程式或是遠程學習時，安全性總是最受到重視的一環。Vigor 路由器的防火牆可以協助保護您本地網路免受外在人物的攻擊，同時它可限制本地網路的使用者存取網際網路。此外它還可以過濾一些由觸發路由器所建立的連線特定封包。

防火牆工具

區域網路上的使用者可以下述的防火牆工具，接受良好的安全防護：

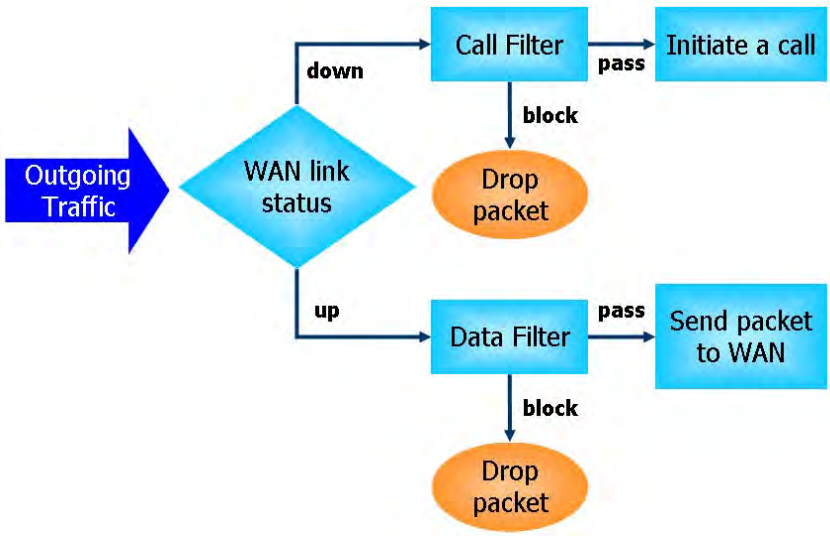
- 用戶設定 IP 過濾器(呼叫過濾器/資料過濾器)
- Stateful Packet Inspection (SPI): 追蹤封包並阻擋未經要求而流入的資料
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS)攻擊防禦

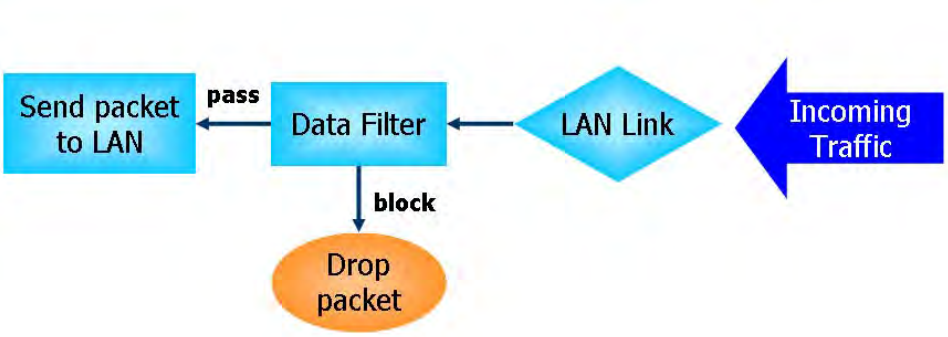
IP 過濾器

依照現有網際網路連線的需求、廣域網路連接狀態(開啓或關閉)的情形，IP 過濾器結構可將資料流量分成二大類：呼叫過濾器和資料過濾器。

- **呼叫過濾器(Call Filter) -**當目前沒有任何網際網路連線時，呼叫過濾器可應用在所有的資料運輸流量上，所有的運輸應該是往外送出。系統會按照過濾器規則檢查封包，如果是合法的，該封包即可通過，然後路由器將啓動一次呼叫來建立網際網路連線，再將該封包傳送往網際網路。
- **資料過濾器(Data Filter) -** 網際網路正處於連線狀態時，資料過濾器可應用在流入與流出的資料傳輸上，系統會按照過濾器規則檢查封包，如果是合法的，該封包即可通過。

以下圖表解釋流入(傳入)與流出(對外)之資料傳輸程式。





封包狀態檢測(SPI)

在網路層級上，封包狀態檢測是一種防火牆結構，它會建立一個封包狀態機器來追蹤防火牆於所有介面的連線狀況，並確保這些連線都是有效的。此類型防火牆並不只是檢查封包標頭資訊，它同時也監視著連線的狀態。

DoS 攻擊防禦 (DoS Defense)

DoS 攻擊防禦功能協助用戶檢測並減輕 DoS 攻擊，這類攻擊通常可分成二大類 – flood 類型攻擊和弱點攻擊。flood 類型攻擊嘗試耗盡您的系統資源，而弱點攻擊則是利用通訊協定或是操作系統的弱點嘗試癱瘓系統。

DoS 攻擊防禦功能的引發是以 Vigor 路由器的攻擊特徵值資料庫爲基礎，執行每一個封包的檢查，任何可能重複產生以癱瘓主機之惡意封包，在安全的區域網路中都將嚴格阻擋，如果您有設定系統紀錄伺服器，那麼系統紀錄訊息也會傳送警告資訊給您。

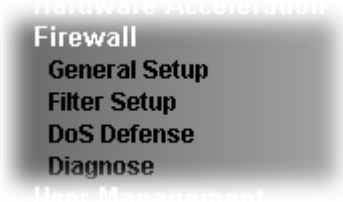
Vigor 路由器也可以監視資料流量，任何違反事先定義的參數的不正常資料流(例如臨界值的數字)，都會被視爲是一種攻擊行爲，Vigor 路由器將啓動防衛機制，及時阻擋減輕災害。

下列表格顯示出 DoS 攻擊防禦功能所能檢測出的攻擊類型。

1. SYN flood attack
2. UDP flood attack
3. ICMP flood attack
4. Port Scan attack
5. IP options
6. Land attack
7. Smurf attack
8. Trace route
9. SYN fragment
10. Fraggle attack
11. TCP flag scan
12. Tear drop attack
13. Ping of Death attack
14. ICMP fragment
15. Unassigned Numbers

網頁使用者介面

下圖爲防火牆的功能項目：



VI-1-1 基本設定(General Setup)

基本設定(General Setup)允許您調整 IP 過濾器和一般選項的設定內容，在此頁面您可以啓動或是關閉**呼叫過濾器(Call Filter)**或**資料過濾器(Data Filter)**。在某些情況下，您的過濾器可利用連結的方式執行一系列過濾工作，因此在這裡，您只要指定**開始過濾器組別(Start Filter Set)**即可。您也可以調整紀錄模式設定，勾選**(Apply IP filter to VPN incoming packets)**與**接受流入的 UDP Fragment 封包(Accept incoming fragmented UDP packets)**。

基本設定頁面

此頁面可讓您啓用/停用呼叫過濾器與資料過濾器，決定過濾進出資料的一般規則。



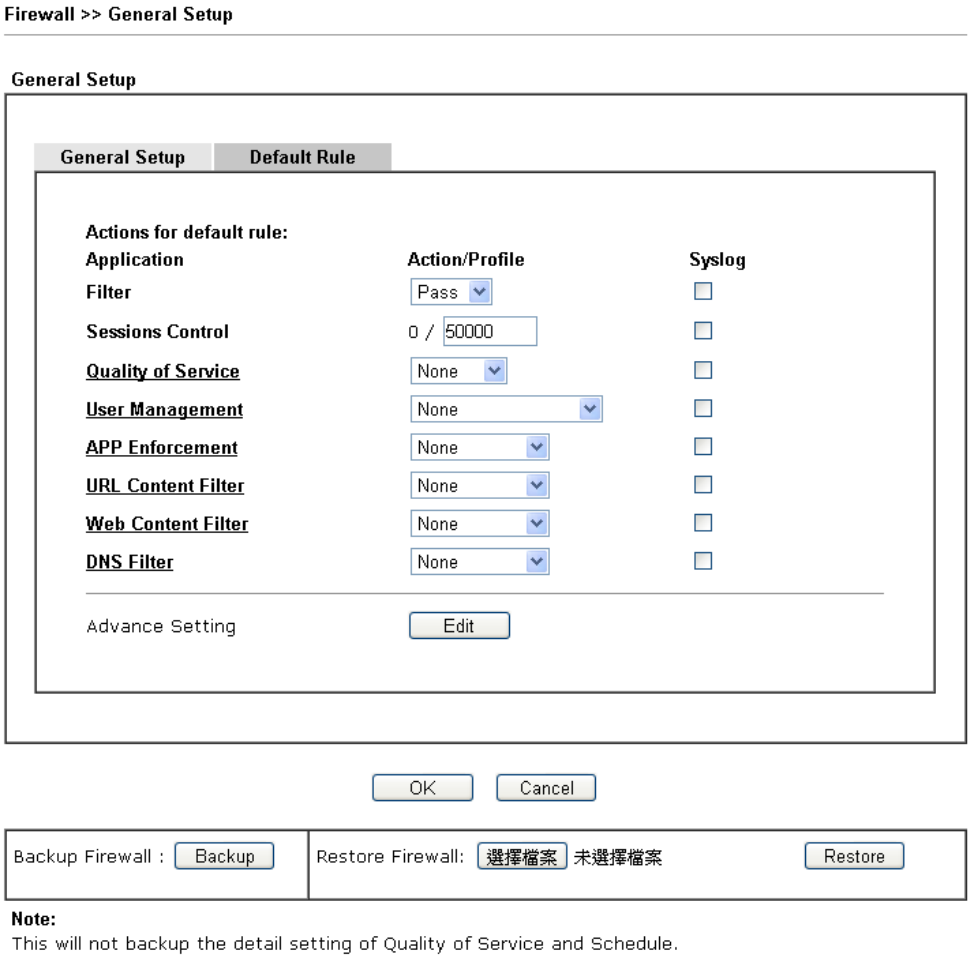
可用設定說明如下：

項目	說明
呼叫過濾器(Call Filter)	選擇**啓用(Enable)**以啓動呼叫過濾器功能，並指定開始過濾器組別。

資料過濾器(Data Filter)	選擇**啓用(Enable)**以啓動資料過濾器功能，並指定開始過濾器組別。
接受流入的大量 UDP 或是 ICMP Fragment 封包 (Always pass inbound fragmented large packets...)	一些線上遊戲都會使用很多的片段 UDP 封包來傳送遊戲資料，出於安全防火牆的本能直覺，Vigor 路由器會將這些片段封包給退回，以避免攻擊發生，除非您啓動**接受流入的大量 UDP 或是 ICMP Fragment 封包(Always pass inbound fragmented large packets...)**勾選此方塊後，您就可以在這些線上遊戲上悠遊。如果安全利害關係具有較高的重要性，您就不要啓動**接受流入的大量 UDP 或是 ICMP Fragment 封包(Always pass inbound fragmented large packets...)**功能。
啓動嚴格安全防火牆策略 (Enable Strict Security Firewall)	爲了安全起見，路由器將會執行嚴格的資料傳輸安全性檢驗動作。 此功能在預設狀態下是啓用的，所有透過路由器傳送的封包都會經過防火牆過濾一番。如果防火牆系統（例如內容過濾伺服器）並未有任何回應（通過或是封鎖），那麼路由器防火牆會直接封鎖所有的封包。
封鎖來自 WAN 的路由封包 (Block connections initiated from WAN)	通常，由 WAN 至 LAN 的 IPv6 網路連線數/流量是允許。 **IPv6** - 勾選此方塊讓路由器得以封鎖透過 IPv6 傳送過來的封包(自 WAN 到 LAN)，這個功能對於封鎖路由封包有效用，但是對於 NAT 過來的封包就沒有作用。 **IPv4** - 勾選此方塊讓路由器得以封鎖透過 IPv4 傳送過來的封包(自 WAN 到 LAN)，這個功能對於封鎖路由封包有效用，但是對於 NAT 過來的封包就沒有作用。
備份防火牆(Backup Firewall)	按此按鈕儲存防火牆設定。
還原防火牆(Restore Firewall)	按下**選擇(Select)**按鈕挑選防火牆設定檔案，接著按下**還原(Restore)**按鈕套用此檔案。

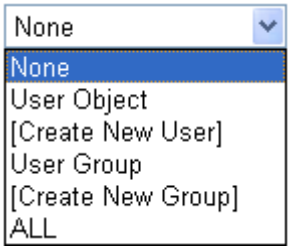
預設規則頁面

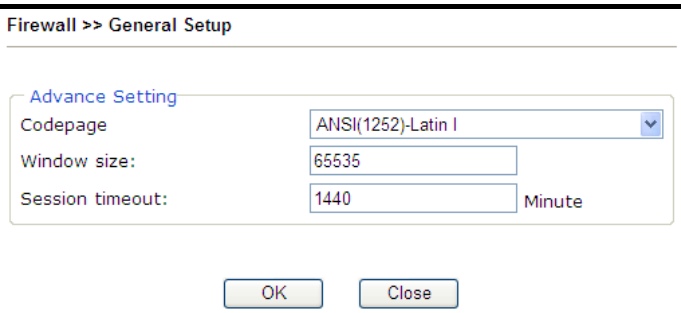
本頁讓您選擇過濾設定檔包含 QoS、負載平衡策略、WCF、應用程式管控、URL 內容過濾、網頁內容過濾、DNS 過濾等等以便透過路由器進行資料傳輸。



可用設定說明如下：

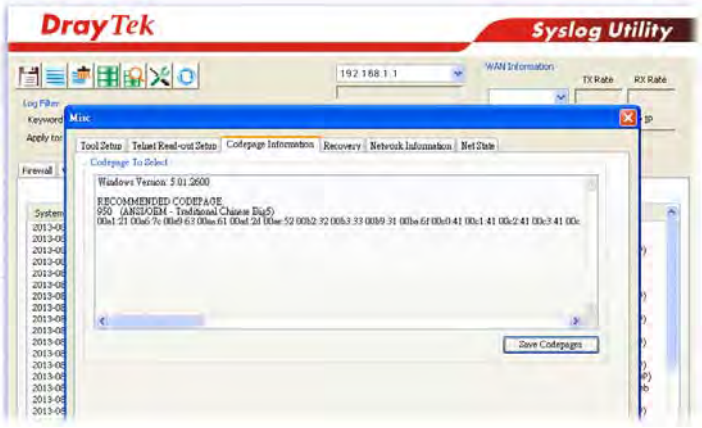
項目	說明
過濾器(Filter)	**通過(Pass)** - 所有的封包都可通過路由器，不需考慮**防火牆>>過濾器**的設定內容。 **封鎖(Block)** - 所有的封包都不許通過路由器，且不需考慮**防火牆>>過濾器**的設定內容。
連線數控制 (Sessions Control)	此處輸入的值爲全部的封包連線數，預設值爲 50000。
服務品質 (Quality of Service)	選擇一組 QoS 規則作爲防火牆規則，設定 QoS 細節資訊部分，請參考稍後的相關章節。 None None Class 1 Class 2 Class 3 Default
使用者管理	本項目僅在**使用者管理>>基本設定(User**

	Management>>General Setup) 中選擇**規則模式 (Rule-Based)** 時可用，一般防火牆規則將套用在使用者/使用者群組/全部使用者上。  **注意:** 當沒有任何使用者設定檔或是使用者群組可供選擇時，系統會出現**建立新使用者[Create New User]**或是**建立新的群組[Create New Group]**選項供您建立新的設定檔。
應用程式管控 (APP Enforcement)	選擇應用程式管控設定檔來封鎖 IM/P2P 之類的應用，如果沒有任何設定檔可供選擇時，請從下拉式清單中選擇**建立新設定([Create New])**來建立一個新的設定檔。所有區域網路中的主機必須依循應用程式管控設定檔內的標準。有關詳細資訊，請參考**數位內容安全管理>>應用程式管控設定檔(CSM>> APP Enforcement)**章節。 因應疑難排解的需要，您可勾選 IM/P2P 紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 **Syslog/郵件警告(Syslog/Mail Alert)**章節。
URL 內容過濾器 (URL Content Filter)	選擇一個 **URL 內容過濾器**設定檔（在**數位內容安全管理(CSM)>> URL 內容過濾器(CSM>> URL Content Filter))**中所建立），請務必先在**數位內容安全管理(CSM)> URL 內容過濾器**中設定一個設定檔，或是從下拉式選單中選擇[建立新檔]產生新的設定檔。因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 **Syslog/郵件警告(Syslog/Mail Alert)**章節。
網頁內容過濾器 (Web Content Filter)	選擇一個**網頁內容過濾器**設定檔（在**數位內容安全管理(CSM)>> 網頁內容過濾器**中所建立），請務必先在**數位內容安全管理(CSM)>> 網頁內容過濾器**中設定一個設定檔，或是從下拉式選單中選擇[建立新檔]產生新的設定檔。因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 **Syslog/郵件警告(Syslog/Mail Alert)**章節
DNS 過濾器 (DNS Filter)	選擇一組 DNS 過濾器設定檔(於**數位內容安全管理>>DNS 過濾器**頁面中建立)，在**數位內容安全管理>>網頁內容過濾器設定檔**頁面中至少要先建立一個設定檔案以供選擇，或是從下拉式清單中選擇 DNS 過濾器連結以重新建立新的設定檔。
進階設定 (Advance Setting)	按**編輯(Edit)**按鈕開啓下述視窗，不過，在此強烈建議您使用預設值爲佳。



選擇編碼語系(Codepage) - 此功能用來比較不同語言之間的字元數，選擇正確的 codepage 可以幫助系統從 URL 解碼資料後能取得正確的 ASCII 碼，並強化 URL 內容過濾器的正確性。預設值爲 ANSI 1252 Latin，如果您未選擇任何的 codepage，URL 解碼動作也不會執行，請自下拉式清單中選擇一個 codepage。

如果您不知道要如何選擇適宜的**編碼語系**，請開啓 Syslog。從 Setup 對話盒中的**編碼語系**(codepage)資訊，您將會看到系統建議的 codepage 內容。



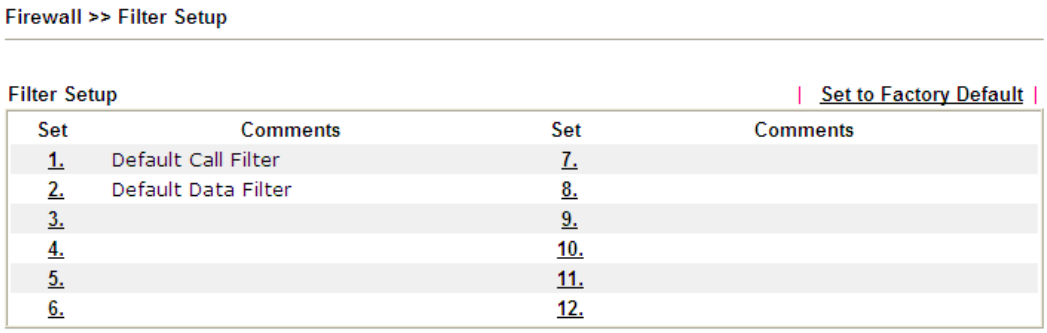
視窗大小(Window size) – 決定 TCP 協定的大小(0~65535)，數值越大，成效越佳，不過網路會較爲不穩定，小的數值比較適合穩定網路。

連線數逾時(Session timeout) – 設定連線數逾時時間可讓網路資源獲得較佳的運用，但是連續暫停僅適用於 TCP 協定，連線數逾時主要是針對符合防火強規則的資料流量而設定。

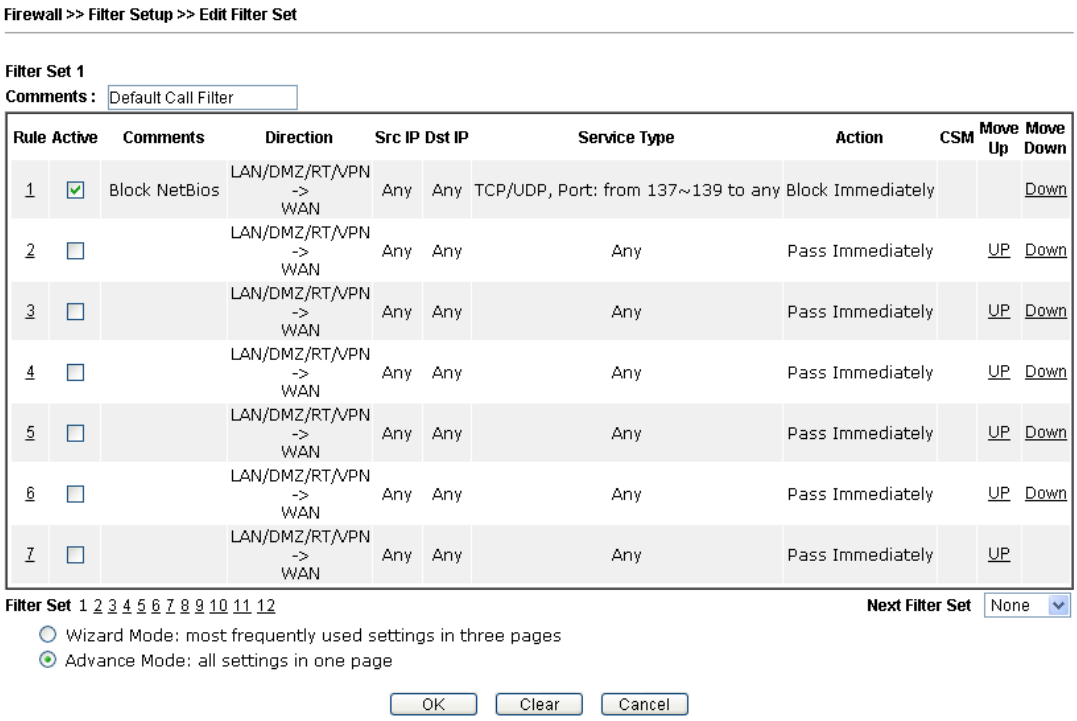
完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

VI-1-2 過濾器設定(Filter Setup)

按**防火牆(Firewall)**並選擇**過濾器設定(Filter Setup)**以開啓如下的設定網頁。



如果要新增一個過濾器，請按組別下方的數字按鈕以便編輯個別設定。如下的頁面將立即出現，每一個過濾器都含有 7 組規則，請按規則按鈕編輯每個規則，勾選**啓用(Active)**則可啓動該項規則。



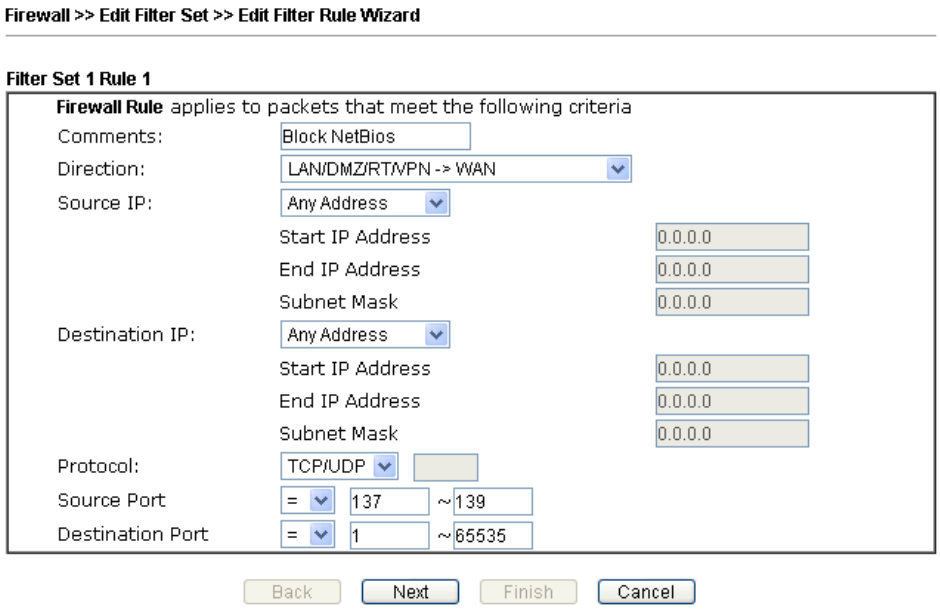
可用設定說明如下：

項目	說明
過濾器規則(Filter Rule)	請按號碼按鈕(1 ~ 7)編輯過濾器的規則，按下此鈕可以開啓過濾器規則網頁，有關詳細的資訊，請參考稍後的說明。
啓用(Active)	啓動或是關閉此項過濾規則。
註解(Comment)	輸入過濾規則註解說明，最大長度可以達到 23 個字元。
方向(Direction)	顯示封包的方向。
來源 IP/目的 IP (Src IP / Dst IP)	顯示來源/目的 IP 位址。
服務類型(Service Type)	顯示封包的類型與埠號。

動作(Action)	顯示處理的封包是通過還是封鎖。
CSM	顯示 CSM 是否啓用。
上移/下移 (Move Up/Down)	使用**上下(Up/ Down)**連結來移動過濾器規則的順序。
下一個過濾器組別(Next Filter Set)	設定前往下一個執行的過濾器連結，請勿讓多個過濾器設定形成一個迴路。
設定精靈模式(Wizard Mode)	允許利用數個設定頁面，配置經常使用的過濾器規則設定。
進階模式(Advance Mode)	允許設定過濾器規則細節內容。

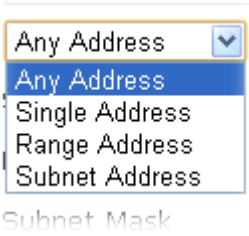
欲使用**設定精靈模式**，請依下述步驟進行：

1. 按下**設定精靈模式(Wizard Mode)**。
2. 按下索引編號 1，設定頁面出現如下：



可用設定說明如下：

項目	說明
註解(Comments)	輸入過濾器設定註解說明，最大長度爲 14 個字元。
方向(Direction)	設定封包流向的方向，此項設定僅適用**資料過濾器(Data Filter)**，對於呼叫過濾器而言，這項設定是不適用的。 **注意:** RT 表示第二個子網的路由網域或是其他 LAN。

來源/目的 IP (Source IP / Destination IP)	手動設定 IP 位址時，請選擇**任一位址/單一位址/位址範圍/子網位址(Any Address/Single Address/Range Address/Subnet Address)**作爲位址類型，並在其後的方框中輸入相應內容。 
通訊協定(Protocol)	指定此過濾器規則將套用的通訊協定。
來源埠號/目的埠號 (Source Port / Destination Port)	*(=)* – 當起始埠號與結束埠號與的數值相同時，此符號表示一個通訊埠。當起始埠號與結束埠號的數值不同時，即表示設定檔所適用的通訊埠範圍。 *(!=)* –當起始埠號與結束的數值相同時，此符號表示除了這裡所指明的通訊埠以外，全都適用於此設定檔。當起始埠號與結束埠號數值不同時，即除了此處所設定的範圍以外，所有的通訊埠都適用於此設定檔。 *(>)* – 大於此數值的通訊埠號皆可使用。 *(<)* – 小於此數值的通訊埠號皆可使用。

3. 按下**一步(Next)** 進入如下頁面：

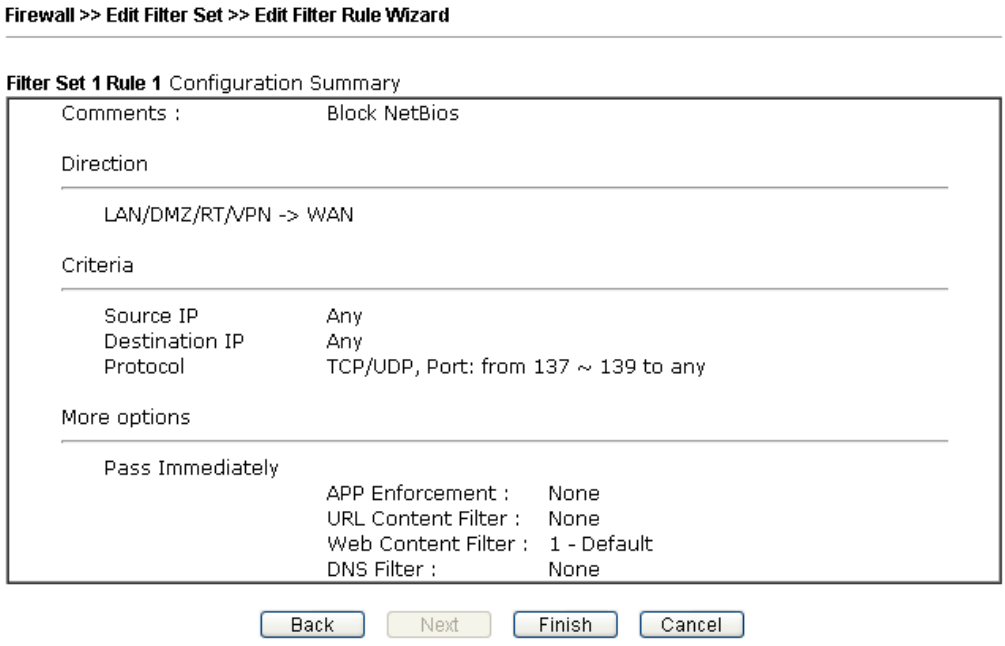


可用設定說明如下：

項目	說明
立刻通過 (Pass Immediately)	符合規則之封包可立即通過。 **應用程式管控(APP Enforcement) -** 選擇應用程式管控設定檔來封鎖 IM/P2P 之類的應用，如果沒有任何設定檔可供選擇時，請從下拉式清單中選擇**建立新設定[Create New]**來建立一個新的設定檔。所有區域網路中的主機必須依循應用程式管控設定檔內的標準。有關詳細資訊，請參考**數位內容安全管理>>應用程式管控設定檔**章節。 因應疑難排解的需要，您可勾選 IM/P2P 紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 Syslog/郵件警告章節。 **URL 內容過濾器(URL Content Filter) -** 選擇一個**URL 內容過**

	濾器設定檔（在**數位內容安全管理(CSM)>> URL 內容過濾器**中所建立），請務必先在**數位內容安全管理(CSM)> URL 內容過濾器**中設定一個設定檔，或是從下拉式選單中選擇**[建立新檔]([Create New])**產生新的設定檔。因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 Syslog/郵件警告章節。 **網頁內容過濾器(Web Content Filter) -** 選擇一個**網頁內容過濾器**設定檔（在**數位內容安全管理(CSM)>> 網頁內容過濾器**中所建立），請務必先在**數位內容安全管理(CSM)>> 網頁內容過濾器**中設定一個設定檔，或是從下拉式選單中選擇**[建立新檔]([Create New])**產生新的設定檔。因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 Syslog/郵件警告章節 **DNS 過濾器(DNS Filter) -** 選擇一組 DNS 過濾器設定檔(於**數位內容安全管理>>DNS 過濾器**頁面中建立)，在**數位內容安全管理>>網頁內容過濾器設定檔**頁面中至少要先建立一個設定檔案以供選擇，或是從下拉式清單中選擇 DNS 過濾器連結以重新建立新的設定檔。
立刻封鎖(Block Immediately)	系統封鎖符合規則之封包。

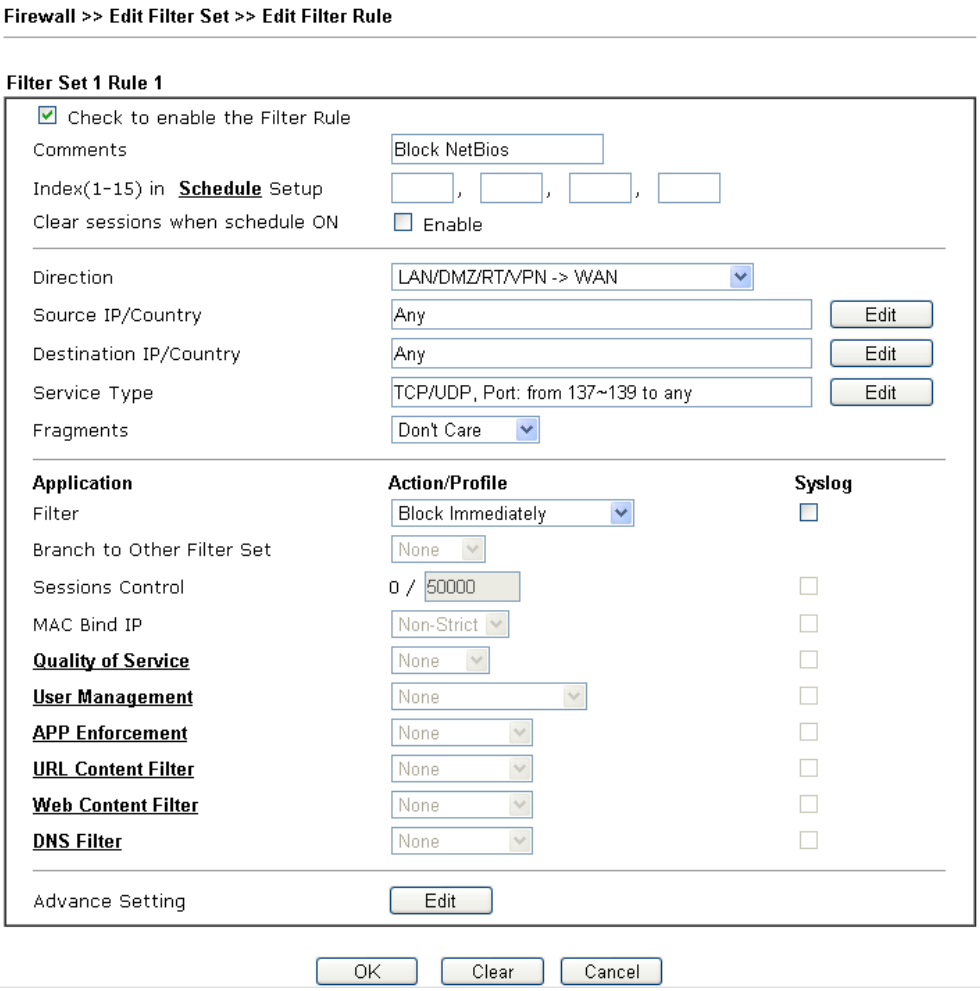
4. 指定相關項目之後，按**下一步(Next)** 進入總結頁面。



5. 若顯示頁面內容無誤，請按**完成(Finish)** 結束精靈設定。

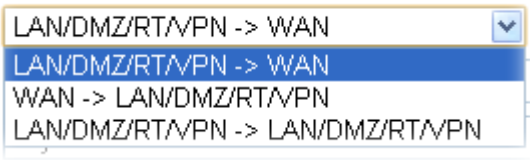
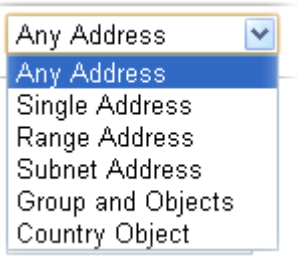
欲使用**進階模式**，請依下述步驟進行：

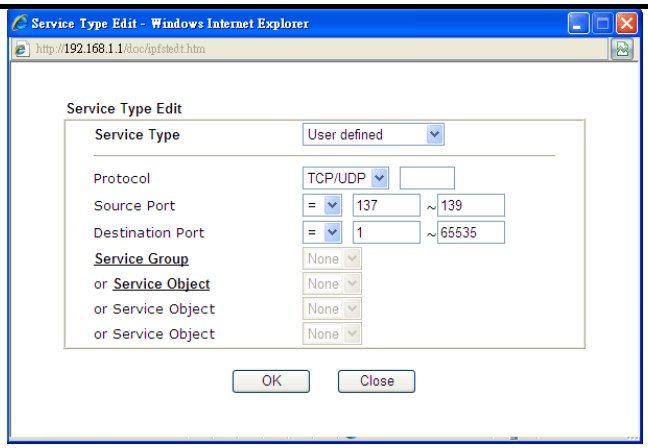
1. 按下**進階模式(Advance Mode)**。
2. 按下索引編號 1，設定頁面出現如下：



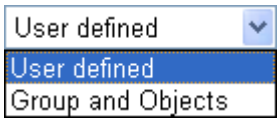
可用設定說明如下：

項目	說明
勾選以啓用過濾規則 (Check to enable the Filter Rule)	勾選此項目以啓動過濾規則。
註解(Comments)	輸入過濾器設定註解說明，最大長度爲 14 個字元。
索引號碼 (1-15) (Index(1-15))	設定區域網路上的電腦工作的時間間隔，您可以輸入四組時間排程，所有的排程都可在**應用>>排程(Applications >> Schedule)**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。
啓用排程時，清除連線數(Clear sessions when schedule ON)	勾選此方框可依據上述排程設定期間清除連線數資料。
方向(Direction)	設定封包流向的方向，此項設定僅適用**資料過濾器(Data Filter)**，對於呼叫過濾器而言，這項設定是不適用的。

	 **注意:** RT 表示第二個子網的路由網域或是其他 LAN。
來源 IP /國家 以及 目的 IP/國家 (Source IP/ Country and Destination IP / Country)	按下**編輯(Edit)**進入如下的畫面，選擇來源/國家/目的 IP 或是 IP 範圍。  欲手動設定 IP 位址，請選擇**任何位址/單一位址/範圍位址/子網位址(Any Address/Single Address/Range Address/Subnet Address)**作爲位址類型，並在此對話方塊輸入相關內容。此外，如果您想要在定義的群組或物件上使用 IP 範圍，請勾選**群組及物件(Group and Objects)**或是**國家物件(Country Object)**。  從 **IP 群組(IP Group)**下拉式清單中，選擇您需要應用的群組，或是使用 **IP 物件(IP Object)**下拉式清單，選擇您所需要的物件。
服務類型(Service Type)	按**編輯(Edit)**進入如下的畫面，以選擇適合之服務類型。



欲手動設定服務類型，請選擇使用者自訂做爲服務類型，並輸入相關的設定資料，此外如果您想要使用群組或是物件中所定義的服務類型，請選擇**群組與物件(Group and Objects)**作爲服務類型。



協定(Protocol) -指定本過濾器規則套用的協定。

來源/目的通訊埠(Source/Destination Port) -

(=) – 當起始埠號與結束埠號與的數值相同時，此符號表示一個通訊埠。當起始埠號與結束埠號的數值不同時，即表示設定檔所適用的通訊埠範圍。

(!=) –當起始埠號與結束的數值相同時，此符號表示除了這裡所指明的通訊埠以外，全都適用於此設定檔。當起始埠號與結束埠號數值不同時，即除了此處所設定的範圍以外，所有的通訊埠都適用於此設定檔。

(>) – 大於此數值的通訊埠號皆可使用。

(<) – 小於此數值的通訊埠號皆可使用。

服務群組/物件(Service Group/Object) - 使用下拉式選項選擇所需的項目。

片段(Fragments)

指定片段封包的執行動作，這個項目也是僅針對**資料過濾器(Data Filter)**。

忽略(*Don't care*) - 不論是怎樣的片端封包，系統皆不採取行動。

無片段(*Unfragmented*) - 應用規則至無片段之封包上。

片段(*Fragmented*)- 應用規則至片段之封包上。

太短了(*Too Short*) - 只有過短無法包含完整封包頭之封包，可應用此規則。

過濾器(Filter)

指定系統針對符合規則之封包所採取的行動。

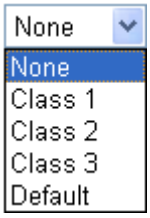
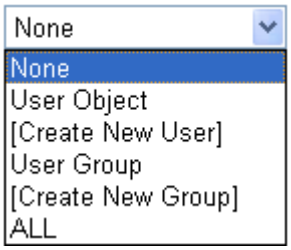
立刻通過(Pass Immediately)- 符合規則之封包可立即通過。

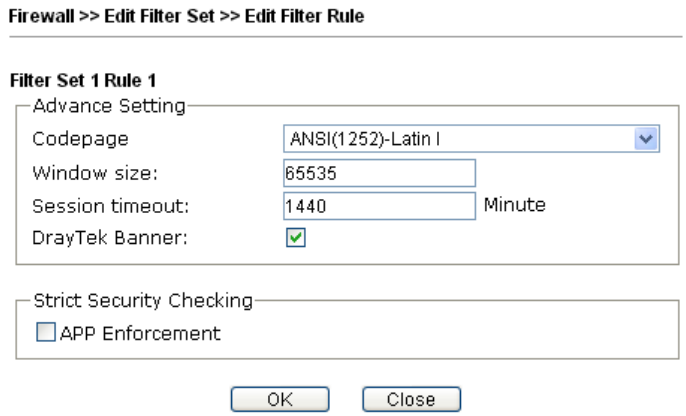
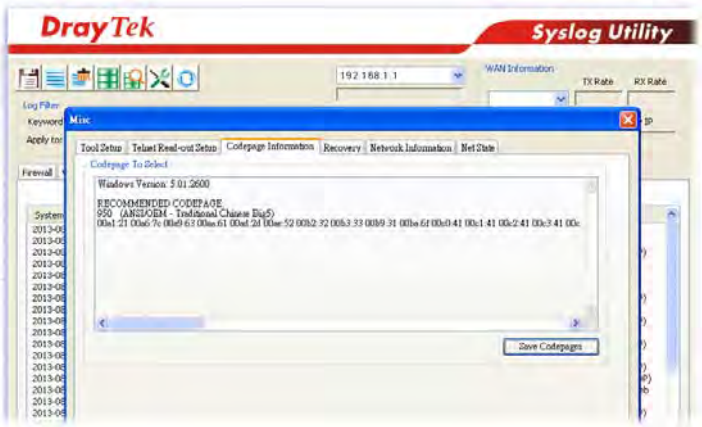
立刻封鎖(Block Immediately) - 系統封鎖符合規則之封包。

若無符合其於規則即通過(Pass If No Further Match) - 符合限定規則且並未符合其他規則之封包可立即通過。

若無符合其於規則即封鎖(Block If No Further Match) - 系統封鎖符合限定規則且並未符合其他規則之封包。

基於疑難排除的需要，您可指定記錄過濾器資訊，只要勾選

	Syslog 方框即可。
分至其他過濾器設定 (Branch to other Filter Set)	封包符合過濾器規則，下一個過濾器規則將分至指定之過濾器設定。請自下拉式選項中選擇下一個過濾器規則以便做分支動作，要注意路由器將會採用指定之過濾器規則，且絕對不會回到先前所設定之過濾器規則。
連線數控制(Sessions Control)	此處輸入的值爲全部的封包連線數，預設值爲 50000。
IP 與 MAC 綁定(MAC Bind IP)	**嚴格的(Strict)** – 讓 IP 物件中設定來源 IP 與目標 IP 中的 MAC 位址與 IP 位址設定完全綁定，並用於此過濾器規則。 **不嚴格的(No-Strict) -** 此指完全沒有限制。
服務品質(Quality of Service)	選擇一組 QoS 規則作爲防火牆規則，設定 QoS 細節資訊部分，請參考稍後的相關章節。 
使用者管理(User Managemen)t	本項目僅在**使用者管理>>基本設定(Management>>General Setup)**中選擇**規則模式**時可用，一般防火牆規則將套用在使用者/使用者群組/全部使用者上。  **注意:** 當沒有任何使用者設定檔或是使用者群組可供選擇時，系統會出現**建立新使用者(Create New User)**或是**建立新的群組(Create New Group)**選項供您建立新的設定檔。
應用程式管控(APP Enforcement)	選擇應用程式管控設定檔來封鎖 IM/P2P 之類的應用，如果沒有任何設定檔可供選擇時，請從下拉式清單中選擇**建立新設定**來建立一個新的設定檔。所有區域網路中的主機必須依循應用程式管控設定檔內的標準。有關詳細資訊，請參考**數位內容安全管理>>應用程式管控設定檔**章節。 因應疑難排解的需要，您可勾選 IM/P2P 紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 Syslog/郵件警告章節。
URL 內容過濾器(URL Content Filter)	選擇一個 **URL 內容過濾器**設定檔（在**數位內容安全管理(CSM)>> URL 內容過濾器**中所建立），請務必先在**數位內容安全管理(CSM)> URL 內容過濾器**中設定一個設定檔，或是從下拉式選單中選擇[建立新檔](**[Create New]**)產生新的設定檔。因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 Syslog/郵件警告章節。
網頁內容過濾器(Web Content Filter)	選擇一個**網頁內容過濾器**設定檔（在**數位內容安全管理(CSM)>> 網頁內容過濾器**中所建立），請務必先在**數位內容安全管理(CSM)>> 網頁內容過濾器**中設定一個設定檔，或是從

	下拉式選單中選擇[建立新檔](**[Create New])**產生新的設定檔。因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 Syslog/郵件警告章節。
DNS 過濾器(DNS Filter)	選擇一組 DNS 過濾器設定檔(於**數位內容安全管理>>DNS 過濾器**頁面中建立)，在**數位內容安全管理>>網頁內容過濾器設定檔**頁面中至少要先建立一個設定檔案以供選擇，或是從下拉式清單中選擇 DNS 過濾器連結以重新建立新的設定檔。
進階設定(Advance Setting)	按**編輯(Edit)**按鈕開啓下述視窗，不過，在此強烈建議您使用預設值爲佳。  **選擇編碼語系** - 此功能用來比較不同語言之間的字元數，選擇正確的 codepage 可以幫助系統從 URL 解碼資料後能取得正確的 ASCII 碼，並強化 URL 內容過濾器的正確性。預設值爲 ANSI 1252 Latin，如果您未選擇任何的 codepage，URL 解碼動作也不會執行，請自下拉式清單中選擇一個 codepage。 如果您不知道要如何選擇適宜的**編碼語系**，請開啓 Syslog。從 Setup 對話盒中的**編碼語系**(codepage)資訊，您將會看到系統建議的 codepage 內容。  **視窗大小(Window size)** – 決定 TCP 協定的大小(0~65535)，數值越大，成效越佳，不過網路會較爲不穩定，小的數值比較適合穩定網路。 **連線數逾時(Session timeout)** – 設定連線數逾時時間可讓網路資源獲得較佳的運用，但是連續暫停僅適用於 TCP 協定，連線數逾時主要是針對符合防火強規則的資料流量而設定。 **DrayTek 橫幅(DrayTek Banner)** – 請勿勾選此方框，下述畫面就不會出現在無法取用的網頁上，預設值是勾選的。

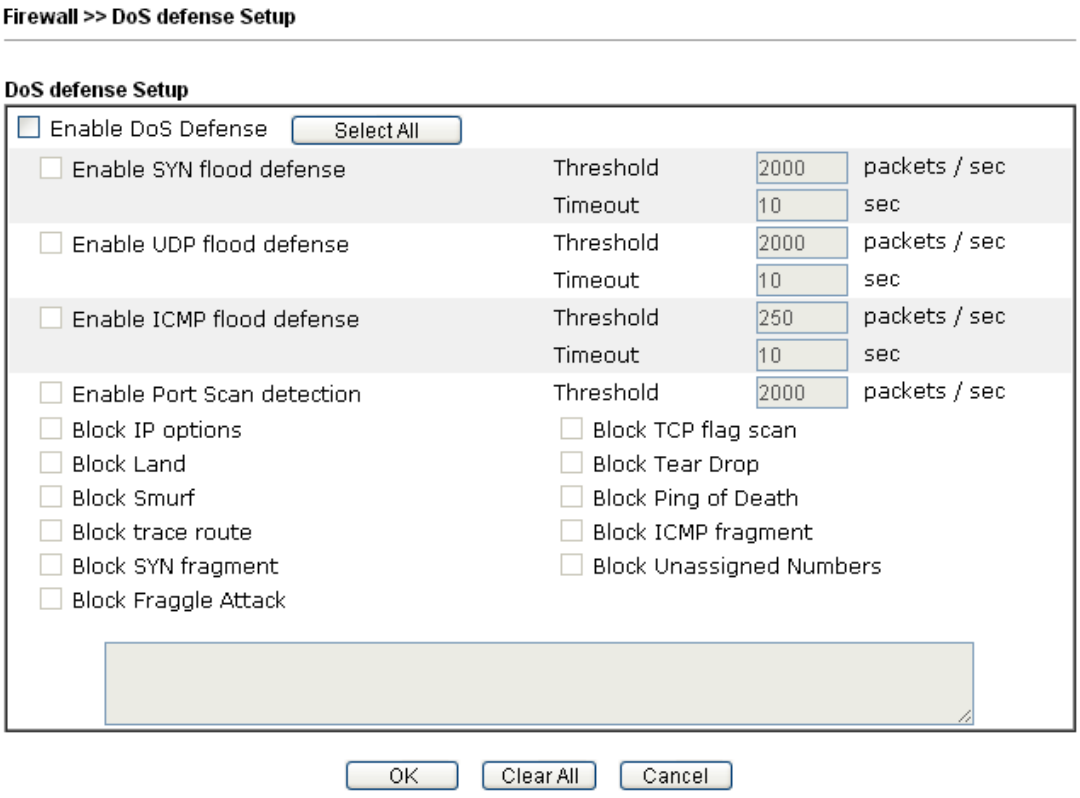
	 **嚴格安全檢測(Strict Security Checking)** - 爲安全起見，您可能會想讓路由器針對資料傳輸進行較爲嚴格的安全性檢測，不過您若進行此項檢測有可能對路由器的成效造成一定的影響。

3. 當您完成上述設定之後，請按**確定(OK)**按鈕儲存並離開頁面。

VI-1-3 DoS 攻擊防禦功能設定(DoS Defense)

這是 **IP 過濾程式/防火牆**的次功能選項，有 15 種檢測/防禦功能類型，DoS 攻擊防禦功能的預設值是關閉的。

按**防火牆(Firewall)**並選擇 **DoS 攻擊防禦功能(DoS Defense)**開啓設定網頁。

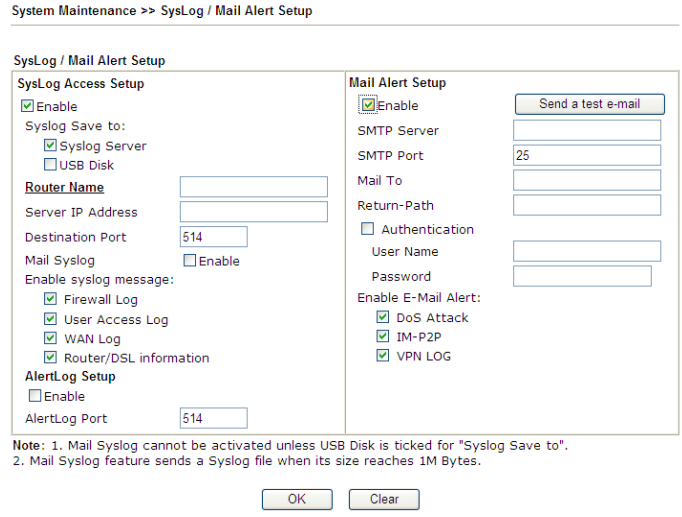


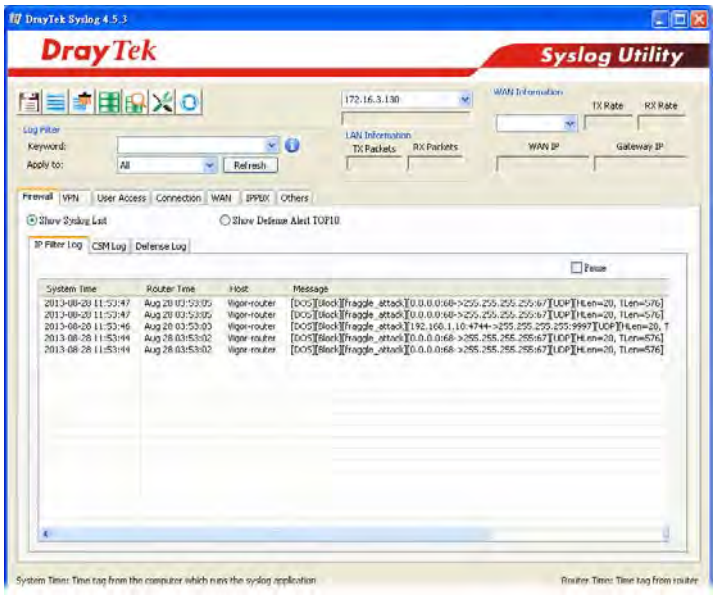
可用設定說明如下：

項目	說明
啓用 Dos Defense (Enable Dos Defense)	勾選此項以啓動 DoS 攻擊防禦功能。
選擇全部(Select All)	按下此鈕選擇下列全部項目。
啓用 SYN flood 攻擊防禦功能(Enable SYN flood defense)	勾選此項以啓動 SYN 攻擊防禦功能，一旦檢查到 TCP SYN 封包的臨界值超過定義數值，Vigor 路由器在所設定之逾時期間即開始捨棄其後之 TCP SYN 封包，這項功能的目的是防止 TCP SYN 封包嚐試耗盡路由器有限的資源。臨界值和逾時的預設值分別爲每秒 2000 個封包和 10 秒。
啓用 UDP flood 攻擊防禦功能(Enable UDP flood defense)	勾選此項以啓動 UDP 攻擊防禦功能， 一旦檢查到 UDP 封包臨界值超過定義數值，Vigor 路由器在所設定之逾時期間即開始捨棄其後之 UDP 封包。臨界值和逾時的預設值分別爲每秒 2000 個封包和 10 秒。 **注意**：勾選此項之後，若有大量流量進出，機制啓動時，設備會無法上網，但內網仍可順利連到管理介面。
攻擊防禦功能(Enable ICMP flood defense)	勾選此項以啓動 ICMP Fragment 封包，與 UDP 攻擊防禦功能相同的是，一旦檢查到 ICMP 封包臨界值超過定義數值，路由器便會於所設定之逾時期間，不再回應來自網際網路的 ICMP

	需求。臨界值和逾時的預設值分別爲每秒 250 個封包和 10 秒。
啓用防禦通訊埠掃瞄偵測功能(Enable Port Scan detection)	通訊埠掃瞄藉由傳送大量封包到數個通訊埠，以嘗試找出未知服務所回應之內容來攻擊 Vigor 路由器。勾選此方塊啓動通訊埠掃瞄檢測功能，當利用通訊埠掃瞄臨界值速率而檢測出惡意探測之行爲時，Vigor 路由器將傳送警告訊息出去。臨界值的預設值爲每秒 2000 個封包。
封鎖 IP 選項(Block IP options)	勾選此項以啓動阻攔 IP options 功能，Vigor 路由器將會忽略資料封包頭中(含 IP 選項區)的 IP 封包。限制的原因是 IP option 的出現是區域網路安全性中的弱點，因爲它攜帶令人注意的資訊像是安全性、TCC (封閉使用者群組)參數、網際網路位址、路由訊息等等，讓外部的竊聽者有機會取得您虛擬網路的細節內容。
封鎖 Land 攻擊(Block Land)	勾選此項以強迫 Vigor 路由器防護 Land 攻擊，Land 攻擊結合含 IP spoofing 的 SYN 攻擊技術，當駭客傳送 spoofed SYN 封包(連同相同來源和目的位元址)，以及通訊埠號至受害一方時，Land 攻擊即由此發生。
封鎖 Smurf 攻擊(Block Smurf)	勾選此項以啓動封鎖 Smurf 攻擊功能，Vigor 路由器將忽略任何一次的播送 ICMP 回應需求。
封鎖路由追蹤(Block trace route)	勾選此項以強迫 Vigor 路由器不轉送任何路由封包的行蹤。
封鎖 SYN Fragment 封包 (Block SYN fragment)	勾選此項以啓動封鎖 SYN Fragment 的封包功能。Vigor 路由器將會停止任何具有 SYN 旗標及更多的區段設定之封包傳送作業。
封鎖 Fraggle 攻擊(Block Fraggle Attack)	勾選此項以啓動封鎖 Fraggle 攻擊功能，任何播送來自網際網路的 UDP 封包都會被封鎖起來。 啓動 DoS/DDoS 防禦功能可能會阻擋一些合法的封包，例如當您啓動 fraggle 攻擊防禦時，所有來自網際網路的 UDP 封包播送都會被阻擋在外，因此得自網際網路的 RIP 封包全都會被阻擋掉。
封鎖 TCP Flags scan (Block TCP flag scan)	勾選此項以啓動阻攔 TCP Flags 掃描功能，任何具有異常 TCP 封包的設定都會被捨棄掉，這些掃描行動包含有 *no flag scan*, *FIN without ACK scan*, *SYN FINscan*, *Xmas scan* 以及 *full Xmas scan* 等等。
封鎖 Tear Drop 攻擊(Block Tear Drop)	勾選此項以啓動封鎖 Tear Drop 攻擊功能，很多機器在接收到超過最大值得 ICMP 資料段(封包)時，系統就會當機。爲了避免這類型的攻擊行爲，Vigor 路由器便被設計成具有捨棄片段 ICMP (超過 1024 位元組)封包的能力。
封鎖 Ping of Death 攻擊 (Block Ping of Death)	勾選此項以啓動封鎖 Ping of Death 攻擊功能，這項攻擊意味著犯罪者傳送重疊封包至目的主機，這些目的主機一旦重新建構封包時就會造成當機現象，Vigor 路由器將會阻擋此種攻擊活動的封包進入。
封鎖 ICMP 封包片段攻擊 (Block ICMP Fragment)	勾選此項以啓動封鎖 ICMP 封包片段功能，任何含有多個片段的 ICMP 封包都會被捨棄阻擋。
封鎖不明封包協定封包 (Block Unassigned Numbers)	勾選此項以啓動封鎖不明封包協定封包功能，個別 IP 封包在資料段封包頭中都擁有一個協定區域，指名該協定於上層運作的類型。
警告訊息(Warning	我們提供使用者系統記錄功能以便檢視路由器發出的訊息。作

Messages)	爲系統紀錄伺服器，使用者可接收來自路由器(系統紀錄用戶端)傳送之報告。 所有與 DoS 攻擊有關的警告訊息都將傳送與使用者，使用者可以重新檢查其內容，在訊息中尋找關鍵字，所遭受的任何攻擊之名稱即可立即檢測出來。



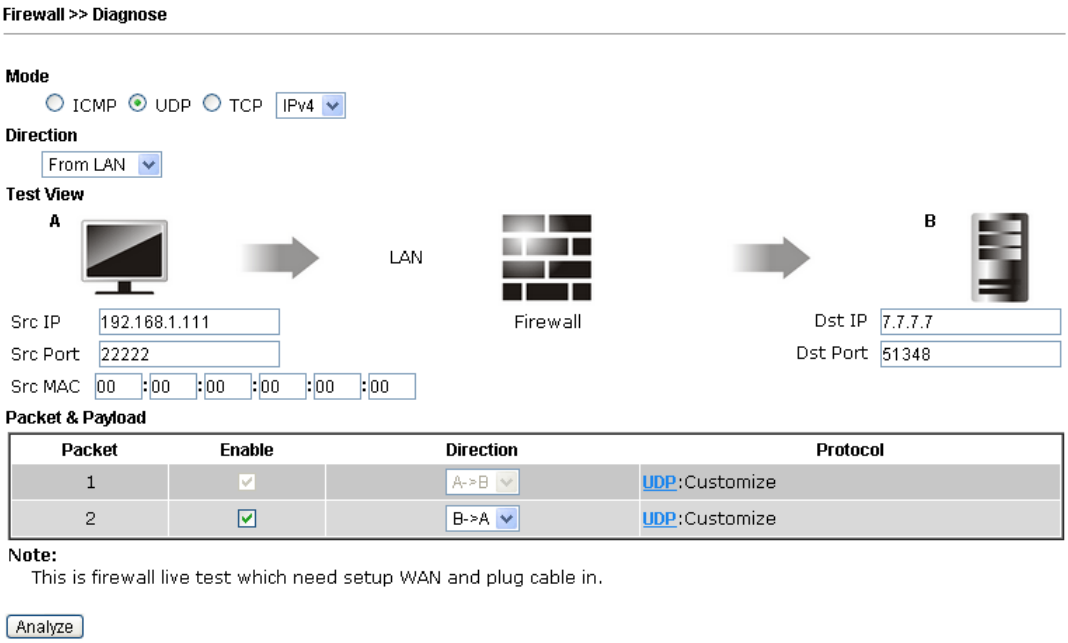


在您完成上述的設定之後，請按**確定(OK)**按鈕來儲存設定。

VI-1-4 診斷(Diagnose)

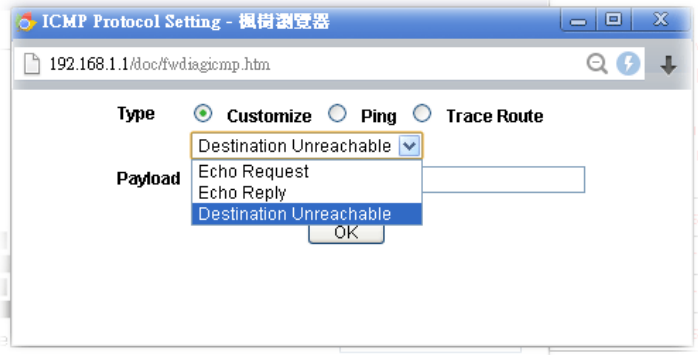
診斷的目的是爲了測試當路由器接收封包，套用的是哪條防火牆規則。測試的結果包含防火牆規則設定檔、封包傳輸時的 IP 位址轉換、防火牆功能狀態等等，同時也會顯示在此頁面上。

資訊	使用診斷工具的測試結果可作爲研發人員除錯之用，依照實際網路連線設定之不同，結果也會不同。



可用設定說明如下：

項目	說明
模式(Mode)	欲執行防火牆測試，請指定服務類型(如 ICMP、UDP、TCP)然後輸入 IP 位址(IPv4/IPv6)。
方向(Direction)	設定路由器接收第一個封包的方向來源以進行測試(來自 WAN 或來自 LAN)。
測試檢視(Test View)	這是動態顯示頁面。 依照指定的方向，測試顯示畫面會呈現圖表引導您輸入 IP 位置、埠號與 MAC 位址。 之後，按下分析按鈕，防火牆規則設定檔的資訊與位址轉換資訊就會呈現在頁面上。
來源 IP(Src IP)	輸入封包來源的 IPv4/IPv6 位址。
來源埠號(Src Port)	輸入封包來源的埠號。
來源 MAC(Src MAC)	輸入封包來源的 MAC 位址。
目的 IP(Dst IP)	輸入封包目的的 IPv4/IPv6 位址。
目的埠號(Dst Port)	輸入封包目的的埠號。
封包與有效承載(Packet & Payload)	在防火牆的診斷中，二個封包屬於一次連線。一般來說，路由器只需要二個封包就可以進行這項測試了。 **啓用(Enable)** – 勾選此框以傳送測試封包。 **方向(Direction)** – 防火牆測試中第一個封包會依循上述指定的方向送出，然而第二個封包的方向有可能不同。請在此選擇第二個封包的傳送方向(自電腦 A 至 B 或是自電腦 B 至 A)。 **通訊協定(Protocol)** – 顯示選擇的模式與狀態，如要必要，可按模式連結設定進階內容。.

	 ● **類型(Type)** – 可選 Customize, Ping 以及 Trace Route。 ● **有效承載(Payload)** – 選擇 Customzie 爲類型時可以在設定此項。請輸入代表特定封包(如 DNS 封包)之 16 進位的字元數字 16 個即可。
分析(Analyze)	執行測試並分析結果。

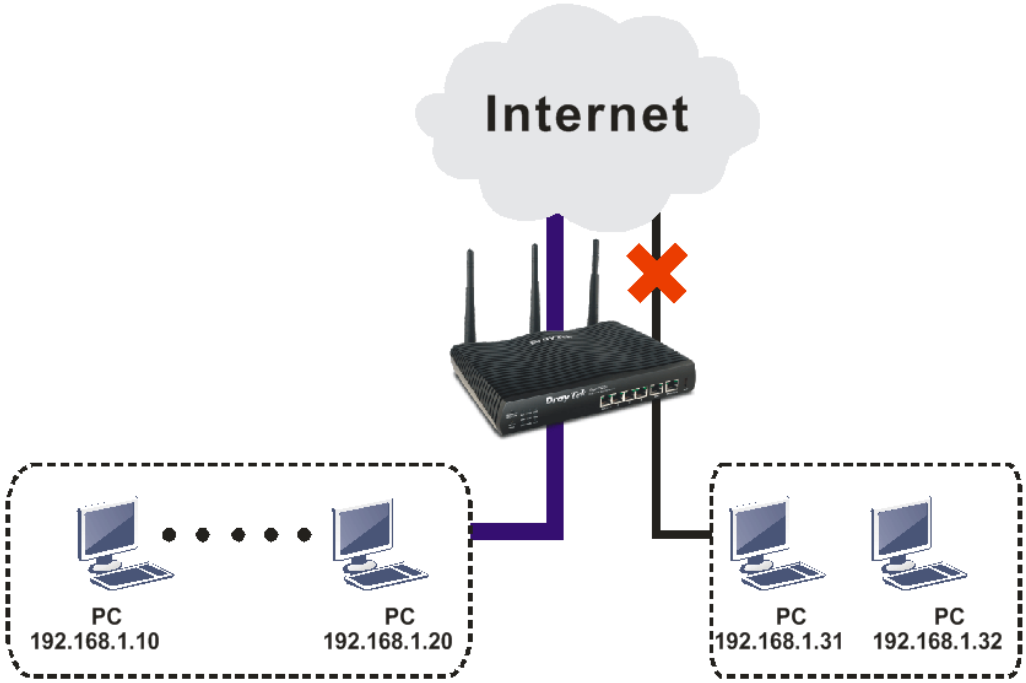
下圖顯示按下**分析(Analyze)**按鈕之後的測試結果，與防火牆有關的功能(如 MAC 過濾器、QoS、使用者管理等等)之狀態也會以綠燈或紅燈呈現在網頁上。



應用說明

A-1 如何限定特定電腦存取網際網路

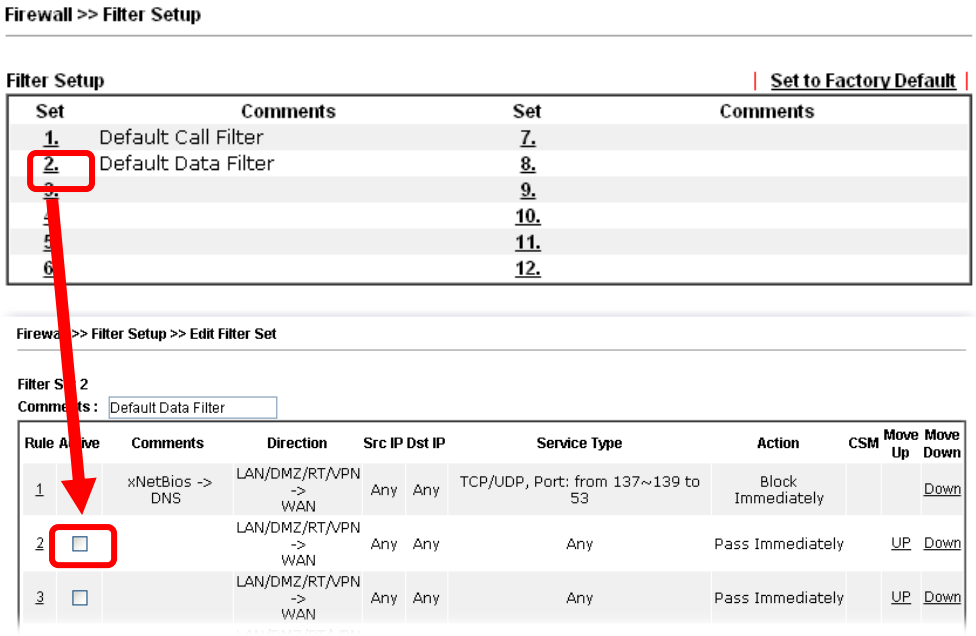
我們可以指定某些電腦(例如 192.168.1.10 ~ 192.168.1.20)透過 Vigor 路由器登入網際網路，其他的電腦(例如 192.168.1.31 與 192.168.1.32)只能存取區域網路內的資訊。



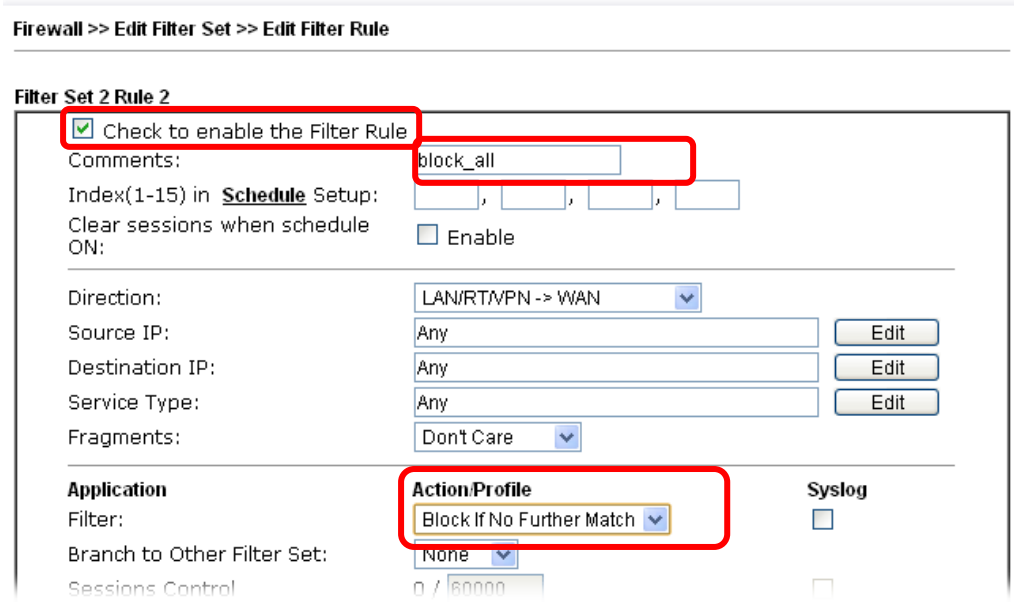
The way we can use is to set two rules under **Firewall**. For **Rule 1** of **Set 2** under **Firewall>>Filter Setup** is used as the default setting, we have to create a new rule starting from Filter Rule 2 of Set 2.

使用的方法是透過防火牆設定二條規則，在**防火牆>>過濾器設定(Firewall>>Filter Setup)**下的規則 1 設定 2 被用來當成預設值設定，我們必須從規則 2 中的設定 2 另外建立新的規則。

1. 登入路由器的網頁設定介面。
2. 開啓**防火牆>>過濾器設定(Firewall>>Filter Setup)**，按下**組別 2** 連結。



3. 勾選**啓用過濾規則(Check to enable the Filter Rule)**，輸入註解內容(例如 **block_all**)，選擇**若無符合其餘規則即封鎖(Block If No Further Match)**作爲過濾器規則，然後按下**確定**。

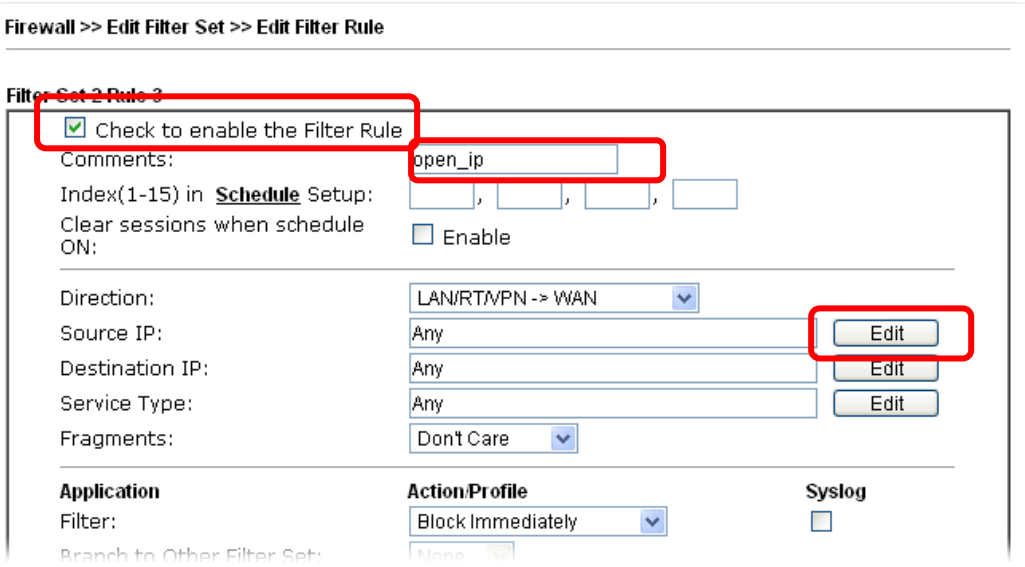


資訊

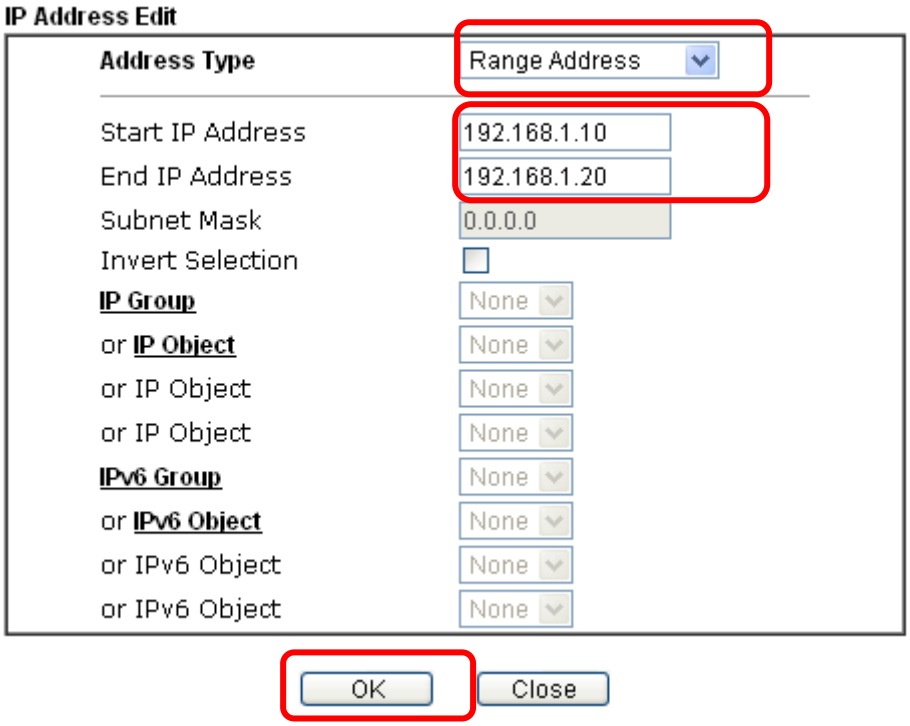
在預設狀態下，路由器檢查封包的順序會以組別 2，過濾器規則 2 開始依序檢查到規則 7，如果您在此選擇了**若無符合其餘規則即封鎖**作爲過濾器規則，路由器的防火牆檢查封包時將會從規則 3 開始直到規則 7，封包不符合規則就會依照規則 2 的規定來處理。

4. 接著，設定另一條規則，同樣開啓**防火牆>>過濾器設定(Firewall>>Filter Setup)**，按下**組別 2** 連結並選擇**過濾器規則 3(Filter Rule 3)**的按鈕。

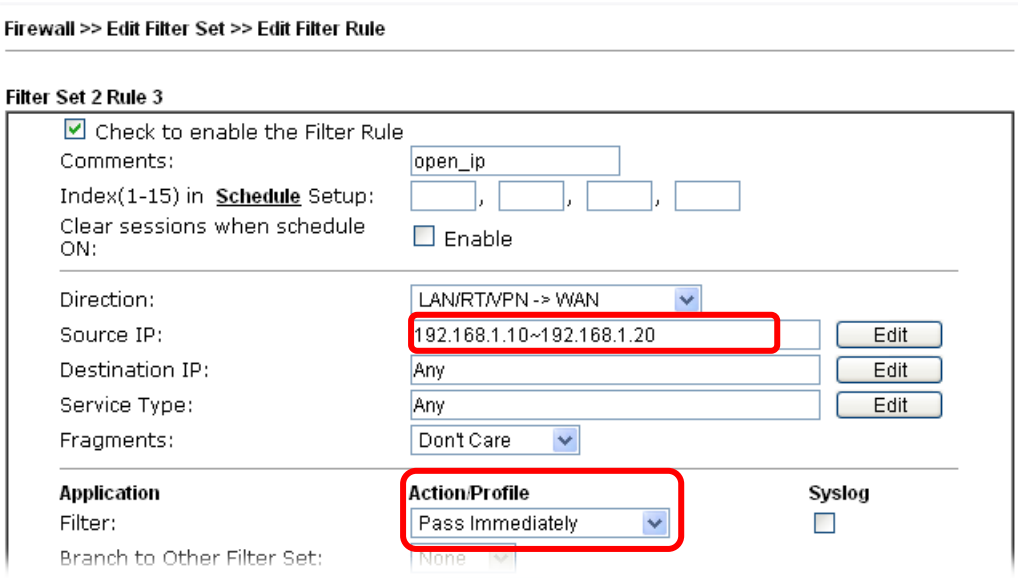
5. 勾選**啓用過濾規則(Check to enable the Filter Rule)**，輸入註解內容(例如 **open_ip**)，按下**來源 IP(Source IP)**的**編輯**按鈕。



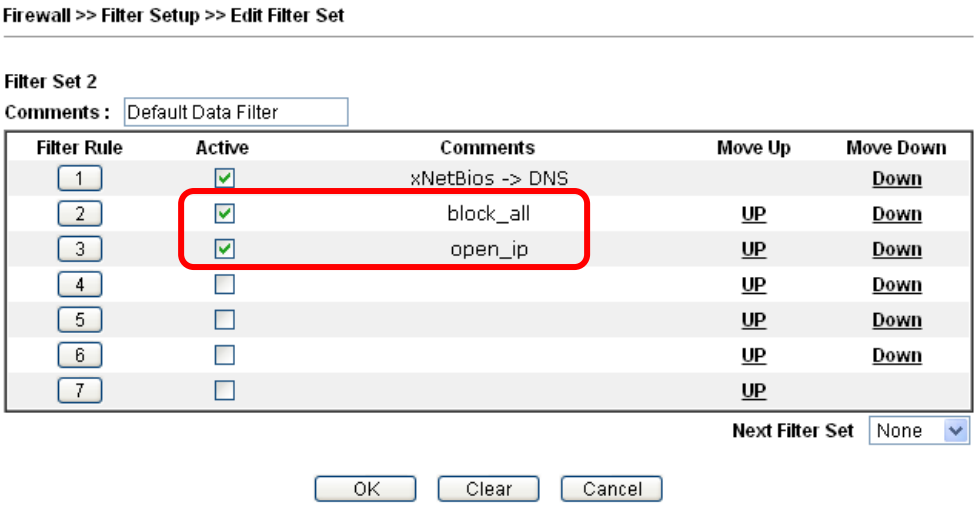
6. 如下的對話盒將會跳出，請選擇**位址範圍(Range Address)**爲**位址形式(Address Type)**。在起始 IP 位址區域輸入 192.168.1.10，結束 IP 位址區域輸入 92.168.1.20，接著按下**確定(OK)**按鈕儲存。位於此範圍中的電腦都能登入網際網路。



7. 現在，檢查**來源 IP(Source IP)**的內容是否正確，過濾器的動作/設定爲**立刻通過(Pass Immediatel)**，接著按**確定(OK)**儲存。



8. 二個過濾器規則皆已設定完成，請再次按下**確定(OK)**按鈕。



所有設定皆已完備，只要位在 192.168.1.10 ~ 192.168.1.20 之間的位址的電腦都可以透過路由器存取網際網路。

VI-2 數位內容安全管理(CSM)

數位內容安全管理(CSM, Content Security Management)主要是用來控制即時通訊、點對點應用、過濾網頁內容以及過濾 URL 內容，以便達成安全管理的效果。

應用程式管控設定檔

由於即時通訊應用程式蓬勃的發展，人與人間的通訊變得越來越容易。然而一些企業利用此種程式作爲與客戶通訊的有力工具時，部分公司對此可能還是抱持保留態度，這是因爲他們想要減少員工在上班時間誤用此程式或是防止未知的安全漏洞發生。對於準備應用點對點程式的公司來說，情況也是相同的，因爲檔案分享可以很方便但是同時也很危險。爲了應付這些需求，我們提供了 CSM 阻擋功能。

URL 內容過濾器

爲了提供一個適當的網路空間給予使用者，Vigor 路由器配有 URL 內容過濾器，可限制一些不合法的資料於網站上進出，同時也禁止隱藏惡意碼的網路特徵於路由器內出入。

一旦使用者輸入關鍵字連結，URL 關鍵字阻擋工具將會拒絕該網頁之 HTTP 需求，如此一來使用者即無法存取該網站。您可以這樣想像一下，URL 內容過濾器爲一個訓練有素的便利商店櫃員，絕對不販售成人雜誌給予未成年的小孩子。在辦公室內，URL 內容過濾器也可以提供與工作相關的環境，由此來增加員工的工作效率。URL 內容過濾器爲什麼可以比傳統防火牆在過濾方面提供更好的服務呢？那是因爲它能夠檢查 URL 字串或是一些隱藏在 TCP 封包負載的 HTTP 資料，而一般防火牆僅能以 TCP/IP 封包標頭來檢測封包。

換言之，Vigor 路由器可以防止使用者意外自網頁下載惡意的程式碼。惡意碼隱藏在執行物件當中是一件很普遍的事情，像是 ActiveX、Java Applet、壓縮檔和其他執行檔案。一旦用戶下載這些類型的檔案，用戶便會有這些可能爲系統帶來威脅的風險，例如一個 ActiveX 控制物件通常用於提供網頁人機通信交換功能，萬一裡面隱藏惡意的程式碼的話，該程式碼就可能會佔據使用者的系統。

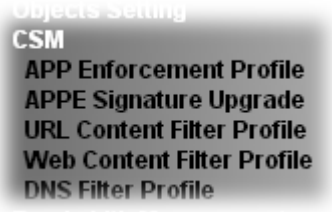
網頁內容過濾器

我們都知道網際網路上的內容，有時候可能並不太合宜，作爲一個負責任的父母或是雇主，您應該保護那些您信賴的人免受危險的侵擾。藉由 Vigor 路由器的網頁過濾服務，您可以保護您的商業機密不受一般常見威脅；對於父母來說，您可以保護您的孩童不致誤闖成人網站或是成人聊天室。

一旦您啓動了網頁內容過濾服務，也選擇一些您想要限制存取的網站目錄，每個 URL 位址需求(例 www.bbc.co.uk) 將在由 SurfControl 所運作的伺服器資料庫中先接受檢測。資料庫涵蓋 70 種語言和 200 個國家，超過 1 億個網頁，區分成 40 種容易瞭解的目錄。此資料庫每一天都由網際網路的國際研究團隊不斷更新，伺服器將查閱 URL 然後傳回其類別給路由器，您的 Vigor 路由器即可按照您所選擇的分類項目來決定是否允許用戶存取該網站，因爲每一個多路負載平衡資料庫伺服器一次可以管理數百萬的分類需求。

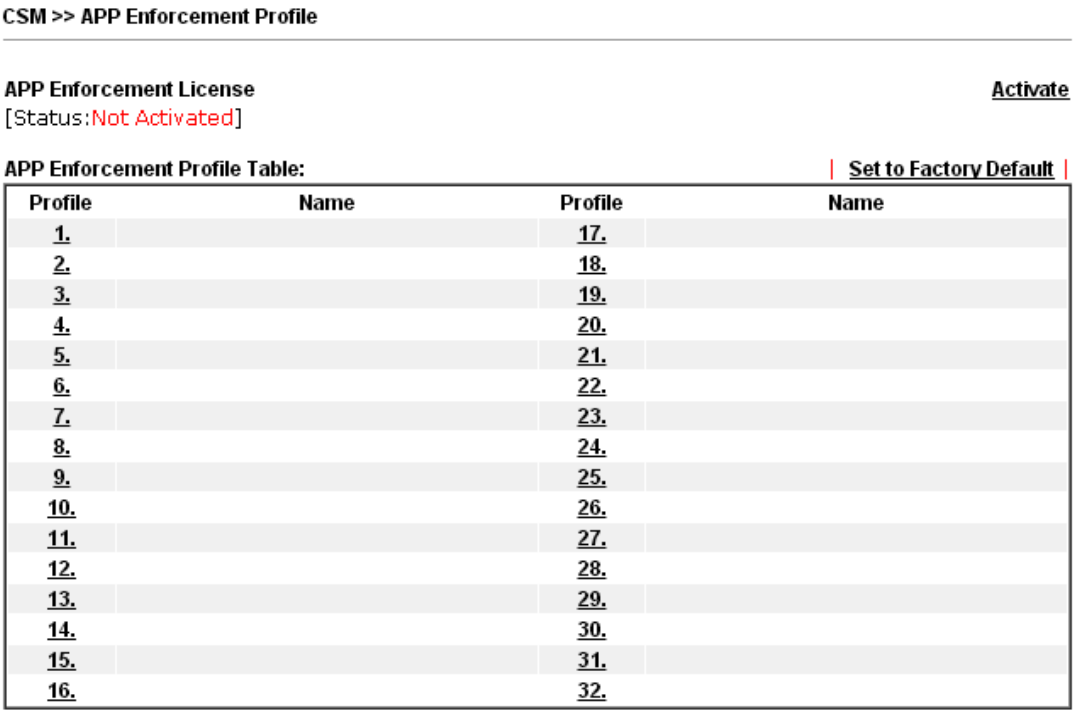
資訊 URL 內容過濾器的優先權高於網頁內容過濾器。

網頁使用者介面



VI-2-1 應用程式管控設定檔(APP Enforcement Profile)

您可針對即時通訊/點對點/通訊協定/其他應用定義不同的策略檔案，以通訊及應用之需要，此處所建立的設定檔可以運用在**防火牆>>基本設定(Firewall>>General Setup)**的**預設規則(Default Rule)**中，做爲主機依循的標準。

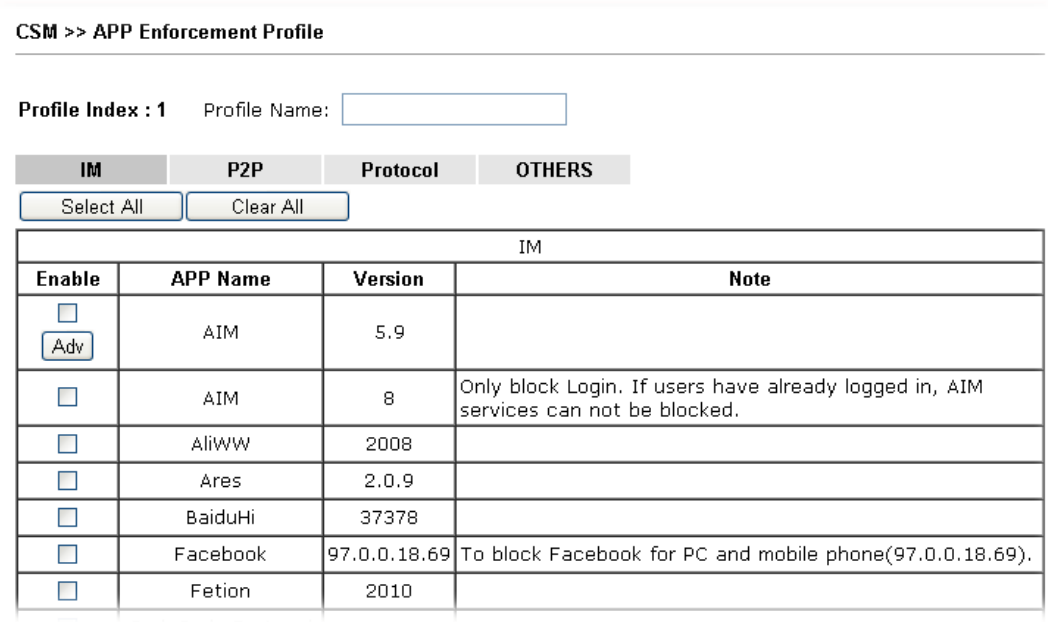


可用設定說明如下：

Item	Description
回復出廠預設值(Set to Factory Default)	清除全部的設定資料。
設定檔(Profile)	顯示索引編號連結讓您點選進入設定頁面。
名稱(Name)	顯示應用程式管控的設定檔名稱。

按索引下方的號碼連結開啓如下視窗進行細節設定。

頁面中呈現四種不同的標籤，IM、P2P、協定與其他。下圖顯示協定標籤下的設定內容與支援的版本內容，您可核取方框選擇該項目阻擋用戶使用：

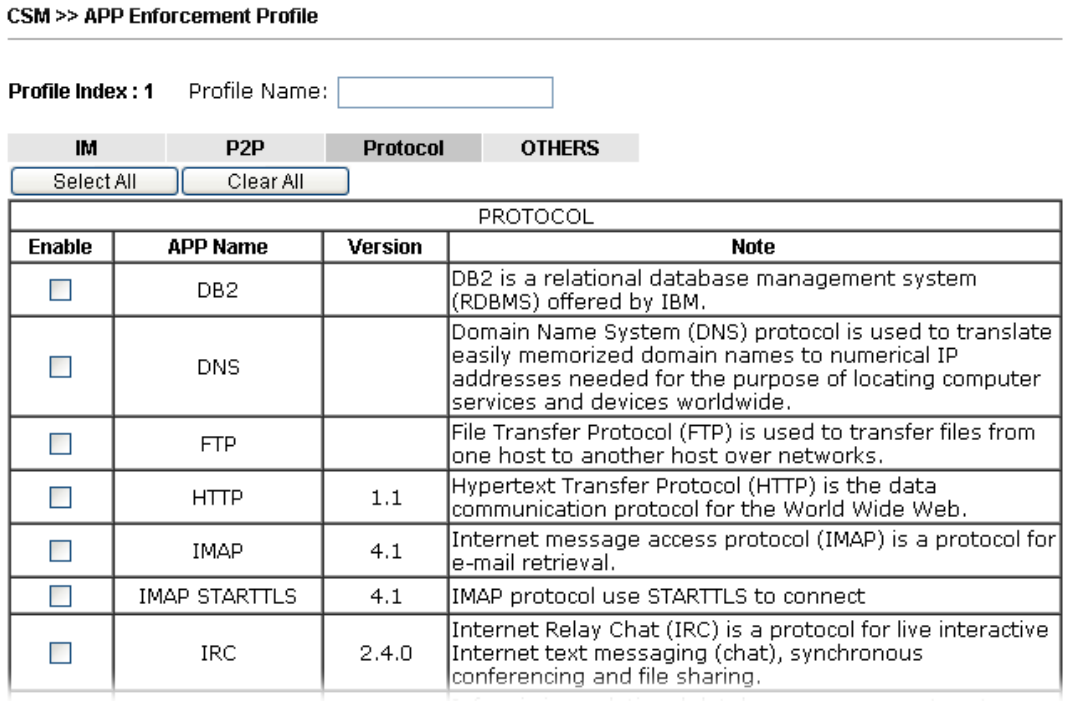


可用設定說明如下：

項目	說明
設定檔名稱(Profile Name)	請輸入此設定檔名稱。
選擇全部(Select All)	按此選擇本頁中全部的設定項目。
清除全部(Clear All)	按此捨棄選擇的項目。
啓用(Enable)	勾選此方框讓路由器封鎖選定的 APP。
進階(Adv)	用以開啓跳出視窗以指定 APP 的活動內容(如訊息、檔案傳輸、遊戲、會議)。

此處設定的設定檔之後可以套用至**防火牆>>基本設定(Firewall>>General Setup)** 以及 **防火牆>>過濾器規則(Firewall>>Filter Setup)** 頁面，做爲主機可以依循的標準。

下圖顯示**協定(Protocol)**類型中的各個項目：



CSM >> APP Enforcement Profile

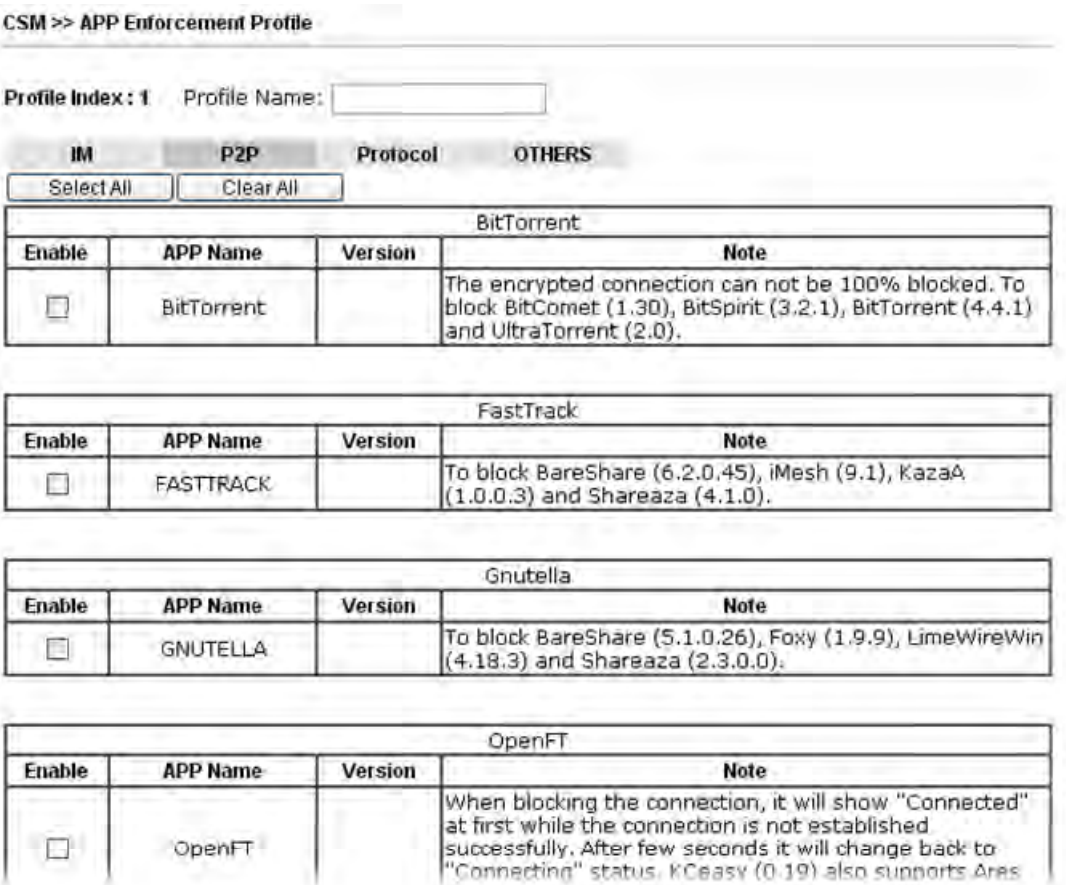
Profile Index : 1 Profile Name:

IM | P2P | Protocol | OTHERS

Select All | Clear All

PROTOCOL			
Enable	APP Name	Version	Note
☐	DB2		DB2 is a relational database management system (RDBMS) offered by IBM.
☐	DNS		Domain Name System (DNS) protocol is used to translate easily memorized domain names to numerical IP addresses needed for the purpose of locating computer services and devices worldwide.
☐	FTP		File Transfer Protocol (FTP) is used to transfer files from one host to another host over networks.
☐	HTTP	1.1	Hypertext Transfer Protocol (HTTP) is the data communication protocol for the World Wide Web.
☐	IMAP	4.1	Internet message access protocol (IMAP) is a protocol for e-mail retrieval.
☐	IMAP STARTTLS	4.1	IMAP protocol use STARTTLS to connect
☐	IRC	2.4.0	Internet Relay Chat (IRC) is a protocol for live interactive Internet text messaging (chat), synchronous conferencing and file sharing.

下圖顯示 **P2P** 類型中的各個項目：



CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM | P2P | Protocol | OTHERS

Select All | Clear All

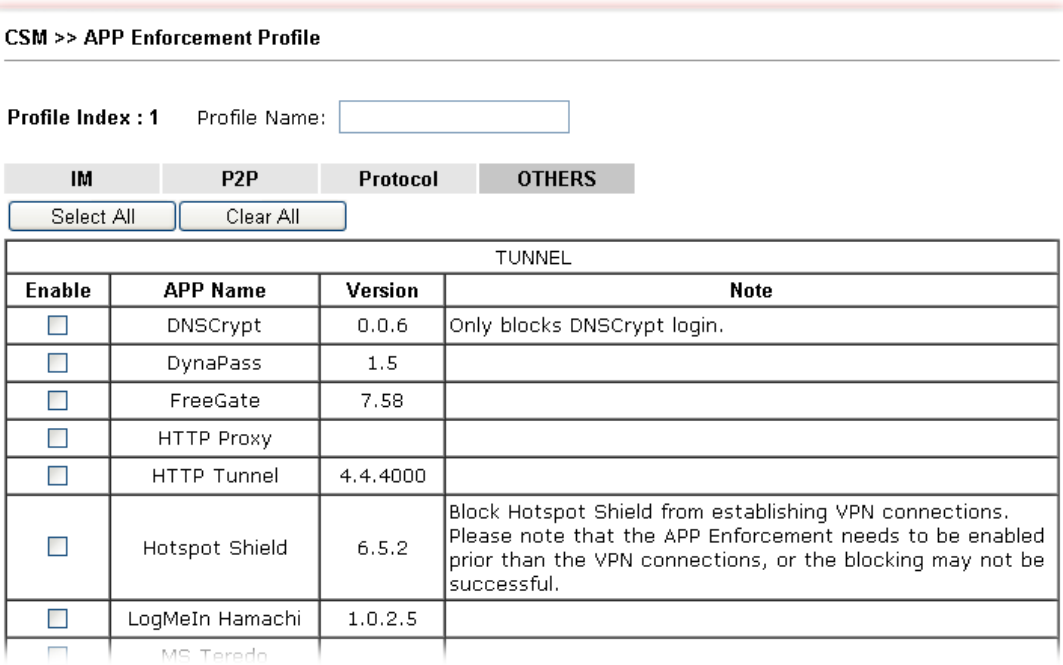
BitTorrent			
Enable	APP Name	Version	Note
☐	BitTorrent		The encrypted connection can not be 100% blocked. To block BitComet (1.30), BitSpirit (3.2.1), BitTorrent (4.4.1) and UltraTorrent (2.0).

FastTrack			
Enable	APP Name	Version	Note
☐	FASTTRACK		To block BareShare (6.2.0.45), iMesh (9.1), KazaA (1.0.0.3) and Shareaza (4.1.0).

Gnutella			
Enable	APP Name	Version	Note
☐	GNUTELLA		To block BareShare (5.1.0.26), Foxy (1.9.9), LimeWireWin (4.18.3) and Shareaza (2.3.0.0).

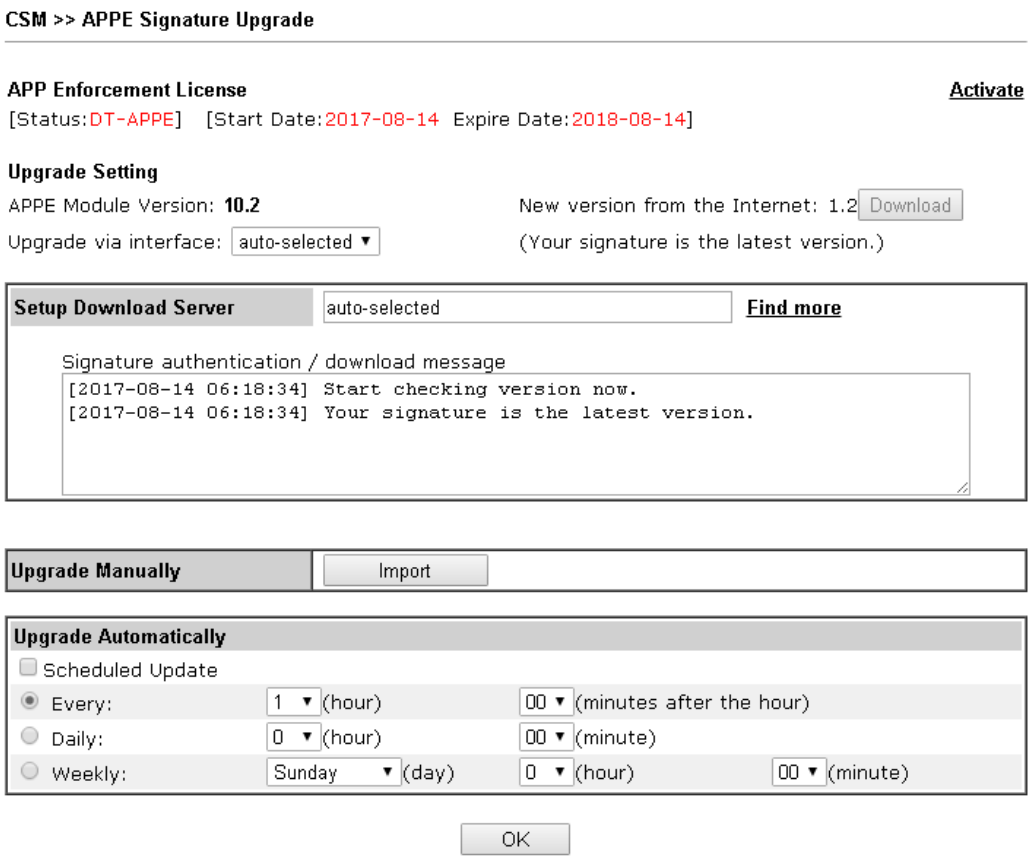
OpenFT			
Enable	APP Name	Version	Note
☐	OpenFT		When blocking the connection, it will show "Connected" at first while the connection is not established successfully. After few seconds it will change back to "Connecting" status. KCeasy (0.19) also supports Ares

下圖顯示**其他(OTHERS)**類型中的各個項目：



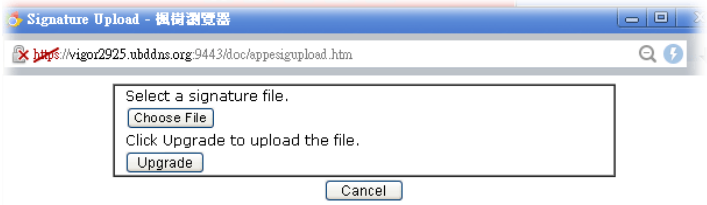
VI-2-2 APPE 特徵碼更新(APPE Signature Upgrade)

路由器採用的 APP 物件設定檔被視爲 APP 特徵碼。居易將定期更新所支援的特徵碼的版本資訊。然而，若由使用者一個接一個來更新 APP 特徵碼，顯得有些不便，本功能乃特別設計用於提供快速執行 APP 版本資訊更新事宜，使用者可手動執行 APP 特徵碼更新或是設定本頁內容讓 Vigor 路由器自動執行 APP 特徵碼更新。



可用設定說明如下：

項目	說明
更新設定(Upgrade Setting)	**APPE 模組版本(APPE Module Version)** – 顯示 APP 特徵碼目前的版本。 **自網際網路取得之新版本(New version from the Internet)**–**下載(Download)**按鈕僅在 Vigor 路由器偵測出新的 APPE 版本之後才會有作用，按下該按鈕之後，畫面將會出現含有新版資訊的對話盒，按下**確定(OK)**按鈕離開該對話盒並開始更新特徵碼。 **透過介面更新(Upgrade via interface)** – 選擇一個 WAN 介面作爲 APP 特徵碼更新的通道。
設定下載伺服器(Setup Download Server)	輸入下載伺服器所在的 URL 以便進行下載作業，您也可以按更多連結來搜尋需要的下載伺服器。 **特徵碼驗證/下載訊息(Signature authentication/download message)**–顯示 APPE 特徵碼更新時的狀態。
手動更新(Upgrade Manually)	**輸入(Import)** – 按下此鈕開啓如下頁面，按**選擇檔案**尋找先前自居易官網下載取得之特徵碼檔案，然後再按**更新(Upgrade)**

	按鈕，等待系統完成更新作業。 
自動更新(Upgrade Automatically)	**排程更新(Scheduled Update) -** 勾選此框讓路由器能在指定的時間內進行 APPE 特徵碼更新。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

VI-2-3 URL 內容過濾器設定檔(URL Content Filter Profile)

爲了提供一個適當的網路空間給予使用者，Vigor 路由器配有 URL 內容過濾器，可限制一些不合法的資料於網站上進出，同時也禁止隱藏惡意碼的網路特徵於路由器內出入。

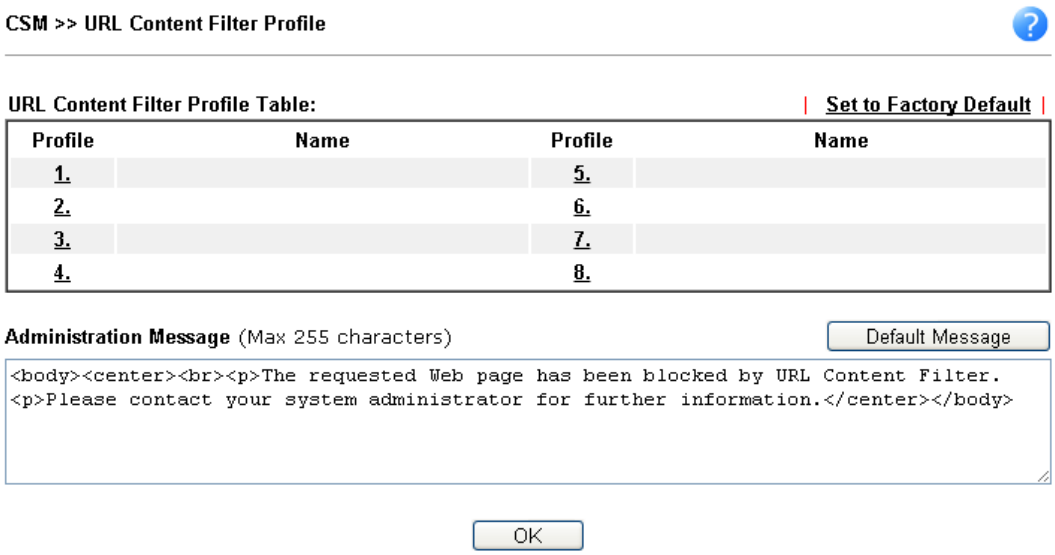
一旦使用者輸入關鍵字連結，URL 關鍵字阻擋工具將會拒絕該網頁之 HTTP 需求，如此一來使用者即無法存取該網站。您可以這樣想像一下，URL 內容過濾器爲一個訓練有素的便利商店櫃員，絕對不販售成人雜誌給予未成年的小孩子。在辦公室內，URL 內容過濾器也可以提供與工作相關的環境，由此來增加員工的工作效率。URL 內容過濾器爲什麼可以比傳統防火牆在過濾方面提供更好的服務呢？那是因爲它能夠檢查 URL 字串或是一些隱藏在 TCP 封包負載的 HTTP 資料，而一般防火牆僅能以 TCP/IP 封包標頭來檢測封包。

換言之，Vigor 路由器可以防止使用者意外自網頁下載惡意的程式碼。惡意碼隱藏在執行物件當中是一件很普遍的事情，像是 ActiveX、Java Applet、壓縮檔和其他執行檔案。一旦用戶下載這些類型的檔案，用戶便會有這些可能爲系統帶來威脅的風險，例如一個 ActiveX 控制物件通常用於提供網頁人機通信交換功能，萬一裡面隱藏惡意的程式碼的話，該程式碼就可能會佔據使用者的系統。

例如，假設您新增關鍵字是“sex(性)” ，路由器即會限制進入某些網頁或是網站存取的功能，比方 www.sex.com、www.backdoor.net/images/sex/p_386.html，或者您也可以指定 URL 全名或部分的名稱如 www.sex.com 或是 sex.com 來加以限制。

此外，Vigor 路由器也會捨棄任何嘗試取回這些惡意程式碼的需求。

請至**數位內容安全管理(CSM)>> URL 內容過濾器設定檔(URL Content Filter Profile)**，下圖將會出現在螢幕上。

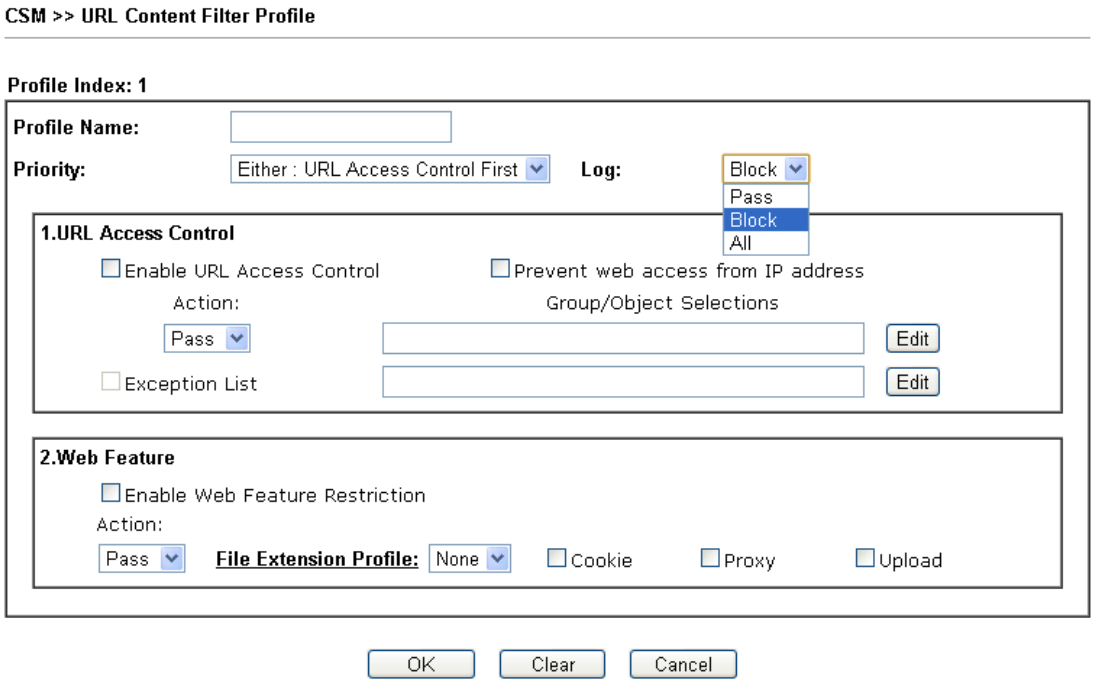


可用設定說明如下：

項目	說明
回復出廠預設值(Set to Factory Default)	清除全部的設定資料。
Profile	顯示索引編號連結讓您點選進入設定頁面。
Name	顯示設定檔名稱。

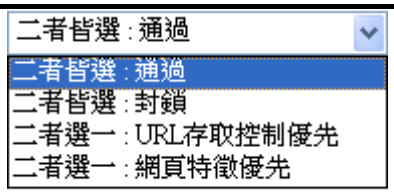
管理訊息(Administration Message)	您可以視您的需要輸入所需的訊息。 **預設訊息內容(Default Message)** - 您可以手動輸入訊息或是按下此按鈕取得預設的訊息，並顯示在**管理訊息(Administration Message)**方框內。

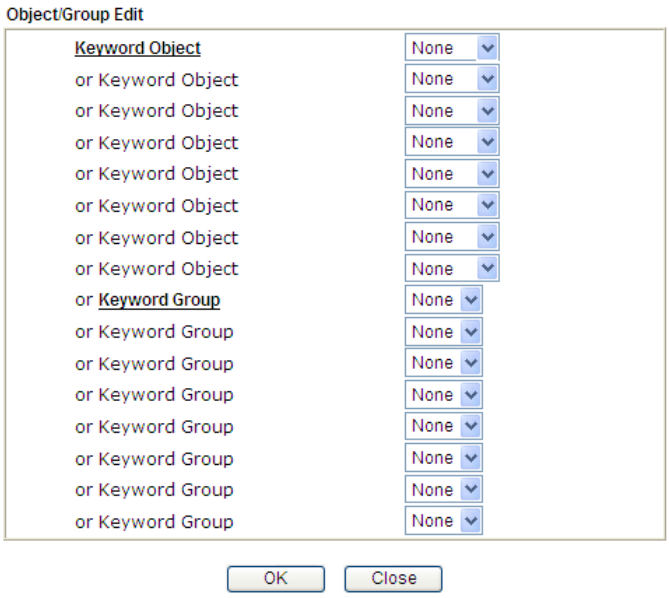
您可設定 8 組 URL 內容過濾器設定檔，請按索引編號連結，開啓如下頁面。



可用設定說明如下：

項目	說明
設定檔名稱(Profile Name)	請輸入此設定檔名稱。
優先權(Priority)	決定路由器採用的動作順序。 **二者皆選:通過(Both: Pass)** – 路由器讓符合 URL 存取控制與網頁特徵所指定條件的封包放行通過，當您選擇此項設定時，本頁針對 URL 存取控制與網頁特徵所設定的限制都將暫停作用。 **二者皆選:封鎖(Both:Bloc)** – 路由器封鎖住任何符合 URL 存取控制與網頁特徵所指定條件的封包，當您選擇此項設定時，本頁針對 URL 存取控制與網頁特徵所設定的限制都將暫停作用。 **二者擇一: URL 存取控制優先(Either: URL Access Control First)** – 當所有封包皆符合 URL 存取控制與網頁特徵之設定條件時，此功能可以決定先執行的動作爲何。針對此項，路由器將先處理符合 URL 存取控制設定條件下的封包，然後再處理符合網頁特徵條件的封包。 **二者擇一: 網頁特徵優先(Either: Web Feature First)** – 當所有封包皆符合 URL 存取控制與網頁內容之設定條件時，此功能可以決定先執行的動作爲何。針對此項，路由器將先處理符合網頁特徵條件下的封包，然後再處理符合 URL 存取控制設定條件的封包。

	
紀錄(Log)	**通過(Pass)** – 只有通過動作會記錄在 Syslog 中。 **封鎖(Block)** – 只有封鎖動作會記錄在 Syslog 中。 **全部(All)** – 所有的動作(包含通過與封鎖)都會記錄在 Syslog 中。
URL 存取控制(URL Access Control)	**啓用 URL 存取控制(Enable URL Access Control)** - 勾選此方塊啓動 URL 存取控制設定，請注意 **URL 存取控制**優先權原本就高於**網頁特徵(Restrict Web Feature)**，如果網頁內容符合 URL 存取控制中的設定，路由器將先執行此區所指定的動作，而忽略網頁特徵中所指定的動作。 **防止從 IP 位址存取網頁(Prevent web access from IP address)**- 勾選此方塊拒絕任何使用 IP 位址例如 http://202.6.3.2 來要求存取資料的活動，這個項目可以防止他人躲避 URL 存取控制的監控，您必須先清除瀏覽器的快取資料，讓 URL 內容過濾器工具能夠在您所造訪的網頁上適當的操作。 **動作(Action)** – 此功能僅在您選擇了**二擇一: URL 存取控制優先(Either：URL Access Control First)**或**二擇一: 網頁特徵優先(Either：Web Feature First)**時才能使用。 ● ***通過(Pass)*** - 允許進入含有關鍵字清單中之關鍵字的網頁。 ● ***封鎖(Block)*** - 不允許進入含有關鍵字清單中之關鍵字的網頁。若網頁並不符合此處所設定的關鍵字清單設定，該網頁將以相反動作來處理。 **除外清單(Exception List)** – 指定物件設定檔，以便採取與上述指定的動作相反的行爲。 **群組/物件選擇(Group/Object Selections)** – Vigor 路由器提供數種方框讓您定義關鍵字，每個方框都支援數個關鍵字。關鍵字可以是一個名詞、數字、部分名稱或是完整的 URL 字串，方框內多數關鍵字可以空白、逗號或是分號來區隔。另外，每個方框最大的長度爲 32 個字元。指定完關鍵字後，Vigor 路由器將婉拒符合任何使用者定義的關鍵字之網頁的 URL 連線需求。注意，封鎖的關鍵字寫得越簡化，Vigor 路由器執行起來也會更加有效率。



網頁特徵(Web Feature)

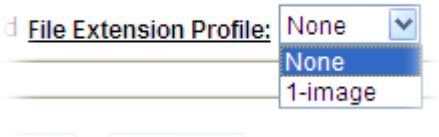
啓用限制網頁特徵(Enable Web Feature Restrictio) - 勾選此方塊讓關鍵字被封鎖或是放行。

動作 - 此功能僅在您選擇了**二者選一: URL 存取控制優先(Either: URL Access Control First)**或**二者選一: 網頁特徵優先(Either: Web Feature First)**時才能使用。

通過(Pass) - 允許進入含有關鍵字清單中之關鍵字的網頁。

封鎖(Block) - 不允許進入含有關鍵字清單中之關鍵字的網頁。若網頁並不符合此處所設定的關鍵字清單設定，該網頁將以相反動作來處理。

副檔名設定檔(File Extension Profile) - 請自**物件設定>>副檔名物件(Object Setting>> File Extension Objects)**中選擇一個事先設定完成的設定檔，並決定其對檔案下載採取封鎖或是放行的動作。



Cookie - 勾選此方塊從內部到外部過濾 cookie 傳輸資料以保護本地用戶的隱私。

Proxy - 勾選此方塊退回任何的伺服器傳輸要求。想要有效控制頻寬，讓封鎖機制過濾從網站下載的多媒體檔案是最有價值的事情。

上傳(Upload) – 勾選此方框以封鎖檔案透過網頁上傳。

完成設定之後，按下確定(OK)按鈕儲存相關設定。

VI-2-4 網頁內容過濾器設定檔(Web Content Filter Profile)

有數種方式可以啓動路由器的網頁內容過濾器(WCF) – 透過**服務啓動精靈(Service Activation Wizard)**、**數位內容安全管理>>網頁內容過濾器設定檔(CSM>>Web Content Filter Profile)**或是**系統維護>>開啓授權碼(System Maintenance>>Activation)**。

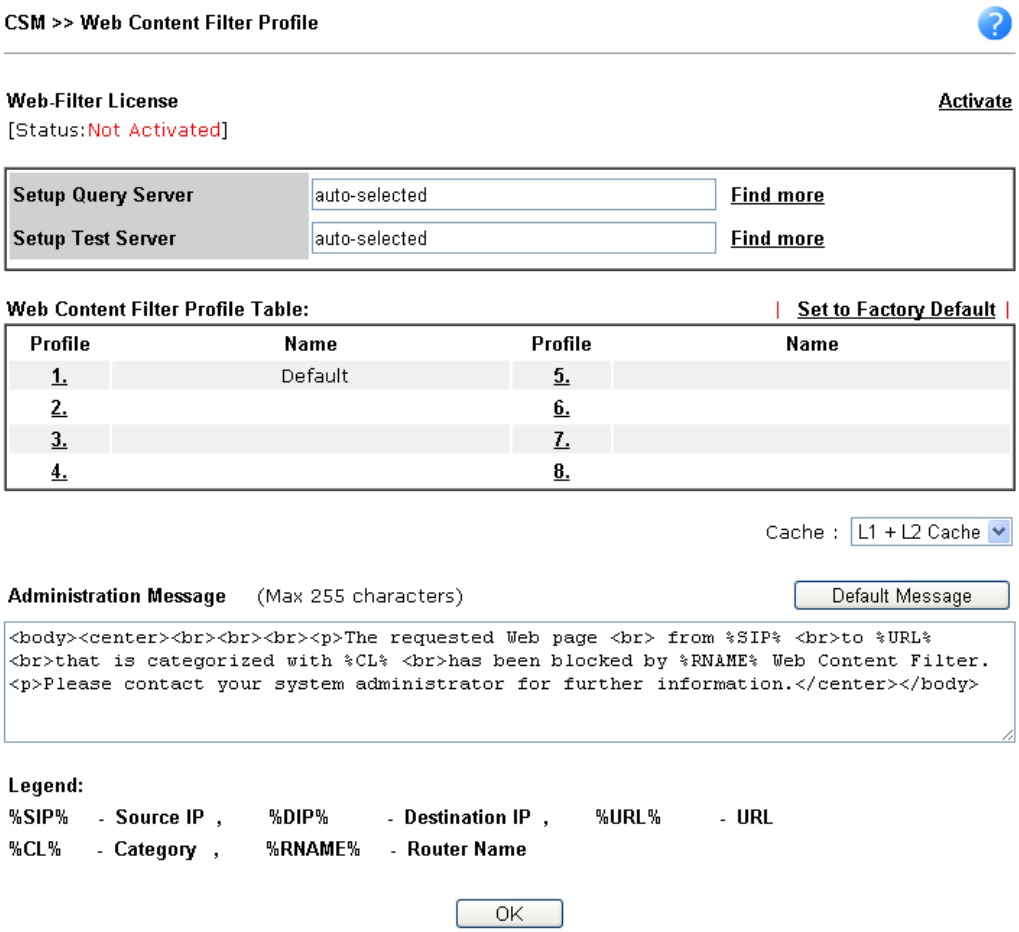
服務啓動精靈讓您使用試用版或是直接更新 WCF 授權碼，無需登入 http://myvigor.draytek.com 的伺服器(***MyVigor***)。

不過，如果您使用網頁內容過濾器設定檔來啓動 WCF 功能，您必須登入(***MyVigor***)伺服器，因此，您得先上伺服器註冊一組帳號才能使用相關的服務，請參考如何建立 MyVigor 帳號相關章節。

WCF 採取特定服務供應商開發的機制來進行，不論是啓動 WCF 功能或是取得新的授權碼，您都必須按下**啓動(Activate)**才能達成要求，要注意的是符合目前 Vigor 路由器需求的服務供應商提供的是短期的試用版，如果您想要購買正式版本，請與通路商或是經銷商聯絡。

按下**數位內容安全管理**(CSM)然後選擇**網頁內容過濾器設定檔(Web Content Filter Profile)**開啓設定頁面，其中，設定搜尋伺服器/設定測試伺服器都是自動選定的，您可以按下**更多(Find more)**連結開啓另一視窗然後選擇需要的伺服器。

資訊 1	WCF 並非 Vigor 路由器的內建機制，該服務是由 Commtouch 公司所提供，如果您想要使用此類服務(試用版或是正式版)，您必須先進行啓用的程序。若您想要使用正式版，請先與經銷商聯絡，獲取更多更詳細的 WCF 資訊。
資訊 2	Commtouch 已經併入 Cyren，其 GlobalView 服務仍將持續提供強大且以雲端爲基準的安全性解決方案相關資訊。請參考：http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239025151.html

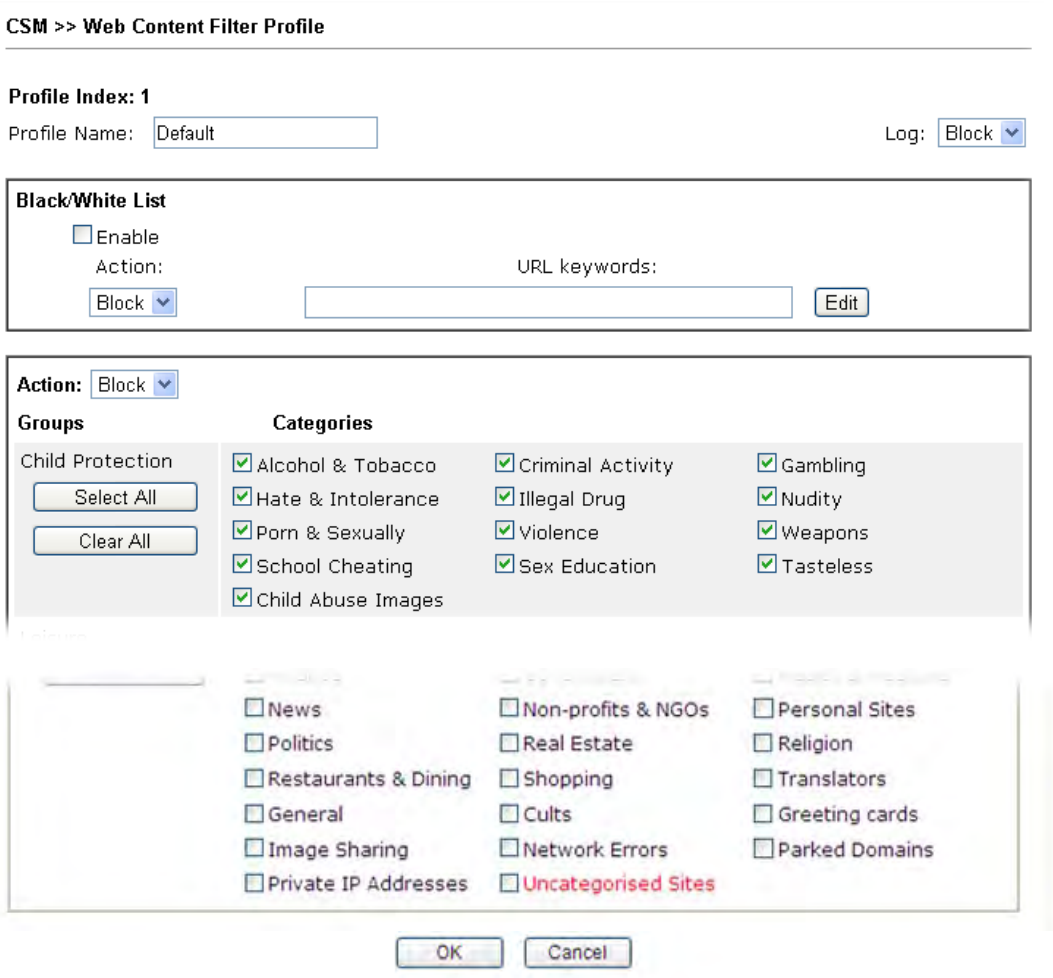


可用設定說明如下：

項目	說明
啓動(Activate)	按下此鈕登入 MyVigor 以便啓動 WCF 服務。
設定搜尋伺服器 (Setup Query Server)	建議您使用預設的設定，當您以 WCF 設定檔爲基準，在瀏覽器上輸入 URL 時，您需要指定伺服器來歸類搜尋的內容。
設定測試伺服器 (Setup Test Server)	建議您使用預設的設定。
Find more (更多)	按下此鈕開啓畫面選擇另外的伺服器。
測試站點，檢查該站是否已被歸類(Test a site to verify whether it is categorized)	按下此連結進行驗證動作。
回復出廠預設值(Set to Factory Default)	按下此連結回復出廠預設值。
管理訊息(Administration Message)	您可以手動輸入訊息或是按下**預設訊息(Default Message)**按鈕取得預設的訊息，並顯示在**管理訊息**方框內。
快取(Cache)	**無(None)** – 路由器將會透過 WCF 機制檢查使用者想要登入的 URL，處理的速度爲一般，這個選項可提供最準確的 URL 過濾作業。 **L1** – 路由器將會透過 WCF 機制檢查使用者想要登入的 URL，如果該 URL 早先已經存取過，系統會將此資料在路由器內儲存非常短暫的時間(大約 1 秒)，讓必要時可以快速登入。此選項可以

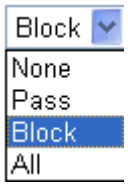
	提供速度較快的 URL 過濾作業。 **L2** – 路由器將會透過 WCF 機制檢查使用者想要登入的 URL，如果該 URL 早先已經存取過，系統會將其 IP 位址在路由器內儲存非常短暫的時間(大約 1 秒)，當使用者想要再次登入相同的 IP 時，路由器會將其與儲存的內容做比對，如果符合，該頁面就會迅速取回並呈現出來。此選項可以提供速度最快的 URL 過濾作業。 **L1+L2 快取** – 路由器將會以 L1 加上 L2 的功能快速檢查 URL。

您可設定 8 組網頁內容過濾器設定檔，請按索引編號連結，開啓如下頁面。分類中的項目依照不同的服務供應商而有所改變，如果您已經且啓動了另一個網頁內容過濾器授權碼，相關的分類項目也會隨之變更。所有 WCF 所做的設定都會被刪除，因此在您變更網頁內容過濾器授權碼之前，請先備份資料。



可用設定說明如下：

項目	說明
設定檔名稱(Profile Name)	輸入網頁內容過濾器設定檔的名稱。
黑名單/白名單(Black/White List)	**啓用(Enable) –** 勾選此方塊啓用過濾機制，利用黑白名單的內文來決定。 **URL Keywords-** Click **Edit** to choose the group or object profile as the content of white/black list. 請按**編輯(Edit)**按鈕開啓視窗，並自其中選擇一個您需要的項目，然後針對此項目再選擇要執行的動作爲何。

	動作，通過(Pass) – 網頁內文符合本區所選定的關鍵字物件/群組內容，於經過路由器時可通行無阻。 **動作，封鎖(Block)** - 網頁內文符合本區所選定的關鍵字物件/群組內容，於經過路由器時會被阻擋下來。
動作(Action)	**通過(Pass)** – 允許進入勾選的方塊等相關類型頁面。 **封鎖(Block)** – 限制進入勾選的方塊等相關類型頁面。如果網頁未符合此處所設定的內容，系統將以反向做爲處理該網頁。
紀錄(Log)	**無(None)** – 沒有任何關於此設定檔的紀錄保留下來。 **通過(Pass)** – 只有通過動作會記錄在 Syslog 中。 **封鎖(Block)** – 只有封鎖動作會記錄在 Syslog 中。 **全部(All)** – 所有的動作(包含通過與封鎖)都會記錄在 Syslog 中。 

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

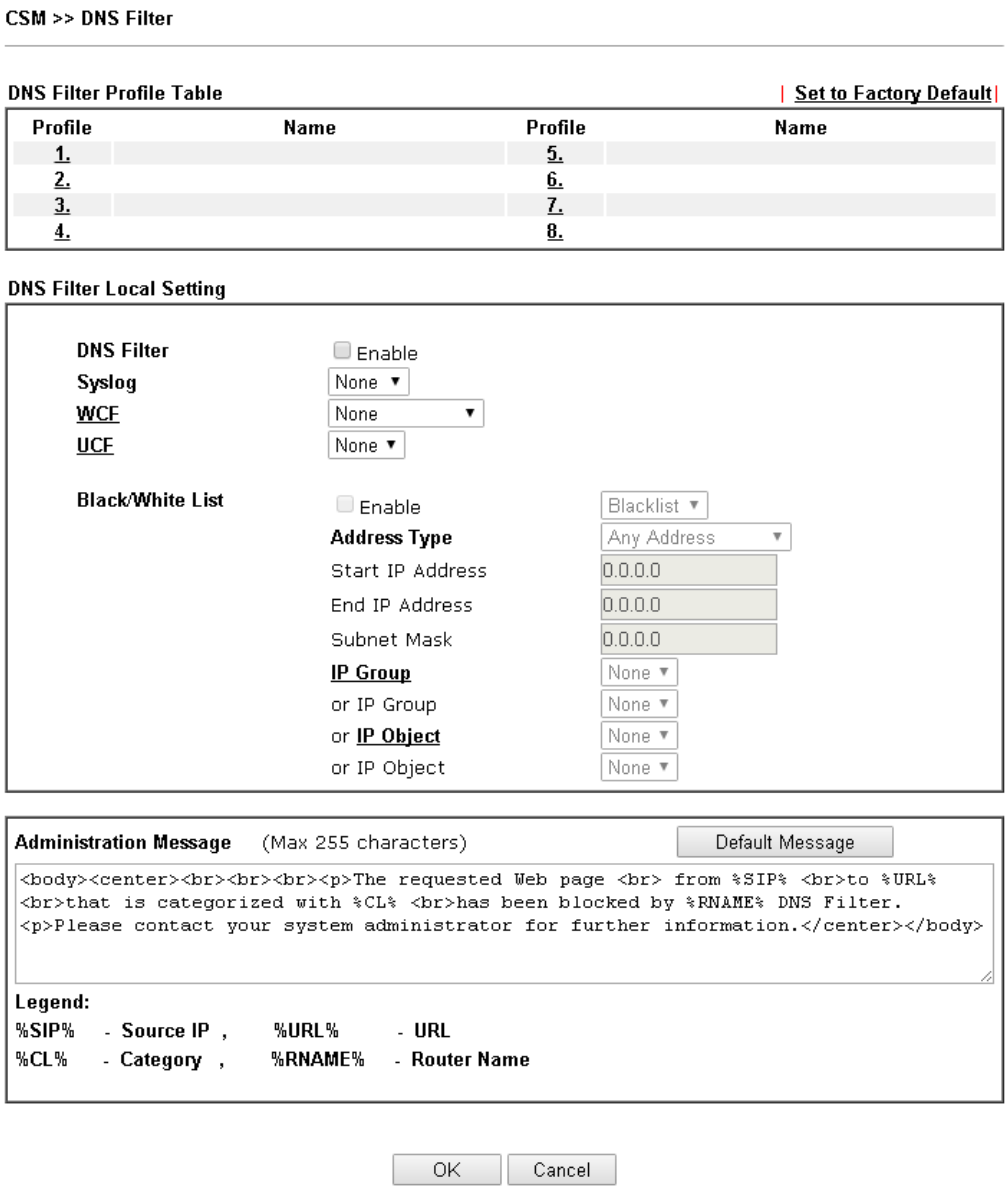
VI-2-5 DNS 過濾器設定檔(DNS Filter Profile)

DNS 過濾器監控 DNS 的諮詢，並將相關資訊傳送至 WCF，以便歸類 HTTPS URL。

DNS 可利用路由器伺服器(例如 168.95.1.1)或是外部 DNS 伺服器(例如 8.8.8.8)於 **LAN>>基本設定**中指定，如果使用路由器伺服器，**DNS 過濾器基本設定(DNS Filter General Setting)**將套用到 LAN 端用戶的 DNS 詢問中。不過如果使用的是外接 DNS 伺服器，**DNS 過濾器設定檔(DNS Filter Profile)**將套用到 LAN 端用戶的 DNS 詢問中。

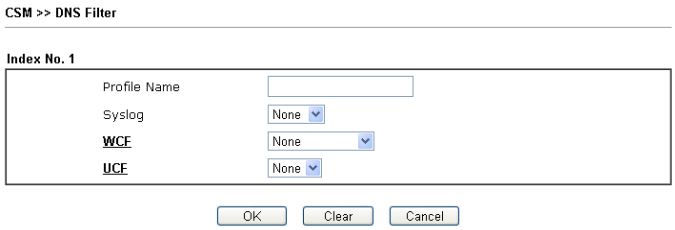
資訊

因爲 DNS 過濾器必須使用 WCF 服務來過濾封包，因此 WCF 授權碼必須事先啓動才行。否則，DNS 過濾器無法對封包產生任何效用。



可用設定說明如下：

項目	說明
DNS 過濾器設定檔表(DNS Filter Profile Table)	顯示不同的 DNS 過濾器設定檔清單資料。 按下索引編號連結開啓如下頁面，然後輸入設定檔名稱並依照

	您的需要指定 WCF/UCF 等過濾器設定檔以資套用。 
DNS 過濾器本地設定(DNS Filter Local Setting)	若尚未設定好任何 DNS 設定檔，此處的基本設定將會套用至 DNS 過濾器。 **DNS 過濾器(DNS Filter) -** 勾選**啓用(Enable)**以便啓用此功能。 **Syslog -** 過濾結果將依照 Syslog 設定來記錄。 ● **無(None)** –此設定沒有任何內容會被記錄下來。 ● **通過(Pass)** –只有封包通過的記錄會被轉往 Syslog。 ● **封鎖(Block)** –只有封包被封鎖的記錄會被轉往 Syslog。 ● **全部(All)** –所有的動作(通過與封鎖)記錄都會被轉往 Syslog。 **WCF-** 設定網頁內容過濾器的過濾條件。 **UCF** - 設定 URL 內容過濾器的過濾條件。 **黑/白名單(Black/White List) -** 可指定 IP 位址、子網遮罩、IP 物件或是 IP 群組作爲黑名單或是白名單，讓路由器可以放行 DNS 封包或是阻擋封包。
管理訊息(Administration Message)	輸入文字或是完整句子，當 Vigor 路由器封鎖頁面時將會呈現此管理訊息。

完成設定之後，按下確定(OK)按鈕儲存相關設定。

應用說明

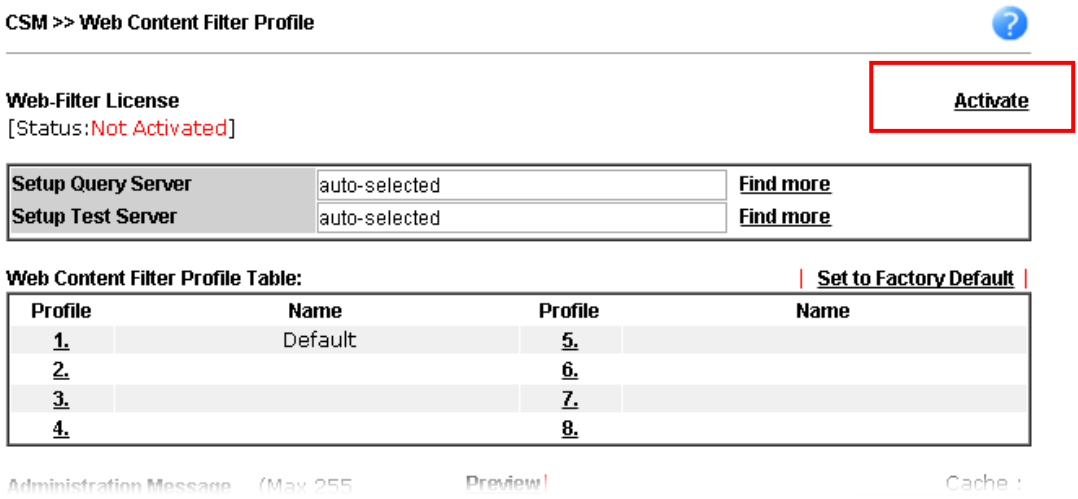
A-1 如何建立一個 MyVigor 帳號

MyVigor 網站(http://myvigor.draytek.com)提供數種有用的服務(諸如防垃圾信、網頁內容過濾、防入侵等等)來過濾網頁，以便保障您的系統的安全。

如要進入 MyVigor 取得更多的資訊，請先建立一個 MyVigor 帳號。

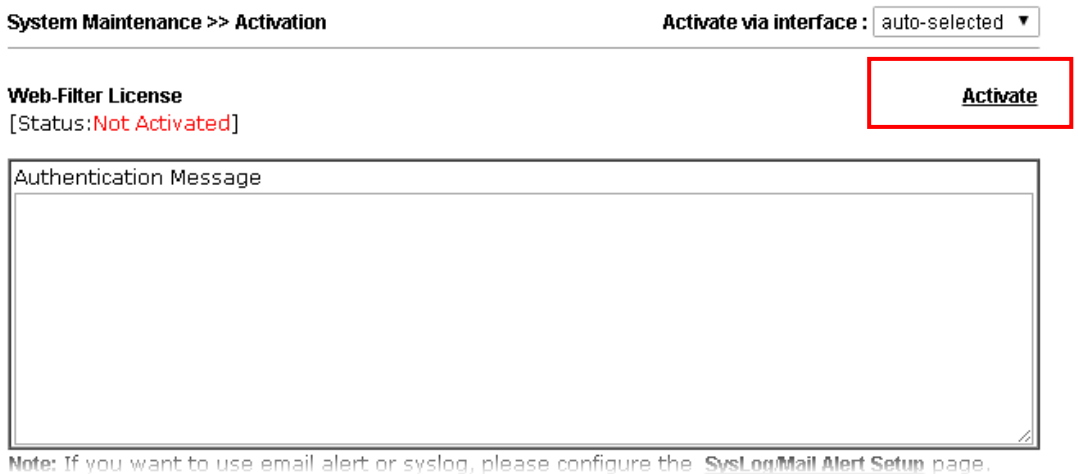
透過 Vigor 路由器來建立

1. 開啓**數位內容安全管理>>網頁內容過濾器設定檔(CSM>> Web Content Filter Profile)**，您可見到如下頁面：

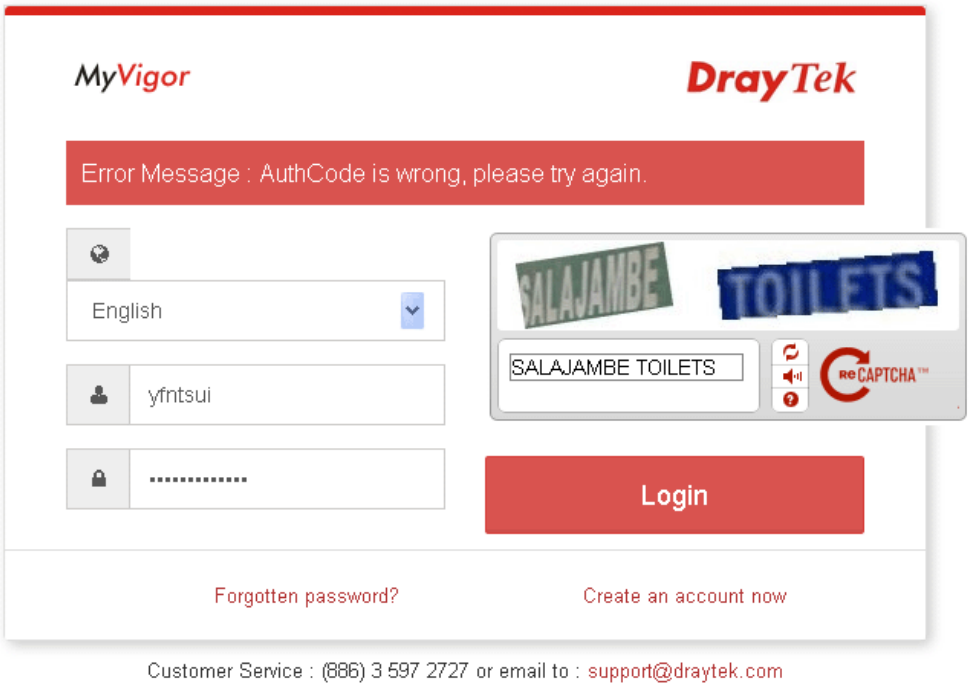


或是

開啓**系統維護>>開啓授權碼(System Maintenance>>Activation)**

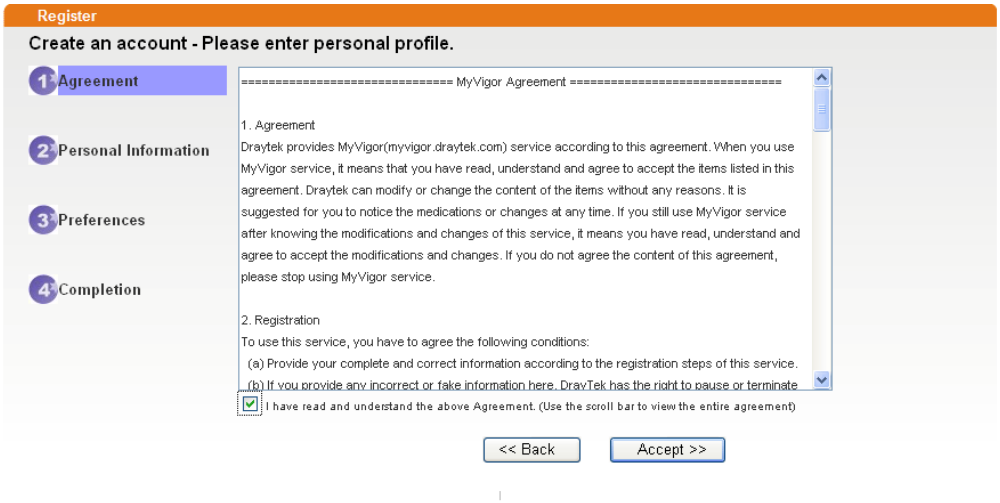


2. 按下**啓動(Activate)**連結，MyVigor 登入視窗將會自動跳出。



3. 按下 **Create an account now** 連結。

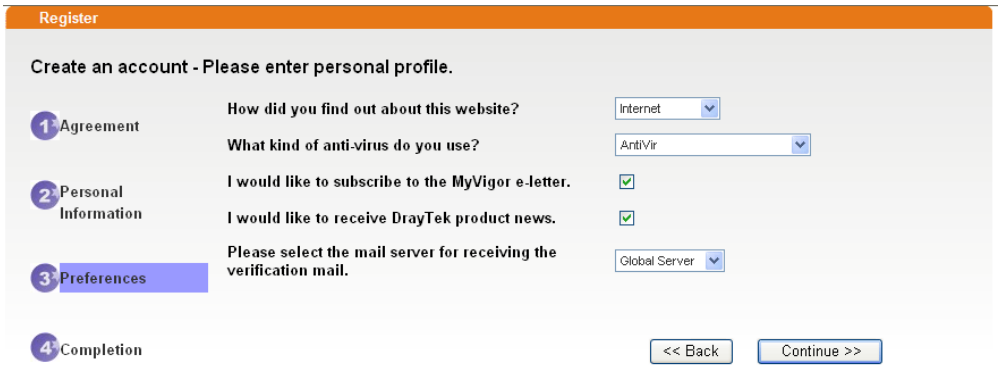
4. 確認您已同意畫面上的聲明並勾選同意方塊，接著按下 **Accept**。



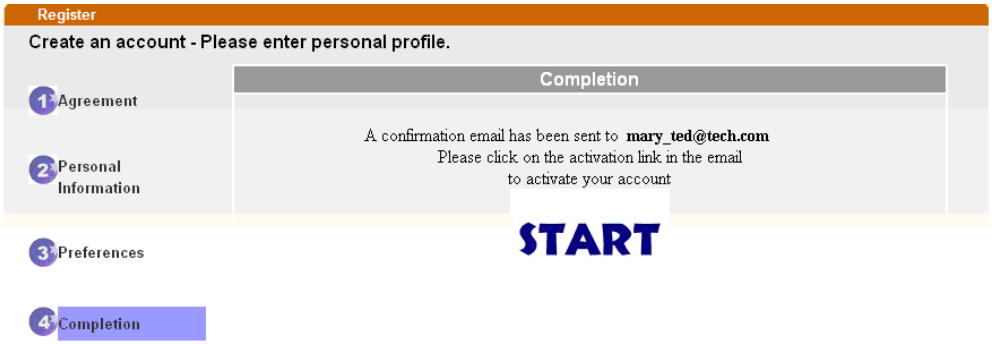
5. 輸入個人資訊並按下 **Continue**。



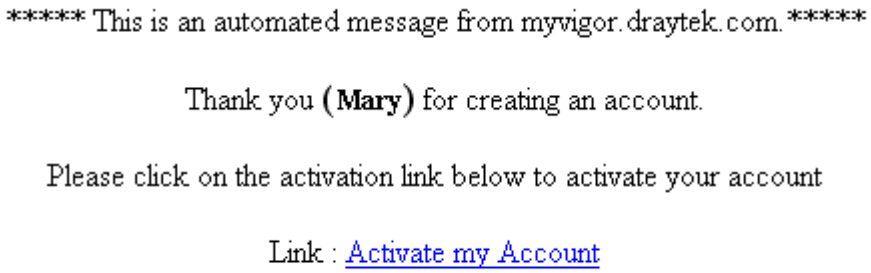
6. 選擇適合您的電腦的選項，再按下 **Continue**。



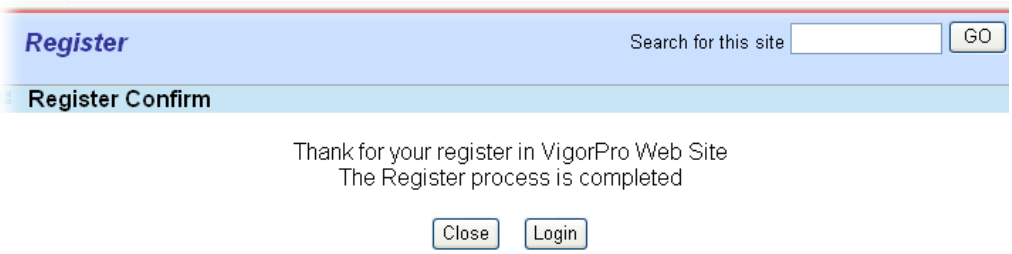
7. 現在您已經成功建立一個帳號了，請按 **START**。



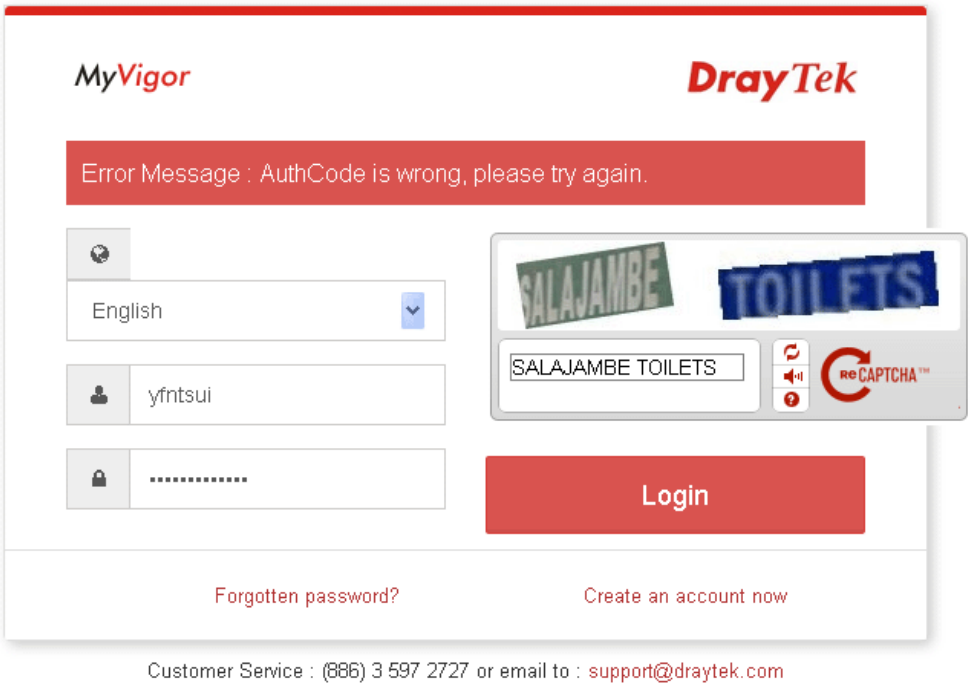
8. 請先去信箱查看郵件，是否收到標題爲 **New Account Confirmation Letter from myvigor.draytek.com** 的信件。



9. 若已收到，請按下 **Activate my Accoun** 連結啓動帳號，下圖將會顯示出來，表示註冊過程已經完成，請按 **Login**。



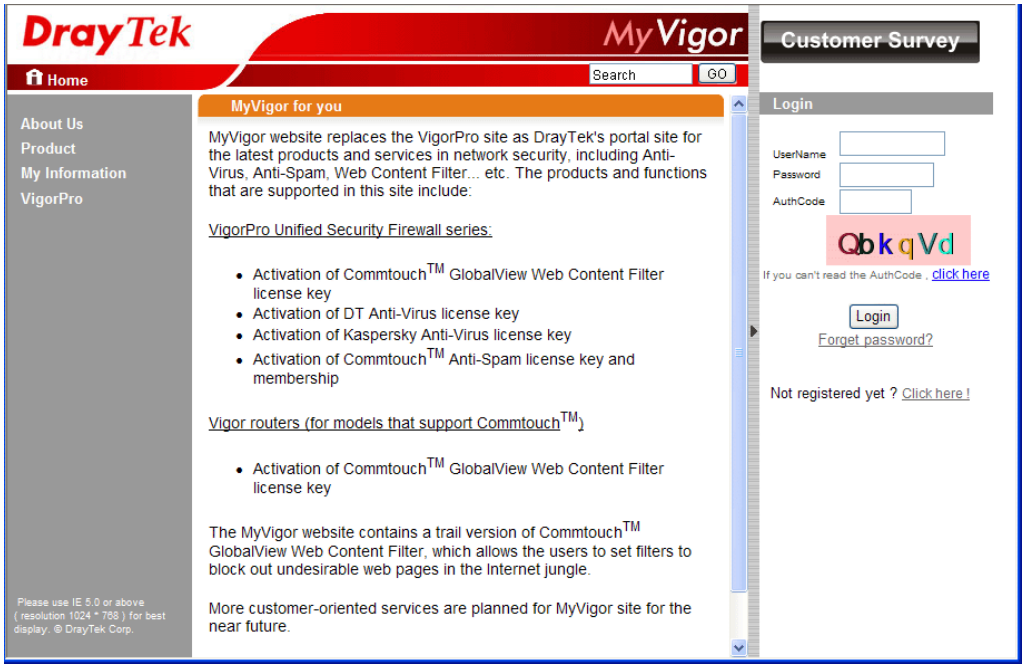
10. 當您看看如下頁面時，請輸入帳號與密碼(您剛剛在前述步驟中建立)。



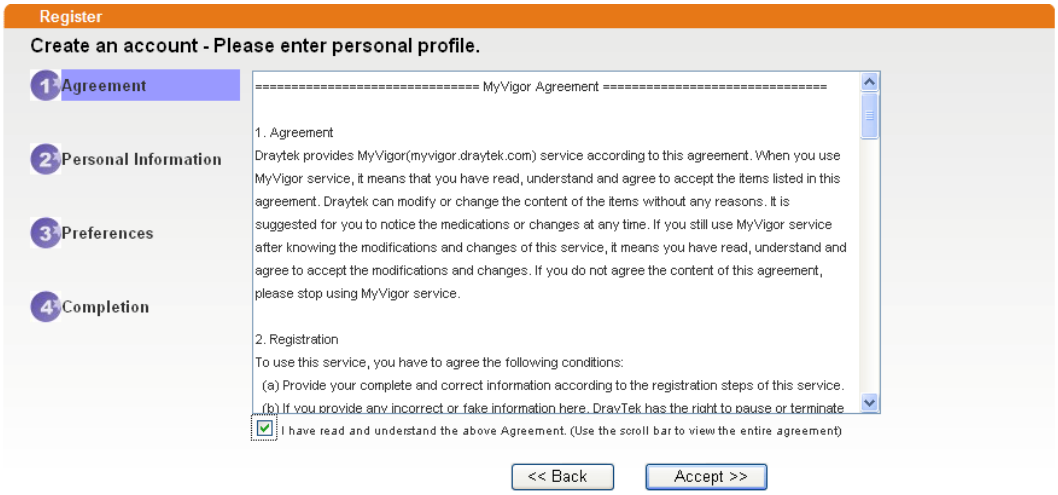
11. 輸入驗證碼之後，按下 Login。系統將帶您進入 MyVigor 伺服器。

透過 MyVigor 網站來建立

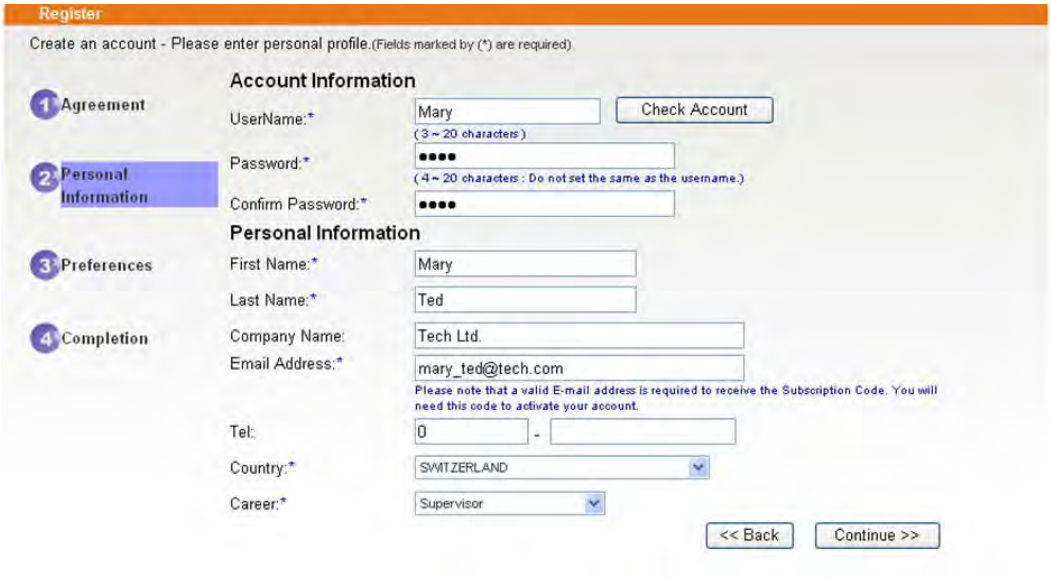
1. 登入 http://myvigor.draytek.com，找到 **Not registered yet?** 這行之後，按下旁邊的 **Click here!** 連結進入下一個畫面。



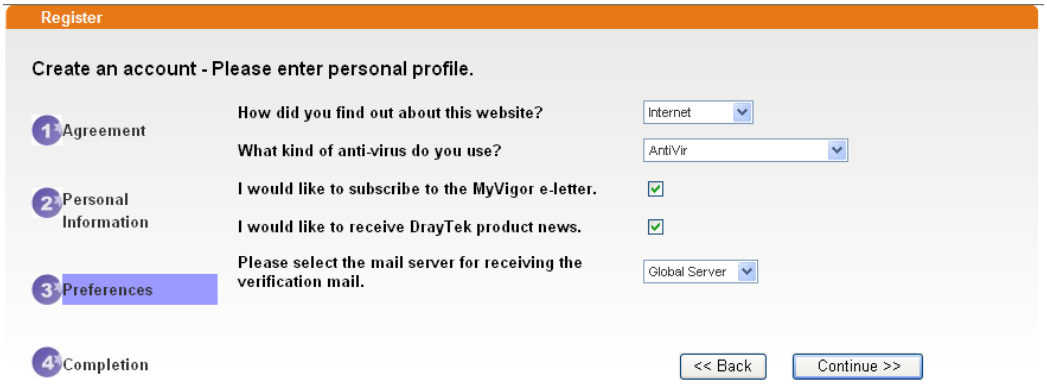
2. 確認您已同意畫面上的聲明並勾選同意方塊，接著按下 **Accept**。



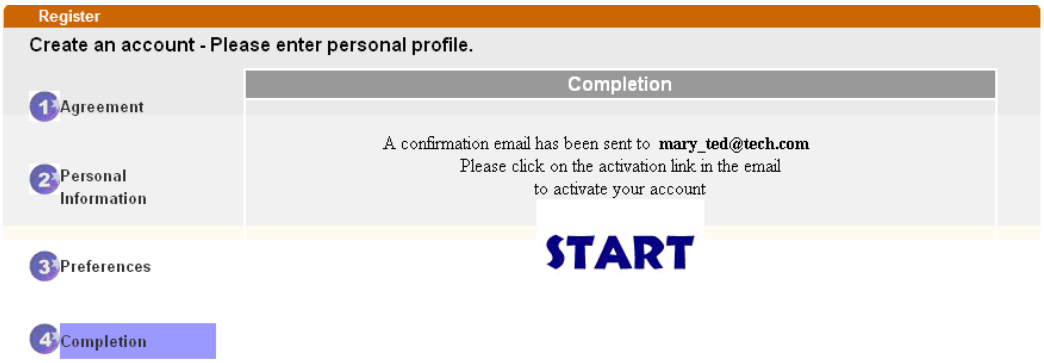
3. 輸入個人資訊並按下 **Continue**。



4. 選擇適合您的電腦的選項，再按下 **Continue**。



5. 現在您已經成功建立一個帳號了，請按 **START**。



6. 請先去信箱查看郵件，是否收到標題爲 **New Account Confirmation Letter from myvigor.draytek.com** 的信件。

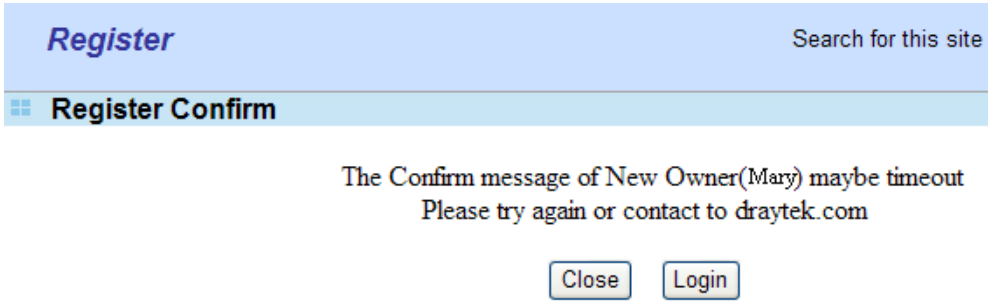
****** This is an automated message from myvigor.draytek.com.******

Thank you (**Mary**) for creating an account.

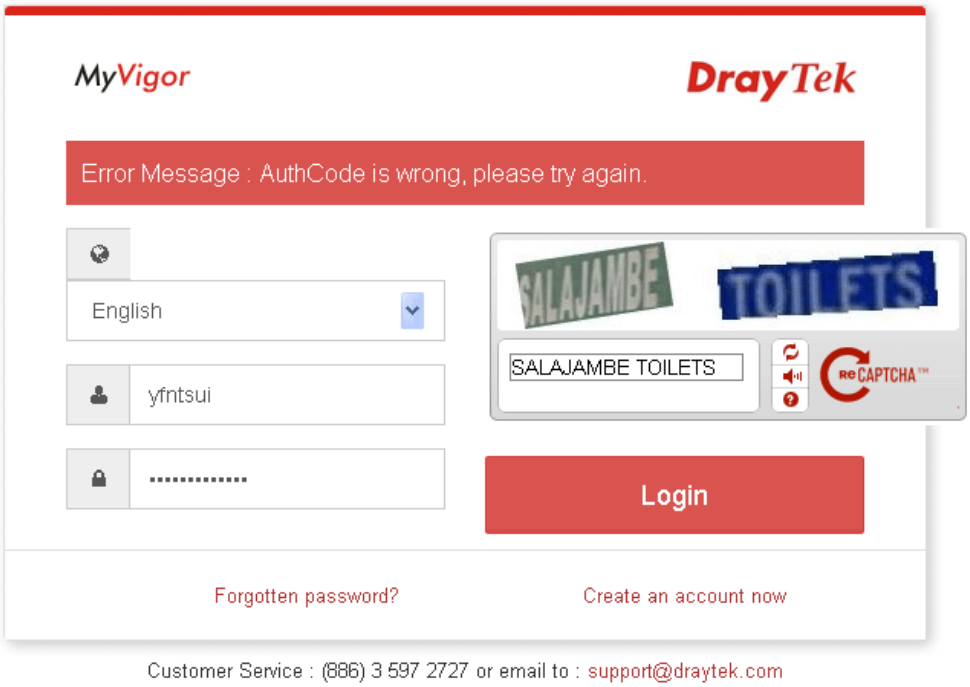
Please click on the activation link below to activate your account

Link : Activate my Account

7. 若已收到，請按下 **Activate my Accoun** 連結啓動帳號，下圖將會顯示出來，表示註冊過程已經完成，請按 **Login**。



8. 當您看看如下頁面時，請輸入帳號與密碼(您剛剛在前述步驟中建立)。



輸入驗證碼之後，按下 Login。系統將帶您進入 MyVigor 伺服器。

A-2 用網頁內容過濾器(WCF) /URL 內容過濾器來阻擋使用者存取 Facebook 服務

阻擋使用者存取 Facebook 網頁有二種方式，網頁內容過濾器(WCF)與 URL 內容過濾器。

網頁內容過濾器(WCF),

優點：簡單迅速套用至您想要阻擋的類別/網站

附註：需搭配授權碼

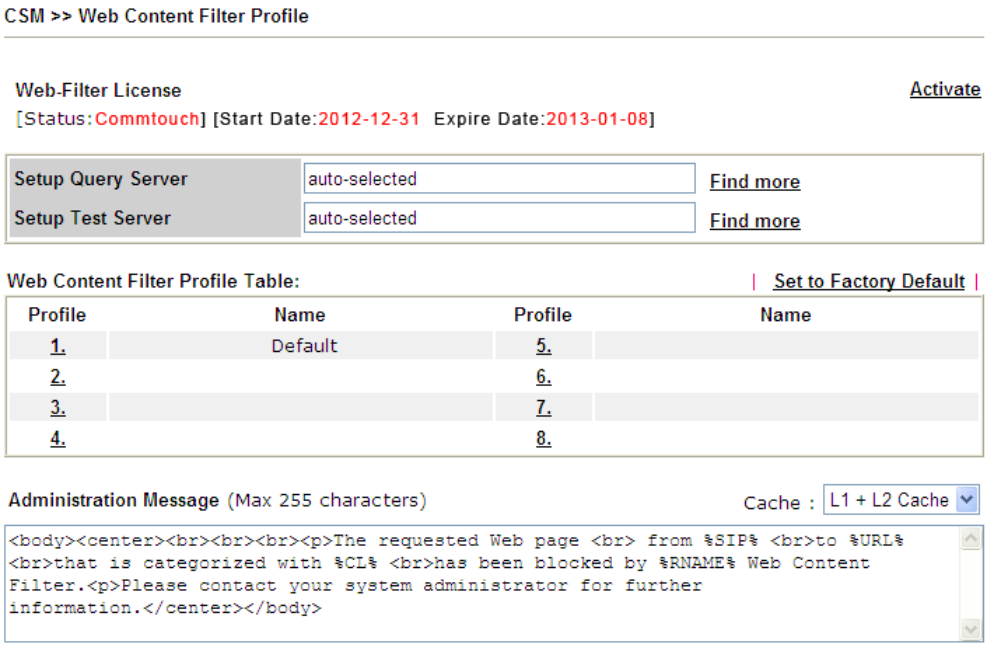
URL 內容過濾器,

優點：免費，對於客製化網頁具有彈性

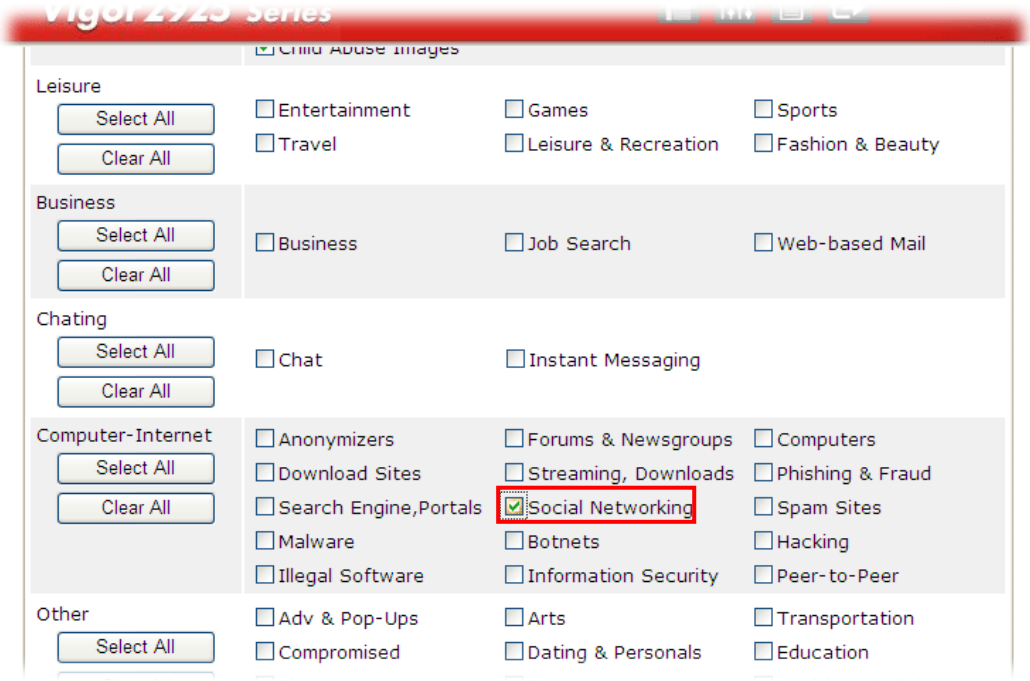
附註：須手動調整設定 (例如一個網站設定一個關鍵字等)

I. 透過網頁內容過濾器(WCF)

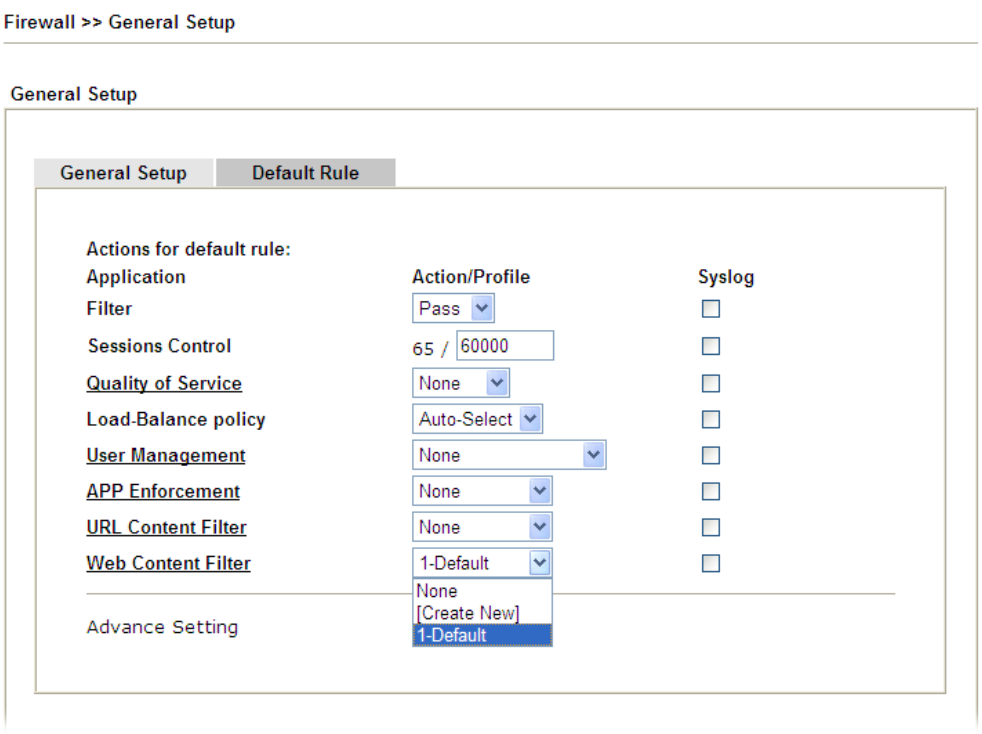
1. 請確認網頁內容過濾器(WCF) (由 Commtouch 提供服務)授權碼仍在有效期內。



2. 開啓**數位內容安全管理(CSM) >> 網頁內容過濾器設定檔(CSM >> Web Content Filter Profile)**建立新的 WCF 設定檔，請勾選**社交網路(Social Networking)**，**動作**請選擇**封鎖(Block)**。



3. 在**防火牆>>基本設定>>預設規則(Firewall>>General Setup>>Default Rule)**這個頁面當中，請用剛剛設定的設定檔。



4. 下次，當用戶嘗試透過路由器進入 Facebook 時，網頁將被封鎖起來，系統並傳送及顯示如下訊息給您。

The requested Web page
from 192.168.2.114
to www.facebook.com/
that is categorized with [Social Networking]
has been blocked by Web Content Filter.

Please contact your system administrator for further information.

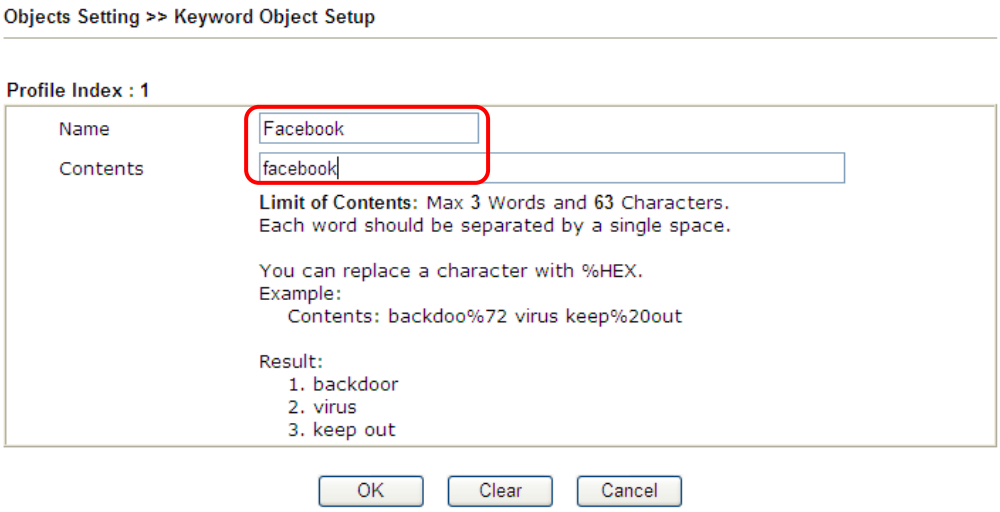
[Powered by DrayTek]

II. 透過 URL 內容過濾器

A. 阻擋存取 Facebook 字眼的網頁

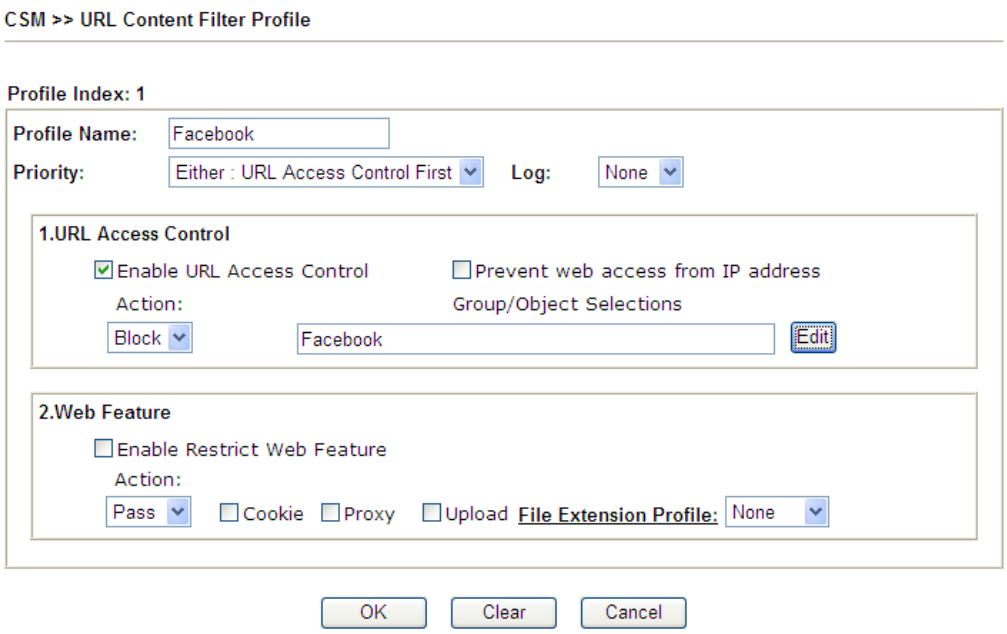
1. 開啓**物件設定>>關鍵字物件(Object Settings>>Keyword Object)**，按下任一索引連結以進入設定頁面。

2. 在**內容(Contents)**區域中，輸入 *facebook*，參考下圖所示。按下**確定(OK)**儲存。



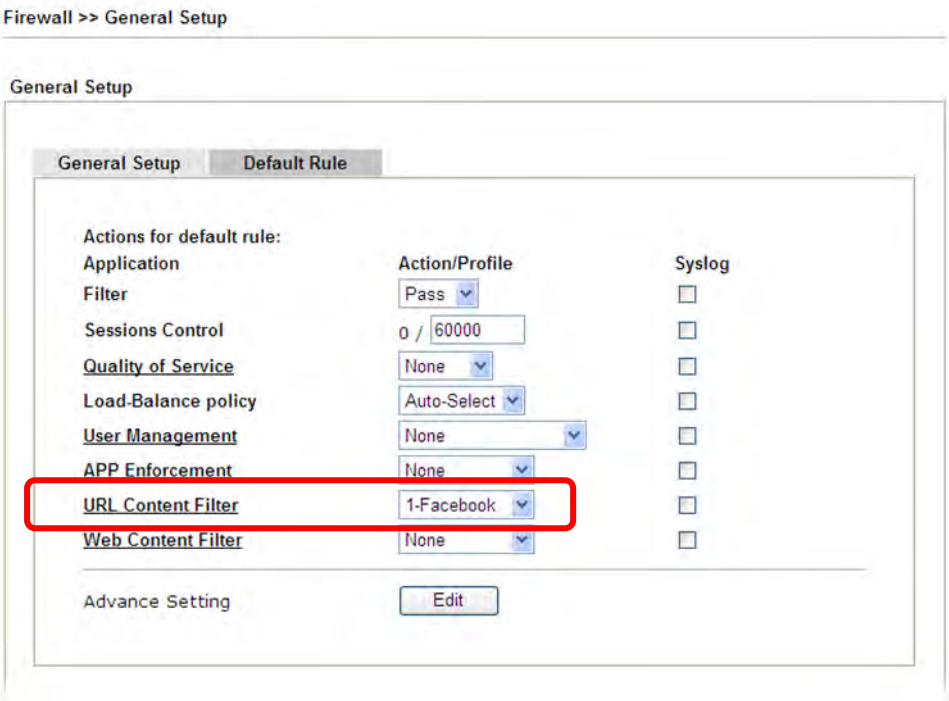
3. 開啓**數位內容安全管理>>URL 內容過濾器設定檔(CSM>>URL Content Filter Profile)**，按下任一索引連結開啓設定頁面。

4. 請按下圖所示輸入內容。



5. 完成上述設定之後，按下**確定(OK)**儲存。接著開啓**防火牆>>基本設定(Firewall>>General Setup)**。

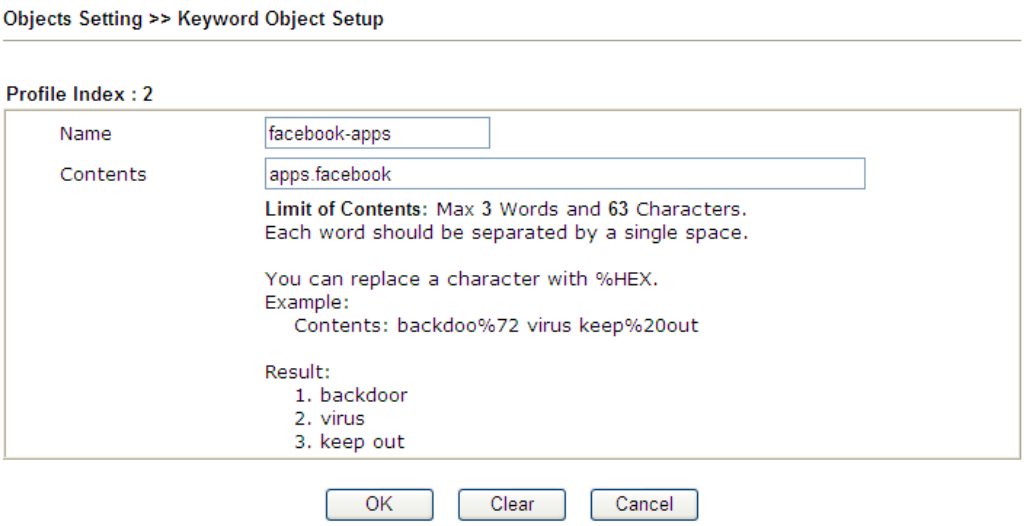
6. 選擇**預設規則(Default Rule)**標籤，在開啓的頁面上，於 **URL 內容過濾器(URL Content Filter)**選項中選擇剛剛設定的設定檔。按下**確定**儲存。



B. 阻擋使用者使用 Facebook 的小遊戲

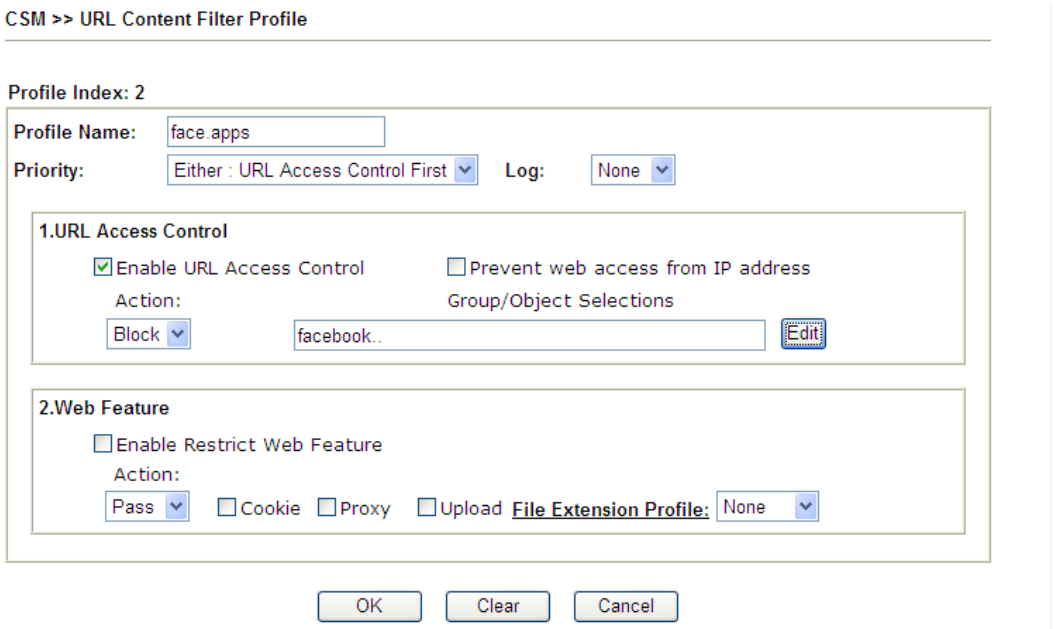
1. 開啓**物件設定>>關鍵字物件(Object Settings>>Keyword Object)**，按下任一索引連結以進入設定頁面。

2. 在**內容(Contents)**區域中，輸入 *apps.facebook*，參考下圖所示。按下**確定(OK)**儲存。



3. 開啓**數位內容安全管理>>URL 內容過濾器設定檔(CSM>>URL Content Filter Profile)**，按下任一索引連結開啓設定頁面。

4. 請按下圖所示輸入內容。

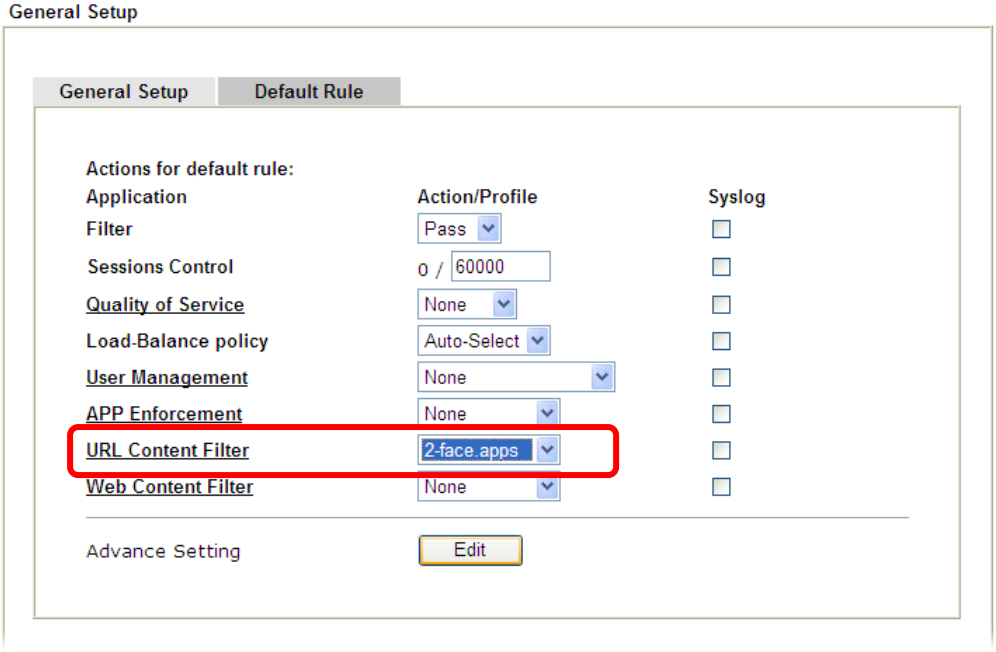


5. 完成上述設定之後，按下**確定**儲存。接著開啓**防火牆>>基本設定(Firewall>>General Setup)**。

6. 選擇**預設規則(Default Rule)**標籤，在開啓的頁面上，於 **URL 內容過濾器**選項中選擇剛剛設定的設定檔。按下**確定**儲存，才能阻擋 apps.facebook 字眼的網址。

Firewall >> General Setup

General Setup



第七篇 管理設定



System Maintenance

路由器系統安裝包含數種項目：系統狀態、TR-069、管理者密碼、使用者密碼、登入頁面歡迎詞、設定備份、Syslog/郵件警告、時間與日期、管理、重新啓動系統、韌體更新與啓動等等。



Bandwidth Management

用於控制資料傳輸之頻寬，主要是透過連線數限制、頻寬限制以及服務品質(QoS) TR-069



User Management

此功能不允許來自特定主機的任何IP流量(除了DHCP相關的封包外)，除非該主機能提供正確的使用者名稱與密碼。

VII-1 系統維護(System Maintenance)

系統設定方面，有數種項目是使用者需要瞭解的：系統狀態、系統管理員密碼、備份組態、系統紀錄/郵件警示、時間設定、重啓系統及韌體升級等等。

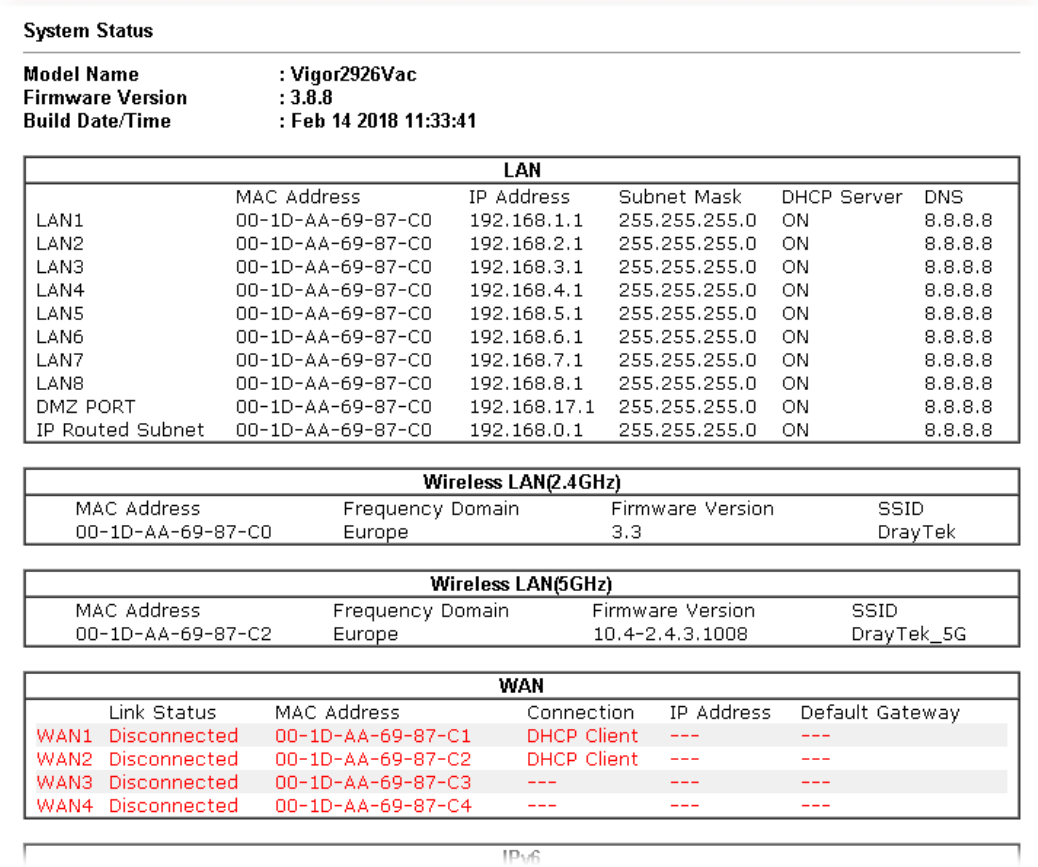
網頁使用者介面

下圖爲系統維護的主要設定功能。



VII-1-1 系統狀態(System Status)

系統狀態提供基本的網路設定，包含區域網路和 WAN 介面等資訊，同時您也可以獲得目前執行中的韌體版本或是韌體其他的相關資訊。



System Status

Model Name : **Vigor2926Vac**
Firmware Version : **3.8.8**
Build Date/Time : **Feb 14 2018 11:33:41**

LAN

	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-1D-AA-69-87-C0	192.168.1.1	255.255.255.0	ON	8.8.8.8
LAN2	00-1D-AA-69-87-C0	192.168.2.1	255.255.255.0	ON	8.8.8.8
LAN3	00-1D-AA-69-87-C0	192.168.3.1	255.255.255.0	ON	8.8.8.8
LAN4	00-1D-AA-69-87-C0	192.168.4.1	255.255.255.0	ON	8.8.8.8
LAN5	00-1D-AA-69-87-C0	192.168.5.1	255.255.255.0	ON	8.8.8.8
LAN6	00-1D-AA-69-87-C0	192.168.6.1	255.255.255.0	ON	8.8.8.8
LAN7	00-1D-AA-69-87-C0	192.168.7.1	255.255.255.0	ON	8.8.8.8
LAN8	00-1D-AA-69-87-C0	192.168.8.1	255.255.255.0	ON	8.8.8.8
DMZ PORT	00-1D-AA-69-87-C0	192.168.17.1	255.255.255.0	ON	8.8.8.8
IP Routed Subnet	00-1D-AA-69-87-C0	192.168.0.1	255.255.255.0	ON	8.8.8.8

Wireless LAN(2.4GHz)

MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-69-87-C0	Europe	3.3	DrayTek

Wireless LAN(5GHz)

MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-69-87-C2	Europe	10.4-2.4.3.1008	DrayTek_5G

WAN

	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-1D-AA-69-87-C1	DHCP Client	---	---
WAN2	Disconnected	00-1D-AA-69-87-C2	DHCP Client	---	---
WAN3	Disconnected	00-1D-AA-69-87-C3	---	---	---
WAN4	Disconnected	00-1D-AA-69-87-C4	---	---	---

IPv6

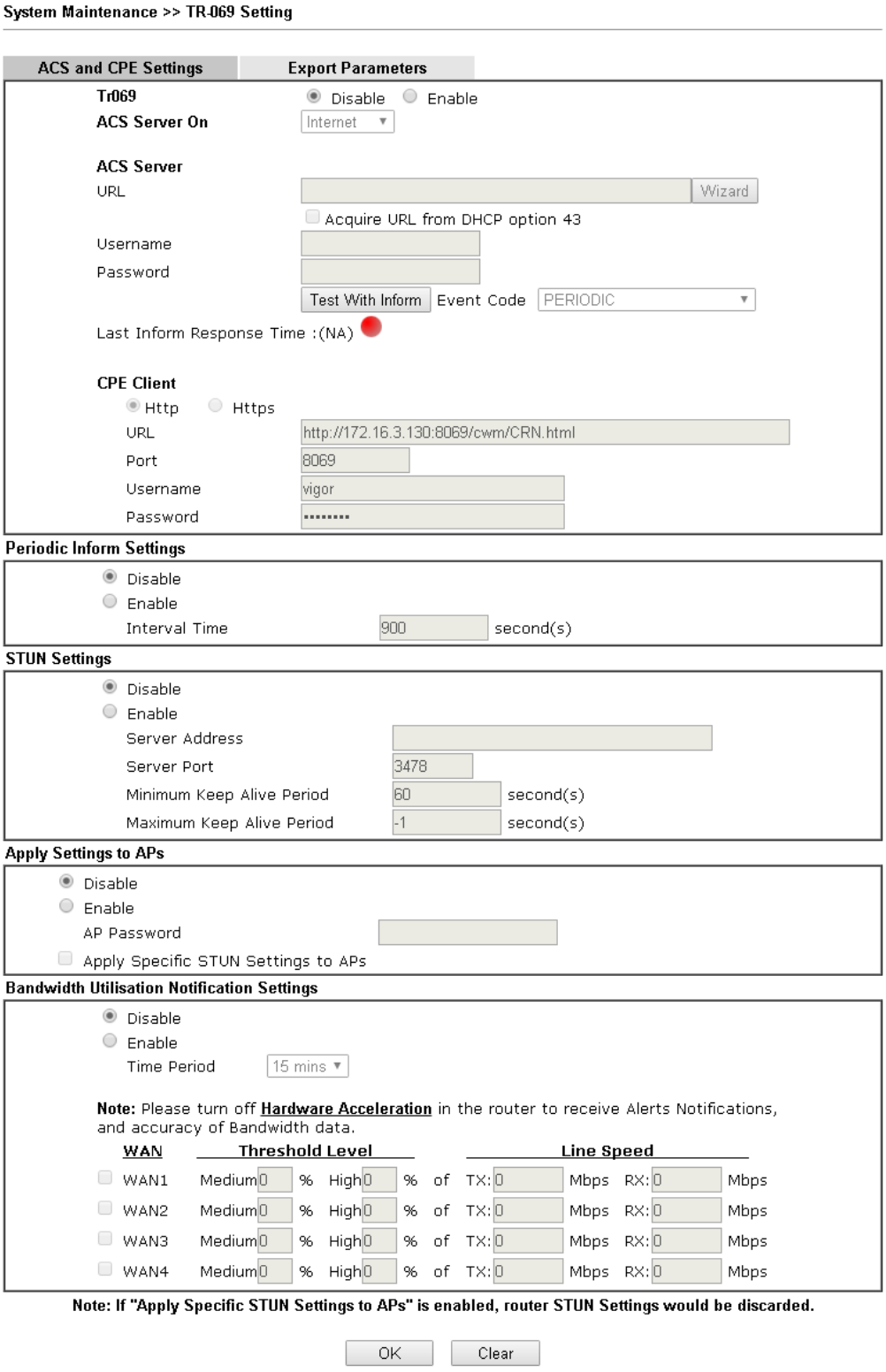
可用設定說明如下：

項目	說明
型號名稱(Model Name)	顯示路由器的型號名稱。
韌體版本(Firmware Version)	顯示路由器的韌體版本。
建立日期與時間 (Build Date/Time)	顯示目前韌體建立的日期與時間。
LAN	**MAC 位址(MAC Address)** - 顯示區域網路介面的 MAC 位址。 **IP 位址(IP Address)** - 顯示區域網路介面的 IP 位址。 **子網路遮罩(Subnet Mask)** - 顯示區域網路介面的子網路遮罩位址。 **DHCP 伺服器(DHCP Server)** - 顯示區域網路介面的 DHCP 伺服器目前的狀態。 **DNS** - 顯示主要 DNS 的 IP 位址。

無線網路(Wireless LAN)	**MAC 位址(MAC Address)** - 顯示無線區域網路的 MAC 位址。 **頻率網域(Frequency)** - 網域可以是歐洲(13 個可用頻道)，美國(11 個可用頻道)，無線產品所支援之可用頻道在不同的國家下是不相同的。 **韌體版本(Firmware Version)** - 表示配備 WLAN miniPCi 卡的詳細資訊，同時可以提供該卡相關的特徵訊息。 **SSID** - 顯示路由器的 SSID。
WAN	**連線狀態(Link Status)** - 顯示目前實體連線的狀態。 **MAC 位址(MAC Address)** - 顯示 WAN 介面的 MAC 位址。 **連線(Connection)** - 顯示目前連線的類型。 **IP 位址(IP Address)** - 顯示 WAN 介面的 IP 位址。 **預設閘道(Default Gateway)** - 顯示預設閘道指定的 IP 位址。
IPv6	**連線狀態(Link Status)** - 顯示目前實體連線的狀態。 **MAC 位址(MAC Address)** - 顯示 WAN 介面的 MAC 位址。 **連線(Connection)** - 顯示目前連線的類型。 **IP 位址(IP Address)** - 顯示 WAN 介面的 IP 位址。 **預設閘道(Default Gateway)** - 顯示預設閘道指定的 IP 位址。

VII-1-2 TR-069

此路由器支援 TR-069 標準，對管理人員來說透過 ACS (例如 VigorACS) 來管理 TR-069 裝置是相當方便的。



可用設定說明如下：

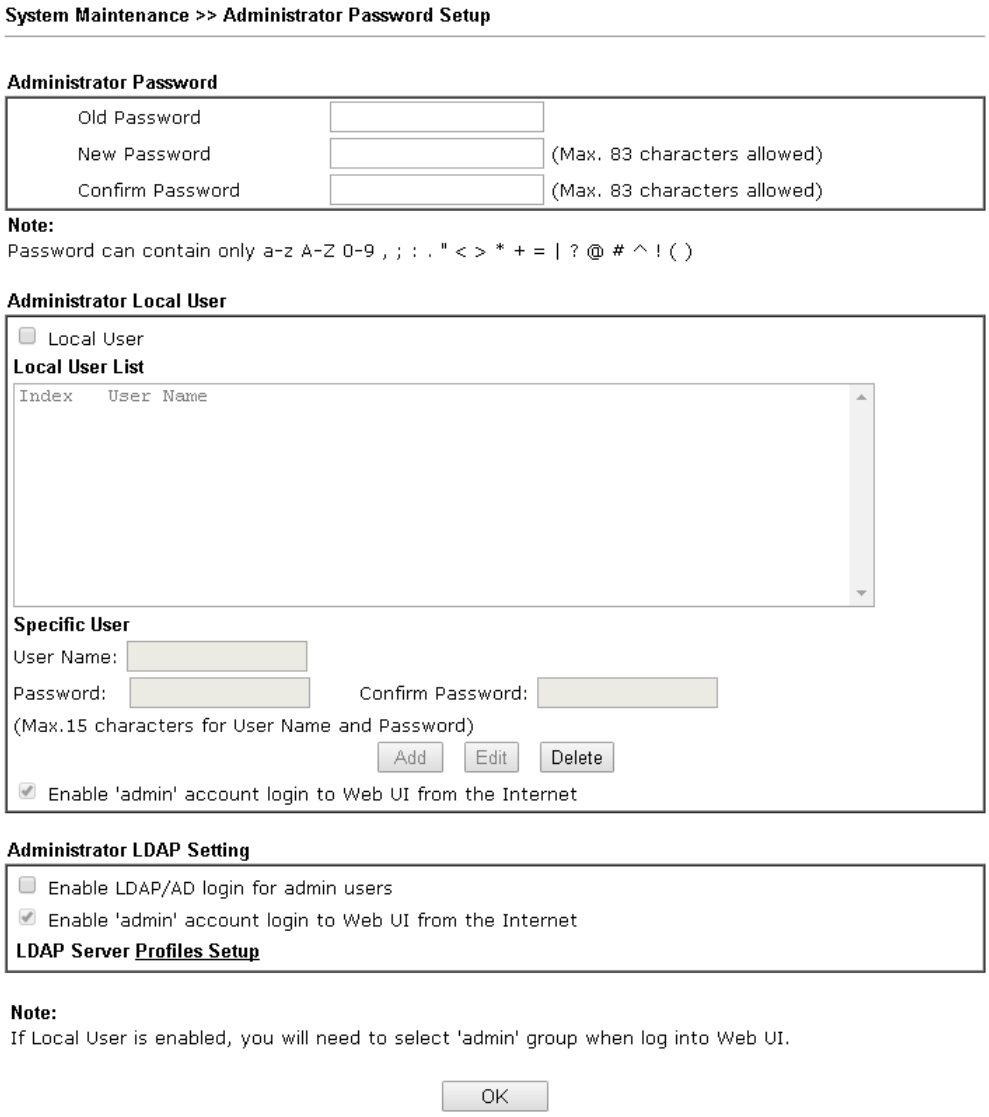
項目	說明
經此連往 ACS 伺服器 (ACS Server On)	選擇路由器連往 ACS 伺服器的介面。
ACS 伺服器 (ACS Server)	**URL/使用者名稱/密碼 (URL/Username/Password) –** 此資料必須依照您想要連結的 ACS 內容來輸入，請參考 ACS 使用者取得詳細的資訊。 **以資訊測試(Test With Inform)** –如果 CPE 能與 VigorACS SI 伺服器溝通，按此傳送以事件代碼選項爲基準的訊息進行測試。 **事件代碼(Event Code)** – 使用下拉式清單指定事件以應測試之需。 **上次通知回應時間(Last Inform Response Time)** – 顯示 VigorACS 伺服器上次接收 CPE 通知訊息並做出回應的時間。
CPE 用戶端 (CPE Client)	基本上您不需要在此輸入任何資料，因爲這邊的資料主要是提供給 ACS 伺服器參考使用的。 **啓用/停用(Enable/Disable)** – 有時候，系統可能會產生埠號衝突，爲解決這個問題，您可能需要改變 CPE 的埠號，請勾選**啓用**再變更埠號。 **埠號(Port)** – 有時候，埠號衝突是可能發生的，爲了解決這樣的困境，您可以替 CPE 變更不同的埠號值。 **使用者名稱與密碼(Username and Password)** – 輸入 VigorACS 用來登入此 CPE 所需之使用者名稱與密碼。
定期通知設定 (Periodic Inform Settings)	預設值爲**啓用(Enable)**，請設定間隔時間或是排程時間，讓路由器傳送通知訊息給 CPE 端，或是選**停用(Disable)**關閉通知機制。
STUN 設定 (STUN Settings)	預設值是**停用**，如果您選擇了**啓用**，請輸入下述相關資料： **伺服器 IP(Server IP) –** 輸入 STUN 伺服器的 IP 位址。 **伺服器埠號(Server Port) –** 輸入 STUN 伺服器的埠號。 **最小維持連線時間(Minimum Keep Alive Period) –** 如果啓用了 STUN，CPE 必須傳送綁定需求至伺服器，以便維持與閘道綁定的需要。請輸入數字作爲最小的維持時間，預設值爲 60 秒。 **最大維持連線時間(Maximum Keep Alive Period) –** 如果啓用了 STUN，CPE 必須傳送綁定需求至伺服器，以便維持與閘道綁定的需要。請輸入數字作爲最大的維持時間，數值-1 表示未指定最大維持時間。
套用設定至 AP (Apply Settings to APs)	啓用此項可讓 TR-069 設定同時套用到路由器管理下的全部 AP 上。 **停用(Disable)** – 相關設定不會套用到 AP 上。 **啓用(Enable)** – 上述 STUN 設定在按下**確定(OK)**之後會套用到 AP 上，啓用此功能之後，請輸入密碼以利後續登入 AP。 ● **AP 密碼(AP Password)** – 輸入您想套用路由器 TR-069 設定之 VigorAP 的登入密碼。 **套用指定 STUN 設定至 AP(Apply Specific STUN Settings to APs)** – 選擇**啓用(Enable)**後，若您僅想要套用 STUN 設定至 VigorAP 上以符合特殊需要，請勾選此框。接著分別輸入伺服器 IP 位址、伺服器埠號、最小維持連線時間與最大維持連線時間。
頻寬使用通知設定 (Bandwidth Utilisation	管理者可利用此功能監控 CPE 的頻寬利用，當頻寬利用超過門檻值時，系統會發佈通知訊息給 VigorACS，在觀察一段時間後，

Notification Settings)	管理者可以決定有無需要增加頻寬給予該 CPE。 **啓用(Enable)** – 點選此項啓用此功能。 **時間(Time Period)** – 選擇時間間隔(15 分鐘、30 分鐘、1 小時、3 小時或 6 小時)以傳送頻寬利用通知訊息予 VigorACS。 **WAN** – 選擇適合的 WAN 介面以便套用頻寬利用通知機制。 **門檻等級(Threshold Level)** – 設定傳輸與接收資料的頻寬百分比做爲判定的門檻值。 **線路速度(Line Speed)** – 制訂指定 WAN 介面的傳輸速率與接收速率。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

VII-1-3 系統管理員密碼(Administrator Password)

本頁允許您設定新的密碼。



可用設定說明如下：

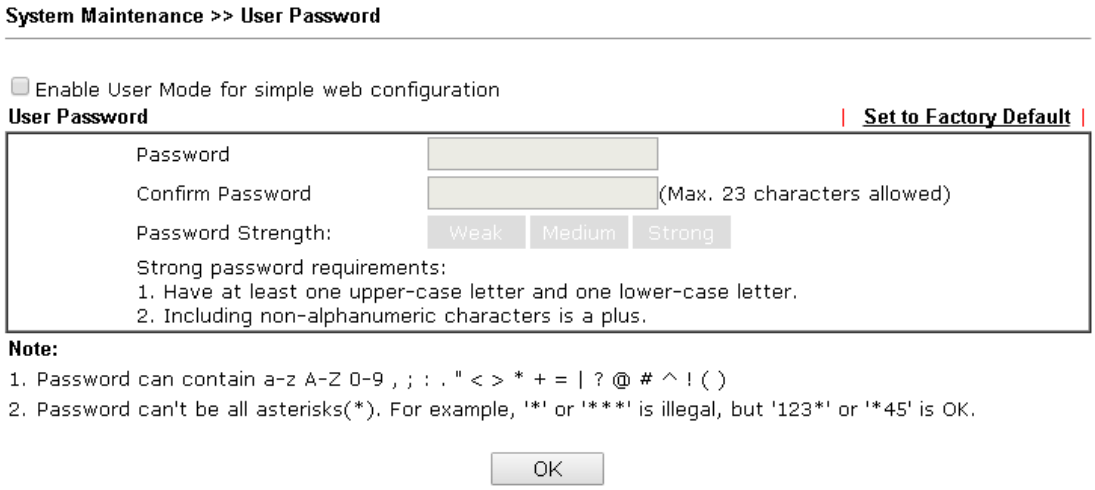
項目	說明
管理者密碼(Administrator Password)	**舊密碼(Old Password)** – 輸入舊的密碼，出廠預設值爲 **"admin"**。 **新密碼(New Password)** – 在本區輸入新的密碼，密碼長度限於 23 個字元。 **確認密碼(Confirm Password)** – 再次輸入新的密碼。
管理者本地使用者 (Administrator Local User)	管理者可以登入 Vigor 路由器的使用者介面，以修改設定符合實際的需要。此項功能讓 LAN 端其他的用戶具有管理者相同的權限，藉以登入路由器的使用者介面。 **本地使用者(Local User)** – 勾選此框啓用本地使用者設定。 **本地使用者清單(Local User List)** – 顯示本地使用者的名稱清單。

	使用者名稱(User Name) – 給予本地用戶之使用者名稱。 **密碼(Password)** – 輸入本地用戶的密碼。 **確認密碼(Confirm Password)** – 再次輸入本地用戶的密碼以確認。 **新增(Add)** – 輸入上述使用者名稱與密碼後，按下此鈕建立新的本地用戶，新的用戶名稱會立即顯示在本地使用者清單上。 **編輯(Edit)** – 如果不滿意上述清單內的某個使用者設定，選擇該名稱，進行修正然後按下此**編輯**按鈕即可更新相關設定資訊。 **刪除(Delete)** – 如果不滿意上述清單內的某個使用者設定，選擇該名稱，按下此**刪除**按鈕即可移除該使用者名稱。 **啓用自 WAN 端管理者登入(Enable 'admin' account login to Web UI from the Internet)** -預設值是啓動的，可確保任何使用者透過"admin/admin"的使用者名稱/密碼，登入 Vigor 路由器的使用者介面。
管理者 LDAP 設定 (Administrator LDAP Setting)	**啓用管理使用者之 LDAP/AD 登入(Enable LDAP/AD login for admin users)** – 若啓用此功能，任何一個使用者都能透過 LDAP 伺服器驗證方式登入路由器的網頁設定介面。 **啓用自 WAN 端管理者登入(Enable 'admin' account login to Web UI from the Internet)**-預設值是啓動的，可確保任何使用者透過"admin/admin"的使用者名稱/密碼，登入 Vigor 路由器的使用者介面。 **LDAP 伺服器設定檔(LDAP Server Profiles)** – 可用的設定檔將顯示在此區。 **設定檔配置(Profile Setup)** – 可讓您建立新的 LDAP 設定檔。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。後續若是離開了網頁設定介面，當您再度登入時，請使用新的密碼。

VII-1-4 使用者密碼(User Password)

本頁允許您設定新的密碼。



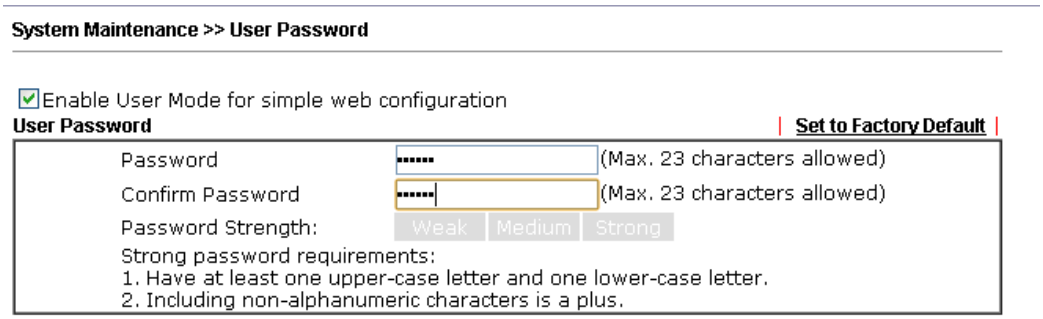
可用設定說明如下：

項目	說明
啓用使用者模式進行簡易網頁設定 (Enable User Mode for simple web configuration)	勾選此框之後，您可以透過此處輸入的密碼登入網頁使用者介面，進行簡易設定。 簡易網頁使用者介面的設定項目，與透過管理者密碼登入的完整使用者介面有些不同。
密碼(Password)	請在本區輸入新密碼。
確認密碼(Confirm Password)	再次輸入新密碼以確認。
密碼強度(Password Strength)	顯示上述指定的密碼其強度等級爲何。
回復出廠預設值(Set to Factory Default)	按此連結回復出廠預設值。

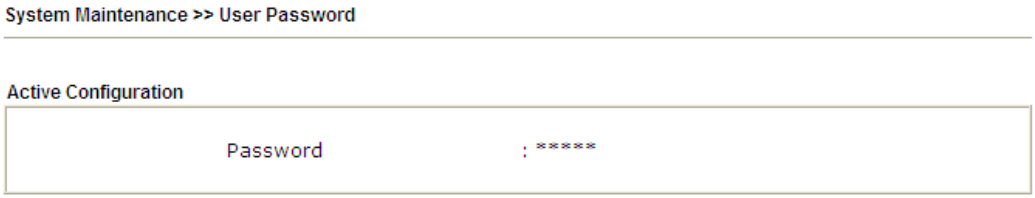
當您按下**確定(OK)**鍵後，登入視窗將會出現，請使用新的密碼以便再次存取網頁設定頁面。

1. 開啓**系統維護>>使用者密碼(System Maintenance>>User Password)**。

2. 勾選啓**用使用者模式進行簡易網頁設定(Enable User Mode for simple web configuration)**以便啓用使用者模式操作。在**密碼(Password)**與**確認密碼(Confirm Password)**欄位中輸入新的密碼，然後按下**確定(OK)**。



3. 下述畫面顯示出來後，按下**確定(OK)**。



4. 按**登出**按鈕離開 Vigor 路由器網頁使用者介面。



5. 接著如下視窗將會開啓要求輸入使用者名稱與密碼，輸入新的密碼然後按下**登入(Login)**。



6. 使用者模式的主要畫面顯示如下：

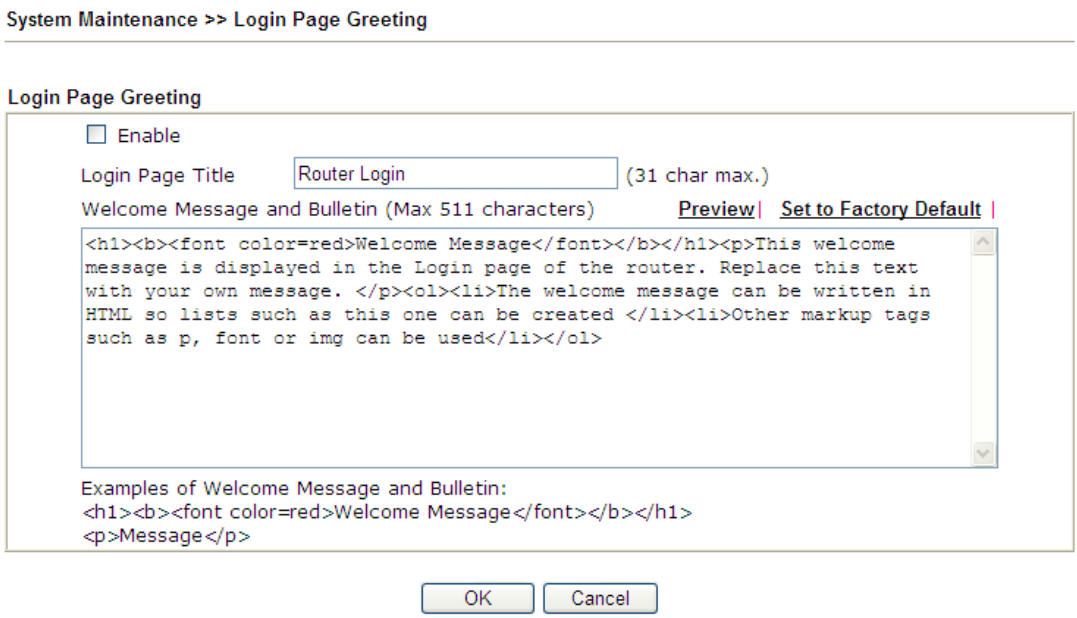


使用者模式中的設定少於管理者模式，只包含基本設定。

資訊	使用者模式中的設定方式如同管理者模式。

VII-1-5 登入頁面設定(Login Page Greeting)

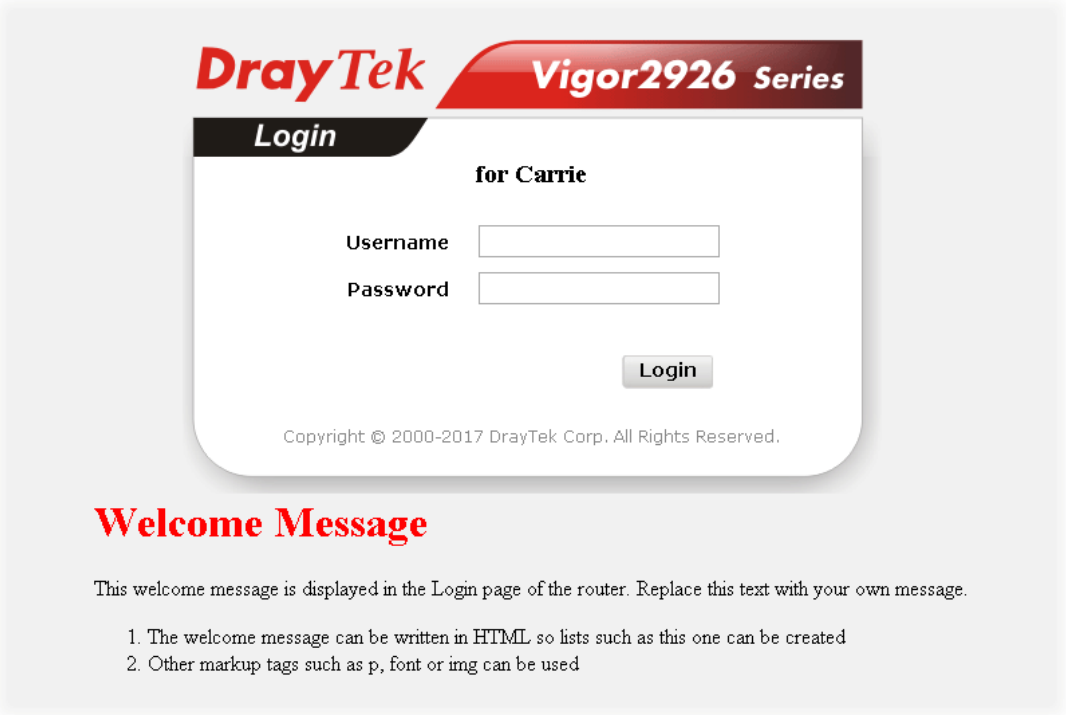
當您想要登入路由器的網頁使用者介面，系統將詢問您提供使用者名稱與密碼，登入視窗網頁的背景是空白且沒有標題在其上，如有需求本頁可讓您在登入視窗中指定登入 URL 以及標題。



可用設定說明如下：

項目	說明
啓用(Enable)	勾選此框啓用登入頁面客製化功能。
登入頁面標題 (Login Page Title)	輸入簡短說明(例如 Welcome to DrayTek)使其顯示在登入對話盒的標題上。
歡迎訊息與佈告欄 (Welcome Message and Bulletin)	輸入文字或文句，這些文字將會出現在佈告訊息欄中，此外，也可以顯示登入對話盒的下方。 注意您不可在此輸入 URL 重導向連結。
預覽(Preview)	按下此連結顯示以本頁設定爲基準的登入視窗的預覽畫面。
回復出廠預設值 (Set to Factory Default)	按下此連結回到出廠預設值。

下圖顯示客製化登入頁面範例：


DrayTek
Vigor2926 Series
Login
for Carrie
Username
Password
Login
Copyright © 2000-2017 DrayTek Corp. All Rights Reserved.
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

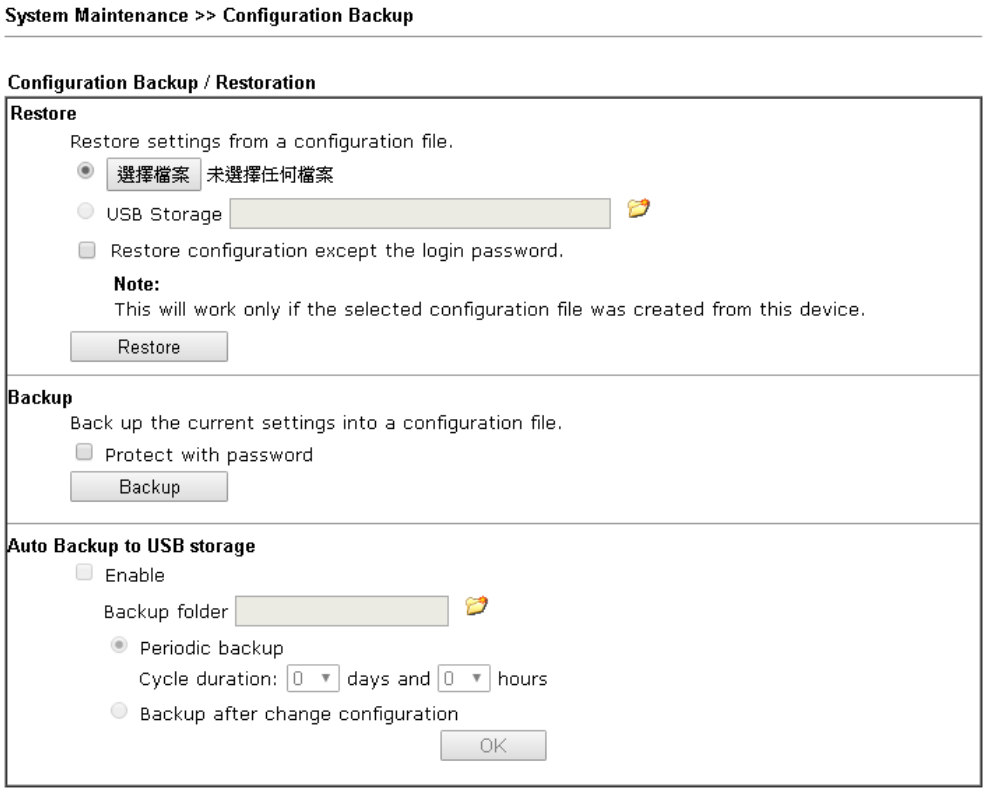
VII-1-6 設定備份(Configuration Backup)

此功能可以將 Vigor2925 上的路由器設定套用至此裝置。

設定備份

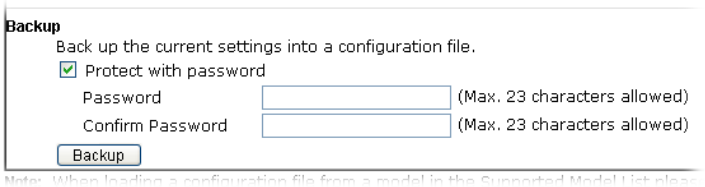
請依照下列步驟備份您的路由器設定。

1. 在**系統維護**群組中按**設定備份(System Maintenance >> Configuration Backup)**，您將可看見如下視窗。

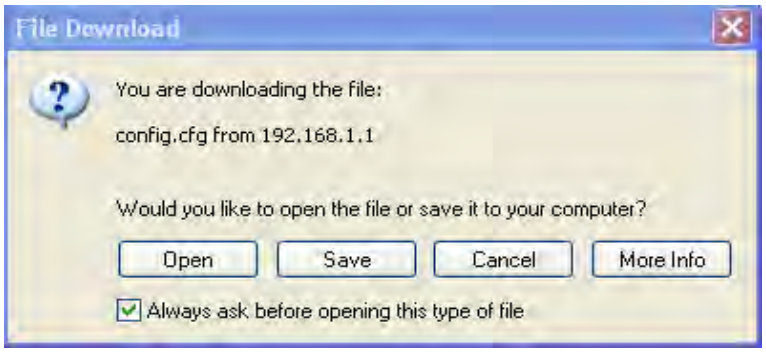


可用設定說明如下：

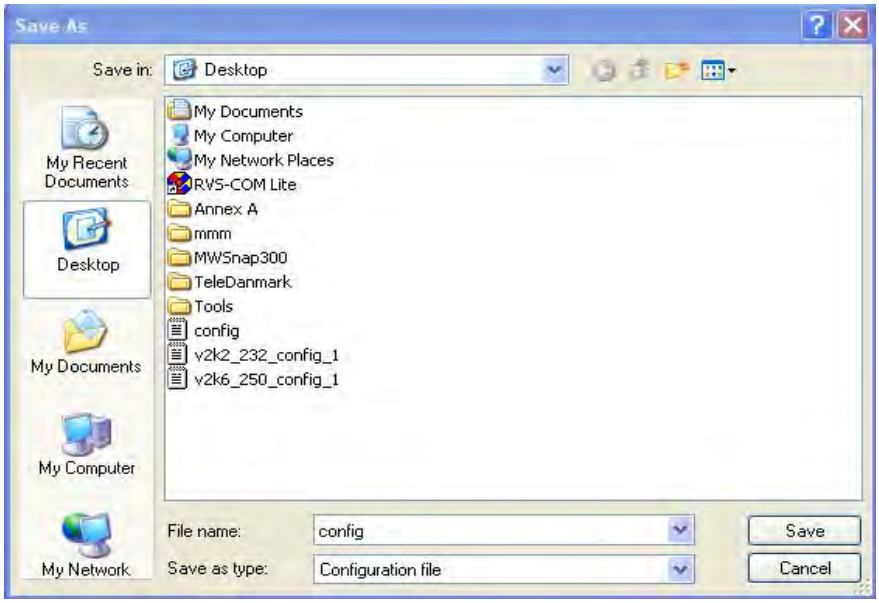
項目	說明
還原(Restore)	**選擇檔案/USB 儲存(Choose File /USB Storage)** – 點選此項以指定檔案還原。 **還原不含密碼的設定(Restore configuration except the login password) -** 若是密碼設定不得還原並套用至此裝置，請選擇此項已排除密碼設定。 按下**還原(Restore)**按鈕還原設定至此裝置，若檔案有加密，系統會詢問您輸入密碼以便解密該設定檔。
備份(Backup)	按下此按鈕進行設定備份。 **受密碼保護(Protect with password)-** 路由器的設定檔可以加密以因應安全性需要。

	 ● **密碼(Password)** – 輸入字元以便作爲解密設定檔之密碼。 ● **確認密碼(Confirm Password)** – 再次輸入密碼確認。
自動備份至 USB 儲存 (Auto Backup to USB sorage)	設定檔可以儲存連接至此裝置的 USB 磁碟上，做爲備份設定。 **備份檔案夾(Backup folder)** – 設定下載的路徑。 **定期備份(Periodicity backup)** – 設定備份的循環期間。 **變更設定之後備份(Backup after change configuration)** – 當設定檔一有變更，立刻採取備份動作。
支援型號清單 (Support Model List)	來自其他 Vigor 路由器(目前只有 Vigor2925)的網頁設定檔案可以套用到此裝置。 本區顯示此裝置能夠接受的路由器網頁設定檔的型號與韌體等資訊。

2. 按**備份(Backup)**按鈕進入下一個對話盒，按**儲存(Save)**按鈕開啓另一個視窗以儲存設定。



3. 在**另存新檔(Save As)**對話盒中，預設檔名爲 **config.cfg**，您也可以在此輸入不同的檔名。



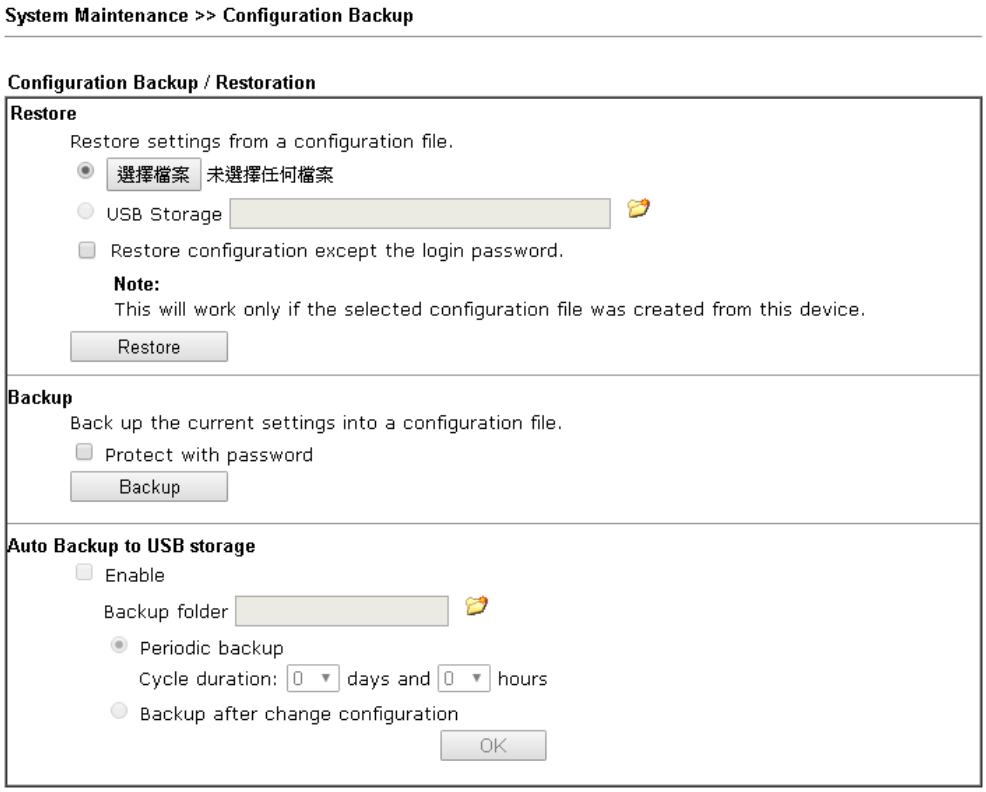
4. 按下**儲存(Save)**按鈕，設定將會以檔名 **config.cfg** 自動下載至電腦上。

上述範例是以 Windows 平臺來完成，對於 **Mac** 或是 **Linux** 平臺的用戶，螢幕上將會出現不一樣的視窗，但是備份的功能仍是有效的。

資訊	憑證備份須以另一種方式來儲存，備份設定並不包含憑證資訊。

還原設定

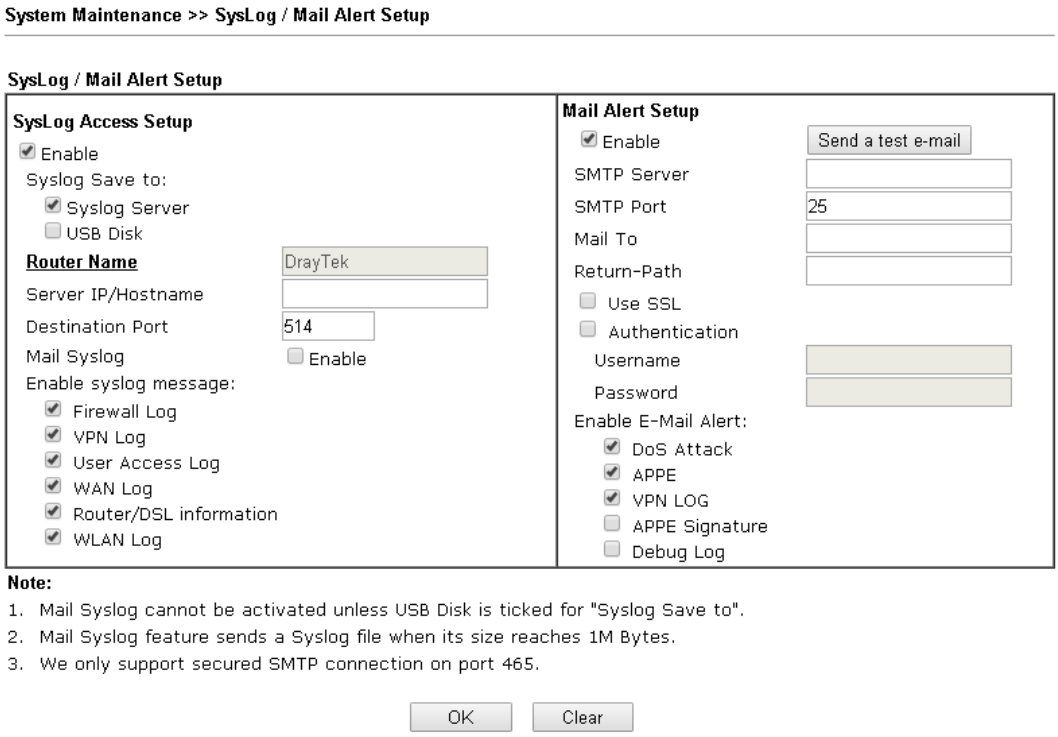
1. 在**系統維護**群組中按**設定備份(System Maintenance >> Configuration Backup)**，您將可看見如下視窗。



2. 按**選擇檔案(Select)**按鈕選擇正確的設定檔案，以便上傳至路由器。
3. 按**還原(Restore)**按鈕並等待數秒鐘。

VII-1-7 Syslog/郵件警示設定(Syslog/Mail Alert)

如果要監視路由器的運作狀態，您可以執行 SysLog 程式擷取路由器上所有的活動。此程式可以在本機電腦或是網際網路上任一遠端電腦上執行，此外 Vigor 路由器提供郵件警示功能，這樣 SysLog 訊息可以郵件方式打包寄給資訊管理人員。



可用設定說明如下：

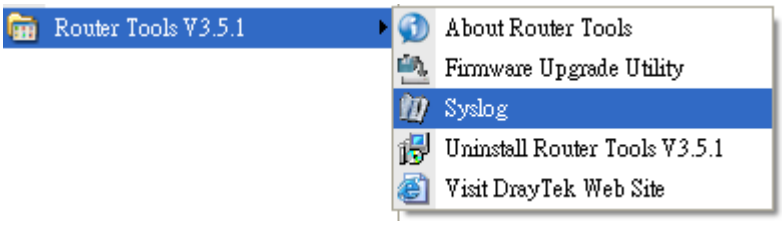
項目	說明
SysLog 存取設定 **(SysLog Access Setup)**	**啓用(Enable) -** 勾選**啓用(Enable)**以啓動系統記錄服務功能/啓動郵件警示功能。 **Syslog 儲存至(Syslog Save to)** – 勾選此框可儲存紀錄至 Syslog 伺服器中。 **USB 磁碟(USB Disk)** - 勾選此框可儲存紀錄至 USB 儲存碟中。
路由器名稱(Router Name)	顯示此路由器於**系統維護>>管理(System Maintenance>>Management)**頁面中設定的名稱。 若此處沒有名稱，請至**系統維護>>管理(System Maintenance>>Management)**設定路由器名稱。 **伺服器 IP 位址(Server IP Address)-**指定全部系統紀錄訊息傳送前往目的地之 IP 位址。 **目標通訊埠(Destination Port)**-指定全部系統紀錄訊息傳送前往目的地之通訊埠。 **郵件 Syslog(Mail Syslog) –** 勾選**啓用(Enable)**以便紀錄郵件事件至 Syslog 上。 **啓用 syslog 訊息(Enable syslog message)**-勾選此頁面上所列的小方塊，傳送防火牆、VPN、使用者存取、撥號、WAN、路由器/DSL 等資訊紀錄至 Syslog 上。

郵件警示功能設定 (Mail Alert Setup)	勾選**啓用(Enable)**以便啓動郵件警示功能。 **傳送測試郵件(Send a test e-mail)**-執行一個簡單的電子郵件測試，請於下方先指定郵件地址，然後在按此測試鈕，以檢查此電子郵件地址是否可用。 **SMTP 伺服器(SMTP Server/SMTP Port) -**指定 SMTP 伺服器的 IP 位址，直接傳送來自 Vigor 路由器的郵件至收信人的信箱。 **收件人(Mail To)-**指定收信人信箱的郵件位址，全部的系統紀錄訊息將會自動傳送至此處。收信人可以是想要檢視或是分析系統紀錄訊息的管理人員。 **回信位址(Return-Path)-**指定另一組信箱的郵件位址，接收因收信人信箱錯誤而造成發生失敗的所有回覆訊息。 **使用 SSL(Use SSL) -** 勾選此框使用埠號 465 作爲 SMTP 伺服器，讓電子郵件伺服器使用 HTTPS 作爲傳輸方式。 **驗證(Authentication)**-當使用電子郵件應用程式，勾選此方塊可啓動驗證的功能。 ● **使用者名稱(User Name)**-輸入驗證所需的使用者名稱。 ● **密碼(Password)**-輸入驗證所需的密碼。 **啓用郵件警告訊息(Enable E-mail Alert)**-勾選此方塊以便在路由器檢測到相關項目時，自動傳送警告訊息至郵件信箱。

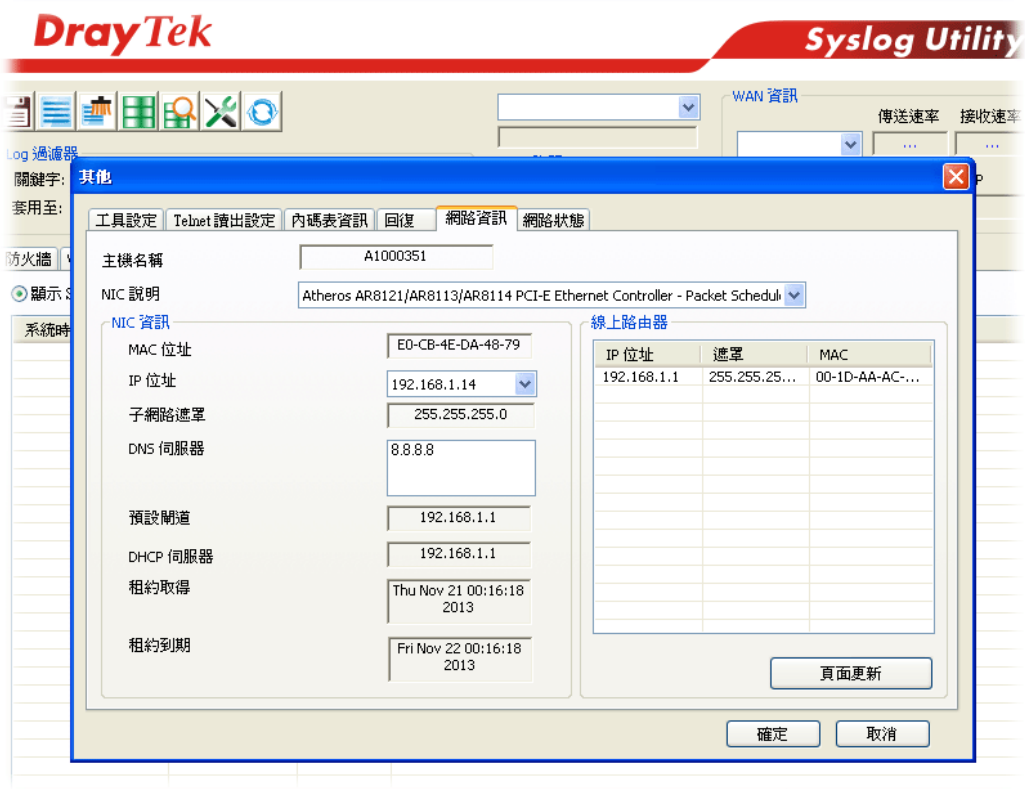
按**確定(OK)**儲存所有的設定。

如欲檢視系統紀錄，請依照下述步驟進行：

1. 請在伺服器 IP 地址中設定監視電腦的 IP 地址。
2. 安裝光碟片中 **Utility** 下的路由器工具，安裝完畢後，請自程式集選取 **Router Tools>>Syslog**。

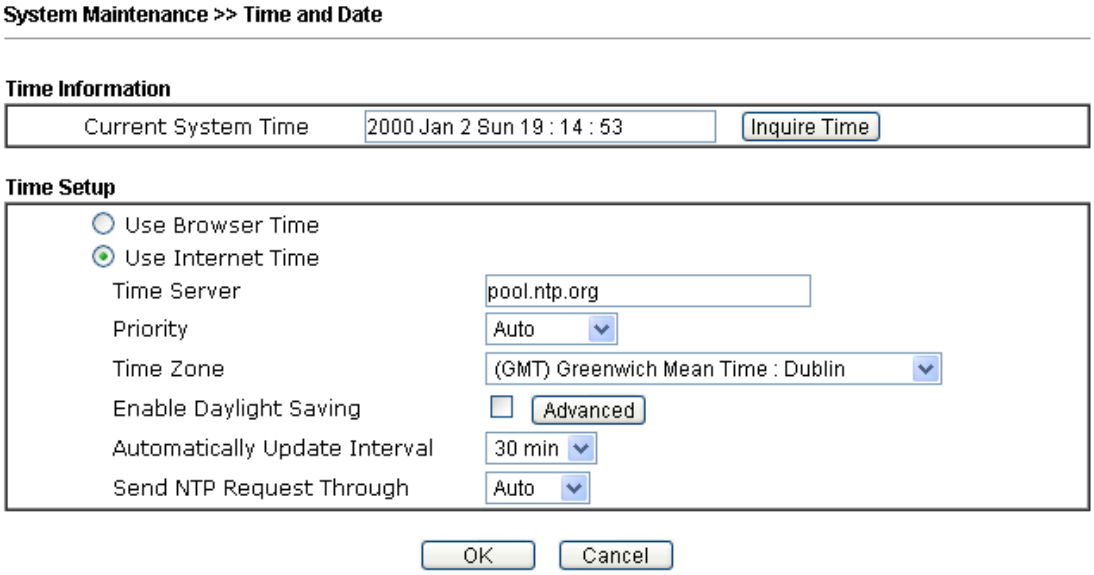


3. 自 Syslog 畫面上，選擇您想要監視的路由器。請記住在網路資訊(**Network Information**)中，選擇用來連接路由器的網路交換器，否則您無法成功檢索來自路由器的資訊。

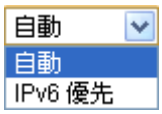


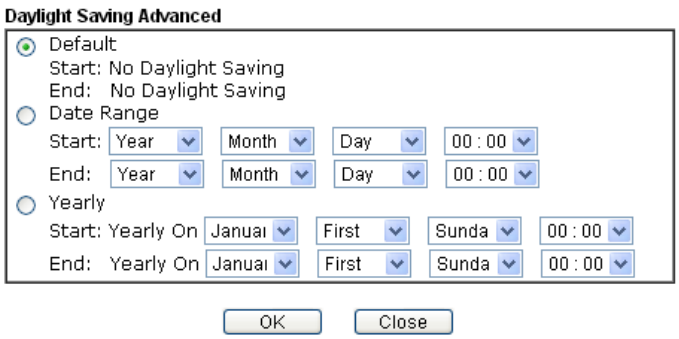
VII-1-8 時間和日期(Time and Date)

允許您指定自何處取得路由器時間。



可用設定說明如下：

項目	說明
目前系統時間 (Current System Time)	按**取得時間(Inquire Time)**按鈕取得目前時間。
使用本台 PC 的時間 (Use Browser Time)	選擇此項以便採用遠端管理者電腦上的瀏覽器時間。
使用網際網路的時間伺服器 (Use Internet Time)	選擇此項以便自網際網路上的時間伺服器選擇所需的時間資訊。
時間伺服器 (Time Server)	輸入時間伺服器所需的 IP 位址或網址。
優先權(Priority)	選擇**自動(Auto)**或是 **IPv6 優先(IPv6 First)**作爲優先選項。 
時區(Time Zone)	選擇路由器所在的時區。
啓動日光節約時間 (Enable Daylight Saving)	勾選此方塊啓動日光節約時間，在某些地區，這個項目是很有用處的。 **進階(Advanced)** – 按此鈕開起如下對話盒。

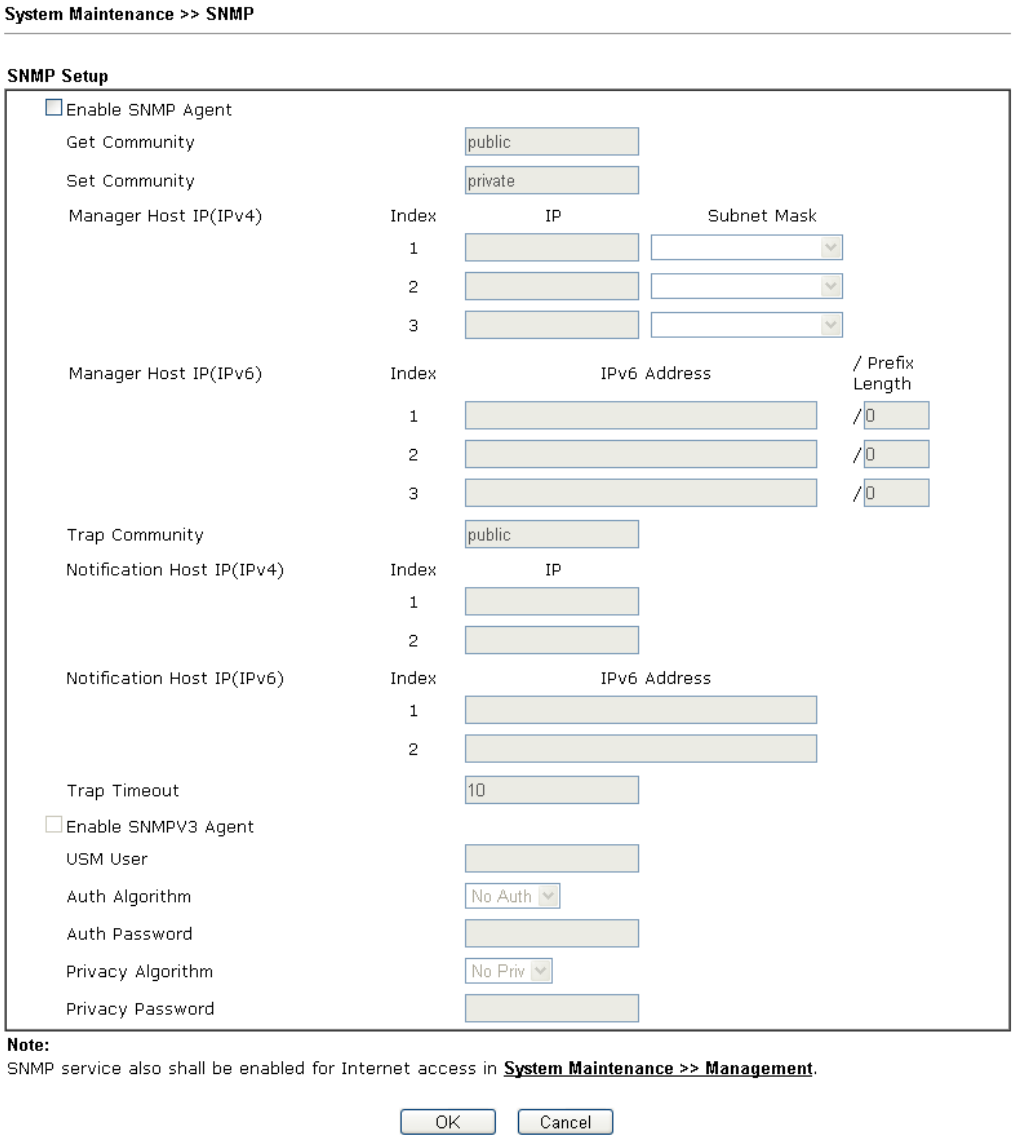
	 依照需要使用預設時間設定或是設定使用者定義時間。
自動更新間隔 (Automatically Update Interval)	選定時間間隔以供 NTP 伺服器更新之用。
傳送 NTP 需求經由(Send NTP Request Through)	指定 WAN 介面已傳送 NTP 需求進行時間同步化。

按**確定(OK)**儲存所有的設定。

VII-1-9 SNMP

本頁讓您設定 SNMP 與 SNMP3 服務的相關設定。

因應管理之需，利用加密(AES 與 DES)與驗證(MD5 與 SHA)二種方法，SNMPv3 比 SNMP 提供更安全的服務。



可用設定說明如下：

項目	說明
啓用 SNMP 代理程式 (Enable SNMP Agent)	勾選此項以啓動此功能。
取得社群 (Get Community)	請輸入適當的文字以設定取得社群名稱，預設名稱爲 **public**。
設定社群 (Set Community)	請輸入適當的名稱以設定社群，預設名稱爲 **private**。
管理者主機 IP (IPv4)	設定一台主機做爲管理者以便執行 SNMP 功能，請輸入 IP 位址(IPv4)指定特定主機。

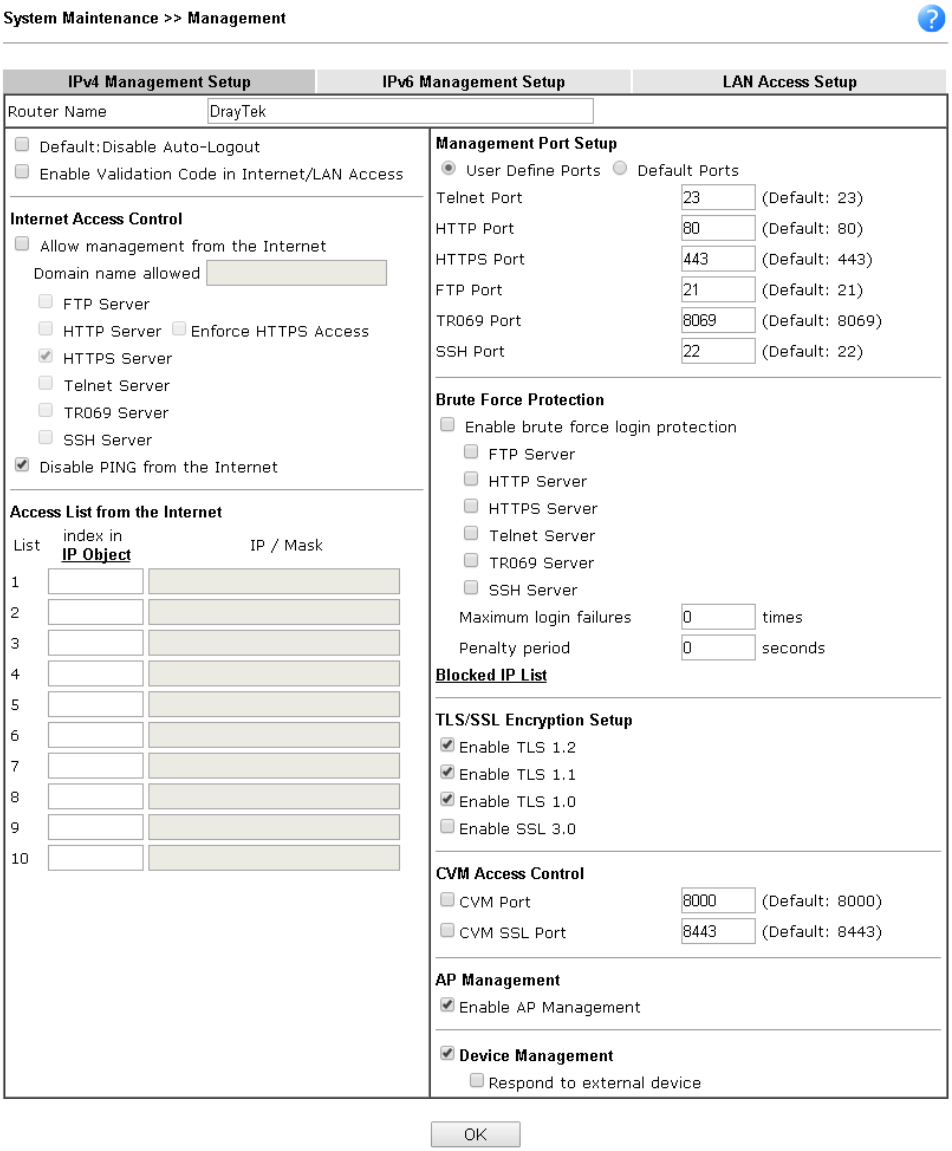
(Manager Host IP (IPv4))	
管理者主機 IP(IPv6) (Manager Host IP (IPv6))	設定一台主機做爲管理者以便執行 SNMP 功能，請輸入 IP 位址(IPv6)指定特定主機。
封鎖社群 (Trap Community)	輸入適當名稱設定封鎖社群，預設名稱爲 **public**。
通知主機 IP(IPv4) (Notification Host IP (IPv4))	設定主機的 IP 位址(IPv4)接收封鎖社群的資料。
通知主機 IP (IPv6) (Notification Host IP (IPv6))	設定主機的 IP 位址(IPv6)接收封鎖社群的資料。
封鎖逾時(Trap Timeout)	預設值爲 10 秒。
啓用 SNMPV3 代理 (Enable SNMPV3 Agent)	勾選此框啓用此功能。
USM 使用者(USM User)	USM 代表使用者爲主的安全模式。 輸入做爲驗證之用的使用者名稱。
驗證演算方式 (Auth Algorithm)	選擇下列任一種方式作爲驗證演算法。 
驗證密碼(Auth Password)	輸入驗證需求的密碼。
隱私演算方式 (Privacy Algorithm)	選擇下列任一種方式作爲隱私演算法。 
隱私密碼(Privacy Password)	輸入隱私需求的密碼。

按**確定(OK)**儲存所有的設定。

VII-1-10 管理(Management)

本頁讓您管理存取控制、存取清單以及通訊埠設定。例如管理存取控制時，埠號用來傳送/接收 SIP 訊息以便建立連線。

針對 IPv4



可用設定說明如下：

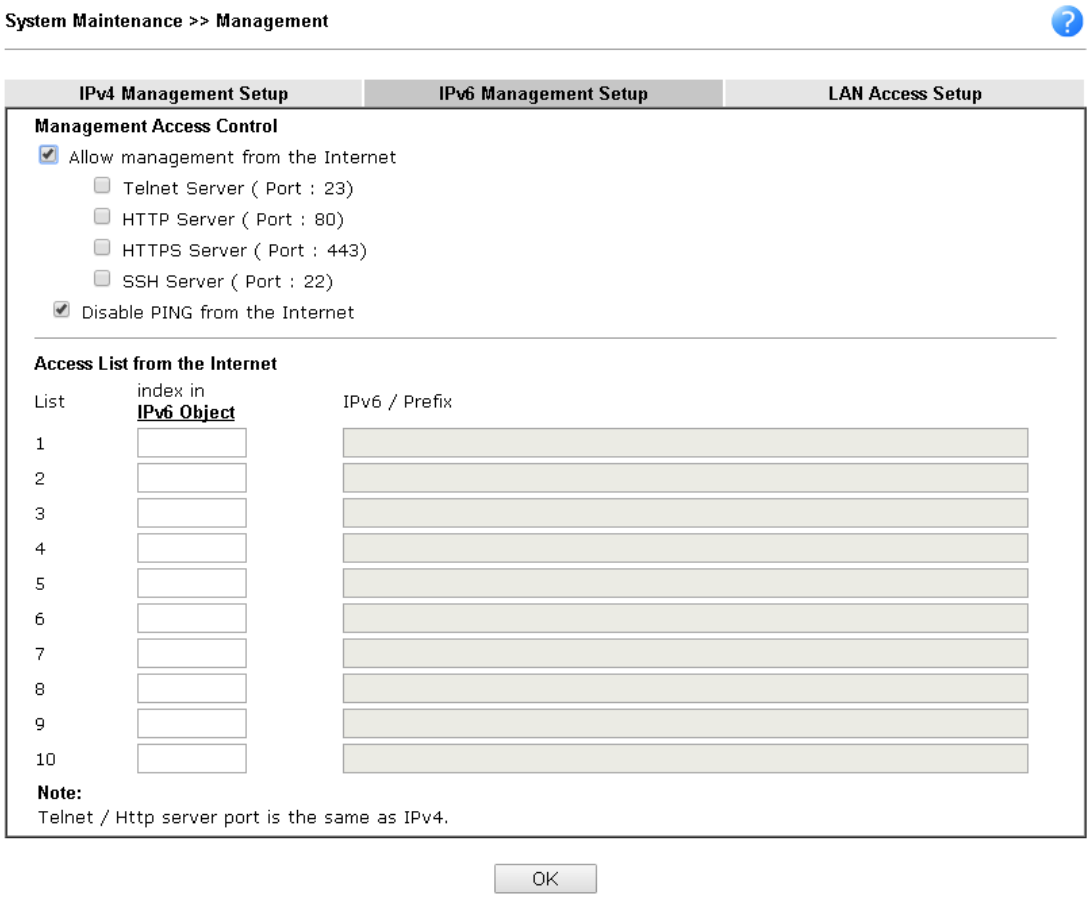
項目	說明
路由器名稱 (Router Name)	輸入路由器的名稱。
預設值：停用自動登出 (Default: Disable Auto-Logout)	若勾選此框，自動登出功能將被停止使用。 

	網頁使用者介面將會持續開啓直到按下手動登出爲止。 
啓用網際網路 LAN 存取之驗證代碼(Enable Validation Code in Internet/LAN Access)	若啓用此功能，路由器將會提供驗證代碼。用戶必須輸入此代碼才能獲准登入網際網路或是路由器的網頁使用者介面。
管理存取控制 **(Internet Access Control)**	**允許從網路管理(Allow management from the Internet) -**勾選此方塊允許系統管理者自網際網路登入。系統提供數種不同的伺服器供您選擇作爲網路管理介面，請勾選所需的項目。 **斷絕來自網際網路的 PING(Disable PING from the Internet) -** 勾選此方塊以退回所有來自網際網路的 PING 封包，考量到安全性問題，這項功能的預設值是啓動的。
存取清單 **(Access List from the Internet)**	您可以指定系統管理者只能從指定的主機或是清單定義的網路上登入，您一次最多可定義數個 IP/子網路遮罩於此區域中。 **IP 物件上的索引編號(index in IP Object)** - 輸入 IP 物件設定檔的索引編號，相關內容將立即呈現在清單內容上。
管理通訊埠設定 **(Management Port Setup)**	**使用者定義通訊埠(User Define Ports)-**勾選此項以指定使用者定義的埠號作爲 Telnet、HTTP 和 FTP 伺服器之用。 **預設通訊埠(Default Ports)-**勾選此項以使用標準埠號作爲 Telnet 和 HTTP 伺服器之用。
暴力攻擊防護(Brute Force Protection)	任何一個嘗試利用 Vigor 路由器登入網際網路使用者都會被要求必須通過使用者驗證程序。此功能可以讓路由器不會受到駭客使用各種字元直到發現正確的密碼組合而發動的網路攻擊。 **啓用暴力攻擊登入防護(Enable brute force login protection) -** 勾選此框啓用此功能。 **登入失敗最多次數(Maximum login failure) -** 用戶使用密碼登入，系統所能容忍的最多錯誤次數。 **罰期(Penalty period) -** 設定一段時期以便封鎖不斷嘗試通過使用者驗證但卻一再失敗的 IP 位址。當到達指定時間，路由器系統將會解所該 IP 並讓人重新使用該 IP 登入 Vigor 路由器。 **封鎖 IP 清單(Blocked IP List) -** 開啓另一個網頁顯示目前被封鎖的 IP 清單。
TLS/SSL 加密設定(TLS/SSL Encryption Setup)	**啓用 SSL 3.0 以及/或 TLS 1.0/1.1/1.2 (Enable SSL 3.0 & TLS 1.0/1.1/1.2) -** 勾選此框啓用 SSL 3.0 以及/或 **TLS 1.0/1.1/1.2** 功能。 鑒於安全考量，路由器內建 HTTPS 與 SSL VPN 伺服器已經更新至 TLS1.x 協定。如果您使用舊式瀏覽器(如 IE6.0) 或是舊版 SmartVPN Client，您可能需要啓用 SSL 3.0 來確保連線，但不建議如此進行。
CVM 存取控制(CVM Access Control)	**CVM 埠號(CVM Port) -** 勾選此框啓用此埠號設定。 **CVM SSL 埠號(CVM SSL Port) -** 勾選此框啓用此埠號設定。
AP 管理(AP Management)	**啓用 AP 管理(Enable AP Management) -** 勾選此框啓用**中央管理>>AP(Central Management>>AP)**功能，若未勾選，**中央管理>>AP(Central Management>>AP)**相關的設定選單將會隱藏

	起來。
裝置管理(Device Management)	勾選此框啓用裝置管理功能。 **回應外接裝置(Respond to external device) -** 若勾選此項，路由器將被視爲次要(slave)裝置，當外接裝置(主要裝置)傳送需求封包至路由器的時候，路由器將回傳資訊以回應外接裝置(可管理路由器)的詢問。

全部設定完成之後，請按**確定(OK)**儲存目前的設定。

針對 IPv6

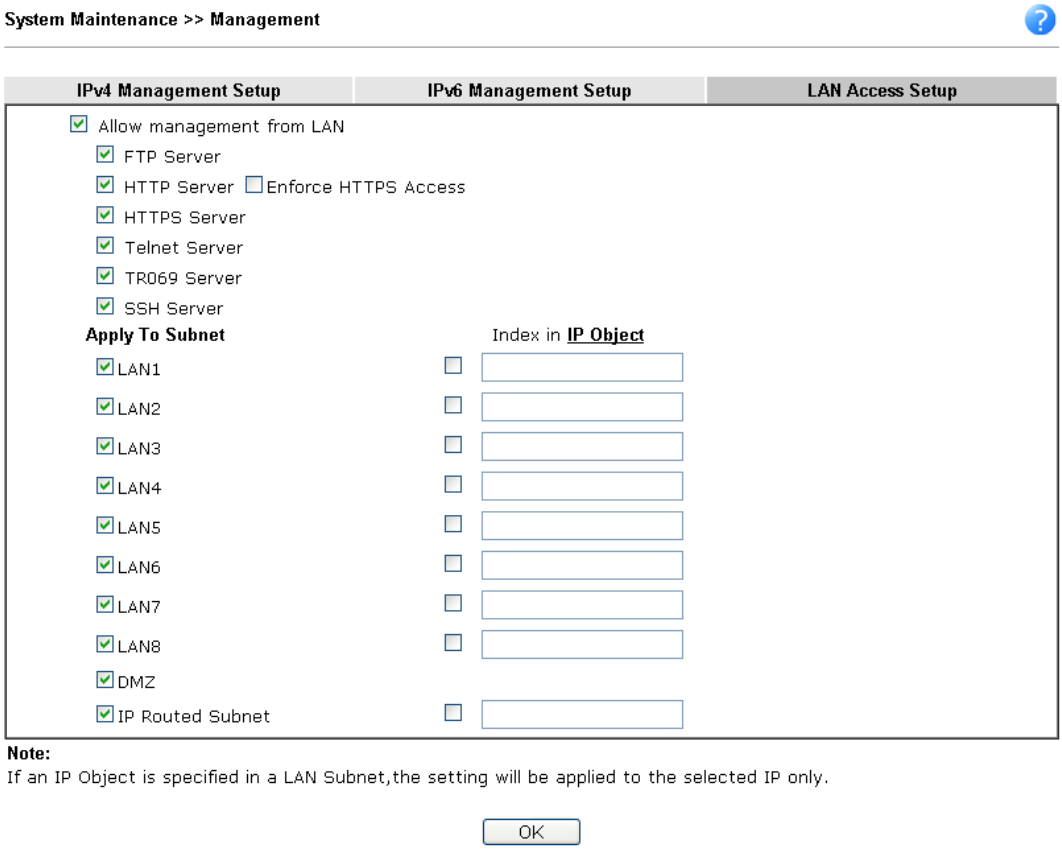


可用設定說明如下：

項目	說明
管理存取控制 (Management Access Control)	**允許從網際網路管理(Allow management from the Internet)** - 勾選下述方框可讓系統管理者自網際網路登入此路由器設定介面，有數種伺服器可以選擇讓您來管理。 **停用來自外部網際網路的 PING(Disable PING from the Internet)**- 勾選此方框可讓系統停止接受來自外部網際網路的封包檢測。
存取清單(Access List)	您可以指定系統管理者只能從特定主機或是網路登入。 **於 IPv6 物件之索引編號(Index in IPv6 Object)**- 輸入 IP 物件設定檔的索引編號，相關的 IP 位址即可自動顯示出來。

全部設定完成之後，請按**確定(OK)**儲存目前的設定。

For LAN



可用設定說明如下：

項目	說明
允許從 LAN 管理(Allow management from LAN)	勾選下述方框可讓系統管理者自 LAN 端登入此路由器設定介面，有數種伺服器可以選擇讓您來管理。
套用至子網(Apply To Subnet)	您可以指定系統管理者可以使用的 LAN 介面以便登入網頁使用者介面。 **於 IP 物件之索引編號(Index in IP Object)**- 輸入 IP 物件設定檔的索引編號，相關的 IP 位址即可自動顯示出來。

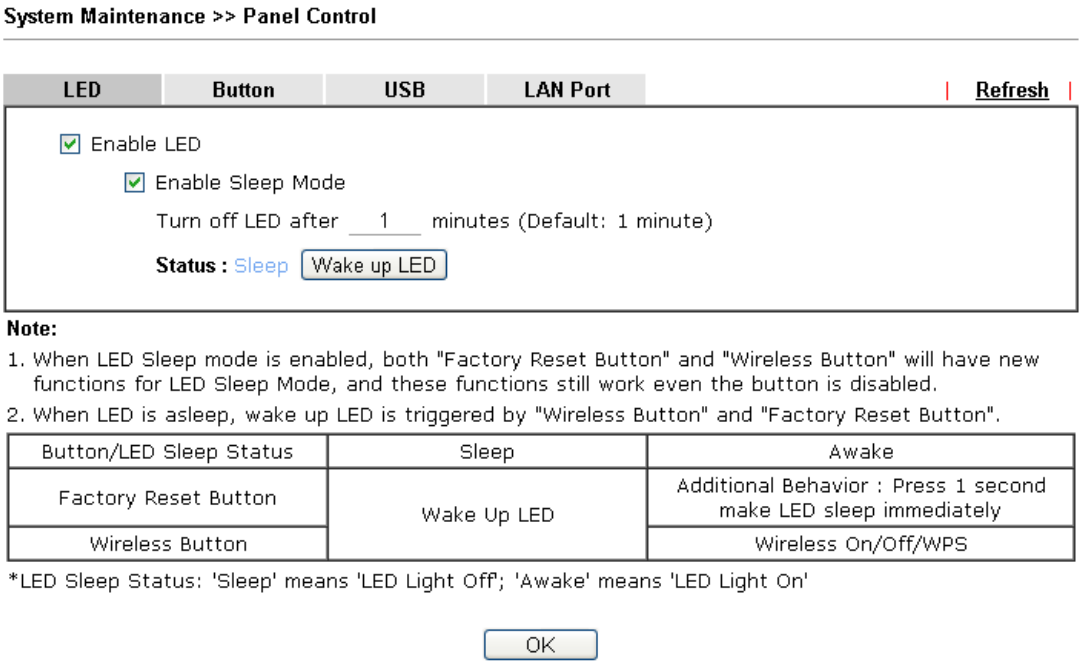
全部設定完成之後，請按**確定(OK)**儲存目前的設定。

VII-1-11 面板控制(Panel Control)

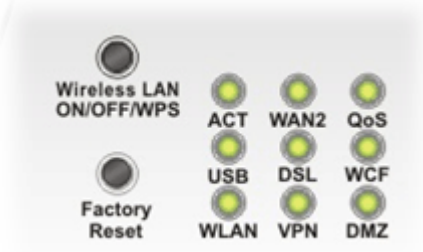
路由器前面板的 LED、按鈕、USB 埠口以及 LAN 埠口的行爲可以視實際需要調整開與關。

對於 LED

所有的 LED 在預設的情況下都是開啓的，也會持續的閃爍來顯示路由器各種功能的運作狀態。不過，這些 LED 燈號可以設定爲關閉狀態，直到按壓某個按鈕來喚醒燈號。



可用設定說明如下：

項目	說明
頁面更新(Refresh)	按此連結更新此頁面以顯示最新的訊息。
啓用 LED(Enable LED)	請勾選此項以便啓用前面板的 LED 燈號。 ● **啓用睡眠模式/關閉 LED 燈號在__分鐘後(Enable Sleep Mode/Turn off LED after _ minutes)** – 當勾選了啓用 LED 後，請選擇此項目並且設定需要的時間以便關閉 LED 燈號。 ● 當睡眠模式啓用時，可以利用按壓 **Wireless LAN ON/OFF/WPS** 按鈕，或前面板的 **Factory Reset** 按鈕，或是此頁面的**喚醒 LED(Wake up LED)**按鈕來喚醒燈號。而當 LED 燈號亮起時，只要按下 **Factory Reset** 按鈕或是此頁面的 **LED 立即睡眠(LED sleep immediately)**按鈕，就可以再度關閉 LED 燈號顯示。 
狀態(Status)	顯示 LED 燈號狀態。 **Status :** Sleep Wake up LED – LED 全都處於睡眠模式下，如果要喚醒燈號，可採取如下方式： ● 按下本頁面上的**喚醒 LED (Wake up LED)** 按鈕 ● 按下路由器前面板的 **Wireless On/Off/WPS** 按鈕 ● 按下路由器前面板的 **Factory Reset** 按鈕

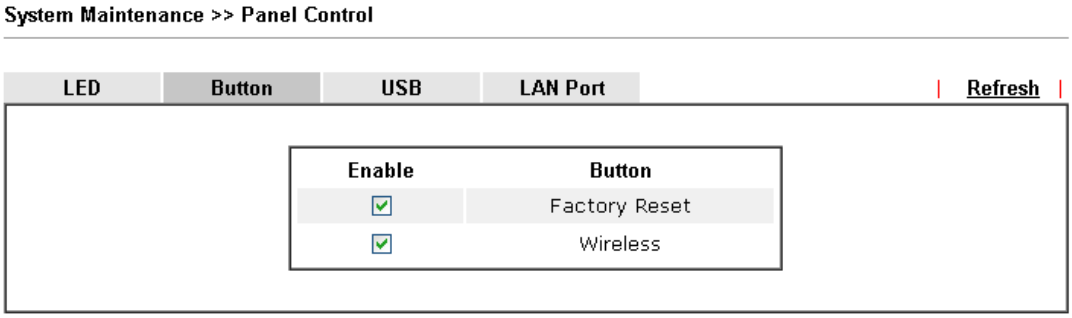
	Status : Awake, sleep after 1 minutes LED sleep immediately – LED 已被喚醒，如果要熄燈號，可採取如下方式： ● 按下本頁面上的 **LED 立即睡眠(LED sleep immediately)** 按鈕 ● 按下路由器前面板的 **Factory Reset** 按鈕 1 秒鐘

全部設定完成之後，請按**確定(OK)**儲存目前的設定。

對於按鈕

路由器前面板的 **Factory Reset** 與 **Wireless ON/OFF/WPS** 按鈕，預設值皆是啓用的，且若有需要可以將其停用。停用出廠預設值(Factory Reset)按鈕可防止被未授權的人竄改，或是防止按鈕用來喚醒 LED 時意外觸發路由器系統重啓。停用無線按鈕可在 LED 睡眠模式啓用時，防止變動到無線網路設定，這二個按鈕基本上都可以用來喚醒/熄滅 LED 燈號。

按下**按鈕(Button)** 標籤開啓如下頁面。



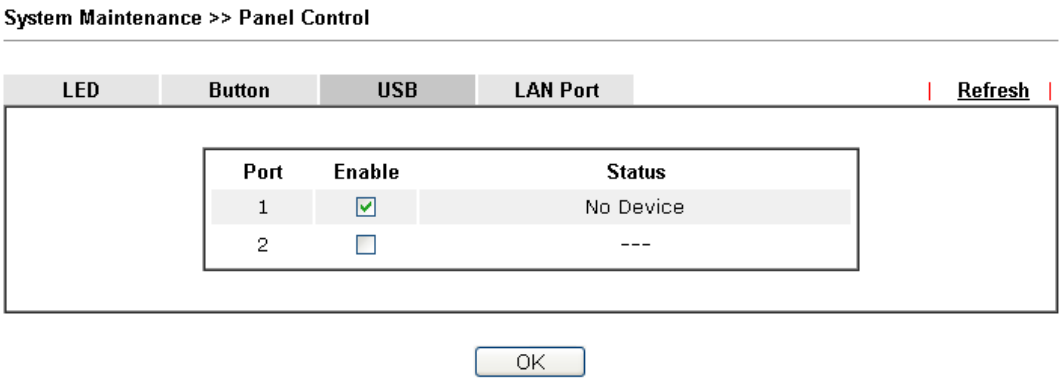
可用設定說明如下：

項目	說明
頁面更新(Refresh)	按此連結更新此頁面以顯示最新的訊息。
啓用出廠預設值按鈕	預設值是啓用的(勾選)。 取消勾選可以停用出廠預設值的系統重啓功能。 停用此按鈕僅可防止其被用來重新啓動路由器，按鈕仍然可以用來喚醒前面板的 LED 燈號(當 LED 睡眠模式啓用時)。
啓用無線網路按鈕	預設值是啓用的(勾選)。 取消勾選可以停用無線網路按鈕控制 WLAN 與 WPS 功能的能力。 停用此按鈕僅可防止其被用來控制 WLAN 功能，按鈕仍然可以用來喚醒前面板的 LED 燈號(當 LED 睡眠模式啓用時) 。

全部設定完成之後，請按**確定(OK)**儲存目前的設定。

對於 USB

USB 埠口可以個別啓用或是停用，當停用 USB 埠口的時候，路由器將無法辨認其上接的裝置。



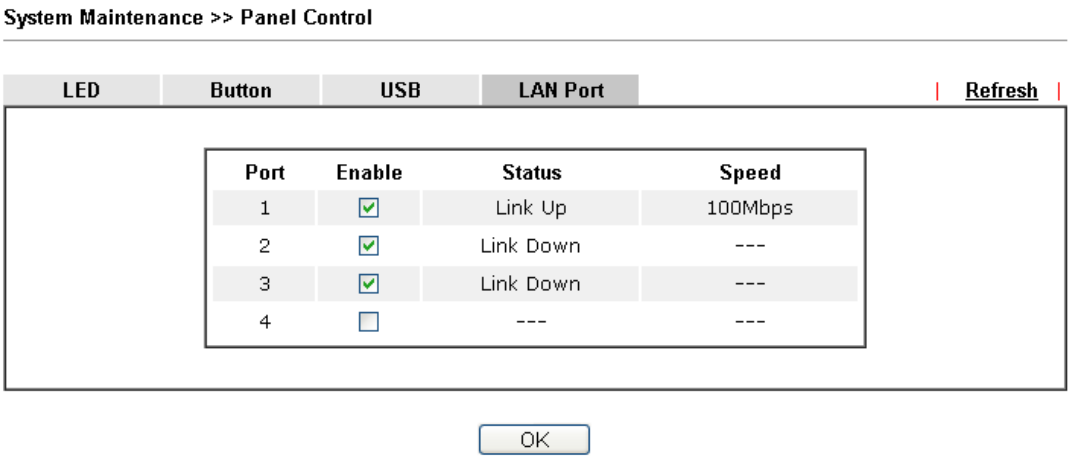
可用設定說明如下：

項目	說明
頁面更新(Refresh)	按此連結更新此頁面以顯示最新的訊息。
埠口(Port)	代表前面板顯示的 USB 埠口(1/2)。
啓用(Enable)	取消勾選可以停用 USB 埠口，預設值是啓用的。
狀態(Status)	顯示 USB 埠口的狀態。 **無裝置(No device)** – 沒有 USB 裝置插入該埠口。 **已連接(Connected)** – 有 USB 裝置插入該埠口。 **---** – USB 埠口已停用。

全部設定完成之後，請按**確定(OK)**儲存目前的設定。

對於 LAN 埠口

LAN 埠口可以個別啓用或是停用，當停用 LAN 埠口的時候，路由器將無法辨認其上接的裝置。



可用設定說明如下：

項目	說明
頁面更新(Refresh)	按此連結更新此頁面以顯示最新的訊息。
埠口(Port)	代表前面板顯示的 LAN 埠口(1/2/3/4)。
啓用(Enable)	取消勾選可以停用 LAN 埠口，預設值是啓用的。
狀態(Status)	顯示 LAN 埠口的狀態。 **Link Up** – 表示目前有乙太網路裝置連接至該埠口。

	Link Down – 表示目前尚未偵測到乙太網路裝置。 **---** – 顯示 USB 埠口的狀態。
速度(Speed)	顯示 LAN 埠口的協商速度。 **1000Mbps** – LAN 埠口的協商速度爲 1000 Mbps。 **100Mbps** – LAN 埠口的協商速度爲 100 Mbps。 **10Mpbs** – LAN 埠口的協商速度爲 10 Mbps。 **---** – LAN 埠口已停用或是沒有任何裝置連接上。

全部設定完成之後，請按**確定(OK)**儲存目前的設定。

VII-1-12 自行簽核憑證(Self-Signed Certificate)

自行簽核憑證是裝置(如 Vigor 路由器)的獨特身分辨識，是由裝置自行產生的憑證以確保路由器的安全性，此自行簽核憑證是以路由器擁有的私鑰來自行簽署。

自行簽核憑證可套用在 SSL VPN, HTTPS 等等，此外，此憑證可以透過各種工具免費產生。



按下**重新產生(Regeneration)**按鈕開啓重新自我簽核憑證**(Regenerate Self-Signed Certificate)**視窗，接著輸入所有相關的資訊，後續按下**產生(GENERATE)**即可。

System Maintenance >> Regenerate Self-Signed Certificate

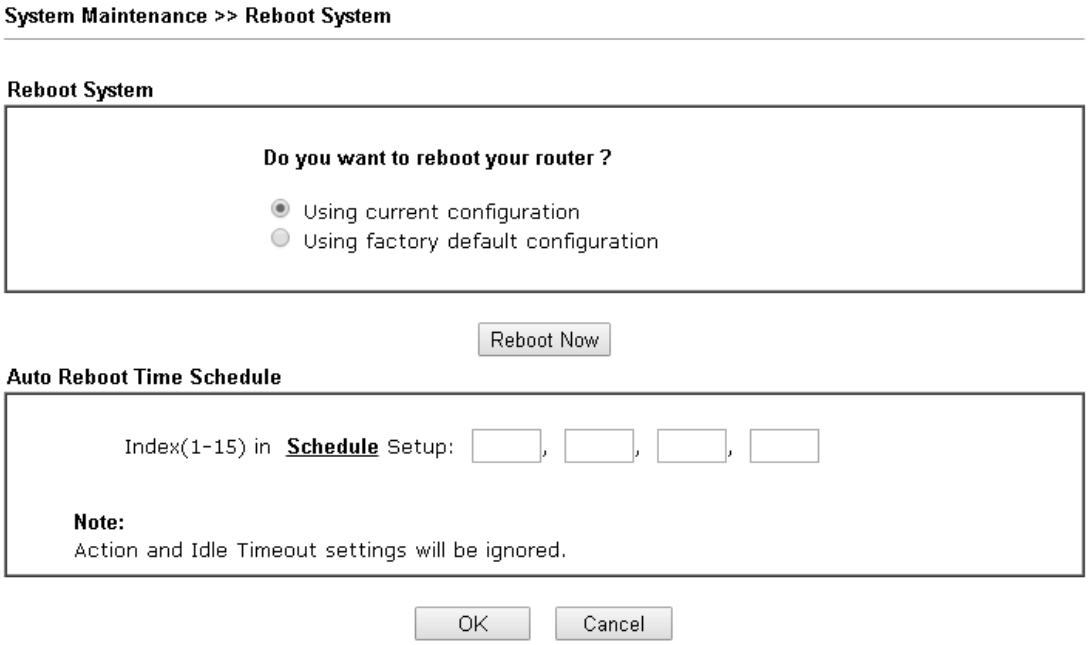
Regenerate Self-Signed Certificate

Certificate Name	**self-signed**
Subject Alternative Name	
Type	IP Address
IP	
Subject Name	
Country (C)	
State (ST)	
Location (L)	
Organization (O)	
Organization Unit (OU)	
Common Name (CN)	
Email (E)	
Key Type	RSA
Key Size	2048 Bit

Generate

VII-1-13 重啟路由器(Reboot System)

此頁面可用來重新啓動路由器，請自**系統維護(System Maintenance)**中按**重啓路由器(Reboot System)**開啓如下頁面。



索引編號(1-15)於排程設定(Index (1-15) in Schedule Setup) - 您可以輸入四組排程設定檔進行系統重啓作業，所有的排程都可以在**其他應用>>排程(Applications >> Schedule)**頁面中先行設定。

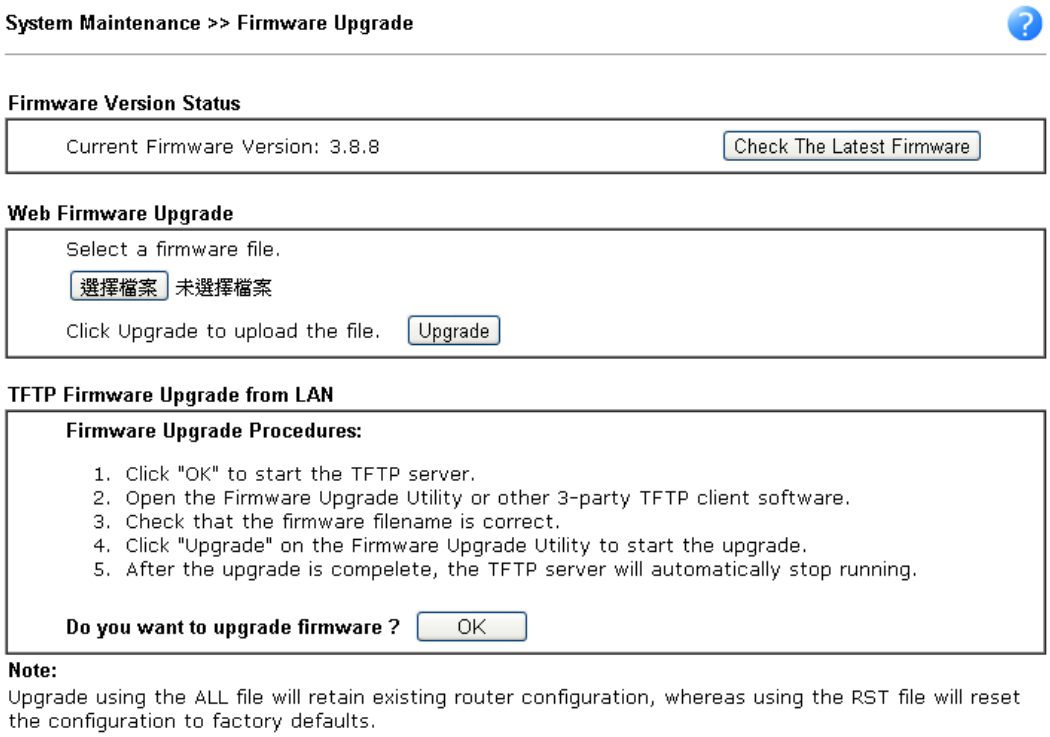
如果您想要使用目前的設定來重新啓動路由器，請勾選**使用目前組態(Using current configuration)**，然後按**立即重啓(Reboot Now)**；如果要重設路由器設定回復成爲預設值，請勾選**使用原廠預設組態(Using factory default configuration)**，然後按**立即重啓**，路由器將會花 5 秒重新啓動系統。

資訊

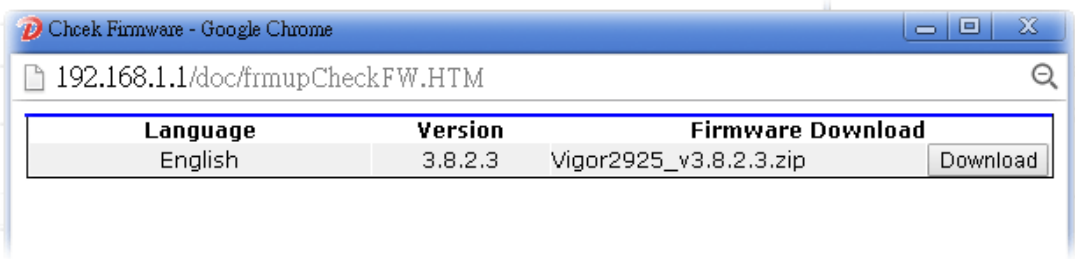
當系統在您完成網頁設定並跳出**重啓路由器(Reboot System)**網頁後，請務必按下**立即重啓(Reboot Now)**以重新啓動路由器，這個動作可以確保系統的操作正常，且可避免未來發生不預期的錯誤。

VII-1-14 韌體升級(Firmware Upgrade)

請自**系統維護**選擇**韌體升級(System Maintenance>> Firmware Upgrade)**以便啓動韌體更新工具。



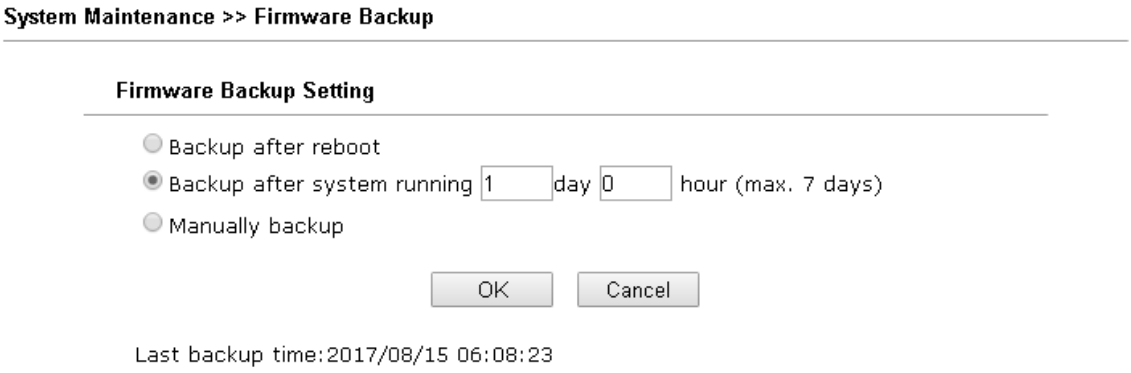
按下**檢查最新韌體(Check The Latest Firmware)**按鈕，系統會跳出視窗顯示此路由器目前最新的韌體版本爲何。



選擇您需要的版本然後按**下載(Download)**，之後按下**選擇(Select)**以指定剛下載的檔案，接著按**更新(Upgrade)**，系統將會自動更新路由器韌體。

VII-1-15 韌體備份(Firmware Backup)

路由器韌體可以儲存在電腦主機做爲備份韌體，之後若路由器因韌體錯誤而造成毀損，就可套用此備份韌體讓路由器恢復正常運作。



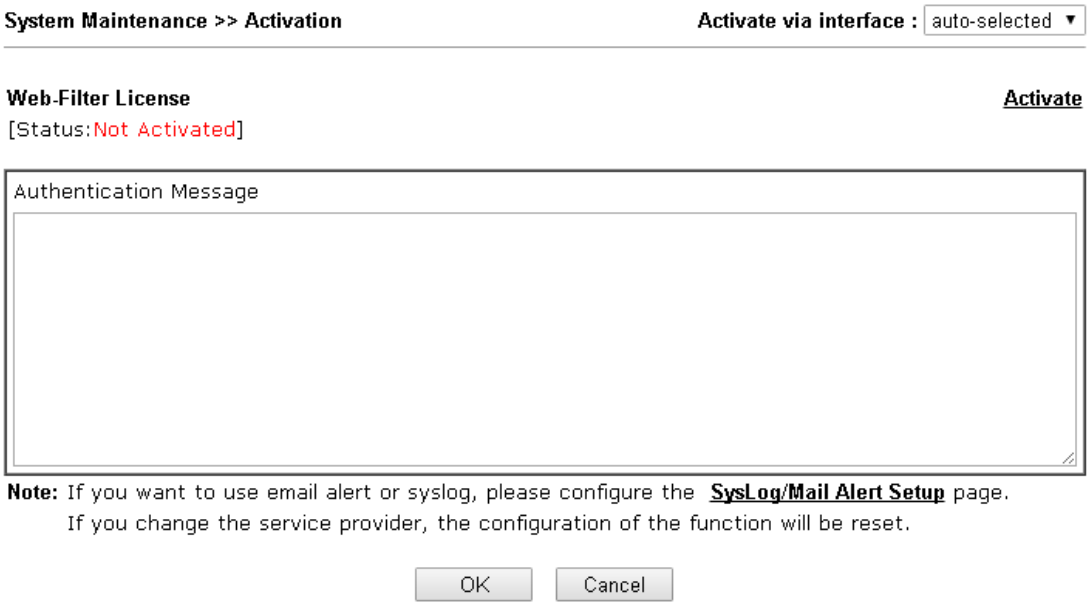
請指定備份條件運作韌體備份，然後按下**確定(OK)**按鈕儲存設定。

VII-1-16 開啟授權碼(Activation)

有三種方式可開啓 Vigor 路由器的網頁內容過濾器服務(WCF)，使用**服務啓動精靈(Service Activation Wizard)**、透過**數位內容安全管理>>網頁內容過濾器設定檔(CSM>>Web Content Filter Profile)**或是透過**系統管理>>開啓授權碼(System Maintenance>>Activation)**。

在您完成 WCF 設定檔之後，您即可啓動網頁內容過濾服務機制。

按**系統管理>>開啓授權碼(System Maintenance>>Activation)**開啓下述頁面以登入 http://myvigor.draytek.com。



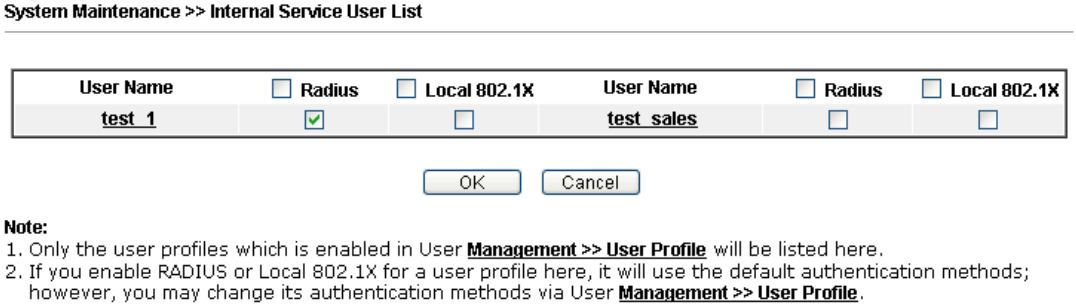
可用設定說明如下：

項目	說明
啓動經由介面(Activate via Interface)	選擇任何一種介面用以啓動網頁內容過濾器。
啓動(Activate)	此連結可讓您登入 www.myvigor.com 完成帳號與路由器的啓動作業。
驗證訊息(Authentication Message)	至於網頁過濾器的驗證資訊，驗證過程會顯示在此框中供您參考。

VII-1-17 內部服務使用者清單(Internal Service User List)

本頁顯示於**使用者管理>>使用者設定檔(User Management>>User Profile)**中所定義的使用者設定檔。

此頁允許您針對使用者設定檔(無需登入使用者管理設定頁面)開啓或關閉安全性驗證服務(由內部 RADIUS 與/或本機 802.1X 提供)。



可用設定說明如下：

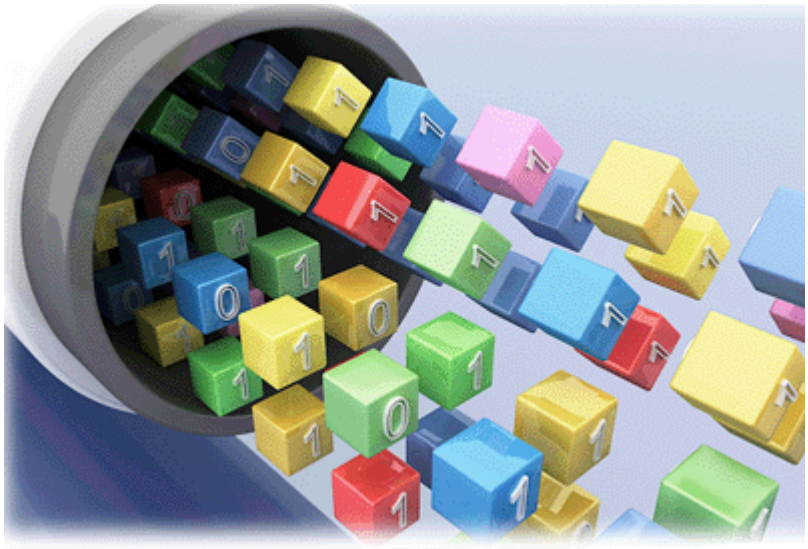
項目	說明
使用者名稱(User Name)	顯示已存在之使用者設定檔，如要修改細部設定內容，只要點下使用者名稱連結就可登入設定頁面。
Radius	勾選/取消勾選此框可啓用/停用內部 RADISU 伺服器提供的安全性驗證服務。 如果勾選項目旁之方塊，列於本頁之全部的使用者設定檔即可同時啓用。
本機 802.1X(Local 802.1X)	勾選/取消勾選此框可啓用/停用本機 802.1X 伺服器提供的安全性驗證服務。 如果勾選項目旁之方塊，列於本頁之全部的使用者設定檔即可同時啓用。

資訊

有關詳細的內部 RADIUS 設定內容，請參考**其他應用>>RADIUS/RACACS+(Applications>>RADIUS/TACACS+)**。

有關詳細的本機 802.1X 設定，請參考 **LAN>>有線 802.1X(LAN>>Wired 802.1X)**以及 **LAN>>安全性設定(LAN>>Security)**。

VII-2 頻寬管理(Bandwidth Management)



頻寬管理

擁有虛擬 IP 的電腦可以透過 NAT 路由器存取網際網路，針對此連線需求路由器將會產生 NAT 連線數的紀錄，P2P (Peer to Peer)應用程式(如 BitTorren)經常需要很大的連線數來處理，同時也會佔據很大的資源空間，造成重要的資料存取動作受到嚴重的影響。爲瞭解決這種問題，您可以使用連線數限制來限制指定主機的連線數。

頻寬限制

從 FTP,HTTP 或是某些 P2P 應用程式的下行或上行資料會佔據很大的頻寬，並影響其他程式的運作。請使用限制頻寬讓頻寬的應用更有效率。

服務品質(QoS)

QoS (Quality of Service)管理部署可確保所有應用程式能夠接收到所需的服務以及足夠的頻寬，符合用戶所期待的效果，此項控制對現代企業網路來說是相當重要的觀點。

使用 QoS 的理由之一是很多 TCP 爲主的應用程式嘗試不斷增加其傳輸速率，導致消耗掉全部的頻寬，我們稱之爲 TCP 慢速啓動。如果其他的應用程式未受 QoS 的保護，那麼他們在擁擠的網路中將會降低效能，對那些無法忍受任何損失、延遲的功能像是 VoIP、視訊會議以及流動影像來說，這項控制尤其必要。

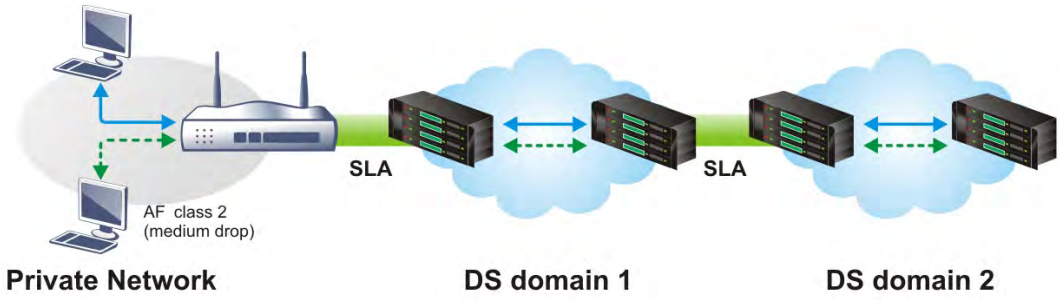
另一個理由是由於網路的擁擠狀況，內部連線迴路速度不符合或是傳輸流量過份聚集，資料封包排隊等候傳送，整個傳輸慢了下來。如果沒有定義後先後順序，以指定在滿檔的隊伍中哪個封包必須丟棄，上述提及的應用程式封包就可能成爲被捨棄掉的一個，這樣的話對應用程式的成效會造成令人無法想像的後果。

在基本設定中有二個元件要注意：

- 分類: 可辨識低潛在因素或是重要的應用程式，並標示這些程式爲高優先權服務等級，以便在網路中能夠強迫執行。
- 排定計畫: 以服務等級分類爲基礎來指定封包排列順序以及整合的服務型態。

基本 QoS 應用是以 IP 封包頭中之服務類型資訊爲基礎來分類及規劃封包，例如爲了確保封包頭之連線，電信工作人員在執行大量運作時，可能會強迫一個 QoS 控制索引保留頻寬予 HTTP 連線。

Vigor 路由器作爲 DS 管理之終端路由器，應該檢查通過流量之 IP 封包頭中標記 DSCP 之數值，這樣才可分配特定資源數量來執行適當政策、分類或是排程。網路骨幹之核心路由器在執行動作前也會做同樣的檢查，以確保整個 QoS 啓動之網路中服務等級保持一致性。



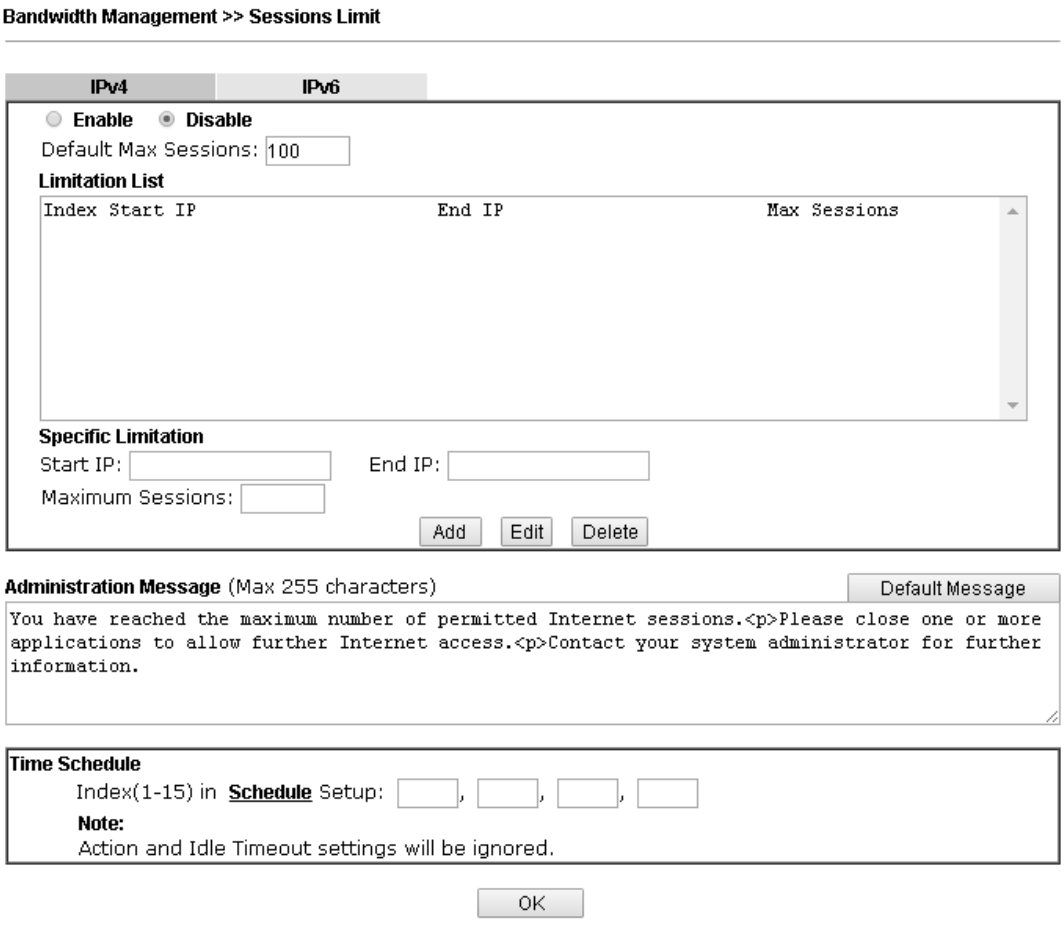
網頁使用者介面

下圖是頻寬管理的設定項目:



VII-2-1 連線數限制(Sessions Limit)

在**頻寬管理(Bandwidth Management)**群組中，按**連線數限制(Sessions Limit)**開啓如下的網頁。



如果要啓動限制連線數的功能，只要在此頁面上按**啓用(Enable)**鈕，並設定預設的連線數限制即可。

可用設定說明如下：

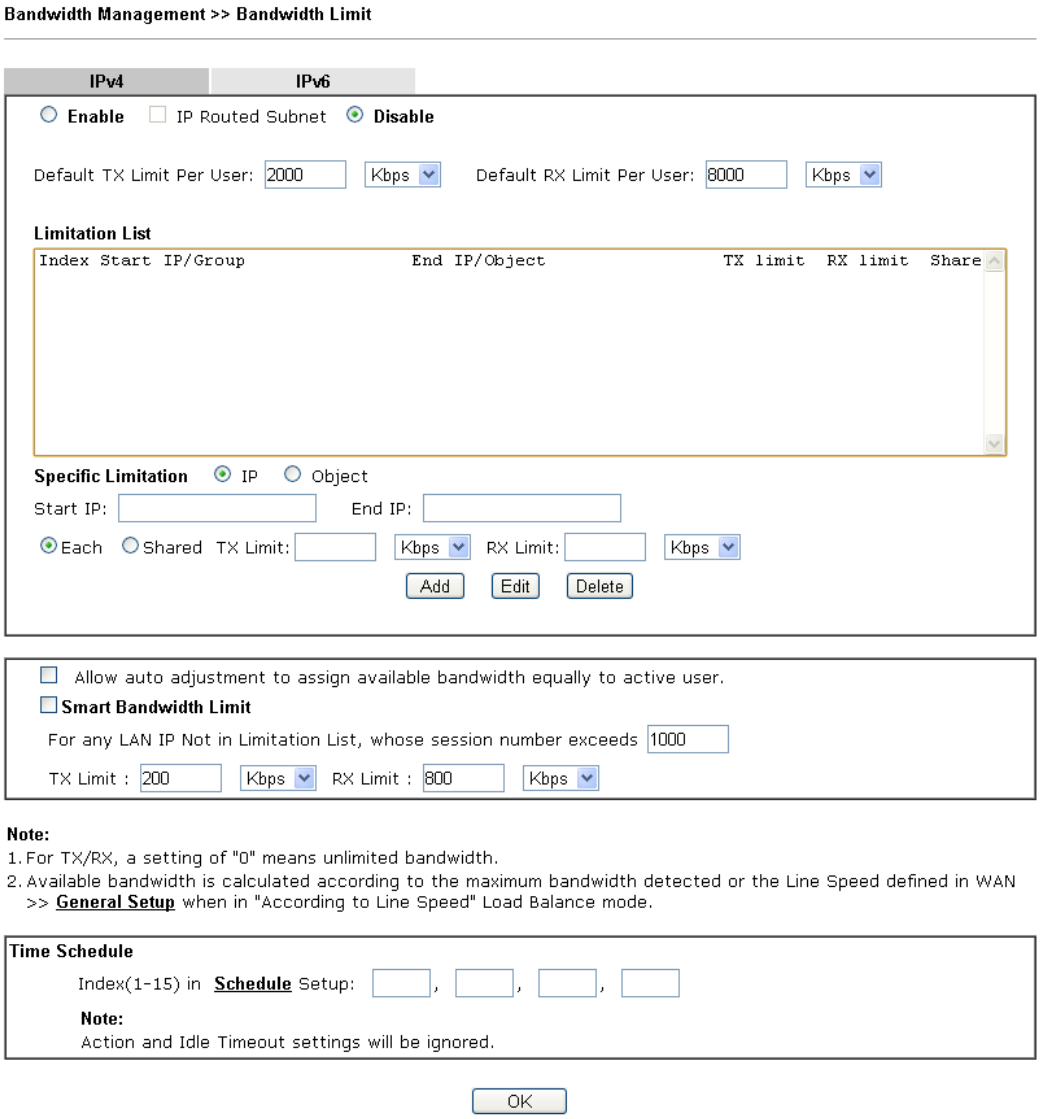
項目	說明
連線數限制 (Session Limit)	**啓用(Enable) -** 按此鈕啓動連線數限制功能。 **停用(Disable) -** 按此鈕關閉連線數限制功能。 **預設最大連線數(Default session limit) -**定義區域網路中每台

	電腦的預設連線數。
限制清單 **(Limitation List)**	顯示網頁中所設定的指定限制之電腦清單資料。
指定限制 **(Specific Limitation)**	**起始 IP(Start IP) -** 定義限制連線數的起始 IP 位址。 **結束 IP (End IP)-**定義限制連線數的結束 IP 位址。 **最大連線數(Maximum Sessions) -** 定義指定 IP 位址的範圍中可用的連線數，如果您沒有在此區設定連線數，系統將會使用此機種所支援之預設連線數。 **新增(Add) -** 新增指定連線數限制並顯示在上面的框框中。 **編輯(Edit)** - 允許您編輯選定的連線數設定。 **刪除(Delete)** - 刪除限制清單上任何一個您所選定的設定。
管理訊息 **(Administration Message)**	請輸入系統允許的網路連線數屆滿時，顯示在螢幕上的文字。 **預設訊息(Default Message) -** 按下此鈕可以直接使用路由器預設的訊息並顯示在管理訊息框內。
索引號碼(1-15)於排程設定.. **(Time Schedule)**	您可以輸入四組時間排程，所有的排程都可在**應用-排程(Index (1-15) in Schedule Setup)**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

VII-2-2 頻寬限制(Bandwidth Limit)

在**頻寬管理(Bandwidth Management)**群組中，按**頻寬限制(Bandwidth Limit)**開啓如下的網頁。



如果要啓動限制頻寬的功能，只要在此頁面上按**啓(Enable)**鈕，並設定預設的上下行資料傳送限制即可。

可用設定說明如下：

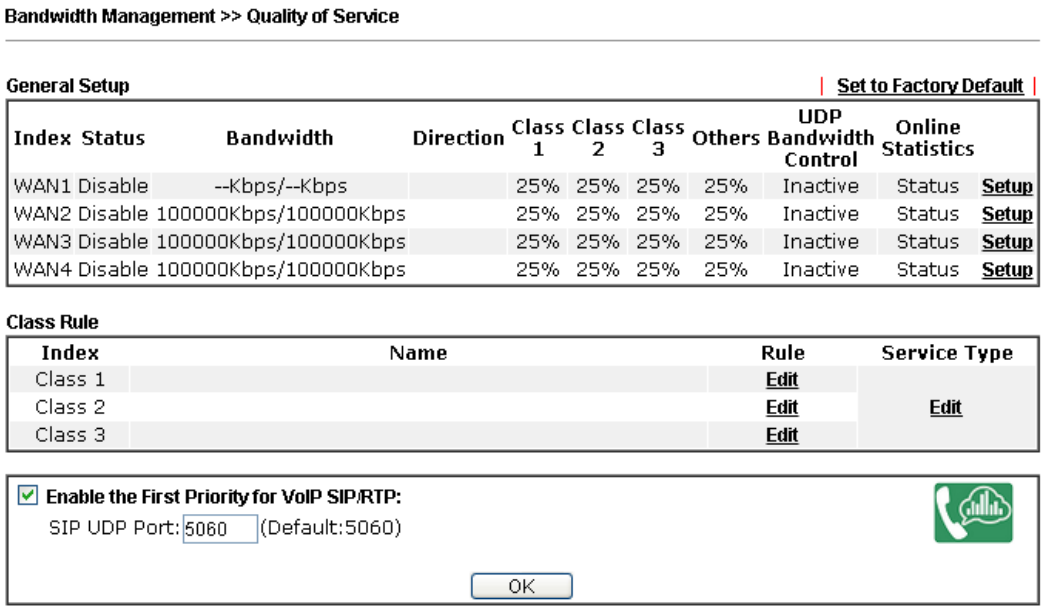
項目	說明
啓用(Enable)	按此鈕啓動限制頻寬功能。 **應用至第二子網路(IP Routed Subnet)** – 勾選此方塊套用頻寬限制至**區域網路>>基本設定(LAN>>General Setup)**中所指定的第二子網。 **預設傳送限制(Default TX limit)** - 定義區域網路中每台電腦預設的上行速度。 **預設接收限制(Default RX limit)** - 定義區域網路中每台電腦預設的下行速度。
停用(Disable)	按此鈕關閉限制頻寬功能。

限制清單 (Limitation List)	顯示網頁中所設定的指定限制之電腦清單資料。
指定限制 (Specific Limitation)	**IP** – 範圍內所有的 IP 都會受限於下方定義的傳送限制與接收限制。 ● **起始 IP(Start IP)** - 定義限制頻寬的起始 IP 位址。 ● **結束 IP(End IP)**- 定義限制頻寬的結束 IP 位址。 **物件(Object)** – 選定 IP 物件或是 IP 群組設定檔內的全部 IP 都會受限於下方定義的傳送限制與接收限制。 ● **IP 群組(IP Group)** – 使用下拉式清單指定一個 IP 群組。 ● **IP 物件(IP Object)** – 使用下拉式清單指定一個 IP 物件。 **每一個/共用(Each /Shared) -** 選擇 Each 讓起始 IP 與結束 IP 範圍內的每個 IP 都能享有傳送限制與接收限制中所定義的速度；選擇 **Shared** 則讓範圍內的 IP 共用傳送限制與接收限制的全部頻寬。 **傳送限制(TX limit) -** 定義上行傳送的速度限制，如果您未在此區設定限制的話，系統將使用您在每個索引內容中索引中所預設的限制速度。 **接收限制(RX limit) -** 定義下行傳送的速度限制，如果您未在此區設定限制的話，系統將使用您在每個索引內容中索引中所預設的限制速度。 **新增(Add)** - 新增指定速度限制並顯示在上面的框框中。 **更新(Edit) -** 允許您編輯選定的限制設定。 **刪除(Delete)** - 刪除限制清單上任何一個您所選定的設定。
允許自動調整取得最佳利用可用頻寬(Allow auto adjustment…)	路由器將會檢查是否保留足夠的頻寬，依照使用者所設定的頻寬限制而定。如果足夠的話，路由器將會調整可用的頻寬給予使用者使用，以便提升整體的效能。
聰明頻寬限制 (Smart Bandwidth Limit)	勾選此框即可由系統自動控制頻寬。 **傳送限制(TX limit) -** 定義上傳速度限制，如果沒有設定限制值，系統將會使用預設的速度。 **接收限制(RX limit) -** 定義下載速度限制，如果沒有設定限制值，系統將會使用預設的速度。
索引號碼(1-15)於排程設定.. (Time Schedule)	您可以輸入四組時間排程，所有的排程都可在**應用-排程 (Application >> Schedule)**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

VII-2-3 服務品質(QoS)

在**頻寬管理(Bandwidth Management)**群組中，選擇**服務品質(Quality of Service)**開啓如下的網頁。



可用設定說明如下：

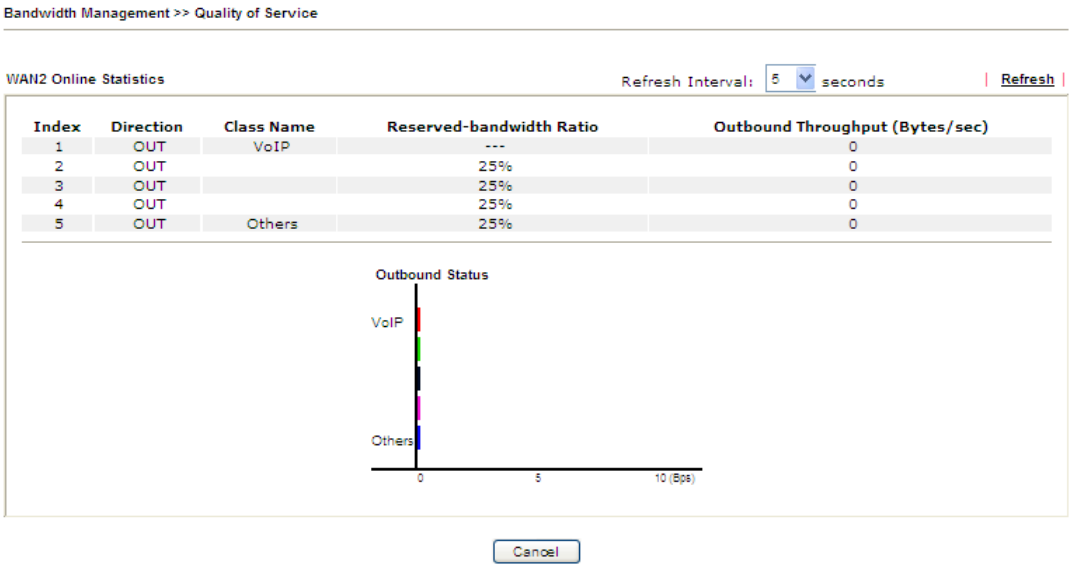
項目	說明
基本設定 (General Setup)	**索引編號(Index)** – 顯示 WAN 介面的編號。 **狀態(Status)** – 顯示該 WAN 介面目前是否爲停用或是啓用。 **頻寬(Bandwidth)** – 顯示該 WAN 介面的上下傳頻寬設定值。 **方向(Direction)** – 顯示此功能會影響的上下傳方向。 **類別 1/類別 2/類別 3/其他(Class 1/Class2/Class 3/Others)** – 顯示每個類別的所佔的頻寬比例。 **UDP 頻寬控制(UDP Bandwidth Control)** – 顯示該控制爲啓用或是停用。 **連線狀態統計(Online Statistics)** – 顯示 QoS 的連線狀態統計情形。 **設定(Setup)** – 允許設定一般 WAN 介面的 QoS 設定。
類別規則(Class Rule)	**索引編號(Index)** – 顯示您可以編輯的類別編號。 **名稱(Name)** – 顯示該類別的名稱。 **規則(Rule)** – 允許設定該選定類別的細部內容。 **服務類型(Service Type)** – 允許設定該服務類型的細部內容。
啓用 VoIP SIP/RTP 第一優先 (Enable the First Priority for VoIP SIP/RTP)	當此功能啓用的時候，VoIP SIP/UDP 封包會以最高優先傳送出去。 **SIP UDP 埠號(SIP UDP Port)** – 設定 SIP 使用的埠號。

本頁顯示 WAN 介面上的 QoS 設定成果，按下**設定(Setup)**連結進入下一層頁面，至於類別規則，則按下該頁面上的**編輯(Edit)**按鈕進入另一層畫面來設定即可。

您可以設定 WAN 介面的一般設定，並視您的需要來編輯類別規則並且編輯類別規則的服務類型。

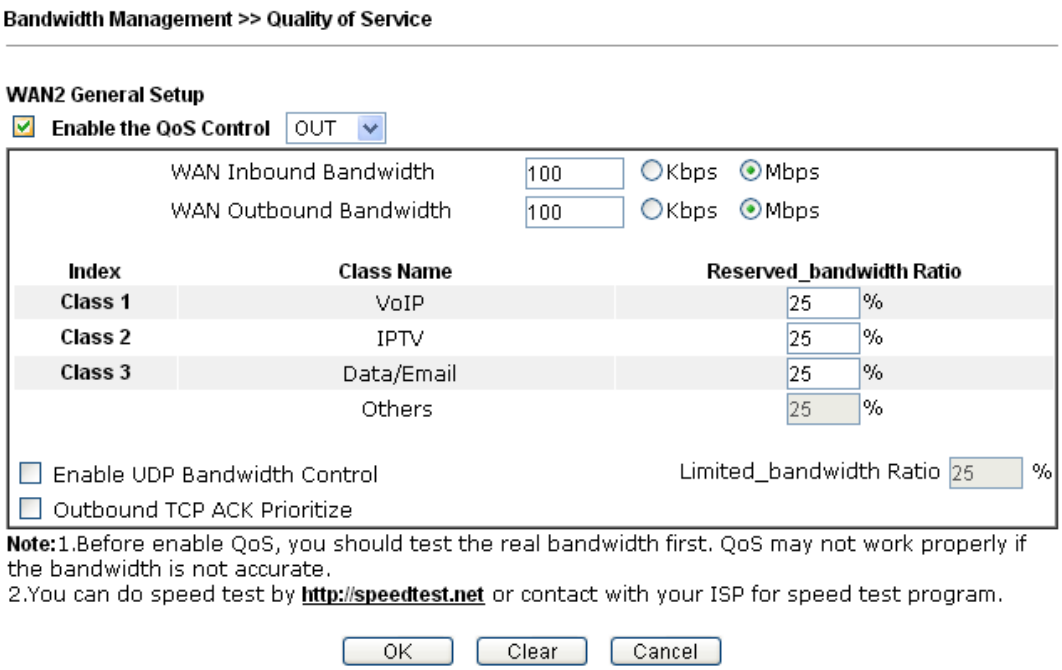
連線狀態統計(Online Statistics)

顯示服務品質的連線狀態統計圖供使用者參考。此功能僅在 QoS 的 WAN 介面已經啓用的狀態下始有作用。



基本設定(General Setup)

當您按下**設定(Setup)**時，您可調整 WAN 介面的 QoS 頻寬比率，系統提供您四種類別作爲 QoS 控制之用，前三種(類別 1 到類別 3)可視您的需求來調整，而最後一個則保留給那些不符合上面定義之規則等封包使用。



可用設定說明如下：

項目	說明
啓用服務品質(QoS)控制 (Enable the QoS Control)	預設狀態下，這個功能是啓用的。 請同時定義 QoS 控制設應所應用的流量方向。 **下載(IN)-** 僅適用於進入的封包。 **上傳(OUT)-** 僅適用於輸出的封包。 **雙向(BOTH)-** 適用於進入與輸出的封包。 勾選此方塊並按下**確定(OK)**，**連線狀態統計(Online Statistics)**連結即可出現在此頁面上。
WAN 下載頻寬 (WAN Inbound Bandwidth)	允許您設定 WAN 資料輸入的連線速度。預設值爲 10000kbps。
WAN 上傳頻寬 (WAN Outbound Bandwidth)	允許您設定 WAN 資料輸入的連線速度。預設值爲 10000kbps。 例如，您的 ADSL 支援 1M 的下行與 256K 上行速度，請將 **WAN 下載頻寬**設定爲 1000kbps 而 **WAN 上傳頻寬**設定爲 256kbps。
保留頻寬比例 (Reserved Bandwidth Ratio)	保留作爲群組索引所可應用的比率。
啓用 UDP 頻寬控制 (Enable UDP Bandwidth Control)	勾選此設定並在右邊設定限制的頻寬比率，這是 TCP 應用的一種保護機制，因爲 UDP 應用程式會消耗很多的頻寬。
優先處理對外 TCP ACK (Outbound TCP ACK Prioritize)	下載和上傳之的頻寬在 ADSL2+ 環境中差異是很大的，因爲下載速度可能會受到上傳 TCP ACK 的影響，您可以勾選此方塊讓 ACK 上傳得快一點，以便讓網路流通的更順暢。

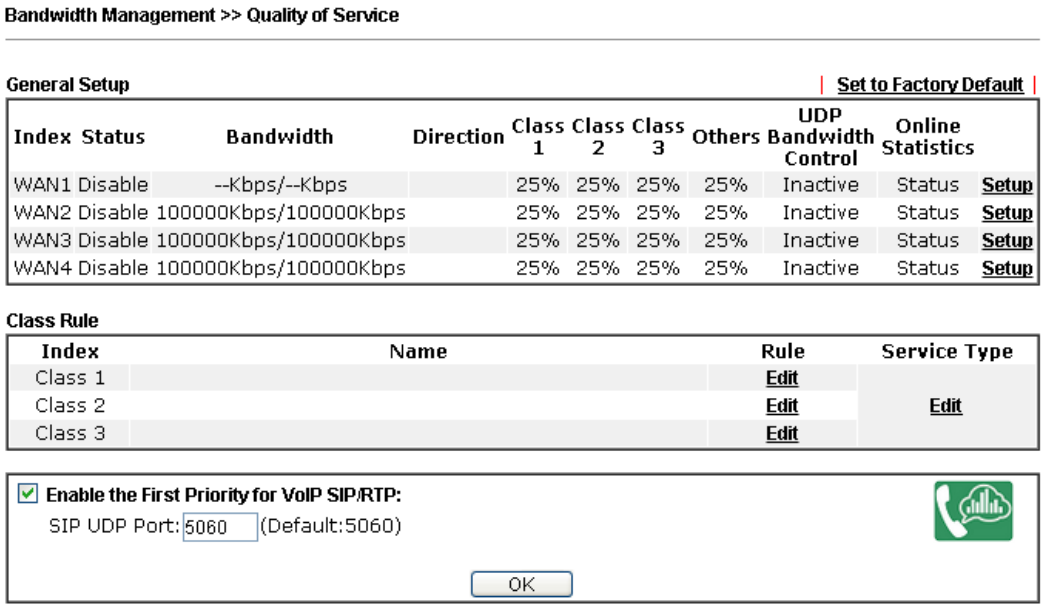
限制頻寬比率 (Limited_bandwidth Ratio)	此處所輸入的比率保留作爲 UDP 應用之需。

資訊

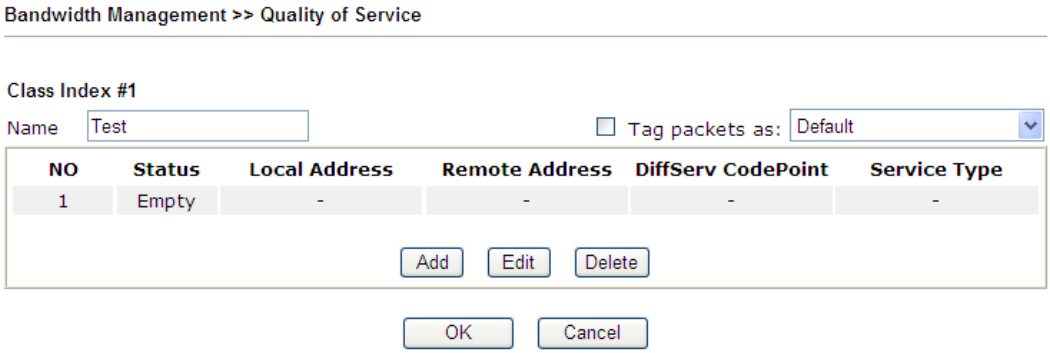
WAN 下載頻寬/上傳頻寬速率必須小於真實的頻寬，以確保 QoS 計算能夠正確執行。建議將下載頻寬/上傳頻寬頻寬值設定爲 ISP 業者所提供的實體網路速度的 80% - 85%，以便達到最佳的 QoS 成效。

編輯 QoS 的類別規則

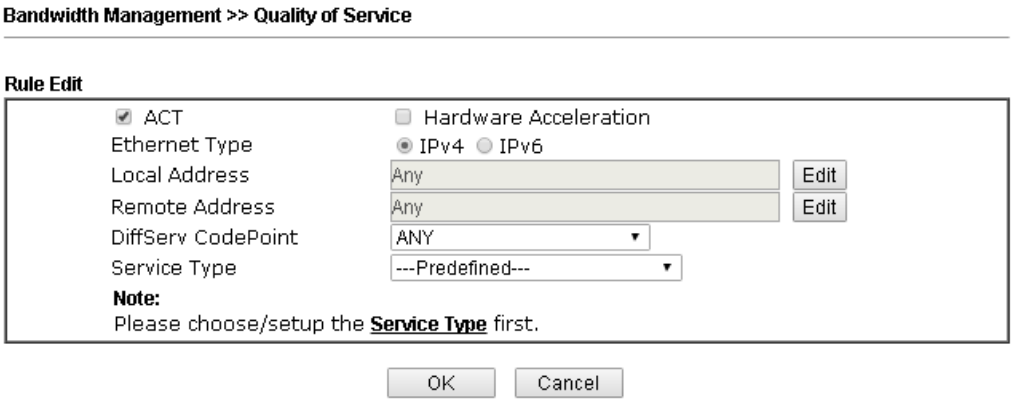
1. 前三種(類別 1 到類別 3)可視您的需求來調整，編輯或是刪除類別規則，請按該項類別的**編輯(Edit)**連結即可。



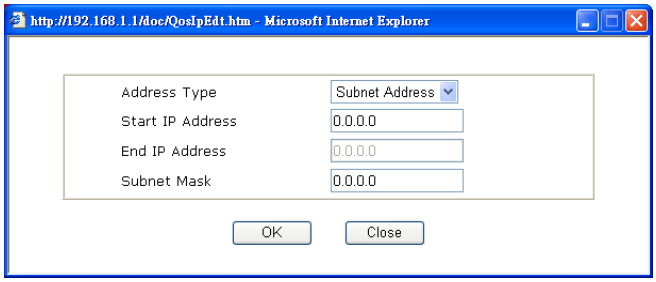
2. 在您按下**編輯(Edit)**連結之後，您可以看到如下的頁面。現在您可以定義該類別的名稱，在本例中，TEST 用來作爲類別索引 1 的名稱。



3. 若要新增一個新的規則，請按**新增(Add)**開啓下列畫面。

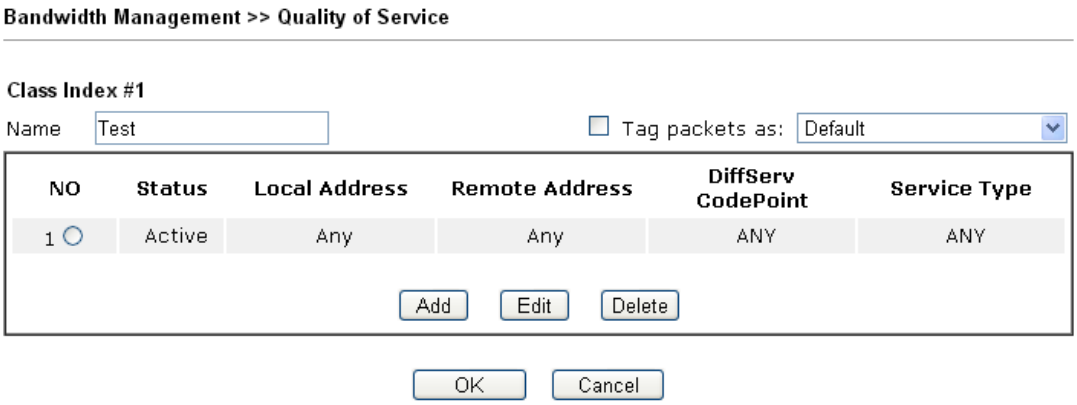


可用設定說明如下：

項目	說明
啓用(ACT)	勾選此方塊啓用本頁的設定。
硬體加速(Hardware Acceleration)	勾選此方塊啓用硬體加速功能。
乙太網路類型 (Ethernet Type)	指定用於此規則的協定類型(IPv4 或是 IPv6)。
本機位址 (Local Address)	按**編輯(Edit)**按鈕以設定規則的來源位址。
遠端位址 (Remote Address)	按**編輯(Edit)**按鈕以設定規則的目標位址。 **編輯(Edit) -** 讓您編輯來源/目標位址資訊。  **位址類型(Address Type) -** 決定來源位址的位址類型。 關於**任何位址(Any)**，您無須填入起始 IP 位址，由系統決定。 關於**單一位址(Single Address)**，您可以填入起始 IP 位址。 關於**範圍位址(Range Address)**，您必須填入起始和終點 IP 位址。 關於**子網路位址(Subnet Address)**，您必須填入起始 IP 位址和子網路遮罩。
DiffServ CodePoint	所有的資料封包將會被切割成不同等級，並且依照系統的等級層別來處理資料封包。請指定資料所需的層級作爲 DoS 控制之用。
服務類型 (Service Type)	決定 QoS 控制處理時資料的服務類型，這項類型可以視情況編輯改變，您可以從下拉式選項中選擇事先定義的服務類型，這些類型都是出廠時即設定好的類型，請自行挑選一種想要使用的類型。

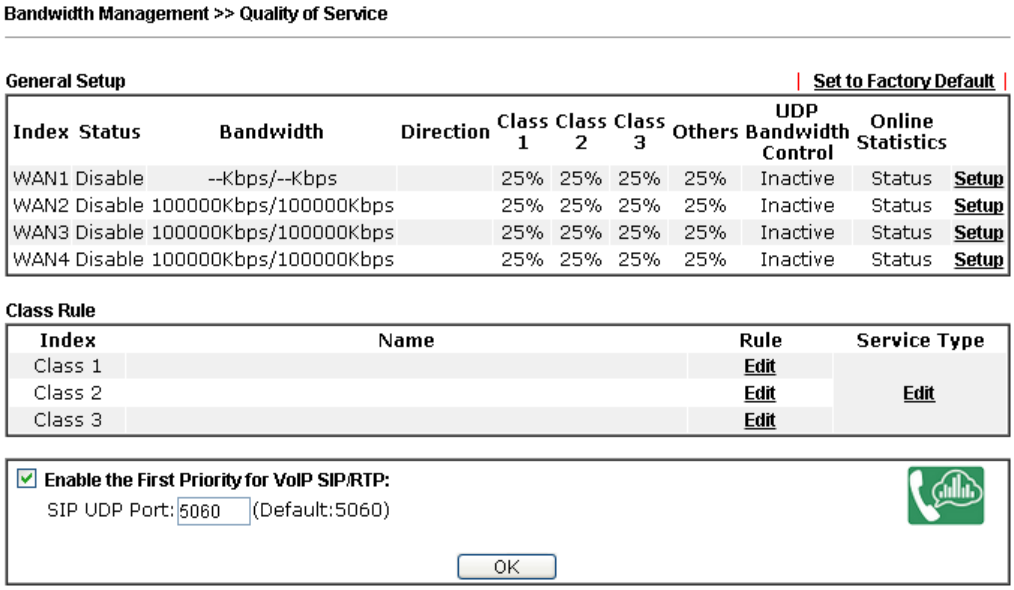
4. 完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

另外，您可以爲一種類別指定 20 組規則，如果您想要編輯現存的規則，請點選該項按鈕，然後按下**編輯(Edit)**鈕開啓編輯視窗以修改該規則。

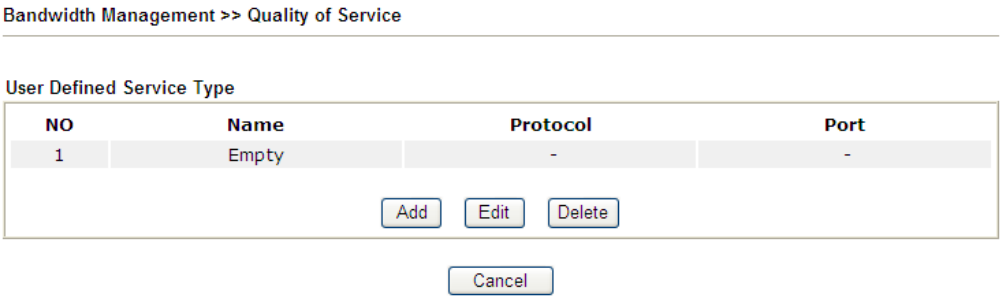


編輯類別規則的服務類型

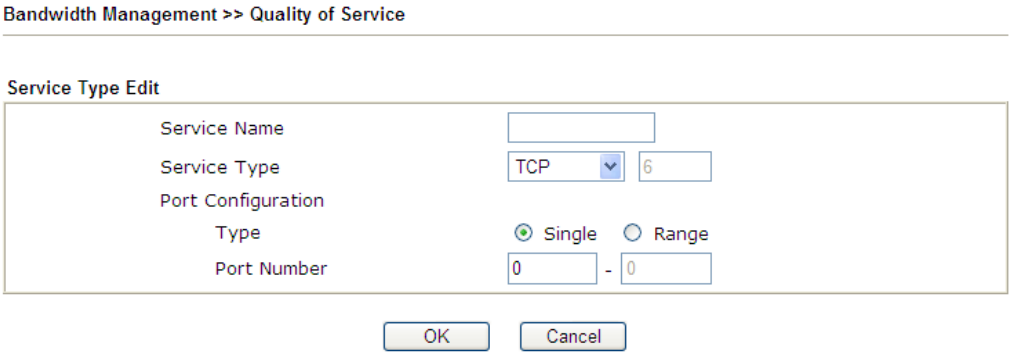
1. 要新增、編輯或刪除服務類型，請按服務類型區域下方的**編輯(Edit)**連結。



2. 在您按下**編輯(Edit)**按鈕之後，下述畫面將會出現。



3. 新增一個規則請按下**新增(Add)**按鈕開啓設定頁面。如果您想要編輯現有的服務類型，請選擇該項並按下**編輯**連結開啓如下頁面：



可用設定說明如下：

項目	說明
服務名稱 (Service Name)	輸入新的服務名稱。
服務類型 (Service Type)	請選擇新服務所需的類型(TCP, UDP or TCP/UDP)。
通訊埠組態 (Port Configuration)	**類型(Type)** - 按**單一(Single)**或是**範圍(Range)**，如果您選擇的是範圍，您必須輸入起始通訊埠號和結束通訊埠號。 **通訊埠號(Port Number)** –如果您選擇範圍爲服務類型，請在此輸入起始和結束通訊埠號。

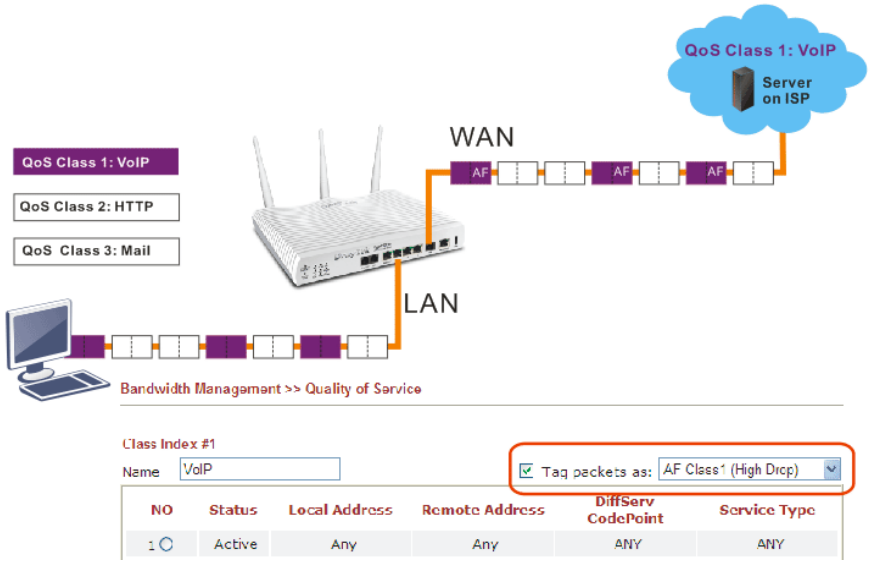
5. 完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

另外，您可以指定 10 組服務類型，如果您想要編輯或是刪除現存的服務類型，請點選該項按鈕，然後按下**編輯(Edit)**鈕開啓編輯視窗以修正該服務類型。

封包重新標籤以供辨識

來自於區域網路 IP 的封包可以透過 QoS 設定封包重新標籤，當該封包透過 WAN 界面傳送出去時，所有的封包都會標示特定的標頭讓 ISP 上的伺服器容易辨識出來。

例如，在下述範例圖當中，區域網路端的 VoIP 封包進入路由器時並沒有任何標頭，但是當它們透過路由器轉往 ISP 的伺服器時，所有的封包就都被標示上 AF 標頭(可在頻寬管理>>服務品質(QoS)類別中設定)。

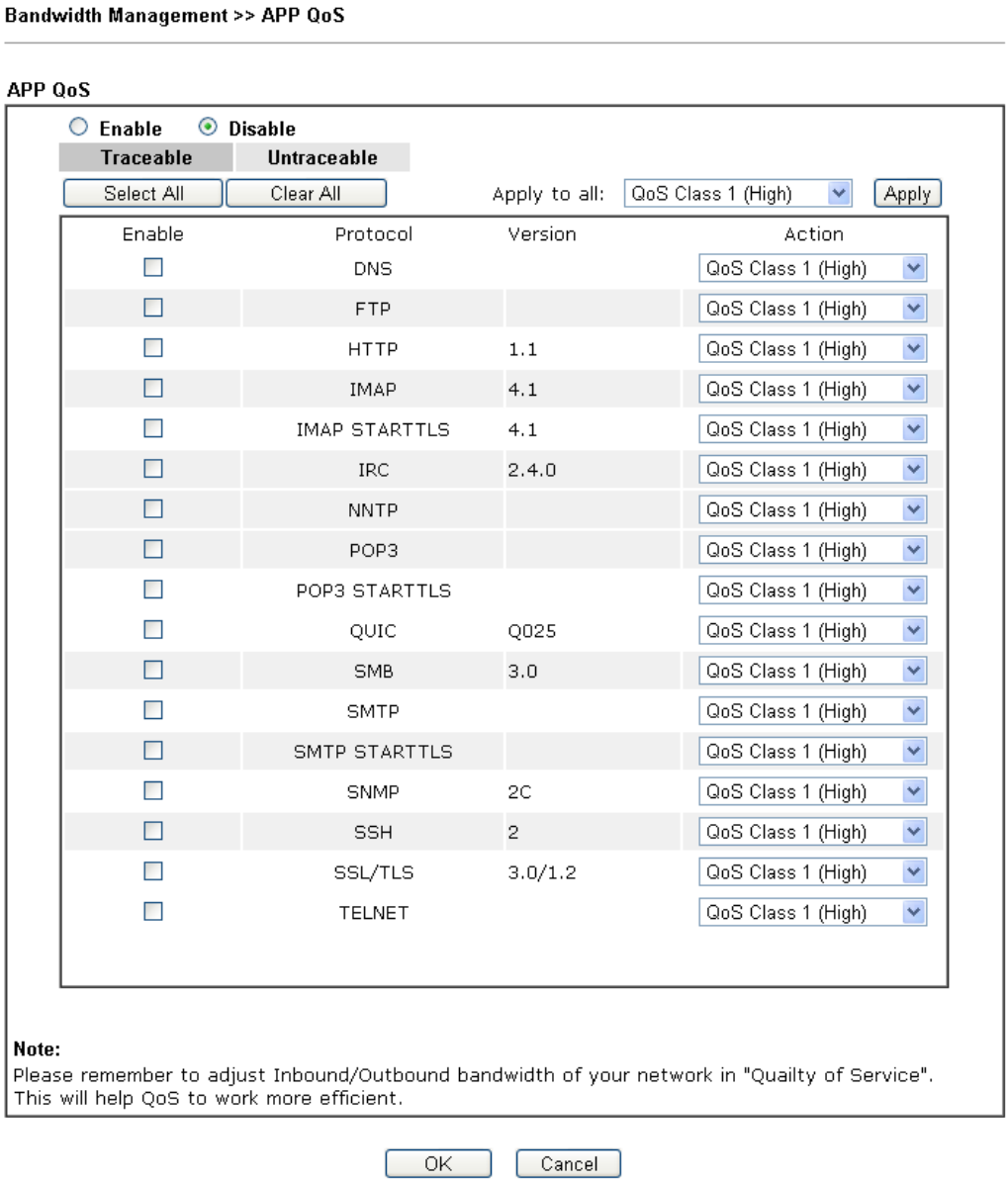


VII-2-4 APP QoS

QoS 功能用於管理特定 IP 或是埠號等服務所需使用的頻寬。然而，對於無固定 IP 或是埠號的 VNC 或是 PPTV 的頻寬管理是完全沒有作用的。

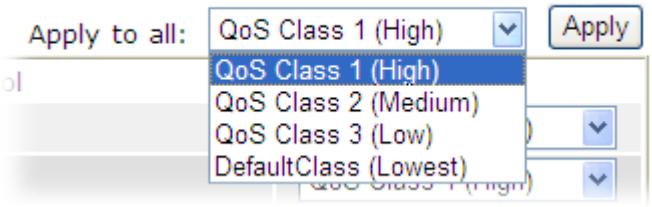
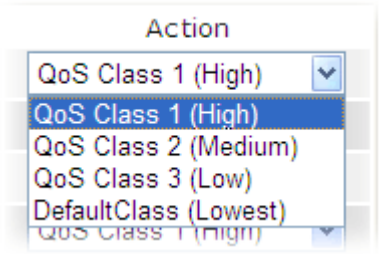
APP QoS 使用應用程式管控功能進行軟體類型偵測，藉由結合 QoS 的功能，路由器可以對通訊協定、串流、遠端管理、網頁硬碟等等進行頻寬管理。

選擇**頻寬管理>>APP QoS (Bandwidth Management>>APP QoS)** 開啓如下頁面：



可用設定說明如下：

項目	說明
啓用/停用 (Enable/Disable)	選**啓用(Enable)**可啓用 APP QoS 功能。 選**停用(Disable)** 停止 APP QoS 功能。
可追蹤(Traceable)	表列的通訊協定可由路由器追蹤。每種標籤提供不同的協定類型。
不可追蹤(Untraceable)	表列的通訊協定無法由路由器追蹤。每種標籤提供不同的協定類型。
選擇全部(Select All)	選擇此頁面上全部的通訊協定。
清除全部(Clear All)	取消選擇此頁面上全部的通訊協定。
套用至全部(Apply to all)	選擇一種動作便於套用至所有的通訊協定上。

	 **套用(Apply)** – 按此可讓選定的動作立刻套用到選定的通訊協定上。
動作(Action)	通訊協定可以分別套用不同的 QoS 等級。 

應用說明

A-1 如何利用 QoS 來最佳化頻寬管理

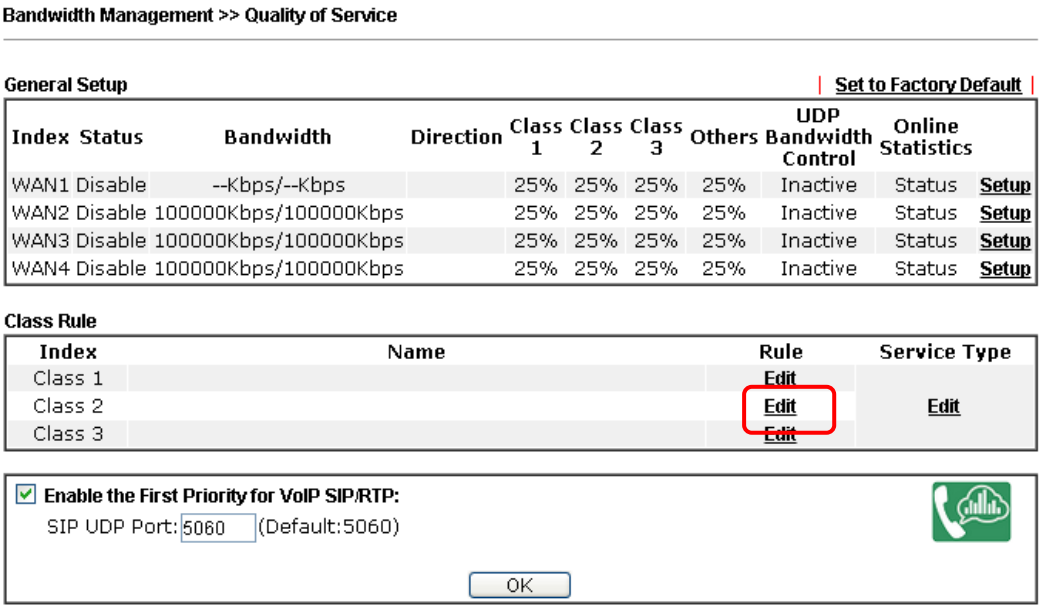
您是否有過上傳/下載檔案(聲音、影像或是電子郵件、資料等等)時受到網際網路連線的頻寬限制或頻寬過窄的問題? Vigor 路由器進階版的 QoS 技術可幫助您依據實際需要分派不同比例的頻寬於不同的用途上。

假設您自 ISP 獲得的連線速度爲 2MB/512Kb，家中需要用到 VoIP 網路電話、IPTV 機上盒以及一般的網路資料傳送，您希望整個頻寬中有 30%用在 VoIP 網路電話，50%用在 IPTV，15%用在網路資料傳送，剩下的 5%用作其他用途，那麼您可以參考下述的作法：

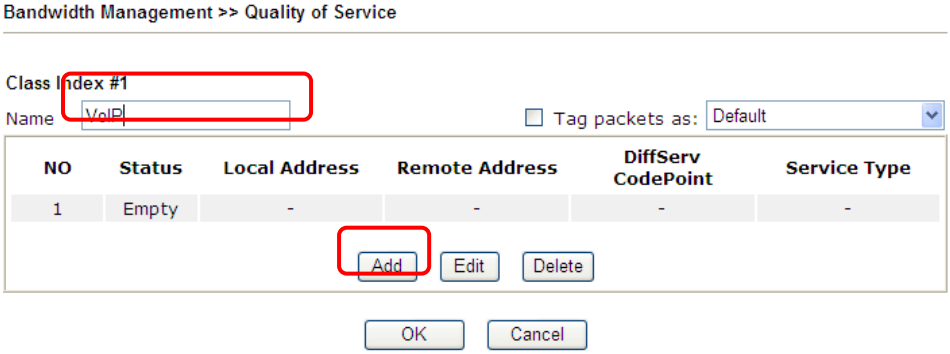
1. 開啓**頻寬管理>>服務品質(Bandwidth Management>> Quality of Service)**。



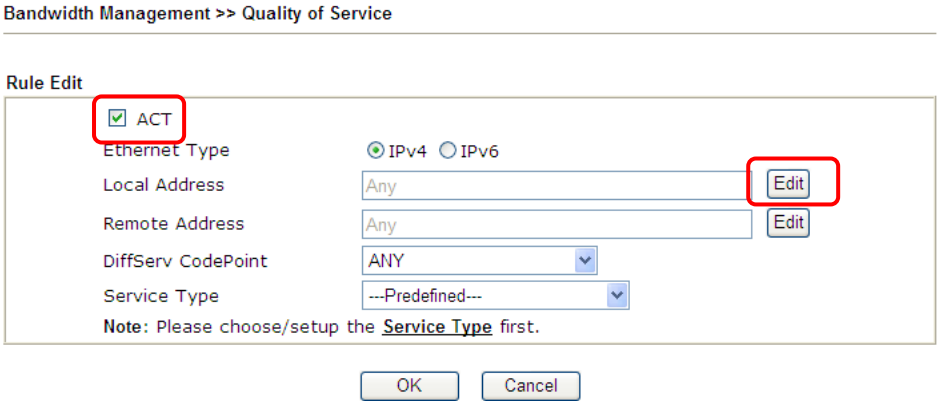
2. 看到如下頁面之後，請按**類別 1** 的**編輯(Edit)**按鈕。



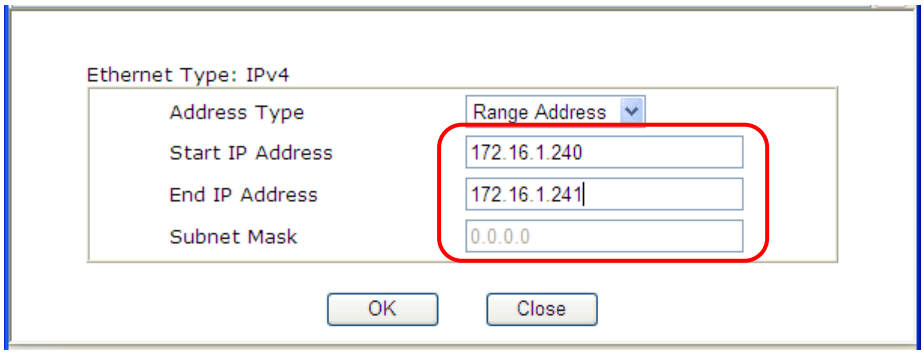
3. 在**名稱**欄位請輸入 VoIP，然後按下**新增(Add)**按鈕。



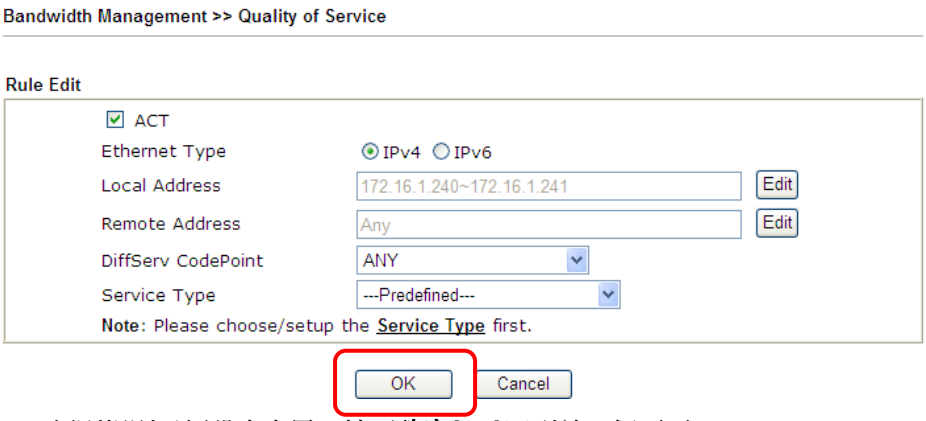
4. 勾選**啓用(ACT)**方塊，在本機地址欄位中按下**編輯(Edit)**按鈕。



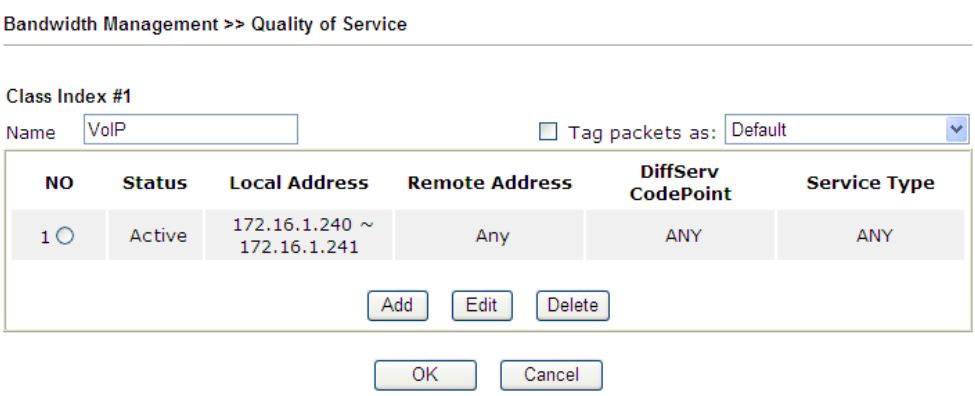
5. 於跳出視窗中，選擇**範圍位址(Range Address)**作爲**位址類型(Address Type)**，輸入起始 IP 位址以及結束 IP 位址，最後按下**確定(OK)**儲存設定並離開此視窗



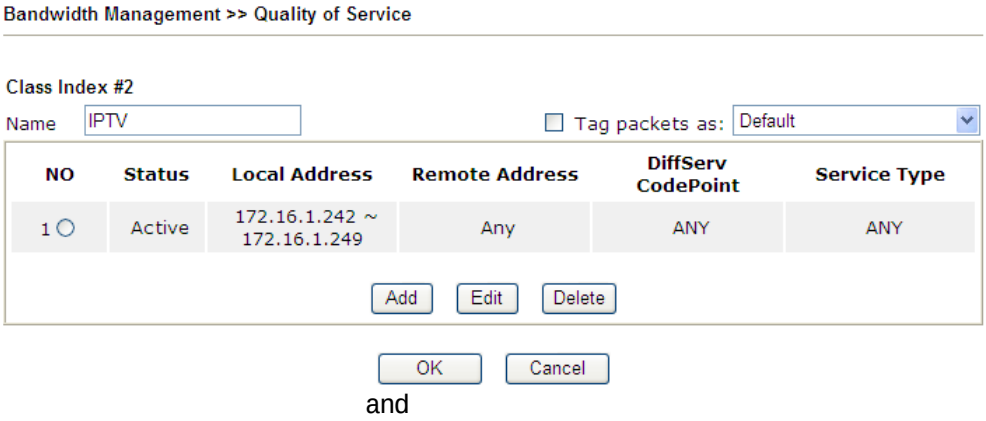
6. 再次按下**確定(OK)**儲存設定。



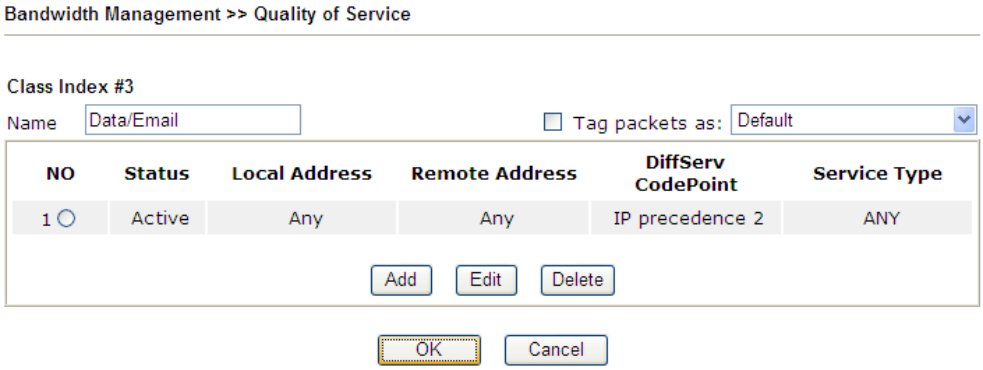
7. VoIP 類別規則已經設定完畢，按下**確定(OK)**回到前一個頁面。



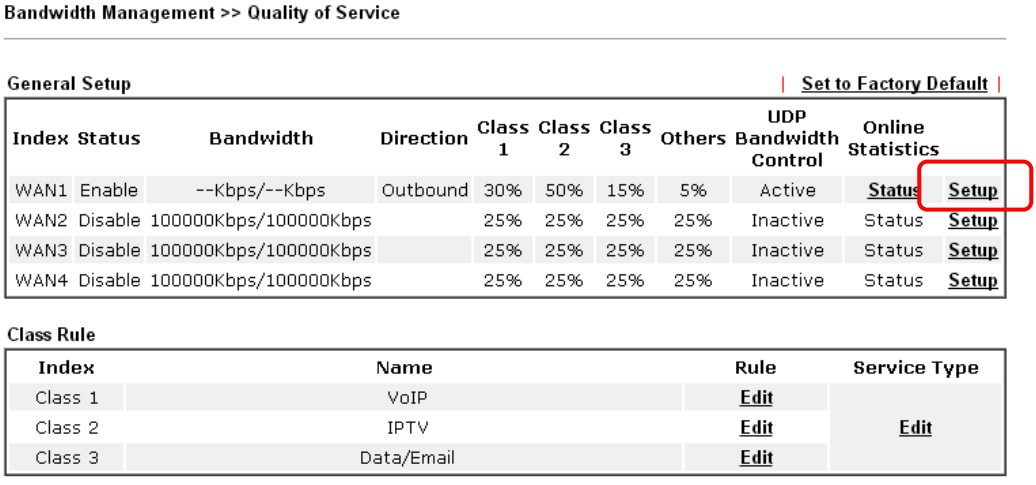
8. 採取同樣的步驟分別再設定 IPTV 與資料/電子郵件傳輸的類別內容。



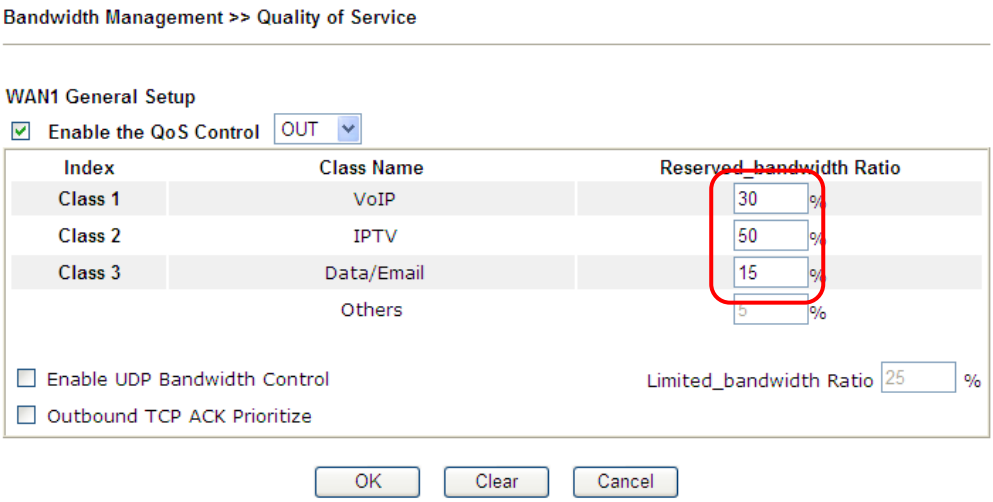
and



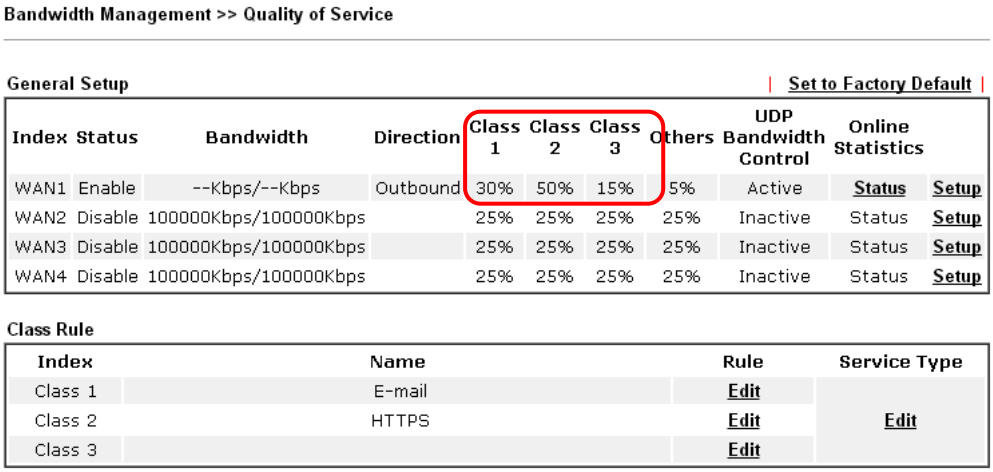
9. 假使您的網路連線有 2MB/512Kb，您可以按下 WAN1 的**設定(Setup)**連結來設定上述不同群組的個別頻寬。



10. 在設定頁面上，勾選**啓用服務品質控制功能(Enable the QoS Control)**方塊，三個類別中分別輸入 30, 50 與 15 等比例，如下圖所示。記得勾選**啓用 UDP 頻寬控制(nable UDP Bandwidth Control)**。

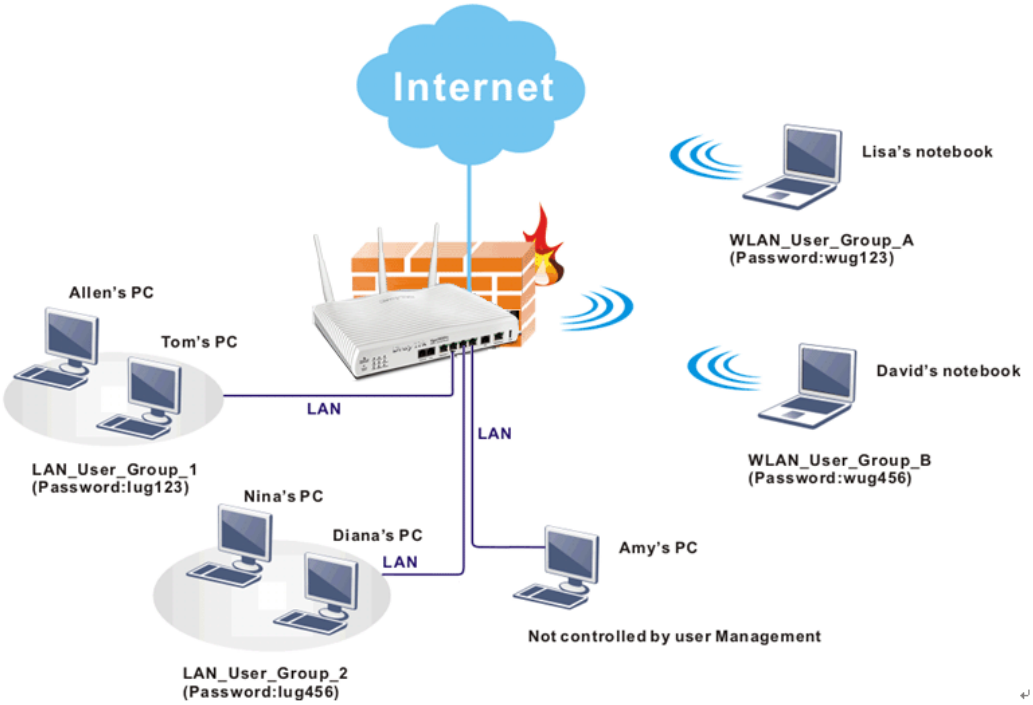


11. 按下**確定(OK)**儲存，WAN1 的類別設定定義將呈現如下：



VII-3 使用者管理(User Management)

使用者管理這項功能具有安全性檢測的效果，除非特定主機提供正確使用者名稱以及密碼，否則它不允許來自該主機任何資料流量(除了 DHCP 相關封包以外)。使用者管理功能可以透過使用者帳號，而非利用 IP 位址/MAC 位址來管理主機。網路管理者可以針對不同主機透過不同使用者管理帳號，提供不同的防火牆策略或是規則。不只提供基本網際網路存取檢測，還能提供額外的防火牆規則諸如數位內容安全管理來保護管理下的各式主機。



資訊

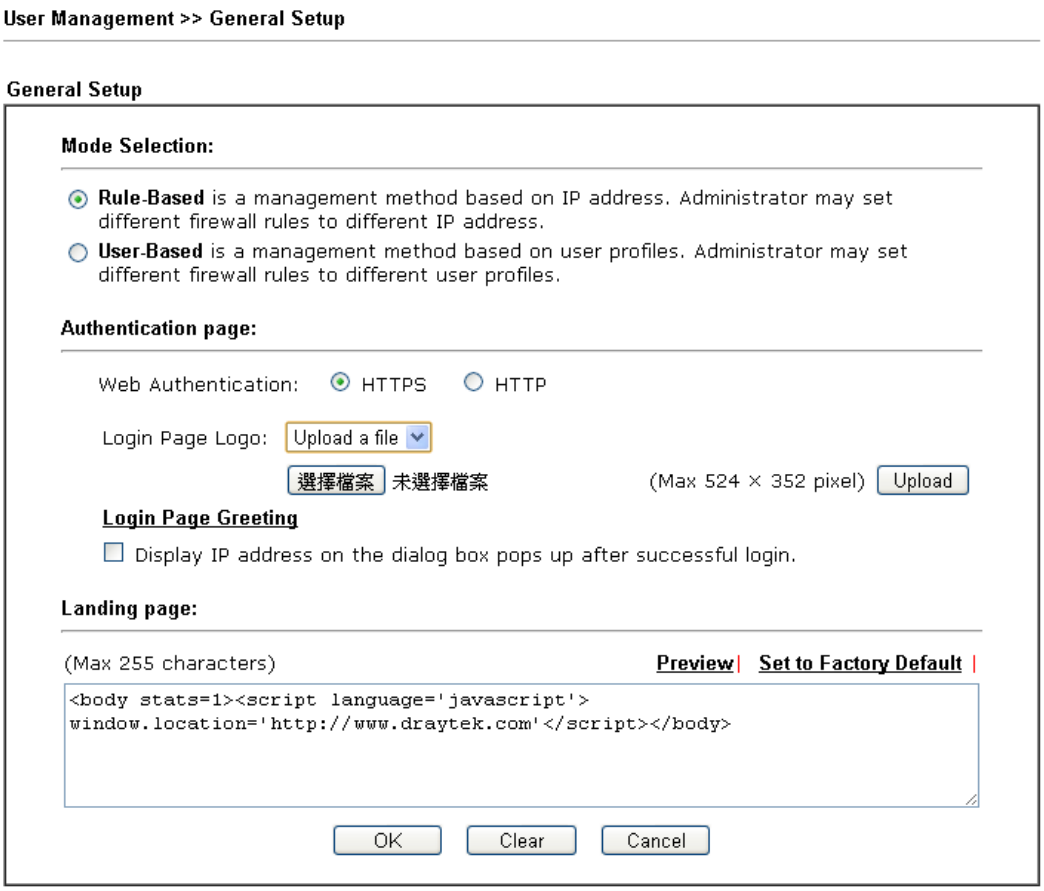
防火牆中過濾器規則通常只會套用再主機上(亦即路由器安裝的那台)，有了使用者管理功能之後，設定的規則就可以套用在連結上該台路由器的每一個使用者電腦上。

網頁使用者介面



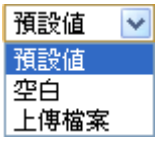
VII-3-1 基本設定(General Setup)

基本設定可以決定使用者管理準備運用在使用者上的標準爲**規則模式**還是**使用者模式**，此處所選擇的模式將會影響套用於每個使用者上的過濾器規則內涵。



可用設定說明如下：

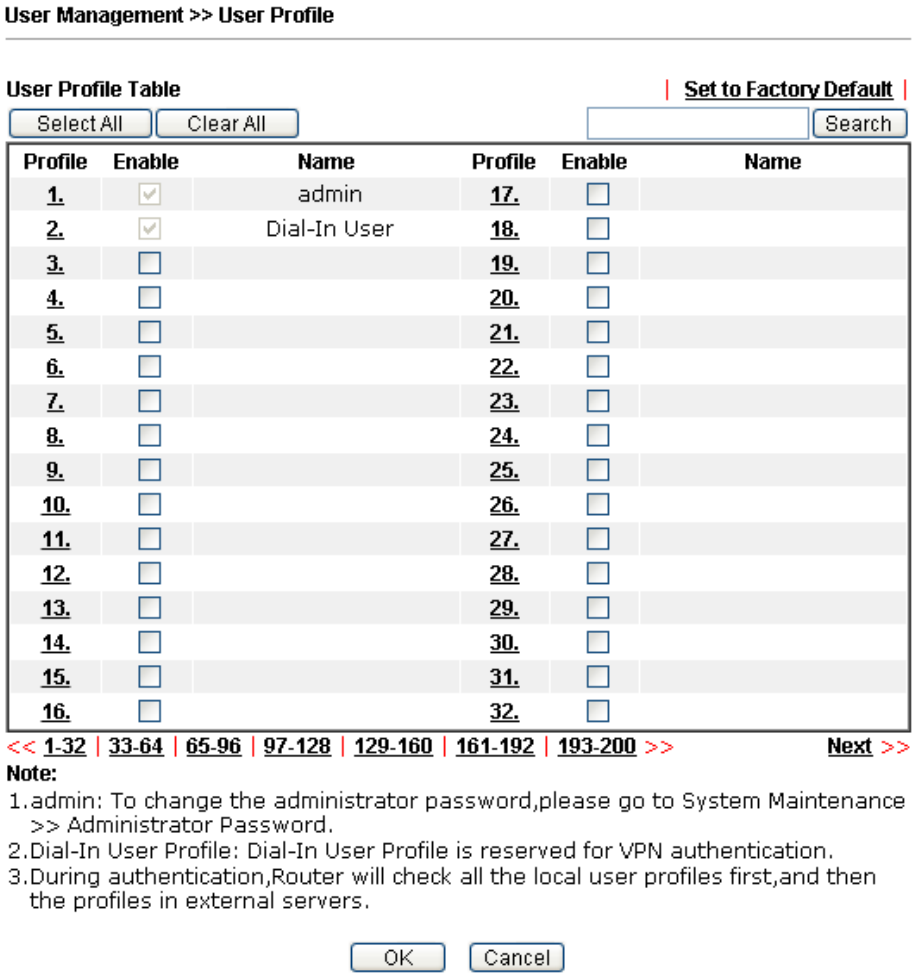
項目	說明
模式選項(Mode)	有二種模式可供您選擇，每種模式都會對受影響的使用者帶來不同的過濾效果。 **使用者模式(User-Based)** - 如果您選擇此模式，路由器將會套用您在**使用者管理>>使用者設定檔(User Management>>User Profile)** 中的過濾規則至使用者上。 **規則模式 (Rule-Based)** – 如果您選擇此模式，路由器將會套用您在**防火牆>>基本設定(Firewall>>General Setup)**中的過濾

	規則至使用者上。
驗證頁面 (Authentication page)	**網頁驗證 (Web Authentication)** - 選擇網頁驗證使用的協定(HTTPS/HTTP)。 **登入頁面 Logo (Login Page Logo)** – 標識能成爲辨識企業的圖示，可以上傳並顯示在登入頁面上，您可以使用預設畫面，空白頁或是上傳其他的影像圖形(尺寸像素大小不要超過 524 × 352)，如此即可針對特定企業給予企業辨識圖示，當然這也帶有廣告的效果。  **登入頁面設定(Login Page Greeting)**- 此連結讓您開啓登入頁面設定網頁，詳細資訊請參考**系統維護>>登入頁面設定 (System Maintenance>>Login Page Greeting)**一節。 **顯示出成功登入後…..(Display IP Address on …)** – 勾選此框以顯示追蹤視窗中用戶端的 IP 位址。
指定首頁(Landing Page)	用戶透過本台路**由器登**入存取網際網路**時，將會先開啓此處所輸入的網站**。

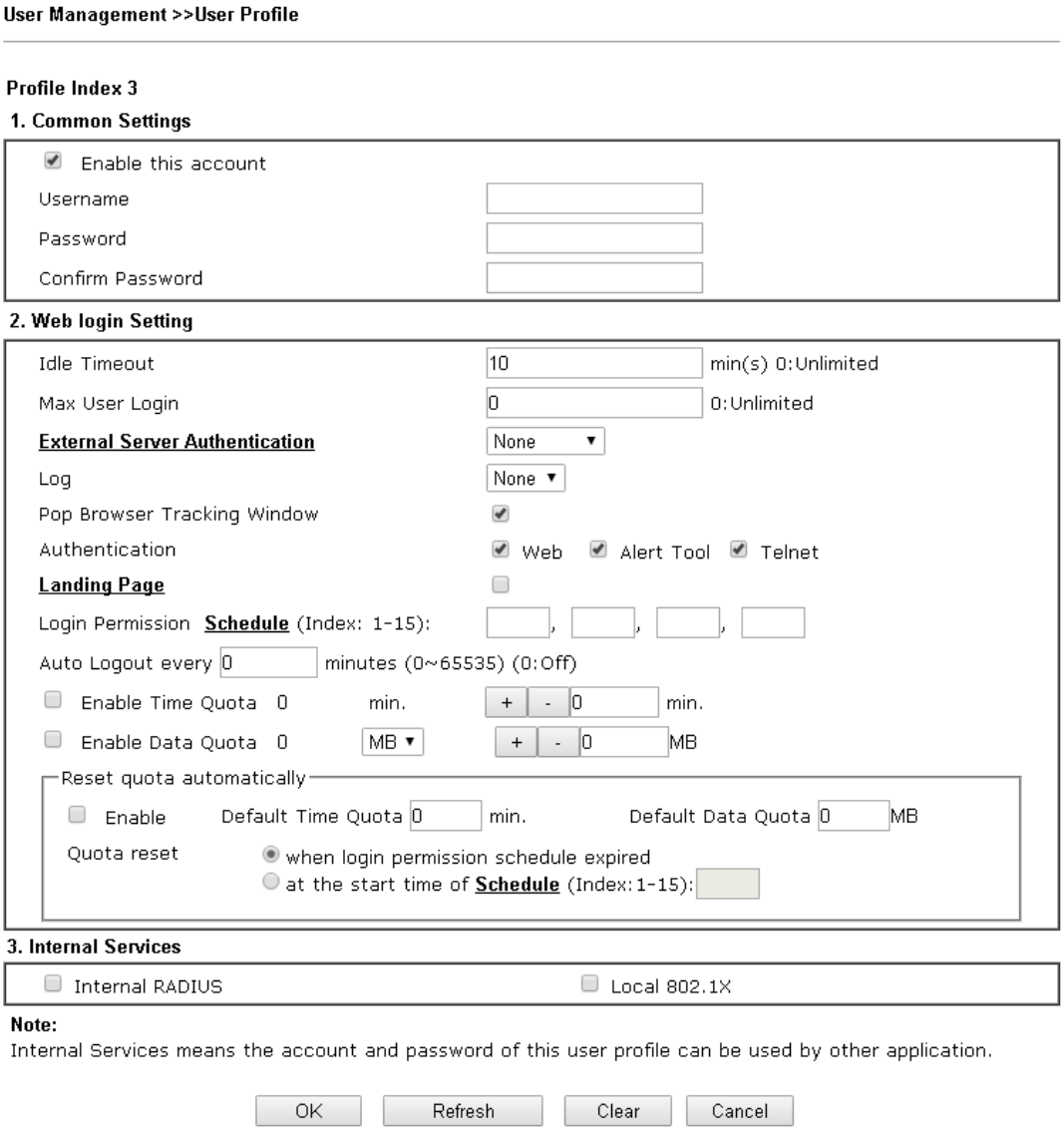
完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

VII-3-2 使用者設定檔(User Profile)

本功能可讓您設定客製化使用者設定檔(最多可設定 200 個)，這些設定檔將會套用於使用者管理之下的使用者帳號。開啓**使用者管理>>使用者設定檔**即可見到如下頁面。

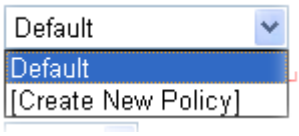
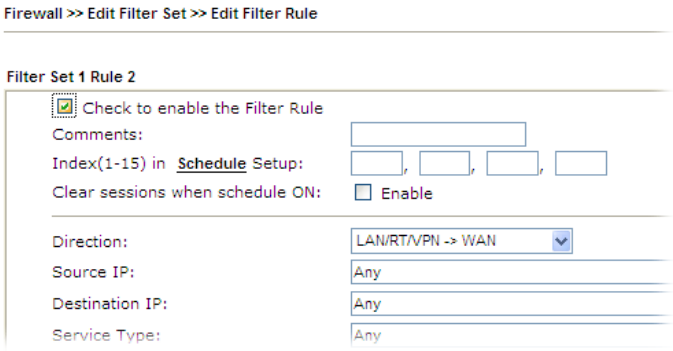
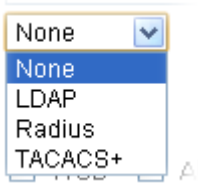


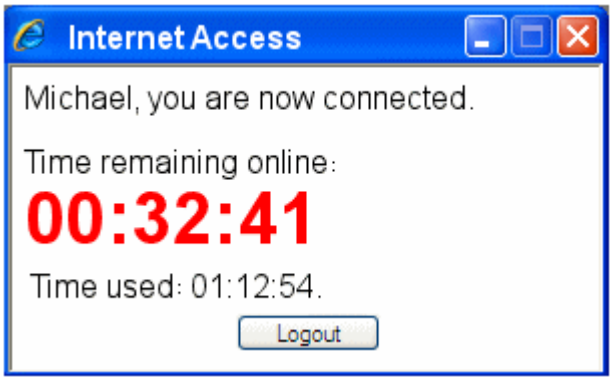
欲設定使用者設定檔，請點選任何一的設定檔編號連結，不過要注意的是連結 1(admin) 與連結 2(Dial-In User)這二個都是預設值。請按連結 3。



可用設定說明如下：

項目	說明
啓動此帳號(Enable this account)	勾選此方塊啓用此設定檔。
使用者名稱(User Name)	請輸入此使用者設定檔的名稱(例如 *LAN_User_Group_1, WLAN_User_Group_A, WLAN_User_Group_B* 等等)，當使用者嘗試利用本路由器登入網際網路時，必須先通過驗證步驟。使用者必須輸入此處所設定的使用者名稱才能通過驗證，一旦通過驗證，使用者即可利用此路由器享受網際網路。不過，在操作網際網路時會受到此設定檔所做的限制。
密碼(Password)	請輸入此使用者設定檔的密碼(例如 *lug123, wug123,wug456* 等等)，當使用者嘗試利用本路由器登入網際網路時，必須先通過驗證步驟。使用者必須輸入此處所設定的密碼才能通過驗證，一旦通過驗證，使用者即可利用此路由器享受網際網路。不過，在操作網際網路時會受到此設定檔所做的限制。
確認密碼(Confirm Password)	再次輸入密碼以確認。

閒置逾時(Idle Timeout)	如果使用者有一段時間沒有任何動作，網路連線將會自動中斷，預設值爲 10 分鐘。
最多登入使用者數目(Max User Login)	此設定檔可以讓很多使用者使用，您可以設定最多登入網際網路的使用者總數。預設值爲 0，這表示沒有人數上的限制。
Policy(原則)	這個功能只有在**使用者管理>>基本設定(User Management>>General Setup)**頁面中選擇了**使用者模式(User-Based)**才會出現。  **預設值(Default)** – 如果您選擇此項，系統會採用防火牆內事先設定的過濾器規則於此設定檔上。 **建立新原則(Create New Policy)** – 如果您選擇此項，下述頁面會跳出方便您定義一個新的過濾器規則。  有關詳細的設定內容，請直接參考**防火牆>>過濾器規則(Firewall>>Filter Rule)**一節。在**防火牆>>基本設定**頁面中**預設規則(Firewall>>General>>Default rule)**內沒被選上的規則可在**使用者管理>>使用者設定檔(User Management>>User Profile)**中運用。
外接伺服器驗證(External Service Authentication)	路由器將透過外部服務例如 LDAP 伺服器或是 RADIUS 伺服器或是自身對撥入使用者進行驗證。如果您在此選擇了 LDAP 伺服器或是 RADIUS 伺服器，上述的密碼設定都可以省略不必設定。 
記錄(Log)	登入登出的時間，封鎖/放行使用者等內容都可傳送並且顯示在 Syslog 上，請選擇任何一個項目以便紀錄與該使用者相關的內容。 
快顯瀏覽器追蹤視窗(Pop Browser Tracking	如果啓用此功能，且設定了閒置逾時的功能，那麼含有倒數計時的視窗即會跳出告訴您還剩下多少時間，不過系統會定期更

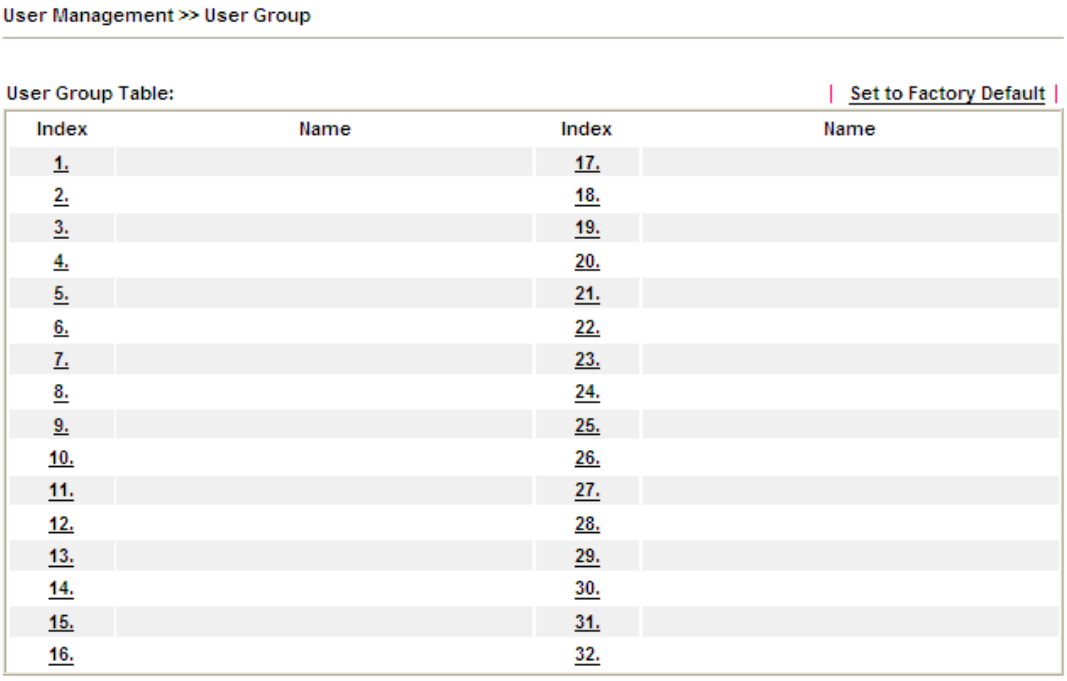
Window)	新時間讓連線維持不斷，如此依來，閒置逾時就不會中斷網路連線了。
驗證(Authentication)	任何使用者(不管是 LAN 端或是 WAN 端)嘗試透過路由器連結網際網路，都必須通過路由器的驗證，有三種方式可讓使用者挑選使用： **網頁(Web)** – 如果選擇此項，使用者可在任何瀏覽器上輸入路由器的 URL，登入視窗將會跳出並要求使用者輸入使用者名稱與密碼。如果通過驗證了，歡迎訊息視窗(可於使**用者管理>>基本設定(User Management >> General Setup)**中設定)會顯示在螢幕上，驗證之後，路由器也會自動導引至目的 URL(若使用者有需要的話)。 **警告工具(Alert Tool)** – 如果選擇此項，使用者必須打開警告工具(Alert Tool)並輸入使用者名稱及密碼進行驗證，通過驗證後，系統會出現小視窗告知使用者剩餘多少時間可以使用網路，接著，使用者可利用任何一個瀏覽器登入網際網路。 **Telnet** – 如果選擇此項，使用者可透過 Telnet 指令來進行驗證作業。
指定首頁(Landing Page)	當使用者利用帳號及密碼登入路由器的使用者介面時，將會被引導至**使用者管理>>基本設定(User Management>>General Setup)**中所設定的指定首頁。 勾選此方塊可開啓此項功能。
索引號碼(1-15)於排程設定(Login Permission Schedule (Index: 1-15))	您可以在此輸入四組時間排程，所有的排程都可在**其他應用>>排程(Application >> Schedule)**頁面事先設定，在本頁您只要將排程的索引編號輸入即可。
啓用時間額度(Enable Time Quota)	時間額度表示路由器針對本設定檔的使用者所允許的全部連線時間，勾選此方塊啓用此功能。 [+] – 按下此方塊可增加此設定檔的時間額度，單位是分鐘，請在後方空格輸入數值。 [-] – 按下此方塊可減少此設定檔的時間額度，單位是分鐘，請在後方空格輸入數值。 **注意:** 當使用者成功透過路由器登入網際網路之後，下述對話盒會跳出通知使用者還有多少時間可以使用網路。  時間一旦到達，所有連線工作包括網路、IM、社交媒體、臉書等等都會暫停。
Enable Data Quota(啓用資料額度)	資料額度表示給予使用者的全部資料傳輸量。

	 – 按下此方塊可增加此設定檔的資料額度，單位是 MB，請在後方空格輸入數值。  –按下此方塊可減少此設定檔的資料額度，單位是 MB，請在後方空格輸入數值。
當時間排程到期時，重新設定額度爲預設值(Reset quota automatically)	設定此檔的預設時間額度與資料額度。當排程時間已到，路由器將會自動使用預設的額度設定。 **啓用** – 勾選此方框使用預設的時間與資料額度值。 **預設時間額度** – 輸入時間額度數值 **預設資料額度** – 輸入資料額度數值。
內部 RADIUS (Internal RADIUS)	勾選此框啓用透過 RADIUS 伺服器驗證安全性。
本機 802.1X(Local 802.1X)	勾選此框啓用透過 802.1X 伺服器驗證安全性。

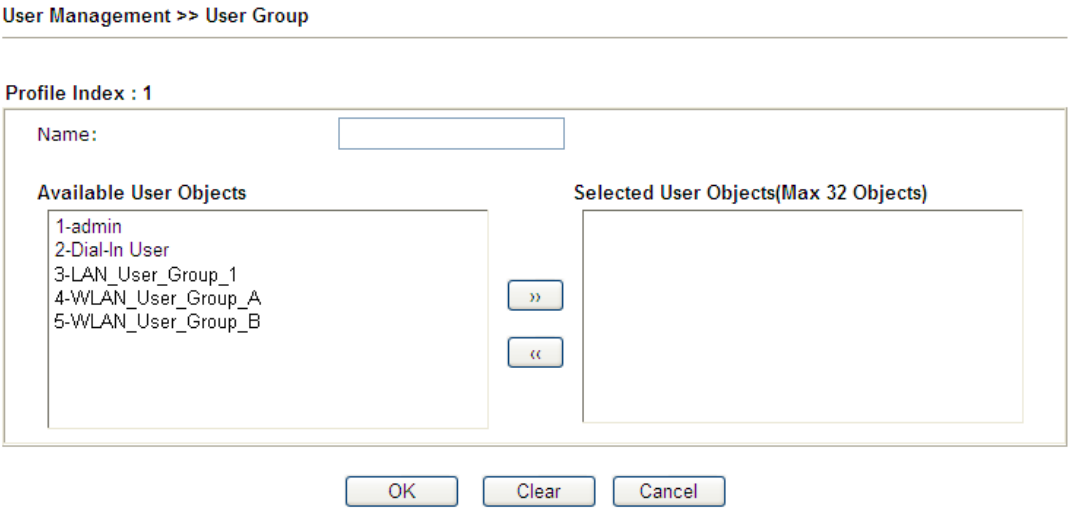
完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

VII-3-3 使用者群組(User Group)

本頁可讓您將數個使用者設定檔歸類成一個使用者群組，這裡所設定的群組也會在**防火牆>>基本設定(Firewall>>General Setup)**中當成過濾器規則來應用。



按下任何一個索引編號連結開啓如下頁面：



可用設定說明如下：

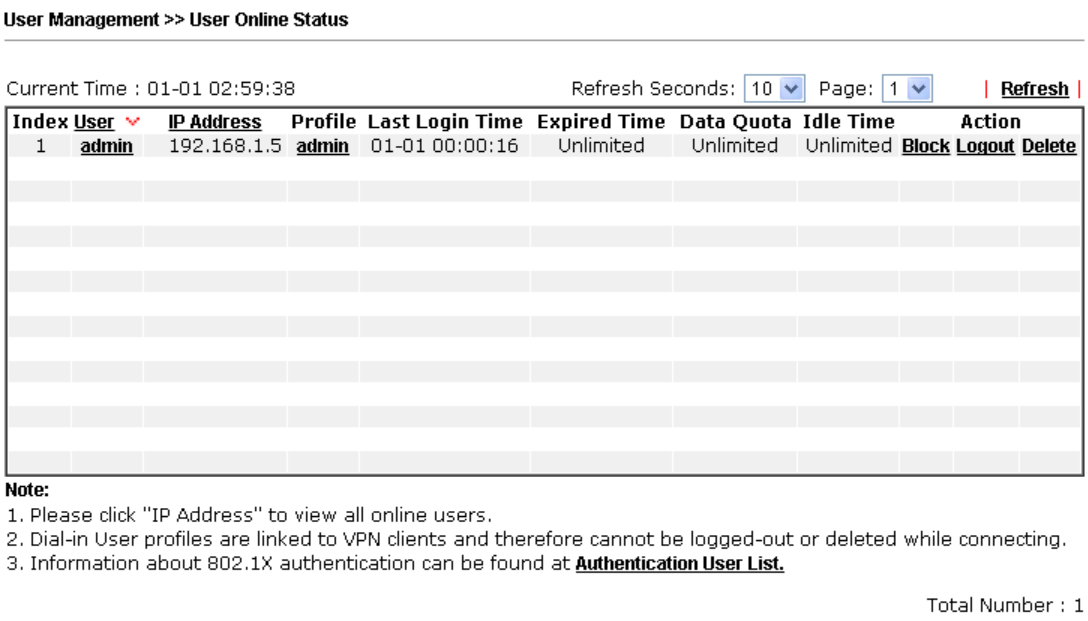
項目	說明
名稱(Name)	輸入使用者群組的名稱。
可用的使用者物件 (Available User Objects)	您可以將數個使用者設定檔(物件)組合爲一個群組，所有可用的使用者物件都會顯示在此區域內，特別注意的是使用者物件 Admin 以及 Dial-In User 乃是預設的物件，可以供您自由設定的物件檔則是編號爲 3, 4, 5 及之後物件連結。

選定的使用者物件 (Selected Keyword Objects)	按下 » 按鈕將選定的使用者物件移至本區。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

VII-3-4 使用者線上狀態(User Online Status)

本頁呈現連接至路由器的使用者，且在固定的間隔時間會自動更新頁面。



可用設定說明如下：

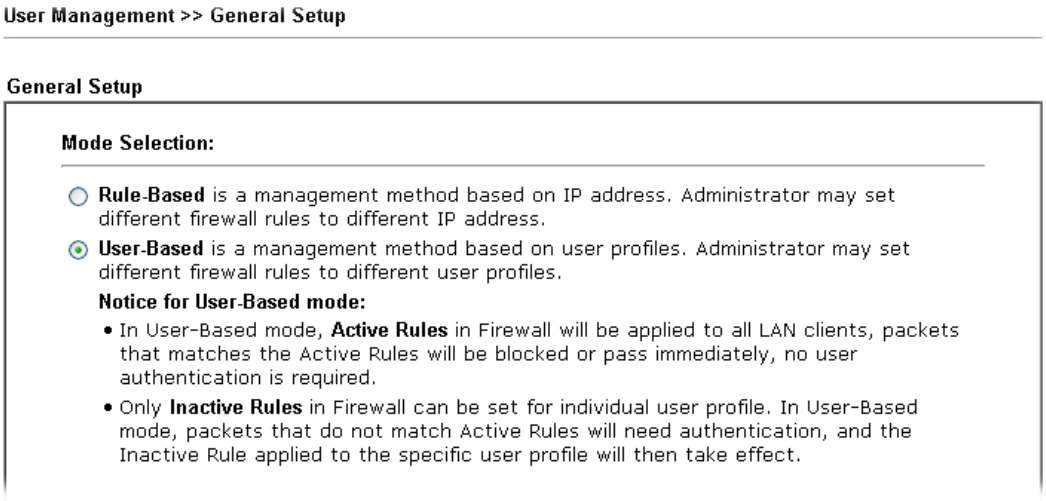
項目	說明
更新秒數 (Refresh Seconds)	使用下拉式清單選擇時間間隔，讓系統於固定時間更新本頁內容。
更新頁面(Refresh)	按下此鈕立即更新頁面。
索引編號(Index)	顯示線上使用者的順序編號。
使用者(User)	顯示目前連結至路由器的使用者，您可按下檔名稱下方連結開啓該使用者設定檔頁面。
IP 位址(IP Address)	顯示裝置的 IP 位址。
設定檔(Profile)	顯示使用者的權限。
上次登入時間 (Last Login Time)	顯示使用者上次登入路由器的時間。
到期時間(Expired Time)	顯示使用者使用網路的到期時間。
資料額度(Data Quota)	顯示資料傳送的額度。
閒置時間(Idle Time)	顯示設定檔的閒置時間設定。

動作 **(Action)**	**封鎖(Block)** - 封鎖使用者使用網路。 **解鎖(Unblock)** – 解除使用者使用網路 **登出(Logout)** – 強迫使用者登出。

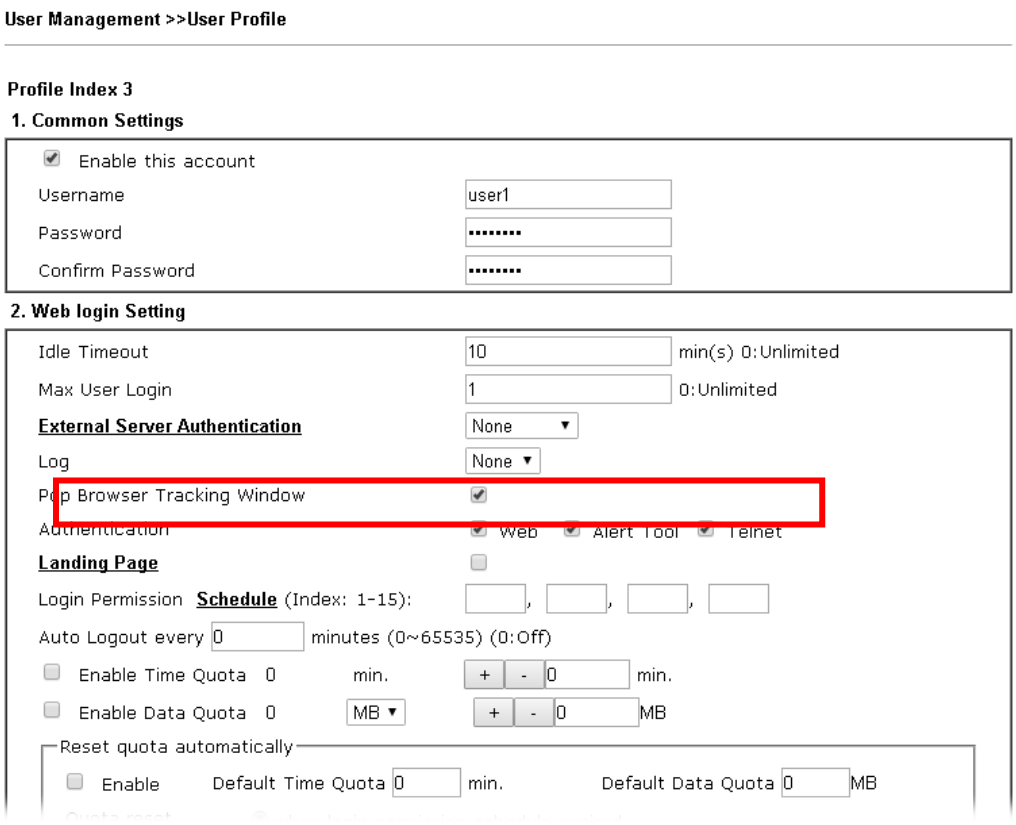
應用說明

A-1 如何透過使用者管理驗證用戶端

在開始設定**使用者管理(User-Based)**功能時，請先確認已經將模式更改爲**使用者模式(**於**使用者管理 >> 基本設定(User Management>>General Setup)**網頁下)。



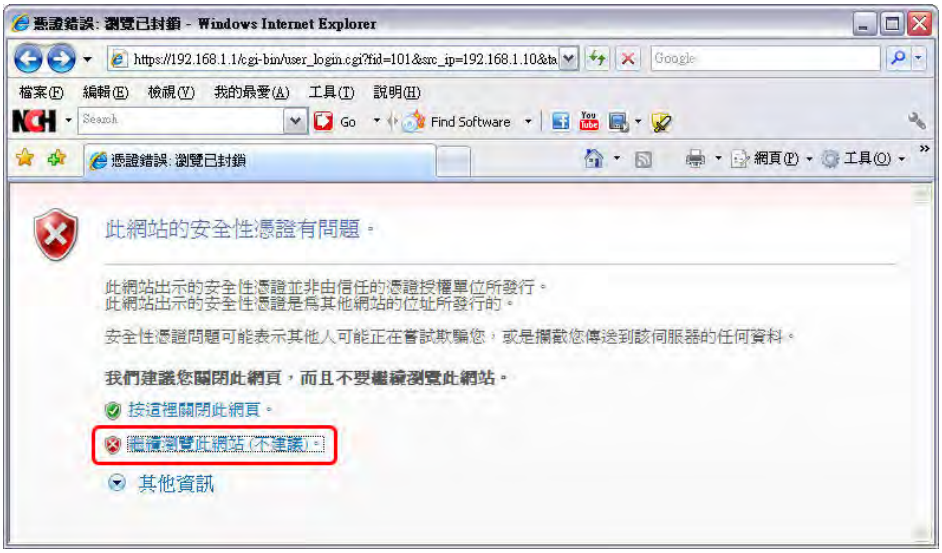
利用**使用者管理(User Management)**功能，在未提供正確的使用者帳號與密碼之前，任何一個用戶都不允許利用此路由器存取網際網路。系統提供三種驗證方式供用戶參考使用**網頁(Web)**、**Telnet** 以及**警告工具(Alert Tool)**。



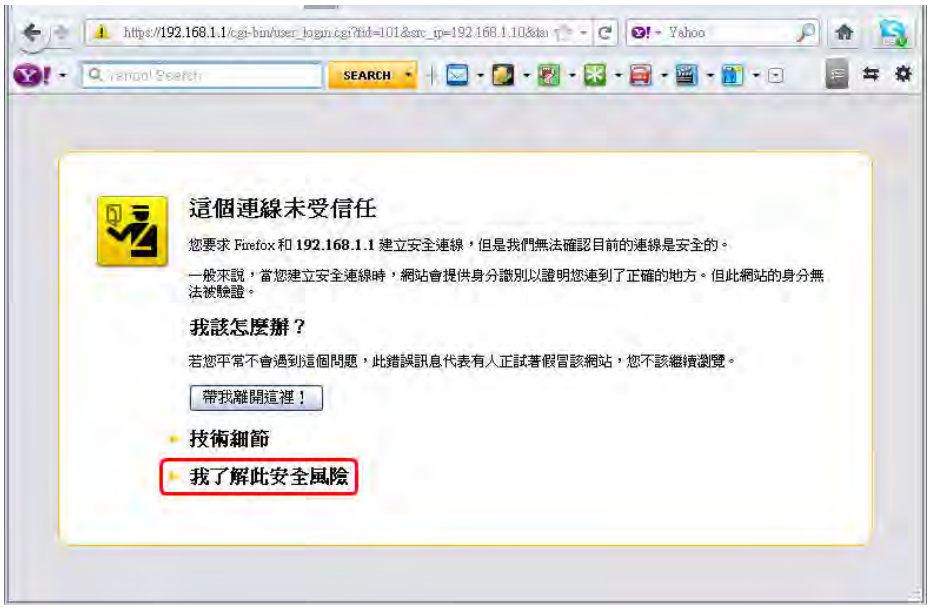
透過網頁驗證

透過網頁驗證有三個層面需注意：

- 假如區域網路用戶在沒有通過驗證的情形下，利用瀏覽器開啓某個外部網站，他會被系統先導引至路由器的網頁驗證介面，用戶可能會嘗試存取 http://www.draytek.com 網站，但系統會他帶至路由器的驗證頁面。由於這種連線屬於 SSL 連線方式，某些網頁瀏覽器可能會在驗證頁面出現之前，先出現警告訊息。參考下述：
  - 如果使用的是微軟的 Internet Explorer 瀏覽器，您看到的警告訊息顯示如下圖，請按下**繼續瀏覽此網站(不建議)**。



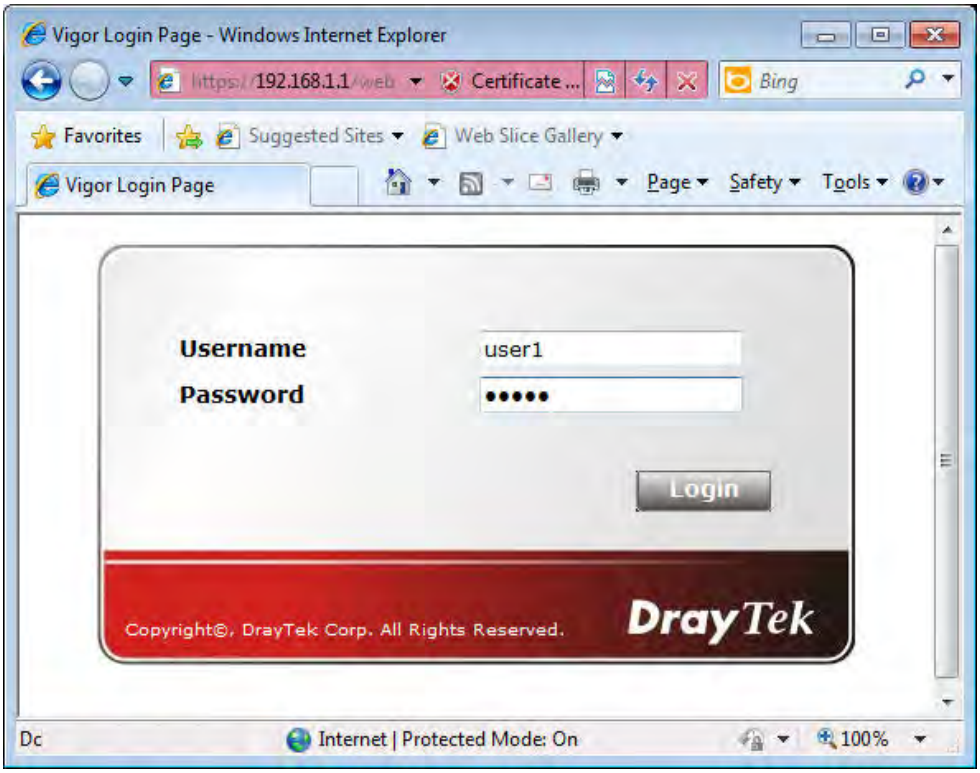
  - 如果使用的是 Mozilla Firefox 瀏覽器，您看到的警告訊息顯示如下圖，請選擇 **我了解此安全風險。**



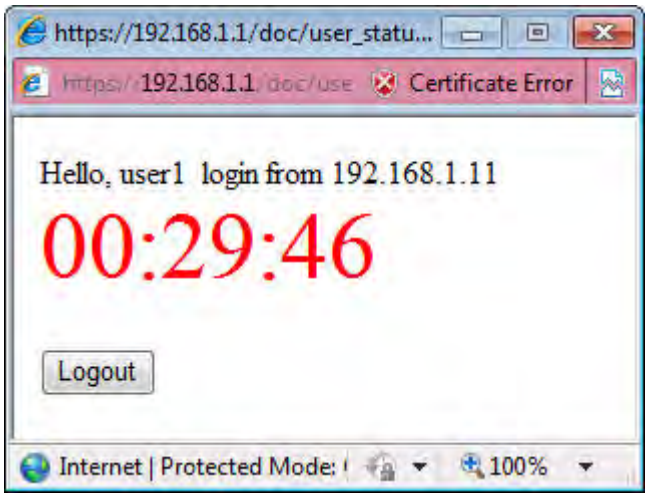
- 如果使用的是 Chrome 瀏覽器，您看到的警告訊息顯示如下圖，請按**仍要繼續**。



之後，網頁驗證視窗就會打開，請輸入您在**使用者管理**所定義的使用者名稱及密碼，然後按下**登入(Login)**。

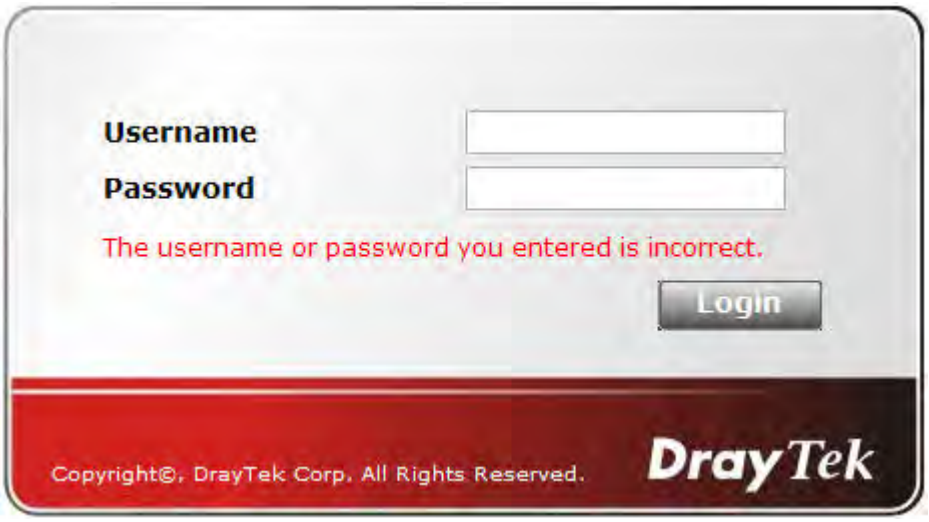


如果驗證成功，用戶即可被導引至想要進入的網站，例如本例中所說的 http://www.draytek.com，接著，使用者還可以看到如下圖所示的視窗，後續就可以進入網際網路瀏覽所需的網頁了。



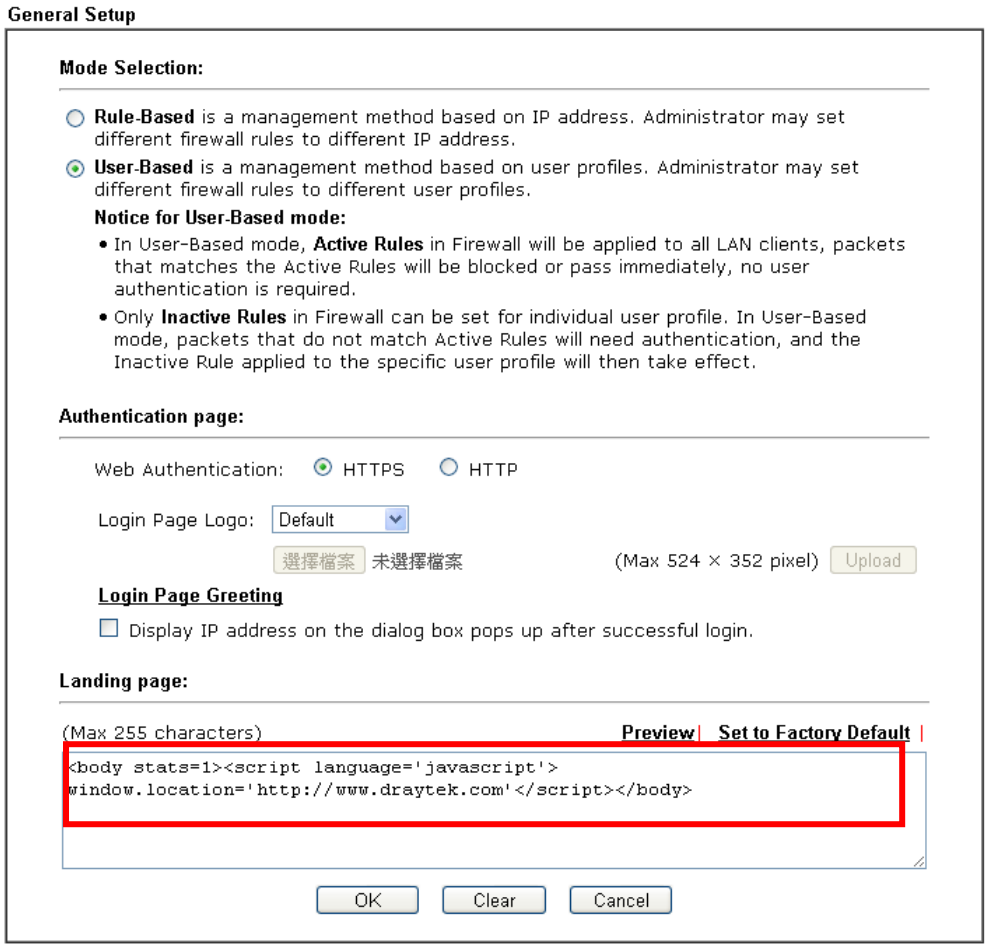
請注意，如果您有設定不准網頁瀏覽器跳出任何視窗，這個視窗便不會正常顯示出來。

如果驗證失敗，您會看到畫面出現錯誤訊息如: **The username or password you entered is incorrect.**，請再輸入一次使用者名稱及密碼。

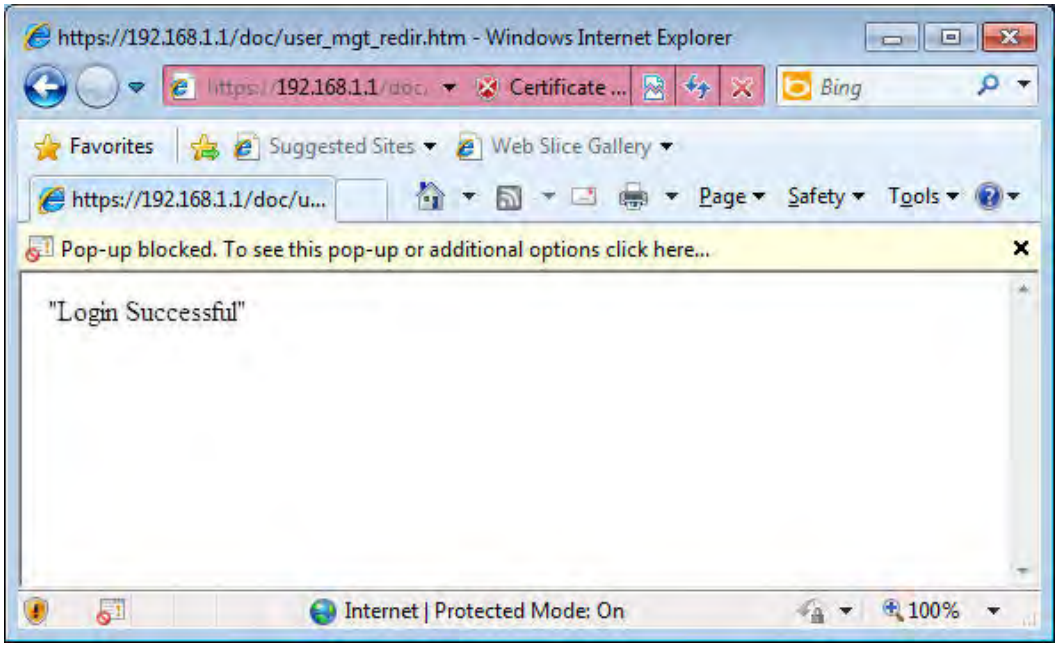


- 在上述說明中，您想進入外部網站因而啓動驗證程序，您也可以直接進入路由器的網頁介面進行驗證動作，HTTP 與 HTTPS 這二種協定系統都有支援，例如 http://192.168.1.1 或 https://192.168.1.1 。如果您的路由器 LAN IP 位址不是 192.168.1.1，您可以替換成實際的位址，預設的管理埠號若已變更，也請在網址後面加上埠號。.

  若驗證成功，您可以看到**使用者管理>>基本設定(User Management >> General Setup)** 中所輸入的歡迎訊息。



因爲歡迎訊息的預設內容是**<body stats=1><script language='javascript'> window.location='http://www.draytek.com'</script></body>**之故，您將被導引至 http://www.draytek.com，如有需要，您可以更改本區的內容。例如在歡迎訊息中輸入 **Login Successful**，等下看到的歡迎訊息就會變成下圖所示的內容：

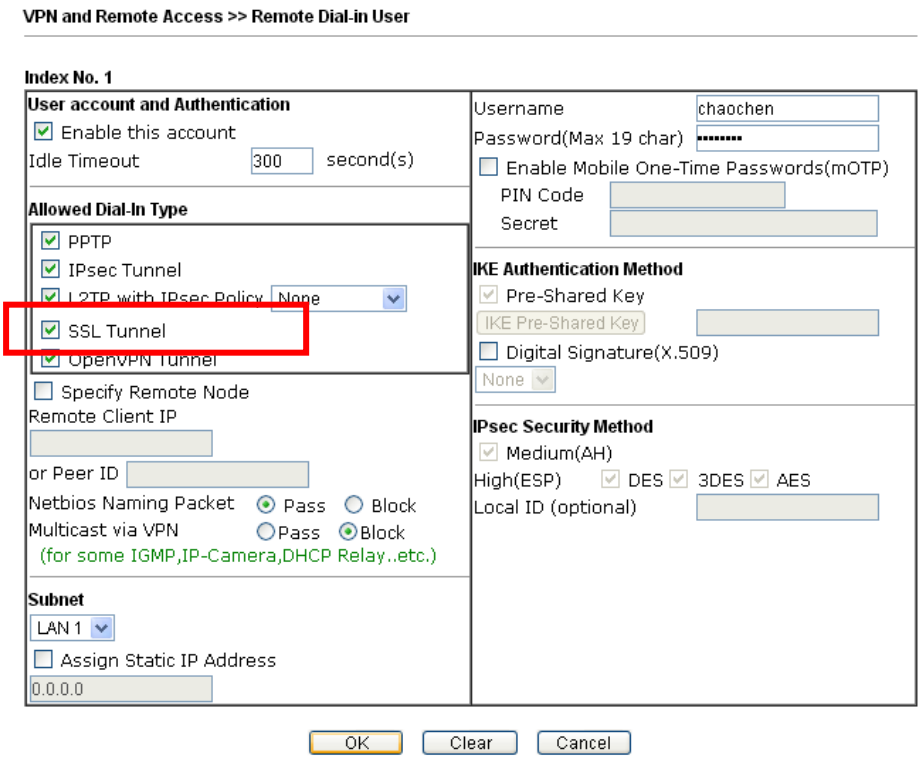


如果您沒有設定不准網頁瀏覽器跳出任何視窗，您還會看到上面所提到的跳出視窗。

- 請勿讓**使用者管理(User Managemen)**的使用者設定檔，與 VPN 遠端撥入帳號使用者設定檔使用相同的帳號名稱(使用者名稱)，否則，您可能會收到不預期的結果，因爲 VPN 遠端撥入使用者設定檔可以讓**使用者管理**中的設定檔延伸驗證之用，如果您需要更進一步的說明，可以參考**預設使用者設定檔的用法**。

  當 VPN 設定檔與使用者管理帳號共享相同的使用者名稱時：

  - 假設 VPN 設定檔中**啓動**了 **SSL Tunnel** 或 **SSL Web Proxy** 類型，**使用者管理(User Management)**中的設定檔就無法用來驗證，例如您建立一個使用者設定檔，帳號/密碼設定爲 **chaochen/test**，而 VPN 遠端撥入帳號設定檔使用相同的使用者名稱(**chaochen**)，但密碼改設爲 1234，透過網頁驗證程序，您只會收到一個錯誤訊息 --**The username or password you entered is incorrect**。

  - 假設 VPN 設定檔中**並未啓動 SSL Tunnel** 或 **SSL Web Proxy** 類型，**使用者管理**與 **VPN** 遠端撥入使用者設定檔就能使用相同的使用者名稱**(chaochen)**，即使密碼不同也沒關係。不過，我們仍然建議您在不同的**使用者管理**設定檔與 VPN 設定檔中，使用不同的使用者名稱(帳號)。

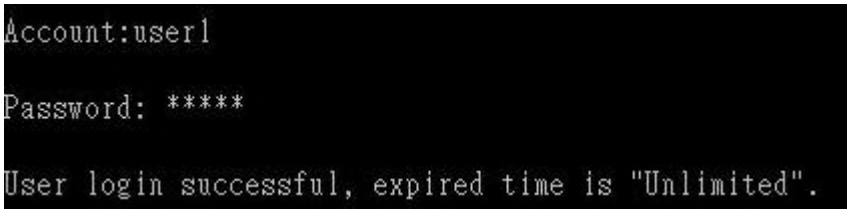
透過 Telnet 驗證

區域網路端的用戶也可以透過 Telnet 使用其帳戶。

1. 請利用 Telnet 打上 LAN IP 位址進入路由器 Telnet 相關頁面，輸入帳號名稱，以便執行驗證。



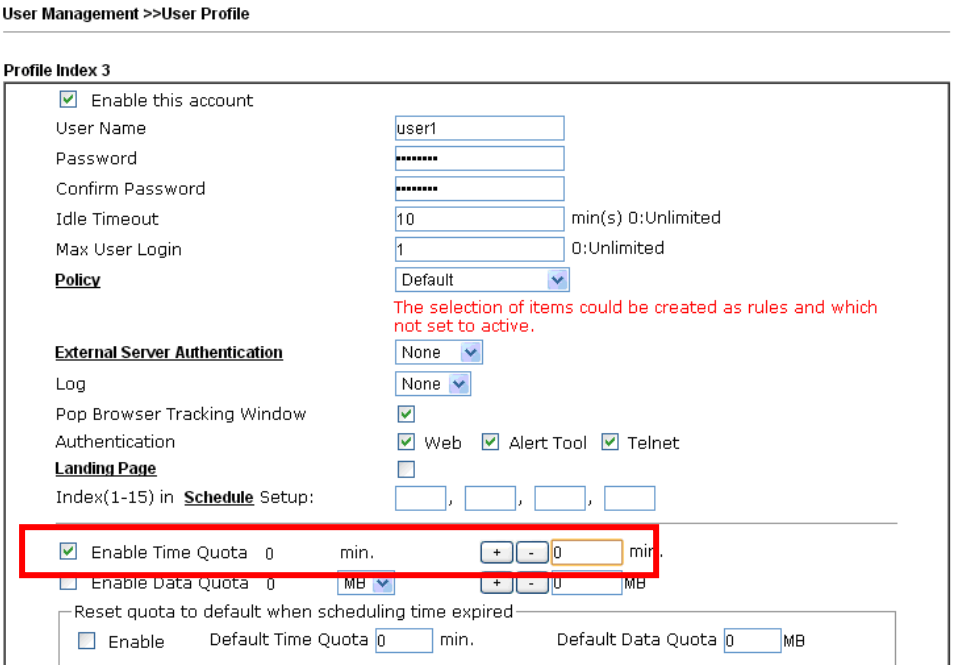
2. 輸入密碼執行驗證並按下 **Enter** 鍵，畫面出現 **User login successful** 以及有效時間(若有事先設定)。



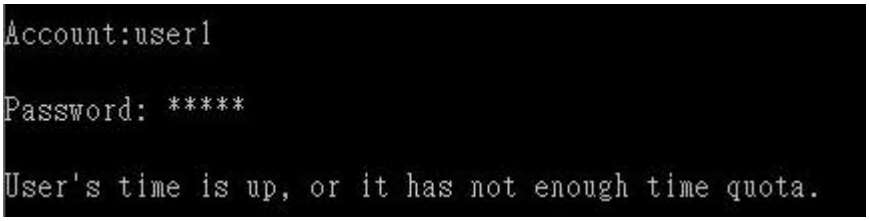
資訊

有效時間若是設定爲 **Unlimited**，即表示**時間定額(Time Quota)**功能並未啓動，在您登入後，該帳號在未登出之前都是有效的。

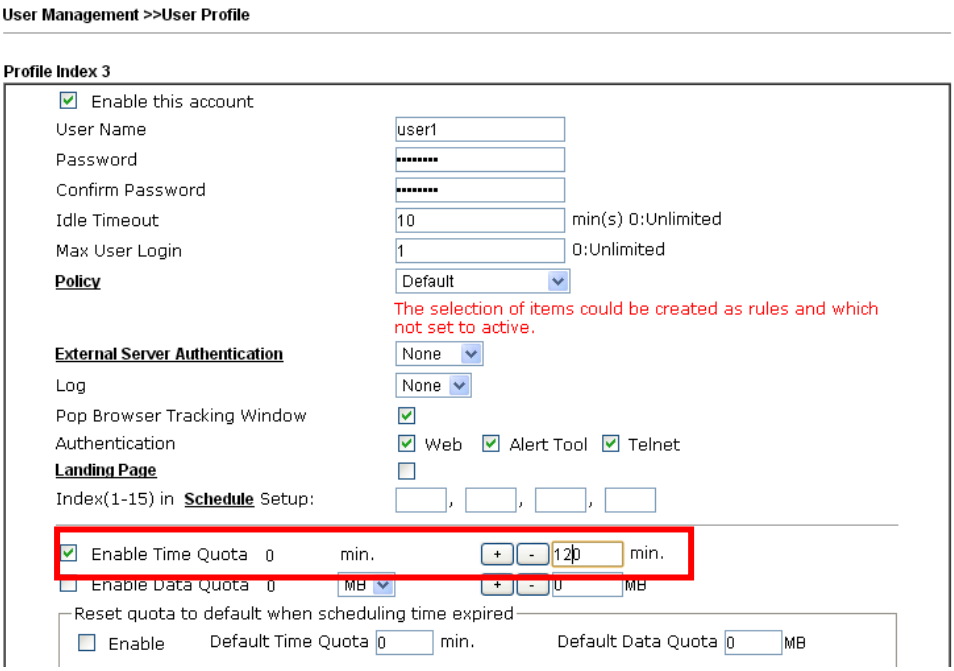
3. 在路由器的網頁設定上，**時間額度(Time Quota)**的設定畫面如下**:**



4. 如果您勾選了啓動**時間額度(Time Quota)**並將時間設定爲 **0**，即表示該帳號沒有時間限制。



如果**時間額度(Time Quota)**已啓動，且設定了時間，



在您登入 telnet 之後即可看見時間限制。



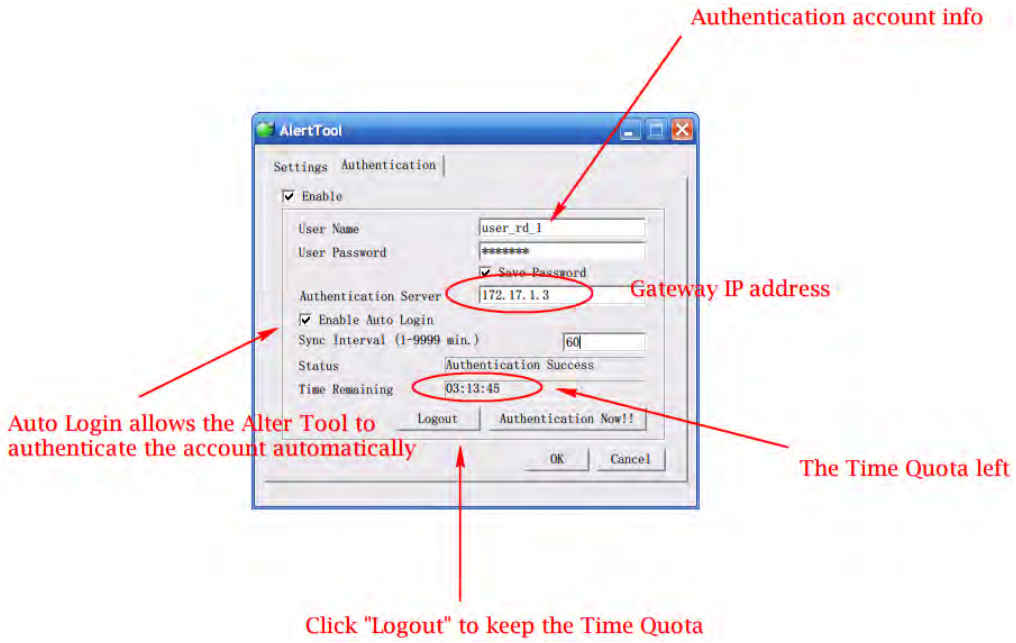
在經過系統允許的時間後，您就無法使用這個帳號了，除非讓管理者爲使用者手動增加使用時間。

透過 VigorPro Alert Notice Tool 驗證

透過網頁或 Telnet 驗證使用者是很方便沒錯，但有些限制存在。如果利用 VigorPro Alert Notice Tool 來操作驗證程序，最大的優勢就是可以自動登入。當路由器爲使用者帳號所設定的逾時時間到達時，路由器將停止用戶端電腦進入網際網路，直到該用戶再執行一次驗證程序，透過 VigorPro Alert Notice Tool 的驗證程序可以讓使用者設定重新驗證的間隔，這樣一來，工具會定期傳送驗證需求，讓用戶不必一次又一次不斷的提出驗證需求。

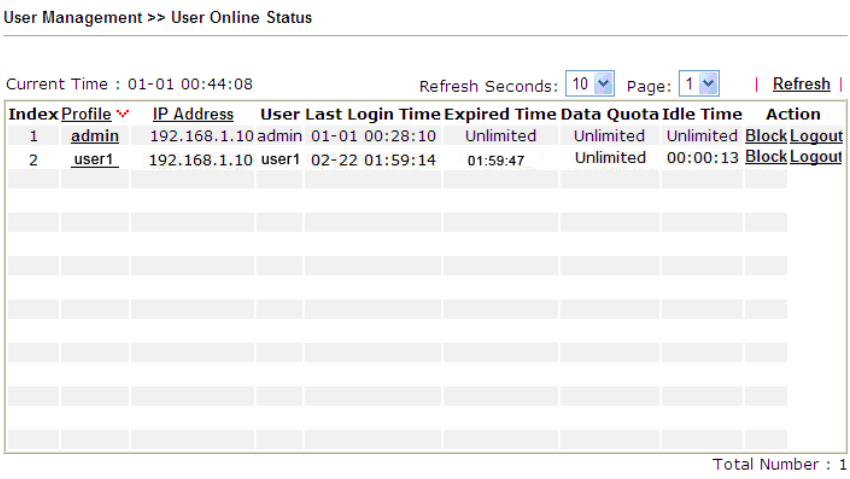
VigorPro Alert Notice Tool 的設定如下：

1. 按 **Authenticate Now!!** 開始執行驗證動作。



2. 請自居易官網取得 **VigorPro Alert Notice Tool** 工具：
http://www.draytek.com

資訊 1	任何一次的防火牆策略修正都會中斷目前使用中的使用者網路連線，使用者必須重新驗證才能繼續使用網際網路。
資訊 2	管理者可以從**使用者線上狀態(User Online Status)**檢查目前的使用者使用情形。

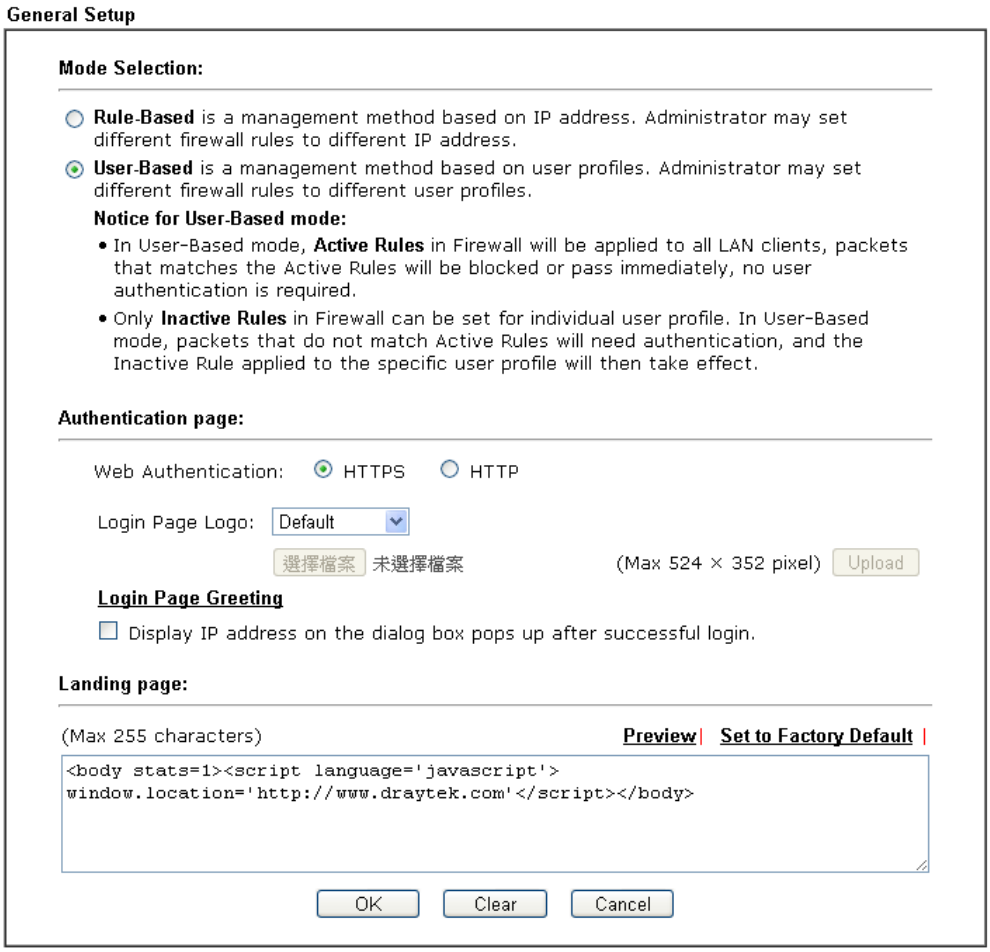


A-2 如何使用指定首頁功能

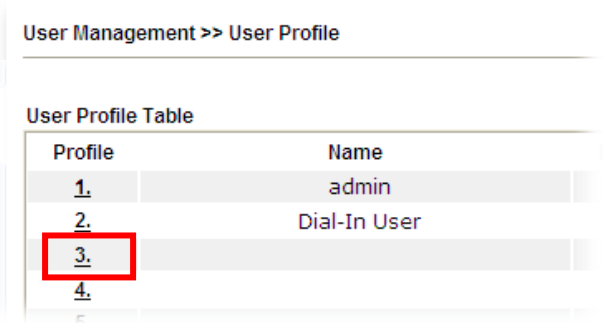
指定首頁(Landing Pag)是**使用者管理(User Management)**選單下一個特殊的功能，它可讓通過驗證的使用者登入網頁看見的指定訊息及內容。

範例 1：使用者可在成功登入網際網路後看見指定的訊息

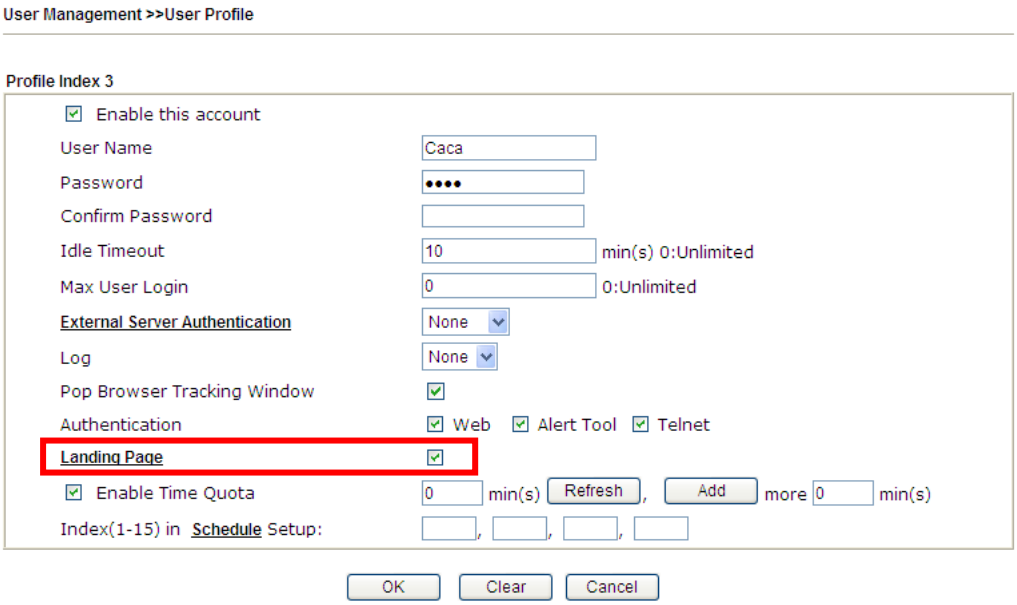
1. 進入路由器的使用者設定介面。
2. 開啓**使用者管理>>基本設定(User Management>>General Setup)**，選擇**使用者模式(User-Based)**，並在訊息框內輸入**"Login Success "**字樣，最多不要超過 255 個字元，接著按下**確定(OK)**按鈕儲存設定。



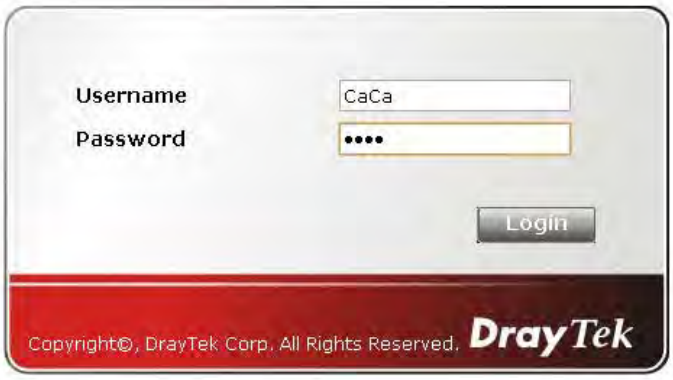
3. 現在您可以啓用指定首頁功能，開啓**使用者管理>>使用者設定檔(User Management >> User Profile)**，建立一個新的使用者設定檔案。



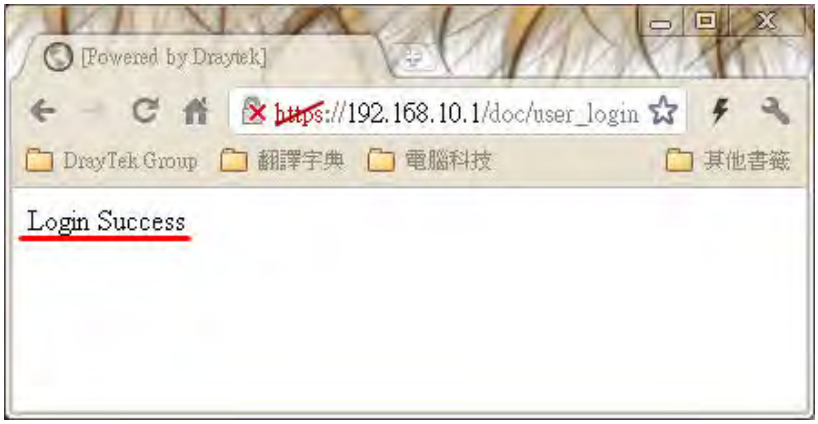
4. 按下任一連結(例如#3)開啓如下頁面，輸入使用者名稱以及密碼，勾選指定首頁方框，然後按下**確定(OK)**按鈕儲存。



5. 在相同的瀏覽器(IE 7.0/FireFox 或更新版本)下開啓另外一個視窗，或是開啓新的瀏覽器。再次登入路由器的使用者介面，在輸入正確的使用者名稱及密碼。



6. 按下**登入(Login)**。如果登入成功，您可以在瀏覽器上看見 **Login Success** 登入成功字樣。

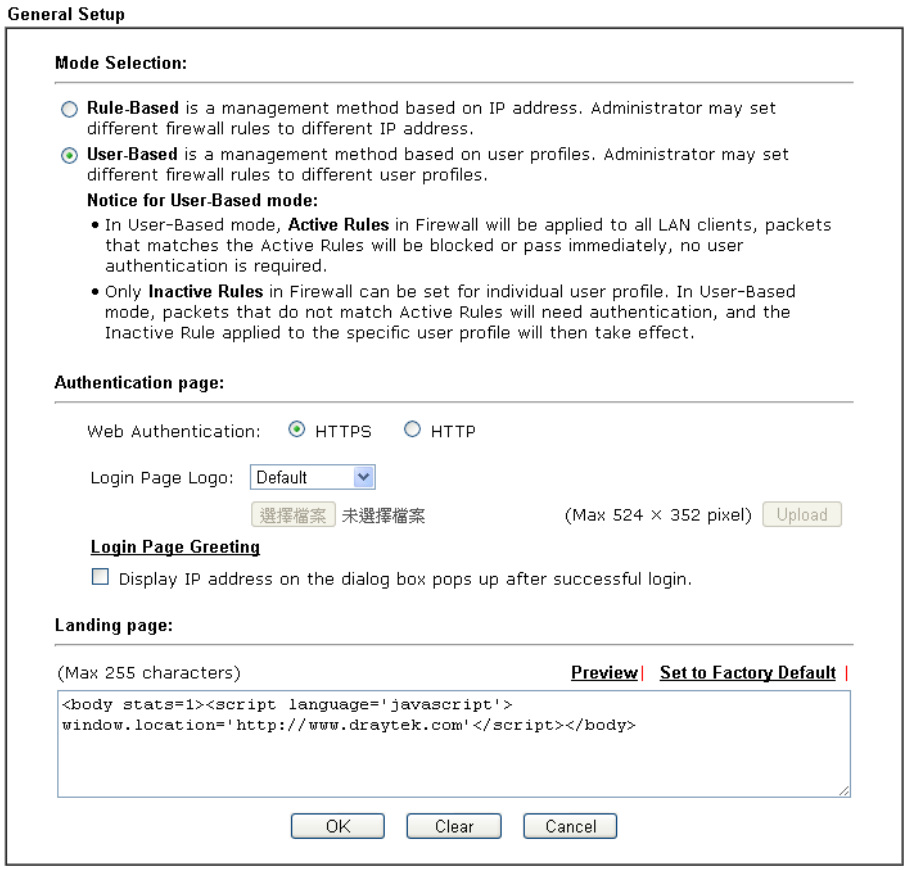


範例 2：成功登入網際網路後，系統將自動連接至 http://www.draytek.com

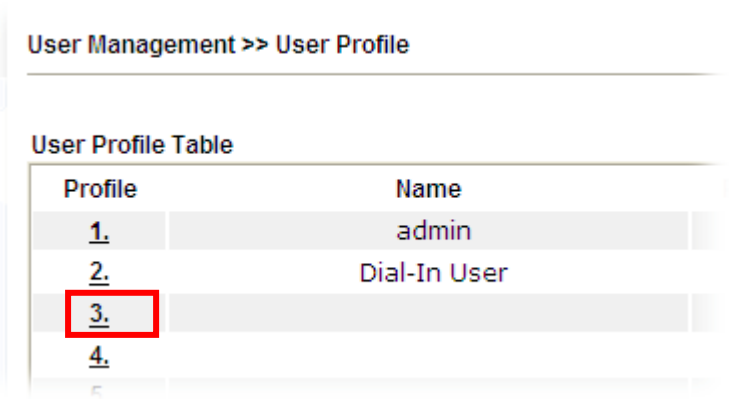
1. 在**指定首頁(Landing Page)**區域中，輸入如下資料：

   “ <body stats=1><script language='javascript'>

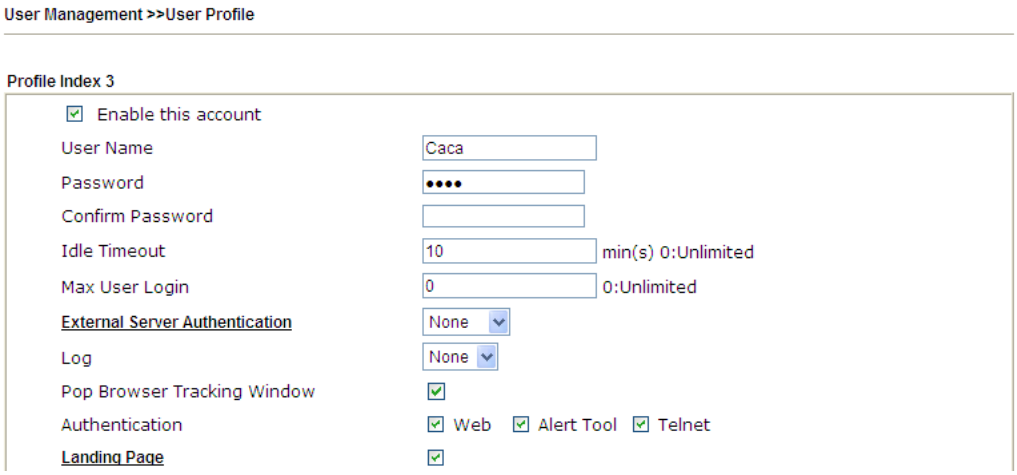
   window.location='http://www.draytek.com'</script></body>”



2. 現在您可以啓用指定首頁功能，開啓**使用者管理>>使用者設定檔(User Management >> User Profile)**，建立一個新的使用者設定檔案。



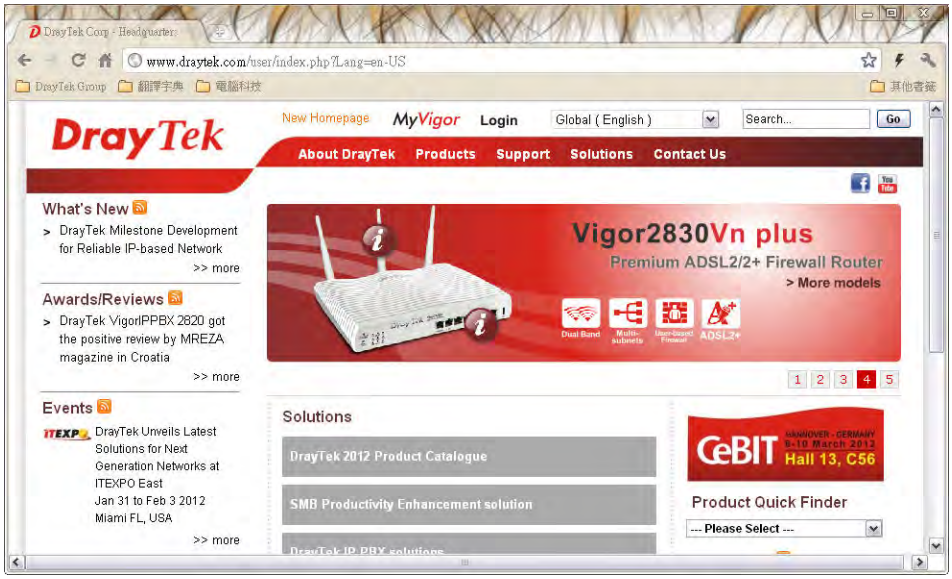
3. 按下任一連結(例如#3)開啓如下頁面，輸入使用者名稱以及密碼，勾選指定首頁方框，然後按下**確定(OK)**按鈕儲存。



4. 在相同的瀏覽器(IE 7.0/FireFox 或更新版本)下開啓另外一個視窗，或是開啓新的瀏覽器。再次登入路由器的使用者介面，在輸入正確的使用者名稱及密碼。



5. 按下**登入**，若是登入成功，您可以直接進入居易公司的官網。



VII-4 客製化入口網站設定(Hotspot Web Portal)

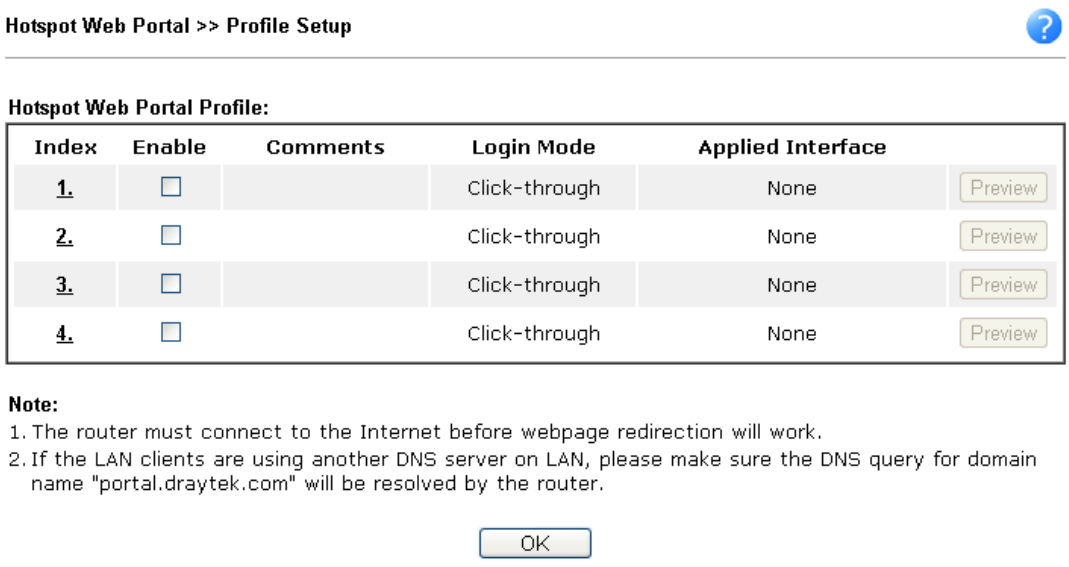
客製化入口網站設定可讓您設定數個設定檔，利用指定 URL 的方式，讓無線用戶/LAN 用戶在登入網際網路時連結至指定的頁面。亦即不論該用戶的目的爲何，都會先被強制導入此頁所指定的網頁。換句話說，若公司行號想要爲其產品對用戶進行廣告宣傳，就可利用此頁面達到不錯的效果。

網頁使用者介面



VII-4-1 設定檔配置(Profile Setup)

選擇**設定檔配置(Profile Setup)** 建立或是修改入口網站設定檔，依照 LAN 子網、WLAN SSID、原始與目的 IP 位址等，最多可以設定 4 個設定檔以因應不同的需要。



可用設定說明如下：

項目	說明
索引編號(Index)	按下索引編號連結可以檢視或是更新設定檔內容。
啓用(Enable)	勾選此框以便啓動此設定檔。
註解(Comments)	顯示此設定檔的說明。
登入模式(Login Mode)	顯示設定檔使用的登入模式。
套用介面(Applied Interface)	顯示設定檔套用的介面。
預覽(Preview)	按此紐預覽即將顯示給使用者觀看的入口網站頁面。

VII-4-1-1 登入模式(Login Modes)

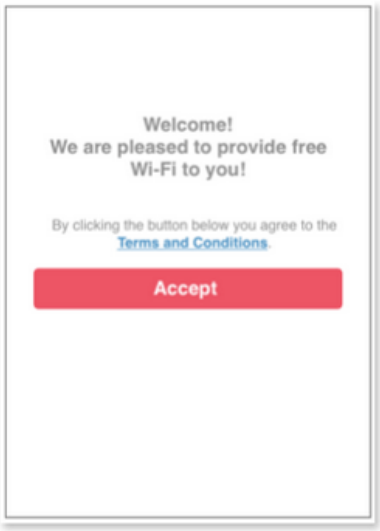
有 5 種登入模式可以用來驗證網路用戶：**跳過登入(Skip Login)**、**透過點擊(Click Through)**、**社群登入(Social Login)**、**PIN 登入(PIN Login)**、**社群或是 PIN 登入(Social or PIN Login)**，每種模式都會帶出不同的網頁。

跳過登入(Skip Login)

這個模式不會執行任何驗證，系統將直接導引使用者至指定首頁，之後使用者可以離開該頁面前網希望造訪的網站。

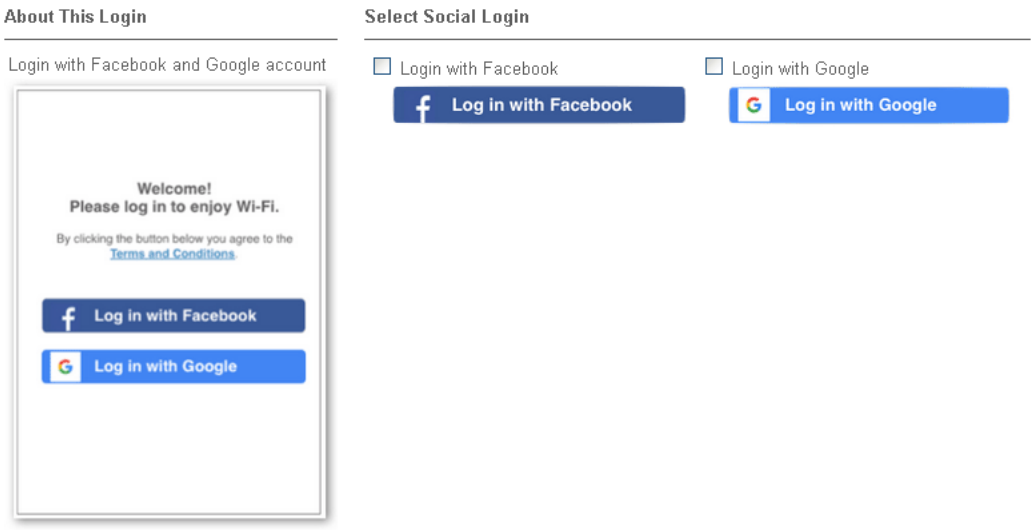
透過點擊(Click Through)

當使用者第一次嘗試登入網際網路時，系統會呈現如下頁面。再按下頁面上的**接受(Accept)**按鈕後，使用者將被導引至指定首頁，然後許可登入網際網路。



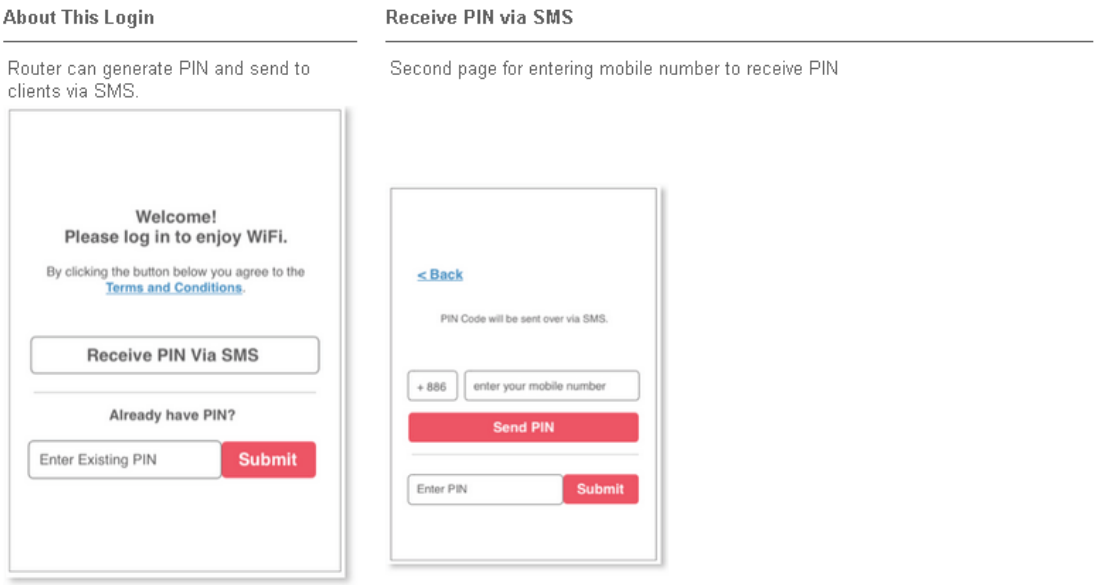
社群登入(Social Login)

當使用者第一次嘗試登入網際網路時，系統會呈現如下頁面。使用臉書或是 Google 帳號進行驗證之後，使用者將被導引至指定首頁，然後許可登入網際網路。



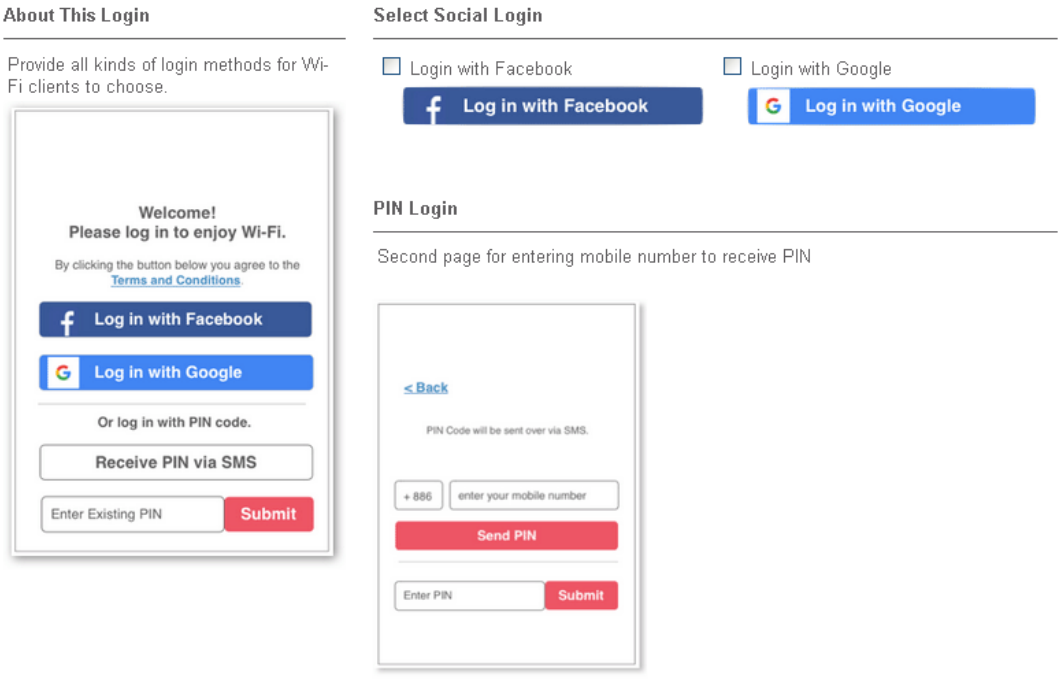
PIN 登入(PIN Login)

當使用者第一次嘗試登入網際網路時，系統會提示使用者輸入行動電話號碼或是透過簡訊接收 PIN 碼，之後使用者輸入 PIN 碼以驗證自身，將被導引至指定首頁，然後許可登入網際網路。



社群或是 PIN 登入(Social or PIN Login)

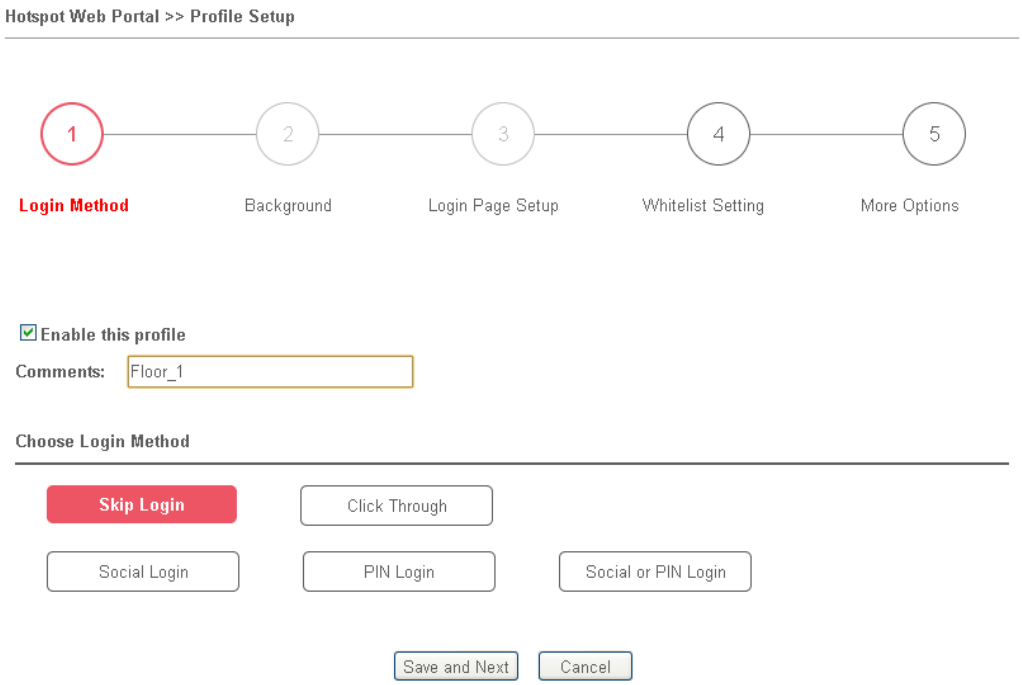
系統會呈現**社群登入(Social Login)**與 **PIN 碼登入(PIN Code Login)**二種模式給使用者，讓使用者選擇喜好的模式進行驗證。



VII-4-1-2 設定入口網站設定檔步驟

1. 登入模式(Login Method)

按下選定設定檔的索引編號連結(例如 #1)顯示如下頁面。



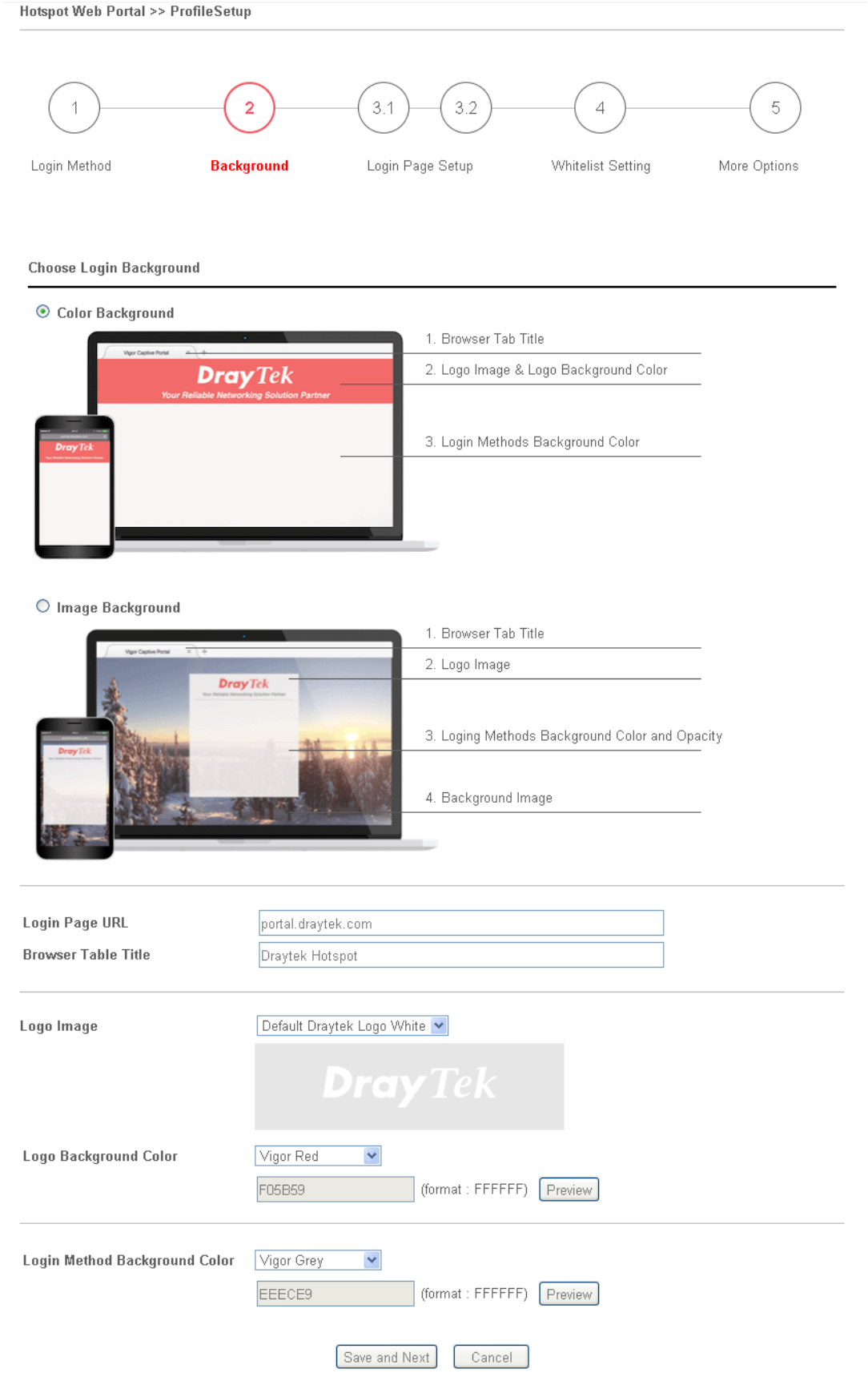
可用設定說明如下：

項目	說明
啓用此設定檔(Enable this profile)	勾選此框啓用此設定檔。
註解(Comments)	輸入可以辨識此設定檔的說明內容。
選擇登入模式(Choose Login Method)	選擇想要的登入模式。
儲存與下一頁(Save and Next)	按此儲存本頁的設定並進入下一頁。
取消(Cancel)	按此捨棄本頁設定並回到前一頁。

若您已經選擇**跳過登入(Skip Login)** 作爲登入模式，請直接跳至步驟 4 *白名單(Whitelisting)*。其他模式請繼續依循步驟 2 與 3 進行。

2. 背景(Background)

若您選擇需要驗證的登入模式，請選擇登入頁面的背景圖樣。



可用設定說明如下：

項目	說明
選擇登入背景	選擇**顏色背景(Color Background)**或是**影像背景(Image**

(Choose Login Background)	**Background**)作爲登入頁面的背景方案。
登入頁面 URL(Login Page URL)	輸入登入頁面的 URL。
瀏覽器標籤標題 (Browser Tab Title)	輸入顯示在瀏覽器網頁的標題文字。
商標影像(Logo Image)	預設狀態下會顯示居易商標，您可以輸入 HTML 文字或是上傳影像取代預設商標影像。
商標背景顏色(Logo Background Color)	從事先定義的顏色清單中選擇商標的背景顏色，或是選擇**客製化顏色 (Customize Color)**並輸入 RGB 值，按**預覽(Preview)**可以檢視選定的顏色。
登入方法背景顏色 (Login Method Background Color)	從事先定義的顏色清單中選擇登入面板的背景顏色，或是選擇**客製化顏色(Customize Color)**並輸入 RGB 值，按**預覽(Preview)**可以檢視選定的顏色。
不透明度(Opacity (10 ~ 100))	當選擇影像背景時，可以設定背景影像的不透明度。
背景影像 (Background Image)	當選擇影像背景時，可以按**瀏覽(Browse...)**按鈕挑選影像檔案(格式爲.JPG 或.PNG)之後按**上傳(Upload)**將檔案上傳至路由器。
儲存與下一頁(Save and Next)	按此儲存本頁的設定並進入下一頁。
取消(Cancel)	按此捨棄本頁設定並回到前一頁。

若您已經選擇**跳過登入(Skip Login)** 作爲登入模式，請直接跳至步驟 4 *白名單(Whitelisting)*。

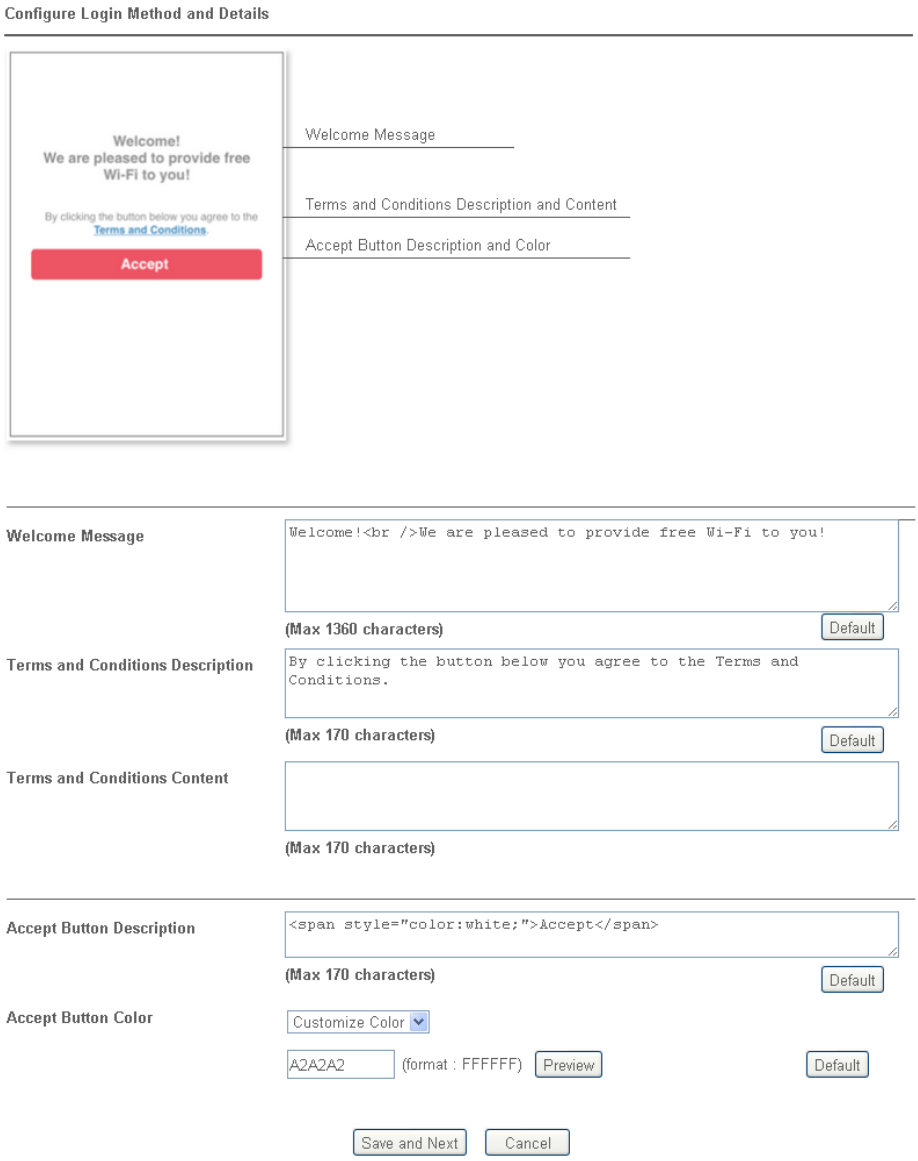
其他模式請繼續依循步驟 3 進行。

3. 登入頁面設定

在此步驟，您可以設定登入頁面的內容。

透過點擊(Click Through)

本節說明透過點擊(Click Through) 登入模式的頁面設定。



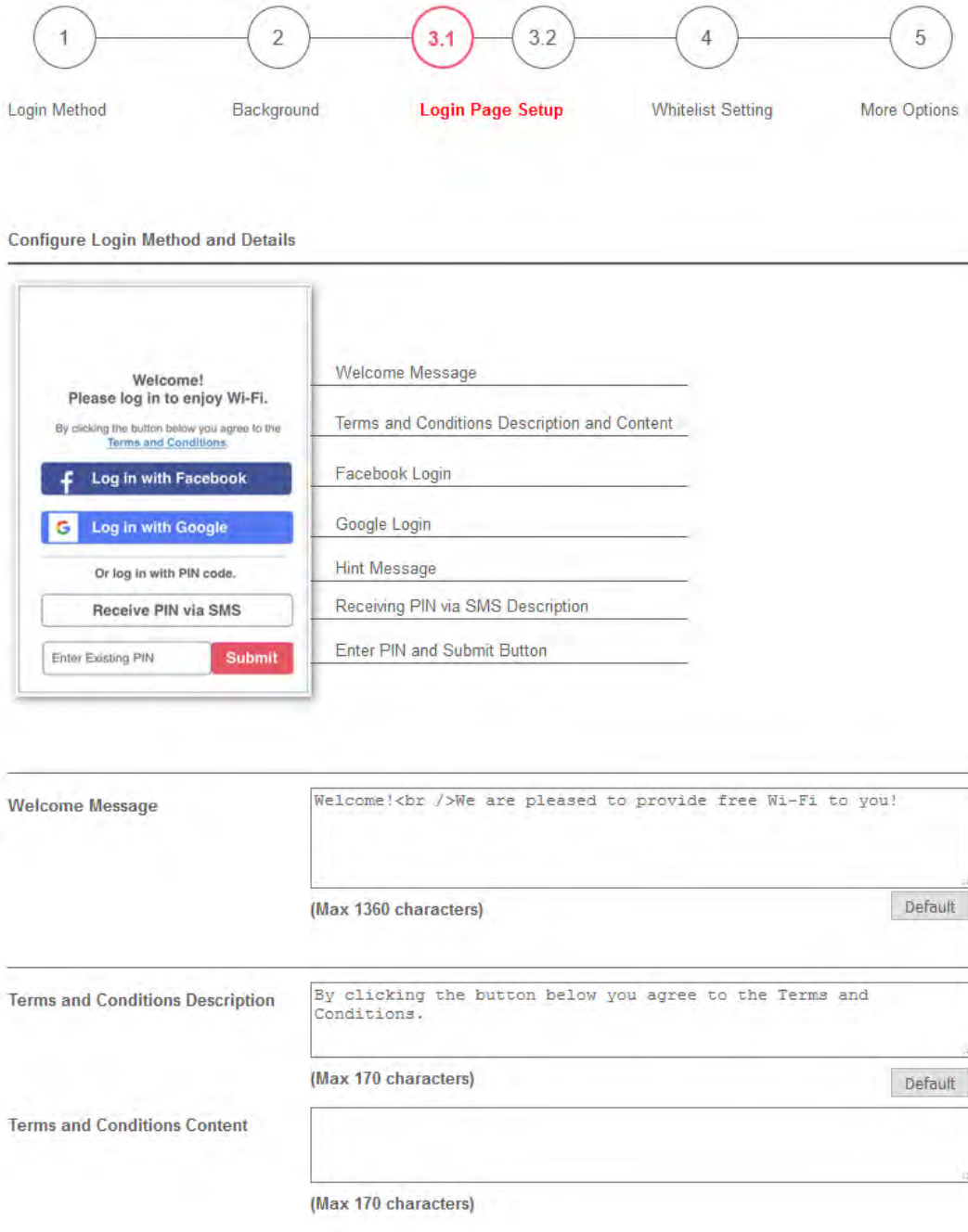
可用設定說明如下：

項目	說明
歡迎訊息(Welcome Message)	輸入顯示於歡迎訊息中的文字。
術語與條件說明 (Terms and Conditions Description)	輸入顯示在術語與條件連結上的文字。
術語與條件內文 (Terms and Conditions Content)	輸入顯示在術語與條件跳出視窗上的文字。
接受按鈕說明 (Accept Button Description)	輸入顯示在接受按鈕上的文字。 Enter the text to be displayed on the accept button
接受按鈕顏色 (Accept Button Color)	自事先定義的顏色清單中選擇接受按鈕的顏色，或是選擇**客製化顏色 (Customize Color)**並輸入 RGB 值。按下**預覽(Preview)**按鈕檢視選定的顏色。

儲存與下一頁(Save and Next)	按此儲存本頁的設定並進入下一頁。
取消(Cancel)	按此捨棄本頁設定並回到前一頁。

社群登入與 PIN 登入(Social Login and PIN Login)

本節說明 PIN 登入(PIN Login)以及/或社群登入(Social Login)登入模式的頁面設定。



相關設定於臉書、Google 與 PIN 驗證的共用設定爲：

項目	說明
歡迎訊息(Welcome Message)	輸入顯示於歡迎訊息中的文字。
術語與條件說明(Terms and	輸入顯示在術語與條件連結上的文字。

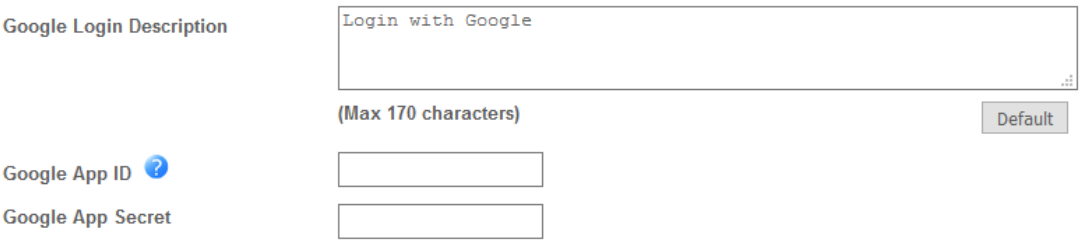
Conditions Description)	
術語與條件內文 (Terms and Conditions Content)	輸入顯示在術語與條件跳出視窗上的文字。

若您選擇了臉書登入(Facebook login)，設定頁面如下：



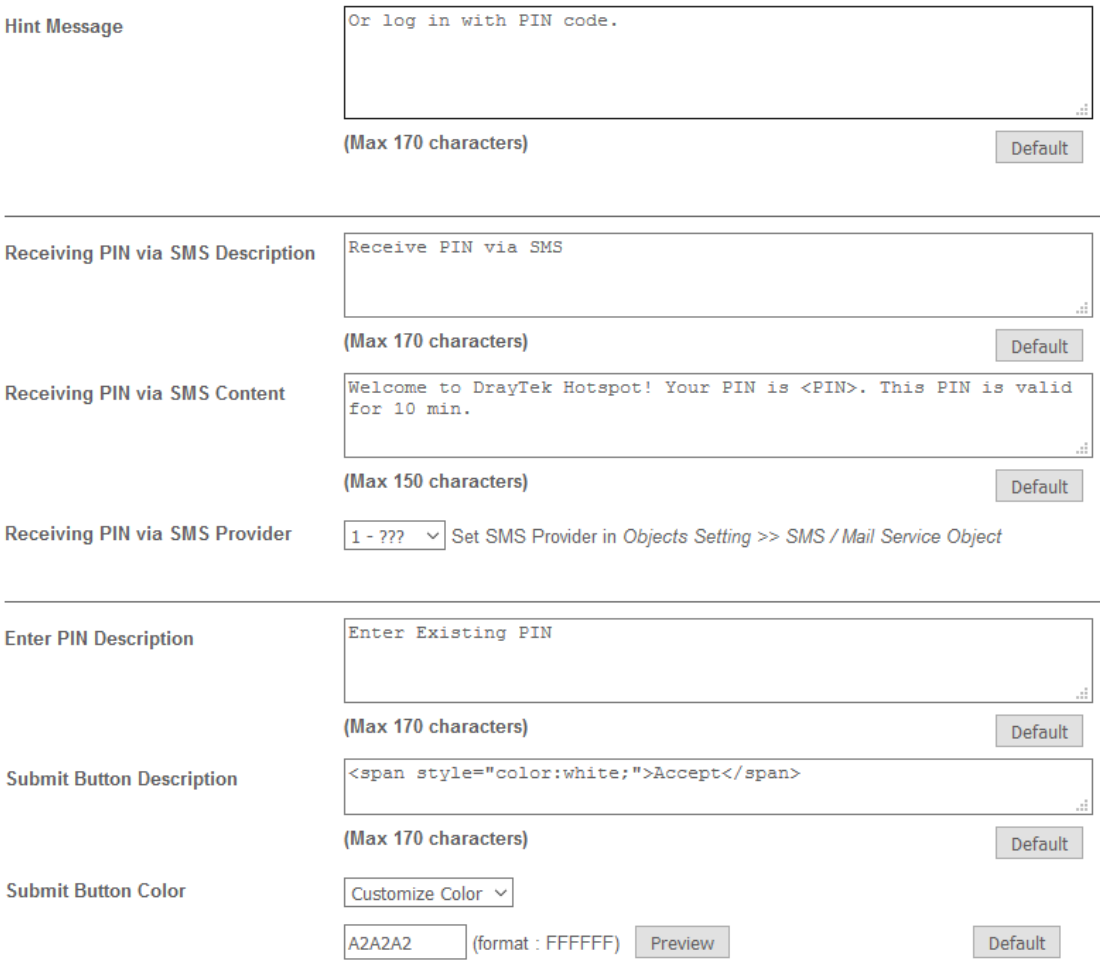
項目	說明
臉書登入說明 (Facebook Login Description)	輸入顯示於臉書登入按鈕上的文字。
臉書 APP ID (Facebook APP ID)	輸入有效的臉書開發商 APP ID。 如果您尚未有 APP ID，請參考節 A-1 如何建立臉書 APP ID 以利網頁入口驗證。
臉書 APP 密鑰 (Facebook APP Secret)	輸入上述 APP ID 需求之密碼。 詳情，請參考節 A-1 如何建立臉書 APP ID 以利網頁入口驗證。

若您選擇了 Google 登入(Google login)，設定頁面如下：



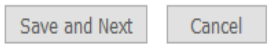
項目	說明
Google 登入說明 (Google Login Description)	輸入顯示於 Google 登入按鈕上的文字。
Google App ID	輸入有效的 Google APP ID。 請參考節 A-1 如果建立 Google APP ID 以利網頁入口驗證。
Google APP 密鑰 (Google App Secret)	輸入上述 APP ID 需求之密碼。 詳情，請參考節 A-1 如果建立 Google APP ID 以利網頁入口驗證。

若您選擇了 PIN 登入(PIN login)，設定頁面如下：



項目	說明
提示訊息(Hint Message)	輸入用來建議使用者選擇簡訊驗證方式的訊息。
透過簡訊說明接收 PIN 碼(Receiving PIN via SMS Description)	輸入使用者點選以接收簡訊 PIN 碼的按鈕上文字。
透過簡訊內容接收 PIN 碼(Receiving PIN via SMS Content)	輸入簡訊發送的文字，以便通知使用者 PIN 碼。其中<PIN>表明實際 PIN 碼的內容。
透過簡訊服務供應商接收 PIN 碼(Receiving PIN via SMS Provider)	選擇發送 PIN 通知的簡訊服務供應商。
輸入 PIN 說明(Enter PIN Description)	輸入顯示在 PIN 文字方塊內的訊息，促使用戶輸入 PIN 碼。
提交按鈕說明(Submit Button Description)	輸入顯示在提交 PIN 按鈕內的文字。
提交按鈕顏色(Submit Button Color)	自事先定義的顏色清單中選擇提交按鈕的顏色，或是選擇**客製化顏色(Customize Color)**並輸入 RGB 值。按下**預覽(Preview)**按鈕檢視選定的顏色。

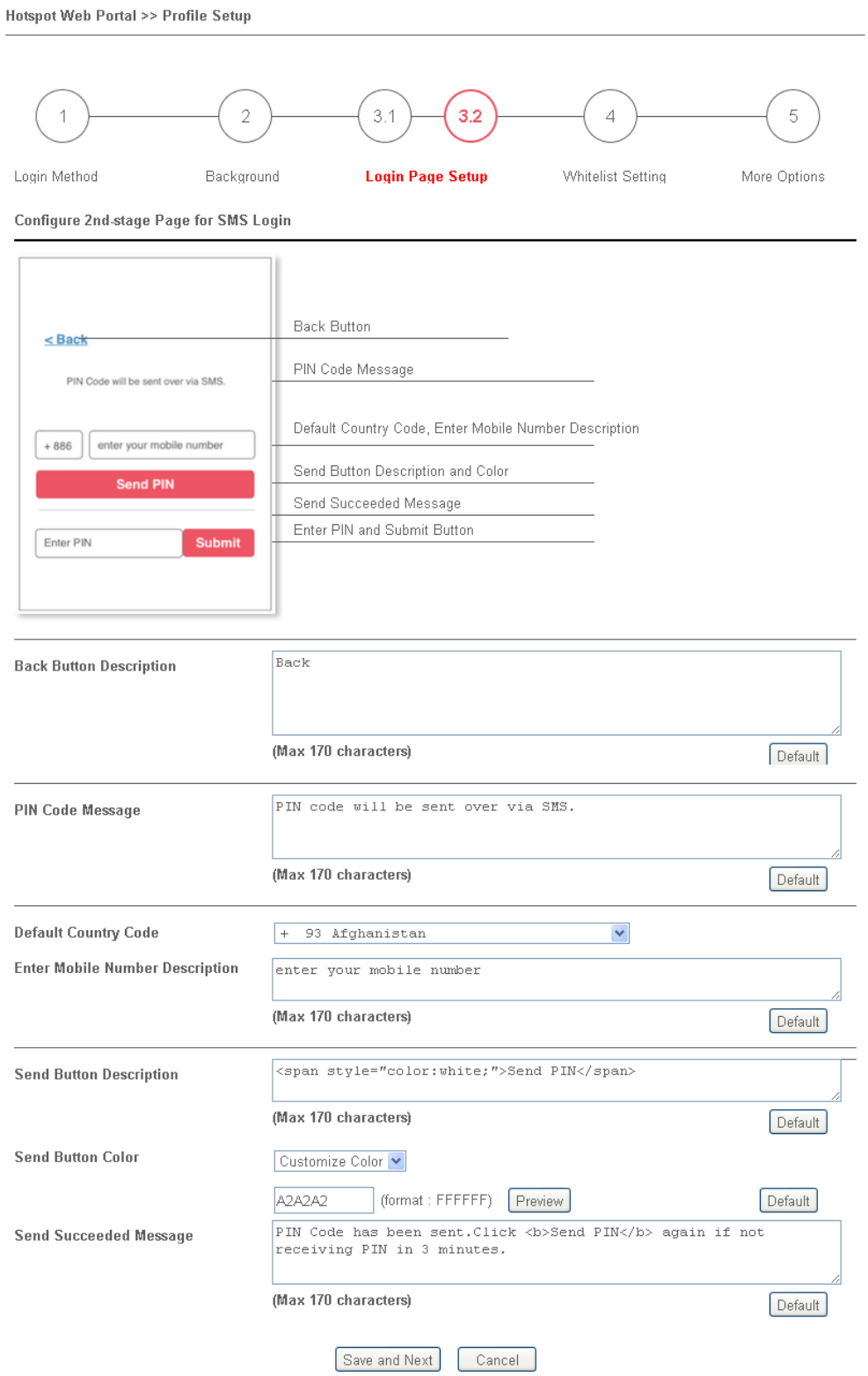
最後，儲存與取消按鈕即顯示如下：



項目	說明
儲存與下一頁(Save and Next)	按此儲存本頁的設定並進入下一頁。
取消(Cancel)	按此捨棄本頁設定並回到前一頁。

PIN 登入的第二階段設定頁面

如果您已選擇了 PIN 登入(PIN login)作爲登入模式，您還需要設定 PIN 碼相關的設定頁面。



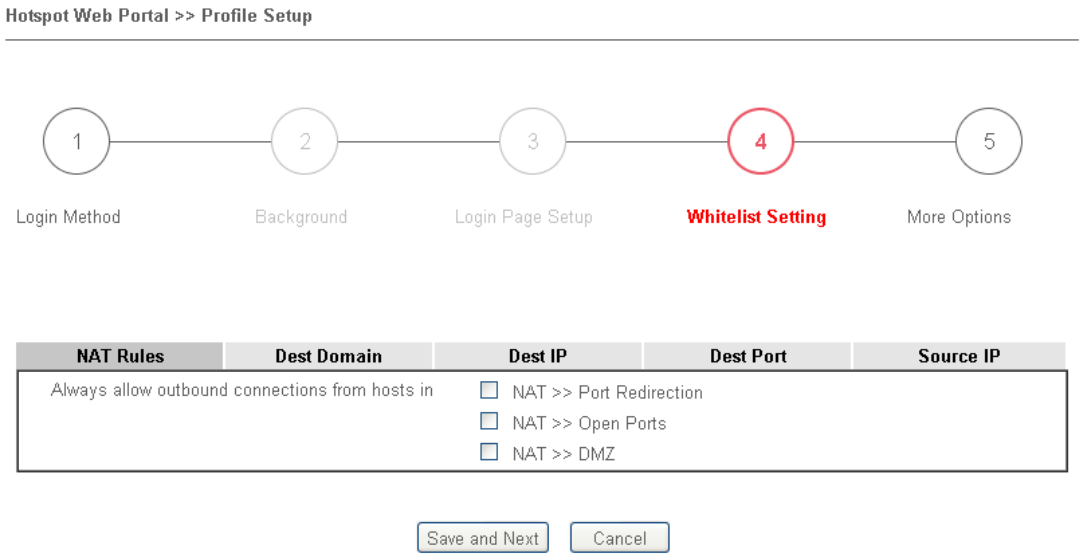
可用設定說明如下：

項目	說明
上一頁按鈕說明 (Back Button Description)	輸入回到前一個頁面的超連結標籤內文。
PIN 碼訊息(PIN Code Message)	輸入顯示在頁面主體內文的文字。

預設國碼(Default Country Code)	選擇顯示在下拉式選單中的預設國碼。
輸入行動電話號碼說明(Enter Mobile Number Description)	輸入於行動電話文字框中，提醒用戶輸入行動電話號碼的訊息。
傳送按鈕說明(Send Button Description)	輸入傳送按鈕的標籤內文。
傳送按鈕顏色(Send Button Color)	自事先定義的顏色清單中選擇傳送按鈕的顏色，或是選擇**客製化顏色(Customize Color)**並輸入 RGB 值。按下**預覽(Preview)**按鈕檢視選定的顏色。
傳送成功訊息(Send Succeeded Message)	輸入於 PIN 碼傳送成功之後，通知用戶成功的訊息。
儲存與下一頁(Save and Next)	按此儲存本頁的設定並進入下一頁。
取消(Cancel)	按此捨棄本頁設定並回到前一頁。

4.白名單設定

在此步驟中，您可以配置白名單設定，允許使用者傳送並接收滿足白名單設定的資料流量。



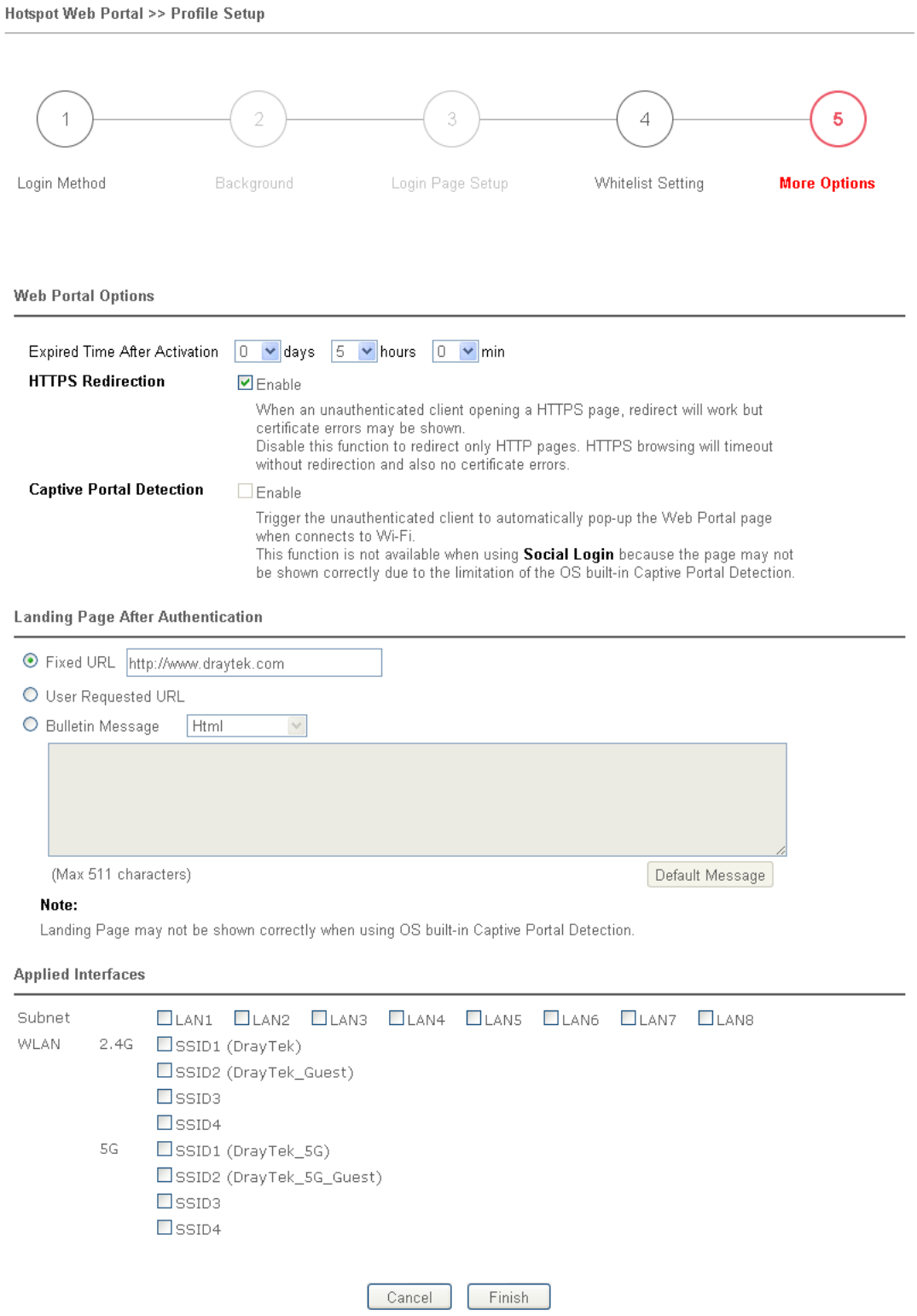
可用設定說明如下：

項目	說明
NAT 規則(NAT Rules)	避免入口網站設定與 NAT 規則產生衝突，導致不預期的錯誤，選擇允許繞過入口網站設定的 NAT 規則，選定 NAT 規則中條列的主機得以允許登入網際網路，不會被入口網站攔截。
目標網域(Dest Domain)	輸入允許通過路由器的目標網域，最多可以設定 30 個。
目標 IP(Dest IP)	輸入允許通過路由器的目標 IP 位址，最多可以設定 30 個。
目標埠號(Dest Port)	輸入允許通過路由器的目標通訊協定，最多可以設定 30 個。
來源 IP(Source IP)	輸入允許通過路由器的來源 IP 位址，最多可以設定 30 個。

儲存與下一頁(Save and Next)	按此儲存本頁的設定並進入下一頁。
取消(Cancel)	按此捨棄本頁設定並回到前一頁。

5. 更多選項

在此步驟中，您可以針對客製化入口網站設定進階選項。



可用設定說明如下：

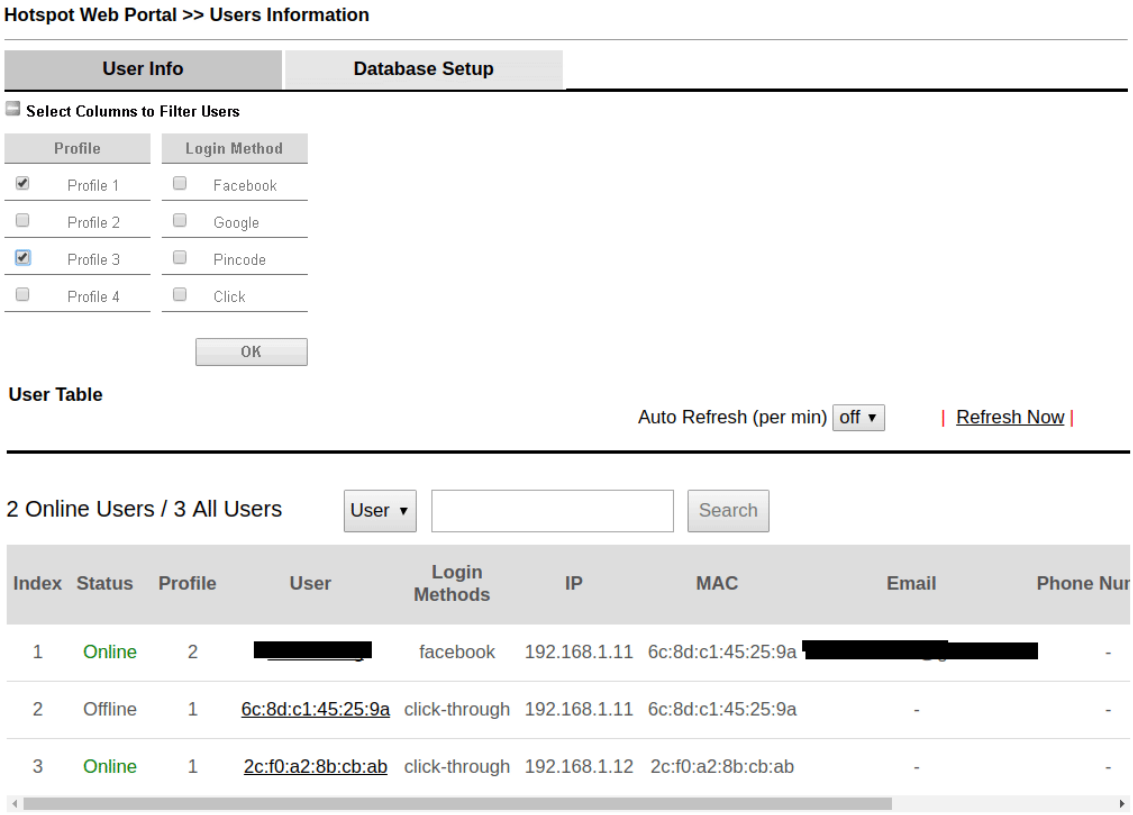
項目	說明
啓用後的到期時間 (Expired Time After Activation)	輸入允許使用者登入且上網的時間(期間)。
HTTPS 重新導向 (HTTPS Redirection)	若選定了此項，嘗試登入 HTTPS 網站未被驗證的使用者會被系統導引至登入頁面，瀏覽器則警告用戶憑證有誤。如果沒有勾選此項，任何 TTPS 網站登入嘗試都會逾時也無重新導向。
強制登錄驗證網頁偵測(Captive Portal Detection)	若選定了此項，當一個未驗證用戶嘗試登入網際網路時，系統會自動觸發入口網站頁面。當登入模式爲社群登入時，這個功能基本上是不可用的，因爲入口網站頁面會因操作系統內建的強制登錄驗證網頁針測之限制，無法正確顯示頁面。
驗證後進入指定首頁 (Landing Page After Authentication)	指定使用者成功驗證之後系統顯示的網頁。 **固定 URL(Fixed URL)** – 使用者將被重新導引至指定的 URL 頁面。這個部份可用於顯示廣告讓用戶參考，例如飯店客人想要使用無線網際網路時先看廣告。 **使用者需求 URL(User Requested URL) –** 使用者將被重新導引至其原本想要登入的 URL。 **佈告欄訊息(Bulletin Message)** – 此處設定的訊息會顯示給用戶檢視數秒。 **預設訊息(Default Message) –** 當選定了佈告欄訊息之後，此按鈕即可啓用，點選此鈕載入預設文字做爲佈告欄顯示的訊息。
套用介面(Applied Interfaces)	**子網(Subnet)** – 目前的客製化入口網站設定檔可對選定子網生效。 **WLAN** – 目前的客製化入口網站設定檔可對選定的 WLAN SSID 生效。
儲存與下一頁(Save and Next)	按此儲存本頁的設定並進入下一頁。
取消(Cancel)	按此捨棄本頁設定並回到前一頁。

VII-4-2 使用者資訊(User Information)

使用者透過入口網站存取網際網路的日誌資訊可以顯示在本頁，按下使用者連結可以開啓另一個網頁，顯示更多的資訊。

VII-4-2-1 使用者資訊(User Info)

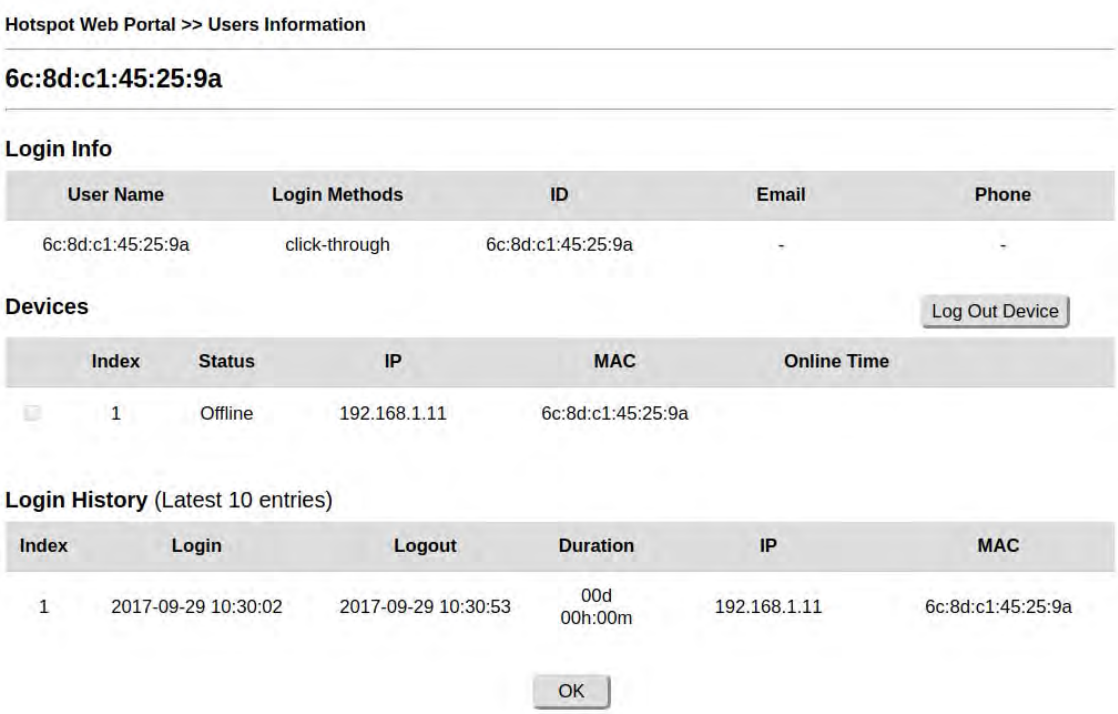
基於使用的過濾條件(設定檔或是登入模式)，本頁可以顯示不同的使用者資訊。



可用設定說明如下：

項目	說明
選擇欄位以過濾使用者(Select Columns to Filter Users)	指定設定檔以及登入方式以便過濾想要透過登入方式存取網際網路的使用者，對系統管理者來說，當有很多的用戶需要登入網際網路時，可以使用此方法並依照不同條件管理使用者登入。
使用者表格(User Table)	本區顯示並紀錄使用者透過入口網站存取網際網路的相關資訊。

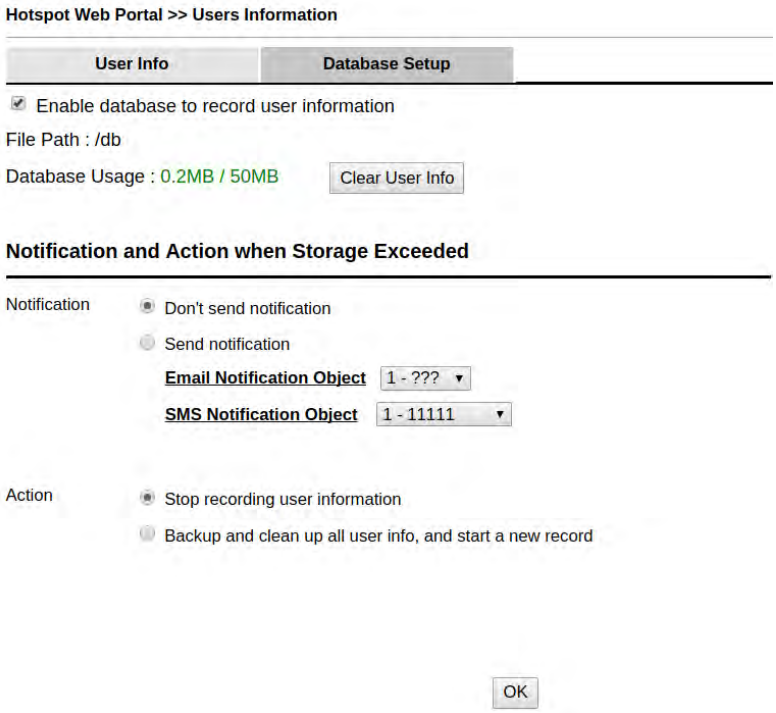
按下特定使用者的 MAC 位址連結，與此裝置有關的資訊頁面將會顯示如下：



裝置的基本資訊顯示在登入資訊欄位；裝置(Devices)區顯示該裝置的線上/斷線狀態；登入歷程(Login History)顯示該裝置的存取時間；此外，爲了強迫登出某裝置，只要選擇該裝置並按下登出裝置(Log Out Device)按鈕。

VII-4-2-2 資料庫設定(Database Setup)

本頁允許使用者進行 USB 磁碟上的資料庫設定。



可用設定說明如下：

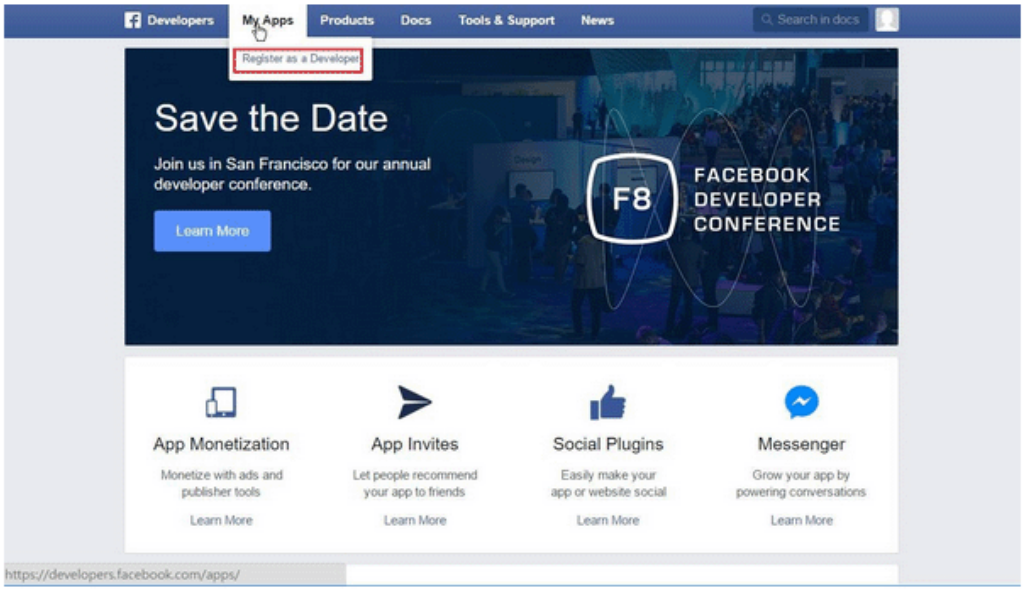
項目	說明
啓用資料庫記錄使用者資(Enable database to record user information)	勾選此框以記錄於路由器資料庫中的使用者資訊。 在勾選之前，請先插入具備足夠空間的 USB 磁碟。
檔案路徑(File Path)	若 USB 磁碟已經插入路由器的 USB 埠口，本區將會顯示檔案路徑。
資料庫用量(Database Usage)	顯示資料庫用量與剩餘空間。 **清除使用者資訊(Clear User Info)**- 使用者資訊將會顯示在使用者資訊(User Info)區中，您可以按此鈕刪除相關資訊。
當儲存量超過如下額度時採取通知以及行動(Notification and Action when Storage Exceeded)	
通知(Notification)	**不傳送通知(Don't send notification) -** Vigor 路由器系統不會傳送任何通知訊息給予收信人。 **傳送通知(Send notification)** - Vigor 路由器系統會傳送通知電郵給指定的收信人(於電子郵件通知物件與簡訊通之物件中所訂定的收件人)。
動作(Action)	**停止紀錄使用者資訊(Stop recording user information) -** Vigor 路由器系統將停止紀錄使用者資訊至 USB 磁碟中。 **備份與清除所有的使用者資訊，開始新的紀錄(Backup and clean up all user info, and start a new record) -** Vigor 路由器系統將備份所有於 USB 磁碟的資訊至主機上，然後清除 USB 磁碟內的資訊，稍後，就可以開始新的紀錄。

應用說明

A-1 如何建立臉書 APP ID 以利網頁入口驗證？

入口網站的新功能支援社群登入作爲驗證的方式，並允許網路管理者透過 Google 或臉書帳號來驗證 LAN 端用戶，本文將告訴您如何在入口網站設定頁面中建立臉書 APP 並產生 APP ID 以及 APP 密鑰。

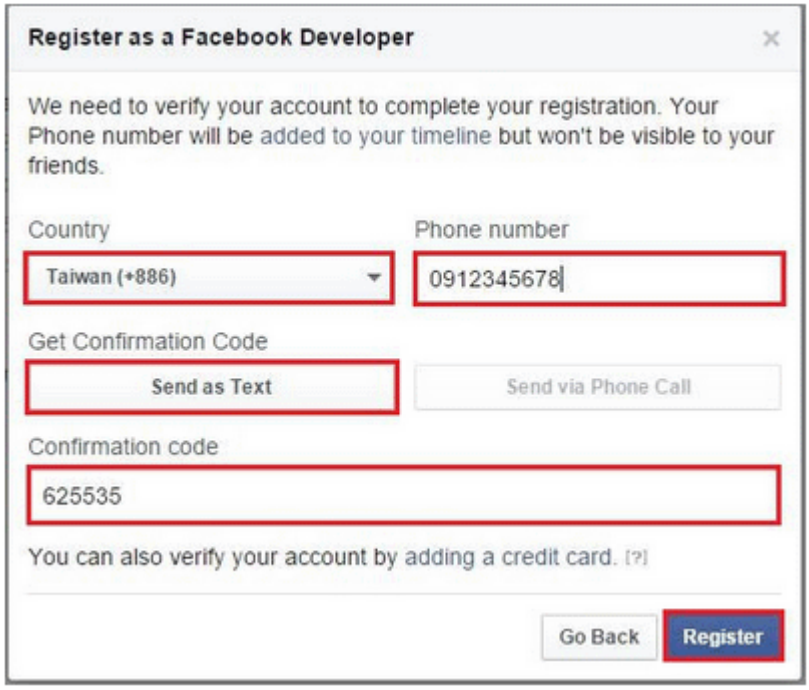
1. 請註冊爲 FB 開發人員，請前往 https://developers.facebook.com/並登入臉書帳號。
2. 以臉書帳號註冊爲開發人員(若帳號先前已經查證過，本步驟可以省略)。
3. 按下 **My Apps** 接著選擇 **Register as Developer**。



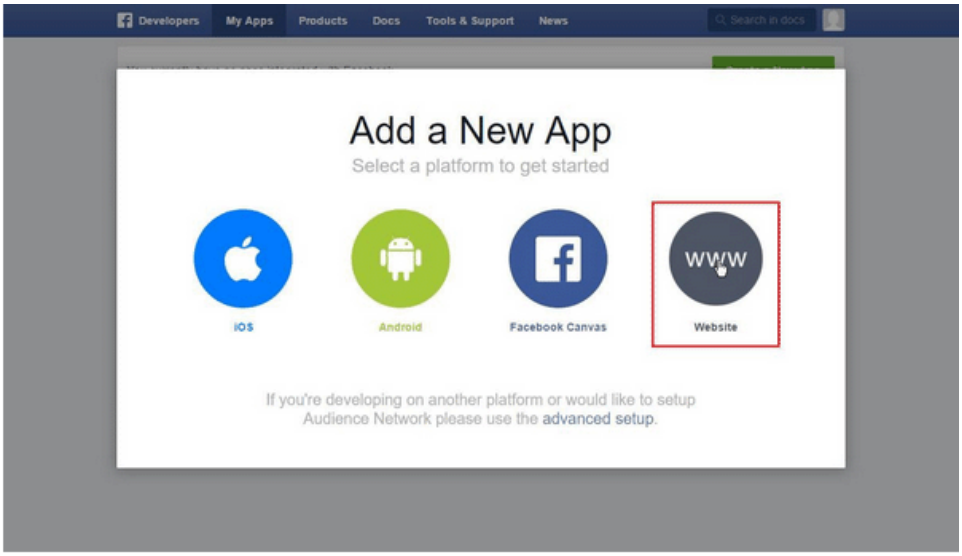
4. 切換到 **YES** 然後於跳出視窗上點選下一頁 **Next**。



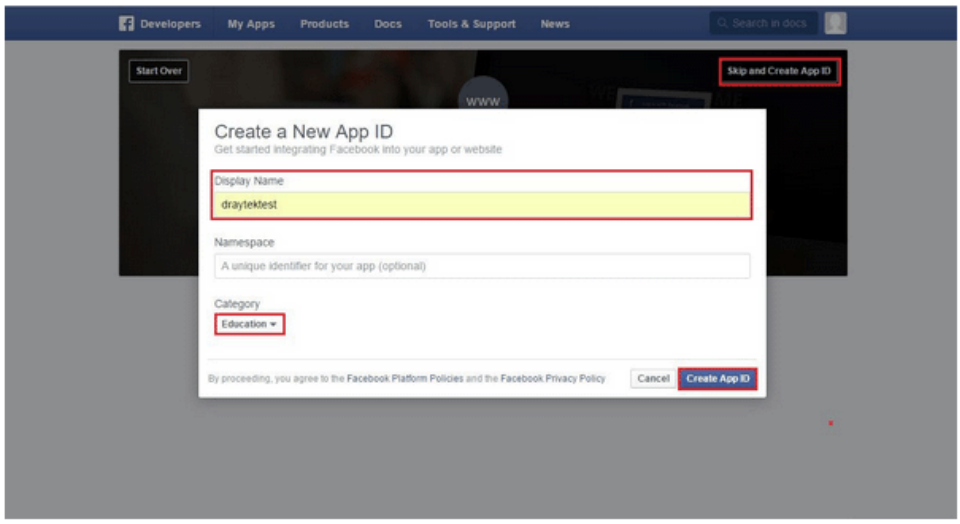
5. 選擇國別 **country** 再輸入電話號碼 **Phone number**，於取得確認碼欄位中按 **Send as Text**，等收到確認碼訊息後，輸入該確認碼。按下 **Register** 已完成註冊過程。



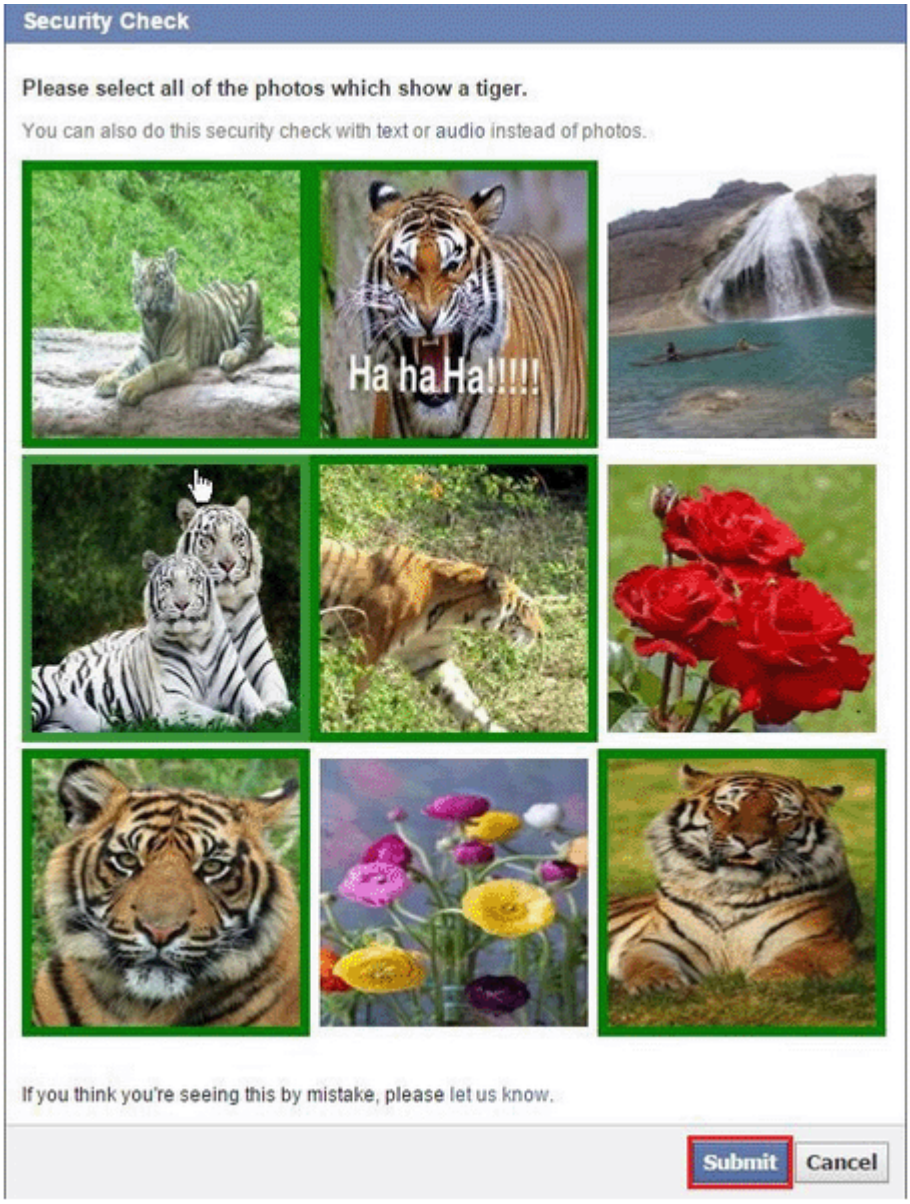
6. 新增一個 App，點選 **My Apps > Add a New App**，選擇 **Website** 平台。



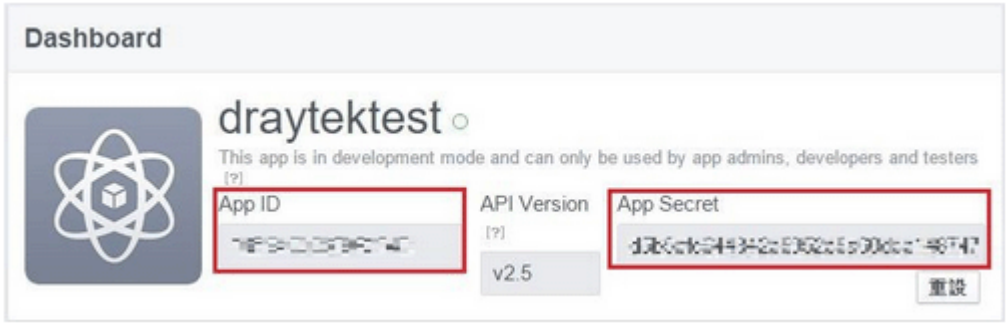
7. 若是第一次使用，請點選 **Skip and Create App ID**，輸入 **Display Name** 再選擇 **Category**。點選 **Create App ID**。



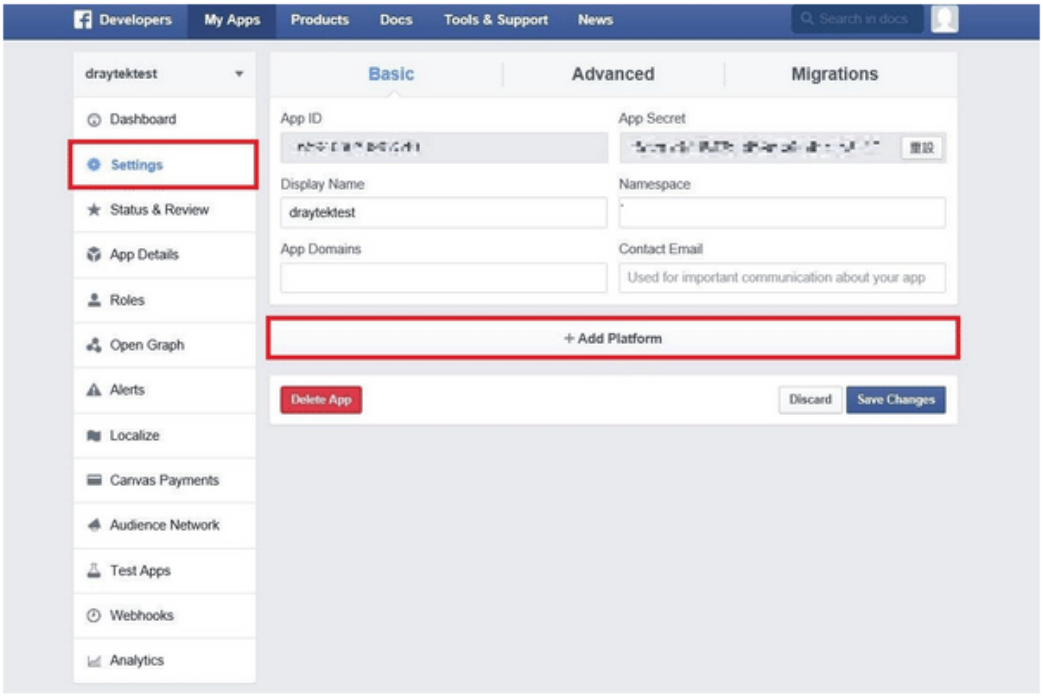
8. 安全性檢查視窗接著跳出，請依文意選擇，然後按 **Submit** 按鈕完成整個過程。



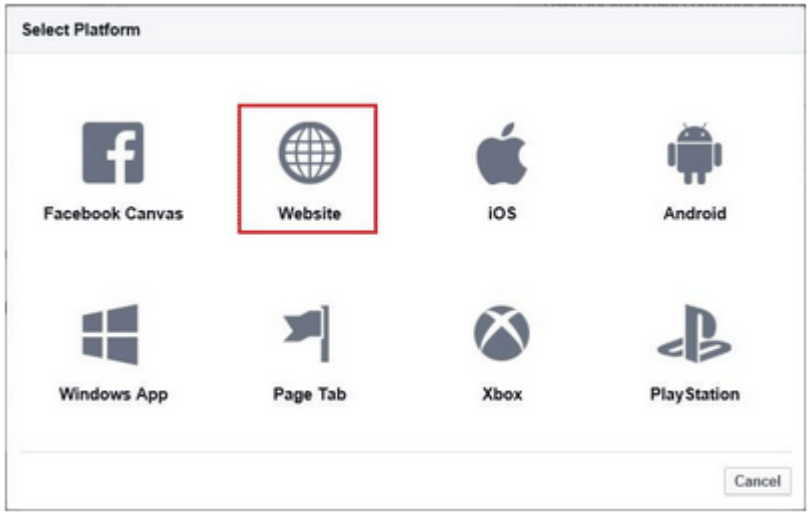
9. 在儀表板上，使用者可以取得 **App ID** 與 **App Secret**，這些資訊將被運用在路由器的入口網站設定上。



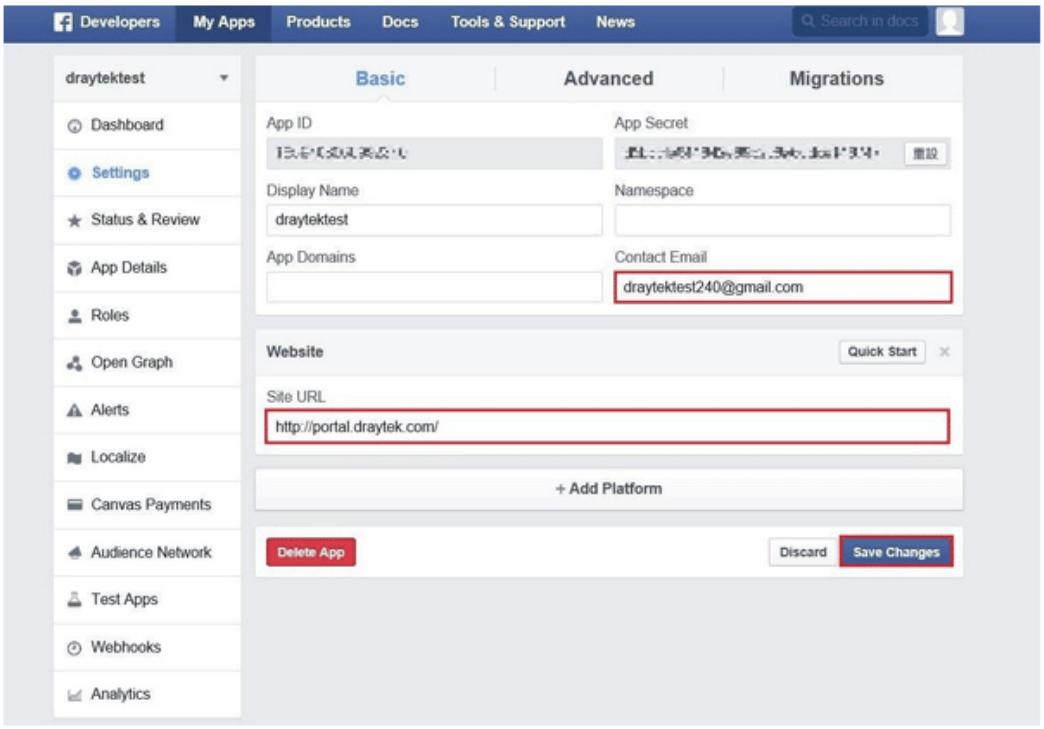
10. 在 My Apps 上新增平台，前往 **Settings** 並選擇 **Add Platform**。



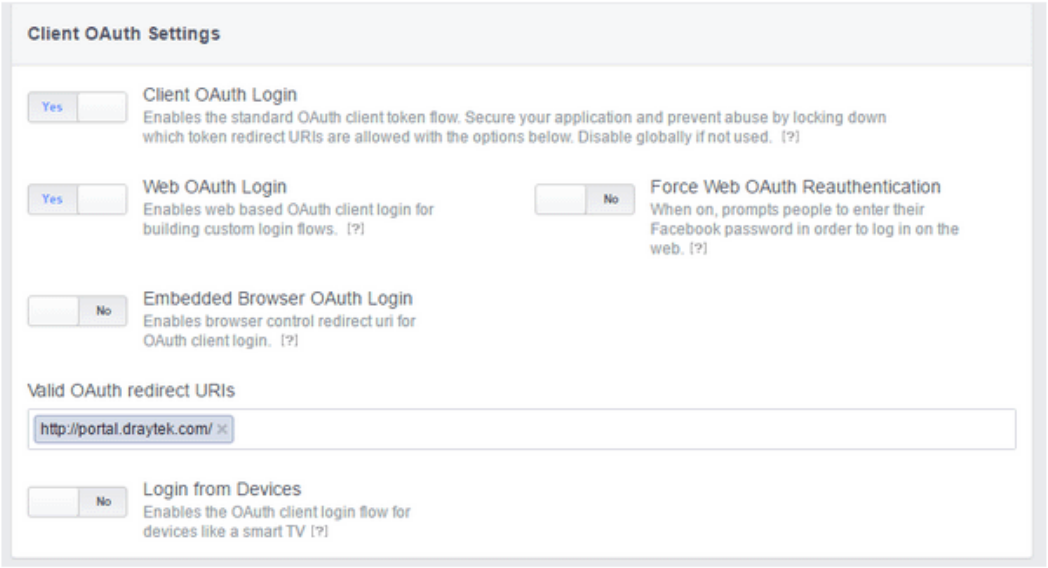
11. 選擇 **Website**。



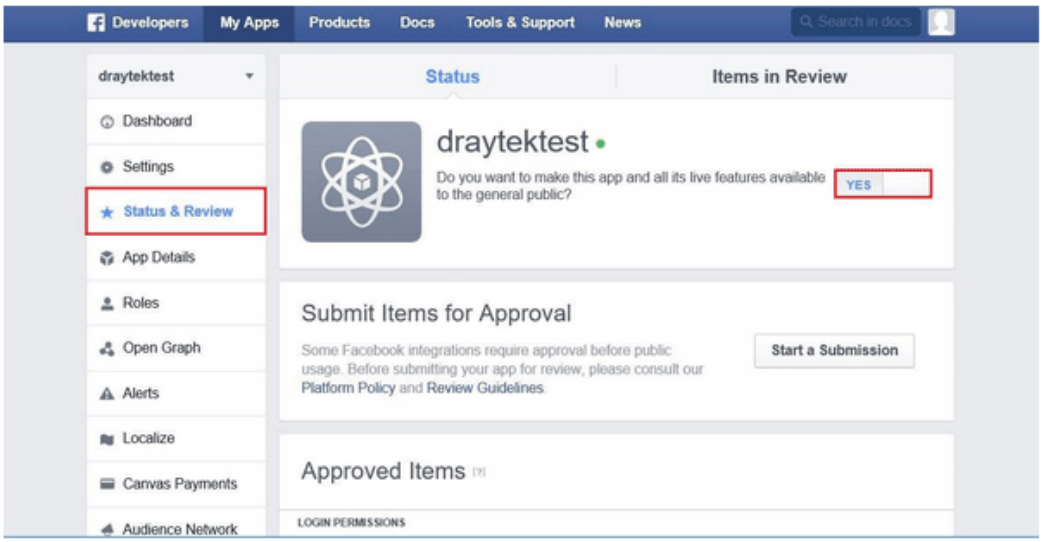
12. 輸入網站 **Site URL:** http://portal.draytek.com. (附註: 如果您改變了 http 埠號，請在 URL 中新增 http 埠號。例如我們使用 8080 做爲 http 埠號，URL 連結爲 http://portal.draytek.com:8080)，輸入連絡電子郵件 **Contact Email**，然後點選儲存變更 **Save Change**。



13. 設定用戶的 Client OAuth，請前往 **Settings** >> **Advanced** >>**Client OAuth Settings**，並在。**Valid OAuth redirect URI** 中輸入 "http://portal.draytek.com"。



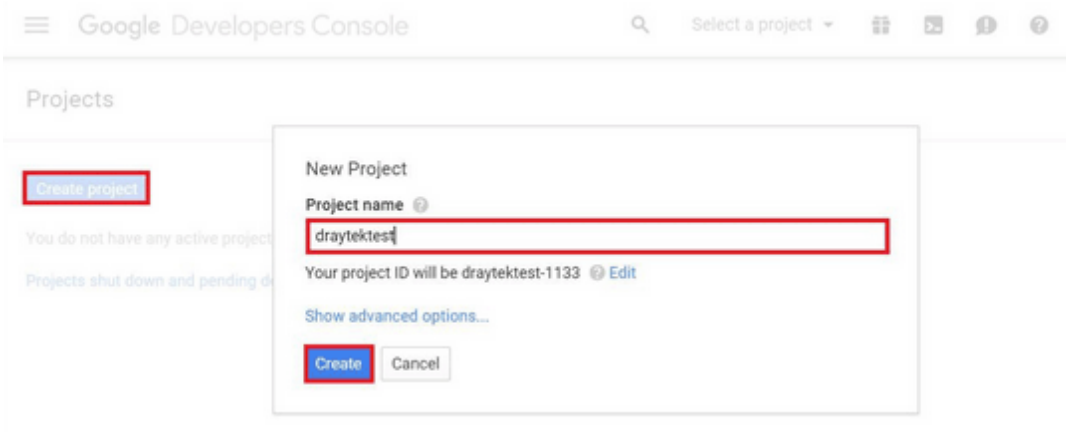
14. 前往 **My Apps>>Status & Review**，切換可用狀態爲 **YES** 以便啓動 APP。


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

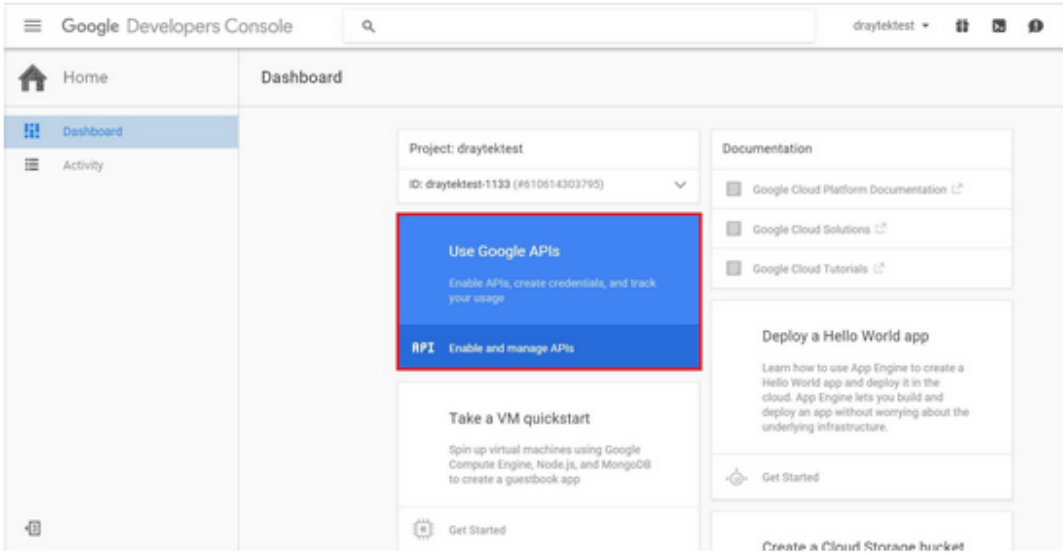
A-2 如何建立 Google APP ID 以利網頁入口驗證

入口網站的新功能支援社群登入作爲驗證的方式，並允許網路管理者透過 Google 或臉書帳號來驗證 LAN 端用戶，本文將告訴您如何在入口網站設定頁面中建立臉書 APP 並產生 APP ID 以及 APP 密鑰。

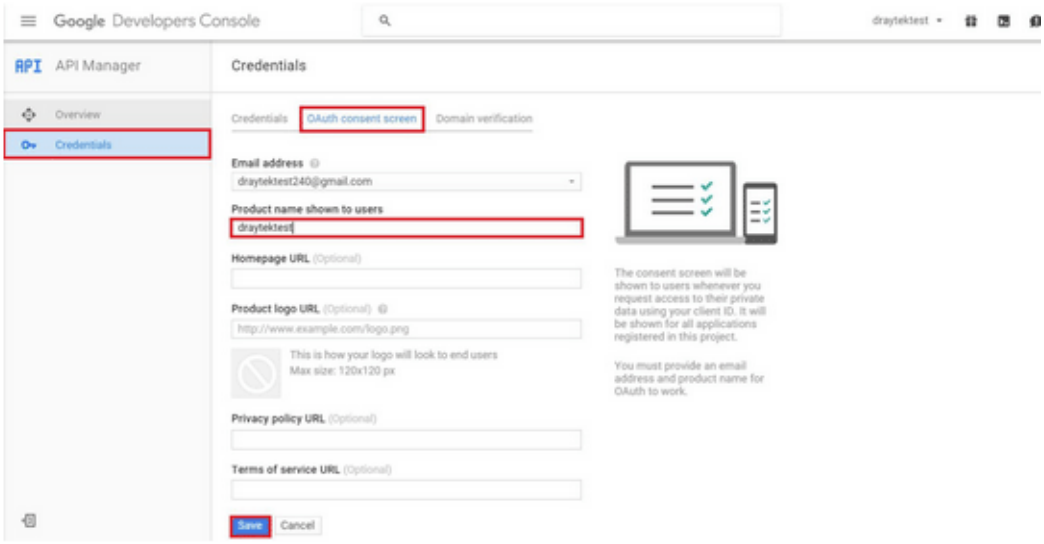
1. 建立開發商項目，前往 https://code.google.com/apis/console，以 Google 帳號登入然後按下建立項目 **Create project**，輸入項目名稱 **project name** 然後按建立 **Create**。



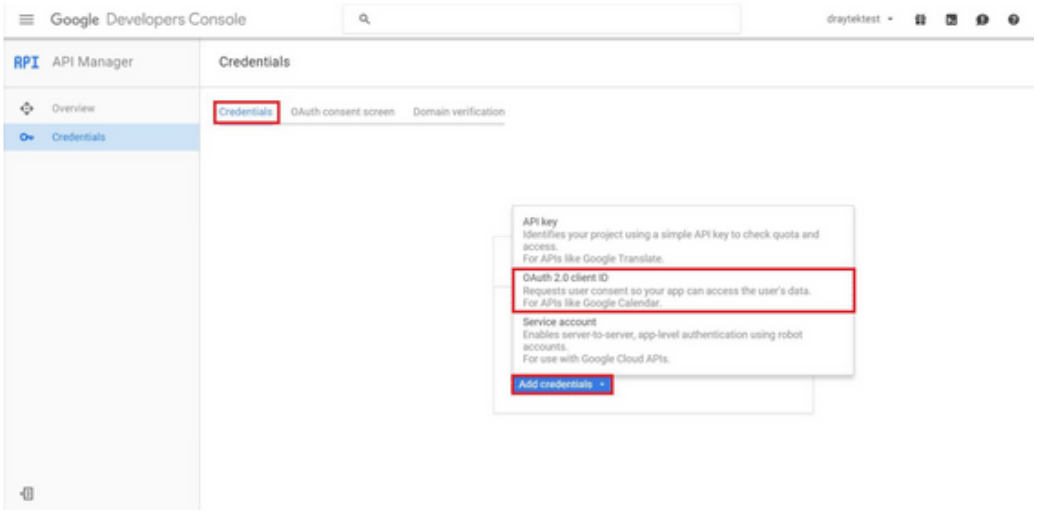
2. 在儀表板 Dashboard 上，選擇 **Use Google APIs**。



3. 編輯驗證同意頁面，前往 **Credentials > Auth consent screen**，輸入電郵 **email**、**產品名稱 product name** 和其他選擇項目，然後按 **Save**。



4. 建立用戶端 Client ID，按 **Credentials** 並選擇 **Add credentials > OAuth2.0 client ID**。



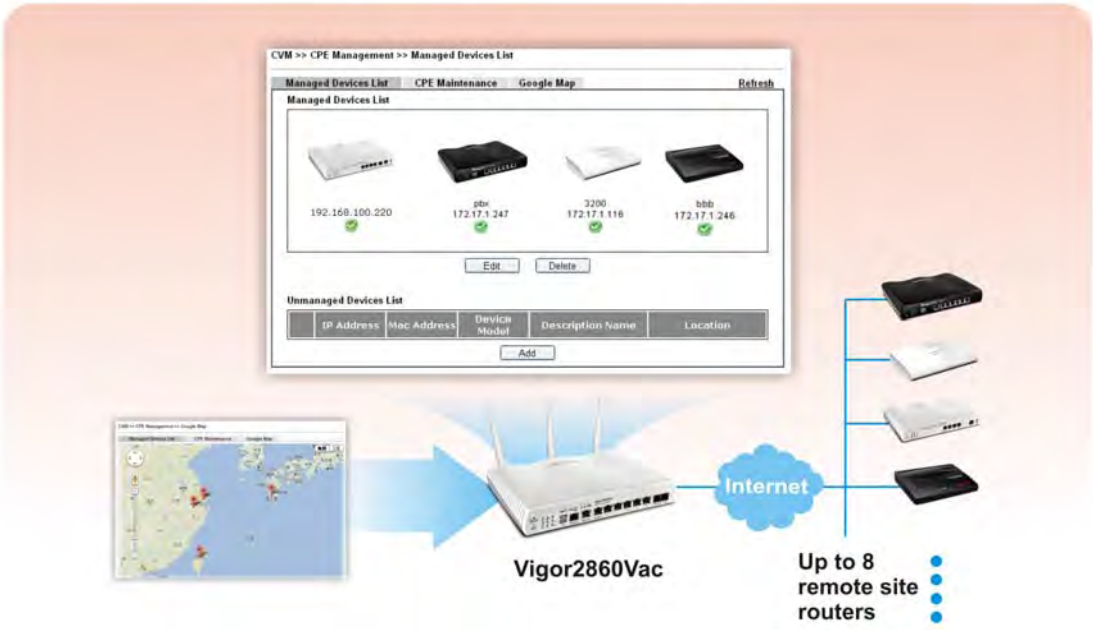
5. 選擇 **Web application** 做爲驗證類型，然後輸入名稱 **name**，設定 **Authorized JavaScript origins** 以及設定 **Authorized redirect URLs** 爲 http://portal.draytek.com 並按 **Create**。(附註: 如果您變更路由器的 http 埠號，請在 URL 中加入 http 埠號，例如我們使用 8080 做爲 http 埠號，如 http://portal.draytek.com:8080)。

6. 取得用戶端 **client ID** 與用戶密碼 **client secret**，相關資訊之後可用於路由器的入口網站設定中。



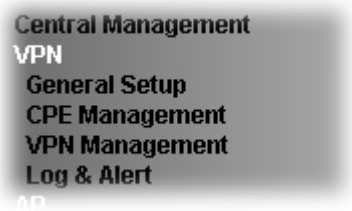
VII-5 中央管理(VPN)

Vigor2926 能夠在自身與其他遵循 TR-069 標準的 CPE 之間，透過中央 VPN 連線管理功能建立虛擬私人網路(VPN)。此外，Vigor2926 還可以被視爲伺服器(稱爲 CVM 伺服器)，管理多重 TR-069 CPE 並定期執行韌體更新、設定備存與設定還原等作業。



網頁使用者介面

VPN 中央管理功能僅能管理透過 WAN 端連接的 CPE。.

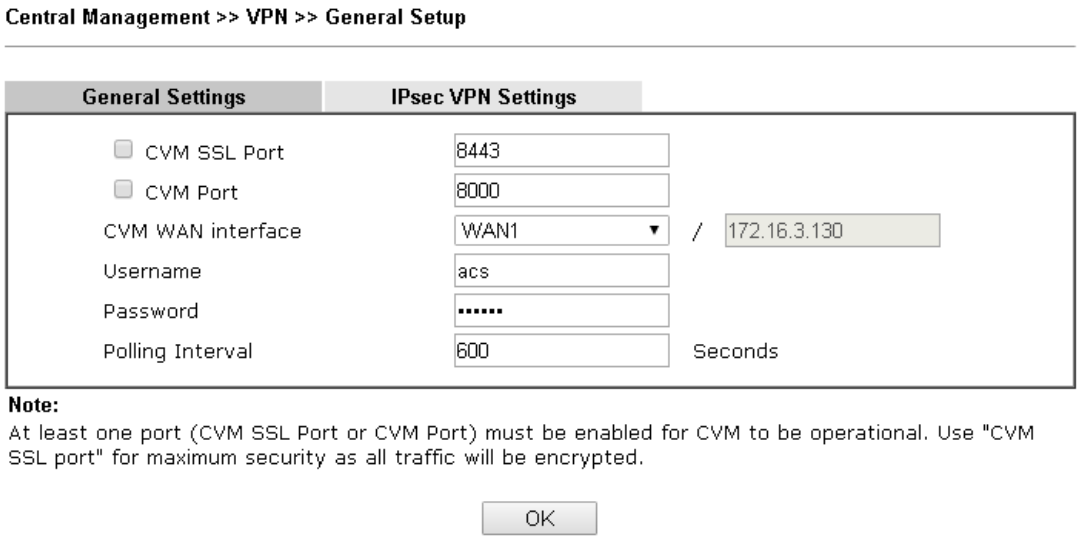


VII-5-1 基本設定(General Setup)

本頁用來設定用戶向 Vigor 路由器登錄註冊所需的相關內容。按下**基本設定(General Settings)**標籤與 **IPsec VPN 設定(IPsec VPN Settings)**標籤設定此機制的基本功能。

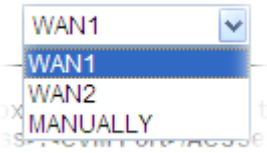
VII-5-1-1 基本設定(General Setup)

欲啓用 CVM 功能，第一步要做的就是啓用 CVM 埠號與 CVM SSL 埠號設定。



可用設定說明如下：

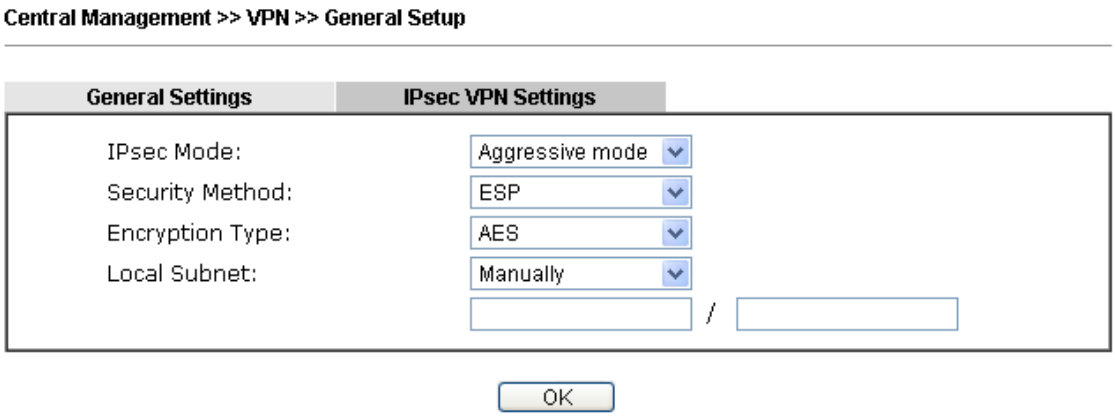
項目	說明
CVM SSL 埠號 (CVM SSL Port)	勾選此框啓用埠號設定。 於方框內輸入埠號值。
CVM 埠號(CVM Port)	勾選此框啓用埠號設定。 於方框內輸入埠號值
遠端連線需求之 WAN IP (WAN IP for Remote Connection)	Vigor 路由器僅能管理來自 WAN 端的用戶，因此您必須指定準備使用的 WAN 介面，如果您選擇**手動(MANUALLY)**，您必須指定 WAN IP 位址。

	
使用者名稱(Username)	輸入任何一台 CPE 嘗試連接至 Vigor 路由器時需要鍵入的使用者名稱。
密碼(Password)	輸入任何一台 CPE 嘗試連接至 Vigor 路由器時需要鍵入的密碼。
Polling 間隔(Polling Interval)	輸入時間值(單位爲秒)，可調範圍在 60 ~ 86400 之間。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

VII-5-1-2 IPsec VPN 設定(IPsec VPN Settings)

VPN 中央管理乃透過 IPsec VPN 連線來操作。



可用設定說明如下：

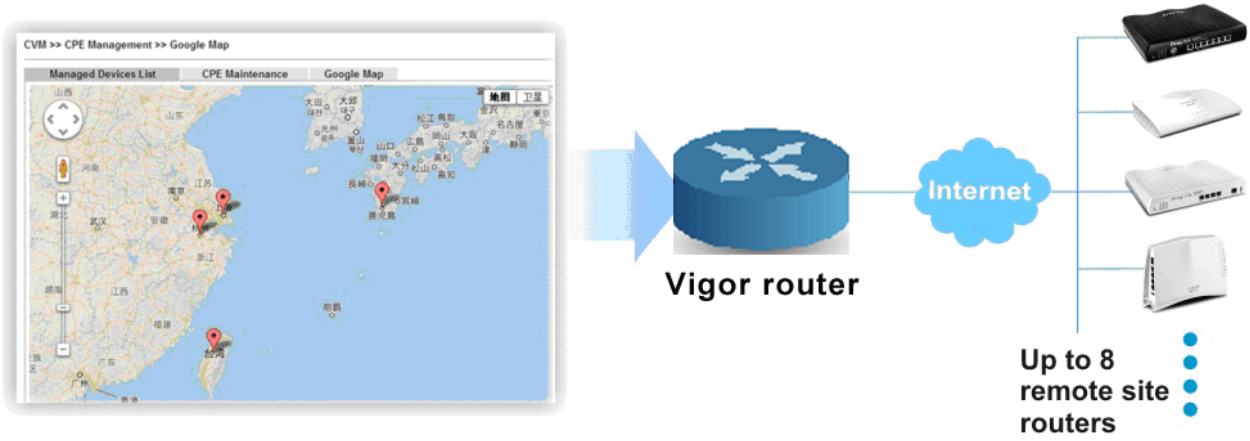
項目	說明
IPsec 模式(IPsec Mode)	選擇 **Aggressive 模式**或是 **Main 模式**。
安全性模式(Security Method)	選擇一種方式來維護資料傳送的安全性(AH 或是 ESP)，例如您選擇 AH 即可指定 IPsec 協定，資料將受到驗證但並未加密。
加密類型(Encryption Type)	自下拉式清單中選擇您需要的加密類型。
本機子網(Local Subnet)	輸入本機的 IP 位址與子網遮罩。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

VII-5-2 CPE 管理(CPE Management)

所有 Vigor2926 管理下的 CPE 都會在本頁中以小圖示的方式呈現出來。

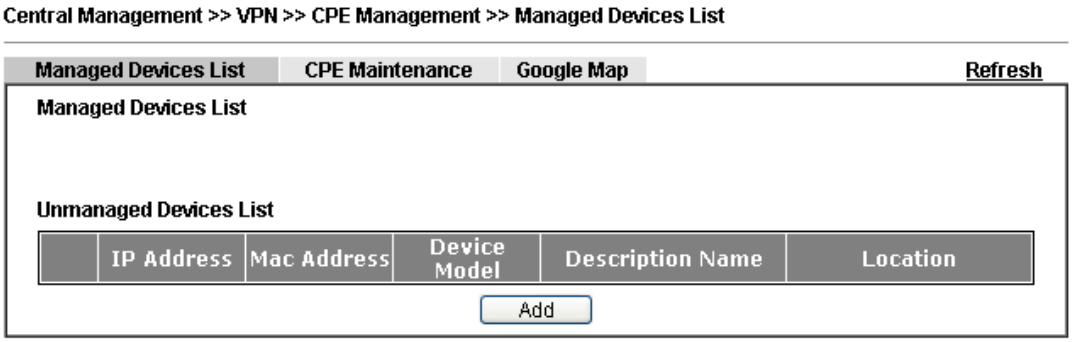
使用此功能之前，請先確認 CVM 埠號設定已經啓用且已設定妥當。



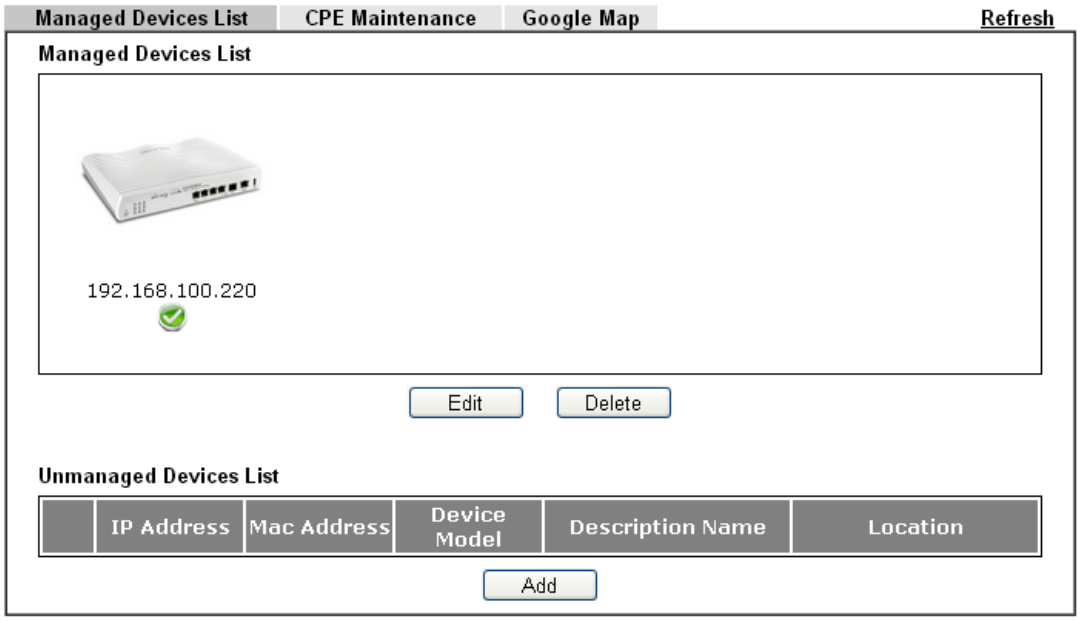
VII-5-2-1 受管理的裝置清單(Managed Device List)

本頁讓您管理連接至 Vigor2926 系列的 CPE 裝置。

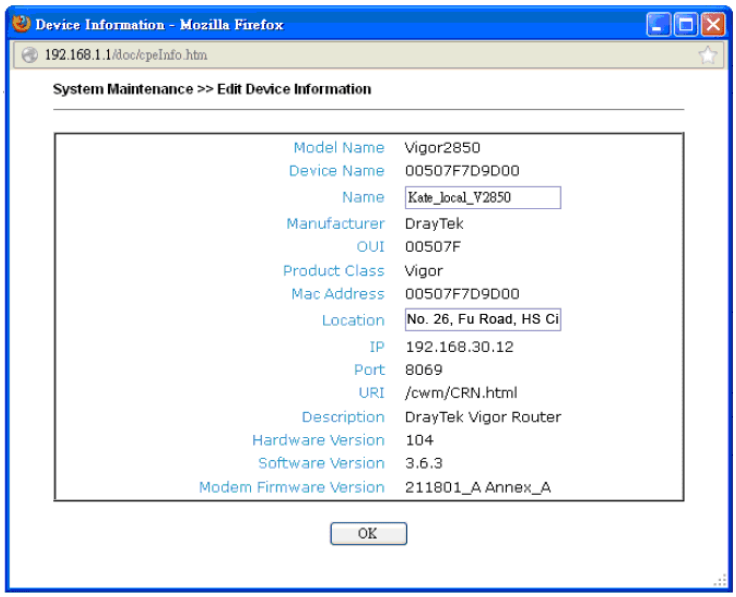
無 CPE 連接的頁面

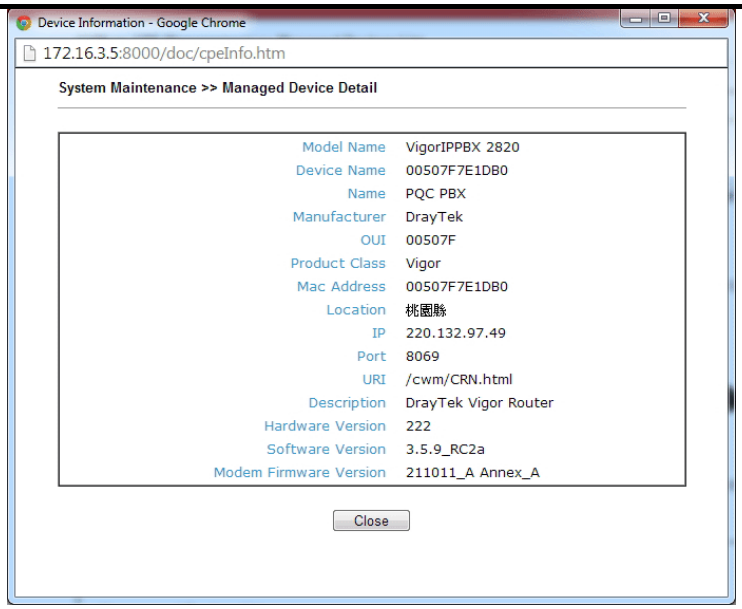


已有 CPE 連接的頁面



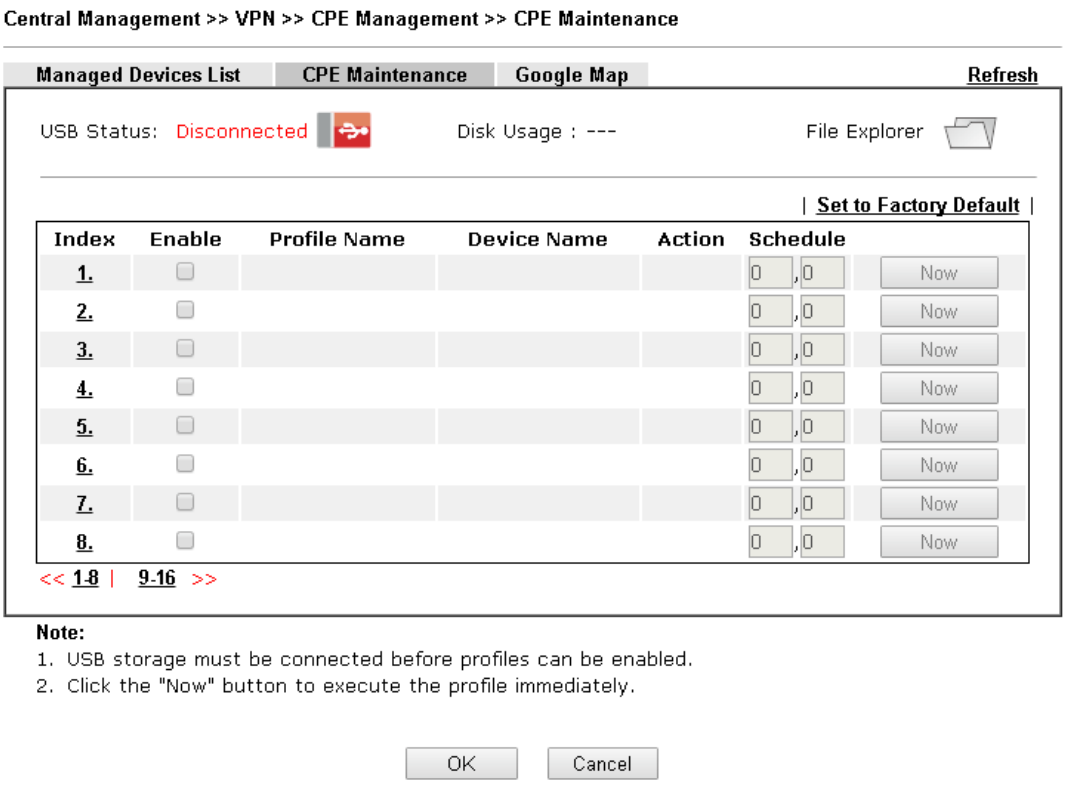
可用設定說明如下：

項目	說明
受管理的裝置清單 (Managed Devices List)	本區顯示已在 Vigor2926 管理下的 CPE 裝置圖示(最多可以有 8 個)。 **編輯(Edit)** – 如果要修改 CPE 裝置的名稱或是位置，請選定該圖示然後按下**編輯(Edit)**按鈕，螢幕將出現跳出的視窗，即可在此視窗內修改名稱與/或位置。  **刪除(Delete)** – 如果要中斷受管理的 CPE 與 Vigor2926 之間的聯繫，選擇該 CPE 之後，按下**刪除(Delete)**按鈕即可。 快速按二下 CPE 圖示也可以跳出受管理的 CPE 細節內容，只不過您無法進行任何名稱或位置修改等事宜。.

	
未受管理的裝置清單 (Unmanaged Devices List)	任何依循 TR-069 標準的 CPE 裝置都可以在此設定並可由 Vigor2926 系列路由器自動偵測出來。 Vigor2926 一次只會管理最多 8 台遠端裝置，因此其他遠端的裝置如果也被偵測出來，便不會顯示在本區。 **新增(Add)** – 將選定的裝置自未受管理的裝置清單區移往受管理的裝置清單區中。 **IP 位址(IP Address)** – 顯示遠端裝置的 IP 位址。 **Mac 位址(Mac Address)** – 顯示遠端裝置的 MAC 位址。 **裝置機型(Device Model)** – 顯示遠端裝置的型號資料。 **說明名稱(Description Name)** – 定義 CPE 附加說明的內容以方便辨識。 **位置(Location)** – 輸入該 CPE 裝置於 Google Map 顯現出來的位置(位址)。
更新頁面(Refresh)	按此連結更新目前頁面。

VII-5-2-2 CPE 維護(CPE Maintenance)

本區顯示所有套用至受管理裝置之設定檔，本頁可幫助管理者進行維護作業，像是韌體更新、設定備份、設定還原等等。



可用設定說明如下：

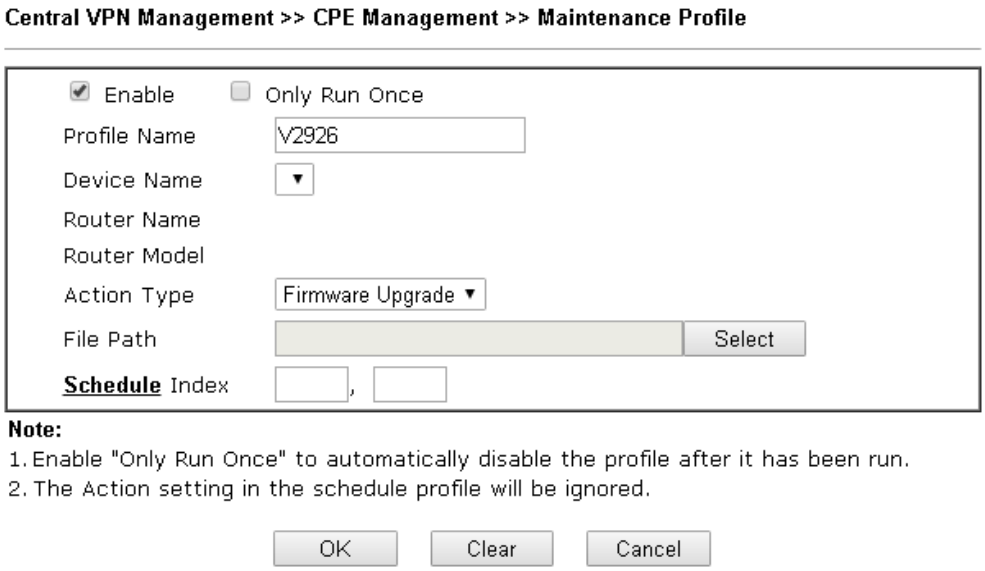
項目	說明
更新頁面(Refresh)	按此更新目前頁面。
USB Disk	USB Disk： - 此即表示 USB 磁碟已經連接上 Vigor2926。 USB Disk： - 此即表示 USB 磁碟並未連接上 Vigor2926。
Disk Usage	Disk Usage：1084MB / 2009MB - 當 USB 磁碟連接至 Vigor2926 時，磁碟的使用狀況與磁碟的容量都會顯示在螢幕上。 磁碟使用狀況：USB 儲存中斷 - 當無任何 USB 磁碟連上 Vigor2926 時，畫面上將出現 USB 磁碟中斷的訊息。
	按此圖示可見 USB 磁碟內容。
回復出廠預設值(Set to Factory Default)	按此清除所有頁面上呈現的資料。
索引編號(Index)	顯示您可以編輯的設定檔之編號連結。
設定檔名稱(Profile Name)	顯示維護設定檔的名稱。

裝置名稱(Device Name)	顯示維護設定檔準備套用的裝置名稱(已接受 Vigor2926 管理者)。
動作(Action)	顯示該 CPE 準備進行的動作爲何。
排程(Schedule)	顯示此設定檔套用的時間排程爲何。
現在(Now)	針對選定的 CPE 須執行的動作將會立刻進行。

如何新增維護設定檔

請按如下的步驟建立新的設定檔。

1. 按下任一個索引編號連結，例如#1。
2. 系統將出現如下頁面。



資訊

當還原某設定至 CPE 時，請務必確認選擇的設定檔早先是從該 CPE 備份下來，因爲若將其他機種備份的檔案還原至此 CPE 裝置，將會造成嚴重的後果(像是不同的 CPE 有不同的 ISP 使用者名稱/密碼等等，且還原錯誤的檔案也會造成無法連線登入網際網路)。

可用設定說明如下：

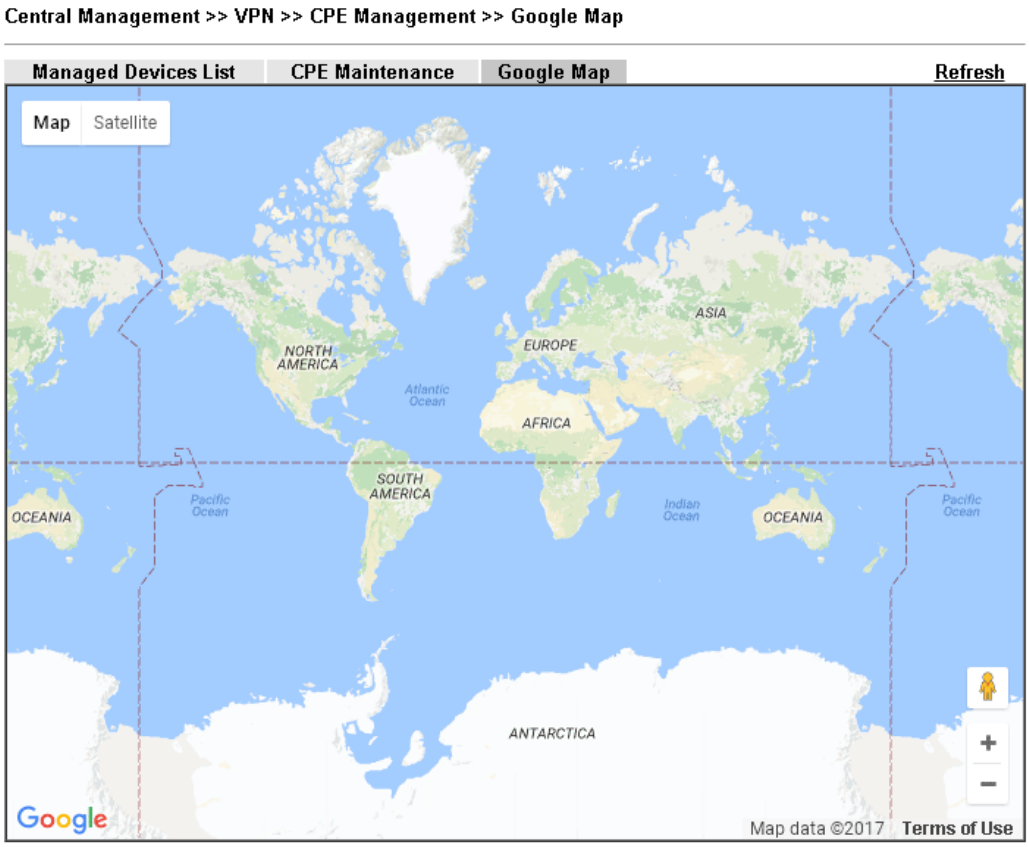
項目	說明
設定檔名稱(Profile Name)	輸入維護設定檔的名稱。
啓用(Enable)	勾選此框啓用此設定檔。
僅運作一次(Only Run Once)	勾選此框讓設定檔僅運用一次。
裝置名稱(Device Name)	下拉式清單將會顯示 Vigor2926 偵測到的 CPE 裝置，可從中選取一台裝置來套用此設定檔。
路由器名稱/型號 (Router Name / Router Model)	顯示路由器的名稱與型號。
Action Type	有數種類型可供選擇：

	● **設定備份(Config Backup)** – 表示此設定檔將用於備份選定的 CPE 裝置的設定。 ● **設定還原(Config Restore)** – 表示此設定檔將用於還原選定的 CPE 裝置的設定。 ● **韌體更新(Firmware Upgrade)** – 此設定檔將用於韌體更新。
檔案/路徑(File/Path)	按**選擇(Select)**尋找您想要儲存、還原或是更新 CPE 裝置的檔案。
索引編號排程(Index in Schedule)	路由器依照此處設定的排程計畫執行上述指定的動作。 請在此指定一至二個排程設定檔(以排成索引編號表示)。

3. 輸入所有的設定之後按下**確定(OK)**。
4. 新的設定檔建立完成。

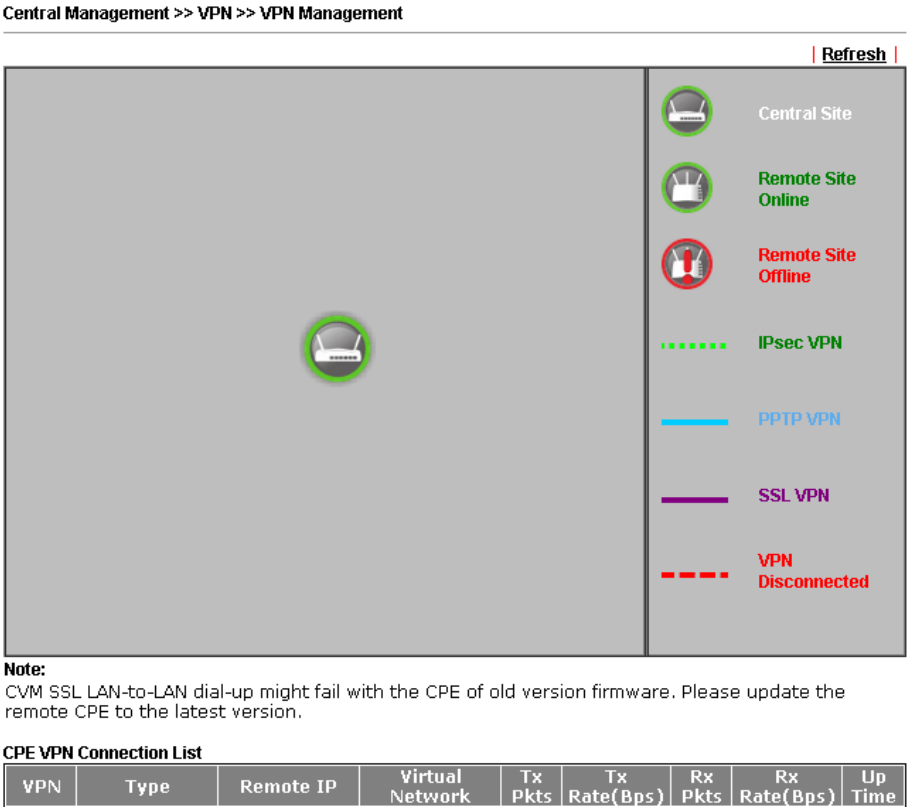
VII-5-2-3 Google 地圖(Google Map)

如果需要顯示管理下的 CPE 位置鳥瞰圖，請開啓 **VPN 中央管理>>CPE 管理(entral VPN Management>>CPE Management)**並按下 **Google 地圖(Google Map)**標籤。



VII-5-3 VPN 管理(VPN Management)

此功能提供一個簡單又快速的方法來設定 VPN 通道以便在 Vigor2926 系列與其它 Vigor 路由器(被視爲 CPE 裝置，VPN 用戶端)之間自動建立 VPN 連線。



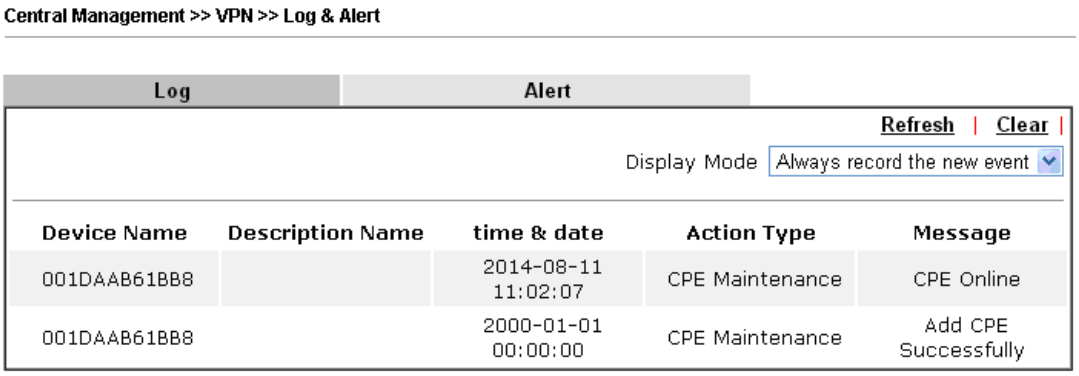
可用設定說明如下：

項目	說明
CPE VPN 連線清單	
VPN	顯示 LAN-to-LAN 設定檔的檔名。 當您按下 PPTP/IPsec/進階按鈕以便在 Vigor2925 與遠端 CPE 裝置建立 VPN 連線時，此檔案會自動產生。
類型(Type)	顯示撥入類型以及驗證方式。
遠端 IP(Remote IP)	顯示遠端 CPE 的 IP 位址與介面。
虛擬網路(Virtual Network)	顯示 Vigor2925 系列的 IP 位址與子網遮罩。
傳送封包(Tx Pkts)	顯示傳送封包的數量。
傳送速率(Tx Rate(Bps))	顯示傳送速率值。
接收封包(Rx Pkts)	顯示接收封包的數量。
接收速率(Rx Rate(Bps))	顯示接收速率值。
上線時間(Up Time)	顯示此 VPN 連線的時間。

一旦 Vigor2926 掌管了裝置，該裝置會立刻顯現在螢幕上，若未顯示，請參考章節“如何透過 Vigor2926 管理 CPE (路由器)?”

VII-5-4 紀錄與警示(Log & Alert)

本頁提供簡易資訊用以辨認連接至 Vigor2926 系列的 CPE 爲何。



可用設定說明如下：

項目	說明
顯示模式(Display Mode)	選擇一種模式讓系統顯示相關資訊於下表: ● **滿碟時停止紀錄(Stop record when fulls) -** 當紀錄已滿系統將停止紀錄。 ● **永遠紀錄最新事件(Always record the new event) -** 系統只紀錄最新事件。
裝置名稱(Device Name)	顯示受管理的 CPE 裝置。
說明名稱(Description Name)	顯示受管理的 CPE 裝置的簡要說明。
時間與日期(Time & date)	顯示路由器掃瞄偵測出的 CPE 裝置的時間與日期。
動作類型(Action Type)	顯示路由器對 CPE 所進行的動作類型。
訊息(Message)	顯示每種事件的簡易資訊。

警示頁面主要提供簡易資訊，以辨識連接至路由器的 CPE 裝置爲何。

應用說明

A-1 CVM 應用–如何透過 Vigor2926 管理 CPE (路由器)?

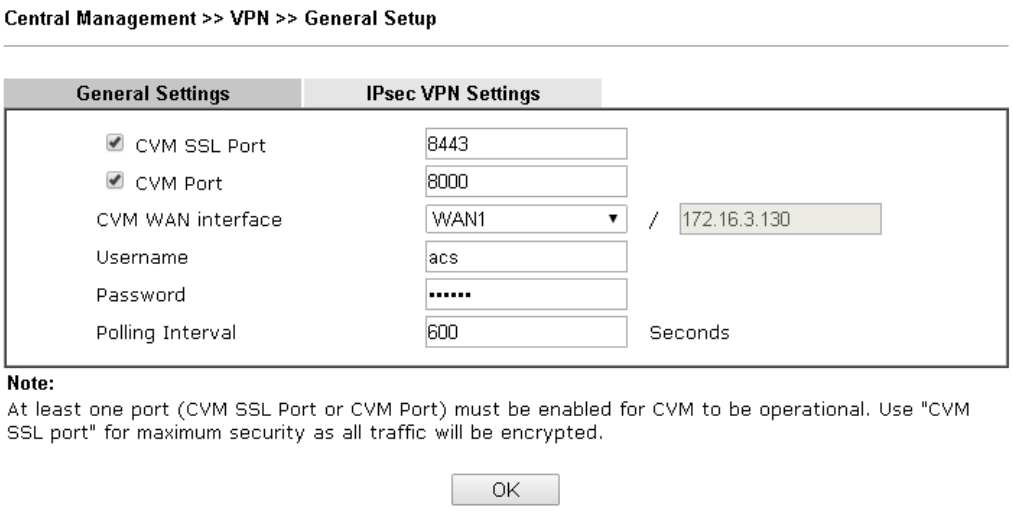
欲透過 Vigor2926 管理 CPE，您必須先設定 CPE 的 ACS URL 再設定 Vigor2926 的使用者名稱與密碼，這個範例中，我們使用 Vigor2850 系列來說明。

設定 Vigor2926

1. 登入 Vigor2926 的網頁使用者設定介面。
2. 開啓 **中央管理>>VPN>>基本設定(Central Management>>VPN>>General Setup)**。



3. 在如下頁面中，勾選 CVM 埠號與 CVM SSL 埠號以便啓用該埠號設定，分別輸入 CVM 埠號值、CVM SSL 埠號值、使用者名稱與密碼，請記住本頁設定的內容。



4. 按下**確定(OK)**儲存。

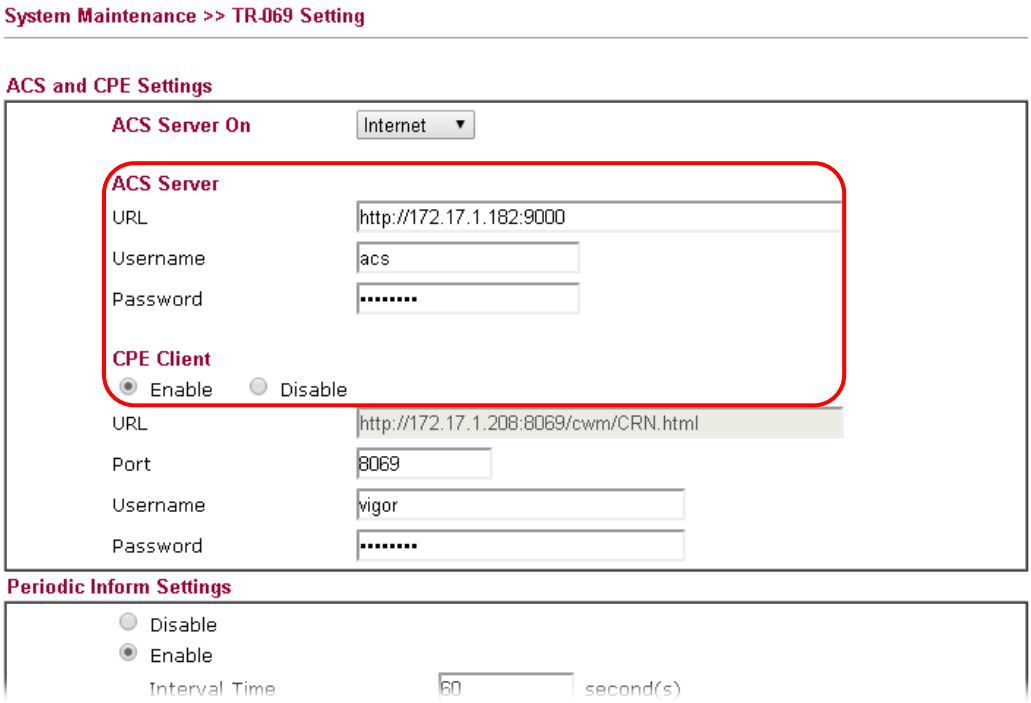
設定 CPE

1. 在連接 CPE 的電腦端，開啓任一網頁瀏覽器(例如 IE, Mozilla Firefox 或 Netscape)，網址欄處輸入 **http://192.168.1.1**。

2. 開啓**系統維護>>TR-069(System Maintenance >> TR-069)**。

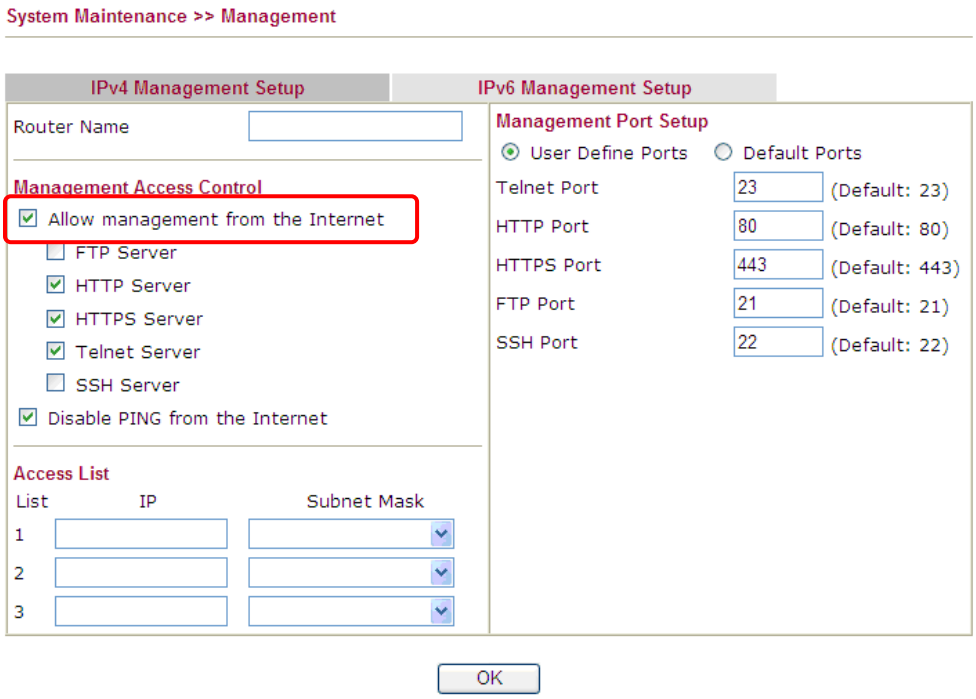


3. 在 ACS Server 欄位中，請輸入 Vigor2926 的 URL (格式爲 http://{IP address of Vigor2925}:{CVM port}/ACSServer/services/ACSServlet)並在 Vigor2926 的**中央管理>>VPN>>基本設定(Central Management>> VPN >>General Setup)** 頁面中輸入與此相同的使用者名稱及密碼資訊，接著，CPE Client 項目按下 **Enable**，再按下**確定(OK)**儲存設定。



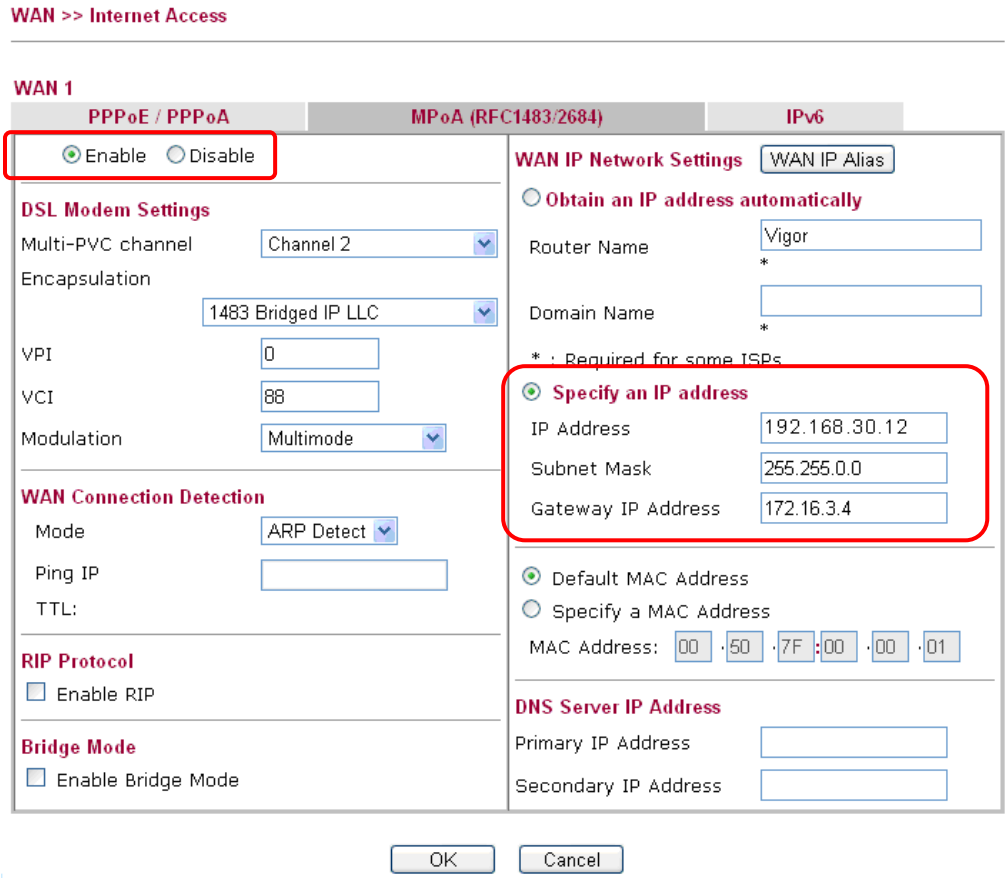
4. 開啓**系統維護>>管理設定(System Maintenance>>Management Setup)**。

5. 勾選**允許遠端管理(Allow management from the Internet)** 進行遠端管理設定，再按**確定(OK)**。



6. 開啓 **WAN>>網際網路連線控制(WAN>>Internet Access)**，在 WAN1 項目下使用**連線模式(Access Mode)**下拉式清單，選擇 **MPoA** (RFC1483/2684)模式，接著按下**細節設定(Details Page)**。

7. 按下**指定 IP 位址(Specify an IP address)**，輸入有關 CPE 正確的 WAN IP 位址，子網遮罩以及閘道 IP 位址，再按下**確定(OK)**儲存。

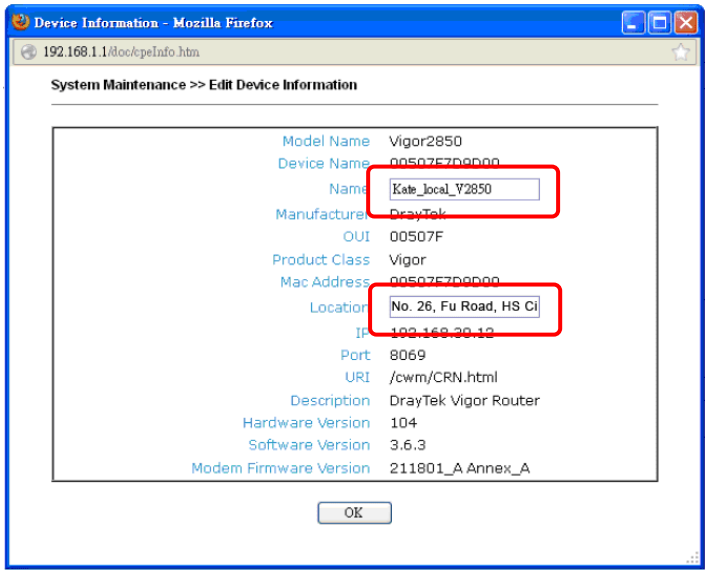


資訊

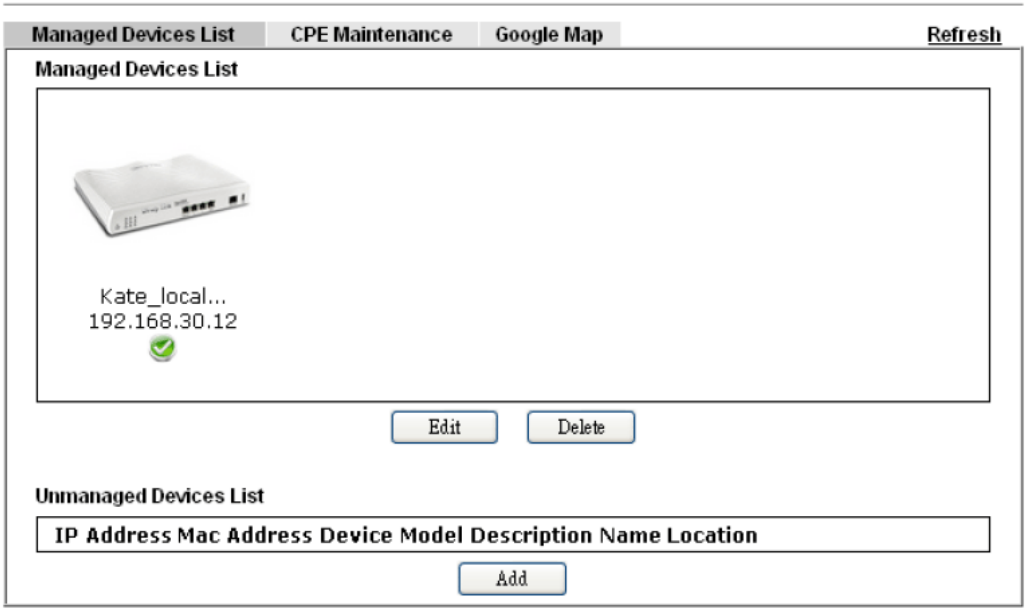
啓動 CPE 並重新登入 Vigor2926，已經登錄至 Vigor2926 的 CPE 將立刻由系統擷取相關資料並會顯示在 Vigor2926 網頁使用者設定介面之**中央管理>>VPN>>CPE 管理(Central Management>>VPN>>CPE Management)**頁面中。

檢查 CPE 管理頁面

1. 回到 Vigor2926 的網頁使用者設定介面。
2. 開啓**中央管理>>VPN>>CPE 管理(Central Management>>VPN>>VPN Management)**。現在已經有一台 CPE 在 Vigor2926 的管理下。
3. 自 Unmanaged Devices List 中選擇一 CPE 並按下**新增(Add)**，下述畫面將會出現，請分別輸入路由器名稱與位置，按**確定(OK)**儲存。



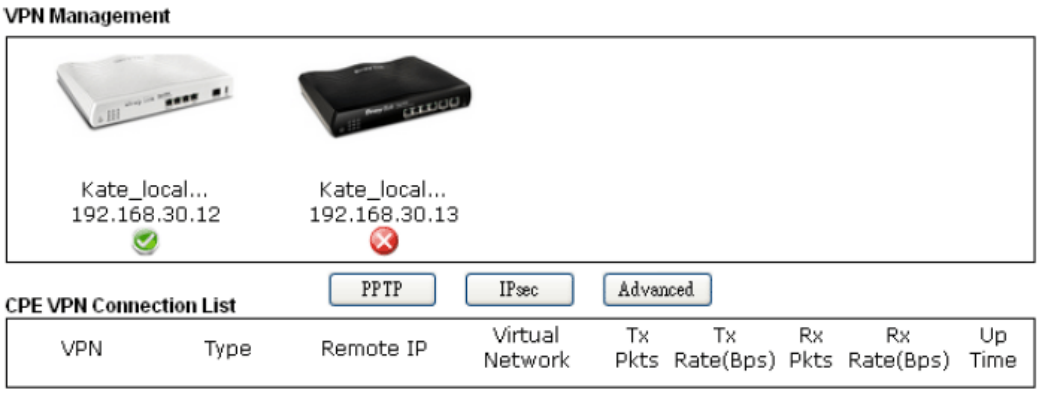
4. 選定的 CPE 將可移往並顯示在 Managed Devices List 區域中，此即表示該裝置已經在 Vigor2926 的管理下。



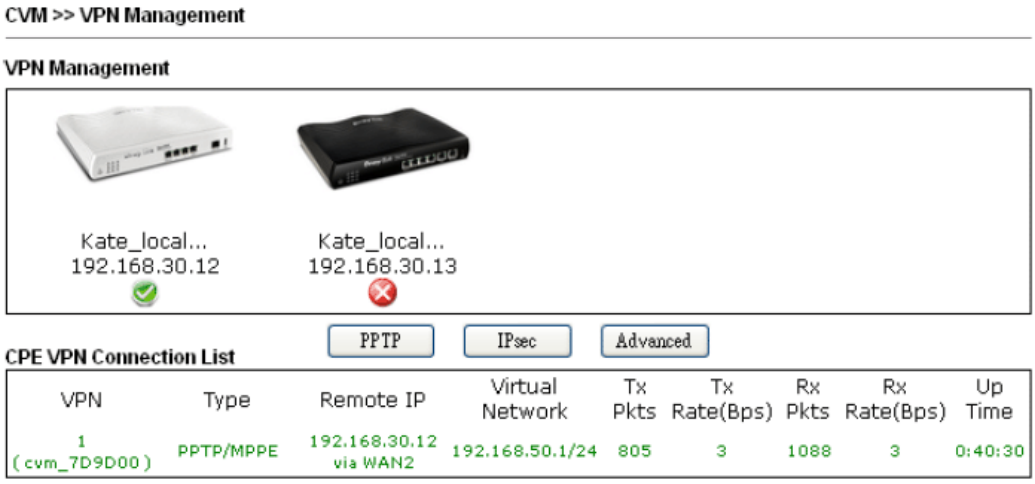
A-2 CVM 應用–如何於 Vigor2926 與遠端設備之間建立 VPN 連線?

當遠端設備已被納入 Vigor2926 管理之下，我們可以很輕易的在這二者之間建立一條 VPN 連線。

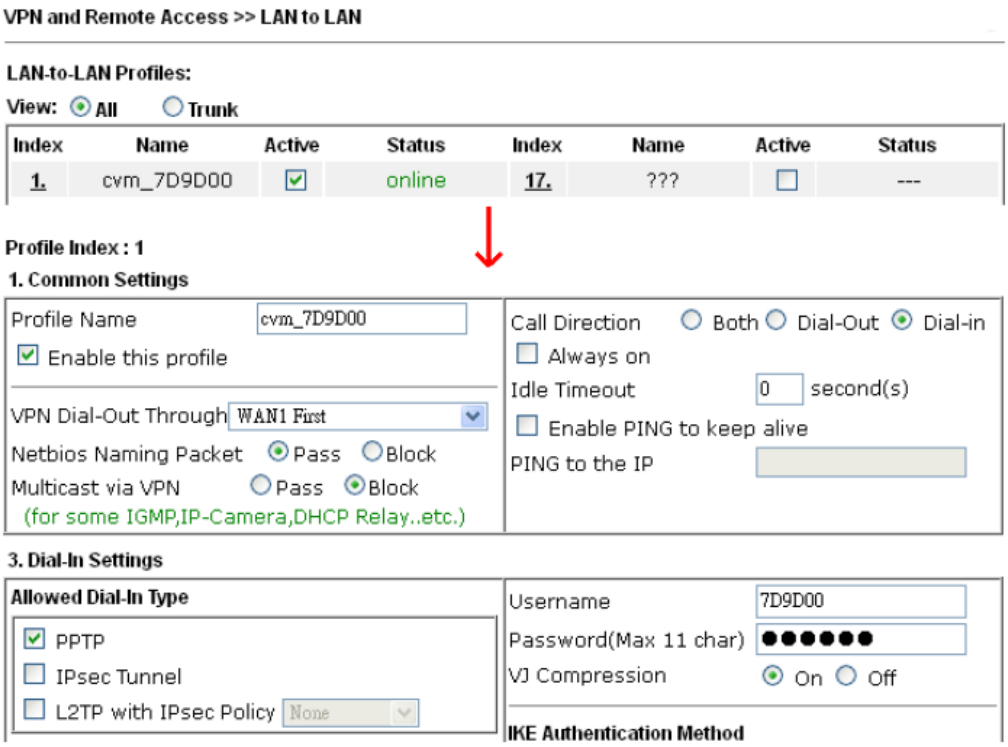
1. 登入 Vigor2926 系列的網頁使用者設定介面。
2. 開啓**中央管理>>VPN>>CPE 管理(Central Management>> VPN >>CPE Management)**。



3. 按下遠端設備圖示(標示)並按下 **PPTP** 或是 **IPsec** 按鈕。
4. 請耐心等候，如果 VPN 連線建立成功，相關資訊將會顯示在畫面下方的**已連接裝置(CPE VPN Connection List)** 區域。



5. 現在針對此 VPN，系統已經自動產生一組 LAN to LAN 設定檔，您可以進入遠端設備的 **VPN 與遠端存取>>LAN to LAN(VPN and Remote Access>>LAN to LAN)**頁面檢視詳細的內容。



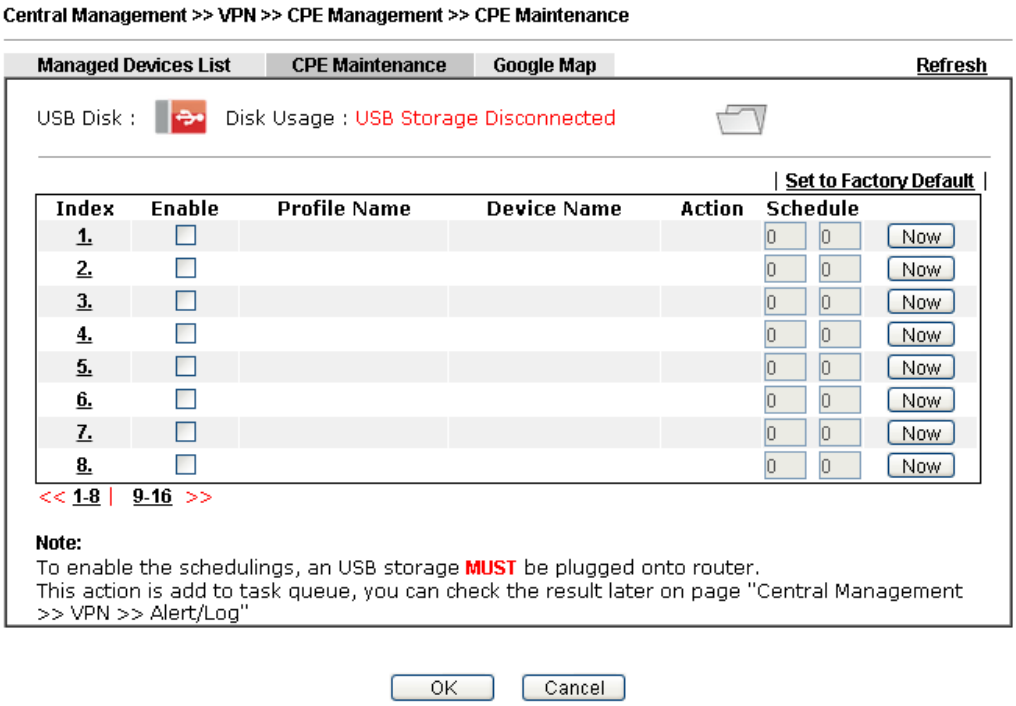
注意，設定檔是由系統自動產生，請勿任意修正內容以免造成 VPN 連線錯誤。

A-3 CVM 應用–如何透過 Vigor2926 更新遠端 CPE 韌體?

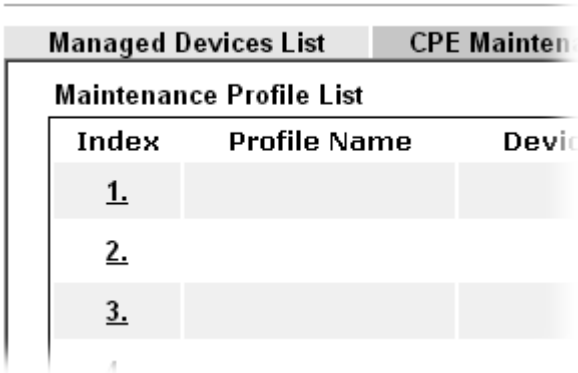
自居易官網下載 Vigor2926 管理下的裝置(例如 Vigor2850)最新的韌體並放置於 USB 儲存碟內。

1. 將 USB 隨身碟插入 Vigor2926 中(可透過 USB 介面)，務必確認 USB 儲存碟已正確插入，否則韌體更新將無法成功。

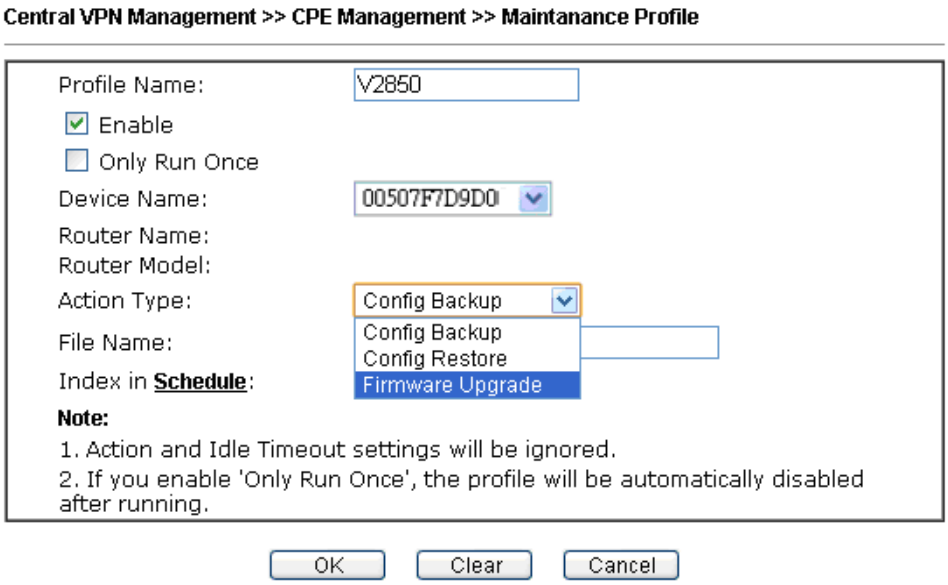
2. 登入 Vigor2926 的網頁設定介面，開啓**中央管理>>VPN>>CPE 維護(Central Management>>VPN>>CPE Management)** 並按下 **CPE 維護(CPE Maintenance)**標籤。



3. 按下任一索引編號例如 1 連結。

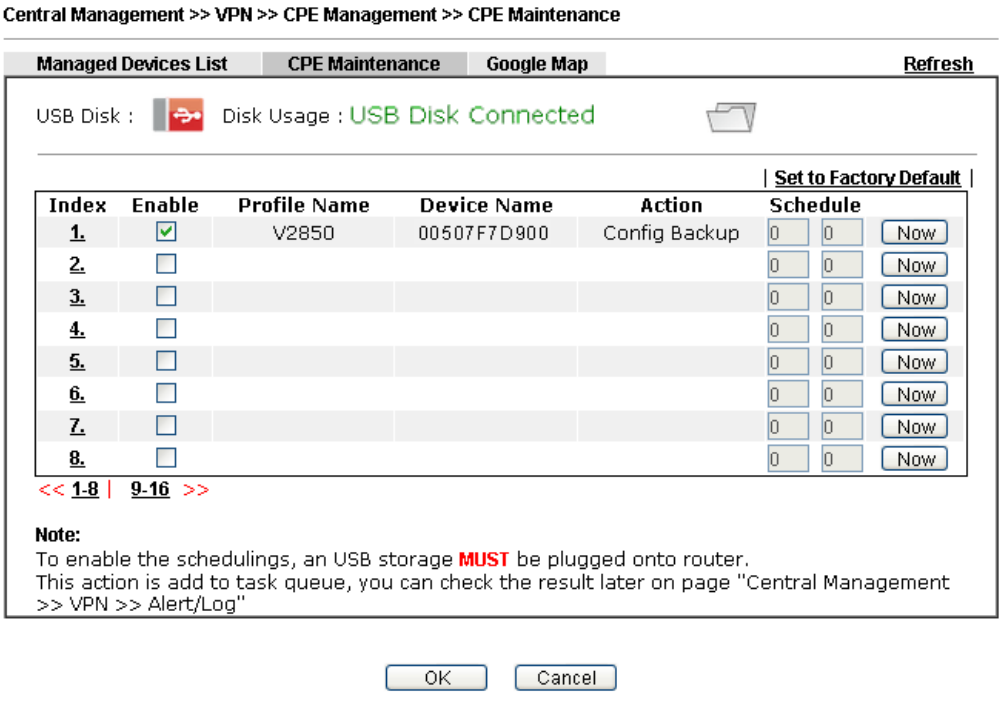


4. 維護設定檔畫面如下顯示。



在設定檔名稱區中，輸入此維護設定檔名稱，勾選啓用；然後選擇**韌體更新**項目，輸入新韌體之檔案/路徑或是按選擇按鈕來挑選，指定排程設定檔，最後，按下**確定(OK)**。

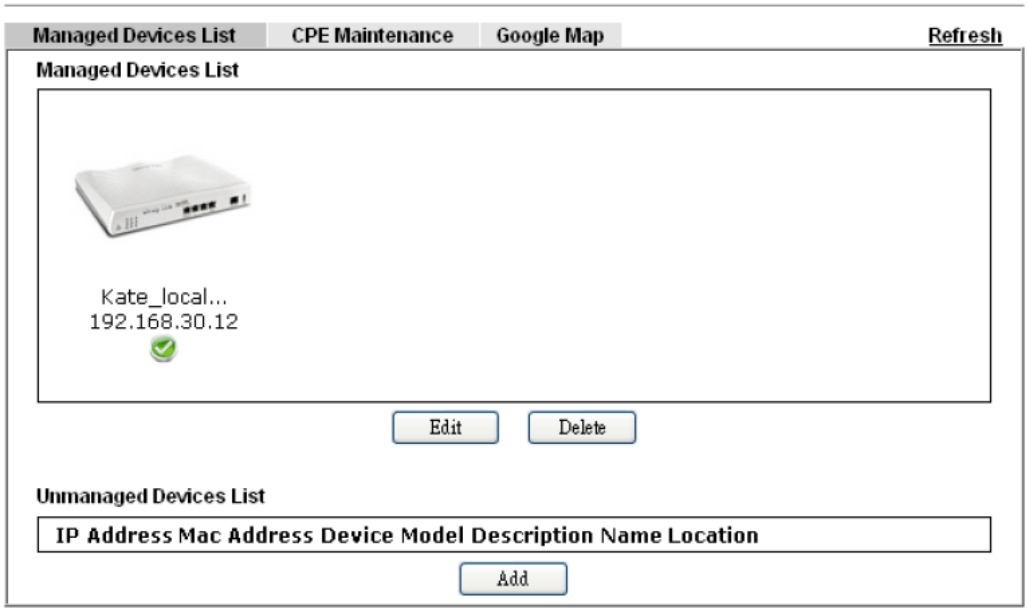
5. 現在您已經完成建立新的維護設定檔。



6. 按下**現在(Now)**按鈕可立即進行 Vigor2850 的韌體更新，如有需要的話。

7. 請等數分鐘讓系統完成更新。

8. 接著檢查裝置的相關資訊，看看韌體更新是否成功，可按下 **Managed Devices List** 標籤來檢視。



按下代表 CPE 的小圖示並按下**編輯(Edit)**按鈕，即可檢視軟體目前的版本狀態，另一個方法是打開**中央管理>>VPN>>紀錄與警示(Central Management>>VPN>>Log & Alert)**亦可檢查韌體更新的狀態。

VII-6 中央管理(AP)

透過中央管理功能，Vigor2926 能管理支援 AP 管理特性的 VigorAP 基地台。

AP 地圖

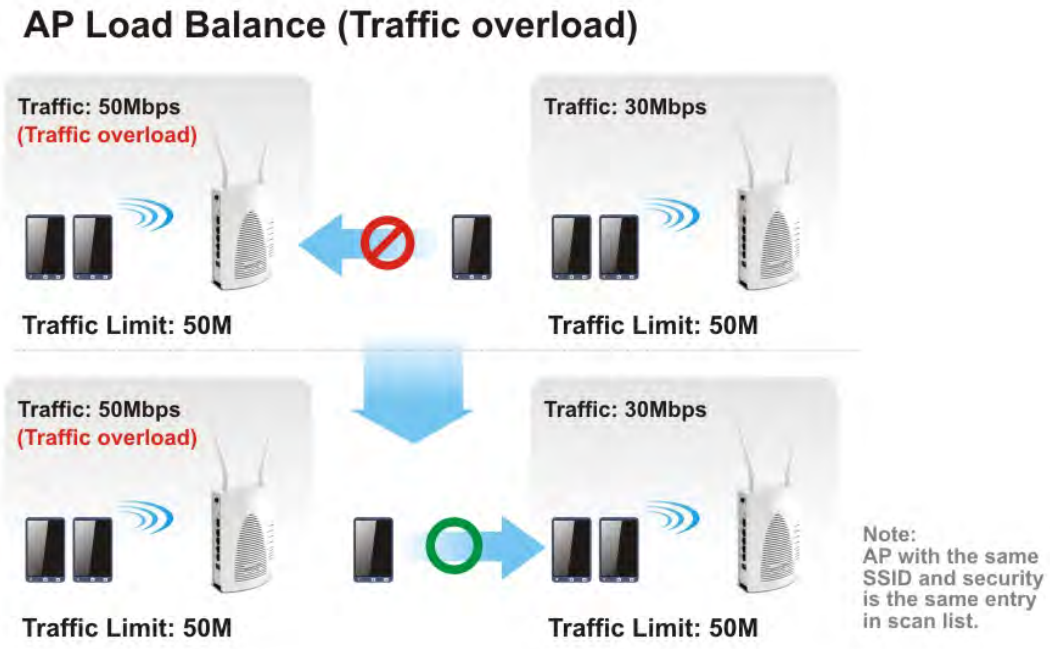
AP 地圖對決定 VigorAP 的最佳位置是很有幫助的，首先需要準備場地的平面圖，接著將可用的 VigorAP 從清單中拖曳到平面圖上，系統會模擬訊號的強度大小，如此一來即可在畫面上清楚見到具備最佳無線涵蓋範圍的地點。

AP 維護

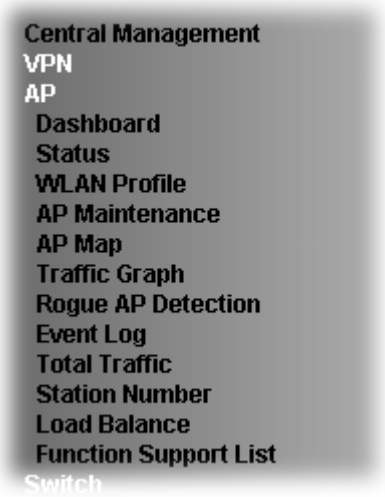
針對受管理的 AP，Vigor 路由器可執行設定備份、設定配置還原、韌體更新與遠端重啓等作業，無需登入基地台的網頁設定介面即可進行相關維護作業，對管理者而言，非常方便。

負載平衡

負載平衡的設定參數可以幫忙分配所有註冊至 Vigor 路由器的 AP 基地台的網路流量，這樣頻寬就不會被特定的基地台佔據過久。

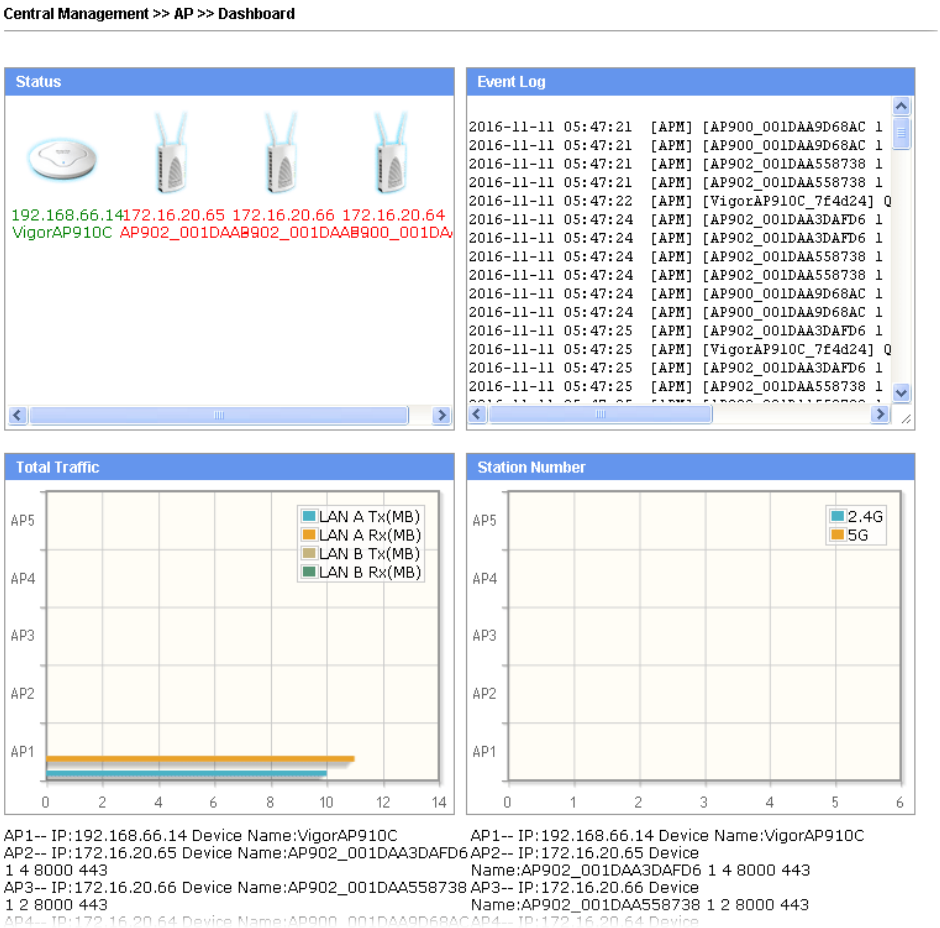


網頁使用者介面



VII-6-1 儀表板(Dashboard)

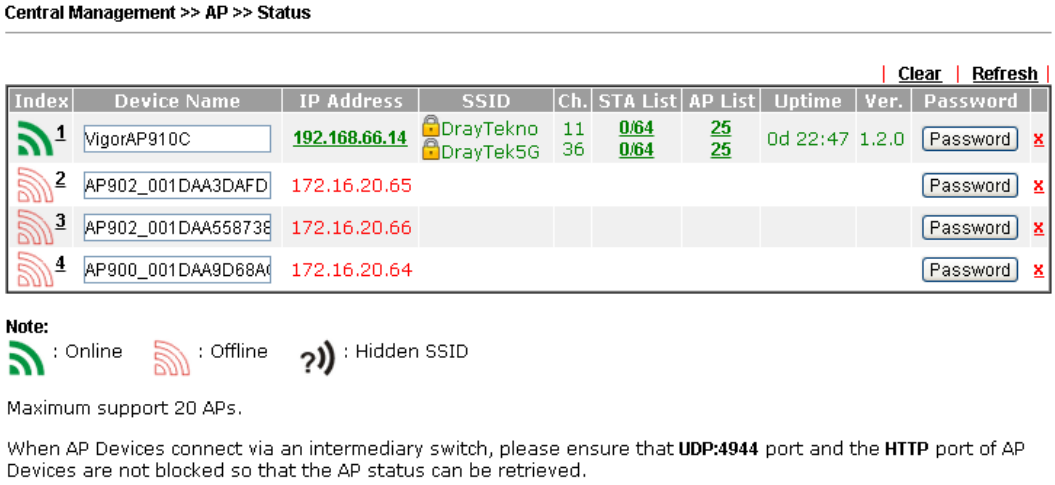
本頁顯示基地台的主要資訊，包含狀態、事件記錄、全部流量或是站台數目等等，移動滑鼠游標至相關顯示項目並按下滑鼠按鈕，相關網頁將會顯示在螢幕上。



欲登入 VigorAP 網頁使用者介面，只要移動滑鼠游標在 VigorAP 的圖示上並按下滑鼠按鈕，系統將會導引登入 VigorAP 的設定介面。

VII-6-2 狀態(Status)

頁顯示 Vigor 路由器所管理的基地台目前的狀態(包含連線、斷線或是隱藏 SSID、IP 位址、加密、頻道、版本、密碼等等資訊)。可進入**中央管理>>AP>>功能支援列表**，檢查支援的 AP 機種有哪些。

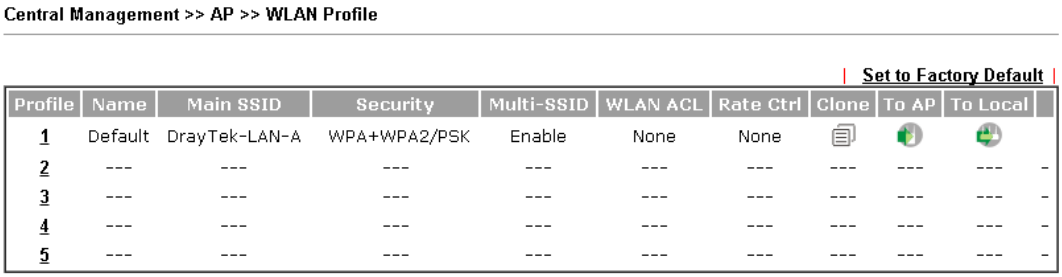


可用設定說明如下：

項目	說明
索引編號(Index)	按下索引編號連結以檢視 AP 基地台的設定總結。
裝置名稱(Device Name)	顯示 Vigor 路由器所管理的 AP 裝置名稱。
IP 位址(IP Address)	顯示 AP 基地台的 IP 位址。
SSID	顯示連接至路由器的 AP 基地台其使用的 SSID 內容。
頻道(Ch.)	顯示 AP 基地台使用的頻道。
無線用戶端(STA List)	顯示連接至 AP 基地台的無線用戶端編號。 其中，0/64 表示最高系統允許 64 台用戶連接至此基地台，但目前尚未有任何無線用戶連接至該基地台。 顯示在左邊的號碼代表 2.4GHz；顯示在右邊的號碼代表 5GHz。
AP 清單(AP List)	顯示環繞此裝置旁其他 AP 的數量。
上線時間(Uptime)	顯示 AP 啓用後持續的時間。
版本(Version)	顯示此 AP 基地台目前使用的韌體版本。
密碼(Password)	顯示路由器得以進入 AP 基地台取得所需的設定資訊的密碼。 此按鈕主要是用來修改登入連結之基地台的密碼。

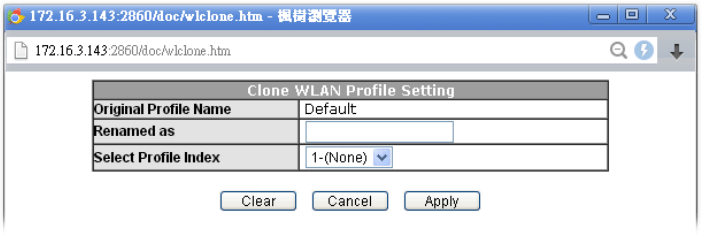
VII-6-3 WLAN 設定檔(WLAN Profile)

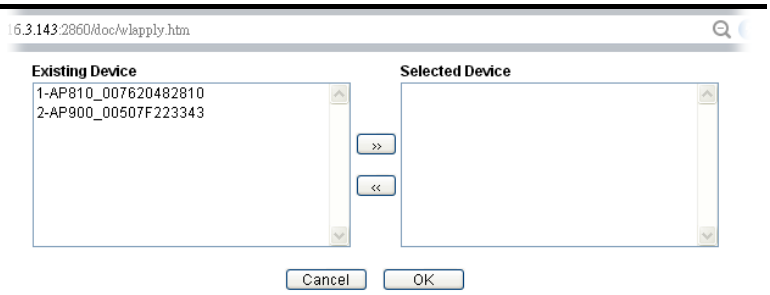
無線網路(WLAN)設定檔可套用至選定的 AP 基地台，無需開啓基地台使用者介面即可變更基地台的設定，對於管理者而言，非常便利。



點選左邊的連結，可修改該設定檔的內容。

可用設定說明如下：

項目	說明
設定檔(Profile)	顯示設定檔的連結。
名稱(Name)	顯示設定檔的名稱。 預設的設定檔名稱(Default)無法更改名稱。
主要 SSID (Main SSID)	顯示此無線設定檔使用的 SSID 名稱。
安全性(Security)	顯示此無線設定檔選定的安全性模式。
多重 SSID (Multi-SSID)	啓用表示多重 SSID 爲活動狀態。 停用表示僅有 SSID1 爲活動狀態。
WLAN ACL	顯示無線控制清單的名稱。
流量控制(Rate Ctrl)	顯示上傳與/或下載的傳輸速率。
複製(Clone)	用以自現有的 WLAN 設定檔複製相同的設定內容至另一個 WLAN 設定檔內。 請先勾選現有的 WLAN 設定檔作爲原始設定檔，接著按下**複製(Clone)**按鈕，下面的對話盒將會出現：  然後，選擇準備套用的設定檔之索引編號，於**更名如(Renamed as)**欄位中再輸入一個新的名稱，最後按下**套用(Apply)**即可儲存相同的設定。 新的設定檔(含有原始設定檔的設定)即可完成建立。
套用至裝置(To AP)	按此鈕可套用選定的無線設定檔至指定的 AP 基地台。

	 自**現有裝置(Existing Device)**區域中選擇您想要的裝置，然後按**>>按**鈕將該選定裝置移往右邊的**選定裝置(Selected Device)**欄位，然後按下**確定(OK)**按鈕。 選定的無線區域網路設定檔將會立即套用至選定的基地台，之後該基地台會自行重新啓動。
套用至本機(To Local)	本頁設定的設定檔主要是提供給連接至路由器的 VigorAP。 如有必要，這些設定也可以運用於路由器上。選擇並勾選無線設定檔，並按下此按鈕以便套用本頁設定至路由器的無線網路設定上。

如何編輯無線區域網路設定檔?

1. 勾選選定之設定檔左邊的方框。
2. 按下**編輯(Edit)**按鈕以顯示如下頁面。

Central Management >> AP >> WLAN Profile

WLAN Profile Edit

Device Settings	
Profile Name	Default ☐ Auto Provision
Administrator	admin
Password	•••••
2nd Subnet	◉ Enable ○ Disable

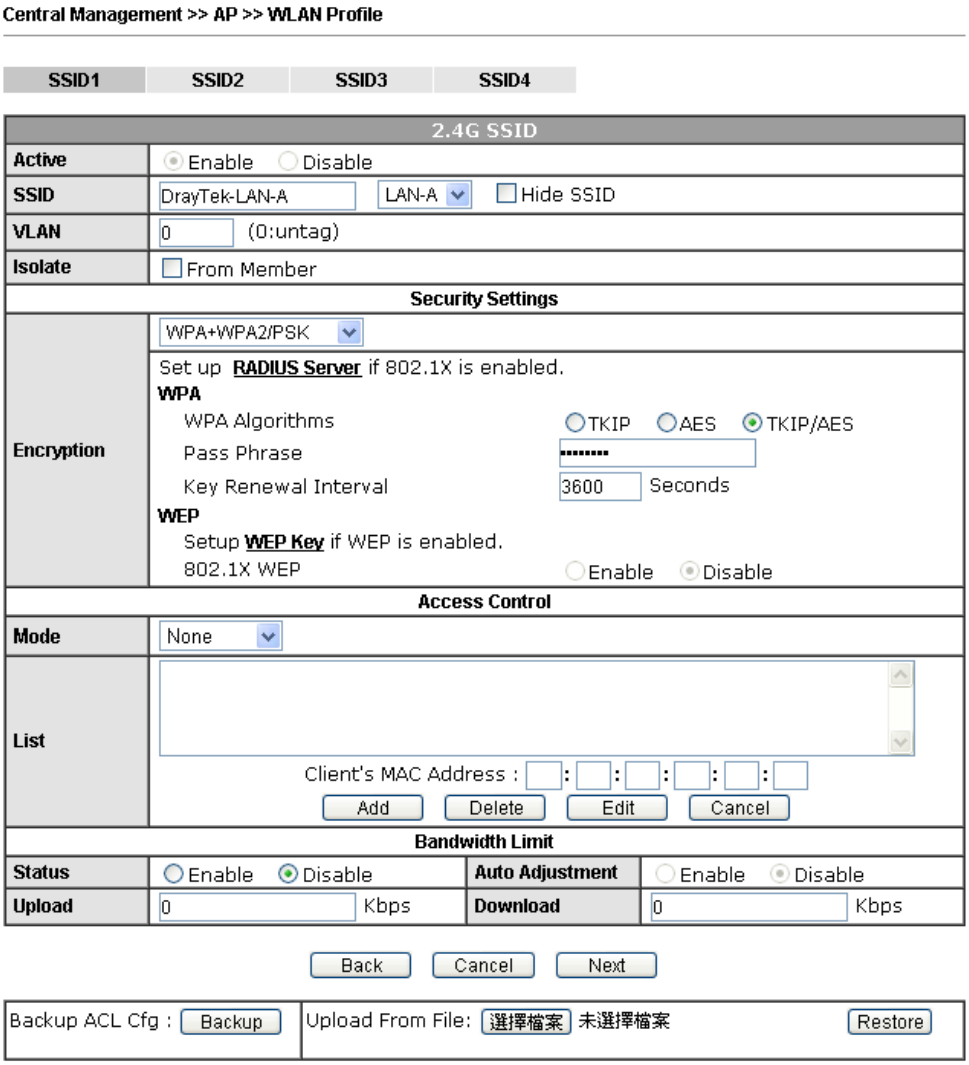
2.4G WLAN General Settings	
Wireless LAN	○ Enable ◉ Disable
Limit Client	☐ Enable 64 (3 ~ 128) (Default: 64)
Operation Mode	AP
2.4G Mode	Mixed(11b+11g+11n)
2.4G Channel	2462MHz (Channel 11)
Airtime Fairness	☐ Enable Airtime Fairness: Triggering Client Number 2 (2 ~ 128) (Default: 2)
Band Steering	☐ Enable Band Steering: Check Time for WLAN Client 5G Cap. 15 sec(s) (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%

5G WLAN General Settings	
Wireless LAN	○ Enable ◉ Disable
Limit Client	☐ Enable 64 (3 ~ 128) (Default: 64)
Operation Mode	AP
5G Mode	Mixed (11a+11n)
5G Channel	5180MHz (Channel36)
Airtime Fairness	☐ Enable Airtime Fairness: Triggering Client Number 2 (2 ~ 128) (Default: 2)
Roaming	☐ Minimum Basic Rate 6 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)

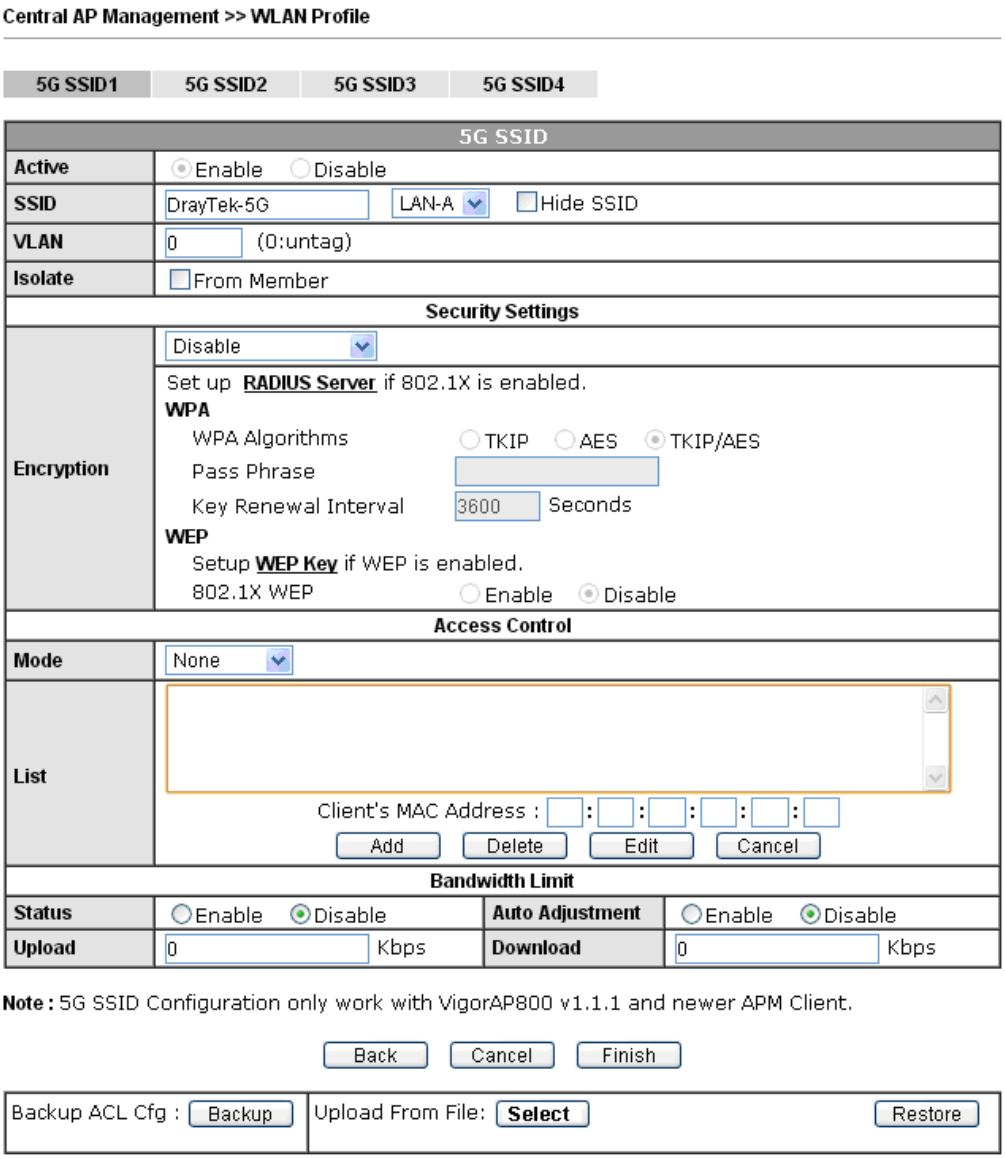
Cancel Next

資訊	Auto Provision 僅在 WLAN 的預設設定檔中可以使用。

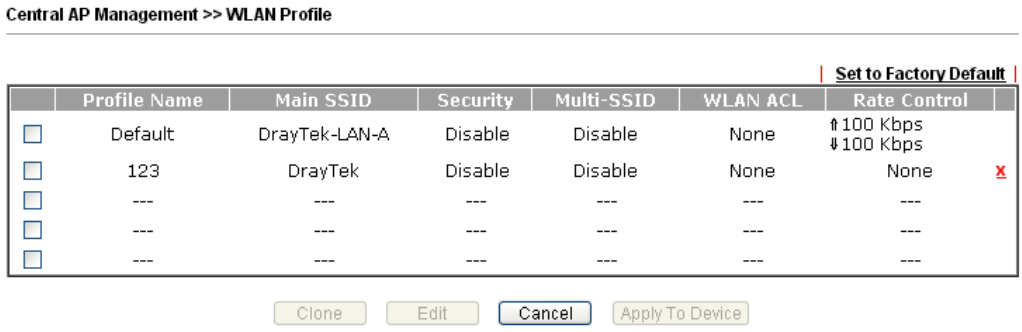
3. 完成基本設定之後，按**下一頁(Next)**開啓如下頁面進行 2.4G 無線安全性設定。



4. 完成上述的頁面設定之後，按**下一頁(Next)**開啓如下頁面進行 5G 無線安全性設定。



5. 完成 5G 無線安全性設定，請按**完成(Finish)** 結束頁面設定。修正後的無線設定檔將會顯示在網頁上。

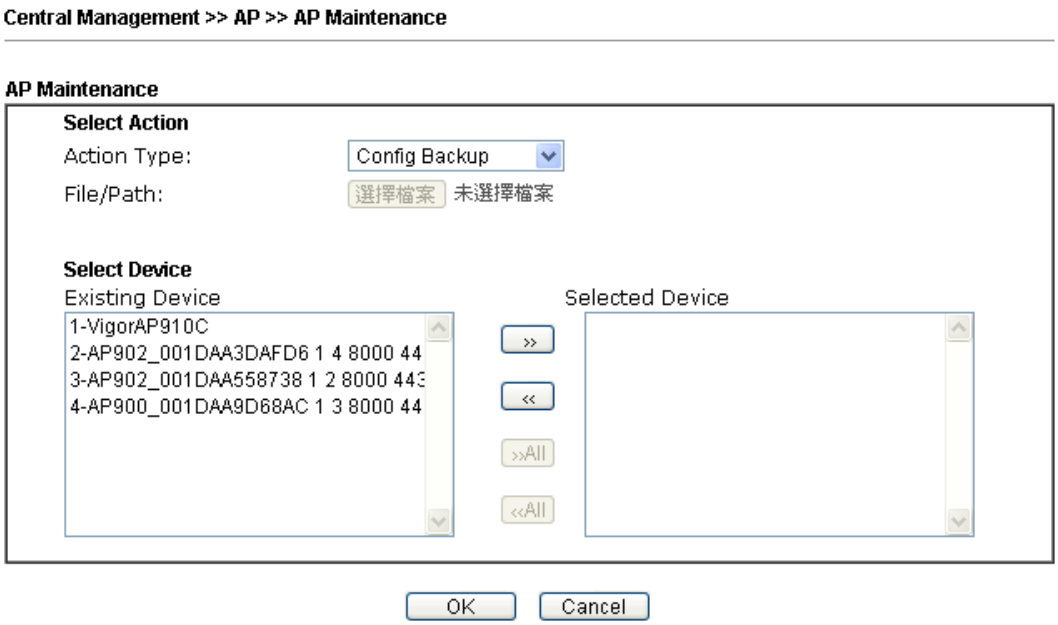


VII-6-4 AP 維護(AP Maintenance)

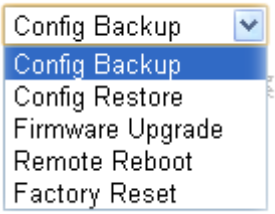
針對受管理的 AP，Vigor 路由器可執行設定備份、設定配置還原、韌體更新與遠端重啓等作業，無需登入基地台的網頁設定介面即可進行相關維護作業，對管理者而言，非常方便。

資訊

透過路由器進行 AP 設定備份一次只能針對一台 AP 進行，其他的功能(如設定還原、韌體更新與遠端重啓則可一次針對數台 AP 進行)。



可用設定說明如下：

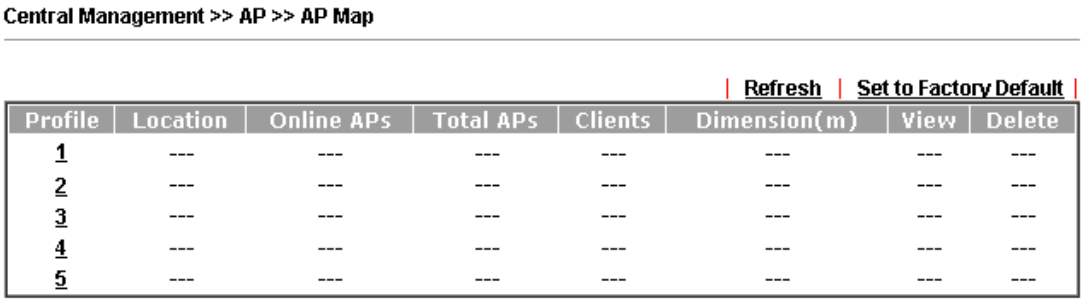
項目	說明
動作類型(Action)	有四種動作可以進行，分別是設定備份(Config Backup)、設定配置還原(Config Restore)、韌體更新(Firmware Upgrade)與遠端重啓(Remote Reboot)以及出廠預設(Factory Reset)。  路由器可以備份選定 AP 的設定，還原選定 AP 的設定，執行選定 AP 的韌體更新，遠端重新啓動選定 AP，以及回復選定 AP 的出廠預設值。
檔案/路徑(File/Path)	指定**設定配置還原(Config Restore)**以及**韌體更新(Firmware Upgrade)**作業需求之檔案與路徑。
現存裝置(Select Device)	顯示路由器管理下的現有的 AP 基地台，按下<<或是>>按鈕讓選定的 AP 於左邊現存裝置區域或右邊選定裝置區域之間移動。

選定裝置(Selected Device)	顯示按下確定按鈕後，將套用此功能的基地台名稱。

完成上述設定之後，按下**確定(OK)**儲存並執行相關作業。

VII-6-5 AP 地圖(AP Map)

AP 地圖對決定 VigorAP 的最佳位置是很有幫助的，首先需要準備場地的平面圖，接著將可用的 VigorAP 從清單中拖曳到平面圖上，系統會模擬訊號的強度大小，如此一來即可在畫面上清楚見到具備最佳無線涵蓋範圍的地點。

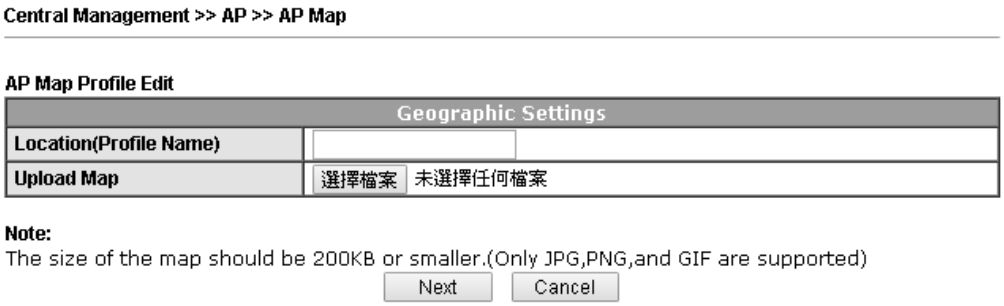


可用設定說明如下：

項目	說明
回復出廠預設值(Set to Factory Default)	按此連結清出目前的頁面設定。
設定檔(Profile)	按此連結可以檢視/編輯 AP 地圖。
地點(Location)	顯示 AP 地圖的簡易說明(如地板、樓層等等)。
線上 AP(Online APs)	顯示已設定且開啓電源之 VigorAP 的數量。
全部 AP(Total APs)	顯示已設定的 VigorAP 全部的數量。
用戶端(Clients)	顯示透過此 AP 存取網際網路的用戶端數目。
尺寸(Dimension(m))	顯示 AP 地圖的長與寬。
檢視(View)	按此檢視選定的 AP 地圖的佈局。

建立/編輯 AP 地圖設定檔

1. 選擇一個索引編號連結，按下**編輯(Edit)**開啓如下頁面。



可用設定說明如下：

項目	說明
地點(設定檔名稱) (Location (Profile Name))	輸入 AP 地圖設定檔的名稱(例如 groudfloor)。
上傳地圖(Upload Map)	按下**選擇(Select)**按鈕挑選平面圖的影像檔案(目前僅支援 JPG 與 PNG 檔案格式)。
取消(Cancel)	按此取消設定。
下一頁(Next)	按此進入下一個設定頁面。

2. 按**下一頁(Next)**，平面圖的尺寸顯示如下：

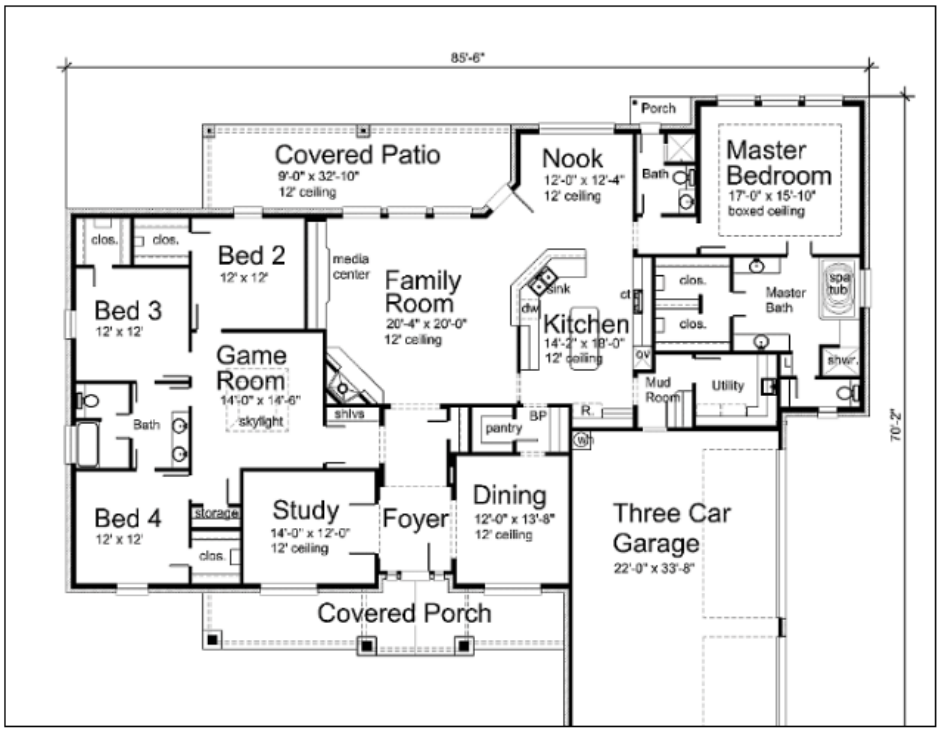
AP Map Profile Edit

Dimension | Planning

Set Dimension

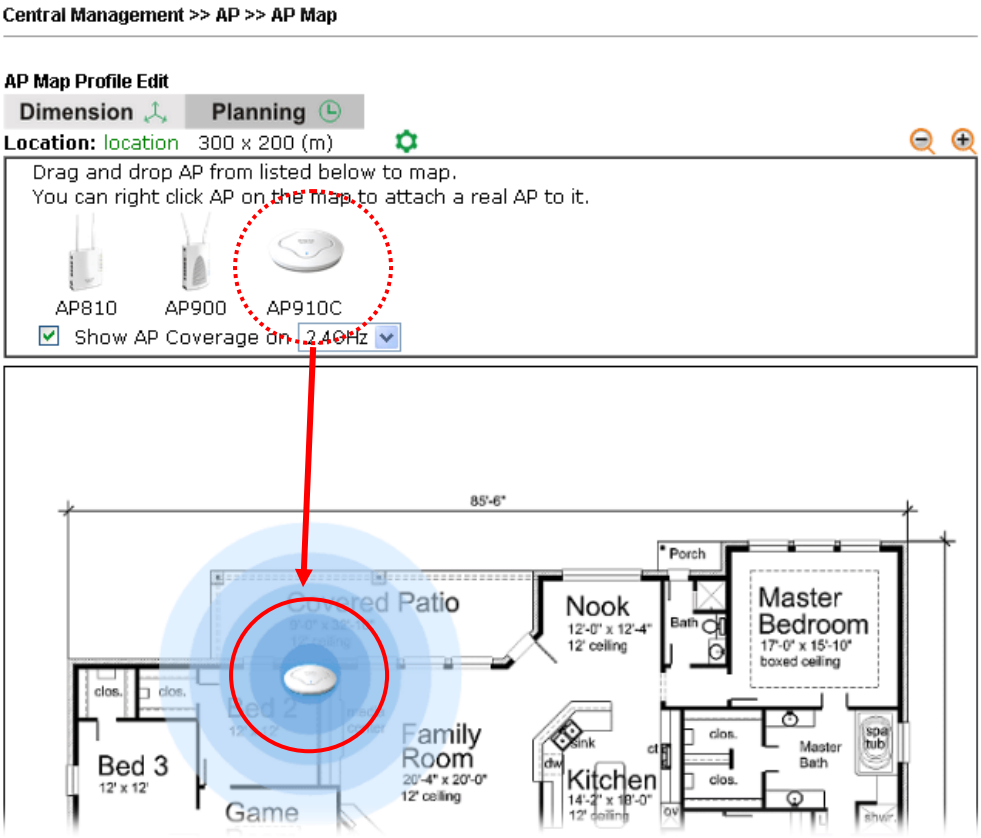
Length 300 m Width 200 m

Click the to draw a line on the map then enter its distance to calculate map dimensions.



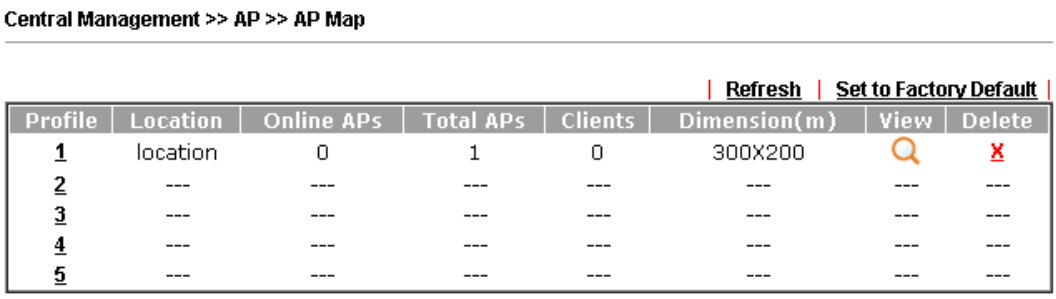
Next Cancel

3. 按下一頁**(Next)**進入設定頁面，拖曳 AP 清單中的 AP 圖示至畫面下方，然後放鬆滑鼠。



4. 勾選**顯示 AP 涵蓋範圍於..(Show AP Coverage on..)**來決定無線網路訊號，之後選擇 2.4GHz 或是 5GHz。

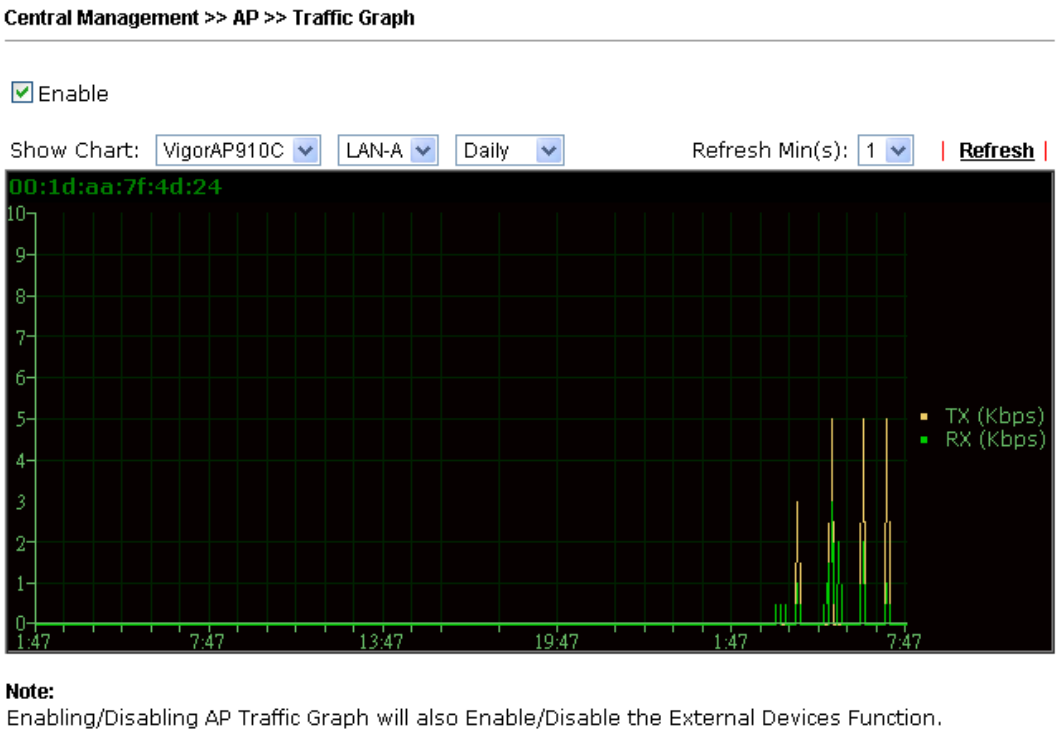
5. 調整地圖上的 AP 位置，找到具有最佳無線涵蓋範圍的位置，最後按下**儲存(Save)**。



Profile	Location	Online APs	Total APs	Clients	Dimension(m)	View	Delete
1	location	0	1	0	300X200		X
2	---	---	---	---	---	---	---
3	---	---	---	---	---	---	---
4	---	---	---	---	---	---	---
5	---	---	---	---	---	---	---

VII-6-6 流量圖表(Traffic Graph)

選擇流量圖表可開啓如下頁面，選擇一台受管理的 AP 基地台(LAN-A 或是 LAN-B)，每日或是每週，以便檢視資料傳輸圖表。按下**更新頁面(Refresh)**可以隨時重新整理顯示的頁面。

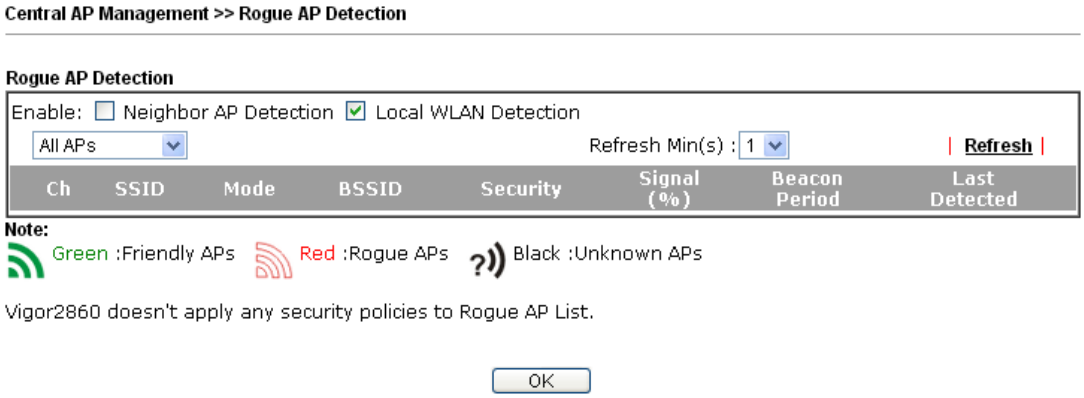


水平軸代表時間；垂直軸代表傳輸速率(單位 kbps)。

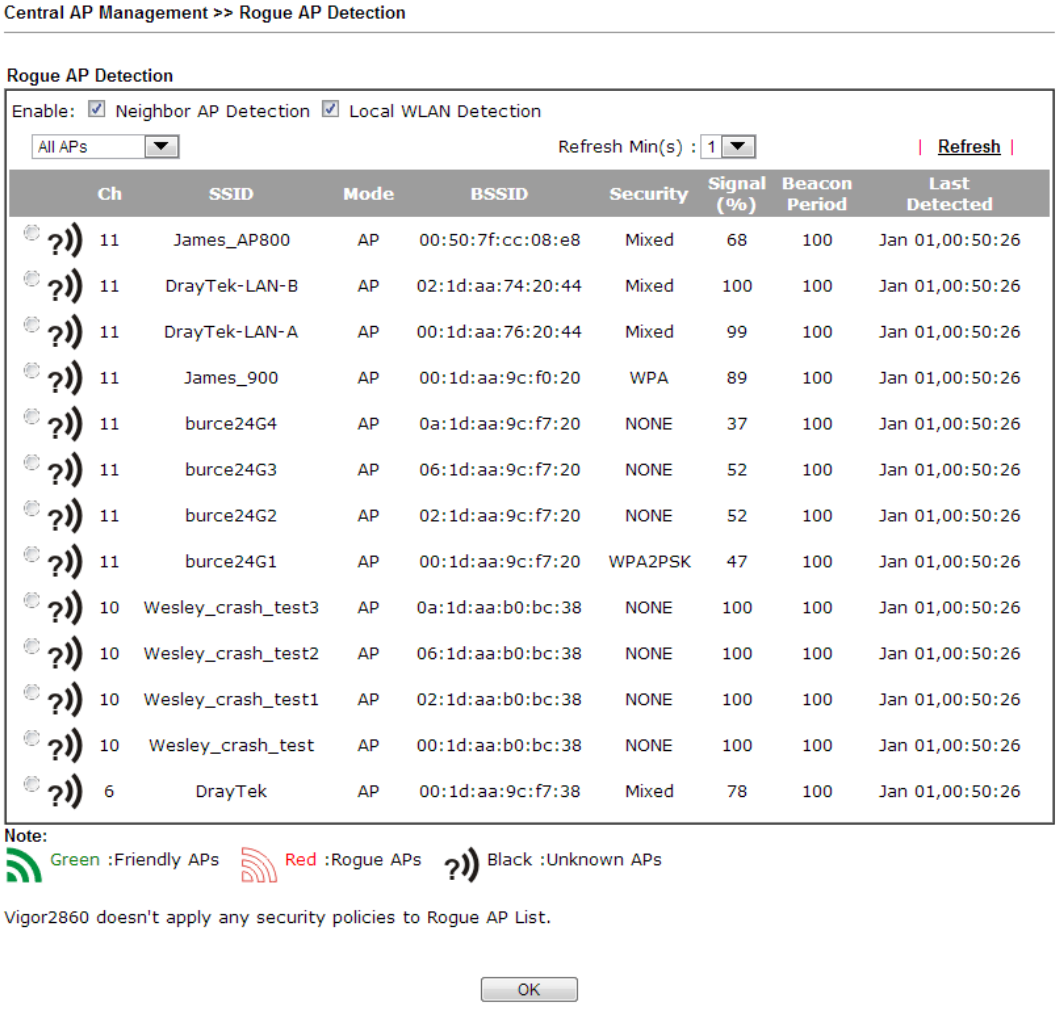
資訊	啓用/停用此功能將會啓用/停用外接裝置功能。

VII-6-7 非法 AP 偵測(Rogue AP Detection)

本頁顯示路由器偵測到的 AP 基地台，這些基地台皆以不同的顏色區分類型分別是友善 AP、非法 AP 以及未知 AP。

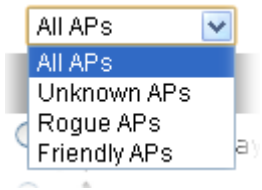


下圖顯示按下**確定(OK)**按鈕後系統偵測到的 AP 基地台資料。



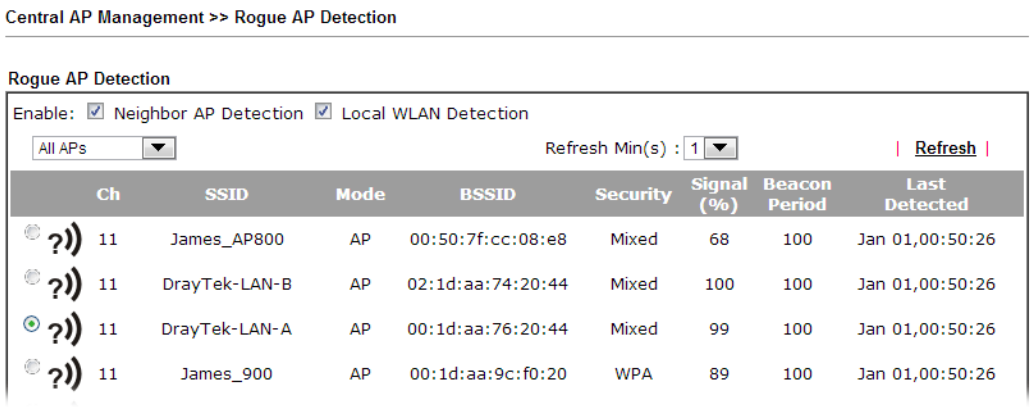
可用設定說明如下：

項目	說明
啓用(Enable)	**鄰近 AP 偵測(Neighbor AP Detection)-** 登錄至 Vigor2926 路由器的 AP 基地台被用來偵測其他的基地台，並傳送掃描結果至

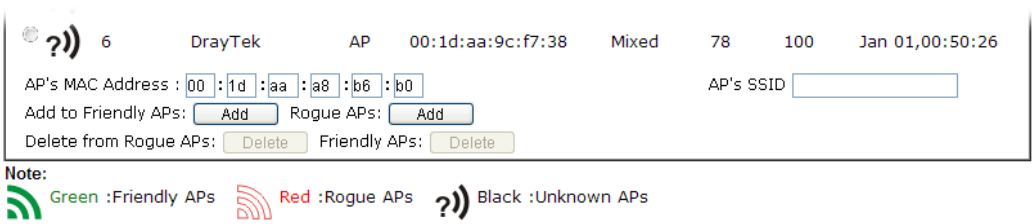
	Vigor2926 路由器，之後，掃描的結果會顯示在本頁。 **本區無線區域網路偵測(Local WLAN Detection) -** 路由器透過無線區域網路連線偵測所有的 AP 基地台。
	AP 被區分爲數種類別，請指定其中一種以顯示在畫面上。
更新時間(分) (Refresh Min(s))	使用下拉式清單指定更新此頁面的需求時間。
更新頁面(Refresh)	按此連結可立即更新此頁面。
頻道(Ch)	顯示被偵測到之 AP 基地台使用的頻道。
SSID	顯示被偵測到之 AP 基地台指定的 SSID。
模式(Mode)	顯示被偵測到之 AP 基地台使用的模式(AP 或是 Ad Hoc)。
BSSID	顯示被偵測到之 AP 基地台的 MAC 位址。
安全性(Security)	顯示 AP 基地台使用的加密模式。
訊號 (%)(Signal (%))	顯示 AP 基地台發送出來的訊號強度(以百分比表示)。。
信標(Beacon)期間 (Beacon Period)	顯示信標的期間，信標訊號將會定期發送出去。
最末偵測 (ast Detected)	顯示此 AP 基地台被路由器偵測到的最近一次日期與時間。

Vigor 路由器偵測出的所有 AP 基地台都將被視爲未知 AP，您必須分別指定哪些爲友善 AP 哪些爲非法 AP，請依照下列步驟執行分類事宜。

1. 選定其中一個 AP 基地台，按下左邊的按鈕，在本例中，選擇的是 DrayTek-LAN-A。



2. 稍後，頁面底部出現細部選項。

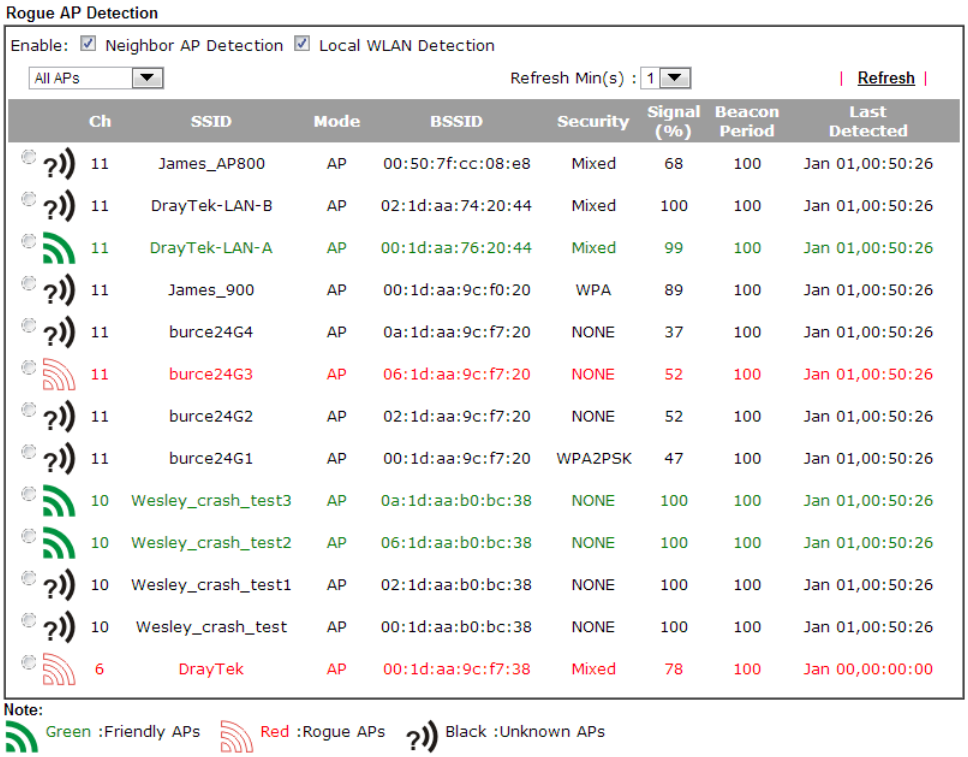


可用設定說明如下：

項目	說明
AP 的 MAC 位址 (AP's MAC Address)	選定 AP 基地台的 MAC 位址將會自動顯示出來。
AP 的 SSID (AP's SSID)	選定 AP 基地台的 SSID 將會自動顯示出來。
新增(Add to)	**加入友善 AP(Friendly APs)** – 若選定 AP 基地台將被視爲友善 AP，請按下新增鈕，系統即會將其分至友善 AP 類別。 **非法 AP (Rogue APs) -** 若選定 AP 基地台將被視爲非法 AP，請按下新增鈕，系統即會將其分至友非法 AP 類別。
自非法 AP 刪除/ 自友善 AP 刪除 (Delete From)	**非法 AP(Rogue APs) -** 如果您想要變更非法 AP 的類別，請選擇該非法 AP 並按下**刪除(Delete)**，之後頁面將會更新，該 AP 自動還原爲**未知 AP**。 **友善 AP(Friendly APs)** -如果您想要變更友善 AP 的類別，請選擇該友善 AP 並按下**刪除(Delete)**，之後頁面將會更新，該 AP 自動還原爲**未知 AP**。

3. 按下**確定(OK)**儲存設定。

下圖以不同顏色呈現不同類別的 AP 基地台之相關資訊。



VII-6-8 事件日誌(Event Log)

透過路由器管理的 VigorAP，發生在其上的事件與時間可以顯示在此頁面上。對於想要觀察事件內容進行疑難排除的人員來說，這個頁面的內容是很有幫助的。

Central Management >> AP >> Event Log

All Event Log | Clear | Refresh |

Time	APM Event Log
2016-11-11 06:12:08	[APM] [VigorAP910C_7f4d24] Query AP status
2016-11-11 06:12:09	[APM] [VigorAP910C_7f4d24] Query AP status success
2016-11-11 06:13:11	[APM] [VigorAP910C_7f4d24] Query AP status
2016-11-11 06:13:12	[APM] [VigorAP910C_7f4d24] Query AP status success
2016-11-11 06:14:10	[APM] [VigorAP910C_7f4d24] Query AP status
2016-11-11 06:14:11	[APM] [VigorAP910C_7f4d24] Query AP status success
2016-11-11 06:14:20	[APM] [VigorAP910C_7f4d24] Query AP status
2016-11-11 06:14:21	[APM] [VigorAP910C_7f4d24] Query AP status success
2016-11-11 06:14:55	[APM] [VigorAP910C_7f4d24] Query AP status
2016-11-11 06:14:56	[APM] [VigorAP910C_7f4d24] Query AP status success
2016-11-11 06:15:25	[APM] [VigorAP910C_7f4d24] Query AP status
2016-11-11 06:15:26	[APM] [VigorAP910C_7f4d24] Query AP status success
2016-11-11 06:15:55	[APM] [VigorAP910C_7f4d24] Query AP status
2016-11-11 06:15:56	[APM] [VigorAP910C_7f4d24] Query AP status success
2016-11-11 06:16:25	[APM] [VigorAP910C_7f4d24] Query AP status
2016-11-11 06:16:26	[APM] [VigorAP910C_7f4d24] Query AP status success
2016-11-11 06:16:54	[APM] [VigorAP910C_7f4d24] Query AP status
2016-11-11 06:16:55	[APM] [VigorAP910C_7f4d24] Query AP status success
2016-11-11 07:34:44	[APM] [AP902_001DAA558738 1 2 8000 443_558738] Query AP status
2016-11-11 07:34:44	[APM] [AP900_001DAA9D68AC 1 3 8000 443_9d68ac] Query AP status
2016-11-11 07:34:44	[APM] [AP900_001DAA9D68AC 1 3 8000 443_9d68ac] Query AP status
2016-11-11 07:34:45	[APM] [AP902_001DAA3DAFD6 1 4 8000 443_3dafd6] Query AP status
2016-11-11 07:34:45	[APM] [AP902_001DAA3DAFD6 1 4 8000 443_3dafd6] Query AP status

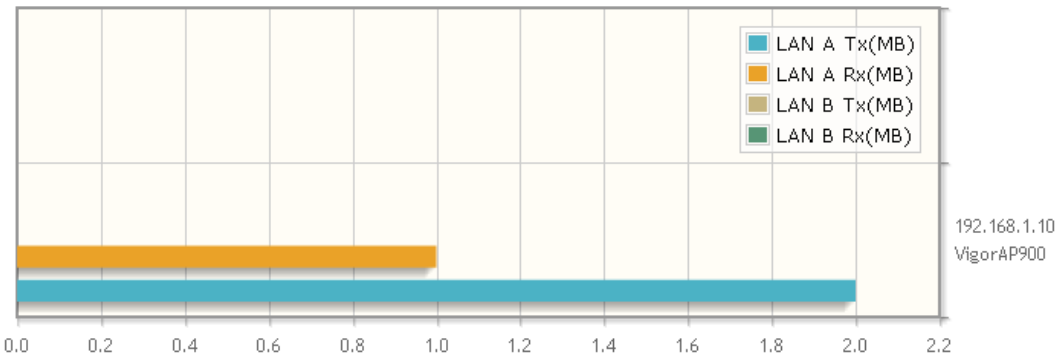
Note:

1. Only browser supporting **HTML5** can display Event Log correctly.
2. The APs Log can be refreshed after at least 30 seconds.

VII-6-9 全部流量(Total Traffic)

本頁將會顯示受到路由器管理的 VigorAP 其接收與傳輸資料的全部流量訊息。

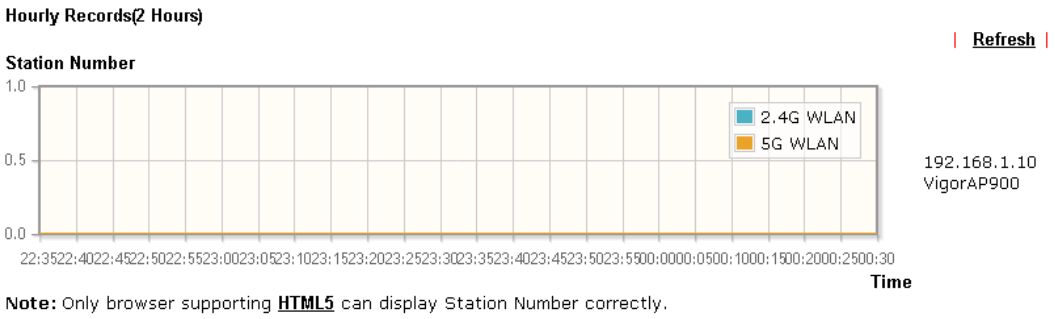
| Refresh |



Note: Only browser supporting **HTML5** can display Total Traffic correctly.

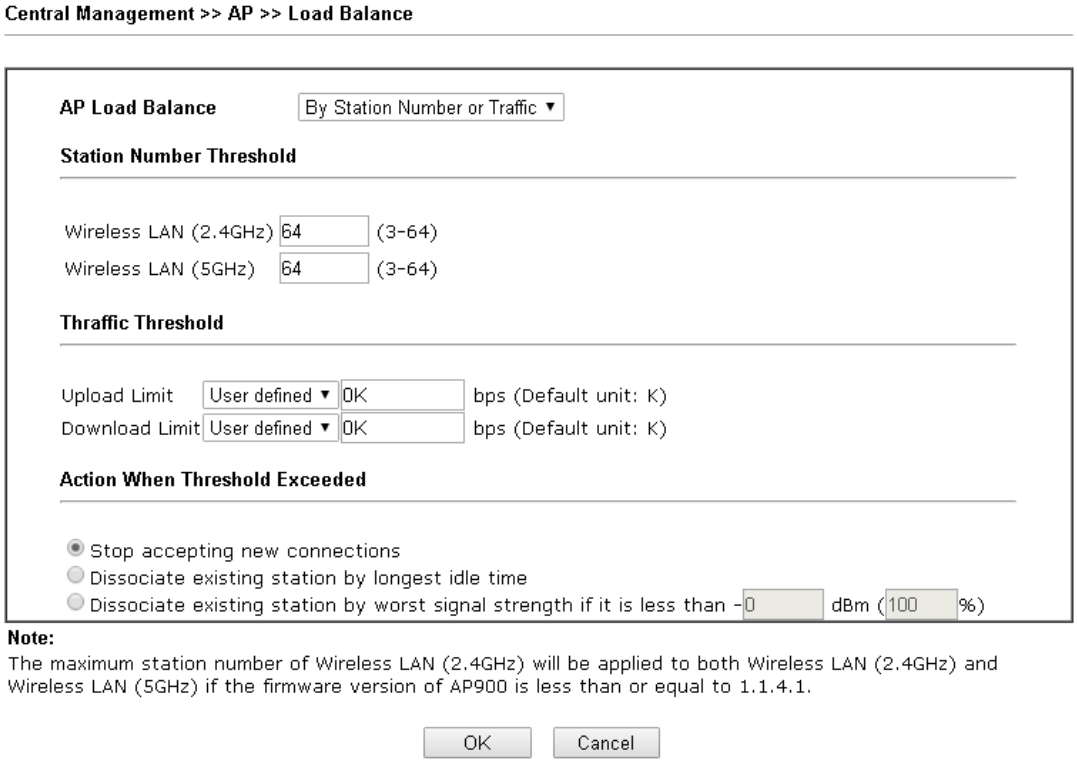
VII-6-10 站台數目(Station Number)

不論該用戶使用的是哪種無線模式登入網際網路，無線用戶站台的全部總額都可以透過此頁面顯示出來。



VII-6-11 負載平衡(Load Balance)

負載平衡的設定參數可以幫忙分配所有註冊至 Vigor 路由器的 AP 基地台的網路流量，這樣頻寬就不會被特定的基地台佔據過久。



可用設定說明如下：

項目	說明
AP 負載平衡(AP Load Balance)	此選項用來決定系統用來偵測過載已啓用負載平衡的模式。 **透過無線用戶數(By Station Number)** – 負載平衡乃依照本頁設定的無線用戶數目爲基準來執行，此項設定可用來限制連接至基地台的無線用戶總數，目的是要避免同時段過多的無線用戶連接

	至AP基地台造成網路塞車不平衡。 **透過流量(By Traffic)** – 依照本頁的流量設定執行負載平衡的運作。 **透過無線用戶數或是流量(By Station Number or Traffic)**–負載平衡的操作依照無線用戶數或是網路流量限制而定。
無線用戶數門檻(Station Number Threshold)	設定無線用戶數目，作爲啓用 AP 負載平衡功能的門檻值。
流量門檻(Traffic Threshold)	**上傳限制** – 使用下拉式清單指定上傳的網路流量限制。 **下載限制** – 使用下拉式清單指定下載的網路流量限制。
當超過門檻時採取的動作(Action When Threshold Exceeded)	**停止接受新的連線(Stop accepting new connections) –** 當無線站台數或是流量達到了設定的門檻值時，路由器將會停止接受任何其他基地台的連線要求。 **分離現有的長期閒置的站台(Dissociate existing station by longest idel time)** - 當 AP 過載時(例如達到無線站台數或是流量的門檻值)，將會中止長期閒置未連線的無線用戶站台。 **分離現有且訊號強度低於此值的站台(Dissociate existing station by worst signal strength if it is less than)** - 當 AP 過載時(例如達到無線站台數或是流量的門檻值)，將會中止訊號強度最弱的無線站台之網路連線。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

VII-6-12 功能支援列表(Function Support List)

Click the **Client** tab to list the AP management functions that the Access Points support under different firmware versions.

Click the **Server** tab to list the AP management functions that Vigor router supports under different firmware versions.

按下**用戶端(Client)**標籤列出 AP 基地台各個不同的韌體下，支援的管理功能有哪些。

按下**伺服器(Server)**標籤列出 Vigor 路由器在不同的韌體下，支援的 AP 管理功能有哪些。

Central AP Management >> Function Support List

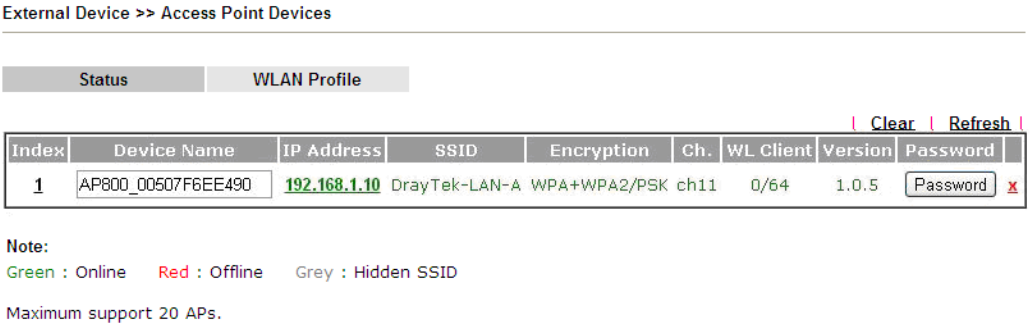
Model Name	AP710	AP800	AP810	AP900	AP902	AP910C
FW Version	**1.2.0**	**1.1.6**	**1.1.6.1**	**1.1.7**	**1.1.7**	**1.1.6**
Register						
DHCP	•	•	•	•	•	•
Static IP	•	•	•	•	•	•
Profile						
2.4GHz	•	•	•	•	•	•
5GHz		• (with N65)		•	•	•
AP Mode	•	•	•	•	•	•
Auto Provision	•	•	•	•	•	•
WLAN Enable/Disable	•	•	•	•	•	•
Limit Client	•		•	•	•	•
Airtime Fairness	•		•	•	•	•

應用說明

A-1 如何使用 AP 管理功能來檢查 AP 狀態並部署 WALN 設定檔?

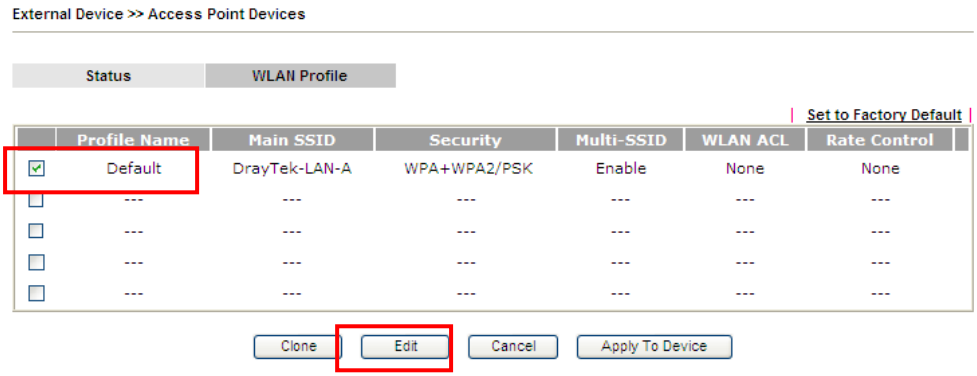
管理者可以管理連接至此路由器的無線基地台。

1. 開啓**外接裝置>>無線基地台裝置(External Devices>>Access Point Devices)**，Vigor2926 可以自動偵測連接至此路由器的無線 AP 並顯示如下：

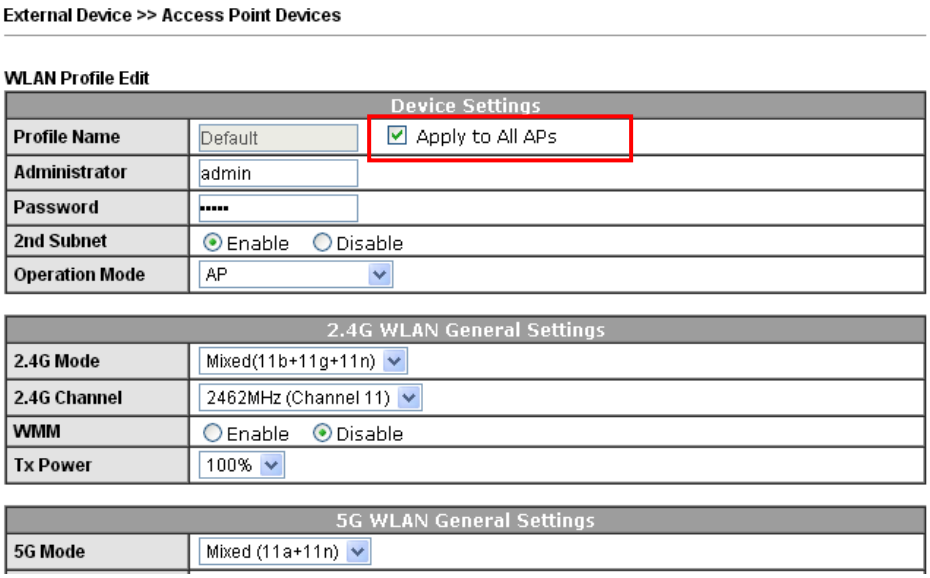


在本例中，路由器偵測到名爲 *AP800_00507F6EE4980* 的裝置。

2. 按下**無線網路設定檔(WLAN Profile)**標籤開啓如下頁面，勾選預設設定檔的核取方塊，**編輯(Edit)**按鈕即可使用。接著按下**編輯(Edit)**按鈕。



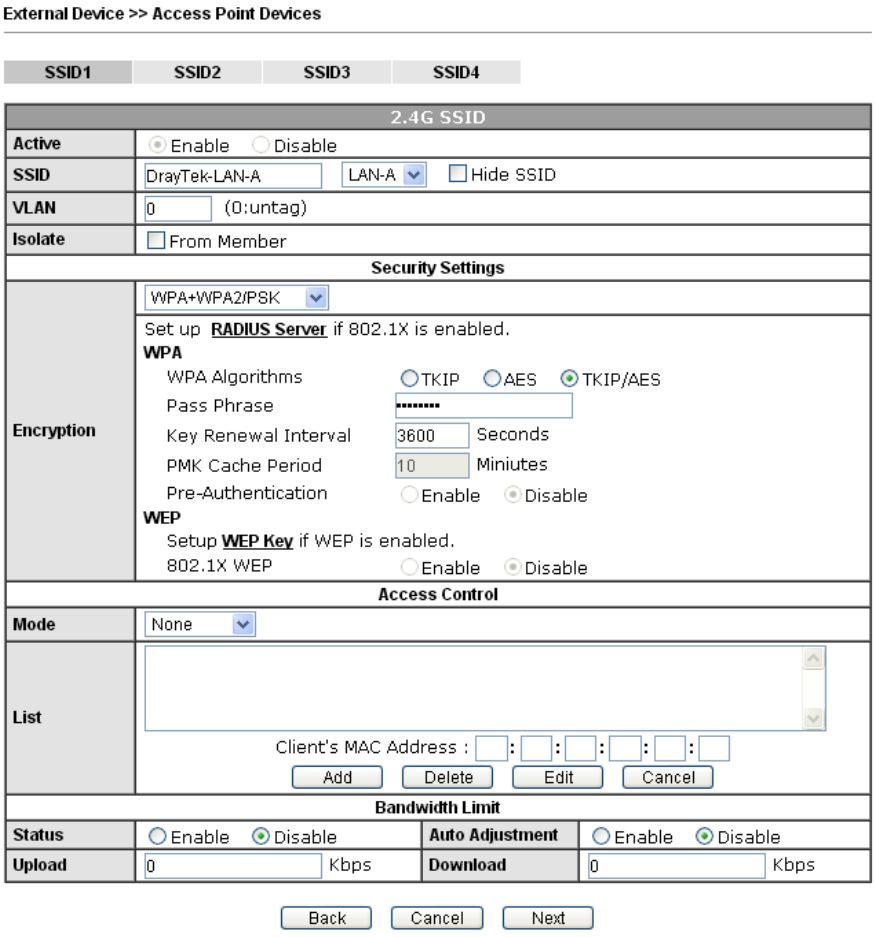
3. 當設定內容出現時，請依照實際需要進行修正，勾選**套用至全部 AP(Apply to All APs)**，再按**下一頁(Next)**。



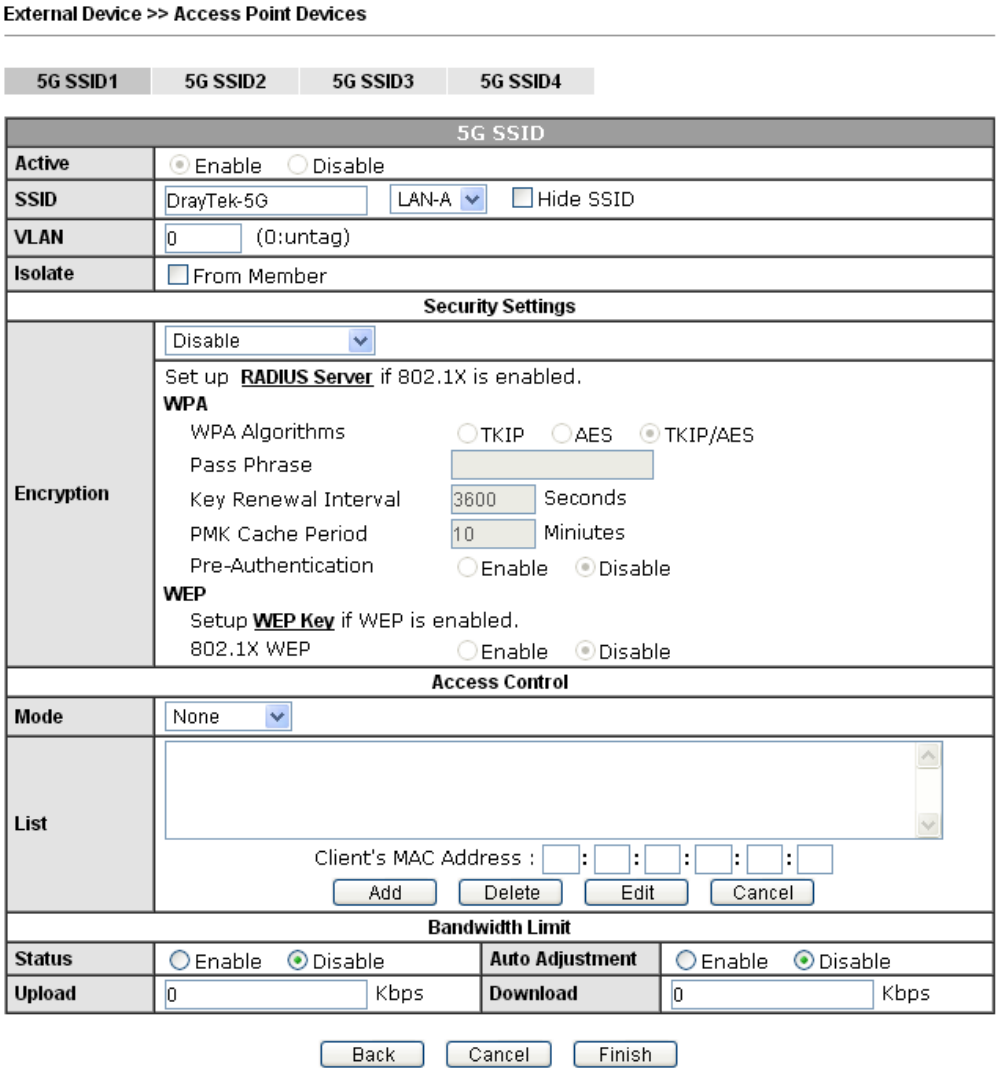
資訊

套用至全部 AP(Apply to All APs) 能自動將預設設定檔內的配置直接套用到在 Vigor 路由器註冊的基地台上，因此您不需要手動分別套用到每一個 AP 上。此功能對於想要在一個展場上，快速部署多個無線 AP 的人們來說相當方便。

4. 接下來的頁面可讓您修改 AP 的 2.4G SSID 相關設定，完成後請按**下一頁(Next)**。



5. 完成上述頁面後，這個頁面則是讓您修改 AP 的 5G SSID 相關設定，如有需要，可在此變更。做完所有的變更之後，按下**完成(Finish)**。



6. 現在，路由器偵測到的 AP (以 *AP800_00507F6EE4980* 表示)將可套用路由器配置好的無線網路設定內容。

VII-7 中央管理(交換器)

Vigor 路由器可以管理與其相連接的 VigorSwitch 裝置，透過設定檔與群組設定，管理人員可進行 VigorSwitch 韌體/設定配置備份、還原、重新啓動裝置或是回復出廠預設值等操作。

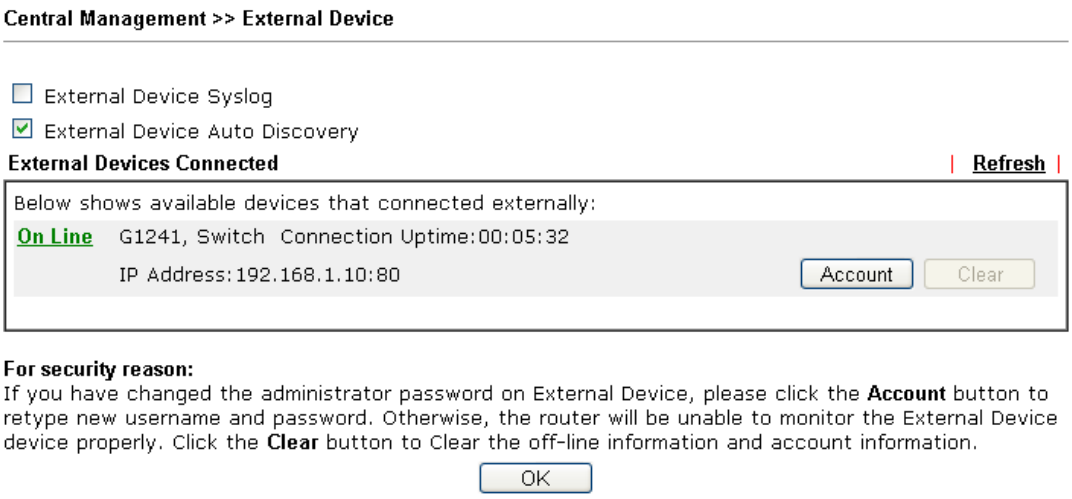


VII-7-1 狀態(Status)

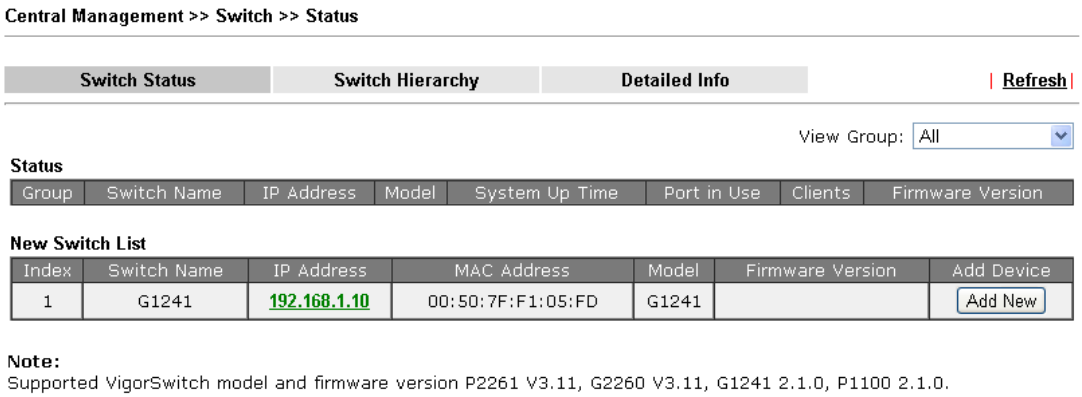
VII-7-1-1 交換器狀態(Switch Status)

此頁面顯示的資訊包含群組、交換器名稱、IP 位址、機型、系統上線時間、使用埠口、用戶端與韌體版本等等。

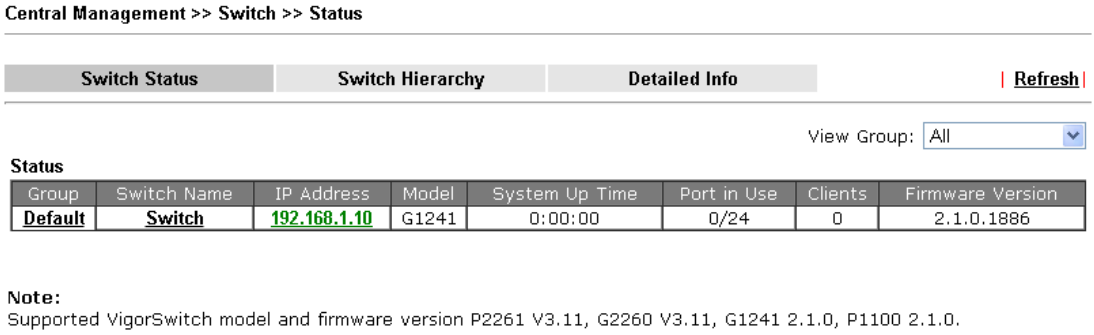
在檢查交換器狀態之前，請前往**中央管理>>外接裝置(Central Management>>External Device)** 啓用外接裝置自動搜尋(**External Device Auto Discovery**)，等待系統顯示可用的裝置。



之後，開啓**中央管理>>交換器>>狀態(Central Management>>Switch>>Status)**，受路由器管理的可用交換器即可列在新交換器清單(New Switch List)。

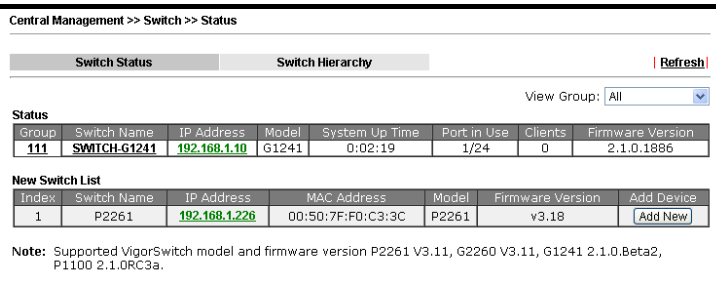


列在狀態下方的 VigorSwitch 表示目前已納入路由器管理的交換器；而列在新交換器清單(New Switch List)下方的 VigorSwitch 表示尚未納入路由器管理的交換器。



可用設定說明如下：

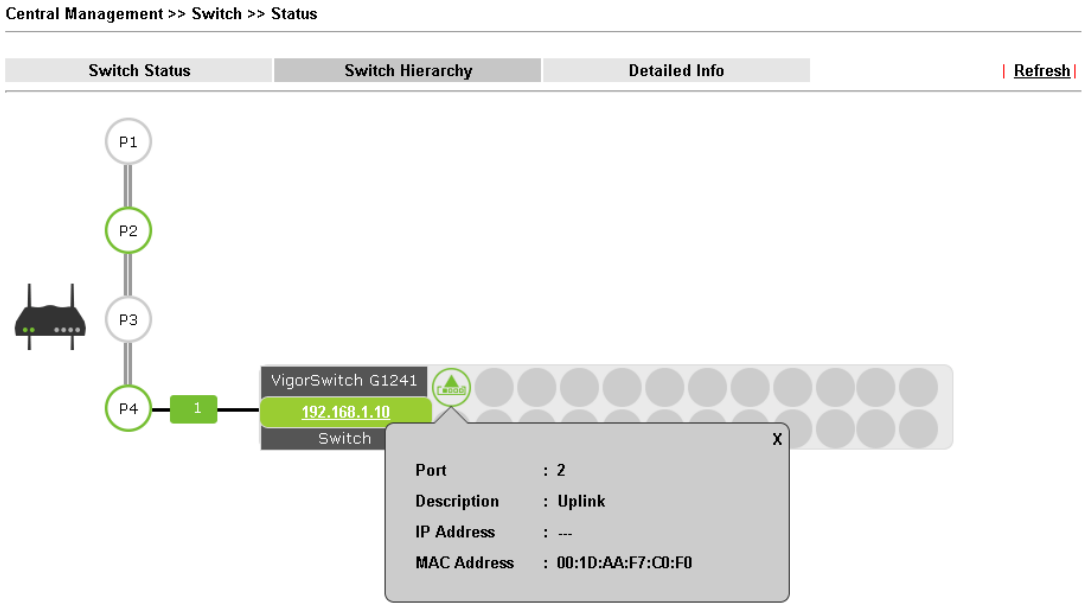
項目	說明
群組(Group)	顯示群組的名稱連結。 您可以點該連結進行群組設定修訂。
交換器名稱(Switch Name)	顯示交換器名稱。 您可以點該連結進行交換器設定檔修訂。
IP 位址(IP Address)	顯示 VigorSwitch 的 IP 位址。
型號(Model)	顯示 VigorSwitch 的型號名稱。
系統連線時間(System Up Time)	顯示 VigorSwitch 開啓電源後累計的時間。
使用埠口(Port in Use)	顯示 VigorSwitch 目前有連接其他裝置的埠口數目。
用戶端(Clients)	顯示與 VigorSwitch 相連的用戶數目。
韌體版本(Firmware Version)	顯示 VigorSwitch 目前使用的韌體版本。
新增(Add New)	此按鈕僅在有一個以上的 VigorSwitch 連接至此路由器時可使用。 在新交換器清單(New Switch List)下方的裝置允許納入目前的群組接受路由器的管理。只要按下**新增(Add New)**按鈕即可。

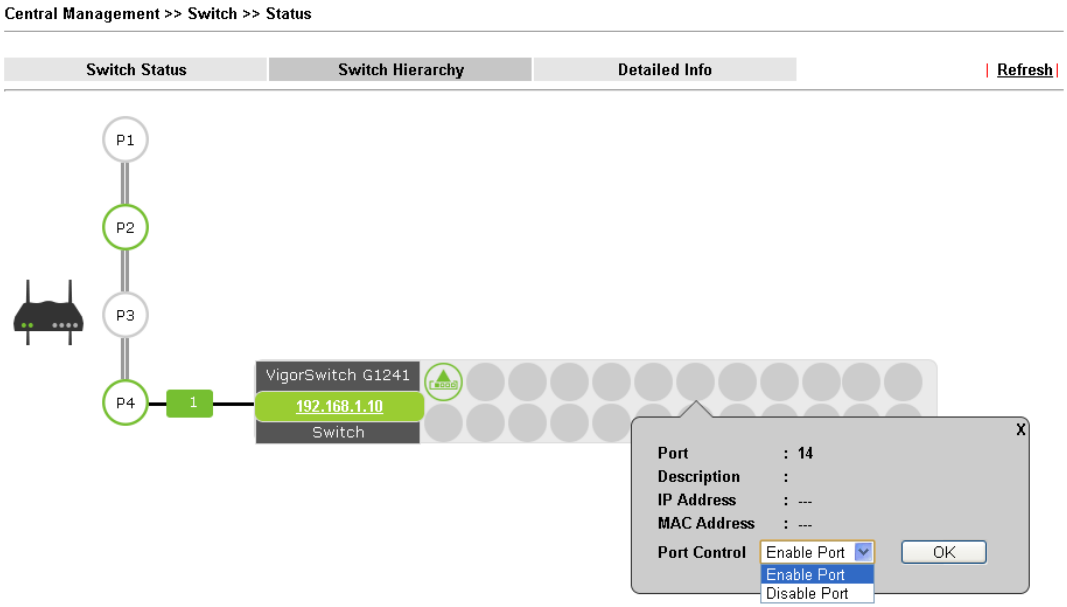


建議相同型號的 VigorSwitch 納入同一個群組管理。

VII-7-1-2 交換器層次結構(Switch Hierarchy)

此頁顯示納入路由器管理的 VigorSwitch 的層次結構。

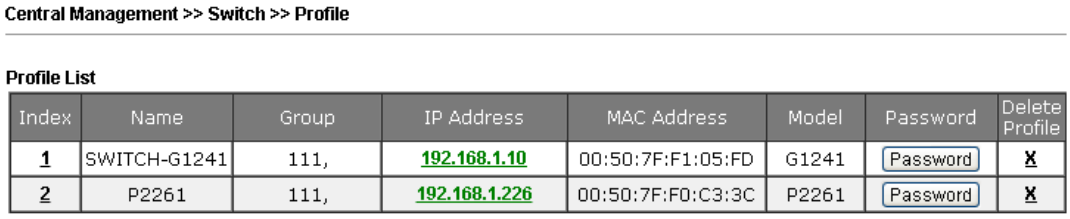




請注意，**停用埠口(Shutdown Port)**在 VigorSwitch 的 LAN 埠口連接一台 LAN 裝置時可用，當您選擇了該埠口時，裝置與 VigorSwitch 之間的網路連線將會在按下**確認(OK)**按鈕後隨即中止。

VII-7-2 設定檔(Profile)

本頁顯示連接至此路由器的 VigorSwitch 的基本資訊，如名稱、群組、IP 位址、MAC 位址、型號與密碼等。點選任一索引編號後，與該 Switch 相關的設定頁面即可開啓。請注意，每個設定檔代表一台 VigorSwitch。

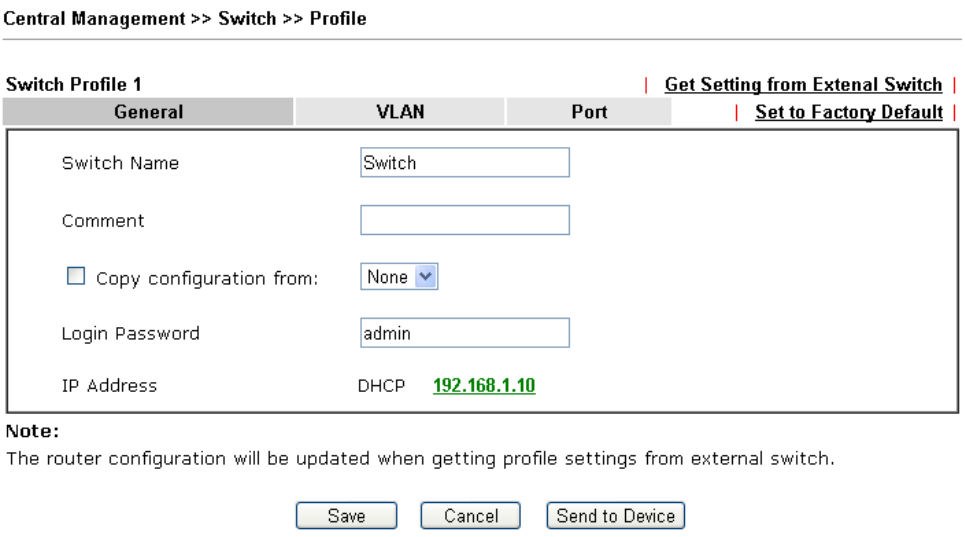


可用設定說明如下：

項目	說明
索引編號(Index)	按下編號連結進入 Switch 設定檔。 請注意，每個相連的 VigorSwitch 皆擁有一個內容配置設定檔，如果有數台 Switch 連接至路由器，系統將以不同的索引編號來代表不同的 VigorSwitch 設定檔。
名稱(Name)	顯示 VigorSwitch 的使用者定義名稱。
群組(Group)	顯示 VigorSwitch 的群組名稱。
IP 位址(IP Address)	顯示 VigorSwitch 的 IP 位址。
MAC 位址(MAC Address)	顯示 VigorSwitch 的 MAC 位址。
型號(Model)	顯示 VigorSwitch 的機種名稱。
密碼(Password)	按此鈕顯示帳號資訊，包含使用者名稱與密碼。
刪除設定檔(Delete Profile)	按“X”符號，刪除該交換器設定檔。

欲編輯選定交換器的設定檔，請依下述步驟進行：

1. 按索引編號連結(例如 #1)開啓如下頁面。

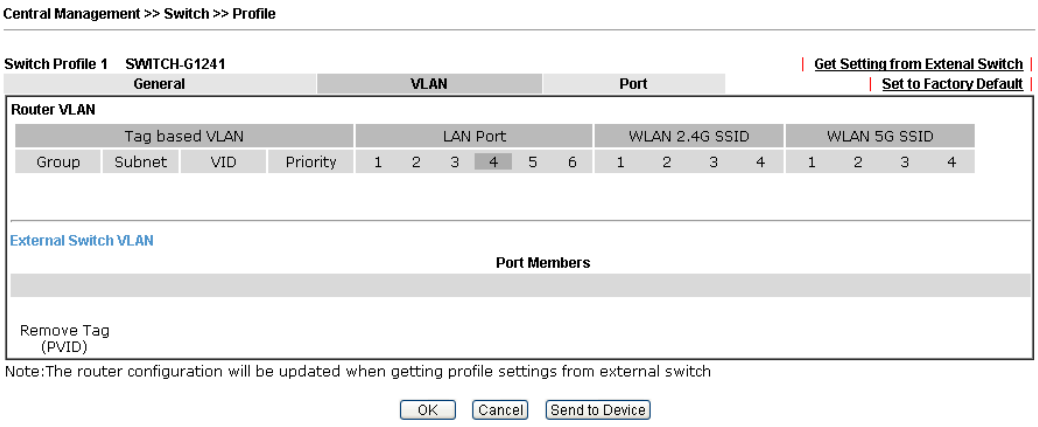


可用設定說明如下：

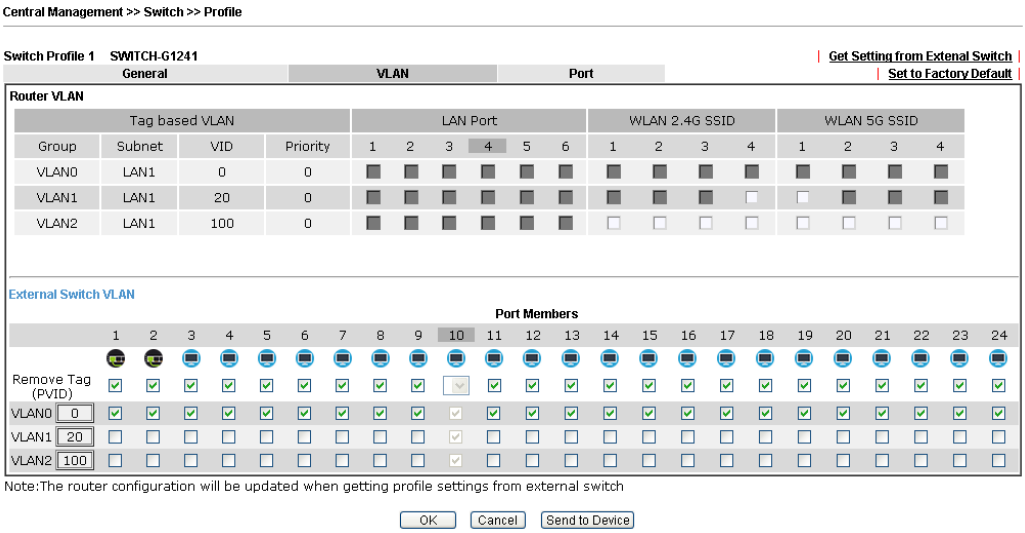
項目	說明
交換器名稱(Switch Name)	輸入交換器的名稱以作爲辨識之用。 當有數台 VigorSwitch(型號相同)連接至路由器時，這個名稱可以輕易的辨識出交換器的身分。
註解(Comment)	若有需要，可以輸入一些文字來說明交換器。
複製設定檔自(Copy configuration from)	勾選此框以複製來自其他裝置的設定，請使用下拉式清單選擇需要的一項。 注意，若僅有一台 VigorSwitch 連結路由器且被路由器納入館哩，此區將無法使用。
登入密碼(Login Password)	顯示 VigorSwitch 的原始登入密碼。 然而，如果群組密碼已經在**中央管理>>交換器>>群組(Central Management >>Switch>>Group)**中以其他字串設定，那麼本區將無法輸入其他的密碼值，僅會顯示群組密碼。
IP 位址(IP Address)	顯示路由器分派給交換器的動態 IP 位址。
儲存(Save)	按此儲存設定。
取消(Cancel)	按此放棄本頁設定並回到前頁。
寄至裝置(Send to Device)	按此立即傳送設定變更(例如登入密碼、交換器名稱等等)至 VigorSwitch 上。

2. 完成上述設定之後，按下 **VLAN** 標籤開啓如下頁面。

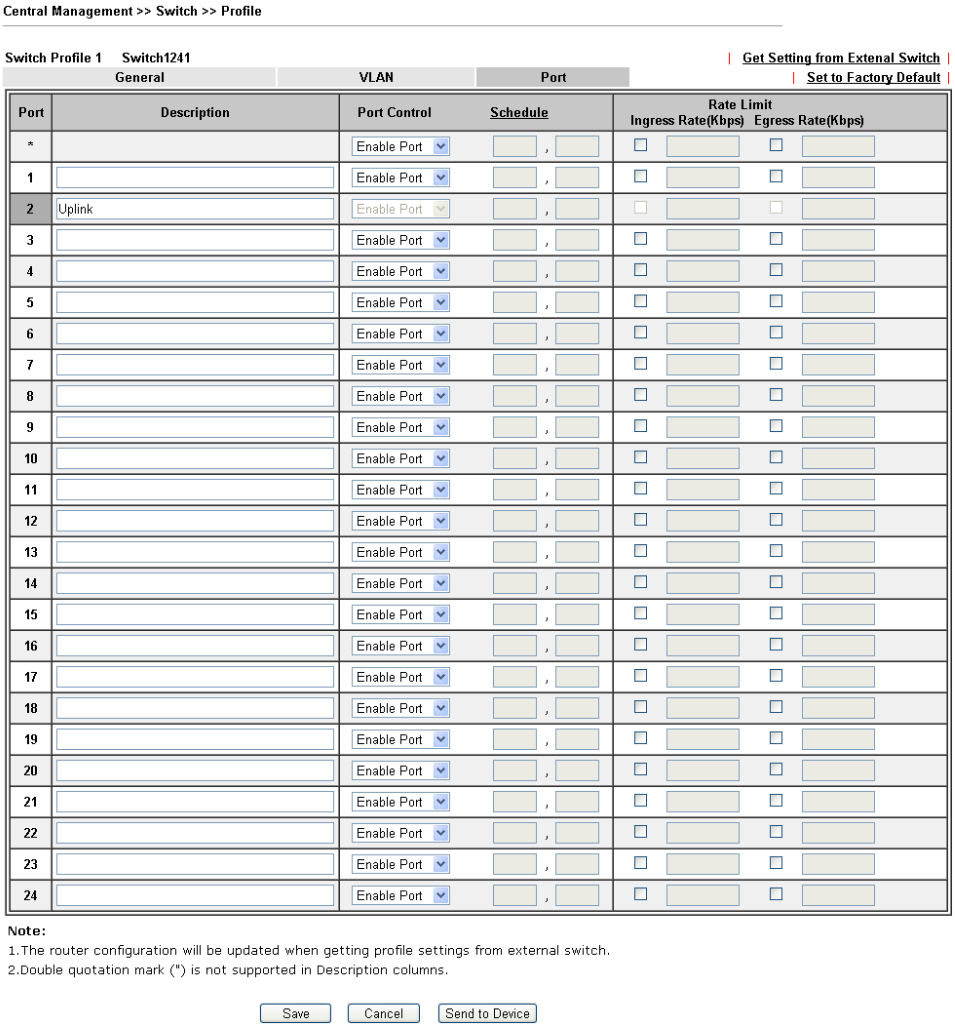
若 LAN>>VLAN 尚未有任何設定，本頁面會呈現空白



若之前已經設定過 LAN>>VLAN ，那麼本頁呈現的內容將如下：



3. 按下**確定(OK)**儲存 VLAN 設定，接著按下**埠口(Port)**標籤開啓如下頁面：

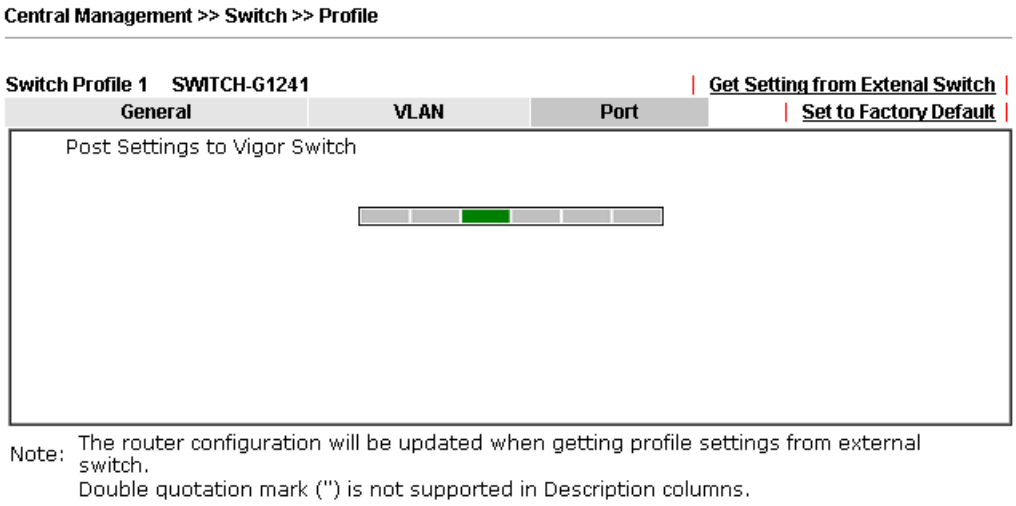


可用設定說明如下：

項目	說明
說明(Description)	如要需要，可以在此輸入簡易的埠口說明。
埠口控制(Port	**停用埠口(Disable Port)** – 用來連接 VigorSwitch 與路由器的埠

Control)	口(例如本例的埠口 2)無法由路由器關閉。 VigorSwitch 其他的 LAN 埠口允許連接任何 LAN 裝置，當選擇了此埠口，在按下**儲存(Save)**按鈕之後，裝置與 VigorSwitch 之間的網路連線將被中斷。 **排程(Schedule)** – 此處可以指定 2 個排程，強迫路由器執行與 VigorSwitch 有關的指定行動。

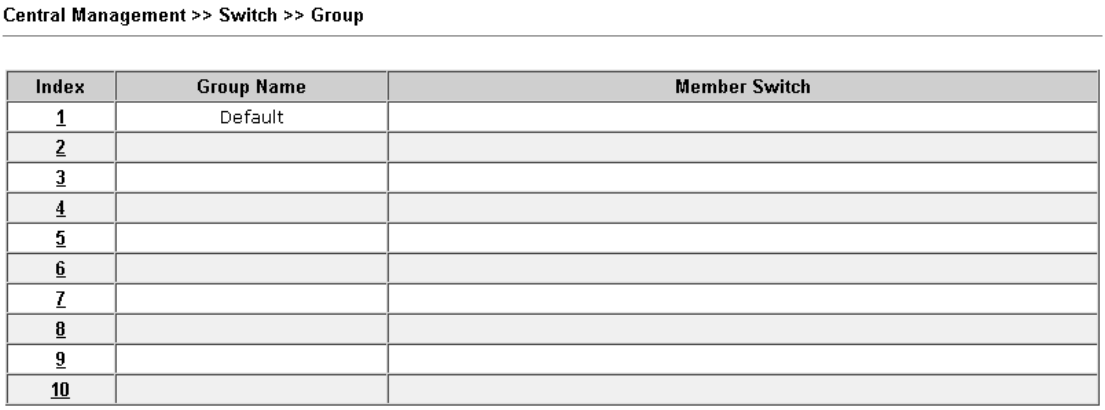
4. 按下確定**(OK)**儲存變更，然後按**寄至裝置(Send to Device)**，相關設定將會立即傳送到 VigorSwitch 上。



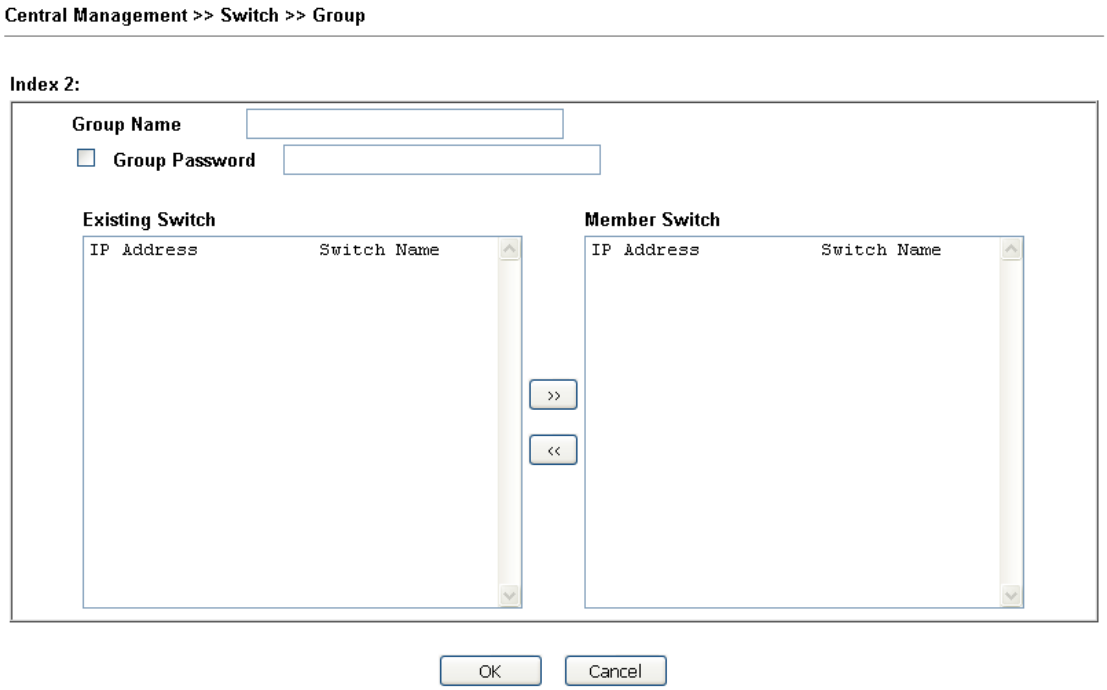
VII-7-3 群組(Group)

不同的交換器可以分成不同的組別，每個組別可以指定一個密碼，並套用到組別內所有的交換器中。

透過共用的密碼設定，系統管理者無須爲了登入 VigorSwitch 裝置，強硬記憶各式各樣的登入密碼。



按下索引號碼連結開啓如下頁面建立新的交換器群組。

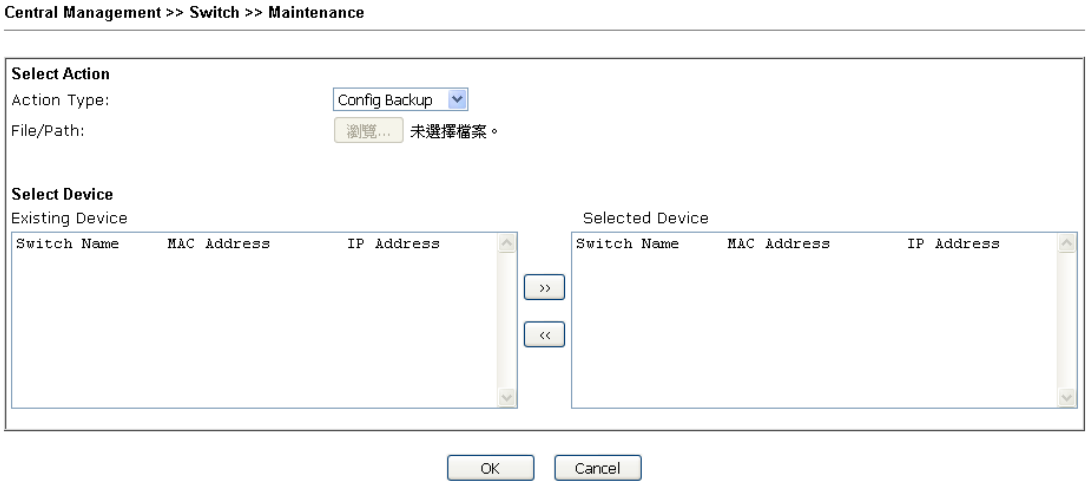


可用設定說明如下：

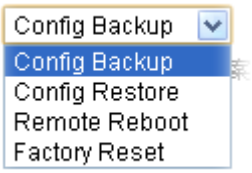
項目	說明
群組名稱(Group Name)	輸入群組的名稱，不同的交換器可以納入一個群組中。
群組密碼(Group Password)	輸入系統管理員可以用來登入連接至路由器的交換器群組密碼，所有群組下方管理的交換器都可以透過此密碼登入網頁設定介面。
現有交換器(Existing Switch)	顯示連接至此路由器的所有 VigorSwitch。
會員交換器(Member Switch)	選擇您想要群組的交換器，按下“>>”鈕移動選定的裝置至會員交換器一區，在會員交換器下方的裝置即可群組在此設定檔下。
確定(OK)	按此儲存設定。
取消(Cancel)	按此放棄本頁設定並回到前頁。

VII-7-4 維護(Maintenance)

此頁面用以執行設定備份、還原選定 VigorSwitch 裝置、遠端重新啓動 VigorSwitch 裝置，或是以出廠預設值重新啓動 VigorSwitch，無須個別登入 VigorSwitch 的網頁使用者介面。



可用設定說明如下：

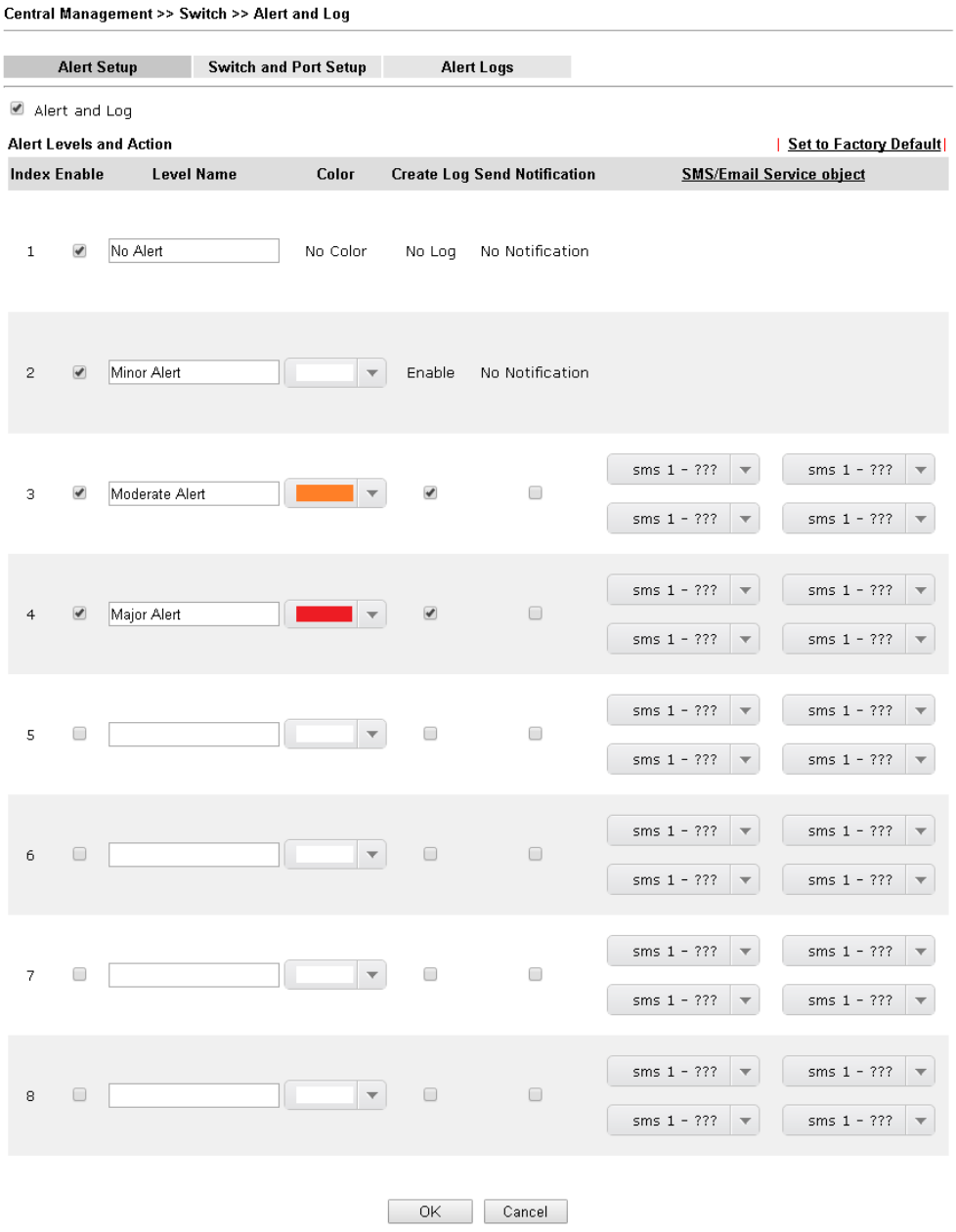
項目	說明
選擇動作(Selection Action)	**動作類型(Action Type)** – 路由器可以對 VigorSwitch 採取四種動作包含設定備份、設定還原、遠端重新啓動、出廠預設值等。  **檔案/路徑(File/Path)** – 按此鈕找尋需要的檔案。
選擇裝置(Select Device)	**現有裝置(Existing Device) –** 顯示連接至此路由器的 VigorSwitch 裝置。 **選定裝置(Selected Device) -**選擇您想要群組的交換器，按下“>>”鈕移動現有裝置至選定裝置一區，在選定裝置下方的裝置即可套用此動作。
確定(OK)	按此立即在選定裝置區執行選定的動作
取消(Cancel)	按此取消設定變更。

VII-7-5 警示與日誌(Alert and Log)

警示與日誌可幫助使用者快速了解發生在 VigorSwitch 的異常狀況，當系統偵測出錯誤時，異常狀況的資訊將會記錄在資料庫中，或是系統會傳送警示給予指定的裝置(透過電子郵件或是簡訊)以警告使用者。

VII-7-5-1 警示設定(Alert Setup)

本頁用於定義警示名稱、警示等級(以顏色表明)以及依照指定的等級來決定記錄資料於資料庫中，或是傳送通知訊息給予使用者。



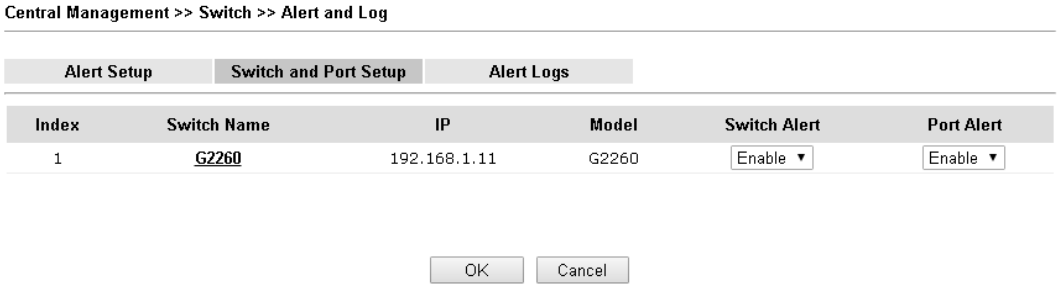
可用設定說明如下：

項目	說明
警示與日誌(Alert and Log)	勾選此框啓用此功能。

警示等級與動作(Alert Levels and Action)	**等級名稱(Level Name) –** 定義代表警示事件嚴重性等級名稱。索引編號 1 到 4 的預設名稱會顯示在每個設定方塊中，索引編號 5 到 8 則保留給使用者定義。 **顏色(Color)** – 定義每個警示的層級顏色，但是索引編號 1 的顏色固定爲無色，無法更改。 **建立日誌(Create Log)** – 勾選此框以建立警示日誌，此日誌可在警示日誌頁面中檢視，請注意索引編號 1 的預設值爲無日誌，索引編號 2 的日誌預設值是啓用的。 **傳送通知(Send Notification)** – 若勾選此項，路由器系統將會透過簡訊發送通知給予指定的用戶。 **簡訊/電子郵件服務物件(SMS/Email Service Object) –** 選擇簡訊物件，最多一次可以選擇 4 個物件。

VII-7-5-2 交換器與埠口設定(Switch and Port Setup)

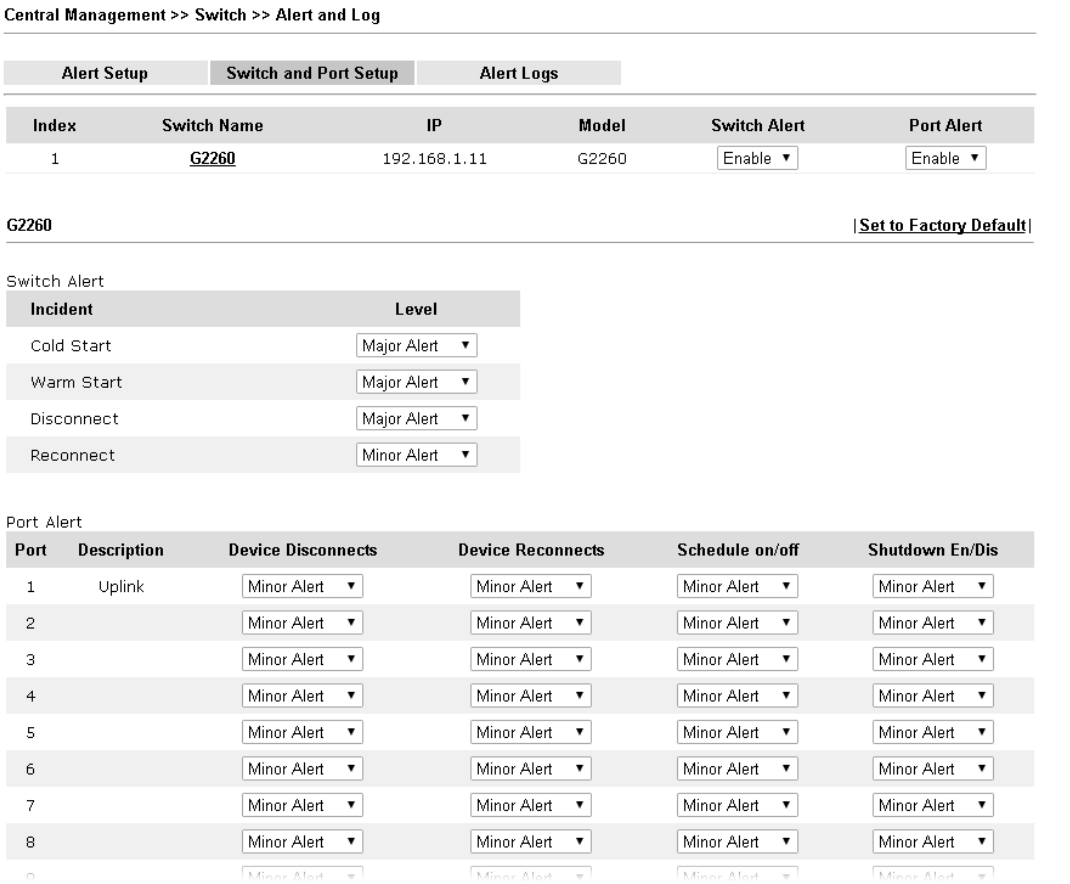
本頁可用於定義啓用交換器警示與/或埠口警示。



可用設定說明如下：

項目	說明
交換器警示(Switch Alert)	**啓用(Enable) –** 選擇此項以啓用 VigorSwitch 警示機制。
埠口警示(Port Alert)	**啓用(Enable) -** 選擇此項以啓用 VigorSwitch 埠口之警示機制。

按下交換器名稱連結(例如本例的 G2260) 以進入細節設定。

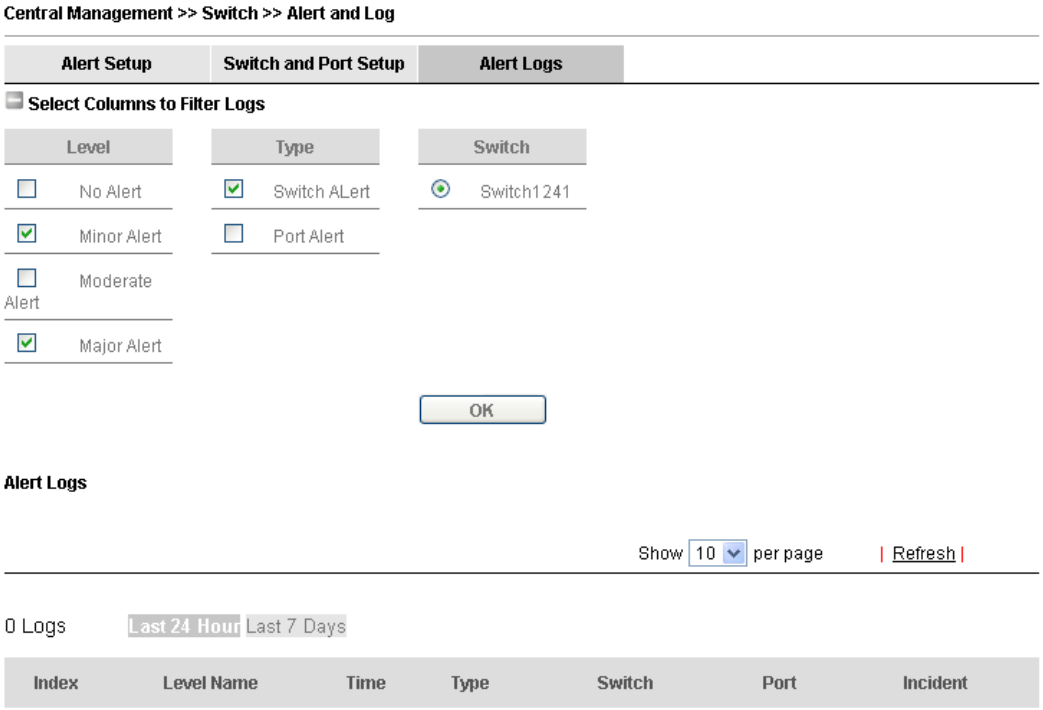


可用設定說明如下：

項目	說明
交換器警示(Switch Alert)	當 VigorSwitch 遇到如下的警示事件時，警示機制將會基於所遭遇的事件嚴重性等級執行相應的動作。 **事件(Incident) -** 目前，**冷啓動(Cold Start)，暖啓動(Warm Start)，中斷與重新連線(Disconnect and Reconnect)** 皆視爲警示事件。 **等級(Level) -** 指定每個事件的嚴重性等級。如需要定義更多的嚴重性等級以供選擇，可開啓**中央管理>>交換器>>警示與日誌(Central Management>>Switch>>Alert and Log)**並按下**警示設定(Alert Setup)**。
埠口警示(Port Alert)	**埠口(Port) -** 選定 VigorSwitch(例如本例的 G2260)可用的乙太網路埠口可顯示在本頁面上，每個埠口皆可設定不同的警示等即以因應不同的事件。

VII-7-5-3 警示日誌(Alert Logs)

使用者可以基於本頁所選定的條件，過濾蒐集的資訊取得需要的內容。

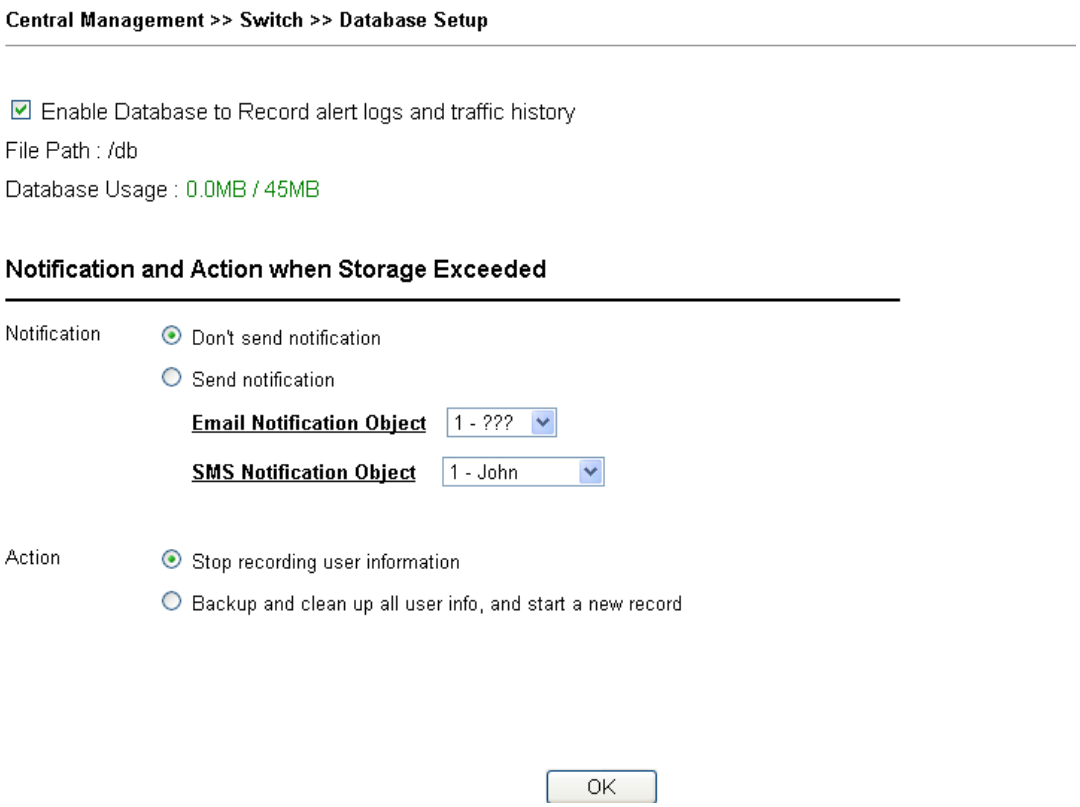


可用設定說明如下：

項目	說明
選擇過濾日誌的欄位(Select Columns to Filter Logs)	**等級(Level) -** 警示可以區分爲數種等級- 沒有警示(No Alert)、次要警示(Minor Alert)、中等警示(Moderate Alert)與主要警示(Major Alert)。請勾選需要的等級。 **類型(Type) -** 勾選日誌的類型(交換器/埠口)以便顯示在警示日誌清單中。 **交換器(Switch) -**本區會顯示與路由器相連的交換器，請選擇需要的裝置。 **確定(OK) -** 按此儲存設定。 與選定項目相關的日誌內容將會顯示在警示日誌清單中。
警示日誌(Alert Logs)	本區顯示路由器管理的 VigorSwitch 相關的日誌(包含等級名稱、時間、類型、交換器、埠口與事件等)。

VII-7-6 資料庫設定(Database Setup)

交換器資料庫可以用來記錄警示日誌以及流量歷程，本頁是用來決定是否要在資料庫中紀錄使用者資訊。



可用設定說明如下：

項目	說明
啓用資料庫記錄警示日治與流量歷程(Enable Database to Record alert logs and traffic history)	勾選此框讓資料庫記錄警示日治與流量歷程於 USB 中。
當儲存超過時須採取的通知與動作	
通知(Notification)	**不寄送通知(Don't send notification)** – 當 USB 磁碟已無空間可以儲存時，系統不會寄發通知出去。 **寄送通知(Send notification)** – 當 USB 磁碟已無空間可以儲存時，系統將會寄發通知出去。
動作(Action)	**停止紀錄使用者資訊(Stop recording user information)** –當容量已滿，系統將停止紀錄。 **備份並清除全部使用者資訊，開始新的紀錄(Backup and clean up all user infor, and start a new record)** - 只有最新的事件會記錄在資料庫中。

完成上述設定之後，請按下**確定(OK)**按鈕儲存設定。

VII-7-7 支援清單(Support List)

本頁列出路由器透過**中央管理>>交換器(Central Management>>Switch)**管理的 VigorSwitch 的機種名稱與韌體版本。

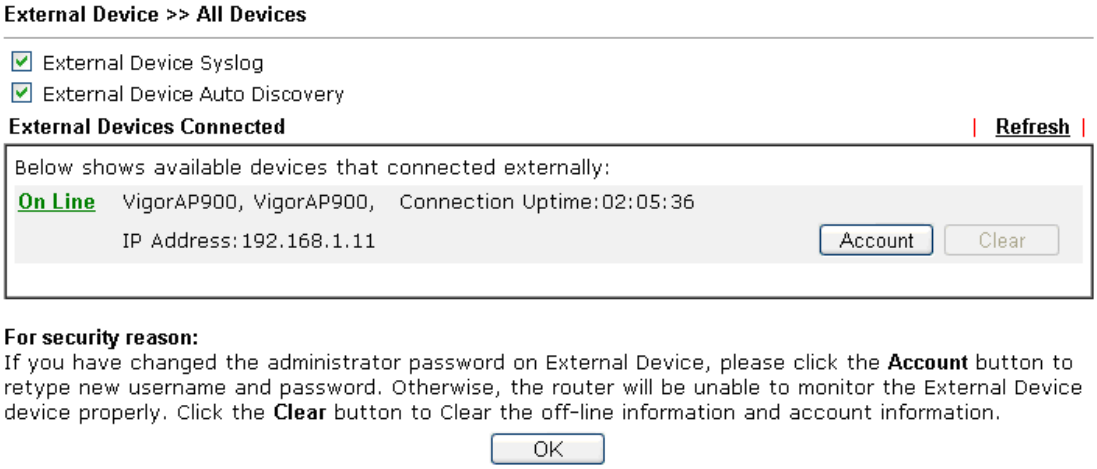
Central Management >> Switch >> Support List

Model	Status	Firmware Version
Vigor Switch P2261	V	v3.11
Vigor Switch G2260	V	v3.11
Vigor Switch P1280	V	v2.0.0

VII-8 中央管理(外接裝置)(Central Management (External Devices))

Vigor 路由器可以用來連結不同類型的外接裝置，爲了方便管理這些外接裝置，請開啓**外接裝置 (External Devices)**以便進行細部設定。

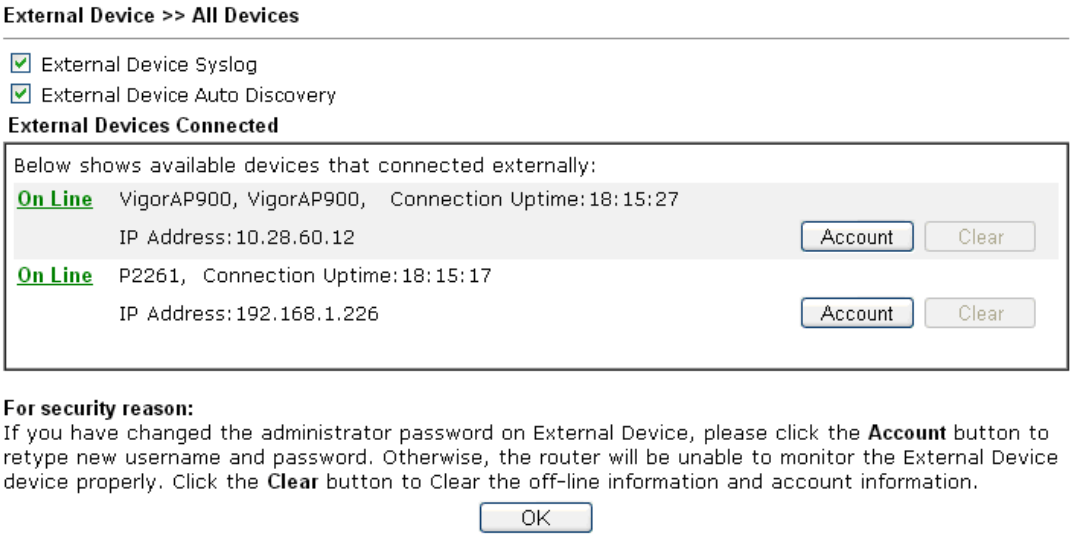
VII-8-1 全部裝置(ll Devices)



可用設定說明如下：

項目	說明
外接裝置 Syslog (External Device Syslog)	勾選此方塊以便在 Syslog 上顯示被偵測裝置的相關資訊。
自動外接裝置搜尋 (External Device Auto Discovery)	勾選此方塊可以讓系統自動偵測外接裝置並顯示在本頁面上。

從這個網頁當中，勾選外接裝置自動搜尋方塊，稍後，所有可用的裝置都將會呈現在螢幕上，並以小圖示顯示。若有需要，您可以更改處在斷線狀態下的裝置名稱。



完成上述設定之後，按**確定(OK)**儲存設定。

資訊	路由器透過此功能所偵測出來的裝置僅包含居易的產品。

第八篇 其他設定



Objects Settings

定義物件如 IP 位址、服務類型、關鍵字、檔案副檔名及其他等等，這些事先預定的物件可以套用在 CSM 中。



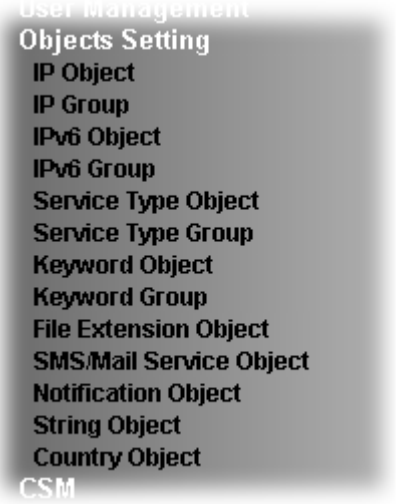
USB

連接至路由器的 USB 裝置可以視之爲伺服器或是 WAN 介面，藉由路由器，LAN 端的用戶可以存取、寫入以及讀取儲存在 USB 磁碟內的資料。

VIII-1 物件設定(Objects Settings)

定義物件如 IP 位址、服務類型、關鍵字、檔案副檔名及其他等等，這些事先預定的物件可以套用在 CSM 中。

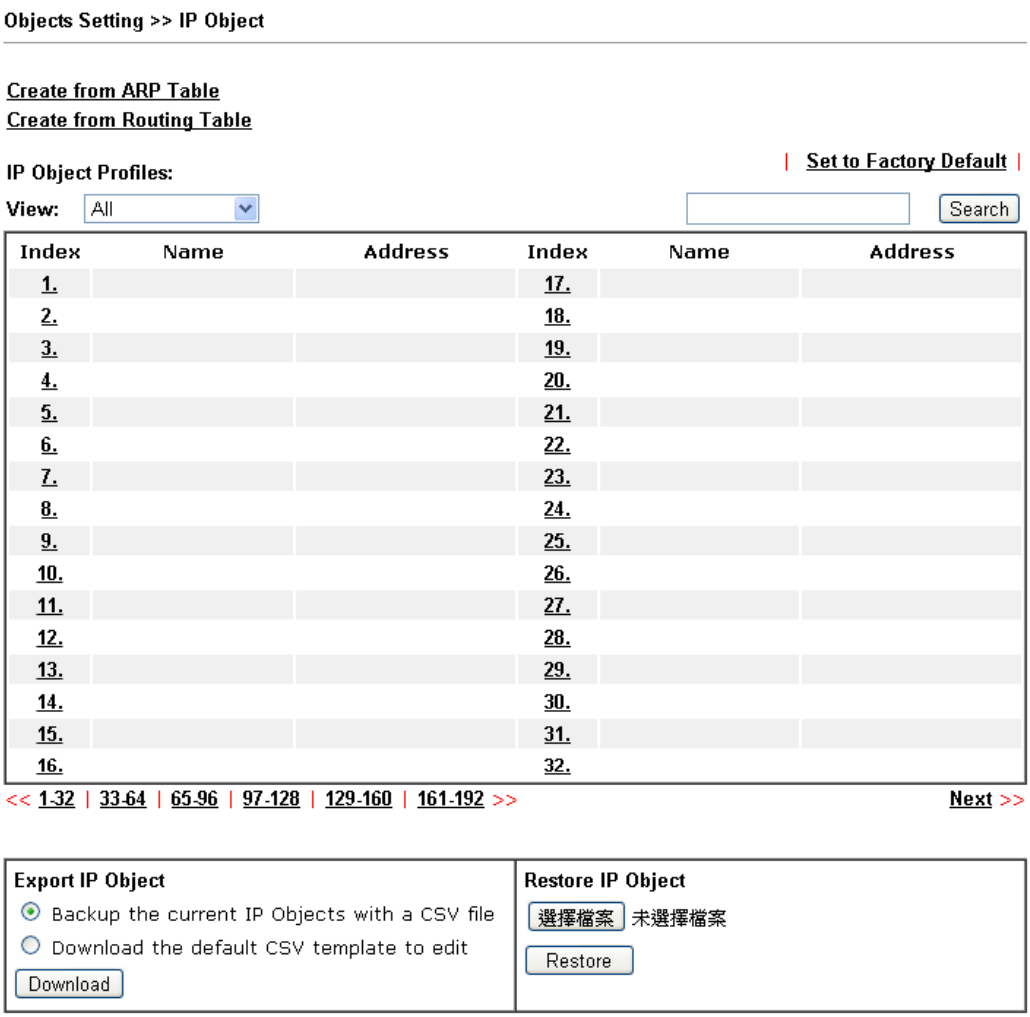
網頁使用者介面



VIII-1-1 IP 物件設定檔(IP Object)

對某些範圍內的 IP 和侷限於特定區域的服務通訊埠，通常可以套用於路由器網頁設定中。因此我們可以將他們定義成爲物件，並結合成群組以便後續能方便的應用。之後，我們可以選擇該物件/群組來套用，比方說，相同部門內所有的 IP 可定義成爲一個 IP 物件(意即 IP 位址範圍)。

您可設定 192 組不同條件的 IP 物件。



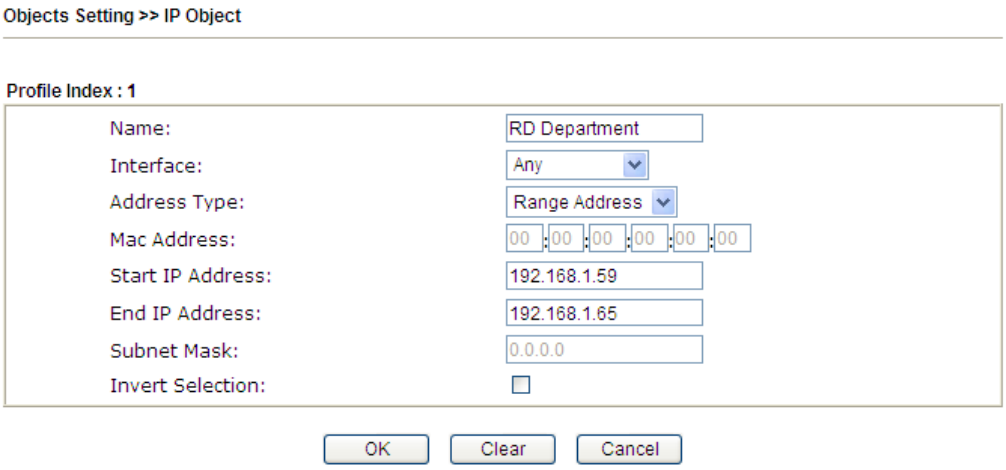
可用設定說明如下：

項目	說明
檢視(View)	使用下拉式清單選擇類型(單一位址、範圍位址、子網位址、MAC 位址或是全部)。與該類型相關的 IP 物件將顯示在頁面上。
回復出廠預設值 (回復出廠預設值(Set to Factory Default))	清除全部的設定資料。
搜尋(Search)	輸入您想要搜尋之 IP 物件的代表字串。
索引(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。
位址(Address)	顯示物件設定檔中設定的 IP 位址。
輸出 IP 物件 (Export IP Object)	一般來說，IP 物件可以透過**物件>>IP 物件(Objects>>IP Object)**網頁來一個一個建立，不過有些使用者想要節省時間並創建大量 IP 物件，因此路由器提供一個快速方式來進行，也就是以單一檔案 CSV 來修改 IP 物件。 所有的 IP 物件皆可透過按壓下載而輸出成檔案形式，使用者即可利用微軟 Excel 開啓此 CSV 檔案同時修改所有的 IP 物件。

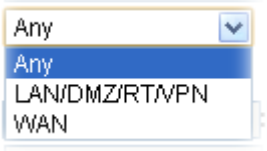
	以 CSV 檔案備份目前的 IP 物件(Backup the current IP Objects with a CSV file) – 按此備份目前的 IP 物件，此 CSV 檔案可以存留以供未來使用。 **下載預設 CSV 模板進行編輯(Download the default CSV template to edit)** – 選擇此項目，按下載儲存預設 CSM 模板(只有表格但無輸入資料)至硬碟上。 **下載(Download)** – 從路由器下載 CSV 檔案並將檔案儲存在硬碟上。
還原 IP 物件(Restore IP Object)	**選擇(Select) -** 按此指定事先預定的 CSV 檔案。 **還原(Restore) -** 將選定的 CSV 檔案輸入至路由器。

如欲建立新的設定檔，請依下述步驟進行：

1. 在索引編號欄位中選擇一個號碼(例如 #1)以便設定細節內容。
2. 設定頁面顯示如下：

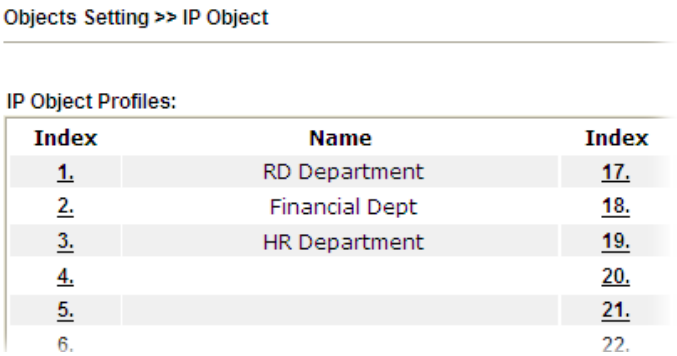


可用設定說明如下：

項目	說明
名稱(Name)	請輸入本設定檔的名稱，最多可以輸入 15 個字元。
介面 (Interface)	請選擇適當的介面。  例如，**編輯過濾器規則(Edit Filter Rule)**中的**方向(Direction)**設定會要求您針對 WAN 或 LAN/DMZ/RT/VPN 介面或是任何 IP 位址，指定一個 IP 或是 IP 範圍，或是任何的 IP 位址，如果您選擇 LAN/DMZ/RT/VPN 作爲介面，並選擇 LAN/DMZ/RT/VPN 作爲**編輯過濾器規則**中的**方向**設定，那麼所有的 LAN/DMZ/RT/VPN 介面的 IP 位址通通都會開放予您在**編輯過濾器規則**頁面上選擇。
位址類型 (Address Type)	決定 IP 位址的位址類型。 如果物件僅包含 IP 位址的話，請選擇**單一位址(Single Address)**。 如果物件包含某個範圍內數個 IP 位址的話，請選擇**範圍位址**

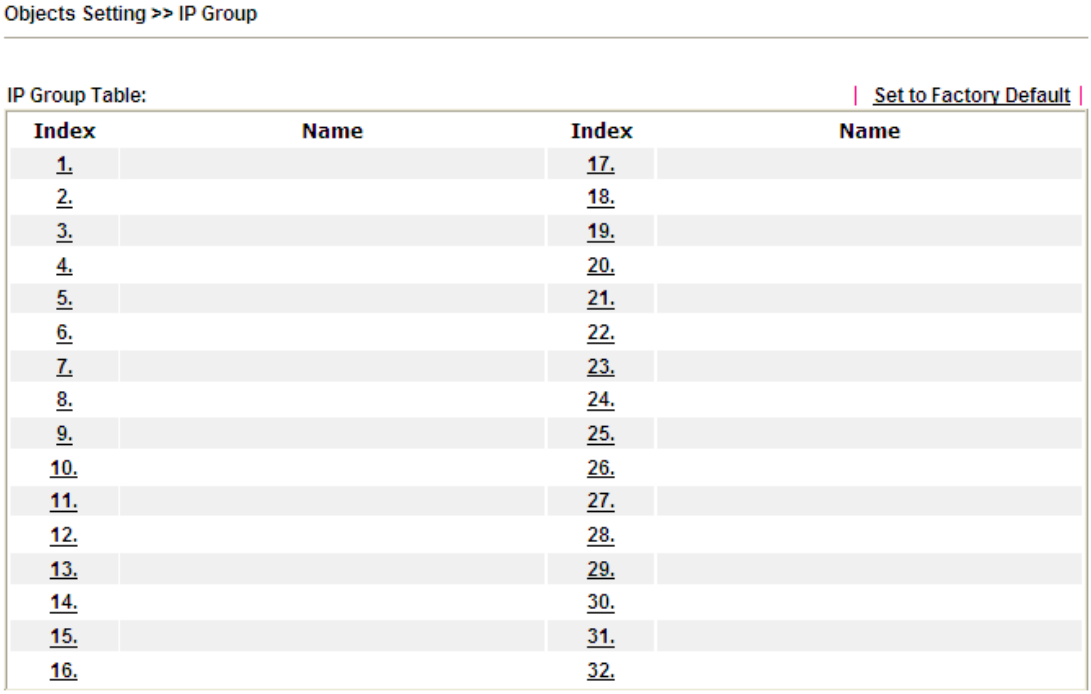
	(Range Address)。 如果物件包含 IP 位址的子網路的話，請選擇**子網路位址(Subnet Address)**。 如果物件包含任何一種 IP 位址的話請選擇**任何位址(Any Address)**。 如果物件包含任何一種 MAC 位址的話請選擇 **MAC 位址(Mac Address)**。
MAC 位址 **(MAC Address)**	如果選擇的是 **MAC 位址**類型，請輸入網卡的 MAC 位址。
起始 IP 位址 **(Start IP Address)**	輸入單一位址類型所需的起始 IP 位址。
結束 IP 位址 **(End IP Address)**	如果選擇的是範圍位址類型，請輸入結束 IP 位址。
子網路遮罩 **(Subnet Mask)**	如果選擇的是子網路位址**(**Subnet Address**)**類型，請輸入子網路遮罩位址。
反向選擇 **(Invert Selection)**	如果勾選此項的話，除了上面所提及的以外，其他的 IP 位址將會在被選擇之後全部套用上設定內容。

4. 完成設定之後，按下確定(OK)按鈕儲存相關設定。下表爲 IP 物件設定的範例之一。



VIII-1-2 IP 群組(IP Group)

本頁可讓您綁定數個 IP 物件成爲一個 IP 群組。



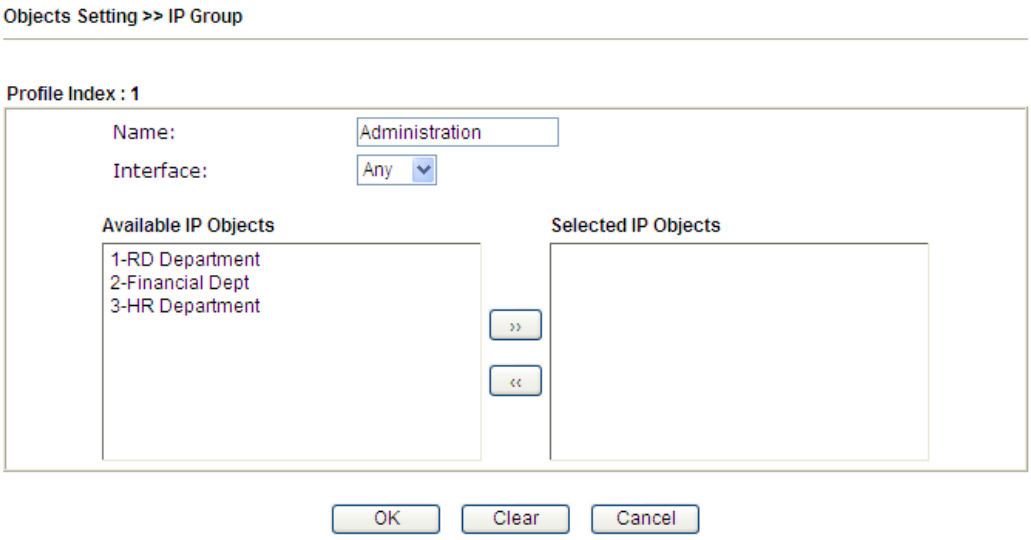
可用設定說明如下：

項目	說明
回復出廠預設值(Set to Factory Default)	清除全部的設定資料。
索引(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 在索引編號欄位中選擇一個號碼(例如 #1)以便設定細節內容。

2. 設定頁面顯示如下：



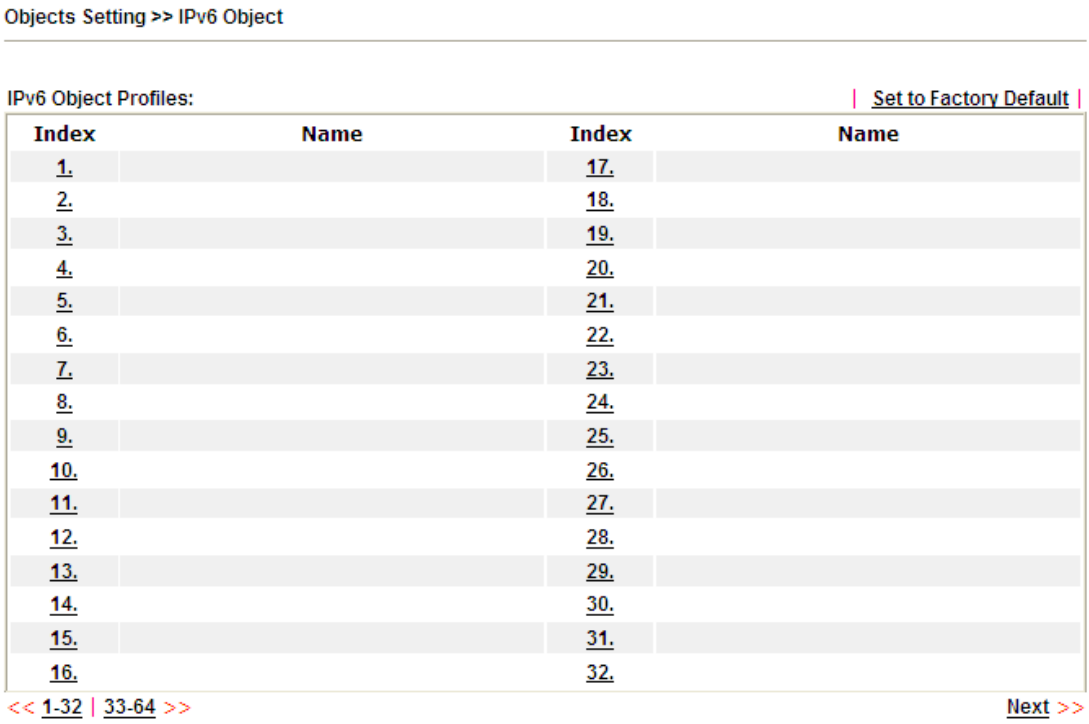
可用設定說明如下：

項目	說明
名稱(Name)	請輸入本設定檔的名稱，最多可以輸入 15 個字元。
介面 (Interface)	請選擇適當的介面(WAN, LAN 或是任何一種)以顯示所有指定介面內的 IP 物件。
可用之 IP 物件 (Available IP Objects)	所有選定之指定介面中可用的 IP 物件全都會顯示在此方塊中。
選定 IP 物件 (Selected IP Objects)	按下 **>>** 按鈕來新增選定 IP 物件並呈現在此方塊內。

3. 完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

VIII-1-3 IPv6 物件(IPv6 Object)

您可設定 64 組不同條件的 IPv6 物件。

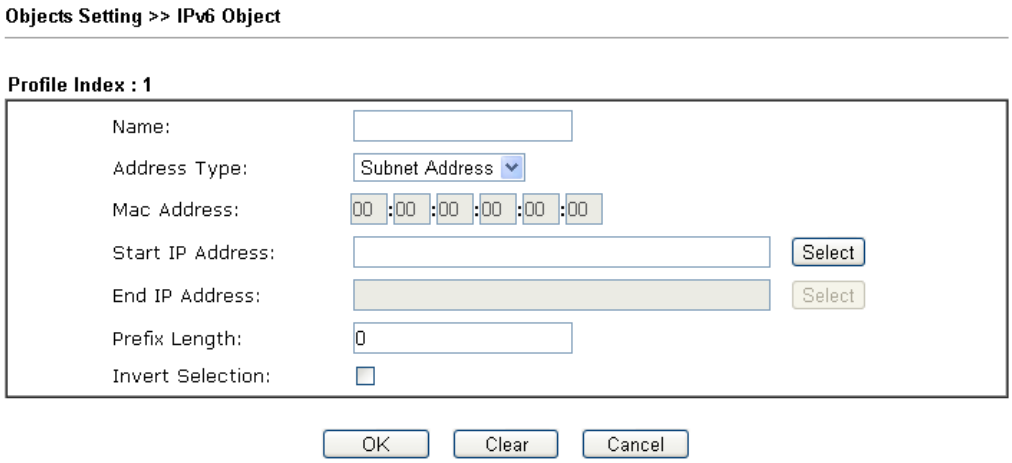


可用設定說明如下：

項目	說明
回復出廠預設值(Set to Factory Default)	清除全部的設定資料。
索引(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 在索引編號欄位中選擇一個號碼(例如 #1)以便設定細節內容。
2. 設定頁面顯示如下：



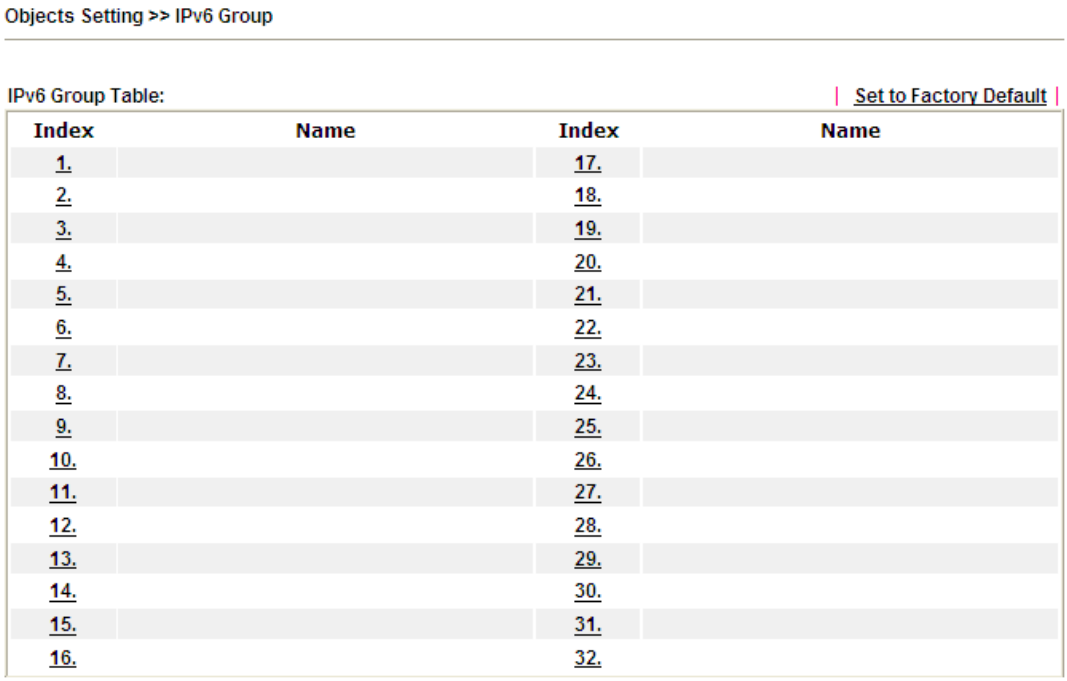
可用設定說明如下：

項目	說明
名稱(Name)	輸入設定檔名稱。
	決定 IPv6 的位址類型。 如果此物件僅含一組 IPv6 位址，請選擇**單一位址(Single Address)**。 如果此物件包含數個 IPv6 位址，請選擇**範圍位址(Range Address)**。 如果此物件包含一個 IPv6 子網路位址，請選擇**子網路位址(Subnet Address)**。 如果此物件包含任何一個 IPv6 位址，，請選擇**任一位址(Any Address)**。 如果此物件包含 MAC 位址，請選擇 **MAC 位址(Mac Address)**。
MAC 位址 **(Mac Address)**	輸入網卡的 MAC 位址。
起始 IP 位址 **(Start IP Address)**	輸入單一位址/範圍位址的起始 IP 位址。
結束 IP 位址 **(End IP Address)**	如果選擇範圍位址，請在此輸入結束 IP 位址。
前置號碼長度 **(Prefix Len)**	輸入 IPv6 位址的前置號碼長度值(例如 64)。
反向選擇 **(Invert Selection)**	若勾選此項，除了上述以外，全部的 IPv6 位址都將套用此物件規則。

3. 完成設定之後，按下確定(OK)按鈕儲存相關設定。

VIII-1-4 IPv6 群組(IPv6 Group)

本頁可讓您綁定數個 IPv6 物件成爲一個 IPv6 群組。

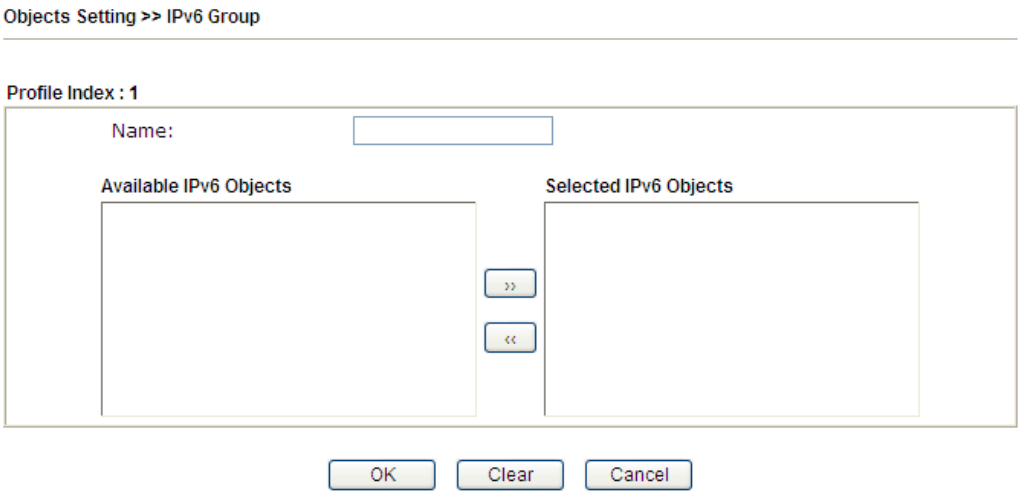


可用設定說明如下：

項目	說明
回復出廠預設值(Set to Factory Default)	清除全部的設定資料。
索引(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 在索引編號欄位中選擇一個號碼(例如 #1)以便設定細節內容。
2. 設定頁面顯示如下：



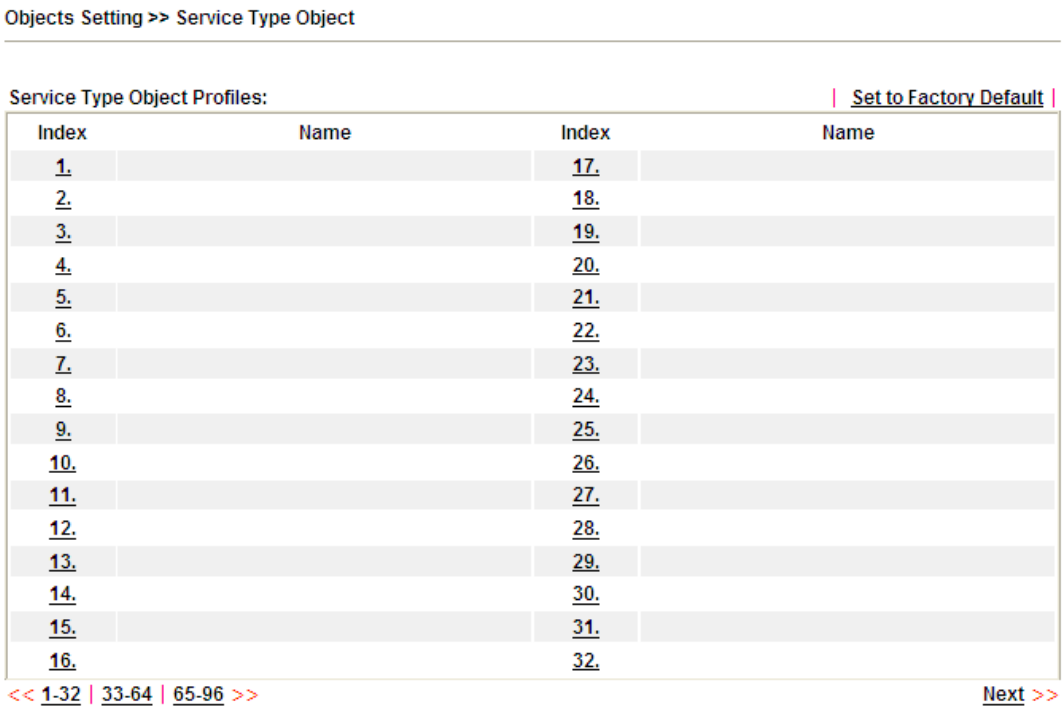
可用設定說明如下：

項目	說明
名稱(Name)	請輸入本設定檔的名稱，最多可以輸入 15 個字元。
可用的 IPv6 物件 (Available IPv6 Objects)	所有可用的 IPv6 物件全都會顯示在此方塊中。
選定的 IPv6 物件 (Selected IPv6 Objects)	按下 **>>** 按鈕來新增選定 IP IPv6 物件並呈現在此方塊內。

3. 完成設定之後，按下確定(OK)按鈕儲存相關設定。

VIII-1-5 服務類型物件(Service Type Object)

您可設定 96 組不同條件的服務類型物件。

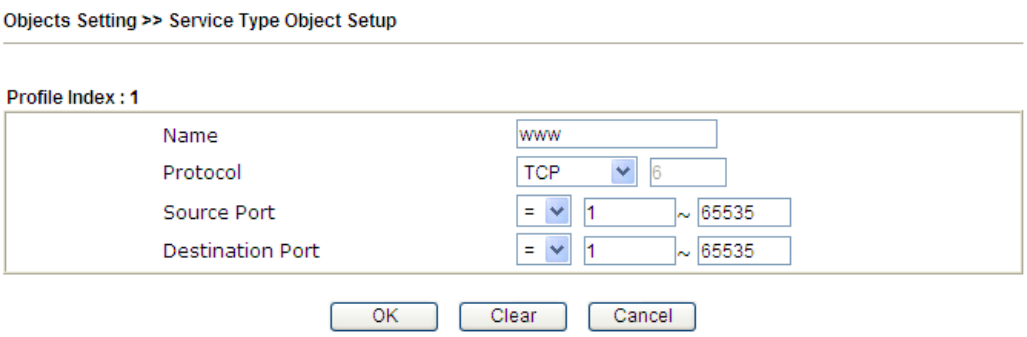


可用設定說明如下：

項目	說明
回復出廠預設值(Set to Factory Default)	清除全部的設定資料。
索引(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

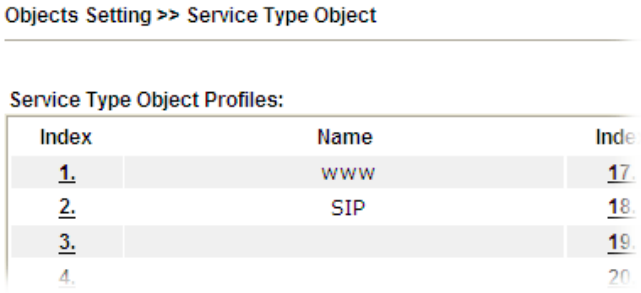
1. 在索引編號欄位中選擇一個號碼(例如 #1)以便設定細節內容。
2. 設定頁面顯示如下：



可用設定說明如下：

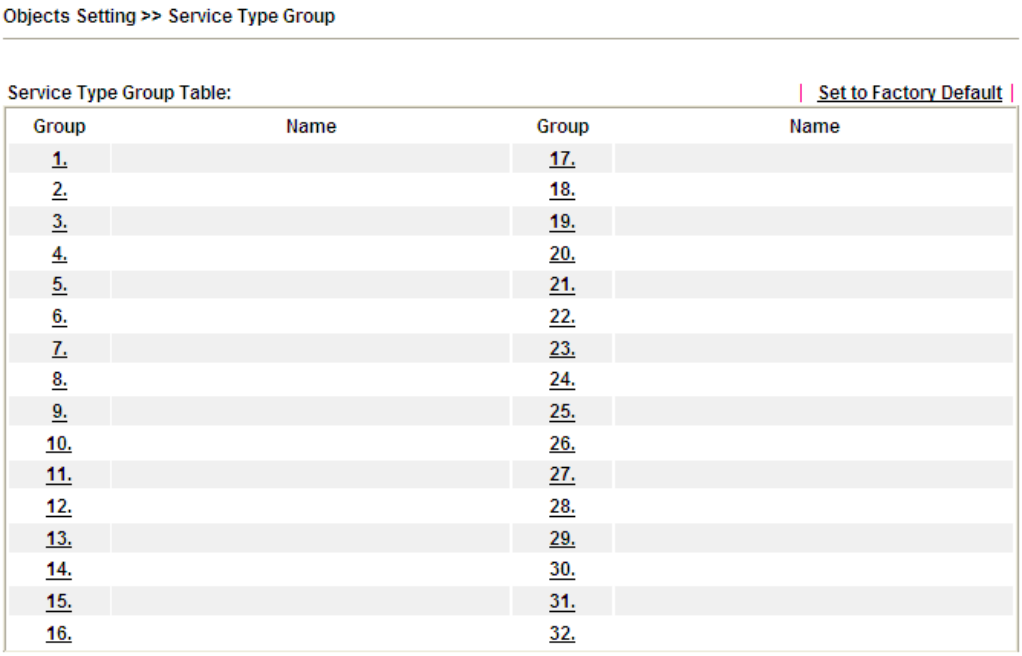
項目	說明
名稱(Name)	輸入此設定檔的名稱。
介面(Protocol)	請選擇此設定檔所要套用的適當介面。
來源/目標通訊埠 (Source/Destination Port)	**來源通訊埠**與**目標通訊埠**欄位皆爲 TCP/UDP 可用之通訊埠，如果是其他的通訊協定，這些欄位即可省略，過濾器規則將可過濾任何一種通訊埠號。 *(=)* – 當第一與最後的數值相同時，此符號表示一個通訊埠。當第一與最後的數值不同時，此符號表示此設定檔所適用的通訊埠號範圍。 *(!=)* –當第一與最後的數值相同時，此符號表示除了這裡所指明的通訊埠以外，全都適用於此設定檔。當第一與最後的數值不同時，此符號表示所有的通訊埠除了此處所設定的範圍以外，全都適用於此設定檔。 *(>)* – 大於此數值的通訊埠號皆可使用。 *(<)* – 小於此數值的通訊埠號皆可使用。

3. 完成設定之後，按下確定(OK)按鈕儲存相關設定。



VIII-1-6 服務類型群組(Service Type Group)

本頁可讓您綁定數個服務類型物件成爲一個群組。

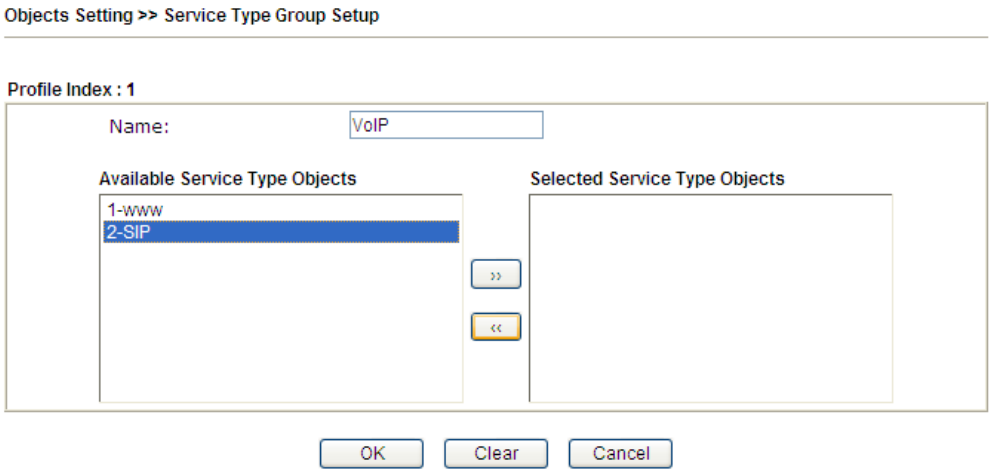


可用設定說明如下：

項目	說明
回復出廠預設值(Set to Factory Default)	清除全部的設定資料。
索引(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。
2. 設定頁面顯示如下：



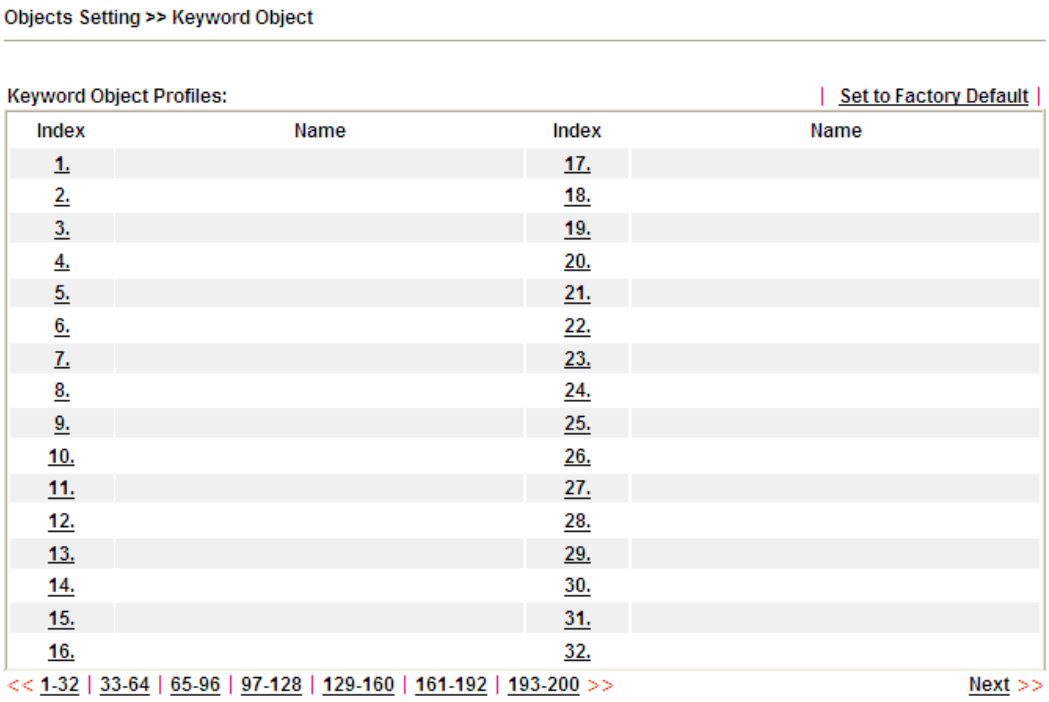
可用設定說明如下：

項目	說明
名稱(Name)	輸入此設定檔的名稱。
可用之服務類型物件 (Available Service Type Objects)	您可以從 IP 物件頁面中先新增一些服務類型，所有可用的服務類型將會顯示在此區域中。
選定之服務類型物件 (Selected Service Type Objects)	按下 **>>** 按鈕來新增選定服務類型並呈現在此方塊內。

3. 完成設定之後，按下確定(OK)按鈕儲存相關設定。

VIII-1-7 關鍵字物件(Keyword Object)

您有 200 組關鍵字物件設定可供您在**數位內容安全管理(CSM)>>URL 網頁內容過濾器設定檔(CSM >>URL Web Content Filter Profile)**中選擇作爲黑白名單之用。

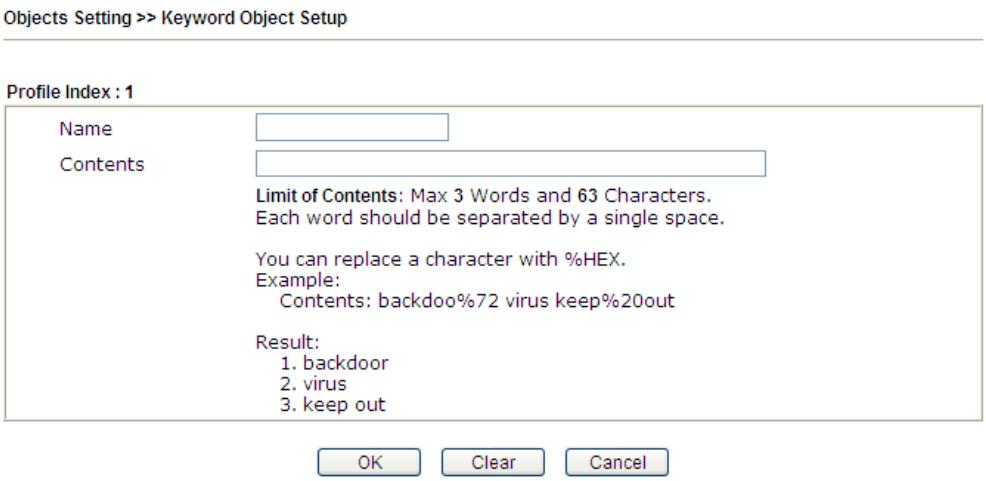


可用設定說明如下：

項目	說明
回復出廠預設值(Set to Factory Default)	清除全部的設定資料。
索引(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 在索引編號欄位中選擇一個號碼(例如 #1)以便設定細節內容。
2. 設定頁面顯示如下：



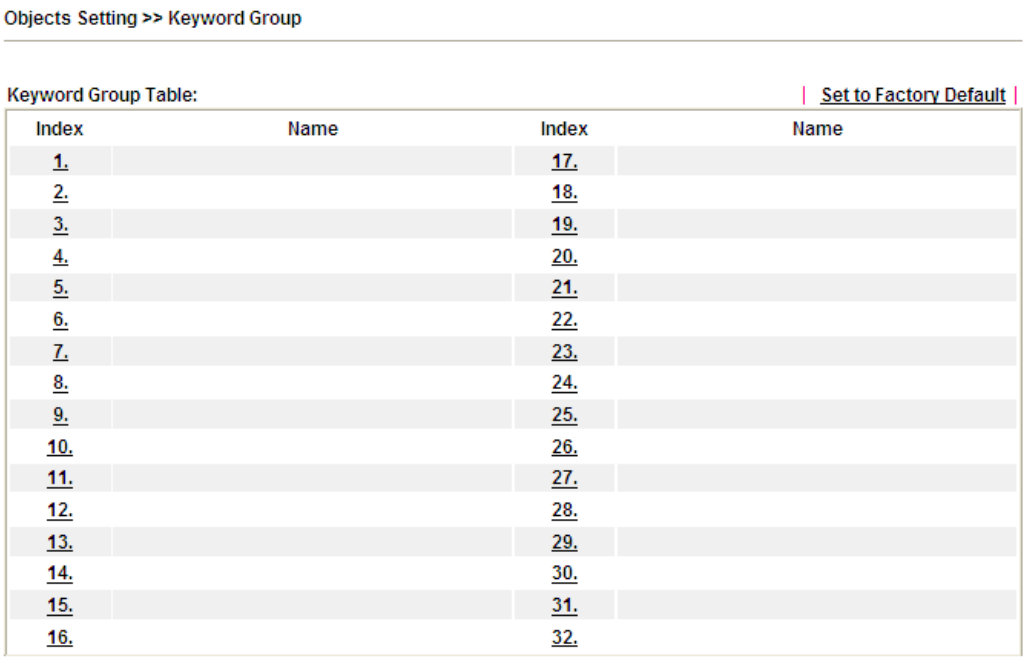
可用設定說明如下：

項目	說明
名稱(Name)	輸入此設定檔的名稱。
內容(Contents)	輸入此設定檔的實際內容，例如可輸入 gambling。當您瀏覽網頁時，含有 gambling (賭博)等訊息之頁面就會被砍掉，並依照防火牆對此的設定放行/封鎖。

3. 完成設定之後，按下確定(OK)按鈕儲存相關設定。

VIII-1-8 關鍵字群組(Keyword Group)

您可以將數個關鍵字物件組合成一個群組，此關鍵字群組可供您在 **CSM>>URL 網頁內容過濾器設定檔(CSM >>URL /Web Content Filter Profile)**中選擇作爲黑白名單之用。

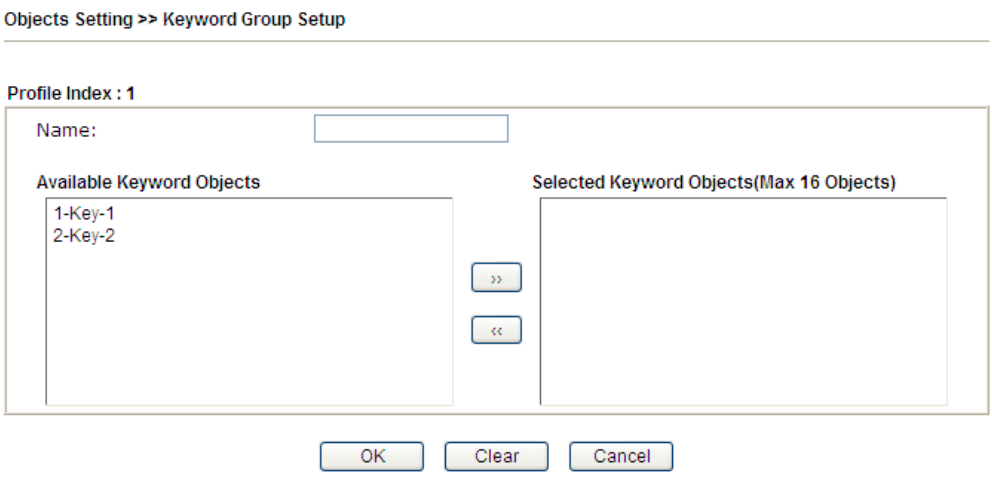


可用設定說明如下：

項目	說明
回復出廠預設值(Set to Factory Default)	清除全部的設定資料。
索引(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 在索引編號欄位中選擇一個號碼(例如 #1)以便設定細節內容。
2. 設定頁面顯示如下：



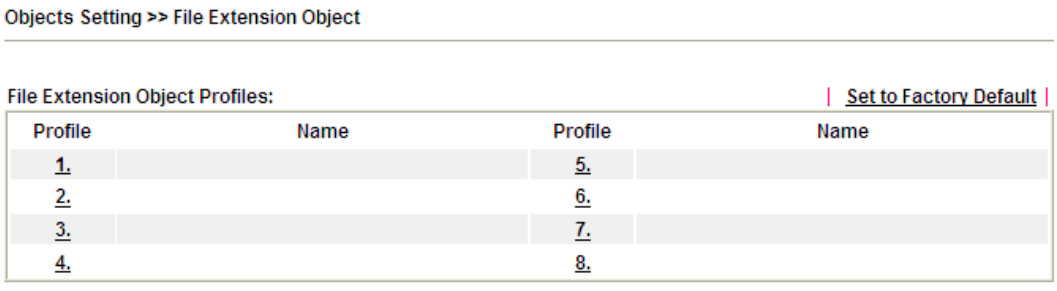
可用設定說明如下：

項目	說明
名稱(Name)	輸入此設定檔的名稱。
可用之關鍵字物件 (Available Keyword Objects)	您可組合關鍵字物件成爲一個關鍵字群組，所有可用的關鍵字物件都會顯示在本方塊區中。
選定關鍵字物件 (Selected Keyword Objects)	按 >> 按鈕增加選定之關鍵字物件於本方塊區中。

3. 完成設定之後，按下確定(OK)按鈕儲存相關設定。

VIII-1-9 副檔名物件(File Extension Object)

本頁允許您設定 8 組設定檔，這些設定檔將應用在**數位內容安全管理(CSM)>>URL 內容過濾器(CSM>>URL Content Filter)**中。設定檔中指定之所有含附檔名稱的檔案都可按照所選擇的動作來處理。



可用設定說明如下：

項目	說明
回復出廠預設值(Set to Factory Default)	清除全部的設定資料。
索引(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。
2. 設定頁面顯示如下：



可用設定說明如下：

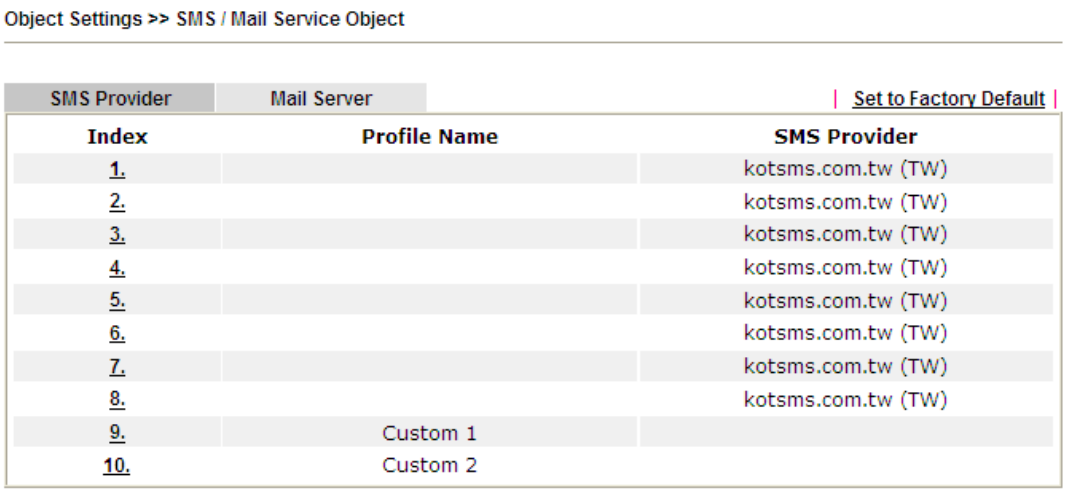
項目	說明
設定檔名稱(Profile Name)	請輸入此設定檔名稱。

3. 輸入設定檔名稱並勾選路由器會處理的副檔名項目，然後按**確定(OK)**儲存本頁的設定。

VIII-1-10 簡訊(SMS)/郵件服務物件(SMS/Mail Service Object)

簡訊服務(SMS)供應商

本頁讓您設定 10 組設定檔，後續將運用在**應用>>簡訊/郵件警示服務(Application>>SMS/Mail Alert Service)**中。

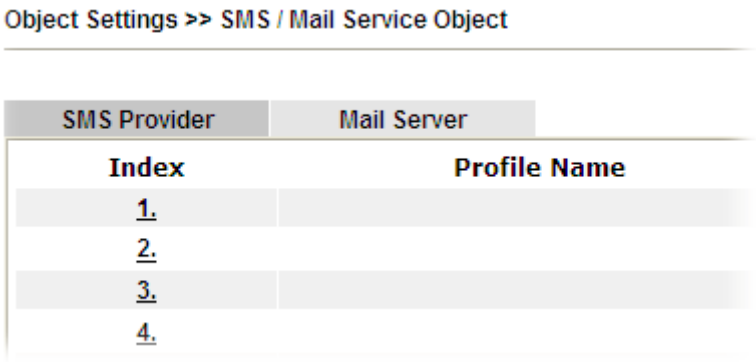


每個項目說明如下：

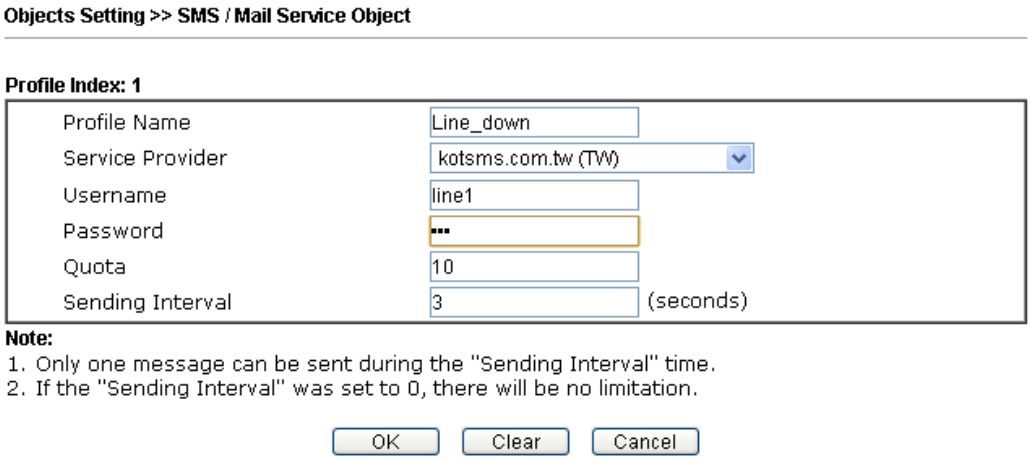
項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部的設定資料。
索引(Index)	顯示您可以設定的設定檔索引編號。
設定檔名稱(Profile)	顯示物件設定檔的檔名。
簡訊服務供應商 (SMS Provider)	顯示提供簡訊服務的供應商名稱。

如欲建立新的設定檔，請依下述步驟進行：

1. 選擇簡訊供應商標籤欄，然後按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。



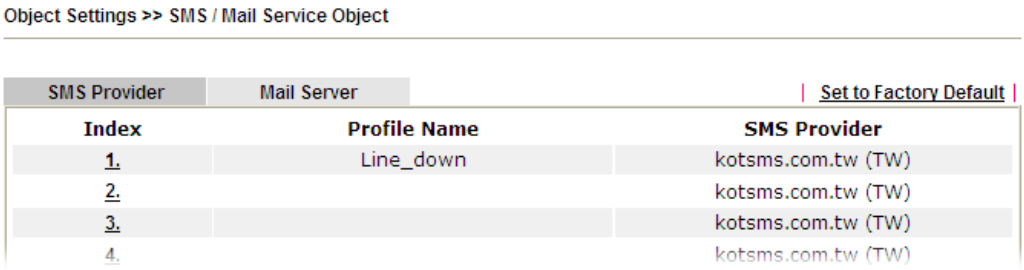
2. 設定頁面顯示如下：



可用設定說明如下：

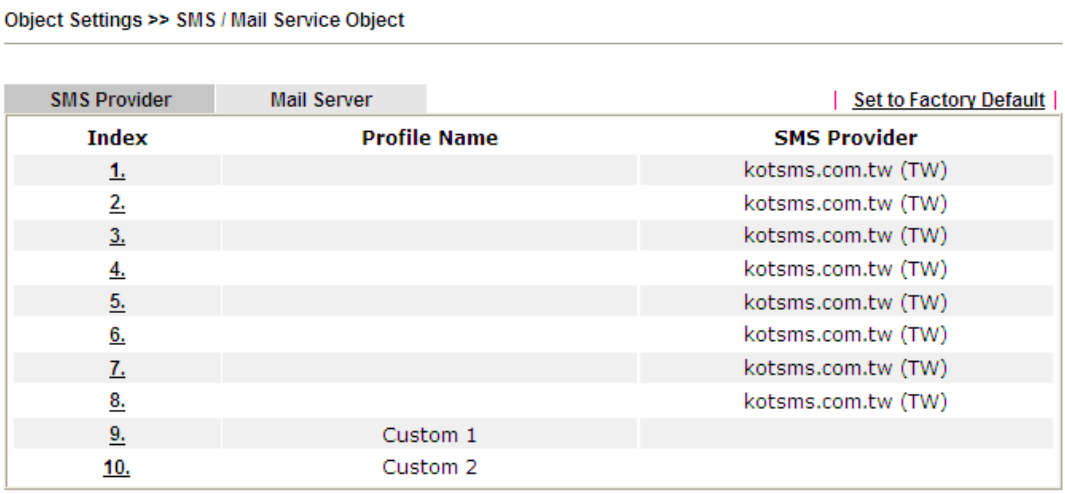
項目	說明
設定檔名稱 (Profile Name)	請輸入此設定檔名稱。
服務供應商 (Service Provider)	使用下拉式清單選擇提供簡訊服務的服務供應商。
使用者名稱 (Username)	輸入發簡訊人員用來註冊選擇簡訊服務供應商所需的名稱。 使用者名稱長度不可超過 31 個字元。
密碼 (Password)	輸入發簡訊人員用來註冊選擇簡訊服務供應商所需的密碼。密碼長度不可超過 31 個字元。
簡訊則數 (Quota)	輸入您自服務供應商所購得的簡訊則數。 注意，每則簡訊等於標準路由中所註記的簡訊文字訊息。
寄送間隔時間 (Sending Interval)	爲了防止發信額度太早用罄，請輸入傳送簡訊所需的間隔時間。

3. 完成設定之後，按下確定(OK)按鈕儲存相關設定。

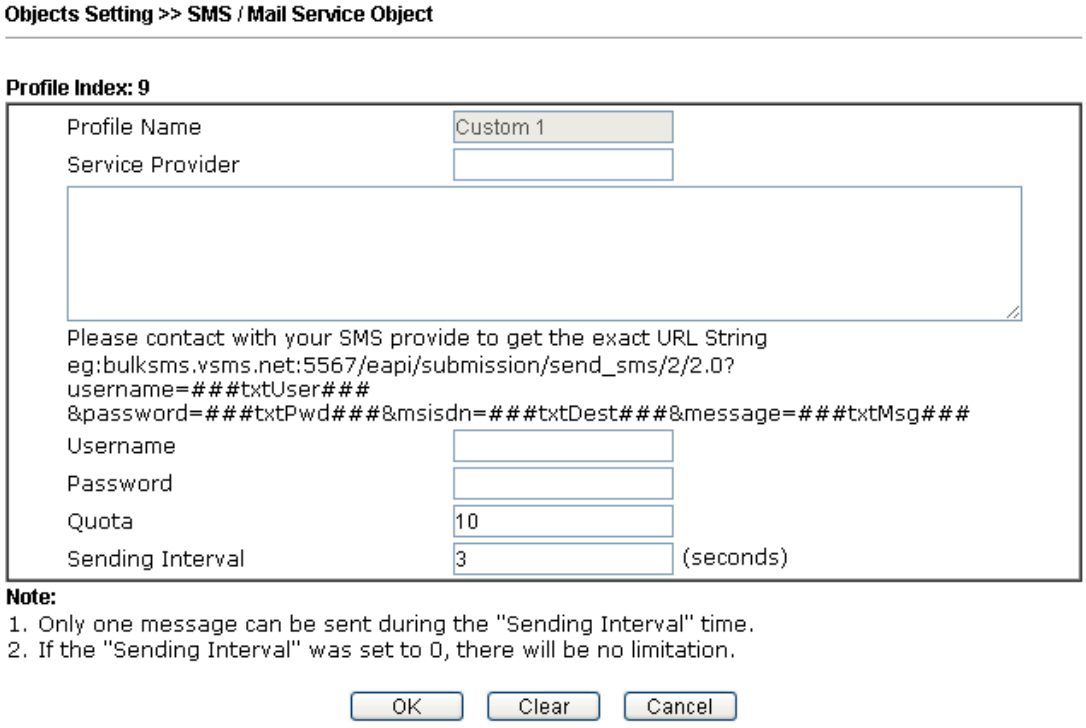


客製化簡訊服務(Customized SMS Service)

路由器提供數種簡訊服務供應商的名稱來供應簡訊服務，然而，如果您的服務供應商不在清單上，您可以透過索引編號 9 與 10 自行設定簡訊服務供應商的相關資料。編號 9 與 10 的設定檔名稱是固定無法改變的。



按下索引編號 9 與 10 開啓設定頁面：



可用設定說明如下：

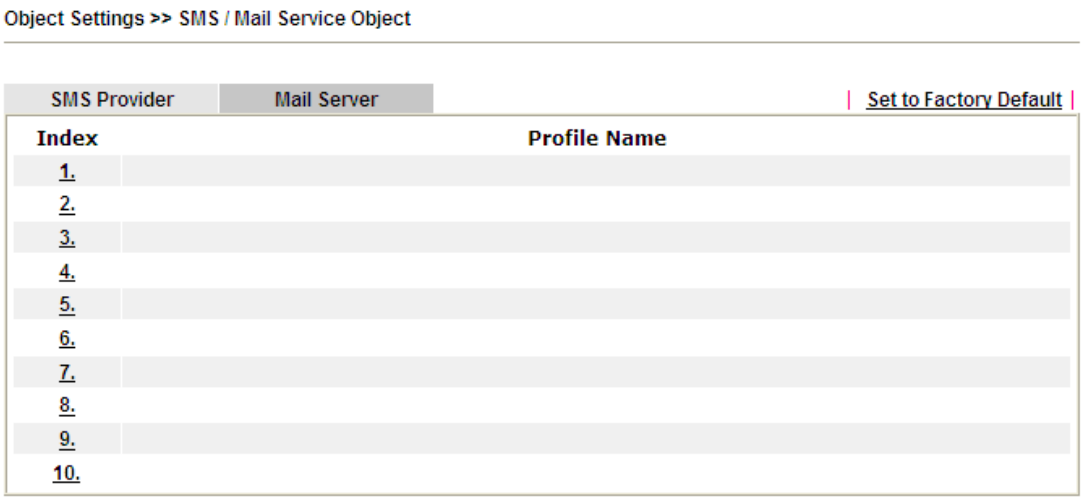
項目	說明
設定檔名稱 (Profile Name)	顯示設定檔名稱。
服務供應商 (Service Provider)	輸入服務供應商的網址。 在此項目的下方區塊中輸入 URL，您必須先與簡訊服務供應商聯絡以便獲得正確的 URL 字串。

使用者名稱 (Username)	輸入發簡訊人員用來註冊選擇簡訊服務供應商所需的名稱。 使用者名稱長度不可超過 31 個字元。
密碼 (Password)	輸入發簡訊人員用來註冊選擇簡訊服務供應商所需的密碼。 密碼長度不可超過 31 個字元。
簡訊則數 (Quota)	輸入您自服務供應商所購得的簡訊則數。 注意，每則簡訊等於標準路由中所註記的簡訊文字訊息。
傳送間隔 (Sending Interval)	爲了防止發信額度太早用罄，請輸入傳送簡訊所需的間隔時間。

完成設定之後，按下確定(OK)按鈕儲存相關設定。

郵件服務物件(Mail Service Object)

本頁讓您設定 10 組設定檔，後續將運用在**應用>>簡訊/郵件警示服務(Application>>SMS/Mail Alert Service)**中。

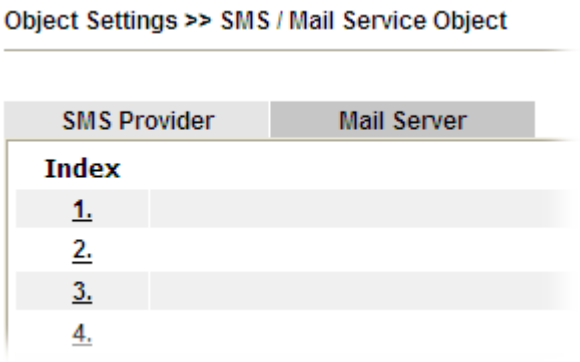


可用設定說明如下：

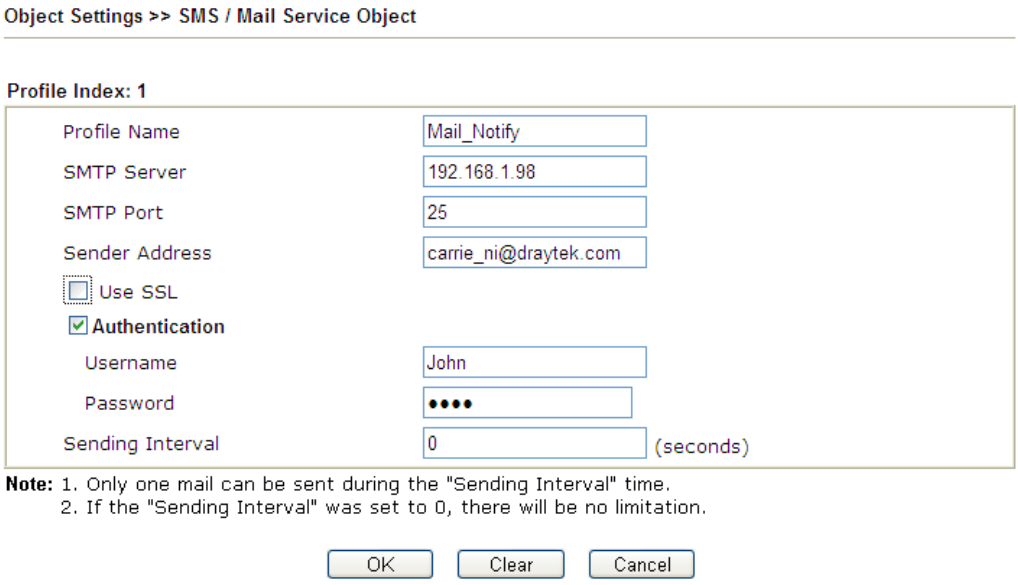
項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部的設定資料。
索引(Index)	顯示您可以設定的設定檔索引編號。
設定檔名稱 (Profile Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 選擇郵件伺服器標籤欄，然後按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。



2. 設定頁面顯示如下：

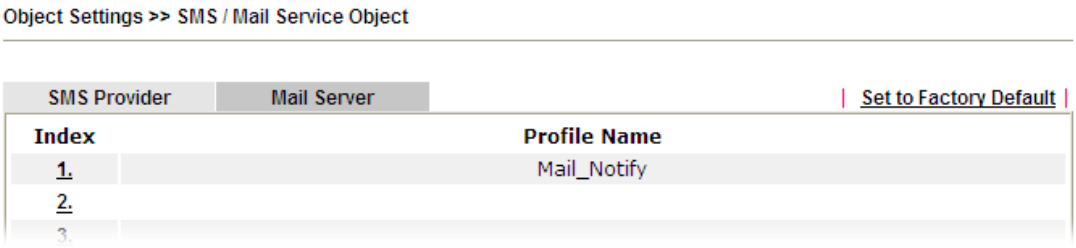


可用設定說明如下：

項目	說明
設定檔名稱 (Profile Name)	請輸入此設定檔名稱。
SMTP 伺服器 (SMTP Server)	輸入郵件伺服器的 IP 位址。
SMTP 埠號 (SMTP Port)	輸入 SMTP 伺服器需要的埠號。
寄件人位址 (Sender Address)	輸入寄件人的電子郵件位址。
使用 SSL (Use SSL)	勾選此方框啓用此功能。
驗證 (Authentication)	郵件伺服器必須透過正確的使用者名稱與密碼來進行驗證，才有權利傳送訊息，請勾選方框啓用此功能。 **使用者名稱(Username)** – 請自訂驗證所需的使用者名稱。 **密碼(Password)** –請自訂驗證所需的密碼。
傳送間隔	請輸入傳送簡訊所需的間隔時間。

(Sending Interval)	

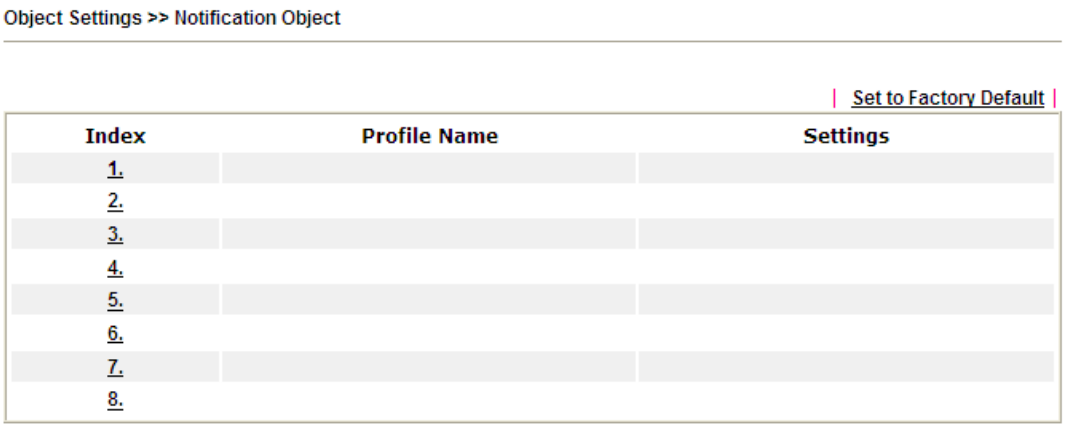
3. 完成設定之後，按下確定(OK)按鈕儲存相關設定。



VIII-1-11 通知物件(Notification Object)

本頁讓您設定 10 組設定檔，後續將運用在**應用>>簡訊/郵件警示服務(Application>>SMS/Mail Alert Service)**中。

每個物件可以設定不同的監控條件。

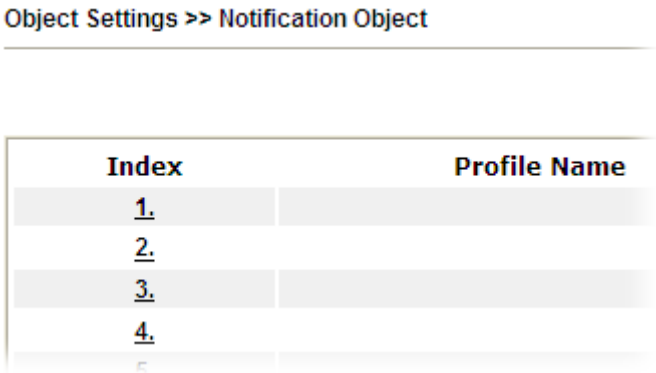


可用設定說明如下：

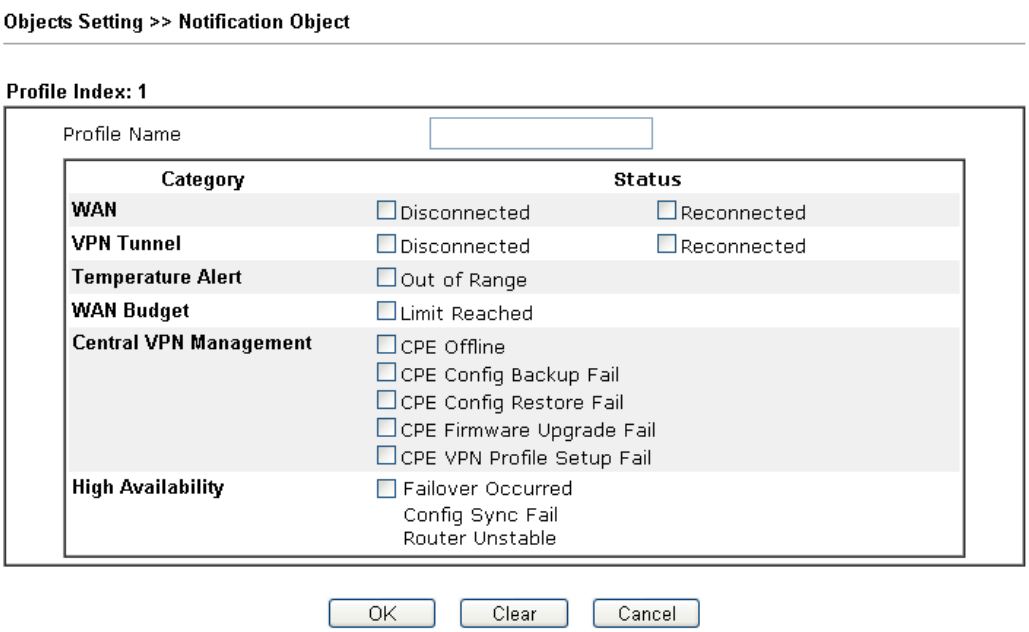
項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部的設定資料。
索引(Index)	顯示您可以設定的設定檔索引編號。
設定檔名稱 (Profile Name)	顯示物件設定檔的檔名。
設定(Settings)	顯示物件設定檔的內容。

如欲建立新的設定檔，請依下述步驟進行：

1. 開啓**物件設定>>通知物件(Object Setting>>Notification Object)**，然後按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。



2. 設定頁面顯示如下：

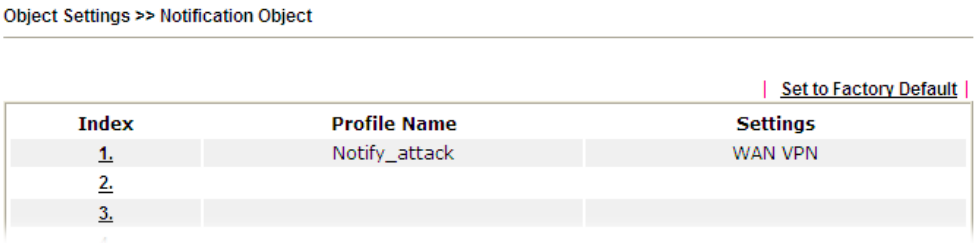


可用設定說明如下：

項目	說明
Profile Name	Type a name for such notification profile. The maximum length of the name you can set is 15 characters.
Category	Display the types that will be monitored.
Status	Display the status for the category. You can check the box to be monitored. For example, the check box of **CPE firmware upgrade fail** under the category of **Central VPN Management** is checked. Once such profile is enabled, Vigor router system will send out notification to the recipient via SMS.
設定檔名稱 (Profile Name)	請輸入此設定檔名稱。
類型 (Category)	顯示被監控的類型。

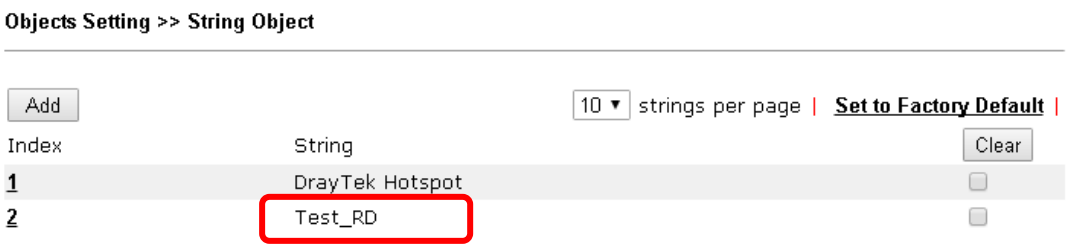
狀態 (Status)	顯示類型的狀態，您可以勾選想要監控的類型狀態方塊。

3. 完成設定之後，按下確定(OK)按鈕儲存相關設定。

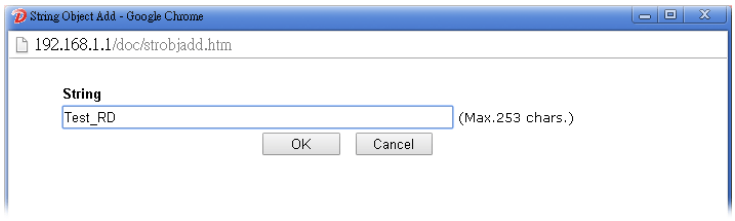


VIII-1-12 字串物件(String Object)

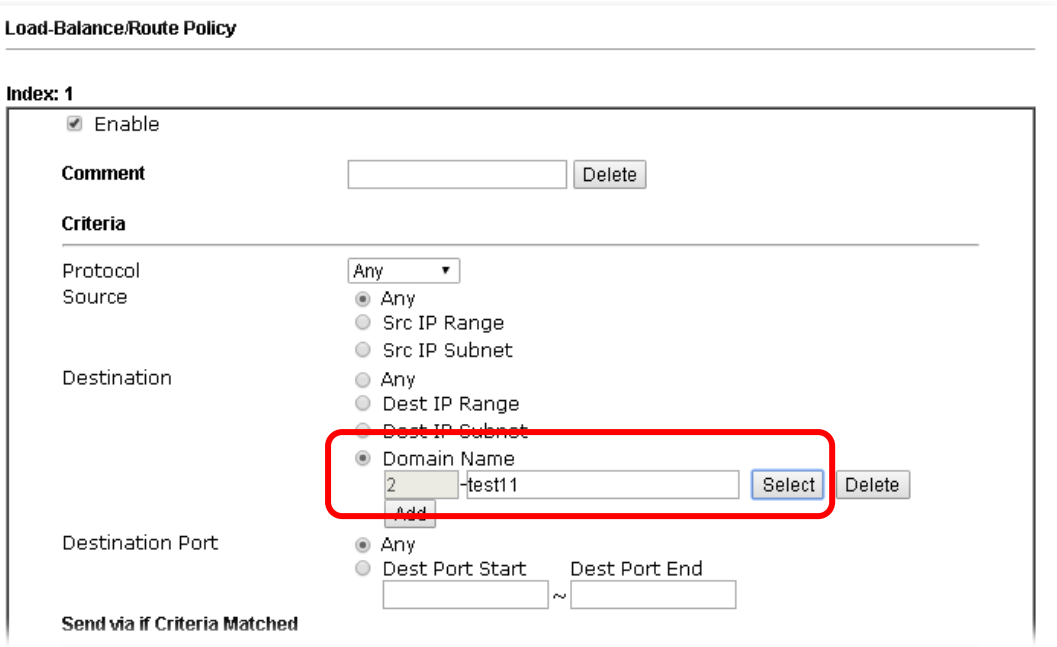
本頁讓您設定字串物件設定檔，可套用在路由策略中(網域名稱選項)、客製化入口網站等等。



可用設定說明如下：

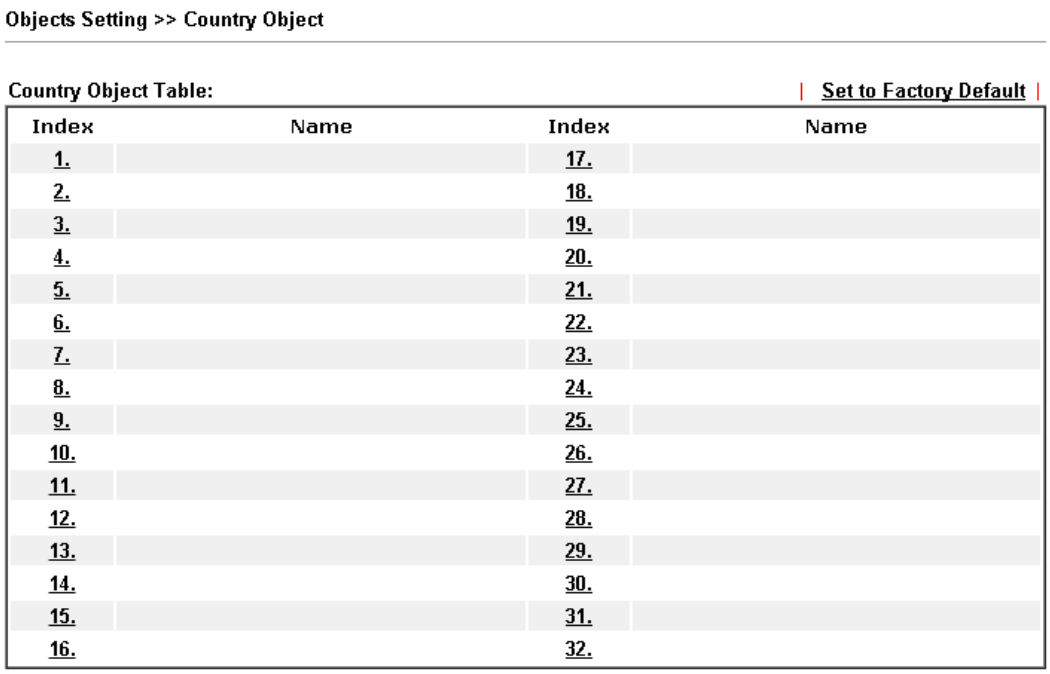
項目	說明
新增(Add)	按此開啓下述頁面以新增字串物件。 
回復出廠預設值(Set to Factory Default)	按此清除本頁所有設定。
索引(Index)	顯示您可以設定的設定檔索引編號。
字串(String)	顯示定義的字串內容。
清除(Clear)	選擇您想要移除的字串，接著按下此鈕刪除選擇的字串。

下列顯示套用字串物件的範例(在路由策略):

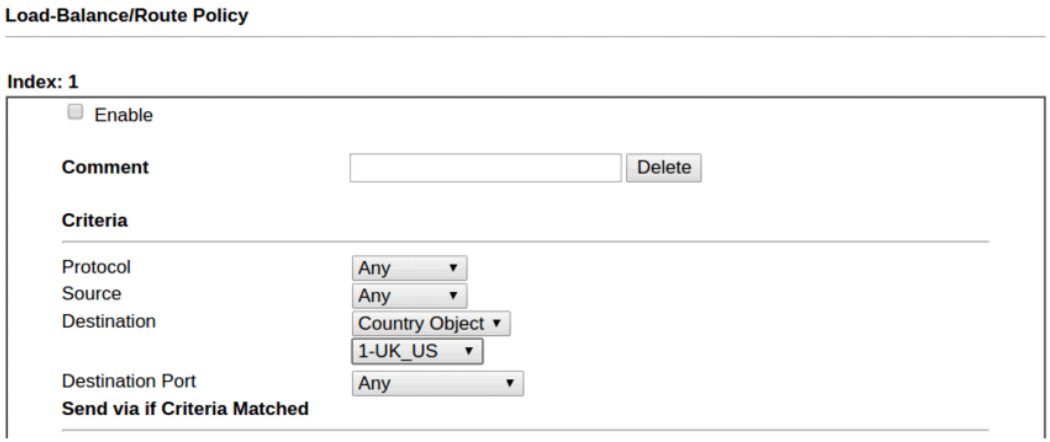


VIII-1-13 國家物件(Country Object)

國家物件可以決定路由器防火牆應該封鎖哪個/些國家。



國家物件，藉由群組多個國家多組 IP 位址，可被其他功能如路由器策略目標使用。請參考以下範例圖：



如欲建立新的設定檔，請依下述步驟進行：

1. 開啓**物件設定>>國家物件(Object Setting>>Country Object)**，按下任一索引編號(如#1)。

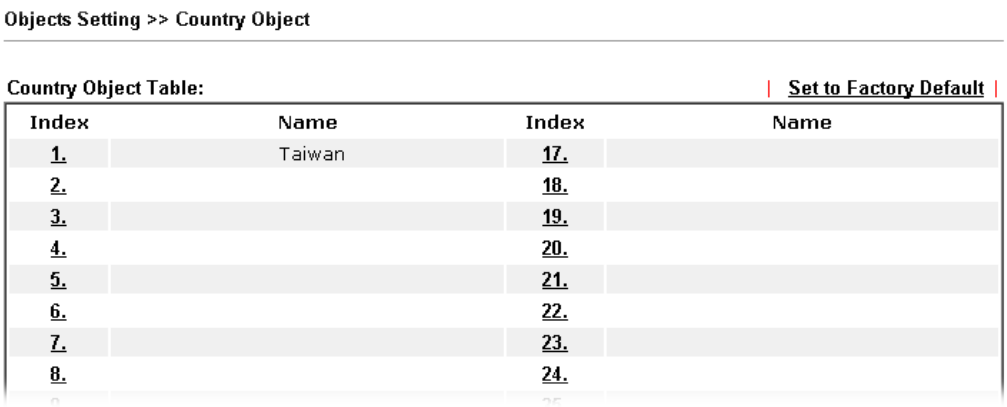
2. 設定頁面顯示如下：



可用設定說明如下：

項目	說明
名稱(Name)	輸入設定檔名稱。
國家(Countries)	請自左方選擇需要被封鎖的國家，按下>>將其移至選定國家區域中。 注意，每一個國家設定檔可包含 1 到 16 個國家。

3. 完成設定之後，按下確定(OK)按鈕儲存相關設定。

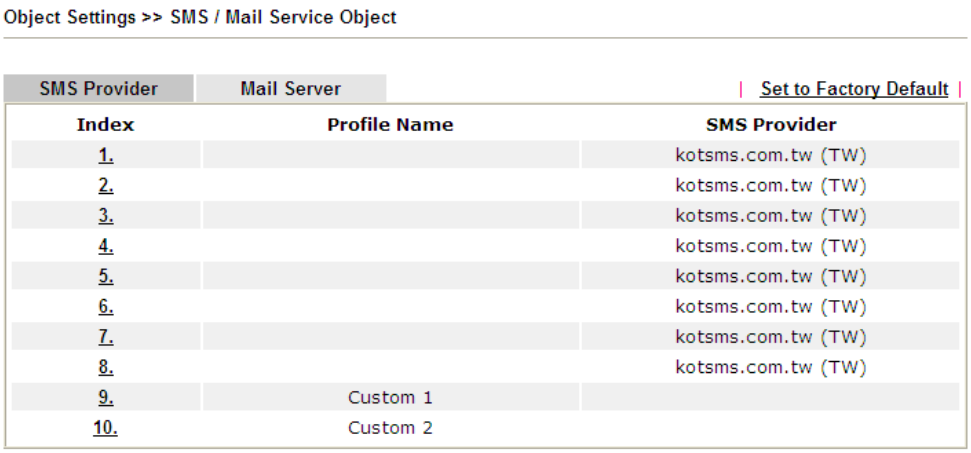


應用說明

A-1 當 WAN 斷線時如何使用 SMS 簡訊服務寄發通知至指定的電話號碼

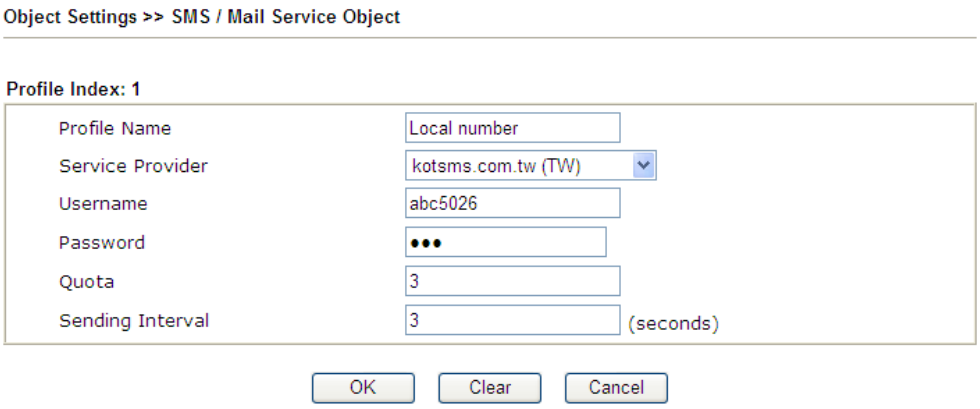
請參考下列步驟：

1. 登入路由器的網頁設定介面。
2. 首先開啓**物件設定>>簡訊(SMS)/郵件服務物件(Object Settings>>SMS/Mail Server Object)**頁面。

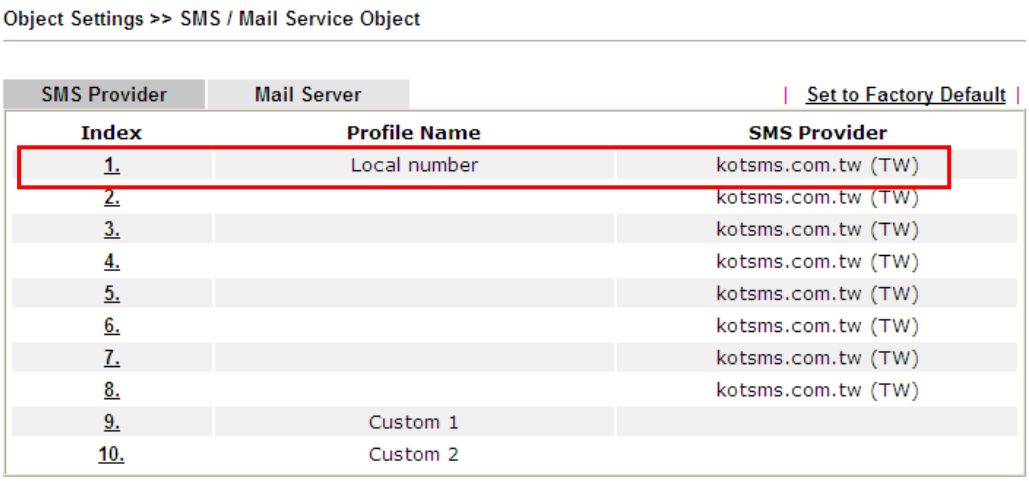


索引編號 1~8 可以讓使用者選取內建的 SMS 簡訊服務供應商，若您所使用的簡訊服務供應商不在內建的清單中，即可使用索引編號 9 與 10 來新增您的 SMS 簡訊服務供應商（請參考備註）。

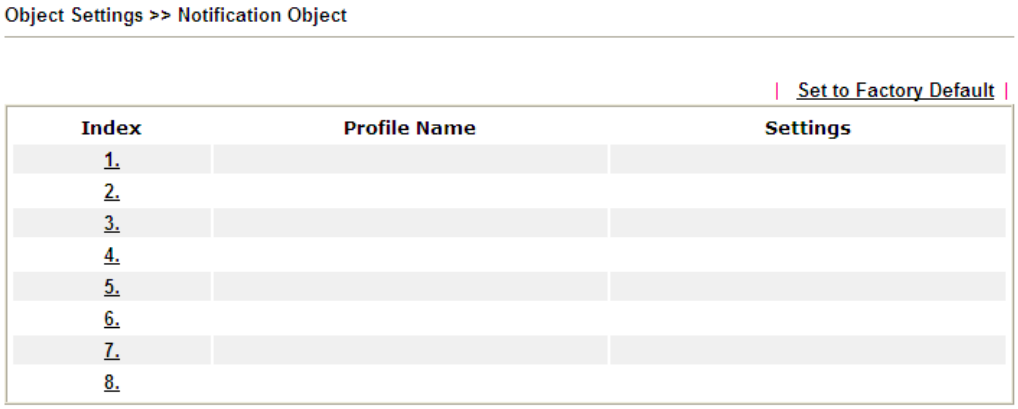
3. 選擇任何一個索引編號(例如本例使用編號 1)進行簡訊服務供應商設定，在下列開啓的頁面中，請填入您的帳號密碼，並設定此路由器可發送的簡訊則數。



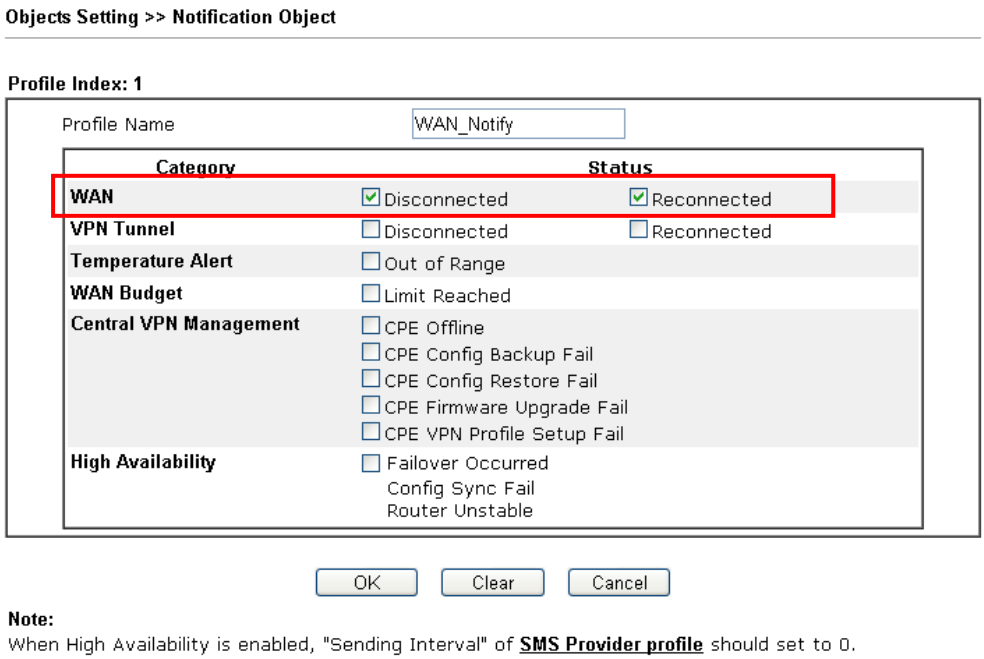
4. 設定完畢之後，按下**確定(OK)**回到上頁，便完成簡訊服務供應商的設定。



5. 接著開啓**物件設定>>通知物件(Object Settings>>Notification Object)**，設定通知的事件內容。



6. 選擇任何一個索引編號(例如本例使用編號 1)進行通知發送的條件設定，在下列開啓的頁面中，輸入設定檔名稱，再勾選 WAN 類別中的**中斷連線**與**重新連線**來呼應本文的主題。



7. 設定完畢之後，按下**確定(OK)**回到上頁，便完成通知設定檔的設定。

Object Settings >> Notification Object

| Set to Factory Default |

Index	Profile Name	Settings
1.	WAN_Notify	WAN
2.		
3.		
4.		
5.		
6.		
7.		
8.		

8. 開啓**其他應用>>簡訊(SMS) / 郵件警告服務(Application >> SMS / Mail Alert Service)**頁面。分別自下拉式清單中選擇您需要的簡訊服務供應商與通知設定檔(設定使用簡[訊發送通知的事件)等設定，然後在**收信人**欄位中填入您欲接收簡訊通知的號碼。

Application >> SMS / Mail Alert Service

SMS Provider | Mail Server | Set to Factory Default |

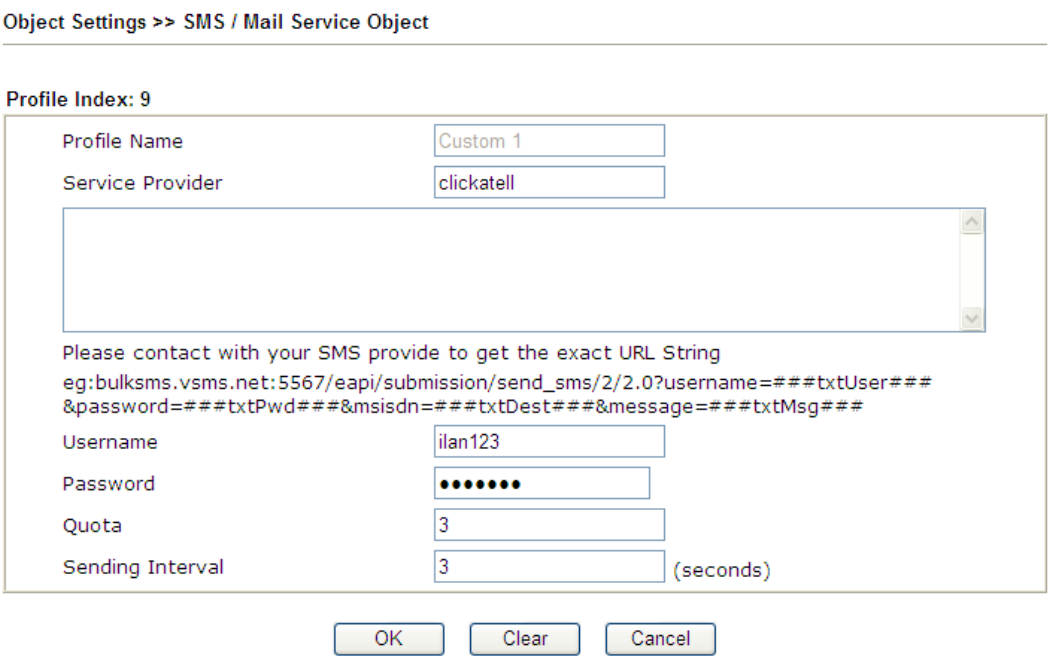
Index	SMS Provider	Recipient	Notify Profile	Schedule(1-15)
1 ☑	1 - Local number	0912345678	1 - WAN_Notify	
2 ☐	1 - Local number		1 - WAN_Notify	
3 ☐	1 - Local number		1 - WAN_Notify	
4 ☐	1 - Local number		1 - WAN_Notify	
5 ☐	1 - Local number		1 - WAN_Notify	
6 ☐	1 - Local number		1 - WAN_Notify	
7 ☐	1 - Local number		1 - WAN_Notify	
8 ☐	1 - Local number		1 - WAN_Notify	
9 ☐	1 - Local number		1 - WAN_Notify	
10 ☐	1 - Local number		1 - WAN_Notify	

OK Cancel

9. 按**確定(OK)**儲存相關設定，之後若路由器有某條 WAN 斷線，系統將會寄出簡訊給指定的人。如果路由器僅有一個 WAN 介面，那麼系統也會重新連接 WAN 介面成功之後，寄送簡訊給指定的人。

備註：如何自訂簡訊服務供應商

開啓**物件設定>>簡訊(SMS)/郵件服務物件(Object Settings>>SMS/Mail Server Object)**，選取任一可自訂的索引連結(例如索引編號 9 或 10)，在開啓的頁面中填入您的簡訊服務供應商的 URL 字串並填入您的帳號密碼，即可新增您所使用的簡訊服務供應商來寄發簡訊 SMS 通知。



VIII-2 USB 應用(USB Application)

連接至路由器的 USB 存取磁碟可以被視爲伺服器的一種。透過 Vigor 路由器，區域網路端的用戶可以透過不同的應用程式登入、寫入並讀取儲存在 USB 儲存碟內的資料。在完成 USB 應用設定之後，您可以在用戶端軟體上輸入路由器的 IP 位址，以及在 **USB 應用>>USB 使用者管理(USB Application>>USB User Management)**頁面所建立的帳號與密碼，然後，用戶端就可以使用 FTP(USB 儲存碟)或是分享檔案服務。



資訊

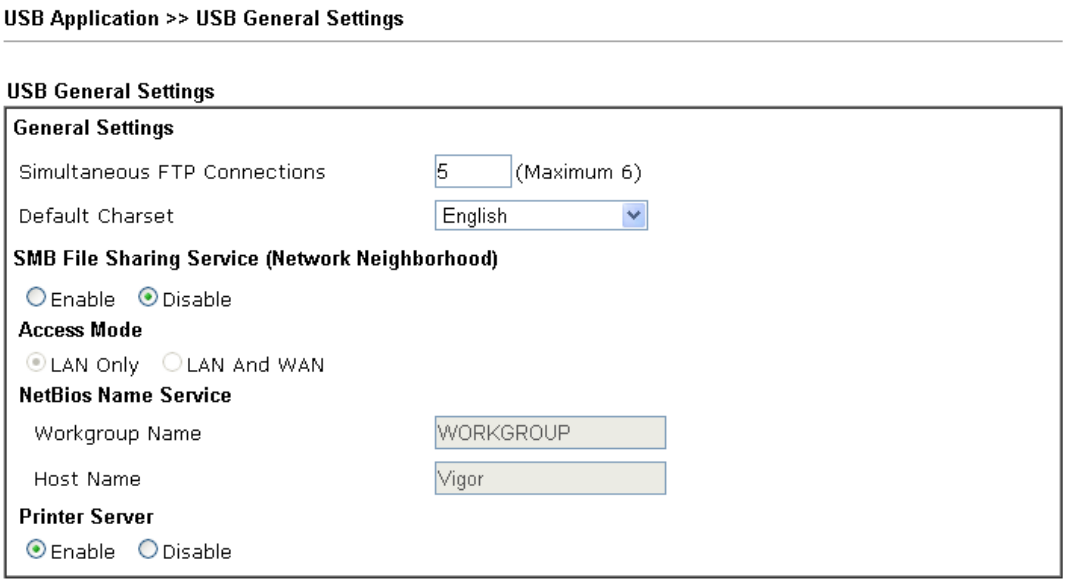
Vigor 路由器的 USB 埠口可用來連接 USB 數據機，Vigor 路由器支援哪些數據機可從 **USB 應用>>數據機支援清單(USB Application>>Modem Support List)** 中取得相關資訊，有關透過 USB 數據機建構的網路連線，請參考 **WAN>>網際網路連線(WAN>>Internet Access)**與 **WAN>>基本設定(WAN>>General Setup)**。

網頁使用者介面



VIII-2-1 USB 基本設定(USB General Settings)

本頁決定同步 FTP 連線的數目、預設字集伺服器以及啓用 Samba 服務，目前，Vigor 路由器可支援格式爲 FAT16 與 FAT32 的 USB 儲存碟，因此在連接 USB 儲存碟之前，請務必確認記憶格式是 FAT16 還是 FAT32。建議您使用 FAT32 來檢視檔案名稱(FAT16 不支援長檔名) 。



可用設定說明如下：

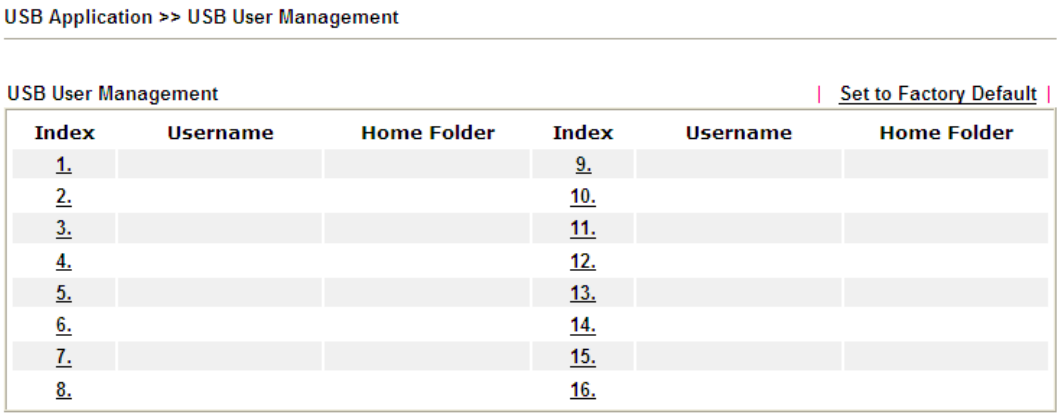
項目	說明
基本設定 (General Settings)	**同步 FTP 連線(Simultaneous FTP Connections) -** 此區用來指定 FTP 連線數總量，路由器允許一次連接 USB 儲存碟數量，最多可達 6 個 FTP 連線數。 **預設字集(Default Charset) -** 目前，Vigor 路由器支援四種語文字集，預設字集爲英文。
SMB 檔案分享服務(SMB File Sharing Service)	按下**啓用(Enable)**以便透過路由器使用 SMB 服務(檔案分享)。
存取模式 (Access Mode)	**限用 LAN(LAN Only)** – 網際網路使用者不可連接至路由器的 samba 伺服器。 **LAN 與 WAN (LAN And WAN)**- LAN 與 WAN 端使用者皆可登入路由器的 samba 伺服器。

NetBios 命名服務 (NetBios Name Service)	針對 USB 儲存碟的 NetBios 服務，您必須指定工作群組名稱以及主機名稱。工作群組名稱不可與主機名稱相同，工作群組名稱最多可有 15 個字元而主機名稱最多可有 23 個字元。二者皆不可包含下述字元; : " < > * + = | ?。 **工作群組名稱(Workgroup Name) -** 輸入工作群組的名稱。 **主機名稱(Host Name) -** 輸入路由器的主機名稱。
印表機伺服器(Printer Server)	**啓用(Enable) -** 按此可讓路由器作爲印表機伺服器(但需外接一台 USB 印表機)。

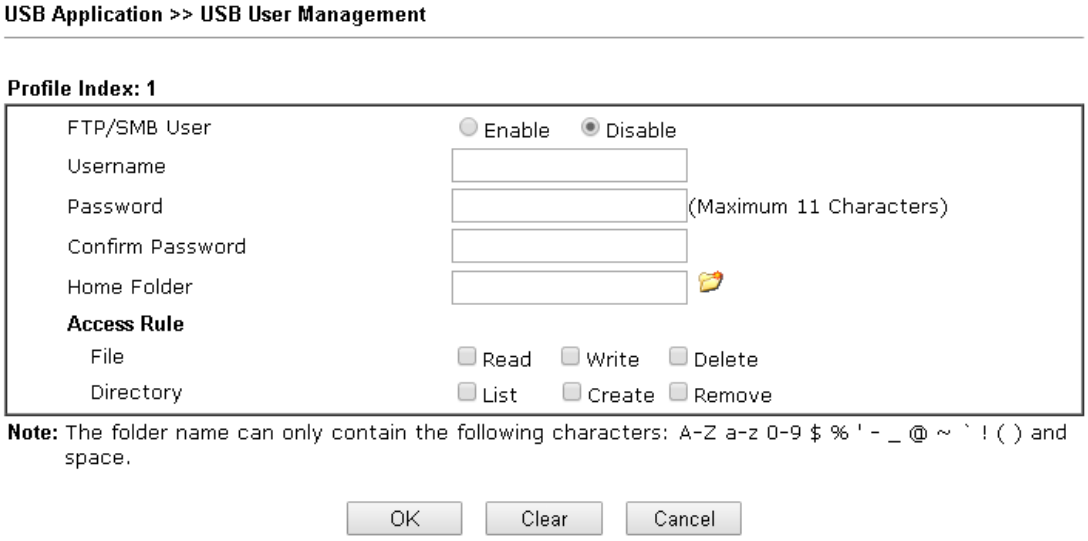
完成設定之後，按下確定(OK)按鈕儲存相關設定。

VIII-2-2 USB 使用者管理(USB User Management)

本頁讓您針對 FTP/SMB 使用者設定數個設定檔，任何想要登入 USB 儲存碟的使用者，必須鍵入與本頁設定相同的使用者名稱與密碼。在新增或是修正本頁設定之前，請先插入 USB 儲存碟，否則系統會出現錯誤訊息。

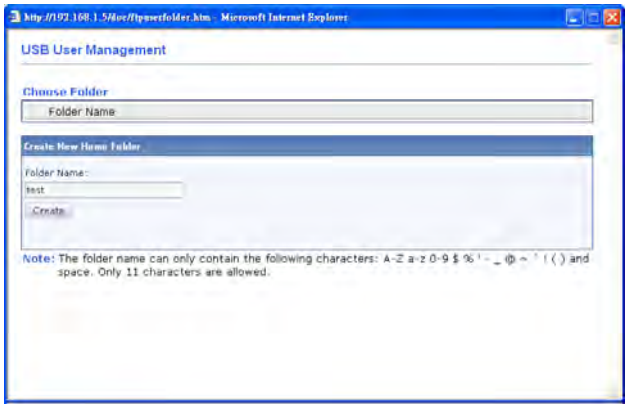


按任一索引號碼連結登入設定頁面。



可用設定說明如下：

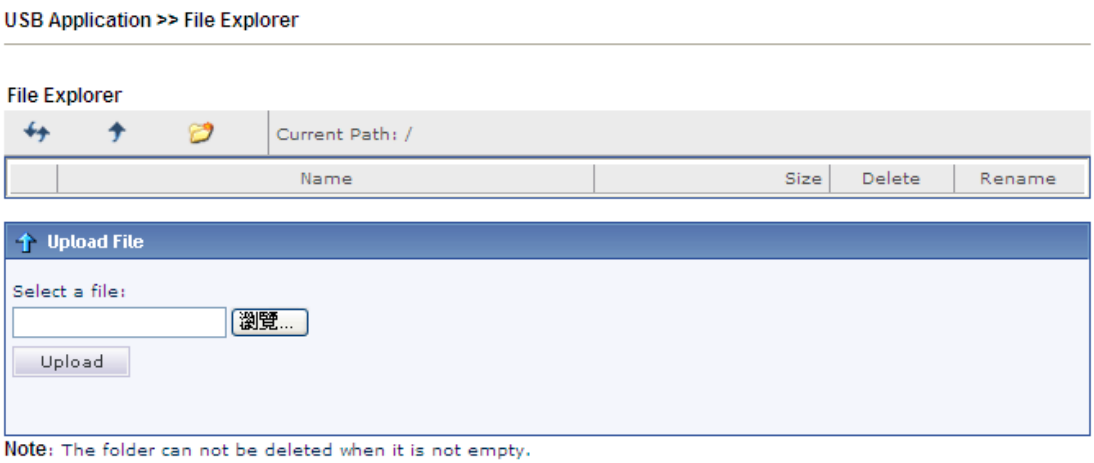
項目	說明

FTP/SMB 使用者 (FTP/SMB User)	**啓用(Enable)** – 按此鈕啓動此 FTP/SMB 服務設定檔，之後，使用者可使用本頁指定的名稱來登入 FTP 伺服器。 **停用(Disable)** – 按下此鈕停用此設定檔。
使用者名稱 (Username)	輸入 FTP/SMB 使用者的使用者名稱以登入 FTP 伺服器(USB 儲存碟)，注意，使用者不可以匿名方式登入 USB 儲存碟，之後您可以打開 FTP 用戶軟體再輸入此處指定的使用者名稱，即可登入 USB 儲存碟。 **注意:** 此處的使用者名稱不可輸入“Admin” ，因爲該名稱是用來登入路由器的使用者介面，同時，該名稱也供 FTP 韌體更新時使用。 **注意:** 路由器不支援 FTP Passive 模式。請在 FTP 用戶端停用此模式。
密碼 (Password)	輸入 FTP/SMB 使用者的密碼以登入 FTP 伺服器(USB 儲存碟)，之後您可以打開 FTP 用戶軟體再輸入此處指定的密碼，即可登入 USB 儲存碟。
確認密碼 (Confirm Password)	再次輸入密碼確認。
預設檔案夾 (Home Folder)	此功能決定用戶登入的檔案夾。 使用者可以在本區輸入目錄名稱，接著按下**確定(OK)**，路由器將會在 USB 儲存碟中建立特定/新的檔案夾，此外，如果使用者輸入“/”，就能進入 USB 儲存碟中所有的檔案夾觀看檔案。 **注意:** 當 USB 儲存碟的防寫狀態開啓時，您就無法在此輸入新檔案夾名稱，在此情況下只有“/”可以運用。 您可以點  以開啓下述對話盒新增檔案夾作爲預設檔案夾。 
存取規則 (Access Rule)	此功能決定設定檔的權限，任何使用此設定檔以便登入 USB 儲存碟的使用者必須遵循此處設定的規則。 **檔案(File)** – 勾選允許開放的項目(讀取、覆寫、刪除)。 **目錄(Directory)** – 勾選允許開放的項目(清單、建立、刪除)。

在您按下**確定(OK)**之後，您必須在路由器的 USB 介面插入 USB 儲存碟，否則您無法儲存設定。

VIII-2-3 檔案瀏覽(File Explorer)

檔案瀏覽提供一個很簡易的方式讓使用者檢視及管理 USB 儲存碟(連接至 Vigor 路由器)的內容。

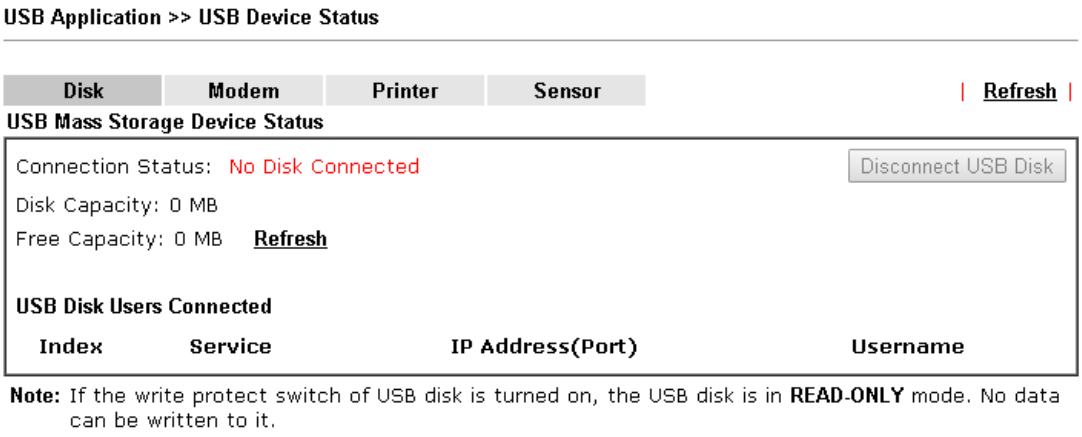


可用設定說明如下：

項目	說明
更新(Refresh)	按此圖示更新檔案清單。
上層(Back)	按此圖示回到上一層目錄。
建立(Create)	按此圖示新增檔案夾。
目前路徑 (Current Path)	顯示目前檔案夾的位址。
上傳 (Upload)	按此鈕上傳選定檔案至 USB 儲存碟，在碟內要上傳的檔案可以給其他 FTP 使用者分享。

VIII-2-4 USB 磁碟狀態(USB Device Status)

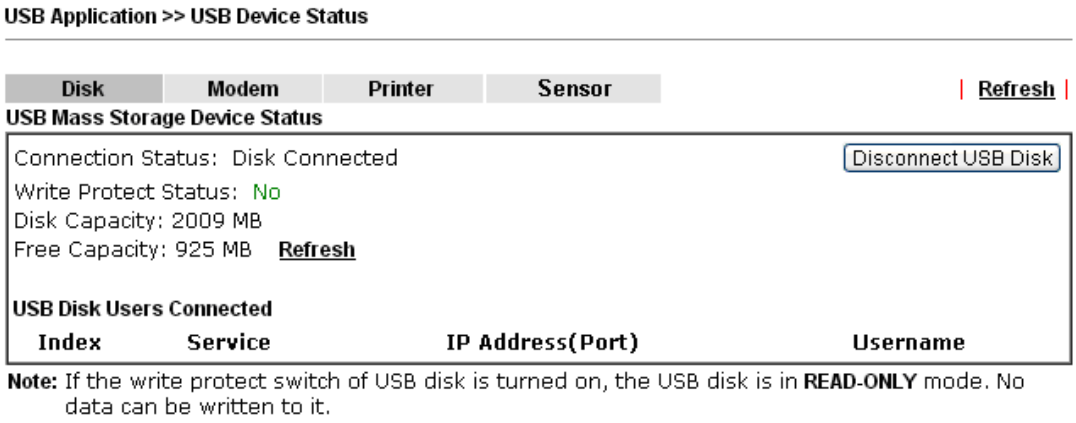
本頁用來監督透過 Vigor 路由器來存取 FTP 或是 Samba 伺服器的使用者狀態，如果您想要從路由器移除 USB 儲存碟，請先按下**中斷 USB 磁碟連線(Disconnect USB Disk)**，然後移除儲存碟。



可用設定說明如下：

項目	說明
連線狀態 (Connection Status)	如果路由器沒有連接任何 USB 儲存碟，此處會顯示"**沒有連接任何磁碟**"("**No Disk Connected**")。
磁碟容量 (Disk Capacity)	顯示 USB 儲存碟的總容量。
可用容量 (Free Capacity)	顯示 USB 儲存碟的目前剩餘的容量。按下**更新頁面(Refresh)**可取得最新的容量資訊。
索引編號 (Index)	顯示使用 USB 儲存碟服務的用戶編號。
IP 位址 (IP Address)	顯示使用 USB 儲存碟服務的用戶的 IP 位址。
使用者名稱 (Username)	顯示使用 USB 儲存碟服務的用戶登入時使用的名稱。

當您將 USB 儲存碟插入 Vigor 路由器時，系統將會在數秒鐘內尋找此裝置。



VIII-2-5 溫度感應器(Temperature Sensor)

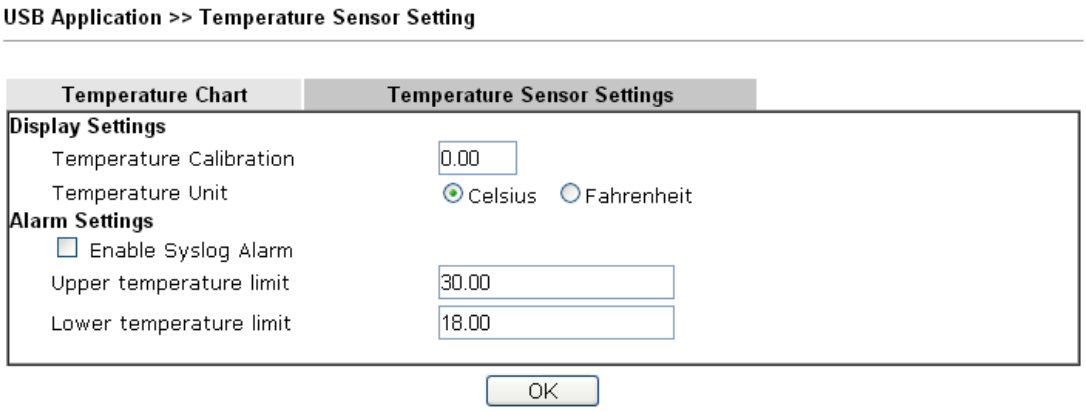
Vigor 路由器允許插入 USB 溫度感應器以便監控環境溫度，如果溫度高於上限或是低於下限時，警示訊息將會發送出去。



尤其是在夏天，確保伺服器或是資料通訊設備有無因冷卻系統失效導致過熱發生，是相當重要的事情。

與 Vigor 路由器相容的溫度計可持續監控周圍環境的溫度，當偵測到已達預先設定的門檻溫度時，系統會透過電子郵件或是簡訊發出警告通知，讓使用者能採取適當的行動。

Temperature Sensor Settings



可用設定說明如下：

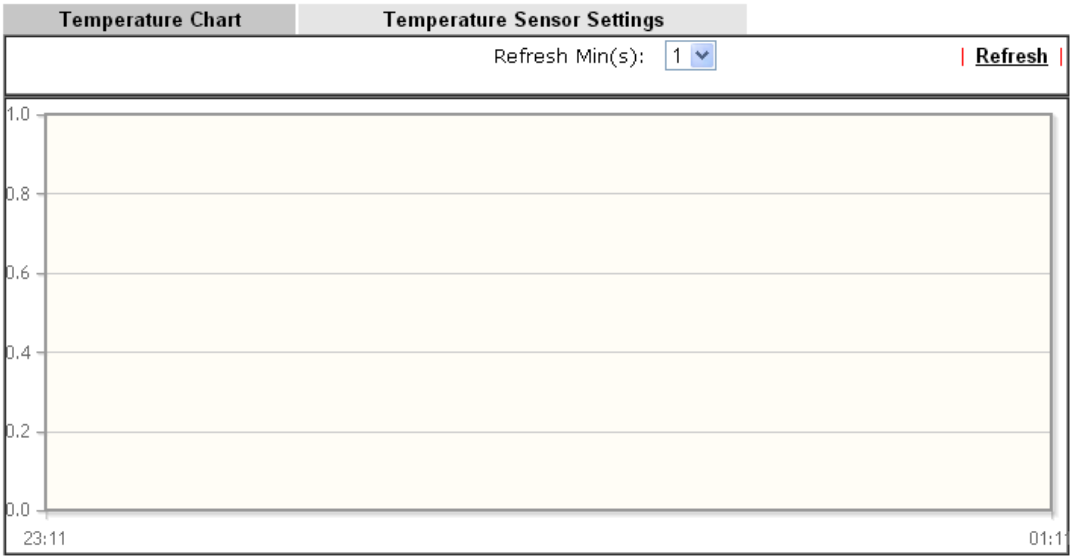
項目	說明
顯示設定	**溫度校對(Temperature Calibration)** - 輸入校正溫度錯誤的數值。 **溫度單位(Temperature Unit) -** 選擇溫度的顯示單位，有二種類型可以選擇。
警示設定	**啓用 Syslog 警示(Enable Syslog Alarm) -** 勾選此框啓用此功能。 **溫度上限/溫度下限(Upper temperature limit/Lower temperature limit)** - 輸入系統傳送溫度警示的上下限溫度。

完成設定之後，請按下**確定(OK)**按鈕儲存。

溫度圖表(Temperature Chart)

下圖爲溫度圖表的範例：

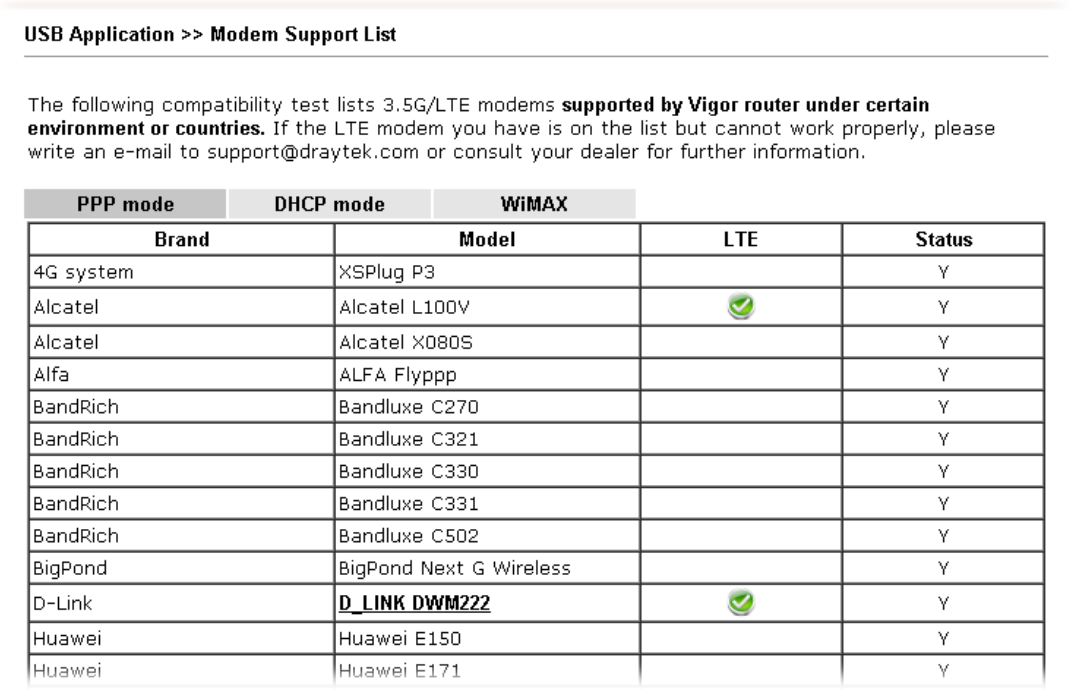
USB Application >> Temperature Sensor Graph



Manufacturer:
Product:
Current Temperature:
Average Temperature:
Maximum Temperature:
Minimum temperature:

VIII-2-6 數據機支援清單(Modem Support List)

本頁提供 Vigor 路由器支援的 USB 數據機的品牌與型號等相關資訊。



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.

PPP mode | DHCP mode | WiMAX

Brand	Model	LTE	Status
4G system	XSPlug P3		Y
Alcatel	Alcatel L100V	✓	Y
Alcatel	Alcatel X080S		Y
Alfa	ALFA Flyppp		Y
BandRich	Bandluxe C270		Y
BandRich	Bandluxe C321		Y
BandRich	Bandluxe C330		Y
BandRich	Bandluxe C331		Y
BandRich	Bandluxe C502		Y
BigPond	BigPond Next G Wireless		Y
D-Link	**D_LINK DWM222**	✓	Y
Huawei	Huawei E150		Y
Huawei	Huawei E171		Y

VIII-2-7 SMB 用戶端支援清單(SMB Client Support List)

此清單提供在不同平台下，檔案分享操作等應用之測試狀態資訊。

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.

應用說明

A-1 如何取得連接至 Vigor 路由器的 USB 裝置內的檔案?

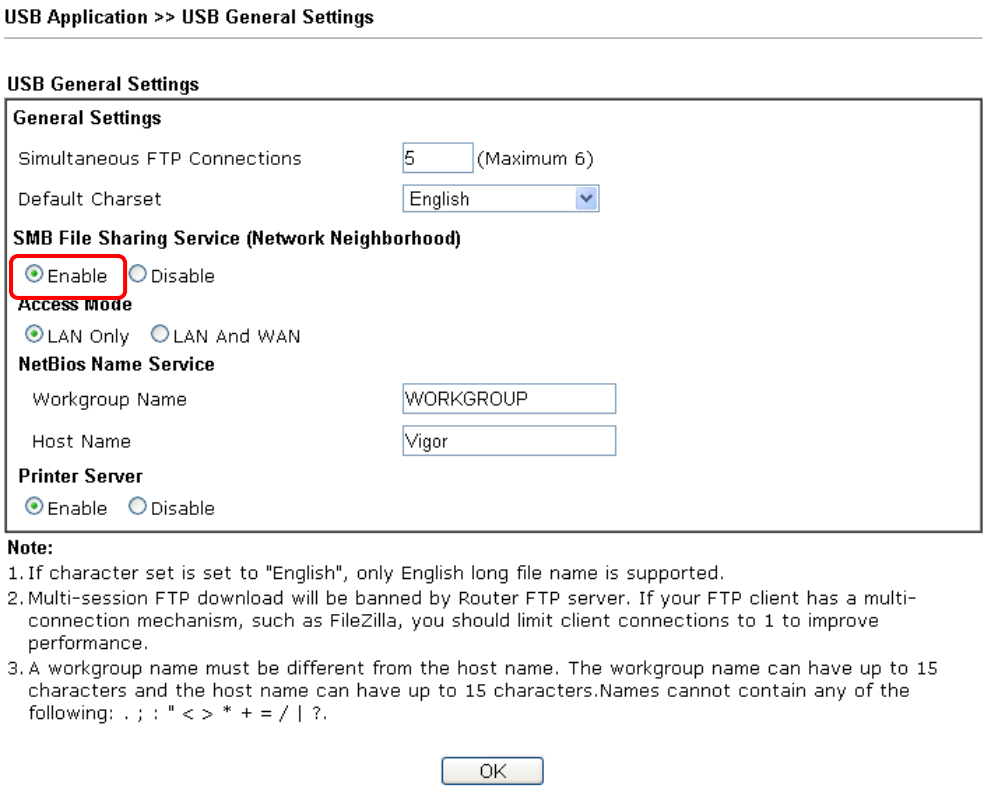
Files on USB storage device can be reviewed by opening **USB Applicaiton>>File Explorer.** If it is necessary for you to delete, copy files on the device or write, paste files to the devcie, it must be done through SMB server or FTP server.

SMB service is based on the original USB FTP service. You will need to setup USB FTP first. We would like to give brief instructions on USB FTP setup here.

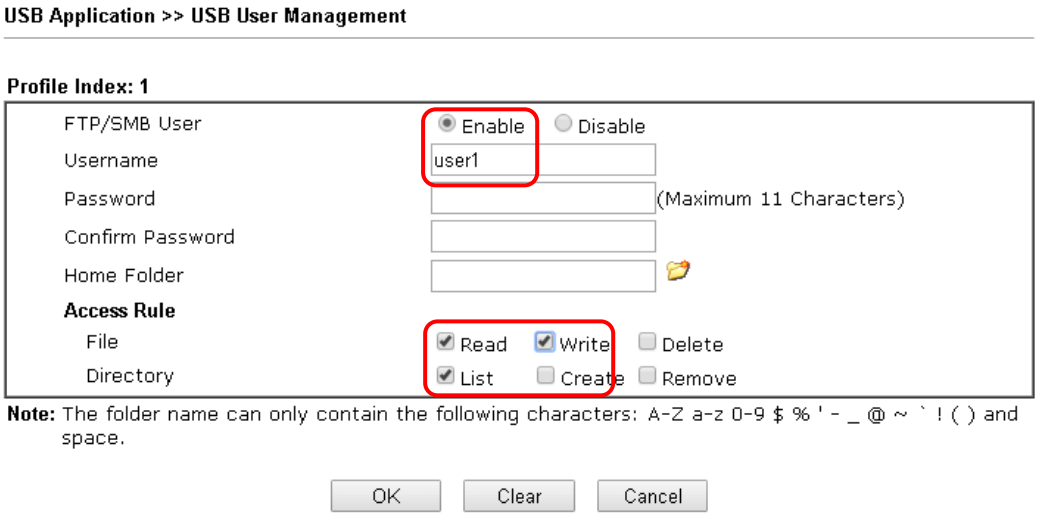
1. 將 USB 裝置連接至路由器的 USB 埠口，務必確認連線狀態欄位中出現**磁碟連線(Disk Connected)**的訊息，如下所示：



2. 開啓 **USB 應用>>USB 基本設定(USB Application >> USB General Settings)**以啓用 SMB 服務，按下**確定(OK)**。

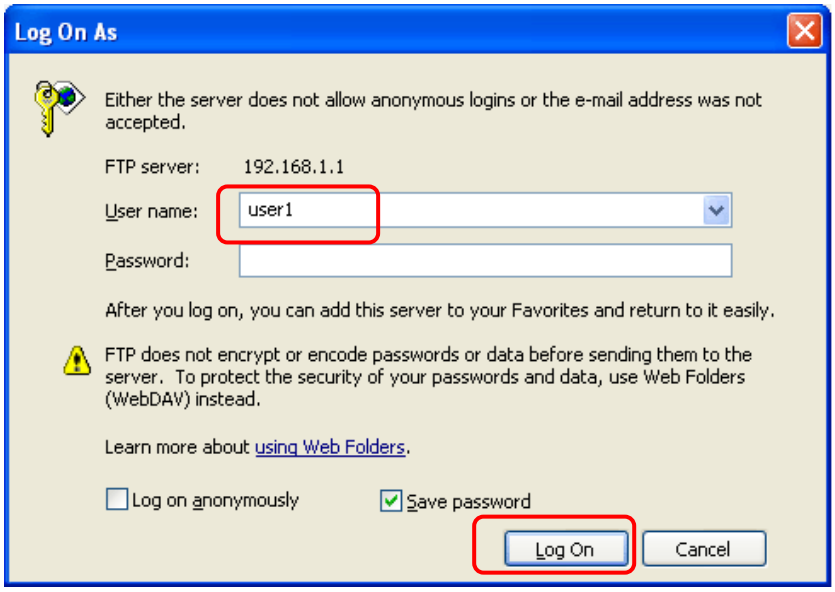


3. **USB 應用>>USB 使用者管理(USB Application >>USB User Management)**設定一組使用 FTP 服務的使用者帳號，按下**啓用(Enable)**以便啓動此 FTP/SMB 使用者帳號，此例我們新增一個名爲 user1 的帳號，給予讀取、覆寫、清單的權限。

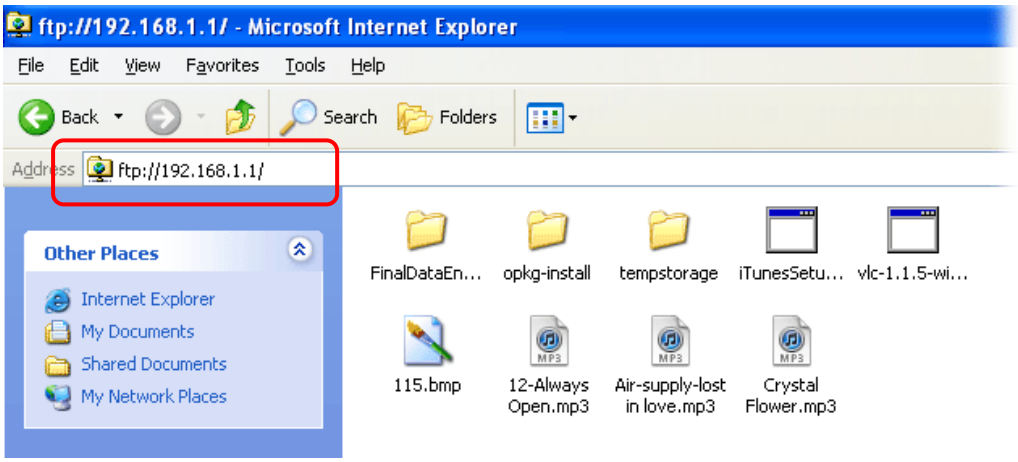


4. 按下**確定(OK)**按鈕儲存設定。

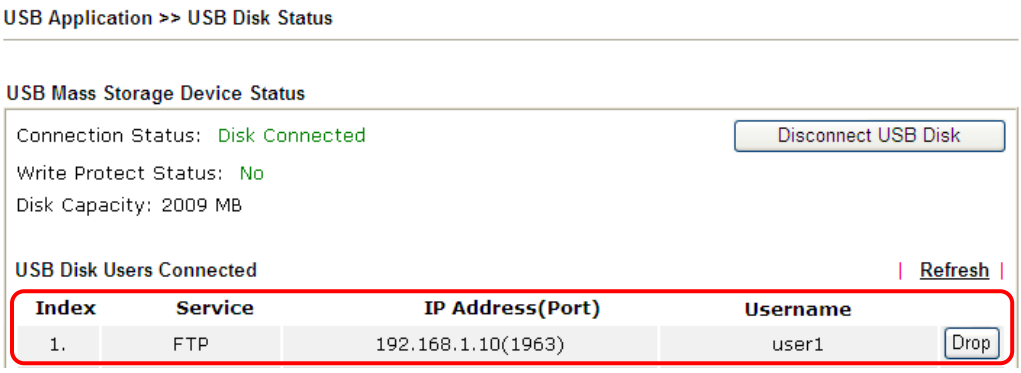
5. 確認 FTP 服務可以順利運作，請開啓任一瀏覽器並鍵入 *ftp://192.168.1.1*。使用帳號 **user1** 來登入。



6. 當下列視窗出現時，即表示 FTP 服務可正常運作。



7. 回到 **USB 應用>>USB 磁碟狀態(USB Application >> USB Disk Status)**，FTP 伺服器資訊將會顯示如下圖：



現在，路由器 LAN 端的使用者可以存取 USB 裝置內容，只要在瀏覽器輸入 ftp://192.168.1.1 即可，使用者可以新增或移除檔案/目錄，相關權限視 **USB 應用>>USB 使用者管理(USB Application >>USB User Management)**中對於 FTP 帳戶設定所做的存取規則而定。

第九篇 故障排除



Troubleshooting

如果安裝並完成路由器設定之後，您無法存取網際網路，本篇可以引導您解決一些異常狀況。

IX-1 自我診斷工具(Diagnostics)

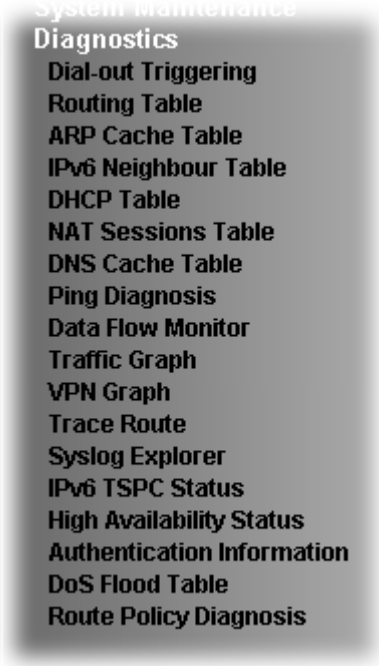
這個章節將會指導您，如何解決在完成安裝和設置路由器後依然無法上網的問題。請按以下方法一步一步地進行檢查。

- 檢查路由器硬體狀態是否正常
- 檢查您電腦的網路連接設置是否正確
- 試試看能否從電腦 ping 到路由器
- 檢查 ISP 的設置是否正常
- 必要的話將路由器恢復至預設出廠設置

如果以上步驟仍無法解決您的問題，您需要聯絡代理商取得進一步的協助。

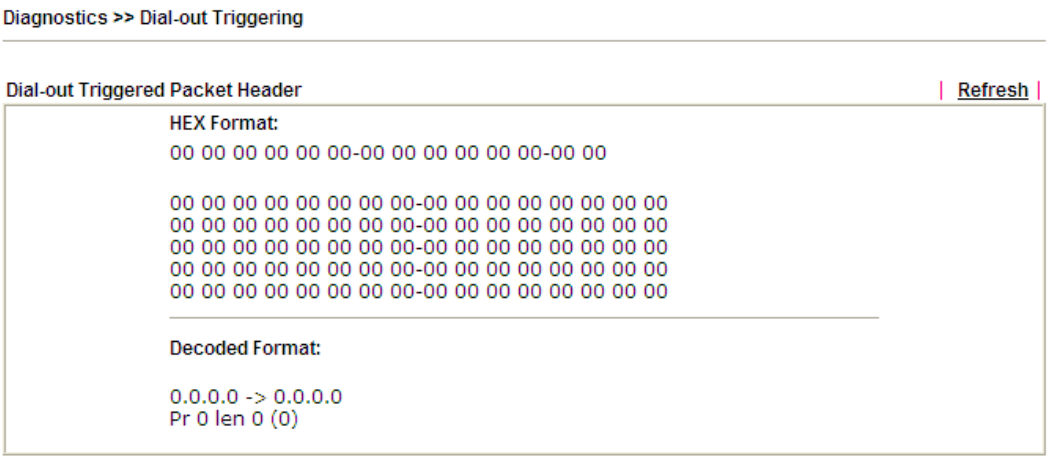
網頁使用者介面

自我診斷工具提供一個非常有效的方式，讓使用者能夠檢視或是診斷路由器的現況。以下爲自我診斷的選單項目：



IX-1-1 撥號觸發器(Dial-out Triggering)

按**自我診斷工具(Diagnostics)**的**撥號觸發器(Dial-out Triggering)**開啓網頁，網際網路連線(如PPPoE)可由來源 IP 位址封包來觸發。



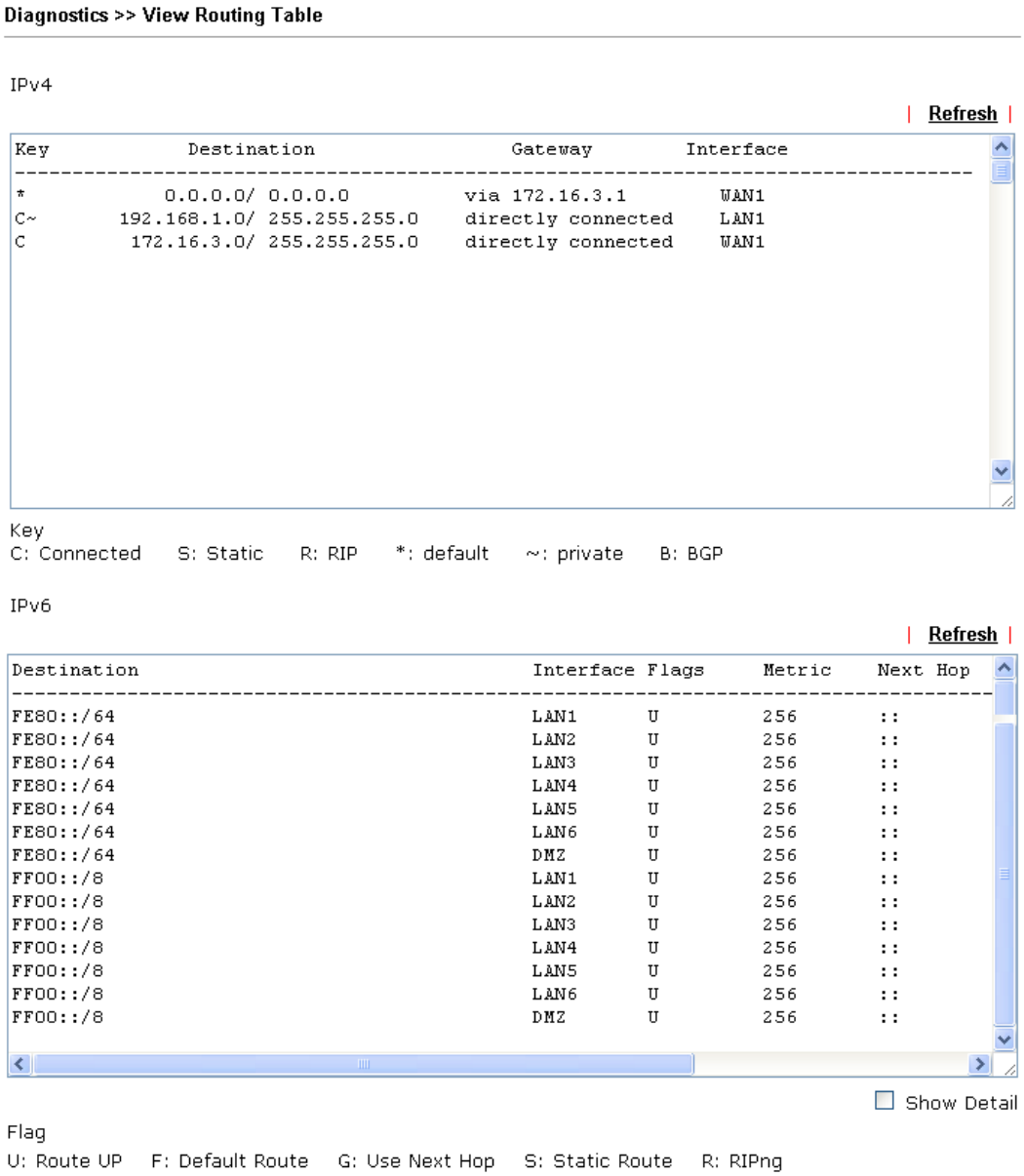
可用設定說明如下：

項目	說明
已解碼格式 (Decoded Format)	顯示來源 IP 位址、目標 IP 位址、通訊協定和封包的長度。

更新頁面 (Refresh)	按此鈕重新載入本頁。

IX-1-2 路由表(Routing Table)

按**自我診斷工具(Diagnostics)**的**路由表(Routing Table)**檢視路由器的路由表格，此表格可提供目前的 IP 路由資訊。

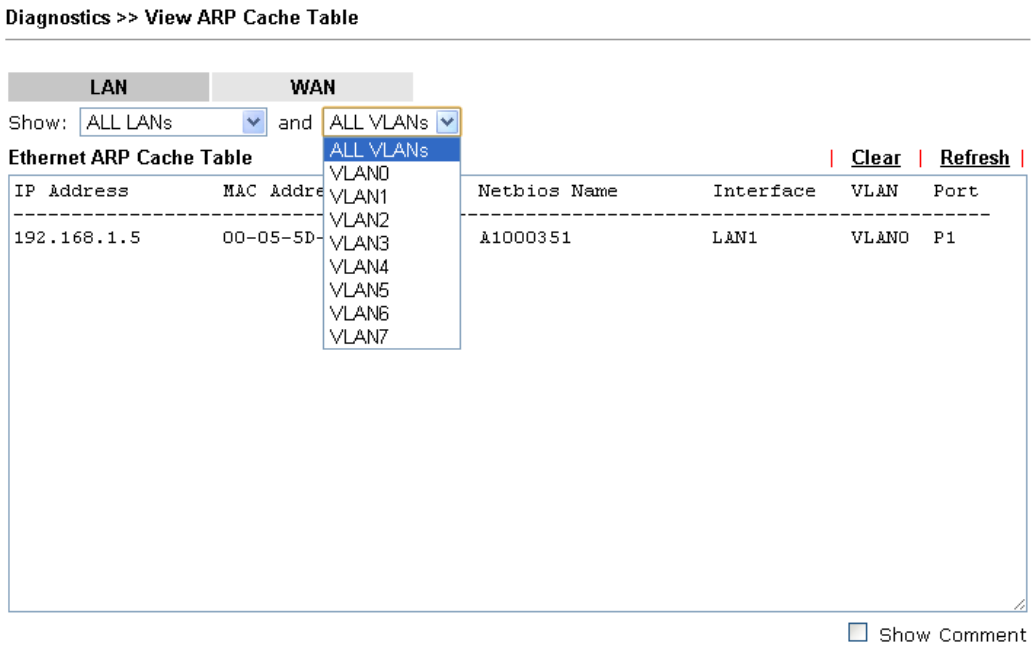


可用設定說明如下：

項目	說明
更新頁面 (Refresh)	按此鈕重新載入本頁。

IX-1-3 ARP 快取表(ARP Cache Table)

按**自我診斷工具(Diagnostics)**的 **ARP 快取表(ARP Cache Table)**檢視路由器中 ARP(Address Resolution Protocol)快取的內容，此表格顯示乙太網路硬體位址(MAC 位址)和 IP 位址間的對應狀況。



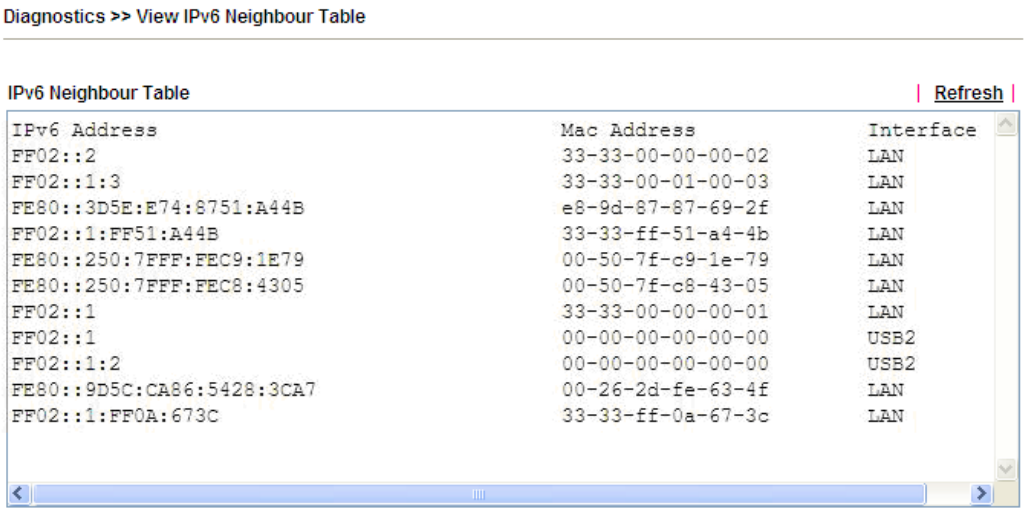
可用設定說明如下：

項目	說明
顯示(Show)	指定 LAN 與 VLAN 顯示相關資訊。 本頁在預設的狀態下將會顯示 LAN 與 VLAN 所有的資訊。
更新頁面 (Refresh)	按此鈕重新載入本頁。

IX-1-4 IPv6 芳鄰表(IPv6 Neighbour Table)

表格顯示乙太網路硬體位址(MAC 位址)與 IPv6 位址之間的對應關係，此項資訊對於診斷網路問題諸如 IP 位址衝突等方面很有幫助。

按**自我診斷工具>> IPv6 芳鄰表(Diagnostics>> IPv6 Neighbour Table)**開啓如下頁面。

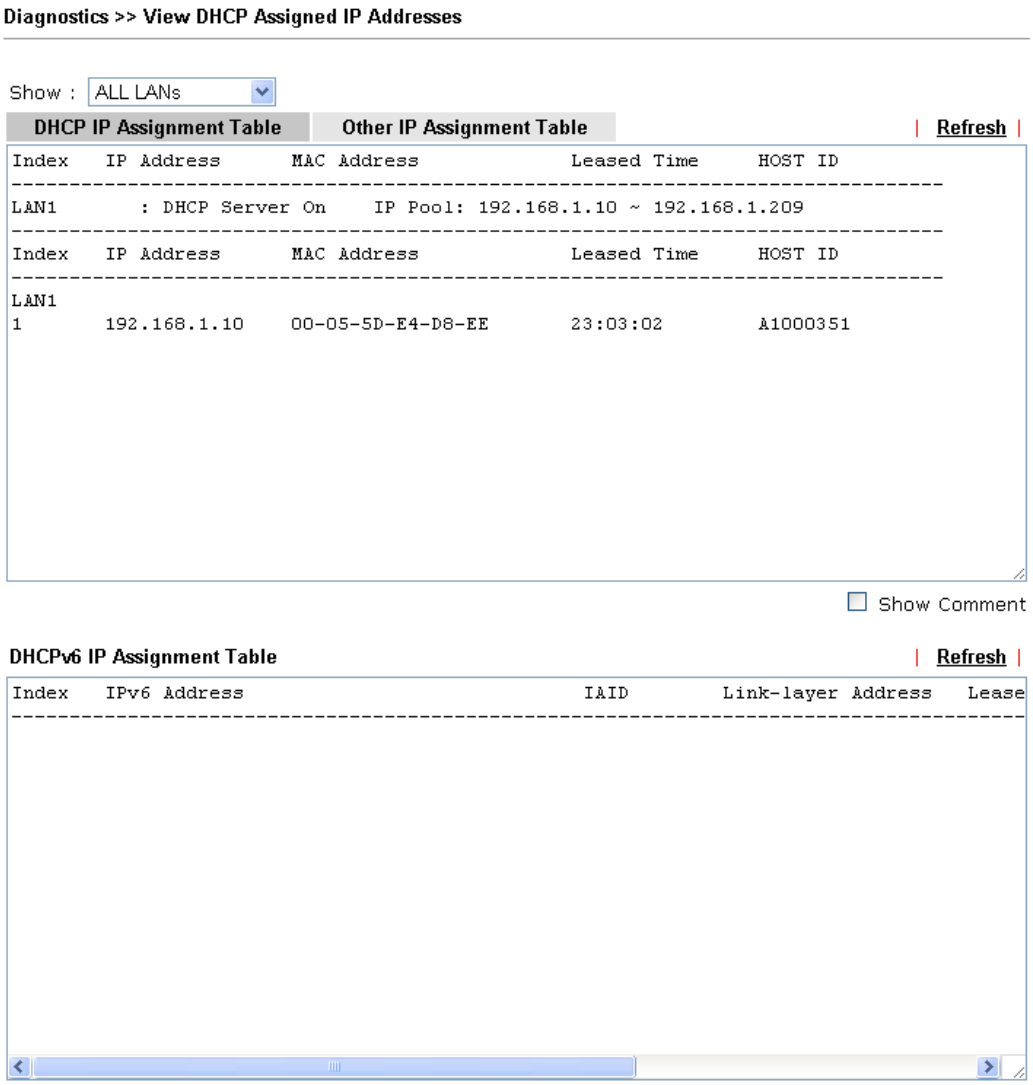


可用設定說明如下：

項目	說明
更新頁面 (Refresh)	按此鈕重新載入本頁。

IX-1-5 DHCP 表(DHCP Table)

此工具提供指派 IP 位址的相關資訊，這項資訊對於診斷網路問題像是 IP 位址衝突等是很有幫助的。按**自我診斷工具(Diagnostics)**，選擇 **DHCP 表(DHCP Table)**開啓相關網頁。

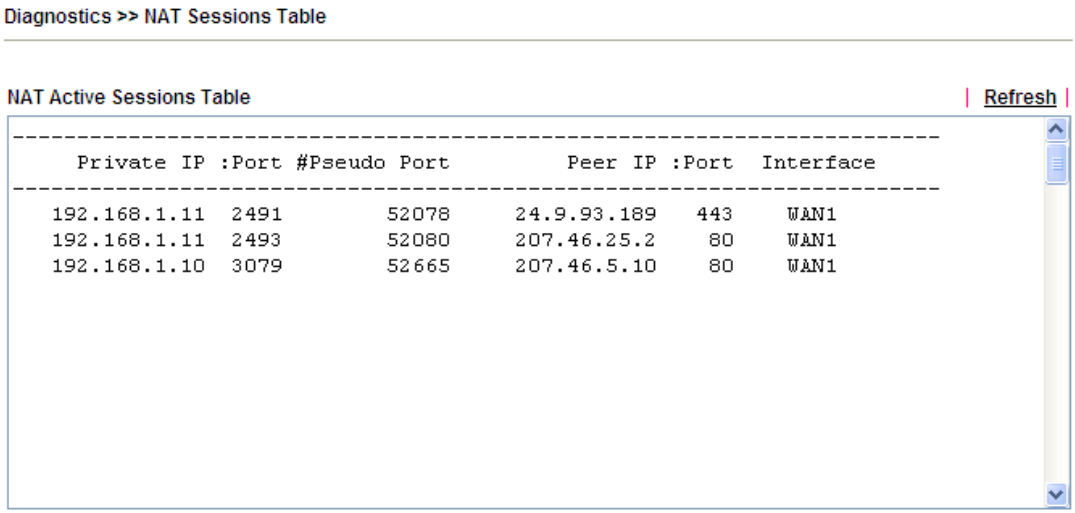


可用設定說明如下：

項目	說明
Index	顯示連線項目編號。
IP Address	顯示路由器指派給特定電腦的 IP 位址。
MAC Address	顯示 DHCP 指派給特定電腦的 MAC 位址。
Leased Time	顯示指定電腦的租約時間。
HOST ID	顯示指定電腦的主機 ID 名稱。
更新頁面 (Refresh)	按此鈕重新載入本頁。

IX-1-6 NAT 連線數狀態表(NAT Sessions Table)

按**自我診斷工具(Diagnostics)**，選擇 **NAT 連線數狀態表(NAT Sessions Table)**開啓相關網頁。



可用設定說明如下：

項目	說明
Private IP:Port	本機電腦的 IP 位址和埠號。
#Pseudo Port	路由器爲了執行 NAT 所使用的暫時通訊埠。
Peer IP:Port	遠端主機的目標 IP 位址與埠號。
Interface	顯示 WAN 連線的介面。
更新頁面 (Refresh)	按此鈕重新載入本頁。

IX-1-7 DNS 快取表(DNS Cache Table)

按下**自我診斷工具>>DNS 快取表 (Diagnostics>>DNS Cache Table)** 開啓設定網頁。

回應 LAN 端的 DNS 詢問的網域名稱與對應 IP 位址記錄，將會儲存在 Vigor 路由器暫存器並顯示於本頁面。

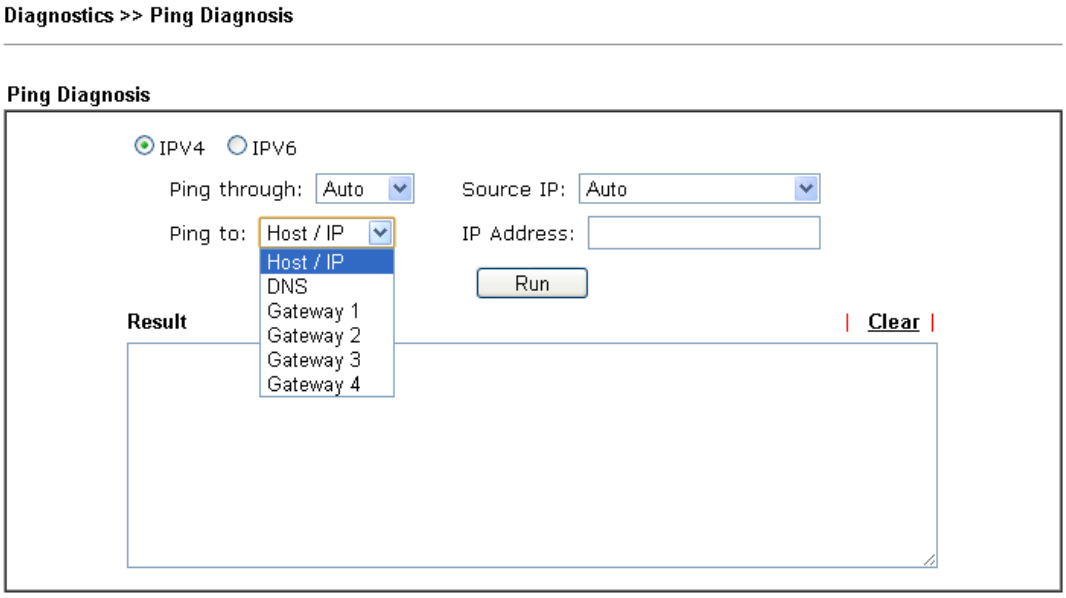


可用設定說明如下：

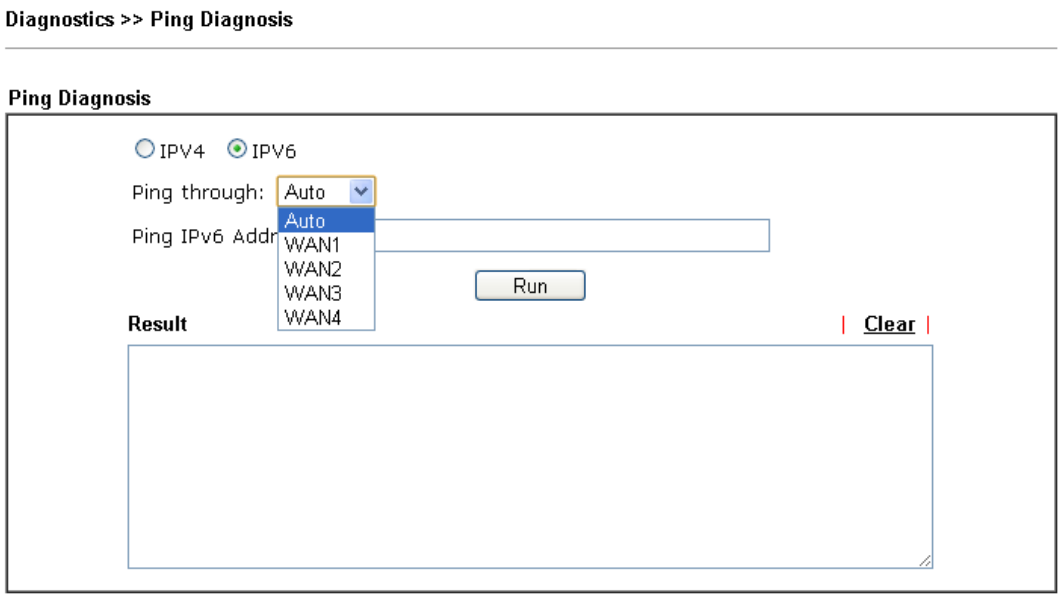
項目	說明
清除(Clear)	按此連結移除畫面上全部的結果。
頁面更新(Refresh)	按此鈕重新載入本頁。
當 TTL 值大於..(When an entry's TTL is larger than....)	勾選此框並輸入 TTL 值，按下確定(OK)按鈕之後，即可啓用此功能。 此數值表示當每個 DNS query 達到 TTL 值，相應的紀錄將自路由器的暫存器中自動刪除。

IX-1-8 Ping 自我診斷(Ping Diagnosis)

按**自我診斷工具(Diagnostics)**，選擇 **Ping 自我診斷(Ping Diagnosis)**開啓相關網頁。



或是



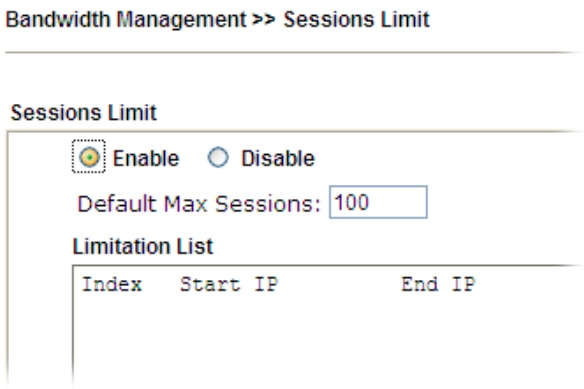
可用設定說明如下：

項目	說明
IPV4 /IPV6	選擇其中一項以便顯示相應的資訊內容。
Ping 經由(Ping through)	使用下拉式清單選擇您想要 Ping 經由的 WAN/LTE 介面。

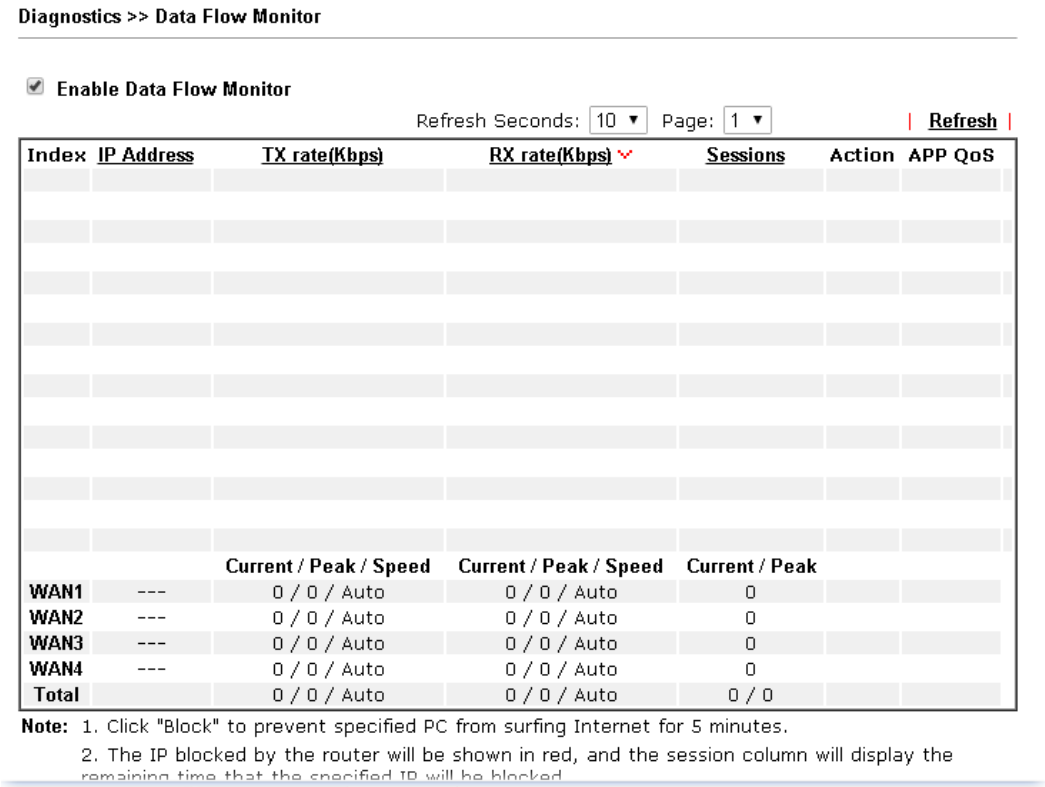
Ping 至(Ping to)	使用下拉式清單選擇您想要 Ping 的目標。
IP 位址 (IP Address)	輸入您想要 Ping 的主機/IP 上的 IP 位址。
Ping IPv6 位址 (Ping IPv6 Address)	輸入您想要 Ping 的主機/IP 上的 IPv6 位址。
執行(Run)	按此鈕啓動 Ping 作業，結果將會顯示在螢幕上。
清除(Clear)	按此連結清除視窗上的結果。

IX-1-9 資料流量監控(Data Flow Monitor)

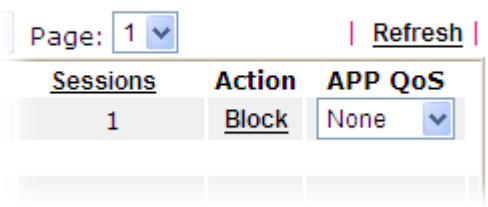
本頁顯示所監視的 IP 位址執行的過程，並在數秒的間隔後重新更新頁面，此處所列出的 IP 位址是在頻寬管理中設定完成的，在啓動資料流量監控之前，您必須啓動 IP 頻寬限制以及 IP 連線數限制。若沒有這麼做的話，系統會出現知會畫面提醒您先啓動相關設定。

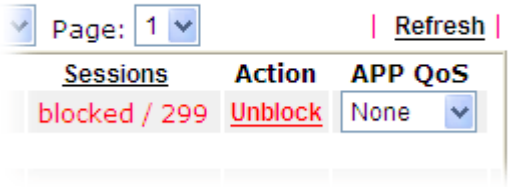
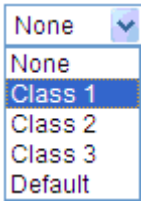


按**自我診斷工具(Diagnostics)**，選擇**資料流量監控(Data Flow Monitor)**開啓相關網頁。您可按下 **IP 位址**、**傳送速率**、**接收速率**或是 **NAT 連線數(IP Address**, **TX rate**, **RX rate** 或 **Session)**來排列資料。



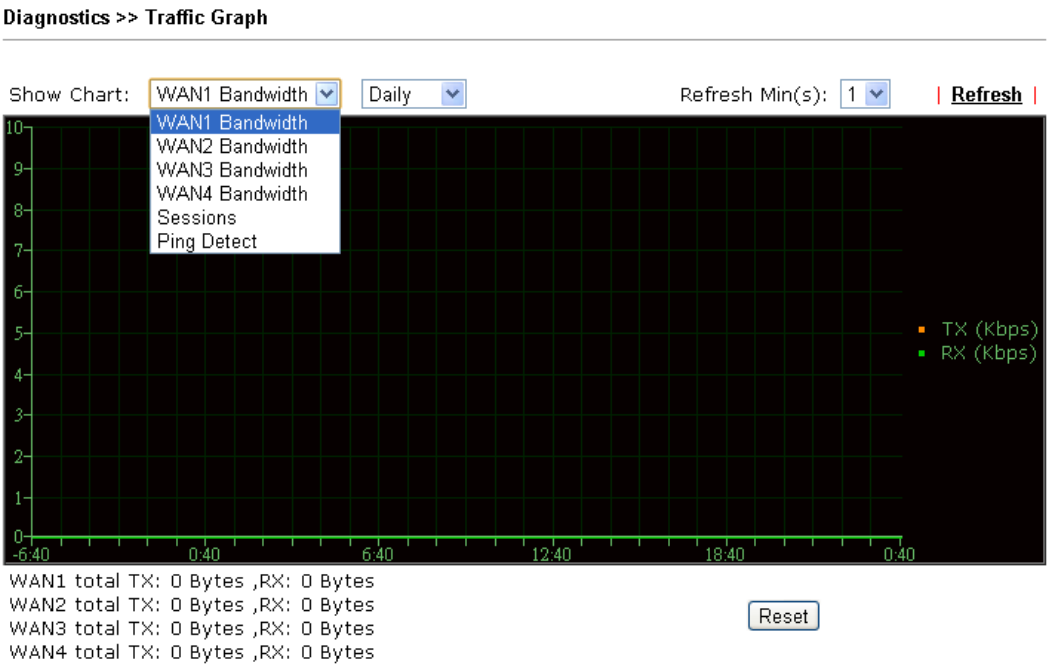
可用設定說明如下：

項目	說明
啓用資料流量監控 (Enable Data Flow Monitor)	勾選此方塊以啓動此功能。
更新秒數(Refresh Seconds)	使用下拉式選項選擇系統自動更新資料的間隔時間。
更新頁面(Refresh)	按此連結更新本頁。
索引編號(Index)	顯示資料流量的項目筆數。
IP 位址(IP Address)	顯示被監視裝置的 IP 位址。
傳送速率 (kbps) (TX rate (kbps))	顯示被監視裝置的傳送速率。
接收速率 (kbps) (RX rate (kbps))	顯示被監視裝置的接收速率。
NAT 連線數(Sessions)	顯示您在連線數限制網頁中所設定的連線數。
動作(Action)	**封鎖(Block)** – 可以避免指定電腦在 5 分鐘內存取網際網路。  **解除(Unblock)** – 指定 IP 位址的裝置將在五分鐘內封鎖起來，

	剩餘時間將顯示在 NAT 連線數欄位中。按下此鈕可以取消封鎖 IP 位址。 
APP QoS	使用下拉式清單選擇指定 IP 位址的資料傳輸的優先順序。 
現值/高峰值/速度 (Current /Peak/Speed)	**現值(Current)**表示目前 WAN 介面的傳輸速率與接收速率。 **高峰值(Peak)**表示路由器在資料傳輸上所檢測到的最高數值。 **速度(Speed)**表示 **WAN>>基本設定(WAN>>General Setup)**中所指定的線路速度，如果您未指定任何速率，這邊將顯示自動，以說明速率由系統自行指定。

IX-1-10 流量圖表(Traffic Graph)

按**自我診斷工具(Diagnostics)**，選擇**流量圖表(Traffic Graph)**開啓相關網頁。可以選擇**WAN1/WAN2/WAN3 頻寬**、**連線數**、**每日**、**每週**來檢視流量圖表。按下**重新設定(Reset)**可以將累計的傳送/接收資料全部歸零。您可隨時按**更新頁面(Refresh)**重新顯示圖表內容。

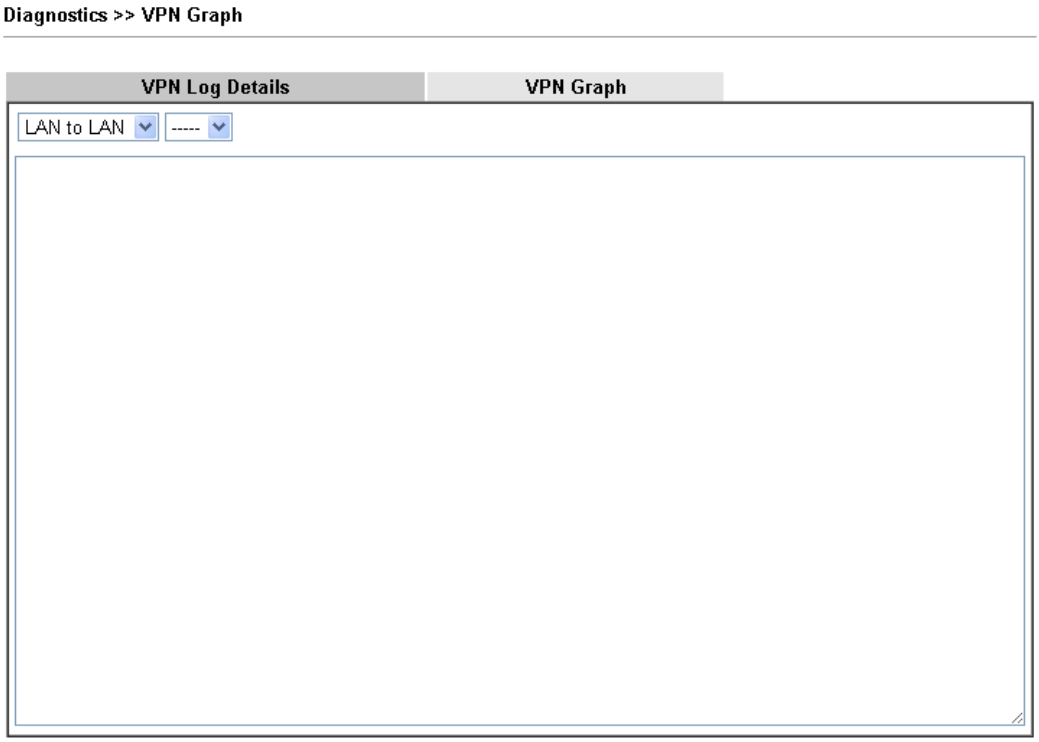


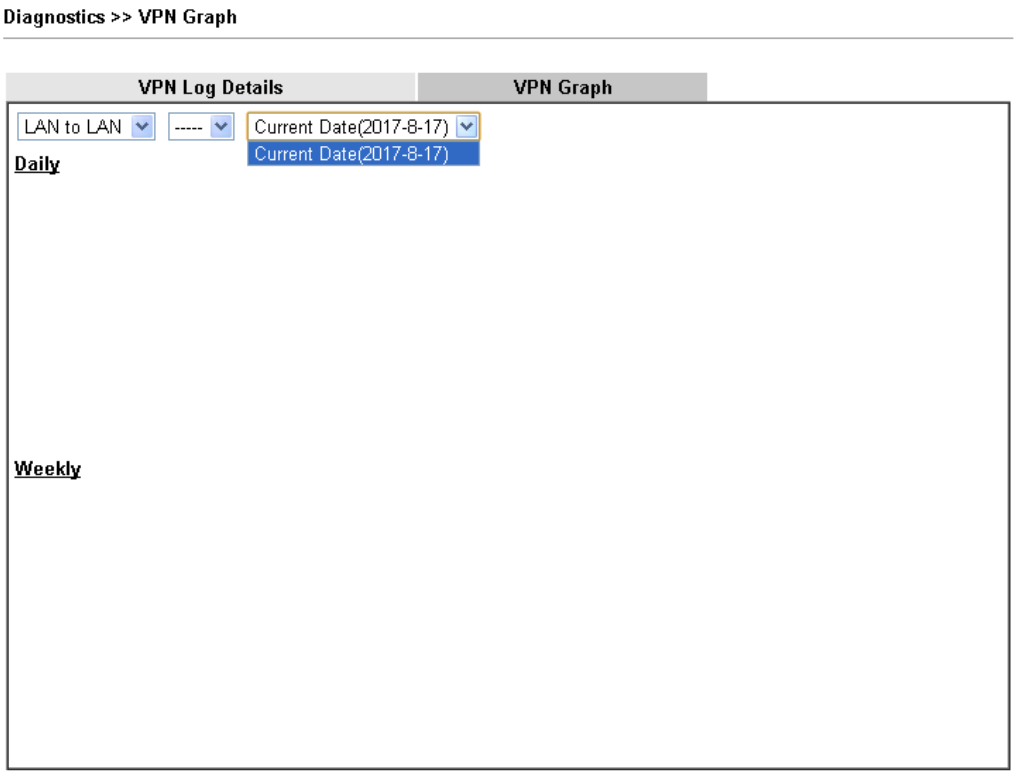
水平軸代表時間；而垂直軸代表的意義就很不同了。對 WAN1/WAN2/WAN3/LTE/WAN4 頻寬圖表而言，垂直軸代表的是過去所傳送與接收封包的數量。

但對連線數圖表來說，垂直軸代表的是過去一段時間之內的 NAT 連線數。

IX-1-11 VPN 圖表(VPN Graph)

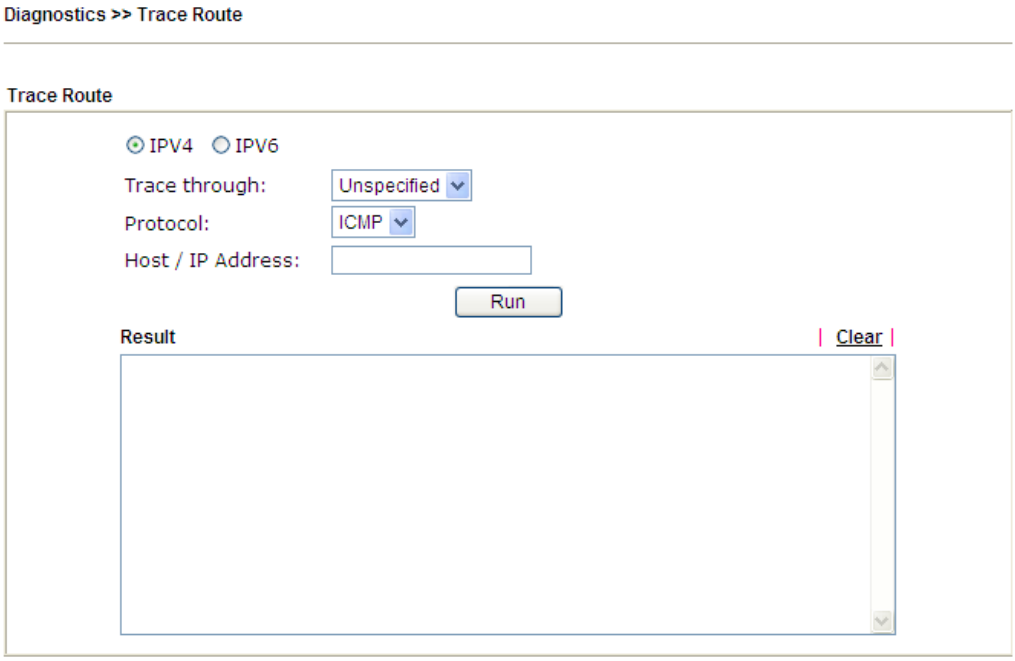
按**自我診斷工具(Diagnostics)**，選擇 **VPN 圖表(VPN Graph)**開啓相關網頁。



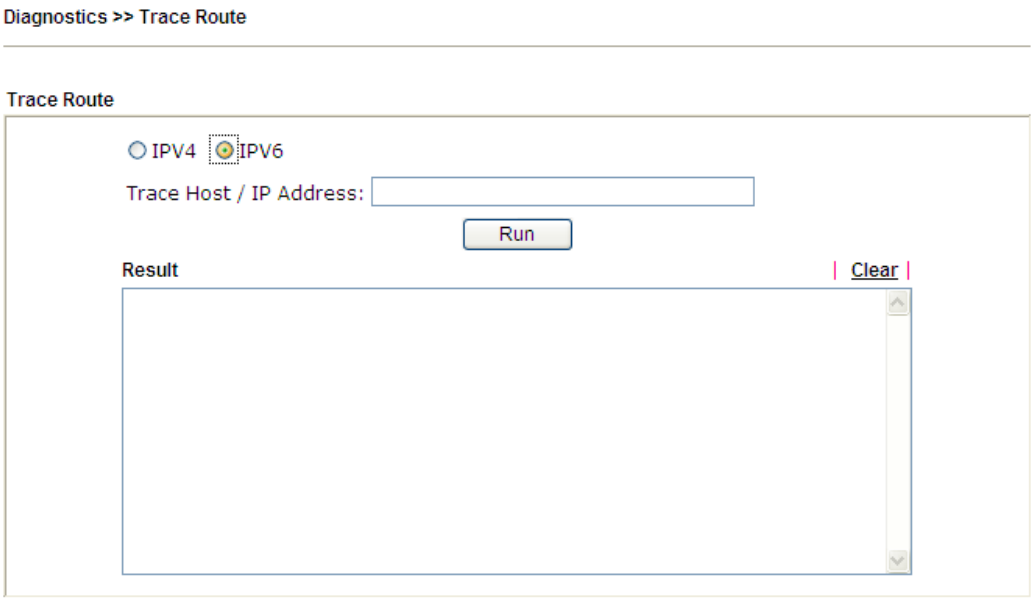


IX-1-12 追蹤路由(Trace Route)

按下**診斷工具(Diagnostics)**，選擇**追蹤路由(Trace Route)**開啓相關網頁。本頁允許您追蹤路由器至主機之間的路由情況，只要簡單的輸入主機的 IP 位址並按下**執行(Run)**按鈕，整個路由狀況都將顯示在螢幕上。



或是



可用設定說明如下：

項目	說明
IPv4 / IPv6	選擇其中一項以便顯示相應的資訊內容。
經由介面(Trace Through)	使用下拉式清單選擇您想要經由其處來追蹤的 WAN 介面，或使

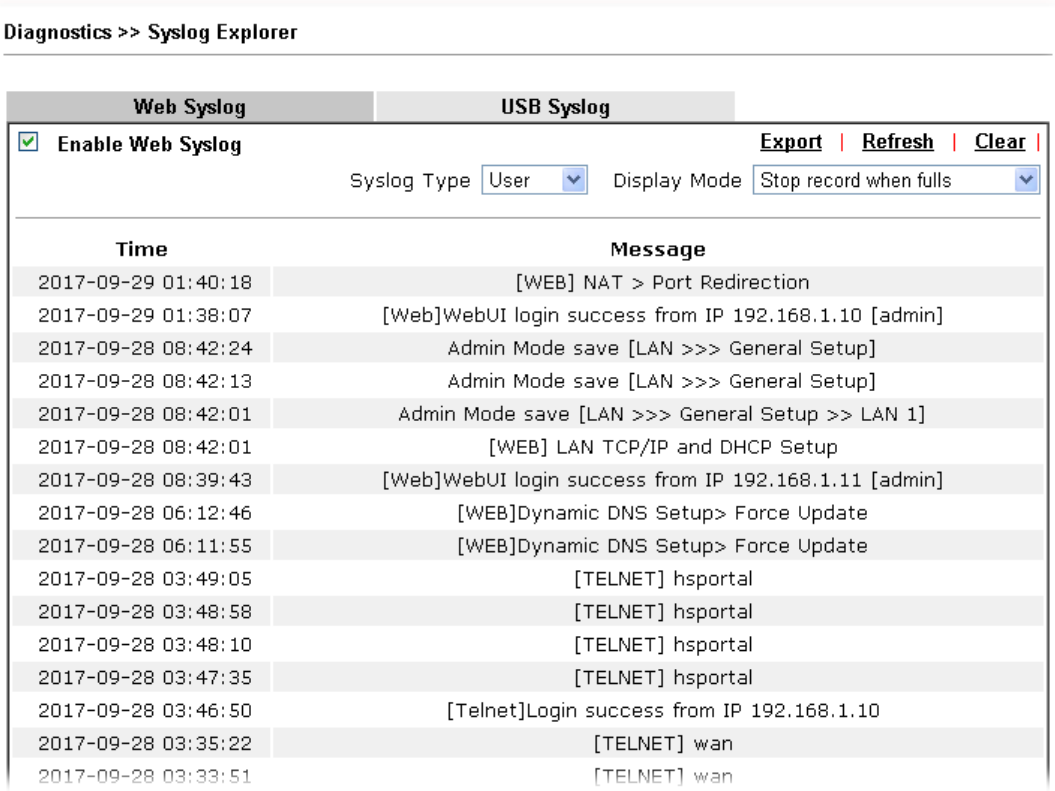
	用**不指定**讓路由器自動決定選擇哪一種介面。
通訊協定(Protocol)	使用下拉式清單選擇您想要通訊協定。
主機/IP 位址 (Host/IP Address)	指明主機的 IP 位址。
追蹤主機/IP 位址 (Trace Host/IP Address)	指明主機的 IPv6 位址。
執行(Run)	按此鈕開始路由追蹤動作。
清除(Clear)	按此連結刪除視窗上的結果。

IX-1-13 Syslog 系統資源管理 (System Explorer)

本頁提供即時的 Syslog 並且在頁面上顯示相關資訊。

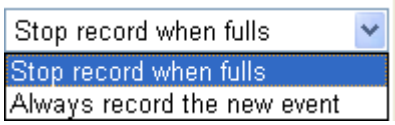
針對網頁 Syslog

本頁顯示使用者/防火牆/電話/WAN/VPN 等設定的時間與訊息，您可以勾選啓用網頁 Syslog 方塊，指定 Syslog 的類型，並選擇顯示的模式。之後，特定類型事件的 Syslog 資料將會顯示於頁面上。



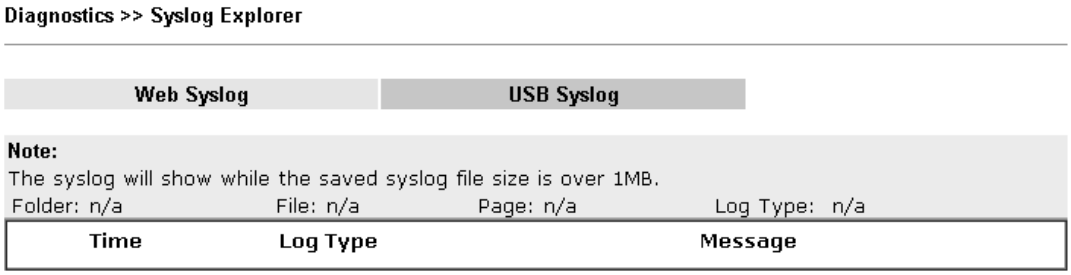
可用設定說明如下：

項目	說明
啓用網頁 Syslog (Enable Web Syslog)	勾選此方塊可啓動網頁 Syslog 記錄功能。
Syslog 類型 (Syslog Type)	使用下拉式清單指定準備顯示出來的 Syslog 的類型。

	
輸出 (Export)	按下此連結可以將本頁紀錄的內容儲存成檔案。
更新頁面 (Refresh)	按下此連結可以手動更新本頁紀錄的內容。
清除 (Clear)	按下此連結可以清除本頁紀錄的內容。
顯示模式 (Display Mode)	有二種模式可以選擇：  **滿碟時停止紀錄(Stop record when fulls) -** 當 syslog 的容量已滿，系統將停止紀錄。 **永遠紀錄最新事件(Always record the new event)-** 系統只紀錄最新的事件。
時間 (Time)	顯示事件發生的時間。
訊息 (Message)	顯示事件發生的相關資訊。

針對 USB Syslog

本頁顯示暫存在 USB 儲存碟內的 Syslog 紀錄。



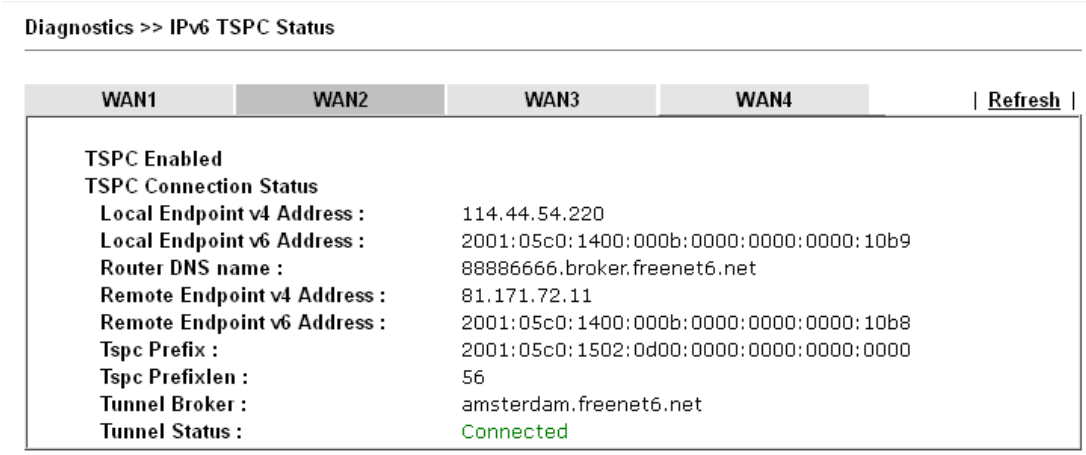
可用設定說明如下：

項目	說明
時間(Time)	顯示事件發生的時間。
紀錄類型(Log Type)	顯示紀錄的類型。
訊息(Message)	顯示事件發生的相關資訊。

IX-1-14 IPv6 TSPC 狀態(IPv6 TSPC Status)

IPv6 TSPC 狀態頁面可以幫助您診斷 TSPC 的連線狀態是否正常。

如果 TSPC 設定無誤，當使用者成功連上通道的時候，路由器將會顯示如下頁面：



可用設定說明如下：

項目	說明
更新頁面 (Refresh)	按下此連結可以手動更新本頁紀錄的內容。

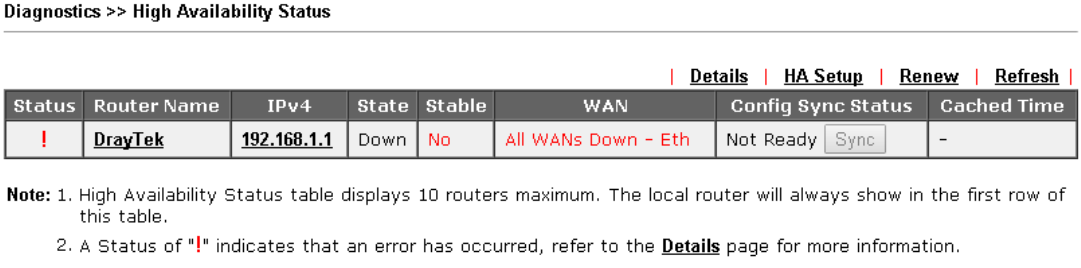
IX-1-15 高可靠度狀態(High Availability Status)

您可以透過此頁檢視相同 DARP (DrayTek Address resolution Protocol)群組下的路由器相關資訊，不過只有部分的路由器狀態會顯示出來。

凡是含有下述條件的 Vigor 路由器皆可視之爲位於相同 DARP 群組

- 啓用高可靠度(HA)功能
- 具有相同 Redundancy 方式
- 相同的群組 ID
- 相同的認證密鑰
- 相同的管理介面

開啓**自我診斷>>高可靠度狀態(Diagnostics>High Availablity Status)**。



可用設定說明如下：

項目	說明
細節/上一頁 (Details/Back)	**細節(Details) -** 按此連結顯示 HA 設定內容狀態。 **上一頁(Back) -** 回到前一個頁面。
HA 設定(HA Setup)	按此連結開啓**應用>>高可靠度(Applications>>High Availability)** 頁面進行設定修正。
更新(Renew)	按此連結取得其他路由器的最新的狀態(主要路由器除外)。
頁面更新(Refresh)	按此連結取得主要路由器的最新狀態。
狀態(Status)	**"!"** 表示有錯誤發生，請參考**細節(Detailed)** 資訊，如有必要則修改 HA 設定。
路由器名稱(Router Name)	顯示此裝置的名稱。
IPv4	顯示路由器的 IPv4 位址。
狀況(State)	"Down" 表示 HA 功能停用了。 "Primary" 表示此路由器在 HA 中代表主要路由器。 "Secondary" 表示此路由器在 HA 中代表次要路由器。
穩定度(Stable)	"No" 表示尚未決定好主要路由器爲何，DARP 仍在處理中。 "YES" 表示已經決定好主要路由器。
WAN	"At Least One UP" 表示至少有一組 WAN 介面連接至網際網路。 "All WANs Down" 表示沒有 WAN 介面連接至網際網路。
設定同步狀態 (Config Sync Status)	"Not Ready" 表示設定同步無法啓用，或是設定同步停用中，或是同步初始化失敗。 "Ready" 表示可準備實施設定同步。 "Progressing" 表示設定同步運作中。 "Fail" 表示設定同步執行但失敗；或是型號名稱有誤。 "Equal" 表示相關設定與主要路由器相同。
快取時間(Cached Time)	顯示上次取得其他路由器最新狀態的時間(主要路由器除外)。

按下 **Status**, **Router Name**, **IPv4** 或 **Details** 等連結，下述頁面將會顯示在螢幕上。

Diagnostics >> High Availability Status >> Details

[Local Router] | Back | HA Setup | Renew | Refresh |

DrayTek			192.168.1.1(FE80::21D:AAFF:FEC6:4C40)	
State	**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:c6:4c:40	**HTTPs Port**	443
Model	Vigor2925Vac	**Firmware Version**	3.8.4_RC6c
Country Code	17 (Spain)		
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
		DMZ	FE80::200:5EFF:FE00:101
Enable Config Sync	Off	**Config Sync Interval**	0 Day 0 Hour 15 Minute

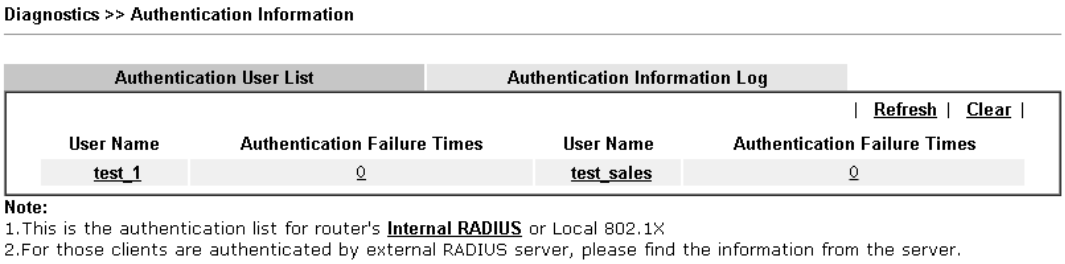
Note:
Displays up to 10 routers. Each router can show up to 7 Virtual IPs.

IX-1-16 認證資訊 (Authentication Information)

認證使用者清單

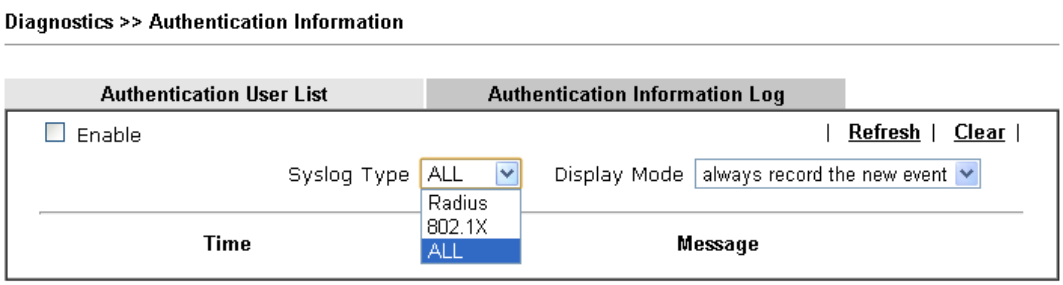
此頁面顯示內部 RADIUS 或是 Local 802.1X 所執行個認證事務。

當滑鼠游標移至使用者名稱下方的連結，關於內部 RADIUS 或是 Local 802.1X 服務之連線訊息(包含認證失敗資訊)將以跳出對話盒顯示在螢幕上。



認證資訊日誌

本頁將顯示完整的認證日誌資訊。



可用設定說明如下：

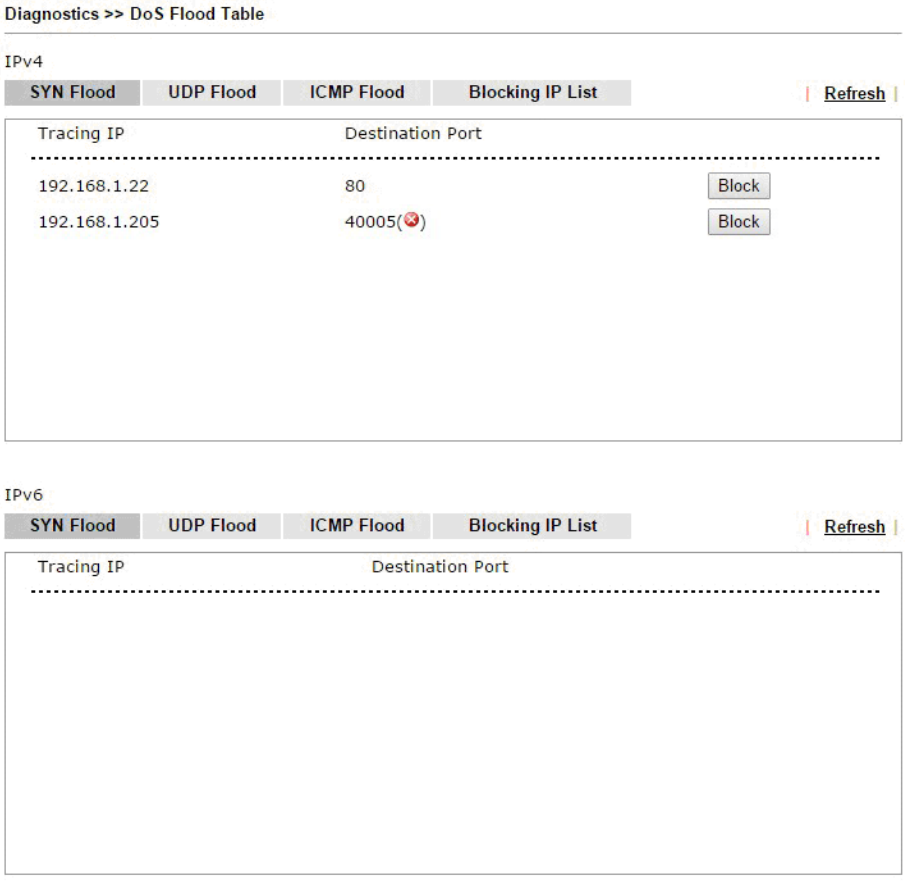
項目	說明
啓用(Enable)	勾選此方塊啓用此功能。
頁面更新(Refresh)	按此連結更新目前頁面。
清除(Clear)	按此連結清除全部紀錄。
Syslog 類型(Syslog Type)	指定 RADIUS、802.1X 或是 All 以顯示相關的認證資訊日誌。
顯示模式(Display Mode)	選擇您想要顯示之模式的相關資訊於表格中。 ● **滿碟時停止紀錄(Stop record when fulls) -** 當 syslog 的容量已滿，系統將停止紀錄。 ● **永遠紀錄最新事件(Always record the new event)-** 系統只紀錄最新的事件。
時間(Time)	顯示使用者認證的時間。
訊息(Message)	顯示認證完成資訊。

IX-1-17 DoS Flood 表格(DoS Flood Table)

本頁顯示 DoS Flooding Defense 機制偵測出的 IP 連線內容，對於網路工程師來說，這項工具有助於檢驗網路環境以期發現有無異常連線

系統可檢測並分別呈現用於 SYN Flood、UDP Flood 與 ICMP Flood 攻擊的 IP 追蹤與目的埠號資訊於不同的頁面上。

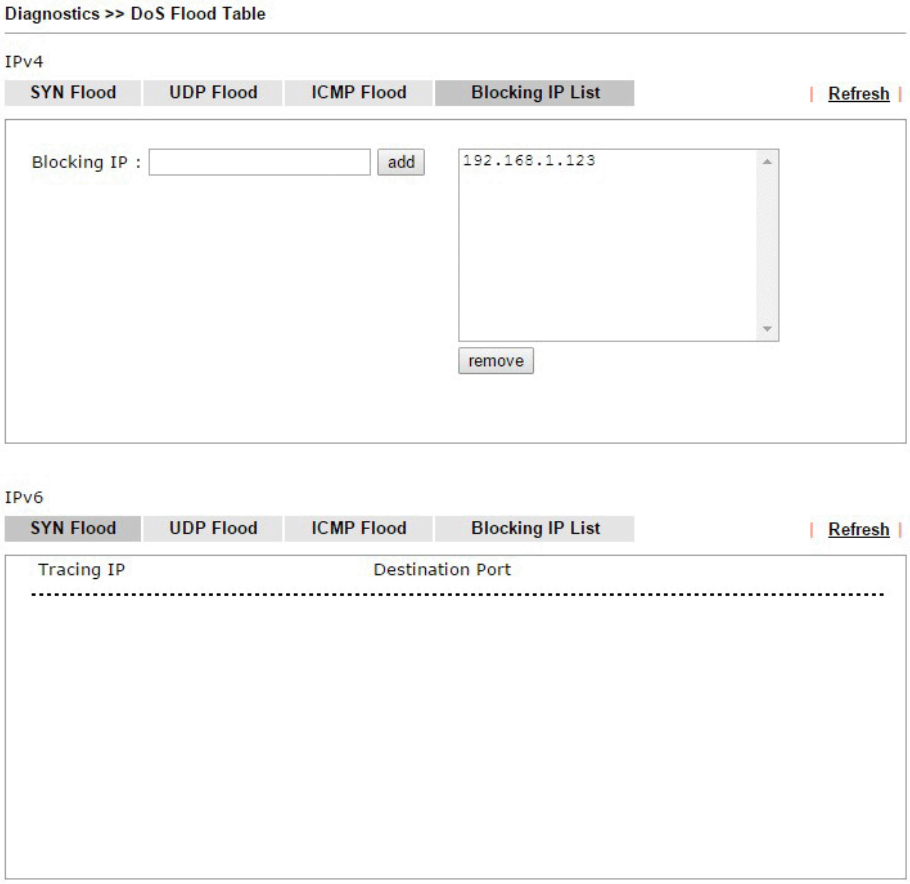
此外，被偵測出可能攻擊網路系統的 IP 位址可以透過 SYN Flood, UDP Flood 與 ICMP Flood 標籤頁面的 Block 按鈕暫時封鎖。



資訊

圖示 - ( )- 表示該 IP 位址出了些問題 (例如攻擊系統等)。

但是，若 IP 位址因其異常行爲之故，而被封鎖住，可以按下 Blocking IP List 標籤好讓該 IP 永遠封鎖起來。例如 IP 位址“192.168.1.123” (顯示在下方圖中)由系統將其永遠封鎖起來。

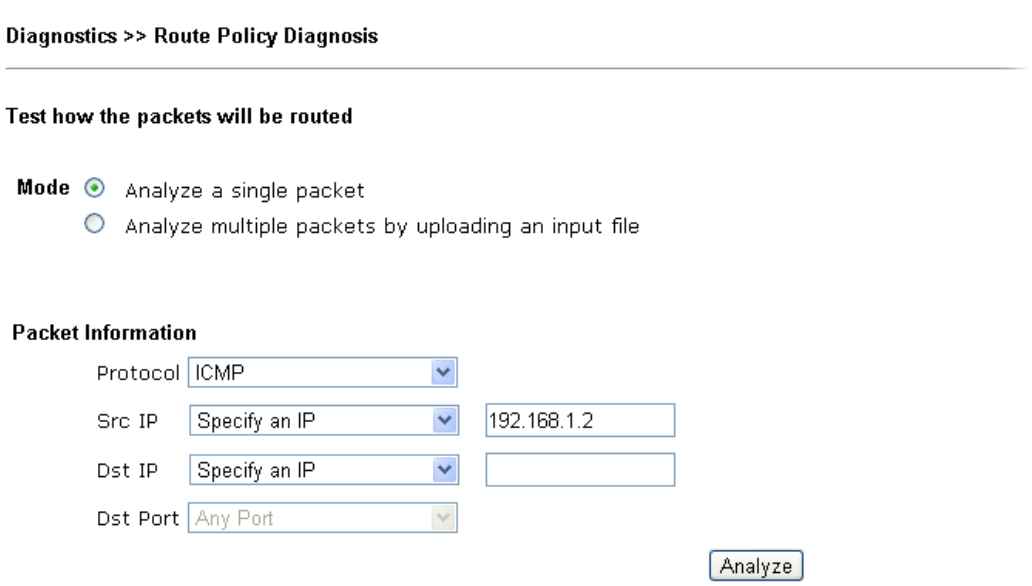


可用設定說明如下：

項目	說明
封鎖 IP(Blocking IP)	輸入 IP 位址並按下**新增(add)**，新輸入的內容將會出現在右邊方框內。 右邊方框的 IP 清單可由路由器系統長久封鎖。 **移除(Remove)** – 移除封鎖 IP 清單中選定的 IP 位址。
頁面更新(Refresh)	按此連結更新目前頁面。

IX-1-18 路由策略診斷(Route Policy Diagnosis)

透過本頁所做的分析內容，可以輕易追蹤傳送至路由器的封包可能的路徑(固定路由、路由表格或是策略路由)。



可用設定說明如下：

項目	說明
模式(Mode)	**分析單一封包(Analyze a single packet)** – 路由器可利用路由策略分析被傳送之單一封包。 **分析多重封包(Analyze multiple packets...)** - 路由器可利用路由策略分析特定檔案中被傳送的多重封包。
封包資訊(Packet Information)	指定由路由器進行分析的封包本質。 **ICMP/UDP/TCP/ANY-** 指定診斷的通訊協定。 **Src IP** – 輸入 IP 位址作爲來源 IP。 **Dst IP** – 輸入 IP 位址作爲目標 IP。 **Dst Port** – 使用下拉式清單指定目標埠號。 **Analyze** – 按此鈕執行分析任務，分析結果會顯示在頁面上。
輸入檔案(Input File)	這個功能只有在選擇**分析多重封包(Analyze multiple packets...)**爲模式時可用。 **選擇(Select)** – 按下下載連結以便取得空白範例檔案，接著按此按鈕選擇 csv 檔案以儲存分析結果。



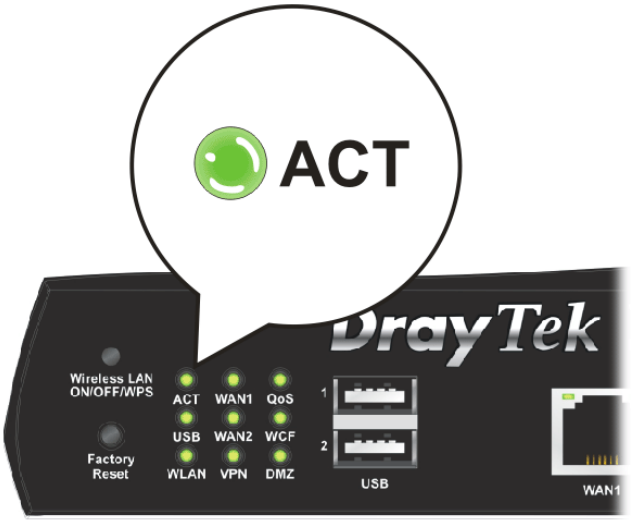
分析(Analyze) – 按此執行分析任務，分析結果將會顯示在頁面上，如有需要，可按**輸出分析(export analysis)**按鈕將結果以檔案方式輸出。



IX-2 檢查路由器硬體狀態是否正常

檢查路由器硬體狀態是否正常

1. 檢查電源線以及 LAN 的連接。詳細資訊請參考“**I-2 硬體安裝**”。
2. 開啓路由器，確認 **ACT** 指示燈差不多每秒閃爍一次，以及相對應的 **LAN** 指示燈是否亮燈。



3. 如果沒有，意味著路由器的硬體有問題。那麼請回到“**I-2 硬體安裝**”，再重新執行一次硬體安裝，然後再試試。

IX-3 檢查您電腦的網路連接設置是否正確

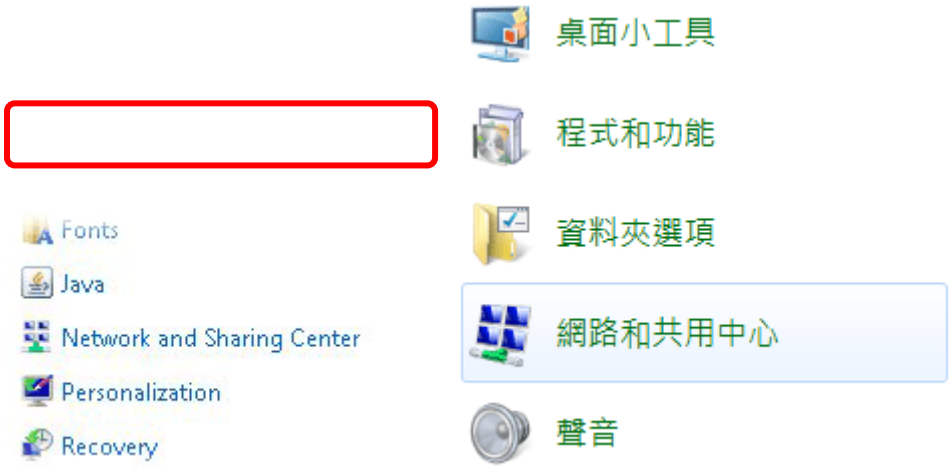
有些時候無法上網是因爲網路連接設置錯誤所造成的，若在嘗試過上面的方法，依然無法連接成功，請按以下步驟確認網路連接是否正常。

對於 Windows 系統

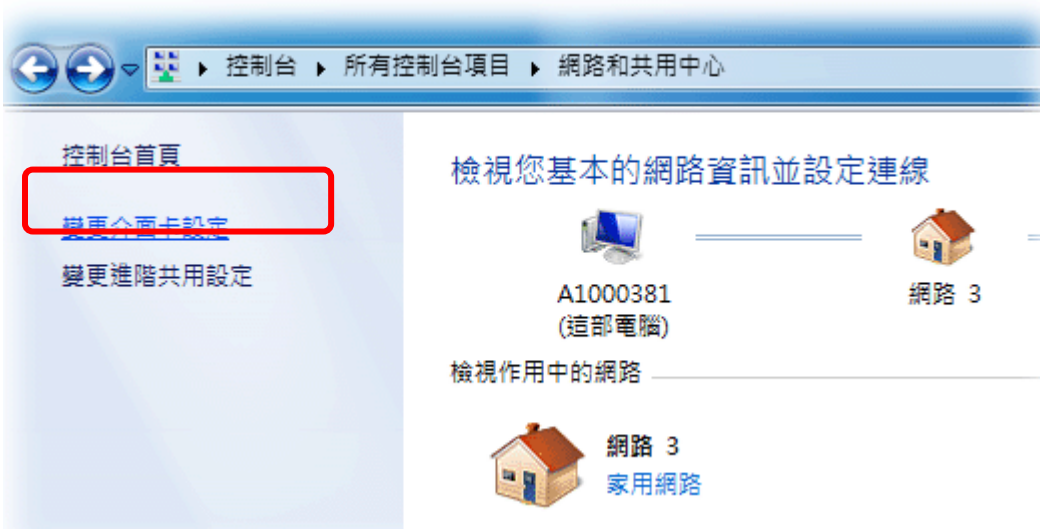
資訊

下列的範例是以 Windows 7 作業系統爲基礎而提供。若您的電腦採用其他的作業系統，請參照相似的步驟或至 www.draytek.com.tw 查閱相關的技術文件說明。

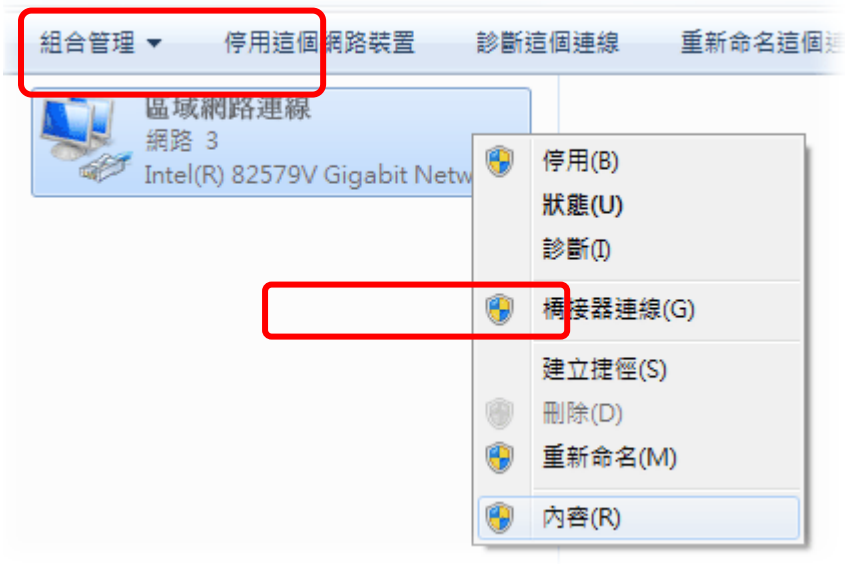
1. 開啓程式集>>控制台，按網路和共用中心。



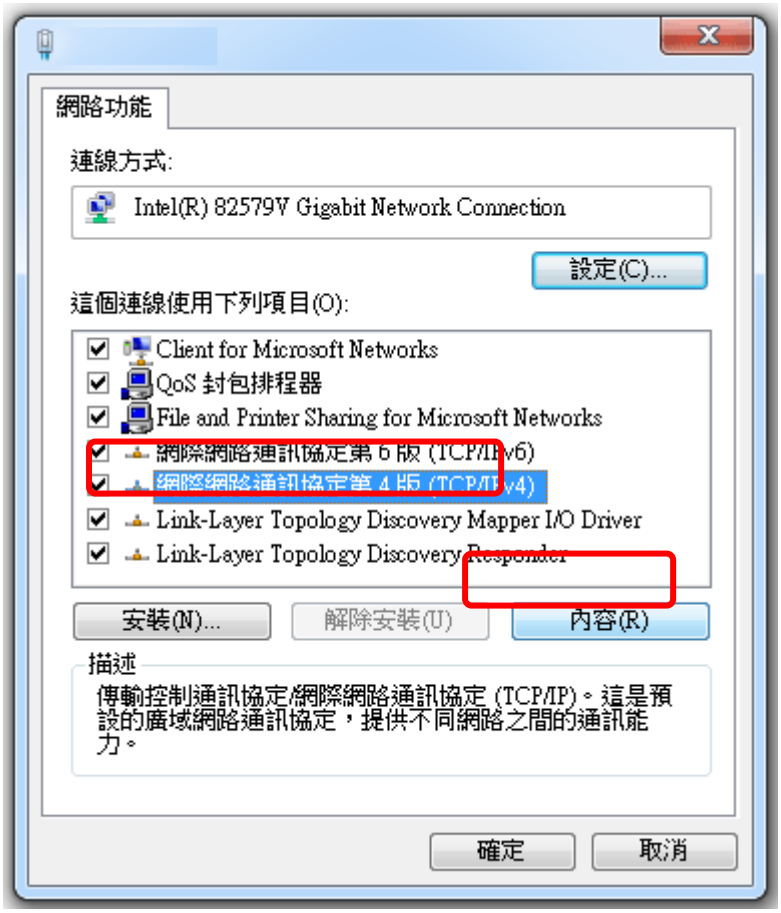
2. 在開啓的畫面上，按下變更介面卡設定連結。



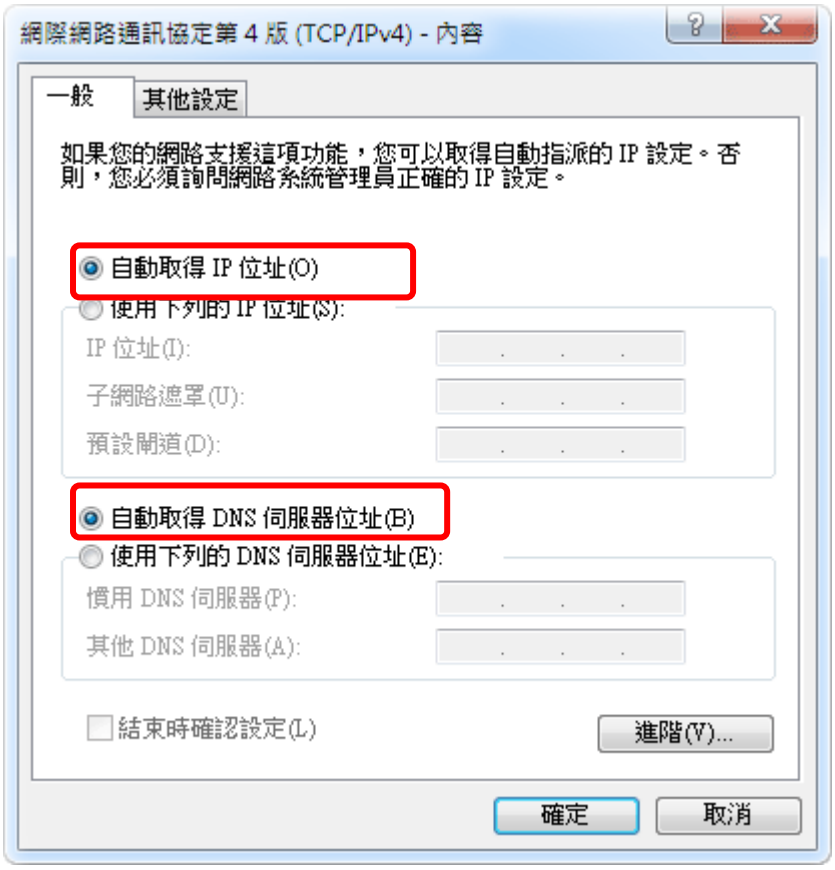
3. 網路連線圖示將會顯示在螢幕上，請在區域網路連線圖示上按下右鍵，然後向下移動點選內容。



4. 進入區域連線內容畫面後，選擇網際網路通訊協定第四版(TCP/IPv4)，再按下內容鍵。



5. 進入網際網路通訊協定第四版的內容畫面後，選擇自動取得 IP 位址及自動取得 DNS 伺服器位址，按下確定鍵後完成設定。


網際網路通訊協定第 4 版 (TCP/IPv4) - 內容
一般
其他設定
如果您的網路支援這項功能，您可以取得自動指派的 IP 設定。否則，您必須詢問網路系統管理員正確的 IP 設定。
自動取得 IP 位址(O)
使用下列的 IP 位址(S):
IP 位址(I):
子網路遮罩(U):
預設閘道(D):
自動取得 DNS 伺服器位址(B)
使用下列的 DNS 伺服器位址(E):
慣用 DNS 伺服器(P):
其他 DNS 伺服器(A):
結束時確認設定(L)
進階(V)...
確定
取消

對於 Mac 系統

1. 在桌面上選擇目前所使用的 MacOS 磁碟機按滑鼠二下。
2. 選擇**應用**檔案夾中的**網路**檔案夾。
3. 進入**網路**畫面，在**設定**選項中，選擇**使用 DHCP**。

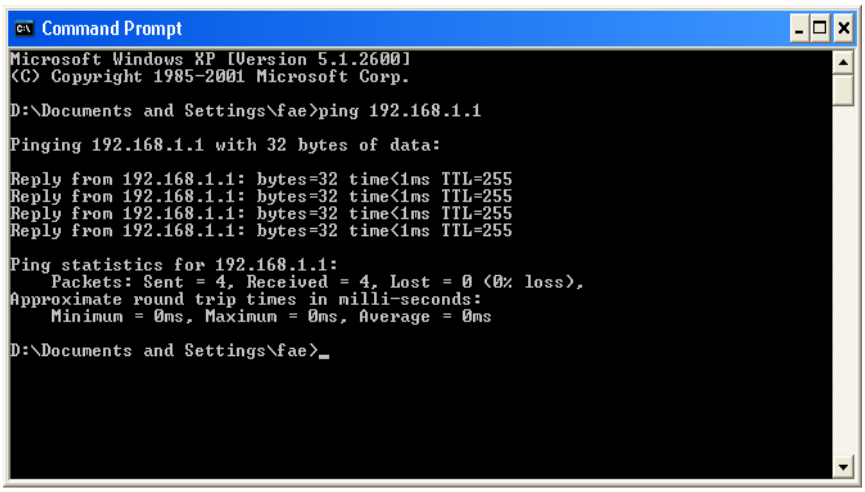


IX-4 從電腦上 Ping 路由器

路由器的預設閘道爲 192.168.1.1. 因爲某些理由，你可能需要使用 " ping " 指令檢查路由器的連結狀態。比較重要的是電腦是否收到來自 192.168.1.1 的回應，如果沒有，請檢查個人電腦上的 IP 位址。我們建議您將網際網路連線設定爲自動取得 IP 位址。(請參照 IX-3 檢查您個人電腦內的網路連線設定是否正確)，請依照以下的步驟正確地 ping 路由器。

對於 Windows 系統

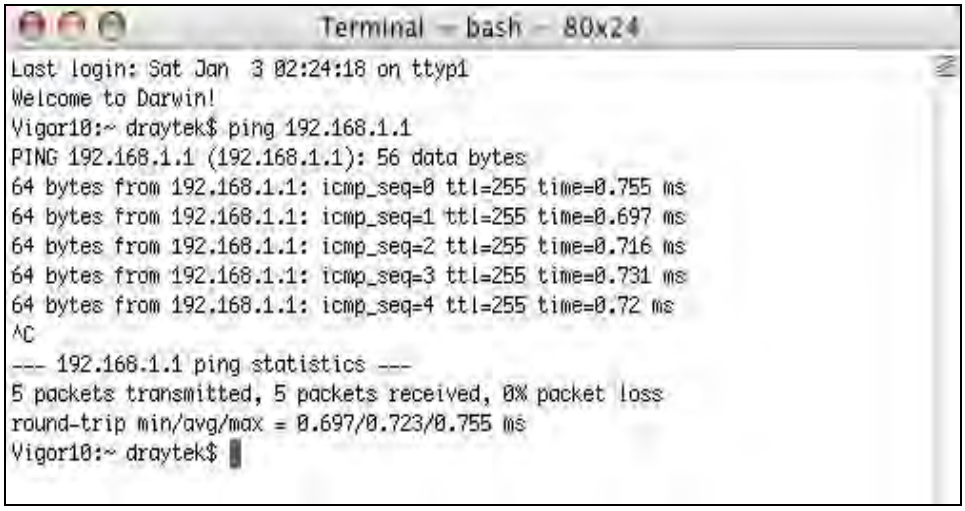
1. 開啓**命令提示字元視窗** (功能表選單**開始>>執行**) 。
2. 輸入 **command** (適用於 Windows 95/98/ME)或 **cmd** (適用於 Windows NT/ 2000/XP/Vista/7)。DOS 命令提示字元視窗將會出現。



3. 輸入 **ping 192.168.1.1** 並按下 **Enter**，如果連結成功，電腦會收到來自 192.168.1.1 的回應“**Reply from 192.168.1.1: bytes=32 time<1ms TTL=255**” 。
4. 如果連結失敗，請確認個人電腦的 IP 位址設定是否有誤。

對於 MacOs (終端機)系統

1. 在桌面上選擇目前所使用的 Mac OS 磁碟機，並在上面按滑鼠二下。
2. 選擇 **Applications** 檔案夾中的 **Utilities** 檔案夾。
3. 滑鼠按二下 **Terminal**；終端機的視窗將會跳出並顯現在螢幕上。
4. 輸入 **ping 192.168.1.1** 並且按下 **Enter** 鍵。如果連結正常，終端機視窗會出現“**64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**” 的訊息。


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$

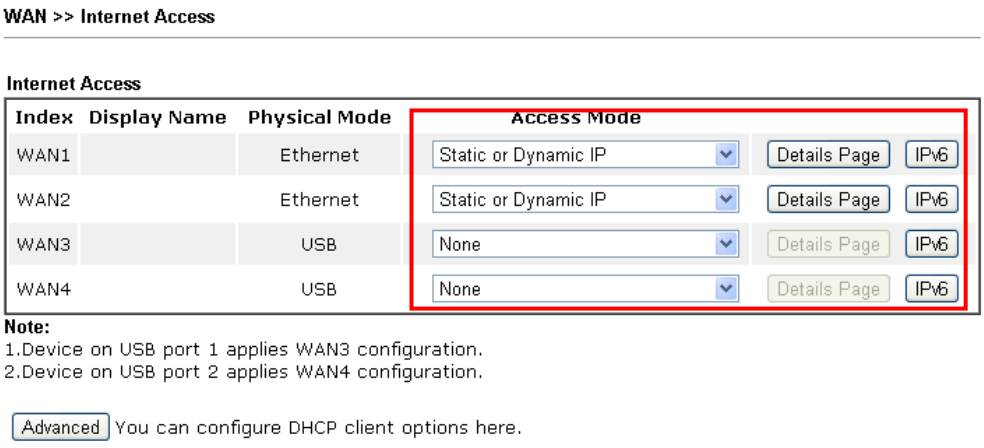
IX-5 檢查 ISP 的設置是否正常

如果 WAN 連不起來，檢查燈號是否正確(依照前述 LED 說明檢查)，或是開啓 **WAN>>網際網路連線(WAN >> Internet Access)**頁面，檢查存取設定模式是否正確，按**細節設定(Details Page)**檢視先前所設定的內容。

- 將實體連線(**Physical Type**)改爲其他的數值(例如 100M 全雙工)等。
- 下一步，將數據機(例如 DSL/FTTX(GPON)/Cable modem)的實體連線類型設定成 ISP 業者提供的類型，檢查路由器的 LED 燈號是否顯示亮燈。
- 如果沒亮燈，請另安裝交換器連接路由器與數據，接著再次檢查路由器的 LED 燈號是否顯示亮燈。
- 如果上述步驟還是無法解決 LED 燈號的問題，請與最近的經銷商聯絡，或是寄郵件予居易客服尋求進一步的技術援助。
- 檢查 ISP 提供的設定是否配置完成。

LED 燈號正確但是 WAN 連線還是無法成功，則：

- 開啓 **WAN>>網際網路連線(WAN >> Internet Access)** ，檢查 ISP 設定是否正確，按下**細節設定(Details Page)** 檢視之前的內容。



IX-6 3G/4G 網路連線相關問題

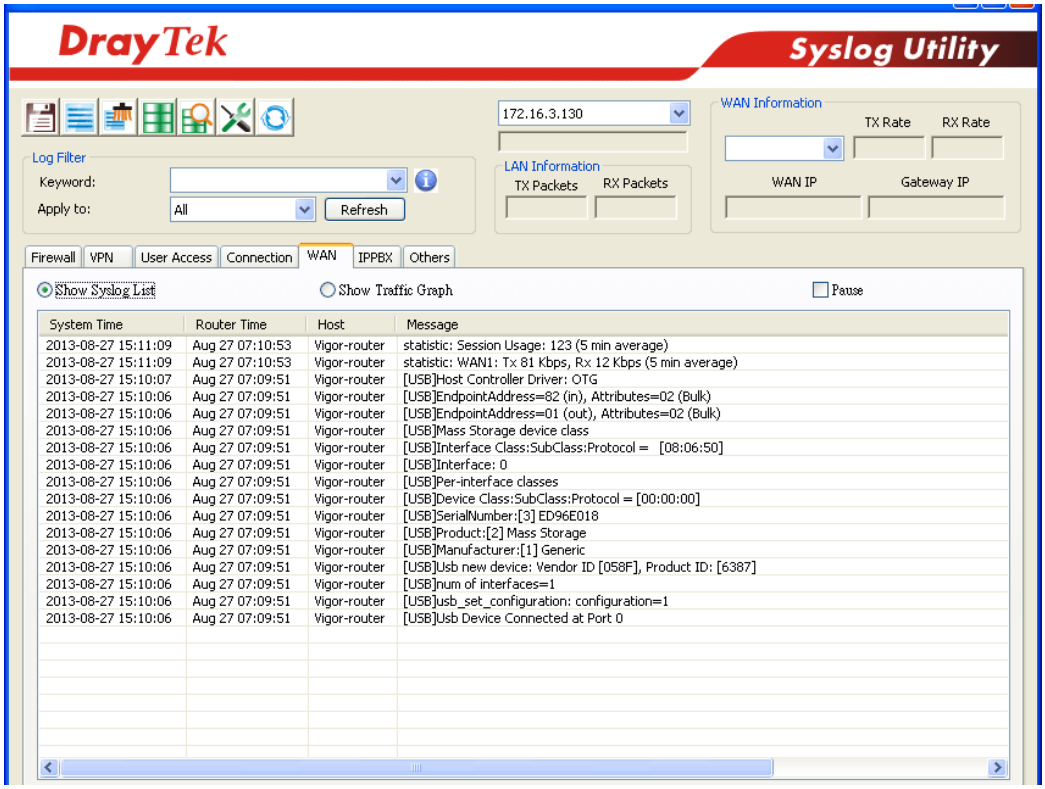
當您使用 3G/4G 網路傳輸發現問題時，請先檢查下列各項：

檢查 USB LED 燈號

在插入 3G/4G USB Modem 至 Vigor2926 後，您必須等待 15 秒左右，稍後 USB LED 會亮燈，表示 3G/4G USB Modem 安裝成功。如果 USB LED 燈號未亮，請將 3G/4G USB Modem 移除再重新插入，如果仍然失敗，請重新啓動路由器。

USB LED 亮燈但是網路連線依然失敗

檢查 SIM 卡上的 PIN 碼是否是關閉的，請使用 3G/4G USB Modem 的工具關閉 PIN 碼然後再試一次。如果還是不行，那就可能是系統的相容性問題，麻煩開啓 DrayTek Syslog 工具擷取連線資訊(WAN Log) 並將此頁面(類似下述畫面)傳送至居易的服務中心尋求解答。



傳輸速率不夠快

利用筆記型電腦連接 3G/4G USB Modem 來測試連線速度，檢查是否這個問題是 Vigor2926 所造成的，此外，請參考 3G/4G USB Modem 手冊中燈號意義，確保數據機是透過 HSDPA 模式連接網際網路。如果您想要在室內使用 3G/4G USB Modem，請放置在靠窗位置以取得較佳的接收信號。

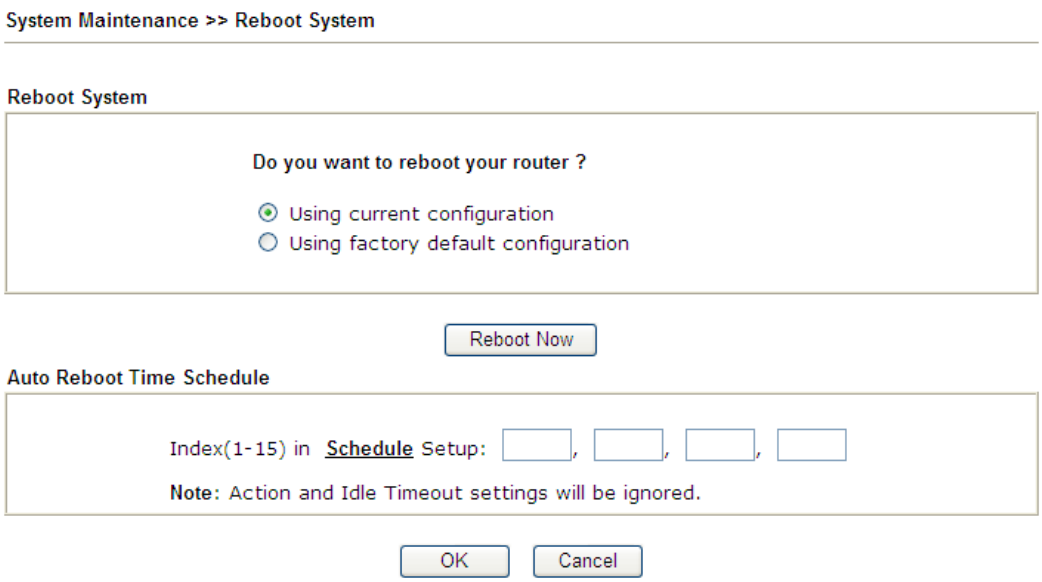
IX-7 還原路由器原廠預設組態

有時，錯誤的連線設定可以藉由還原廠預設組態來重新設定，您可以利用**重啓路由器**或硬體重新設定的方法還原路由器的設定值。此供能僅在**管理者模式**下可以運作。

資訊	在使用原廠預設組態後，您之前針對分享器所調整的設定都將恢復成預設值。請確實記錄之前路由器所有的設定。

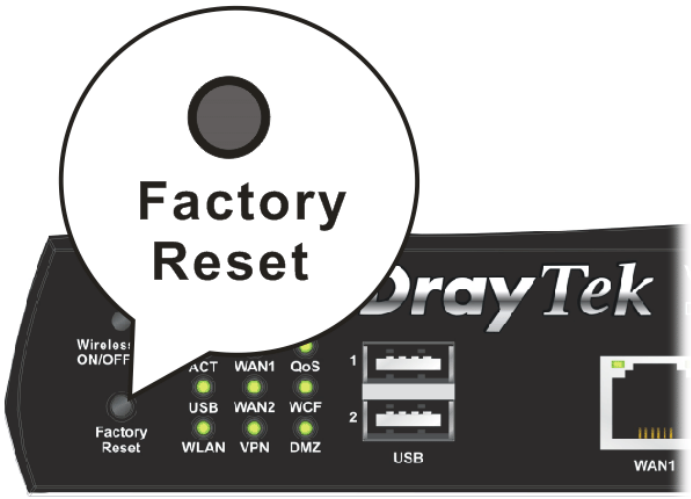
軟體重新設定

請進入管理者模式，再到網頁介面上的**系統維護>>重啓路由器(System Maintenance>> Reboot System)**，可見下圖。選擇**使用原廠預設組態(sing factory default configuration)**，並按下**立即重啓(Reboot Now)**。幾秒鐘後，路由器就會恢復至出廠預設設定。



硬體重新設定

當路由器正在運作時（ACT 燈號閃爍），如果您壓住 **Factory Reset** 按鈕超過 5 秒以上，且看到 ACT 燈號開始快速閃爍時，請鬆開 **Factory Reset** 按鈕，此時，路由器將會還原成出廠預設值狀態。



恢復至出廠預設值後，您就可以按個人需要，重新設定路由器。

IX-8 聯絡居易

假如經過多次嘗試設定後，路由器仍舊無法正常運作，請立即與經銷商聯絡或與居易科技技術服務部聯絡 support@draytek.com.tw。

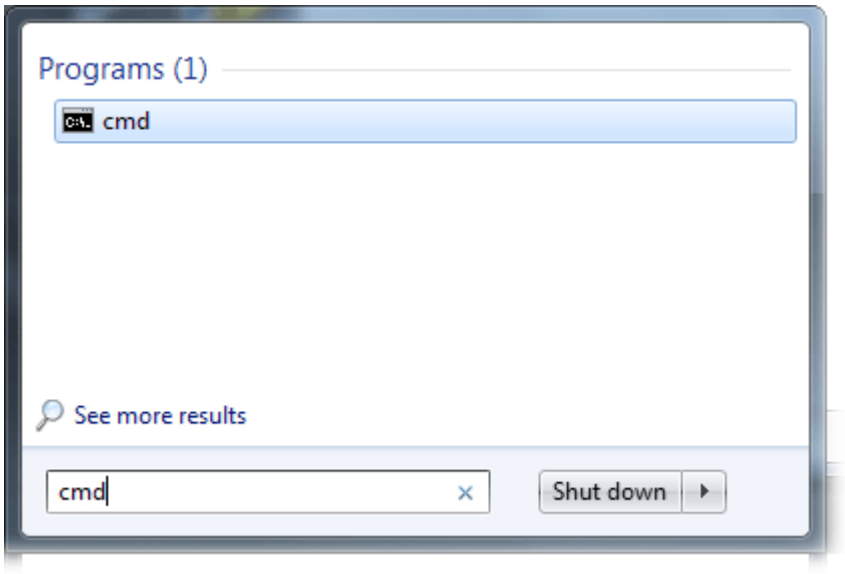
第十篇 Telnet 指令設定

進入路由器 Telnet

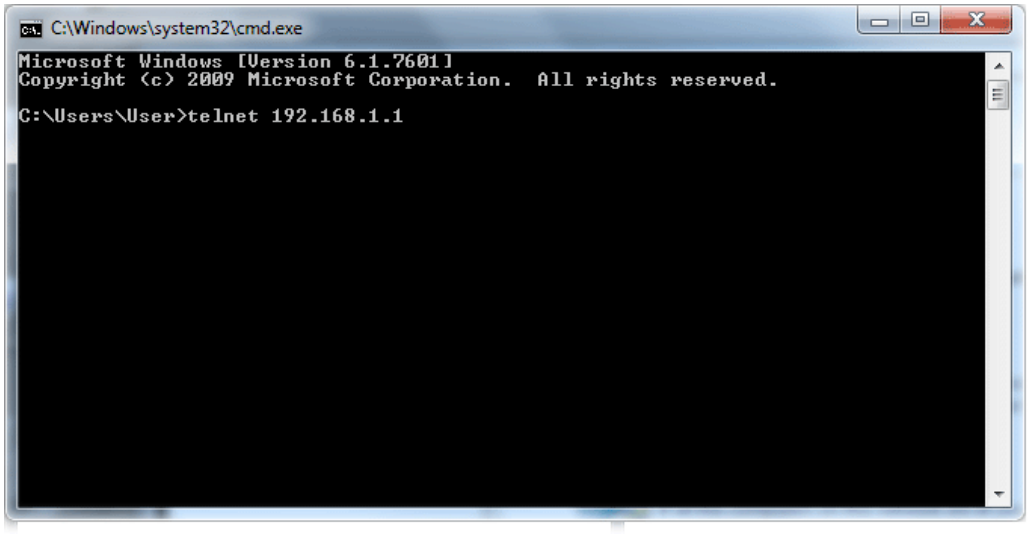
本章將會告訴您如何使用 Telnet 指令並提供指令的相關說明

資訊	對於 Windows 7 使用者，請務必確定在 **Control Panel>>Programs** 中 Telnet Client 功能已經啓用。

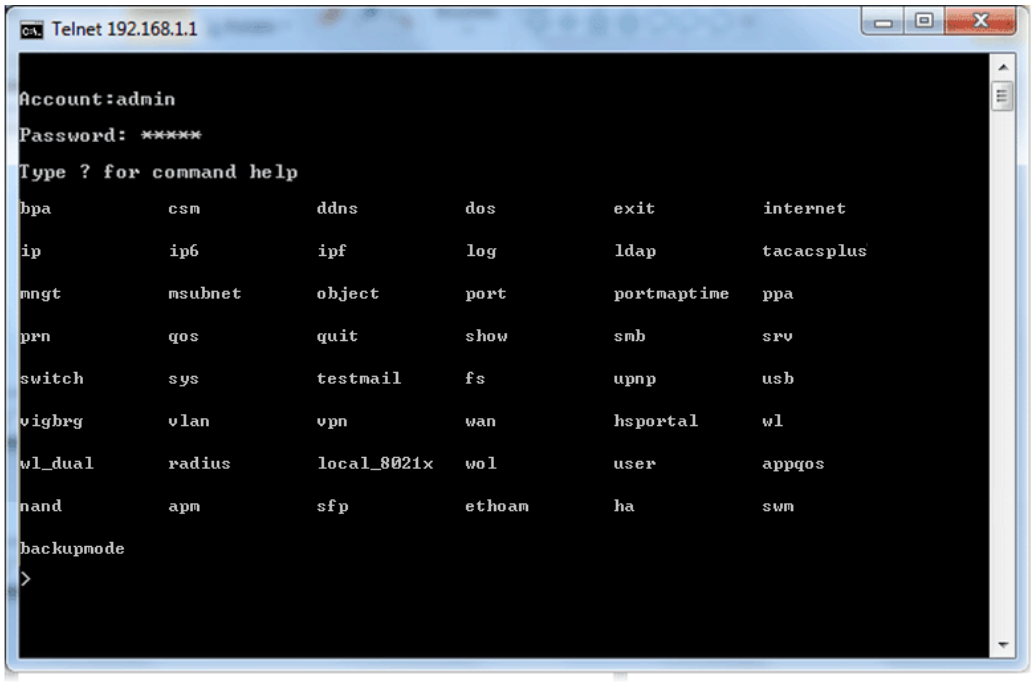
輸入 **cmd** 然後按下 Enter，Telnet 終端機畫面將會出現。



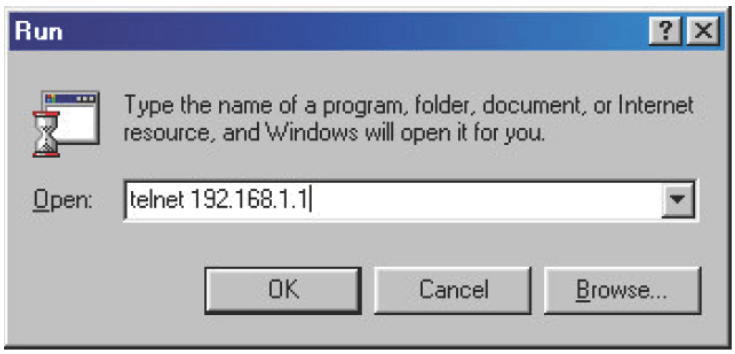
在下述小視窗中，輸入 telnet 192.168.1.1 然後按 Enter 鍵。範例中所使用的 IP 位址是路由器的預設 IP，如果您有改變了預設 IP 的位址，請輸入變更後的 IP 內容。

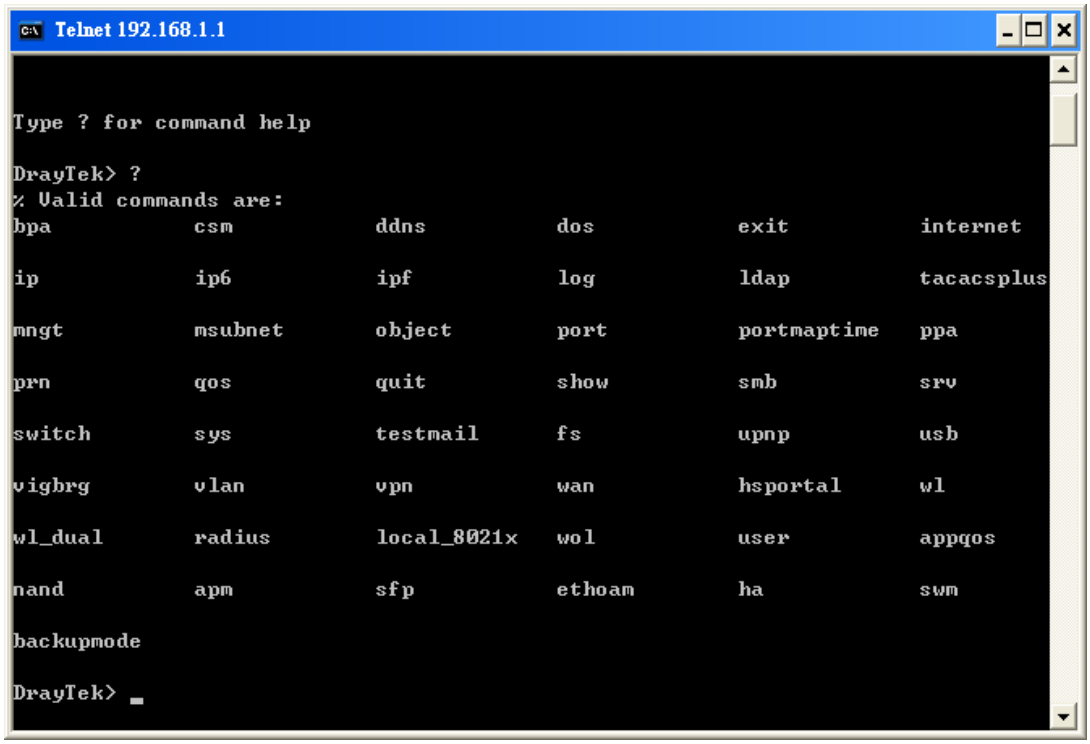


接著輸入帳號密碼 admin/admin，在輸入?之後您將會看到此台路由器所具備的有效/常見的指令。



對使用早先的 Windows 系統，可以按 **Start >> Run** 在輸入 **Telnet 192.168.1.1**，接著輸入帳密 admin/admin，然後輸入?，就會看到此台路由器所具備的有效/常見的指令。





Telnet Command: bpa

This command allows to configure a network setting specified for Australia's ISP.

Syntax

bpa m *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
m	Available settings are 1 and 2.
-a <enable>	1/0 to enable/disable this entry
-n <UserName>	contact UserName(max. 24 characters)
-p <PassWord>	contact PassWord (max. 24 characters)
-s <select>	It means to specify an IP address for Server. 0 : no selection. 1 : NSW(61.9.192.13) 2 : QLD(61.9.208.13), 3 : VIC(61.9.128.13) 4 : SA(61.9.224.13), 5 : WA(61.9.240.13)
-l <List>	List all settings configured.

Example

```
> bpa 1 -a 1 -n testUser -p testPassword -s 4
> bpa -l
-------index: 1 active------
UserName[1]: testUser
PassWord[1]: testPassword
ServerIP[1]:4

-------index: 2 inactive------
UserName[2]:
PassWord[2]:
ServerIP[2]:0

>
```

Telnet Command: csm appe prof

Commands under CSM allow you to set CSM profile to define policy profiles for different policy of IM (Instant Messenger)/P2P (Peer to Peer) application.

"csm appe prof " is used to configure the APP Enforcement Profile name. Such profile will be applied in **Default Rule** of **Firewall>>General Setup** for filtering.

Syntax

csm appe prof -i *INDEX [-v | -n NAME|setdefault]*

Syntax Description

Parameter	Description
INDEX	It means to specify the index number of CSM profile, from 1 to 32.
- v	It means to view the configuration of the CSM profile.
- n	It means to set a name for the CSM profile.
NAME	It means to specify a name for the CSM profile, less then 15 characters.
setdefault	Reset to default settings.

Example

```
> csm appe prof -i 1 -n games
The name of APPE Profile 1 was setted.
```

Telnet Command: csm appe set

It is used to configure group settings for IM/P2P/Protocol and Others in APP Enforcement Profile.

csm appe set *-i INDEX [-v GROUP| -e AP_IDX | -d AP_IDX]*

Syntax Description

Parameter	Description
INDEX	Specify the index number of CSM profile, from 1 to 32.
- v	View the IM/P2P/Protocol and Others configuration of the CSM profile.
-e	Enable to block specific application.
-d	Disable to block specific application.
GROUP	Specify the category of the application. Available options are: IM, P2P, Protocol and Others.
AP_IDX	Each application has independent index number for identification in CLI command. Specify the index number of the application here. If you have no idea of the inex number, do the following (Take IM as an example): Type "csm appe set –I 1 –v IM", the system will list all of the index numbers of the applications categorized under IM.

Example

```
>Vigor> csm appe set -i 1 -e 1
Profile 1 - : AIM is enabled.
```

Telnet Command: csm appe show

It is used to display group (IM/P2P/Protocol and Others) information APP Enforcement Profile.

csm appe show *[-a|-i|-p|-t|-m]*

Syntax Description

Parameter	Description
-a	View the configuration status for All groups.
-i	View the configuration status of IM group.
-p	View the configuration status of P2P group.
-t	View the configuration status of protocol group.
-m	View the configuration status of Others group.

Example

```
>csm appe show -t

         Type    Index                Name        Version   Advance
 Advanced Option: (M)essage, (F)ile Transfer, (G)ame, (C)onference, and (O)ther
Activities
-------------------------------------------------------------
      PROTOCOL       52                 DB2
      PROTOCOL       53                 DNS
      PROTOCOL       54                 FTP
      PROTOCOL       55                HTTP            1.1
      PROTOCOL       56                IMAP            4.1
      PROTOCOL       57         IMAP STARTTLS           4.1
      PROTOCOL       58                 IRC          2.4.0            ……
```

Telnet Command: csm appe config

It is used to display the configuration status (enabled or disabled) for IM/P2P/Protocol/Other applications.

csm appe config -v *INDEX [-i|-p|-t|-m]*

Syntax Description

Parameter	Description
INDEX	Specify the index number of CSM profile, from 1 to 32.
-i	View the configuration status of IM group.
-p	View the configuration status of P2P group.
-t	View the configuration status of protocol group.
-m	View the configuration status of Others group.

Example

```
> csm appe config -v 1 -m

    Group         Type    Index               Name        Enable     A
vance Enable
 Advance abbreviation: Message, File Transfer, Game, Conference, and Other
 Advance abbreviation: : M, F, G, C, and O
-----------------------------------------------------------------------
   OTHERS        TUNNEL       75            DNSCrypt           Disable
   OTHERS        TUNNEL       76            DynaPass           Disable
   OTHERS        TUNNEL       77               FreeU           Disable
```

```
    OTHERS        TUNNEL       78          HTTP Proxy          Disable
    OTHERS        TUNNEL       79          HTTP Tunnel         Disable
    OTHERS        TUNNEL       80             Hamachi          Disable
    OTHERS        TUNNEL       81       Hotspot Shield         Disable
    OTHERS        TUNNEL       82            MS Teredo         Disable
    OTHERS        TUNNEL       83              PGPNet          Disable
    OTHERS        TUNNEL       84          Ping Tunnel         Disable
.
.
.
-----------------------------------------------------------------
Total 66 APPs
>
```

Telnet Command: csm appe interface

It is used to configure APPE signature download interface.

csm appe interface *[AUTO/WAN#]*

Syntax Description

Parameter	Description
AUTO	Vigor router specifies WAN interface automatically.
WAN	Specify the WAN interface for signature downloading.

Example

```
> csm appe interface wan1
Download interface is set as "WAN1" now.
> csm appe interface auto
Download interface is set as "auto-selected" now.
```

Telnet Command: csm appe email

It is used to set notification e-mail for APPE signature based on the settings configured in **System Maintenance>>SysLog/Mail Alert Setup (**in which, the box of **APPE Signature** is checkd under **Enable E-Mail Alert**).

csm appe email *[-e|-d|-s]*

Syntax Description

Parameter	Description
-e	Enable notification e-mail mechanism.
-d	Disable notification e-mail mechanism.
-s	Send an example e-mail.

Example

```
> csm appe email -e
Enable APPE email.
```

Telnet Command: csm ucf

It is used to configure settings for URL control filter profile.

Syntax

csm ucf show

csm ucf setdefault

csm ucf msg *MSG*

csm ucf obj *INDEX [-n PROFILE_NAME | -l [P|B|A|N] | uac | wf]*

csm ucf obj *INDEX -n PROFILE_NAME*

csm ucf obj *INDEX -p VALUE*

csm ucf obj *INDEX -l P|B|A|N*

csm ucf obj *INDEX uac*

csm ucf obj *INDEX wf*

Syntax Description

Parameter	Description
show	It means to display all of the profiles.
setdefault	It means to return to default settings for all of the profile.
msg MSG	It means de set the administration message. MSG means the content (less than 255 characters) of the message itself.
obj	It means to specify the object for the profile.
INDEX	It means to specify the index number of CSM profile, from 1 to 8.
-n	It means to set the profile name.
PROFILE_NAME	It means to specify the name of the profile (less than 16 characters)
-p	Set the priority (defined by the number specified in VALUE) for the profile.

VALUE	Number 0 to 3 represent different conditions. 0: It means Bundle: Pass. 1: It means Bundle: Block. 2: It means Either: URL Access Control First. 3: It means Either: Web Feature First.
-l	It means the log type of the profile. They are: P: Pass, B: Block, A: All, N: None
MSG	It means to specify the Administration Message, less then 255 characters
uac	It means to set URL Access Control part.
wf	It means to set Web Feature part.

Example

```
> csm ucf obj 1 -n game -l B
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
 Action:[pass]
[ ]Prevent web access from IP address.
  No  Obj NO.    Object Name
 --- -------- ---------------------------------

  No  Grp NO.    Group Name
 --- -------- ---------------------------------
```

Telnet Command: csm ucf obj INDEX uac

It means to configure the settings regarding to URL Access Control (uac).

Syntax

csm ucf obj *INDEX uac -v*

csm ucf obj *INDEX uac -e*

csm ucf obj *INDEX uac -d*

csm ucf obj *INDEX uac -a P|B*

csm ucf obj *INDEX uac -i E|D*

csm ucf obj *INDEX uac -o KEY_WORD_Object_Index*

csm ucf obj *INDEX uac -g KEY_WORD_Group_Index*

Syntax Description

Parameter	Description
INDEX	It means to specify the index number of CSM profile, from 1 to 8.

- v	It means to view the protocol configuration of the CSM profile.
-e	It means to enable the function of URL Access Control.
-d	It means to disable the function of URL Access Control.
-a	Set the action of specific application, P or B. B: Block. The web access meets the URL Access Control will be blocked. P: Pass. The web access meets the URL Access Control will be passed.
-i	Prevent the web access from any IP address. E: Enable the function. The Internet access from any IP address will be blocked. D: Disable the function.
-o	Set the keyword object.
KEY_WORD_Object_Index	Specify the index number of the object profile.
-g	Set the keyword group.
KEY_WORD_Group_Index	Specify the index number of the group profile.

Example

```
> csm ucf obj 1 uac -i E
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
 Action:[pass]
 [v]Prevent web access from IP address.
  No  Obj NO.    Object Name
 --- -------- ---------------------------------

  No  Grp NO.    Group Name
 --- -------- ---------------------------------

> csm ucf obj 1 uac -a B
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
 Action:[block]
 [v]Prevent web access from IP address.
  No  Obj NO.    Object Name
 --- -------- ---------------------------------

  No  Grp NO.    Group Name
 --- -------- ---------------------------------
```

Telnet Command: csm ucf obj INDEX wf

It means to configure the settings regarding to Web Feature (wf).

Syntax

csm ucf obj *INDEX wf -v*

csm ucf obj *INDEX wf -e*

csm ucf obj *INDEX wf -d*

csm ucf obj *INDEX wf -a P|B*

csm ucf obj *INDEX wf -s WEB_FEATURE*

csm ucf obj *INDEX wf -u WEB_FEATURE*

csm ucf obj *INDEX wf -f File_Extension_Object_index*

Syntax Description

Parameter	Description
INDEX	It means to specify the index number of CSM profile, from 1 to 8.
- v	It means to view the protocol configuration of the CSM profile.
-e	It means to enable the restriction of web feature.
-d	It means to disable the restriction of web feature.
-a	Set the action of web feature, P or B. B: Block. The web access meets the web feature will be blocked. P: Pass. The web access meets the web feature will be passed.
-s	It means to enable the the Web Feature configuration. Features available for configuration are: c: Cookie p: Proxy u: Upload
-u	It means to cancel the web feature configuration.
-f	It means to set the file extension object index number.
File_Extension_Object_index	Type the index number (1 to 8) for the file extension object.

Example

```
> csm ucf obj 1 wf -s c
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
 Action:[block]
 [v] Prevent web access from IP address.
  No  Obj NO.    Object Name
 --- -------- ---------------------------------

  No  Grp NO.    Group Name
 --- -------- ---------------------------------
```

```
[ ]Enable Restrict Web Feature
 Action:[pass]
 File Extension Object Index : [0]      Profile Name : []
 [V] Cookie [ ] Proxy [ ] Upload
```

Telnet Command: csm wcf

It means to configure the settings regarding to web control filter (wcf).

Syntax

csm wcf show

csm wcf look

csm wcf cache

csm wcf server WCF_SERVER

csm wcf msg MSG

csm wcf setdefault

csm wcf obj *INDEX -v*

csm wcf obj *INDEX -a P|B*

csm wcf obj *INDEX -n PROFILE_NAME*

csm wcf obj *INDEX -l N|P|B|A*

csm wcf obj *INDEX -o KEY_WORD Object Index*

csm wcf obj *INDEX -g KEY_WORD Group Index*

csm wcf obj *INDEX -w E|D|P|B*

csm wcf obj *INDEX -s CATEGORY|WEB_GROUP*

csm wcf obj *INDEX -u CATEGORY|WEB_GROUP*

Syntax Description

Parameter	Description
show	It means to display the web content filter profiles.
Look	It means to display the license information of WCF.
Cache	It means to set the cache level for the profile.
Server WCF_SERVER	It means to set web content filter server.
Msg MSG	It means de set the administration message. MSG means the content (less than 255 characters) of the message itself.
setdefault	It means to return to default settings for all of the profile.
obj	It means to specify the object profile.
INDEX	It means to specify the index number of web content filter profile, from 1 to 8.
- v	It means to view the web content filter profile.
-a	Set the action of web content filter profile, P or B. B: Block. The web access meets the web feature will be blocked. P: Pass. The web access meets the web feature will be passed.
-n	It means to set the profile name.
PROFILE_NAME	It means to specify the name of the profile (less than 16 characters)
-l	It means the log type of the profile. They are:

	P: Pass, B: Block, A: All, N: None
-o	Set the keyword object.
KEY_WORD_Object_Index	Specify the index number of the object profile.
-g	Set the keyword group.
KEY_WORD_Group_Index	Specify the index number of the group profile.
-w	It means to set the action for the black and white list. E:Enable, D:Disable, P:Pass, B:Block
-s	It means to choose the items under CATEGORY or WEB_GROUP.
-u	It means to discard items under CATEGORY or WEB_GROUP.
WEB_GROUP	Child_Protection, Leisure, Business, Chating, Computer Internet, Other
CATEGORY	Includes: Alcohol & Tobacco, Criminal Activity, Gambling, Hate & Intoleranc, Illegal Drug, Nudity, Pornography/Sexually Explicit, Weapons, Violence, School Cheating,Sex Education, Tasteless, Child Abuse Imges, Entertainment, Games, Sports, Travel, Leisure & Recreation, Fashin & Beauty, Business, Job Search, Web-based Emai, Chat, Instant Messaging, Anonymizers, Forums & Newsgroups, Computers & Technology, Download Sites, Streaming Media & Downloads, Phishing & Fraud, Search Engines & Portals, Social Networking, Spam Sites,Malware, Botnets, Hacking, Illegal Software, Information Security,Peer-to-eer, Advertisements & Pop-Ups, Arts, Transportation, Compromised, Dating & Personals, , Education, Finance, Government,Health & Medcine, News, Non-profits & NGOs, Personal Sites,Politics, Real Estate, Rligion, Restaurants & Dining,Shopping, Translators, General, Cults,Greetig cards, Image Sharing, Network Errors, Parked Domains, Private IP Addresses)

Example

```
> csm wcf obj 1 -n test_wcf
Profile Index: 1
Profile Name:[test_wcf]
[]White/Black list
Action:[block]
  No  Obj NO.    Object Name
 --- -------- --------------------------------
  No  Grp NO.    Group Name
 --- -------- --------------------------------
Action:[block]
 Log:[block]
-------------------------------------------------------------------
-------------
child Protection Group:
  [v]Alcohol & Tobacco    [v]Criminal & Activity   [v]Gambling
  [v]Hate & Intolerance    [v]Illegal Drug        [v]Nudity
  [v]Pornography & Sexually explicit  [v]Violence
[v]Weapons

  [v]School Cheating      [v]Sex Education        [v]Tasteless
  [v]Child Abuse Images
-------------------------------------------------------------------
-------------
leisure Group:
  [ ]Entertainment        [ ]Games               [ ]Sports
  [ ]Travel              [ ]Leisure & Recreation  [ ]Fashion & Beauty
.
.
>
```

Telnet Command: csm dnsf

It means to configure the settings regarding to DNS filter.

csm dnsf enable *ON|OFF*

csm dnsf syslog *N|P|B|A*

csm dnsf service WCF_PROFILE

csm dnsf service_ucf UCF_PROFILE

csm dnsf time CACHE_TIME

csm dnsf blockpage *show/on/off*

csm dnsf profile_show

csm dnsf profile_edit *INDEX*

csm dnsf profile_edit *INDEX -n PROFILE_NAME*

csm dnsf profile_edit *INDEX -l N|P|B|A*

csm dnsf profile_edit *INDEX -w WCF_PROFILE*

csm dnsf profile_edit *INDEX -u UCF_PROFILE*

csm dnsf profile_edit *INDEX -c CACHE_TIME*

Syntax Description

Parameter	Description
enable	Enable or disable DNS Filter. ON: enable. OFF: disable.
syslog	Determine the content of records transmitting to Syslog. P: Pass. Records for the packets passing through DNS filter will be sent to Syslog. B: Block. Records for the packets blocked by DNS filter will be sent to Syslog. A: All. Records for the packets passing through or blocked by DNS filter will be sent to Syslog. N: None. No record will be sent to Syslog.
service WCF_PROFILE	WCF_PROFILE: Specify a WCF profile as the base of DNS filtering. Type a number to indicate the index number of WCF profile (1 is first profile, 2 is second profile, and so on ...).
time CACHE_TIME	CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on ...) for DNS filter.
blockpage	DNS sends block page for redirect port. When a web page is blocked by DNS filter, the router system will send a message page to describe that the page is not allowed to be visisted. ON: Enable the function of displaying message page. OFF: Disable the function of displaying message page. SHOW: Display the function of displaying message page is ON or OFF.
profile_show	Display the table of the DNS filter profile.
profile_edit	Modify the content of the DNS filter profile.
-n PROFILE_NAME	PROFILE_NAME: Type the name of the DNS filter profile that you want to modify.
-l N|P|B|A	Specify the log type of the profile. P: Pass. B: Block. A: All. N: None.
-w WCF_PROFILE	WCF_PROFILE: Type the index number of the WCF profile.
-u UCF_PROFILE	UCF_PROFILE: Type the index number of the UCF profile.
-c CACHE_TIME	-c means to set the cache time for DNS filter. CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on ...) for DNS filter.

Example

```
> csm dnsf service 2
dns service set up!!!
>csm dnsf service 3
wcf profile 3 is empty.....
>csm dnsf cachetime 1
dns cache time set up!!!
```

Telnet Command: ddns enable

This command allows users to enable or disable the DDNS service.

Syntax

ddns enable *[0/1]*

Syntax Description

Parameter	Description
0/1	0 – Disable the DDNS service. 1 – Enable the DDNS service.

Example

```
> ddns enable 1
 Enable Dynamic DNS Setup
>
```

Telnet Command: ddns set

This command allows users to set Dynamica DNS account.

Syntax

ddns set *[option]*

ddns set *-i [account index] -S [service provider] -T [service type] -D [hostname] -L [username] -P [password]*

Syntax Description

Parameter	Description
-i [value]	It means index number of Dynamic DNS Account. value: 1-6
-E [value]	It means to enable /disable Dynamic DNS Account. value: 0: Disable, 1:Enable
-W [value]	It means to specify WAN Interface. [value]: Must be between 1-8 1: WAN1 First 2: WAN1 Only 3: WAN2 First 4: WAN2 Only example: To set WAN Interface: WAN1 First
-L [value]	It means to type Login Name. [value]: limit up to 64 characters
-P [value]	It means to type Password. [value]: limit up to 24 characters
-C [value]	It means to enable /disable Wildcards. [value]: 0: Disable, 1:Enable
-B [value]	It means to enable / disable Backup MX. [value]: 0: Disable, 1:Enable
-M [value]	It means to type Mail Extender.

	[value]: limit up to 60 characters
-R [value]	It means to type Determine Real WAN IP. [value]: 0: WAN IP, 1: Internet IP
-S [value]	It means to specify Servive Provider. If user want to set User-Defined page, value must select 1. [value]: value must be between 1-19. 1 >> User-Defined 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 Free (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 [value]	It means to type Servive Type. [value]: value must be between 1-3. 1: Dynamic 2: Custom 3: Static
-D <Host Name> <sub Domain Name>	It means to type Domain Name. i.e: Account index 1 setting Domain Name for Dynamic Service Type >> ddns set -i 1 -T 1 -D "host ddns.com.cn" i.e: Account index 2 setting Domain Name for Custom Service Type >> ddns set -i 2 -T 2 -D "domain name" i.e: Account index 3 setting Domain Name for Static Service Type >> ddns set -i 3 -T 3 -D "domain name"
-H [value]	It means to type User-Defined Provider Host. [value]: limit up to 64 characters
-A [value]	It means to type User-Defined Service API. [value]: limit up to 256 characters
-a [value]	It means to type User-Defined Auth Type. [value]: 0: basic 1: URL
-N [value]	It means to type User-Defined Connection Type. [value]: 0: Http 1: Https
-O [value]	It means to type User-Defined Server Response. [value]: limit up to 32 characters

Example

```
> ddns set -i 1 -S 6 -T 1 -D "hostname dnsalias.net" -L user1 -P pwd1
> Save OK
```

Telnet Command: ddns log

Displays the DDNS log.

Example

```
> ddns log
> ddns log2017-09-04 04:43:46.5 >>>>>  DDNS is updating.
<<<<<2017-09-04
 04:43:05.6 >>>>>  DDNS is updating.  <<<<<
```

Telnet Command: ddns time

Sets and displays the DDNS time.

Syntax

ddns time *[update in minutes]*

Syntax Description

Parameter	Description
Update in minutes	Type the value as DDNS time. The range is from 1 to 14400.

Example

```
> ddns time
ddns time <update in minutes>
Valid: 1 ~ 1440
%Now: 1440
> ddns time 1000
ddns time <update in minutes>
Valid: 1 ~ 1440
%Now: 1000
```

Telnet Command: ddns forceupdate

This command will update DDNS automatically.

Example

```
> ddns forceupdate
 Now updating DDNS ...
 Please check result by using command "ddns log"
```

Telnet Command: ddns setdefault

This command will return DDS with factory default settings.

Example

```
>ddns setdefault
>回復出廠預設值(Set to Factory Default).
```

Telnet Command: ddns show

This command allows users to check the content of selected DDNS account.

Syntax

ddns show -i *[value]*

Syntax Description

Parameter	Description
-I [value]	Display the content of selected DDNS account. [value]: value must be between 1-6

Example

```
> ddns show -i 1
-------------------------------------------------
 Index: 1
 [ ] Enable Dynamic DNS Account
 WAN Interface: WAN1 First
 Service Provider: dyn.com (www.dyn.com)
 Service Type: Dynamic
 Domain Name: [].[]
 Login Name:
 [ ] Wildcards
 [ ] Backup MX
 Mail Extender:
 Determine Real WAN IP: WAN IP

DrayTek>
```

Telnet Command: dos

This command allows users to configure the settings for DoS defense system.

Syntax

dos *[-V | D | A]*

dos *[-s ATTACK_F [THRESHOLD][TIMEOUT]]*

dos *[-a | e [ATTACK_F][ATTACK_0] | d [ATTACK_F][ATTACK_0]]*

Syntax Description

Parameter	Description
-V	It means to view the configuration of DoS defense system.
-D	It means to deactivate the DoS defense system.
-A	It means to activate the DoS defense system.
-s	It means to enable the defense function for a specific attack and set its parameter(s).
ATTACK_F	It means to specify the name of flooding attack(s) or portscan, e.g., synflood, udpflood, icmpflood, or postscan.
THRESHOLD	It means the packet rate (packet/second) that a flooding attack will be detected. Set a value larger than 20.
TIMEOUT	It means the time (seconds) that a flooding attack will be blocked. Set a value larger than 5.
-a	It means to enable the defense function for all attacks listed in ATTACK_0.

-e	It means to enable defense function for a specific attack(s).
ATTACK_0	It means to specify a name of the following attacks: ip_option, tcp_flag, land, teardrop, smurf, pingofdeath, traceroute, icmp_frag, syn_frag, unknow_proto, fraggle.
-d	It means to disable the defense function for a specific attack(s).

Example

```
>dos –A
The Dos Defense system is Activated
>dos –s synflood 50 10
Synflood is enabled! Threshold=50 <pke/sec> timeout=10 <pke/sec>
```

Telnet Command: exit

Type this command will leave telnet window.

Telnet Command: Internet

This command allows you to configure detailed settings for WAN connection.

Syntax

internet *-W n -M n [-<command> <parameter> | …]*

Syntax Description

Parameter	Description
-W n	W means to select WAN interface. n: 1: WAN1 ,2: WAN2, … x: WANx. Default is WAN1.
-M n	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 – 7, A, B) n=0: Offline n=1: PPPoE n=2: Dynamic IP n=3: Static IP n=4: PPTP with Dynamic IP, n=5: PPTP with Static IP, n=6: L2TP with Dynamic IP n=7: L2TP with Static IP n=A: 3G/4G USB Modem(PPP mode) n=B: 3G/4G USB Modem(DHCP mode)
<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-S <isp name>	It means to set ISP Name (max. 23 characters).
-P <on/off>	It means to enable PPPoE Service.
-u <username>	It means to set username (max. 49 characters) for Internet accessing.
-p <password>	It means to set password (max. 49 characters) for Internet accessing.
-a n	It means to set PPP Authentication Type and n means different types (represented by 0-1).

	n=0: PAP/CHAP (this is default setting) n=1: PAP Only
-t n	It means to set connection duration and n means different conditions. n=-1: Always-on n=1 ~ 999: Idle time for offline (default 180 seconds)
-i <ip address>	It means that *PPPoE server* will assign an IP address specified here for CPE (PPPoE client). If you type 0.0.0.0 as the <ip address>, ISP will assign suitable IP address for you. However, if you type an IP address here, the router will use that one as a fixed IP.
-w <ip address>	It means to assign WAN IP address for such connection. Please type an IP address here for WAN port.
-n <netmask>	It means to assign netmask for WAN connection. You have to type 255.255.255.xxx (x is changeable) as the netmask for WAN port.
-g <gateway>	It means to assign gateway IP for such WAN connection.
-s <server ip>	It means to set PPTP/L2TP Server IP. <server ip>= ppp.qqq.rrr.sss: PPTP/L2TP server IP
-A <idx>	Set to Always On mode, and <idx> as backup WAN#.
-B <mode>	Set to Backup mode. <mode> 0: When any WAN disconnect; 1: When all WAN disconnect.
-V	It means to view Internet Access profile.
-C <sim pin code>	Set (PPP mode) SIM PIN code (max. 15 characters) for 3G/4G USB Modem.
-O <init string>	Set (PPP mode) Modem Initial String (max. 47 characters) for 3G/4G USB Modem.
-T <init string2>	Set (PPP mode) Modem Initial String2 (max. 47 characters) for 3G/4G USB Modem.
-D <dial string>	Set (PPP mode) Modem Dial String (max. 31 characters) for 3G/4G USB Modem.
-v <service name>	Set (PPP mode) Service Name (max. 23 characters) for 3G/4G USB Modem.
-m <ppp username>	Set (PPP mode) PPP Username (max. 63 characters) for 3G/4G USB Modem.
-o <ppp password>	Set (PPP mode) PPP Password (max. 62 characters) for 3G/4G USB Modem.
-e n	Set (PPP mode) PPP Authentication Type for 3G/4G USB Modem. n= 0: PAP/CHAP (default), 1: PAP Only
-q n	(PPP mode) Index(1-15) in Schedule Setup-One
-x n	(PPP mode) Index(1-15) in Schedule Setup-Two
-y n	(PPP mode) Index(1-15) in Schedule Setup-Three
-z n	(PPP mode) Index(1-15) in Schedule Setup-Four
-Q <mode>	Set (PPP mode or DHCP mode) WAN Connection Detection Mode. <mode> 0: ARP Detect; 1: Ping Detect
-I <ping ip>	Set (PPP mode or DHCP mode) WAN Connection Detection Ping IP. <ping ip>= ppp.qqq.rrr.sss: WAN Connection Detection Ping IP

-L n	Set (PPP mode) WAN Connection Detection TTL (1-255) value.
-E <sim pin code>	Set (DHCP mode) SIM PIN code (max. 19 characters).
-G <mode>	Set (DHCP mode) Network Mode. <mode> 0: 4G/3G/2G; 1: 4G Only; 2: 3G Only; 3: 2G Only
-N <apn name>	Set (DHCP mode) APN Name (max. 47 characters)
-U n	(DHCP mode) MTU(1000-1440)

Example

```
>internet -M 1 -S tcom -u username -p password -a 0 -t -1  -i 0.0.0.0
 WAN1 Internet Mode set to PPPoE/PPPoA
 WAN1 ISP Name set to tcom
 WAN1 Username set to username
 WAN1 Password set successful
 WAN1 PPP Authentication Type set to PAP/CHAP
 WAN1 Idle timeout set to always-on
 WAN1 Gateway IP set to 0.0.0.0
> internet -V
WAN1 Internet Mode:PPPoE
ISP Name: tcom
Username: username
Authentication: PAP/CHAP
Idle Timeout: -1
WAN IP: Dynamic IP
> internet -M 1 -u link1 -p link1 -a 0
 WAN1 Internet Mode set to PPPoE/PPPoA
 WAN1 Username set to link1
 WAN1 Password set successful
 WAN1 PPP Authentication Type set to PAP/CHAP
```

Telnet Command: ip pubsubnet

This command allows users to enable or disable the public subnet for your router.

Syntax

ip pubsubnet <*Enable*/*Disable*>

Syntax Description

Parameter	Description
Enable	Enable the function.
Disable	Disable the function.

Example

```
> ip pubsubnet enable
public subnet enabled!
```

Telnet Command: ip pubaddr

This command allows to set the **IP routed subnet** for the router.

Syntax

ip pubaddr *?*

ip pubaddr <*public subnet IP address*>

Syntax Description

Parameter	Description
?	Display an IP address which allows users set as the public subnet IP address.
public subnet IP address	Specify an IP address. The system will set the one that you specified as the public subnet IP address.

Example

```
> ip pubaddr ?
% ip addr <public subnet IP address>
% Now: 192.168.0.1

> ip pubaddr 192.168.2.5
% Set public subnet IP address done !!!
```

Telnet Command: ip pubmask

This command allows users to set the mask for IP routed subnet of your router.

Syntax

ip pubmask *?*

ip pubmask <*public subnet mask*>

Syntax Description

Parameter	Description
?	Display an IP address which allows users set as the public subnet mask.
public subnet IP address	Specify a subnet mask. The system will set the one that you specified as the public subnet mask.

Example

```
> ip pubmask ?
% ip pubmask <public subnet mask>
% Now: 255.255.255.0

> ip pubmask 255.255.0.0
% Set public subnet mask done !!!
```

Telnet Command: ip aux

This command is used for configuring WAN IP Alias.

Syntax

ip aux add *[IP] [Join to NAT Pool][wanX]*

ip aux remove *[index]*

Syntax Description

Parameter	Description
add	It means to create a new WAN IP address.
remove	It means to delete an existed WAN IP address.
IP	It means the auxiliary WAN IP address.
Join to NAT Pool	0 (disable) or 1 (enable).
wanX	Add or remove an address for WAN interface.
index	Type the index number of the table displayed on your screen.

Example

```
> ip aux add 192.168.1.65 1
% 192.168.1.65 has added in index 2.

> ip aux ?%% ip aux add [IP] [Join to NAT Pool]
%% ip aux remove [Index]

%%    Where IP = Auxiliary WAN IP Address.
%%         Join to NAT Pool = 0 or 1.
%%         Index = The Index number of table.

Now auxiliary WAN1 IP Address table:
Index no.      Status  IP address     NAT IP pool
-----------------------------------------------------
  1          Disable 0.0.0.0 Yes
  2          Enable  192.168.1.65   Yes
```

When you type *ip aux*?, the current auxiliary WAN IP Address table will be shown as the following:

```
Index no.   Status  IP address      IP pool
-------------------------------------------
    1       Enable  172.16.3.229    Yes
    2       Enable  172.16.3.56     No
    3       Enable  172.16.3.113    No
```

Telnet Command: ip addr

This command allows users to set/add a specified LAN IP your router.

Syntax

ip addr *[IP address]*

Syntax Description

Parameter	Description
IP address	It means the LAN IP address.

Example

```
>ip addr 192.168.50.1
% Set IP address OK !!!
```

Info

When the LAN IP address is changed, the start IP address of DHCP server are still the same. To make the IP assignment of the DHCP server being consistent with this new IP address (they should be in the same network segment), the IP address of the PC must be fixed with the same LAN IP address (network segment) set by this command for accessing into the 網頁使用者介面 of the router. Later, modify the start addresses for the DHCP server.

Telnet Command: ip nmask

This command allows users to set/add a specified netmask for your router.

Syntax

ip nmask *[IP netmask]*

Syntax Description

Parameter	Description
IP netmask	It means the netmask of LAN IP.

Example

```
> ip nmask 255.255.0.0
% Set IP netmask OK !!!
```

Telnet Command: ip arp

ARP displays the matching condition for IP and MAC address.

Syntax

ip arp add *[IP address] [MAC address] [LAN or WAN]*

ip arp del *[IP address] [LAN or WAN]*

ip arp flush

ip arp status

ip arp accept *[0/1/2/3/4/5/status]*

ip arp setCacheLife *[time]*

In which, **arp add** allows users to add a new IP address into the ARP table; **arp del** allows users to remove an IP address; **arp flush** allows users to clear arp cache; **arp status** allows users to review current status for the arp table; **arp accept** allows to accept or reject the source /destination MAC address; arp **setCacheLife** allows users to configure the duration in which ARP caches can be stored on the system. If **ip arp setCacheLife** is set with "60", it means you have an ARP cache at 0 second. Sixty seconds later without any ARP messages received, the system will think such ARP cache is expired. The system will issue a few ARP request to see if this cache is still valid.

Syntax Description

Parameter	Description
IP address	It means the LAN IP address.
MAC address	It means the MAC address of your router.
LAN or WAN	It indicates the direction for the arp function.
0/1/2/3/4/5	0: disable to accept illegal source mac address 1: enable to accept illegal source mac address 2: disable to accept illegal dest mac address 3: enable to accept illegal dest mac address 4: Decline VRRP mac into arp table 5: Accept VRRP mac into arp table status: display the setting status.
Time	Available settings will be 10, 20, 30,....2550 seconds.

Example

```
> ip arp accept status
Accept illegal source mac arp: disable

Accept illegal dest mac arp: disable

Accept VRRP mac into arp table: disable
> ip arp status
[ARP Table]
 Index IP Address       MAC Address        Netbios Name
   1   192.168.1.113     00-05-5D-E4-D8-EE    A1000351
```

Telnet Command: ip dhcpc

This command is available for WAN DHCP.

Syntax

ip dhcpc *option*

ip dhcpc *option -h|l*

ip dhcpc *option -d [idx]*

ip dhcpc *option -e [1 or 0] -w [wan unmber] -c [option number] -v [option value]*

ip dhcpc *option -e [1 or 0] -w [wan unmber] -c [option number] -x "[option value]"*

ip dhcpc *option -u [idx unmber]*

ip dhcpc *release [wan number]*

ip dhcpc *renew [wan number]*

ip dhcpc *status*

Syntax Description

Parameter	Description
option	It is an optional setting for DHCP server. -h: display usage -l: list all custom set DHCP options -d: delete custom dhcp client option by index number

	-e: enable/disable option feature, 1:enable, 0:disable -w: set WAN number (e.g., 1=WAN1) -c: set option number: 0~255 -v: set option value by string -x: set option value by raw byte (hex) -u: update by index number
release	It means to release current WAN IP address.
renew	It means to renew the WAN IP address and obtain another new one.
status	It displays current status of DHCP client.

Example

```
>ip dhcpc status
I/F#3 DHCP Client Status:

DHCP Server IP      : 172.16.3.7
WAN Ipm             : 172.16.3.40
WAN Netmask         : 255.255.255.0
WAN Gateway         : 172.16.3.1
Primary DNS         : 168.95.192.1
Secondary DNS       : 0.0.0.0
Leased Time         : 259200
Leased Time T1      : 129600
Leased Time T2      : 226800
Leased Elapsed      : 259194
Leased Elapsed T1   : 129594
Leased Elapsed T2   : 226794
```

Telnet Command: ip ping

This command allows users to ping IP address of WAN1/WAN2/PVC3/PVC4/PVC5 for verifying if the WAN connection is OK or not.

Syntax

ip ping *[IP address] [WAN1 /PVC3/PVC4/PVC5]*

Syntax Description

Parameter	Description
IP address	It means the WAN IP address.
WAN1/PVC3/PVC4/PVC5	It means the WAN port /PVC that the above IP address passes through.

Example

```
>ip ping 172.16.3.229 WAN1
Pinging 172.16.3.229 with 64 bytes of Data:
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
Packets: Sent = 5, Received = 5, Lost = 0 <0% loss>
```

Telnet Command: ip tracert

This command allows users to trace the routes from the router to the host.

Syntax

ip tracert *[Host/IP address] [WAN1/WAN2] [Udp/Icmp]*

Syntax Description

Parameter	Description
IP address	It means the target IP address.
WAN1/WAN2	It means the WAN port that the above IP address passes through.
Udp/Icmp	It means the UDP or ICMP.

Example

```
>ip tracert 22.128.2.62 WAN1
Traceroute to 22.128.2.62, 30 hops max
1   172.16.3.7  10ms
2   172.16.1.2  10ms
3   Request Time out.
4   168.95.90.66    50ms
5   211.22.38.134   50ms
6   220.128.2.62    50ms
Trace complete
```

Telnet Command: ip telnet

This command allows users to access specified device by telnet.

Syntax

ip telnet *[IP address][Port]*

Syntax Description

Parameter	Description
IP address	Type the WAN or LAN IP address of the remote device.
Port	Type a port number (e.g., 23). Available settings: 0 ~65535.

Example

```
> ip telnet 172.17.3.252 23
>
```

Telnet Command: ip rip

This command allows users to set the RIP (routing information protocol) of IP.

Syntax

ip rip *[0/1/2]*

Syntax Description

Parameter	Description
0/1/2	0 means disable; 1 means first subnet and 2 means second subnet.

Example

```
> ip rip 1
%% Set RIP 1st subnet.
```

Telnet Command: ip wanrip

This command allows users to set the RIP (routing information protocol) of WAN IP.

Syntax

ip wanrip *[ifno] -e [0/1]*

Syntax Description

Parameter	Description
ifno	It means the connection interface. 1: WAN1,2: WAN2, 3: PVC3,4: PVC4,5: PVC5 **Note**: PVC3 ~PVC5 are virtual WANs.
-e	It means to disable or enable RIP setting for specified WAN interface. 1: Enable the function of setting RIP of WAN IP. 0: Disable the function.

Example

```
> ip wanrip ?
 Valid ex:ip wanrip <ifno> -e <0/1>
 <ifno> 1: WAN1,2: WAN2
       3: PVC3,4: PVC4,5: PVC5
 -e <0/1>  0: disable, 1: enable
 Now status:
 WAN[1] Rip Protocol disable
 WAN[2] Rip Protocol disable
 WAN[3] Rip Protocol disable
 WAN[4] Rip Protocol disable
 WAN[5] Rip Protocol disable
> ip wanrip 5 -e 1
> ip wanrip ?
 Valid ex:ip wanrip <ifno> -e <0/1>
 <ifno> 1: WAN1,2: WAN2
       3: PVC3,4: PVC4,5: PVC5
 -e <0/1>  0: disable, 1: enable
 Now status:
 WAN[1] Rip Protocol disable
 WAN[2] Rip Protocol disable
 WAN[3] Rip Protocol disable
 WAN[4] Rip Protocol disable
 WAN[5] Rip Protocol enable
```

Telnet Command: ip route

This command allows users to set static route.

Syntax

ip route *add [dst] [netmask][gateway][ifno][rtype]*

ip route *del [dst] [netmask][rtype]*

ip route *status*

ip route *cnc*

ip route *default [wan1/wan2/off/?]*

ip route *clean [1/0]*

Syntax Description

Parameter	Description
add	It means to add an IP address as static route.
del	It means to delete specified IP address.
status	It means current status of static route.
dst	It means the IP address of the destination.
netmask	It means the netmask of the specified IP address.
gateway	It means the gateway of the connected router.
ifno	It means the connection interface. 3=WAN1 5=WAN3,6=WAN4,7=WAN5 However, WAN3, WAN4, WAN5 are router-borne WANs
rtype	It means the type of the route. default : default route; static: static route.
cnc	It means current IP range for CNC Network.
default	Set WAN1/WAN2/off as current default route.
clean	Clean all of the route settings. 1: Enable the function. 0: Disable the function.

Example

```
> ip route add 172.16.2.0 255.255.255.0 172.16.2.4 3 static
> ip route status

Codes: C - connected, S - static, R - RIP, * - default, ~ - private
C~      192.168.1.0/   255.255.255.0 is directly connected, LAN1
S        172.16.2.0/   255.255.255.0 via 172.16.2.4, WAN1
```

Telnet Command: ip igmp_proxy

This command allows users to enable/disable igmp proxy server.

Syntax

ip igmp_proxy *set*

ip igmp_proxy *reset*

ip igmp_proxy *wan*

ip igmp_proxy *t_home[on/off/show/help]*

ip igmp_proxy *query*

ip igmp_proxy *ppp [0/1]*

ip igmp_proxy *status*

Syntax Description

Parameter	Description
set	It means to enable proxy server.
reset	It means to disable proxy server.
wan	It means to specify WAN interface for IGMP service.
t_home	It means to specify t_home proxy server for using.
On/off/show/help	It means to turn on/off/display or get more information of the T_home service.
query	It means to set IGMP general query interval. The default value is 125000 ms.
ppp	0 – No need to set IGMP with PPP header. 1 – Set IGMP with PPP header.
status	It means to display current status for proxy server.

Example

```
> ip igmp t_home on
%T-Home Setting:
%T-Home Service is turned on.
%WAN1 : Enabled, connection type: PPPoE, without tag for ADSL
%WAN5 : Enabled, connection type: DHCP, tag: 8
%: PVC4(WAN5) is bound to PVC0(WAN1), protocol=MPoA 1483 Bridge
%IGMP Proxy Interface: WAN5(PVC)
%WAN5 for Router-borne Application/ IPTV on/off: ON
> ip igmp_proxy query 130000
 This command is for setting IGMP General Query Interval
 The default value is 125000 ms
 Current Setting is:130000 ms
>
```

Telnet Command: ip igmp_snoop

This command allows users to enable or disable IGMP snoop function.

Syntax

ip igmp_snoop enable

ip igmp_snoop disable

ip igmp_snoop status

ip igmp_snoop table

ip igmp_snoop txquery

ip igmp_snoop mode

ip igmp_snoop chkleave

ip igmp_snoop separate

ip igmp_snoop portchk

Syntax Description

Parameter	Description
enable	It means to enable igmp snoop function
disable	It means to disable igmp snoop function.
status	It means to display current igmp configuration.
table	It means to display current configuration of igmp.
txquery	It means to send out IGMP QUERY to LAN periodically.
mode	It means to set software or hardware mode for snooping working on.
chkleave	It means to check the leave status. On: enable the IGMP snoop leave checking function. Off: it will drop LEAVE if still clients on the same group.
separate	It means to set IGMP packets being separated by NAT/Bridge. On: The packets will be separated. Off: The packets will not be separated by NAT/Bridge.
portchk	It means to perform LAN port checking for IGMP packets. On: Perform the LAN port checking. Off: No perform the LAN port checking.

Example

```
> ip igmp_snoop enable
%% ip igmp snooping [enable|disable|status], IGMP Snooping is Enabled.
> ip igmp_snoop disable
%% ip igmp snooping [enable|disable|status], IGMP Snooping is Disabled.
> ip igmp_snoop mode hw
 igmp snooping works on SW mode now.
> ip igmp_snoop mode ?
% ip igmp mode [hw/sw]
 igmp snooping works on HW mode now.
> ip igmp_snoop separate ?
% ip igmp separate [on/off]
 igmp snoop seprate is ON now.
 igmp packets will be separated by  NAT/Bridge.
```

Telnet Command: ip igmp_fl

This command allows users to activate IGMP fast leave and display current status for IGMP fast leave.

Syntax

ip igmp_fl enable

ip igmp_fl disable

ip igmp_fl status

Syntax Description

Parameter	Description
enable / disable	It means to enable / disable the function of IGMP fast leave.
status	It menas to show current status of IGMP fast leave.

Example

```
> ip igmp_snoop enable
%% ip igmp snooping [enable|disable|status], IGMP Snooping is Enabled.
> ip igmp_fl enable
%% ip igmp_fl [enable|disable|status], IGMP Fast Leave is Enabled.
> ip igmp_fl status
%% ip igmp_fl [enable|disable|status], IGMP Fast Leave is Disabled.
```

Telnet Command: ip dmz

Specify MAC address of certain device as the DMZ host.

Syntax

ip dmz *[mac]*

Syntax Description

Parameter	Description
mac	It means the MAC address of the device that you want to specify

Example

```
>ip dmz ?
% ip dmz <mac>,  now : 00-00-00-00-00-00
> ip dmz 11-22-33-44-55-66
> ip dmz ?
% ip dmz <mac>,  now : 11-22-33-44-55-66
>
```

Telnet Command: ip dmzswitch

This command allows users to set DMZ mode.

ip dmzswitch *off*

ip dmzswitch *private*

ip dmzswitch *trueip*

ip dmzswitch *active_trueip*

Syntax Description

Parameter	Description
off	It means to turn off DMZ function.
private	It means to set DMZ with private IP.
trueip	It means to set DMZ with true IP.
active_trueip	It means to set the DMZ with active true IP.

Example

```
>ip ip dmzswitch off
>
```

Telnet Command: ip session

This command allows users to set maximum session limit number for the specified IP; set message for exceeding session limit and set how many seconds the IP session block works.

Syntax

ip session *on*

ip session *off*

ip session *default [num]*

ip session *defaultp2p [num]*

ip session *status*

ip session *show*

ip session *timer [num]*

ip session *[block/unblock][IP]*

ip session *[add/del][IP1-IP2][num][p2pnum]*

Syntax Description

Parameter	Description
on	It means to turn on session limit for each IP.
off	It means to turn off session limit for each IP.
default [num]	It means to set the default number of session num limit.
Defaultlp2p [num]	It means to set the default number of session num limit for p2p.
status	It means to display the current settings.
show	It means to display all session limit settings in the IP range.
timer [num]	It means to set when the IP session block works. The unit is second.
[block/unblock][IP]	It means to block/unblock the specified IP address. Block: The IP cannot access Internet through the router. Unblock: The specified IP can access Internet through the router.
add	It means to add the session limits in an IP range.
del	It means to delete the session limits in an IP range.

IP1-IP2	It means the range of IP address specified for this command.
num	It means the number of the session limits, e.g., 100.
p2pnum	It means the number of the session limits, e.g., 50 for P2P.

Example

```
>ip session default 100
> ip session add 192.168.1.5-192.168.1.100 100 50
> ip session on
> ip session status

  IP range:
    192.168.1.5 - 192.168.1.100 : 100

  Current ip session limit is turn on

  Current default session number is 100
```

Telnet Command: ip bandwidth

This command allows users to set maximum bandwidth limit number for the specified IP.

Syntax

ip bandwidth *on*

ip bandwidth *off*

ip bandwidth *default [tx_rate][rx_rate]*

ip bandwidth *status*

ip bandwidth *show*

ip bandwidth *[add/del] [IP1-IP2][tx][rx][shared]*

Syntax Description

Parameter	Description
on	It means to turn on the IP bandwidth limit.
off	It means to turn off the IP bandwidth limit.
default [tx_rate][rx_rate]	It means to set default tx and rx rate of bandwidth limit. The range is from 0 – 65535 Kpbs.
status	It means to display the current settings.
show	It means to display all the bandwidth limits settings within the IP range.
add	It means to add the bandwidth within the IP range.
del	It means to delete the bandwidth within the IP range.
IP1-IP2	It means the range of IP address specified for this command.
tx	It means to set transmission rate for bandwidth limit.
rx	It means to set receiving rate for bandwidth limit.
shared	It means that the bandwidth will be shared for the IP range.

Example

```
> ip bandwidth default 200 800
> ip bandwidth add 192.168.1.50-192.168.1.100 10 60
> ip bandwidth status

  IP range:
    192.168.1.50 - 192.168.1.100 : Tx:10K Rx:60K

  Current ip Bandwidth limit is turn off


  Auto adjustment is off
```

Telnet Command: ip bindmac

This command allows users to set IP-MAC binding for LAN host.

Syntax

ip bindmac *on*

ip bindmac *off*

ip bindmac *strict_on*

ip bindmac *show*

ip bindmac *add [IP][MAC][Comment]*

ip bindmac *del [IP]/all*

Syntax Description

Parameter	Description
on	It means to turn on IP bandmac policy. Even the IP is not in the policy table, it can still access into network.
off	It means to turn off all the bindmac policy.
strict_on	It means that only those IP address in IP bindmac policy table can access into network.
show	It means to display the IP address and MAC address of the pair of binded one.
add	It means to add one ip bindmac.
del	It means to delete one ip bindmac.
IP	It means to type the IP address for binding with specified MAC address.
MAC	It means to type the MAC address for binding with the IP address specified.
Comment	It means to type words as a brief description.
All	It means to delete all the IP bindmac settings.

Example

```
> ip bindmac add 192.168.1.46 00:50:7f:22:33:55 just for test
> ip bindmac show
ip bind mac function is turned ON
IP : 192.168.1.46 bind MAC : 00-50-7f-22-33-55 Comment : just
```

Telnet Command: ip bgp

This command allows users to configure settings for BGP.

Syntax

ip bgp mode *[0/1]*

ip bgp as *[value]*

ip bgp hold *[value]*

ip bgp retry *[value]*

ip bgp id *[value]*

ip bgp show

ip bgp neighbor *[idx]* **mode** *[0/1]*

ip bgp neighbor *[idx]* **name** *[max len: 20]*

ip bgp neighbor *[idx]* **ip** *[x.x.x.x]*

ip bgp neighbor *[idx]* **as** *[1~4294967295]*

ip bgp neighbor *[idx]* **show**

ip bgp neighbor show all

ip bgp static *[sidx][ip][<netmask]*

ip bgp static *[sidx]* **delete**

ip bgp static show

Syntax Description

Parameter	Description
mode <0/1>	It means to enable / disable BGP mode. 0: disable 1: enable
as <value>	It means to set the AS number for local router. <value>: Available number is between 0 and 4294967295.
hold <value>	It means to set the time interval to determine the peer is dead when the router is unable to receive any keepalive message from the peer within the time. <value>: Available number is between 10 and 65535 (unit: second). The default is 180 (seconds).
retry <value>	It means to set a period of time to reconnect if the router fails to connect to the neighboring router. <value>: Available number is between 3 and 255 (unit: second). The default is 120 (seconds).
id <value>	It means to specify the LAN subnet <1~16> as router ID. <value>: Available number is between 1 and 16.
show	It means to display information related to BGP settings.
neighbor <idx> mode <0/1>	It means to enable / disable the basic BGP function for neighboring router. <idx>: Available profile number is between 1 and 8. <0/1>: 0- disable; 1- enable
neighbor <idx> name <max len: 20>	It means to define a profile name for neighboring router. <idx>: Available profile number is between 1 and 8. <max len>: The maximum name length shall not be over 20

	characters.
neighbor <idx> ip <x.x.x.x>	It means to set the IP address specified for the neighboring router. <idx>: Available profile number is between 1 and 8. <x.x.x.x>: Type the IP address, e.g., 100.100.100.100.
neighbor <idx> as <1~4294967295>	It means to set the AS number for the neightboring router. <idx>: Available profile number is between 1 and 8. <value>: Available number is between 1 and 4294967295.
neighbor <idx> show	It means to display information for the specified profile. <idx>: Available profile number is between 1 and 8.
neighbor show all	It means to display information for all neighboring routers.
static <sidx> <ip> <netmask>	It means to configure the neighboring router(s) for exchanging the routing information with the local router. <sidx>: Available profile number is between 1 and 6. <ip>: Type the IP address, e.g., 100.100.100.200. <netmask>: Type the subnet mask for the neighboring router, e.g., 255.255.255.0.
static <sidx> delete	It means to delete static network settings for neighboring router. <sidx>: Available profile number is between 1 and 6.
static show	It means to display setting information for exchanging the routing information with the local router.

Example

```
> ip bgp static 1 192.168.2.56 255.255.255.0
Set static network index: 1
IP addr: 192.168.2.56
Net mask: 255.255.255.0
> ip bgp static show
BGP static networks:
Index: 1, IP addr: 192.168.2.56, mask: 255.255.255.0
```

Telnet Command: ip maxnatuser

This command is used to set the maximum number of NAT users.

Syntax

ip maxnatuser *user no*

Syntax Description

Parameter	Description
User no	A number specified here means the total NAT users that Vigor router supports. 0 – It means no limitation.

Example

```
> ip maxnatuser 100
% Max NAT user = 100
```

Telnet Command: ip policy_rt

This command is used to set the IP policy route profile.

Syntax

ip policy_rt *[-<command> <parameter> | …]*

Syntax Description

Parameter	Description
<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
General Setup for Policy Route	
-i [value]	Specify an index number for setting policy route profile. Value: 1 to 60. "-1" means to get a free policy index automatically.
-e [0/1]	0: Disable the selected policy route profile. 1: Enable the selected policy route profile.
-o [value]	Determine the operation of the policy route. Value: add – Create a new policy rotue profile. del – Remove an existed policy route profile. edit – Modify an existed policy route profile. flush – Reset policy route to default setting.
-1 [any/range]	Specify the source IP mode. Range: Indicate a range of IP addresses. Any: It means any IP address will be treated as source IP address.
-2 [any/ip_range/ip_subnet/domain]	Specify the destination IP mode. Any: No need to specify an IP address for any IP address will be treated as destination IP address. ip_range: Indicates a range of IP addresses. ip_subnet: Indicates the IP subnet. domain: Indicates the domain name.
-3 [any/range]	Specify the destination port mode. Range: Indicate a range of port number.

	Any: It means any port number can be used as destination port.
-G [default/specific]	Specify the gateway mode.
-L [default/specific]	Specify the failover gateway mode.
-s [value]	Indicate the source IP start. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.1.0)
-S [value]	Indicate the source IP end. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.1.100)
-d [value]	Indicate the destination IP start. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.2.0)
-D [value]	Indicate the destination IP end. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.2.100)
-p [value]	Indicate the destination port start. Value: Type a number (1 ~ 65535) as the port start (e.g., 1000).
-P [value]	Indicate the destination port end. Value: Type a number (1 ~ 65535) as the port end (e.g., 2000).
-y [value]	Indicate the priority of the policy route profile. Value: Type a number (0 ~ 250). The default value is “150”.
-I [value]	Indicate the interface specified for the policy route profile. Value: Available interfaces include, LAN1 ~ LAN8, IP_Routed_Subnet, DMZ_Subnet, WAN1 ~ WAN5, VPN_PROFILE_1 ~ VPN_PROFILE_100, WAN_1_IP_ALIAS_1 ~ WAN_4_IP_ALIAS_8
-g [value]	Indicate the gateway IP address. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.3.1)
-I [value]	Indicate the failover IP address. Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.4.1)
-t [value]	It means “protocol”. Value: Available settings include “TCP”, “UDP”, “TCP/UDP”, “ICMP” and “Any”.
-n [0/1]	Indicates the function of “Force NAT”. 0: Disable the function. 1: Enable the function.
-a [0/1]	Indicates to enable the function of failover. 0: Disable the function. 1: Enable the function.
-f [value]	It means to specify the interface for failover. Value: Avaialbe interfaces include, NO_FAILOVER, Default_WAN, Policy1 ~ Policy60 LAN1 ~ LAN8 IP_Routed_Subnet, DMZ_Subnet, WAN1 ~ WAN5, VPN_PROFILE_1 ~ VPN_PROFILE_100, WAN_1_IP_ALIAS_1 ~ WAN_4_IP_ALIAS_8
-b [value]	It means “failback”. Value: Available settings include, 0: Disable the function of “failback”.

	1: Enable the function of “failback”. -v: View current failback setting.
Diagnose for Policy Route	
-s [value]	It means “source IP”. Value: Available settings include: Any: It indicates any IP address can be used as source IP address. “xxx.xxx.xxx.xxx”: The type format (e.g, 192.168.1.0).
-d [value]	It means “destination IP”. Value : Available settings include: Any: It indicates any IP address can be used as destination IP address. “xxx.xxx.xxx.xxx”: Specify an IP address.
-p [value]	It means “destination port”. Value: Specify a number or type Any (indicating any number).
-t [value]	It means “protocol”. Value: Available settings include “ICMP”, “TCP”, “UDP” and “Any”.

Example

```
> ip policy_rt diagnose -s 192.168.1.100 -d any -p any -t ICMP

   ------------------------------------------------
      Matched Route  (Priority)
   ------------------------------------------------
   * No_Match

   ------------------------------------------------
      Matched Policy (Priority)
   ------------------------------------------------
   * Policy_1 (200)

   * Conclusion:The packet was dropped because the send-to interface
of the mat
ched policy "policy 1" was inactive and there was no failover setting
> 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
```

Telnet Command: ip lanDNSRes

This command is used to set LAN DNS profiles. With such feature, the user can configure some services (such as ftp, www or database) with domain name which is easy to be accessed.

Syntax

ip lanDNSRes *[-<command> <parameter> | ...]*

Parameter	Description
-a <IP Address>	It is used to configure IP address mapping (IPv4/IPv6 Address or multiple subnet addresses). *IP Address:* type the IP address (e.g., 192.168.1.56).
-d <address mapping index number>	It means to delete index number with address mapping configured. *address mapping index number :* type the index number which represents the address mapping profile.
-e <0/1>	It means to enable or disable the function of LAN DNS or DNS Forwarding Profile.

	0: disable *1*: enable
-i <profile setting index number>	It means to create LAN DNS profile with specified domain name. *profile setting index number :* type the index number which represents the profile with domain name configured.
-l	It means to list detailed information of profile configuration**.** > ip lanDNSRes -l % % Idx: 7 % State: Enable % Profile: DrayTekFTP % Domain Name: ftp.draytek.com % -------- Address Mapping Table -------- % Idx ReplyOnlySameSubnet IP Address % 1 Yes 172.16.2.10 % 2 Yes 172.16.3.10 % 3 Yes 172.16.4.10
-n<domain name>	It means to specify a domain name to be accessed.
-p<profile name>	It means to set name of the LAN DNS profile.
-r	It means to clear specified domain name profile and the address mapping setting.
-s<0/1>	It means to determine all subnet packets or only the packets with the same subnet will be replied for address mapping profile. *0:* reply all subnet packets. *1*: reply only same subnet packet.
-z	It means to update LAN DNS configuration to DNS cache.

Example

```
> ip lanDNSRes -i 1 -n ftp.drayTek.com
% Configure Set1's DomainName:ftp.drayTek.com
> ip lanDNSRes -i 1 -n ftp.drayTek.com
> ip lanDNSRes -i 1 -a 172.16.2.10 -s 1
> ip lanDNSRes -i 1 -a 172.16.3.10 -s 1
> ip lanDNSRes -i 1 -a 172.16.4.10 -s 1
> ip lanDNSRes -l
%
% Idx: 7
% State: Enable
% Profile: DrayTekFTP
% Domain Name: ftp.draytek.com
% -------- Address Mapping Table --------
% Idx ReplyOnlySameSubnet IP Address
% 1   Yes               172.16.2.10
% 2   Yes               172.16.3.10
% 3   Yes               172.16.4.10
```

Telnet Command: ip dnsforward

This command is used to set LAN DNS profile for conditional DNS forwarding.

ip dnsforward *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
[<command>	The available commands with parameters are listed below.

<parameter>|…]	*[…]* means that you can type in several commands in one line.
-a <IP Address>	Set forwarded DNS server IP Address.
-d <DNS server mapping index number>	Delete the selected LAN DNS profile.
-e <0/1>	0: disable such function. 1: enable such function.
-i <profile setting index number>	Type the index number of the profile.
-l	List the content of LAN DNS profile (including domain name, IP address and message).
-n <domain name>	Set domain name.
-p <profile name>	Set profile name for LAN DNS.
-r	Reset the settings for selected profile.

Example

```
> ip dnsforward -i 1 -n ftp.drayTek.com
% Configure Set1's DomainName:ftp.drayTek.com
> ip dnsforward -i 1 -a 172.16.1.1
% Configure Set1's IP:172.16.1.1
> ip dnsforward -i 1 -l
% Idx: 1
% State: Disable
% Profile: test
% Domain Name: ftp.drayTek.com
% DNS Server IP: 172.16.1.1
>
```

Telnet Command: ip6 addr

This command allows users to set the IPv6 address for your router.

Syntax

ip6 addr -s *[prefix] [prefix-length] [LAN|WAN1|WAN2|iface#]*

ip6 addr -d *[prefix] [prefix-length] [LAN|WAN1|WAN2|iface#]*

ip6 addr -a *[LAN|WAN1|WAN2|iface#]*

Syntax Description

Parameter	Description
-s	It means to add a static ipv6 address.
-d	It means to delete an ipv6 address.
-a	It means to show current address(es) status.
-u	It means to show only unicast addresses.
prefix	It means to type the prefix number of IPv6 address.
prefix-length	It means to type a fixed value as the length of the prefix.
LAN|WAN1|WAN2|iface#	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 addr -a
LAN
Unicast Address:
 FE80::250:7FFF:FE00:0/64 (Link)
Multicast Address:
 FF02::2
 FF02::1:FF00:0
 FF02::1
```

Telnet Command: ip6 dhcp req_opt

This command is used to configure option-request settings for DHCPv6 client.

Syntax

ip6 dhcp *req_opt* [*LAN*|*WAN1*|*WAN2*|*iface#] [-<*command*> <*parameter*>| …]

Syntax Description

Parameter	Description
req_opt	It means option-request.
LAN|*WAN1*|*WAN2*|*iface#*	It means to specify LAN or WAN interface for such address.
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-a	It means to show current DHCPv6 status.
-s	It means to ask the SIP.
-S	It means to ask the SIP name.
-d	It means to ask the DNS setting.
-D	It means to ask the DNS name.
-n	It means to ask NTP.
-i	It means to ask NIS.
-I	It means to ask NIS name.
-p	It means to ask NISP.
-P	It means to ask NISP name.
-b	It means to ask BCMCS.
-B	It means to ask BCMCS name.
-r	It means to ask refresh time.
Parameter	1: the parameter related to the request will be displayed. 0: the parameter related to the request will not be displayed.

Example

```
> ip6 dhcp req_opt WAN2 -S 1
> ip6 dhcp req_opt WAN2 -r 1
> ip6 dhcp req_opt WAN2 -a
% Interface WAN2 is set to request following DHCPv6 options:
%    sip name
```

```
>
```

Telnet Command: ip6 dhcp client

This command allows you to use DHCPv6 protocol to obtain IPv6 address from server.

Syntax

ip6 dhcp *client [WAN1|WAN2|iface#] [-<command> <parameter>| ...]*

Syntax Description

Parameter	Description
client	It means the dhcp client settings.
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-a	It means to show current DHCPv6 status.
-p [IAID]	It means to request identity association ID for Prefix Delegation.
-n [IAID]	It means to request identity association ID for Non-temporary Address.
-c [parameter]	It means to send rapid commit to server.
-i [parameter]	It means to send information request to server.
-e[parameter]	It means to enable or disable the DHCPv6 client. 1: Enable 0: Disable

Example

```
> ip6 dhcp client WAN2 –p 2008::1
> ip6 dhcp client WAN2 –a
  Interface WAN2 has following DHCPv6 client settings:
      DHCPv6 client enabled
      request IA_PD whose IAID equals to 2008
> ip6 dhcp client WAN2 –n 1023456
> ip6 dhcp client WAN2 –a
  Interface WAN2 has following DHCPv6 client settings:
      DHCPv6 client enabled
      request IA_NA whose IAID equals to 2008
> system reboot
```

Telnet Command: ip6 dhcp server

This command allows you to configure DHCPv6 server.

Syntax

ip6 dhcp *server [-<command> <parameter>| ...]*

Syntax Description

Parameter	Description
server	It means the dhcp server settings.
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.

-a	It means to show current DHCPv6 status.
-i<pool_min_addr>	It means to set the start IPv6 address of the address pool.
-x<pool_max_addr>	It means to set the end IPv6 address of the address pool.
-d<addr>	It means to set the first DNS IPv6 address.
-D<addr>	It means to set the second DNS IPv6 address.
-c<parameter>	It means to send rapid commit to server. 1: Enable 0: Disable
-e<parameter>	It means to enable or disable the DHCPv6 server. 1: Enable 0: Disable

Example

```
> ip6 dhcp server -d FF02::1
> ip6 dhcp server -i ff02::1
> ip6 dhcp server -x ff02::3
> ip6 dhcp server -a
% Interface LAN has following DHCPv6 server settings:
%    DHCPv6 server disabled
%    maximum address of the pool: FF02::3
%    minimum address of the pool: FF02::1
%   1st DNS IPv6 Addr: FF02::1
```

Telnet Command: ip6 internet

This command allows you to configure settings for accessing Internet.

Syntax

ip6 internet *-W n -M n [-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
-W n	**W** means to set WAN interface and **n** means different selections. Default is WAN1. n=1: WAN1 n=2: WAN2 n=3: WAN3 . . n=X: WANx
-M n	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 – 5) n= 0: Offline, n=1: PPP, n=2: TSPC, n=3: AICCU, n=4: DHCPv6, n=5: Static n=6:6in4-Static

	n=7:6rd
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-m n	It means to set IPv6 MTU. N = any value (0 means “unspecified”).
-u <username>	It means to set Username. <username>= type a name as the username (maximum 63 characters).
-p <password>	It means to set Password. <password> = type a password (maximum 63 characters).
-s <server>	It means to set Tunnel Server IP. <server>= IPv4 address or URL (maximum 63 characters).
-d <server>	It means to set the primary DNS Server IP. <server>= type an IPv6 address for first DNS server.
-D <server>	It means to set the secondary DNS Server IP. <server>= type an IPv6 address for second DNS server.
-t <dhcp/ra/none>	It means to set IPv6 PPP WAN test mode for DHCP or RADVD. <dhcp/ra/none>= type IPv6 address.
-V	It means to view IPv6 Internet Access Profile.
-o	It means to set AICCU always on. 1=On, 0=Off

Example

```
> ip6 internet -W 2 -M 2 -u 88886666 -p draytek123456 –s
amsterdam.freenet6.net
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> system reboot
```

Telnet Command: ip6 neigh

This command allows you to display IPv6 neighbour table.

Syntax

ip6 neigh *-s[inet6_addr] [eth_addr] [LAN|WAN1|WAN2]*

ip6 neigh *-d [inet6_addr] [LAN|WAN1|WAN2]*

ip6 neigh *-a [inet6_addr] [-N LAN|WAN1|WAN2]*

Syntax Description

Parameter	Description
-s	It means to add a neighbour.
-d	It means to delete a neighbour.
-a	It means to show neighbour status.
inet6_addr	Type an IPv6 address
eth_addr	Type submask address.
LAN|WAN1|WAN2	Specify an interface for the neighbor.

Example

```
> ip6 neigh -s 2001:2222:3333::1111 00:50:7F:11:ac:22:WAN2
        Neighbour 2001:2222:3333::1111 successfully added!
> ip6 neigh -a

I/F  ADDR                                      MAC                  STATE
-------------------------------------------------------------------------
LAN FF02::1                                 33-33-00-00-00-01    CONNECTED
WAN2 2001:5C0:1400:B::10B8                  00-00-00-00-00-00    CONNECTED
WAN2 2001:2222:3333::1111                   00-00-00-00-00-00    CONNECTED
WAN2 2001:2222:6666::1111                   00-00-00-00-00-00    CONNECTED
WAN2 ::                                     00-00-00-00-00-00    CONNECTED
LAN  ::                                                          NONE
>
```

Telnet Command: ip6 pneigh

This command allows you to add a proxy neighbour.

Syntax

ip6 pneigh *-s inet6_addr [LAN|WAN1|WAN2]*

ip6 pneigh *-d inet6_addr [LAN|WAN1|WAN2]*

ip6 pneigh *-a [inet6_addr] [-N LAN|WAN1|WAN2]*

Syntax Description

Parameter	Description
-s	It means to add a proxy neighbour.
-d	It means to delete a proxy neighbour.
-a	It means to show proxy neighbour status.
inet6_addr	Type an IPv6 address
LAN|WAN1|WAN2	Specify an interface for the proxy neighbor.

Example

```
> ip6 neigh -s FE80::250:7FFF:FE12:300 LAN
%      Neighbour FE80::250:7FFF:FE12:300 successfully added!
```

Telnet Command: ip6 route

This command allows you to

Syntax

ip6 route *-s [prefix] [prefix-length] [gateway] [LAN|WAN1|WAN2|iface#> [-D]*

ip6 route -*d [prefix] [prefix-length]*

ip6 route -*a [LAN|WAN1|WAN2|iface#]*

Syntax Description

Parameter	Description
-s	It means to add a route.
-*d*	It means to delete a route.
-*a*	It means to show the route status.
-D	It means that such route will be treated as the default route.
prefix	It means to type the prefix number of IPv6 address.
prefix-length	It means to type a fixed value as the length of the prefix.
gateway	It means the gateway of the router.
LAN|WAN1|WAN2|iface#	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 route -s FE80::250:7FFF:FE12:500 16 FE80::250:7FFF:FE12:100 LAN
%      Route FE80::250:7FFF:FE12:500/16 successfully added!
> ip6 route -a LAN
```

```
 PREFIX/PREFIX-LEN  _EXPIRES_  _NEXT-HOP_   I/F  METRIC    STATE     FLAGS
-------------------------------------------------------------------------
 FE80::/128                                  LAN      0   UNICAST     U
                         0    ::
 FE80::250:7FFF:FE00:0/128                   LAN      0   UNICAST     U
                         0    ::
 FE80::/64                                   LAN    256   UNICAST     U
                         0
 FE80::/16                                   LAN   1024   UNICAST     UGA
                         0    FE80::250:7FFF:FE12:100
 FF02::1/128                                  LAN      0   UNICAST     UC
                         0    FF02::1
 FF00::/8                                    LAN    256   UNICAST     U
                         0
 ::/0                                        LAN     -1   UNREACHABLE !
                         0
```

Telnet Command: ip6 ping

This command allows you to pin an IPv6 address or a host.

Syntax

ip6 ping *[IPV6 address/Host] [LAN/WAN1/WAN2]*

Syntax Description

Parameter	Description
IPV6 address/Host	It means to specify the IPv6 address or host for ping.
LAN/WAN1/WAN2	It means to specify LAN or WAN interface for such address.

Example

```
> ip6 ping 2001:4860:4860::8888 WAN2

Pinging 2001:4860:4860::8888 with 64 bytes of Data:

Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms
Receive reply from 2001:4860:4860::8888, time=330ms

Packets: Sent = 5, Received = 5, Lost = 0 <% loss>
>
```

Telnet Command: ip6 tracert

This command allows you to trace the routes from the router to the host.

Syntax

ip6 tracert *[IPV6 address/Host]*

Syntax Description

Parameter	Description
IPV6 address/Host	It means to specify the IPv6 address or host for ping.

Example

```
> ip6 tracert 2001:4860:4860::8888
traceroute to 2001:4860:4860::8888, 30 hops max through protocol ICMP
  1 2001:5C0:1400:B::10B8    340 ms
  2 2001:4DE0:1000:A22::1    330 ms
  3 2001:4DE0:A::1           330 ms
  4 2001:4DE0:1000:34::1     340 ms
  5 2001:7F8:1: :A501:5169:1 330 ms
  6 2001:4860::1:0:4B3       350 ms
  7 2001:4860::8:0:2DAF      330 ms
  8 2001:4860::2:0:66E       340 ms
  9 Request timed out.          *
 10 2001:4860:4860::8888     350 ms
Trace complete.
>
```

Telnet Command: ip6 tspc

This command allows you to display TSPC status.

Syntax

ip6 tspc *[ifno]*

Syntax Description

Parameter	Description
ifno	It means the connection interface. Ifno=1 (means WAN1) Info=2 (means WAN2)

Example

```
> ip6 tspc 2
Local Endpoint v4 Address : 111.243.177.223
Local Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b9
Router DNS name : 8886666.broker.freenet6.net
Remote Endpoint v4 Address :81.171.72.11
Remote Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b8
Tspc Prefixlen : 56
Tunnel Broker: Amsterdam.freenet.net
```

```
Status: Connected

>
```

Telnet Command: ip6 radvd

This command allows you to enable or disable RADVD server.

Syntax

Ip6 radvd *–s [1|0] [lifetime]*

ip6 radvd *–V*

Syntax Description

Parameter	Description
-s	It means to enable or disable the default lifetime of the RADVD server. 1: Enable the RADVD server. 0: Disable the RADVD server.
Lifetime	It means to set the lifetime. The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list. Type the number (unit: second) you want.
-V	It means to show the RADVD configuration.
-r	It means RA default test.
-r [num]	It means RA test for item [num].

Example

```
> ip6 radvd -s 1 1800
> ip6 radvd -V
%  IPv6 Radvd Config:
Radvd : Enable, Default Lifetime : 1800 seconds
```

Telnet Command: ip6 mngt

This command allows you to manage the settings for access list.

Syntax

ip6 mngt list

ip6 mngt list *[add<index> <prefix> <prefix-length>|remove <index>|flush]*

ip6 mngt status

ip6 mngt *[http|telnet|ping|https|ssh] [on|off]*

Syntax Description

Parameter	Description
list	It means to show the setting information of the access list.
status	It means to show the status of IPv6 management.

add	It means to add an IPv6 address which can be used to execute management through Internet.
index	It means the number (1, 2 and 3) allowed to be configured for IPv6 management.
prefix	It means to type the IPv6 address which will be used for accessing Internet.
prefix-length	It means to type a fixed value as the length of the prefix.
remove	It means to remove (delete) the specified index number with IPv6 settings.
flush	It means to clear the IPv6 access table.
http|telnet|ping|https|ssh	These protocols are used for accessing Internet.
on|off	It means to enable (on) or disable (off) the Internet accessing through http/telnet/ping.

Example

```
> ip6 mngt list add 1 FE80::250:7FFF:FE12:1010 128
> ip6 mngt list add 2 FE80::250:7FFF:FE12:1020 128
> ip6 mngt list add 3 FE80::250:7FFF:FE12:2080 128
> ip6 mngt list
% IPv6 Access List :
Index   IPv6 Prefix    Prefix Length
========================================
1      FE80::250:7FFF:FE12:1010       128
2      FE80::250:7FFF:FE12:1020       128
3      FE80::250:7FFF:FE12:2080       128

> ip6 mngt status
% IPv6 Remote Management :
telnet : off,   http : off,    ping : off
```

Telnet Command: ip6 online

This command allows you to check the online status of IPv6 LAN /WAN.

Syntax

ip6 *online [ifno]*

Syntax Description

Parameter	Description
ifno	It means the connection interface. 0=LAN1 1=WAN1 2=WAN2

Example

```
> ip6 online 0
 % LAN 1 online status :
 % Interface : UP
 % IPv6 DNS Server: :: Static
 % IPv6 DNS Server: :: Static
```

```
 % IPv6 DNS Server: :: Static
 % Tx packets = 408, Tx bytes = 32160, Rx packets = 428, Rx bytes =
33636

> ip6 online 1
 % WAN 1 online status :
 % IPv6 WAN1 Disabled
 % Default Gateway : ::
 % UpTime : 0:00:00
 % Interface : DOWN
 % IPv6 DNS Server: :: Static
 % IPv6 DNS Server: :: Static
 % IPv6 DNS Server: :: Static
 % Tx packets = 0, Tx bytes = 0, Rx packets = 0, Rx bytes = 0
```

Telnet Command: ip6 aiccu

This command allows you to set IPv6 settings for WAN interface with connection type of AICCU.

Syntax

ip6 aiccu *[ifno]*

ip6 aiccu subnet *[add <ifno> <prefix> <prefix-length>|remove <ifno>|show <info>]*

Syntax Description

Parameter	Description
ifno	It means the connection interface. 1=WAN1 2=WAN2
add	It means to add an IPv6 address which can be used to execute management through Internet.
prefix	It means to type the IPv6 address which will be used for accessing Internet.
prefix-length	It means to type a fixed value as the length of the prefix.
remove	It means to remove (delete) the specified index number with IPv6 settings.
show	It means to display the AICCU status.

Example

```
> ip6 aiccu subnet add 2 2001:1111:0000::1111 64
> ip6 aiccu 2
Status: Connecting

>ip6 aiccu subnet show 2
IPv6 WAN2 AICCU Subnet Prefix Config:
2001:1111::1111/64
>
```

Telnet Command: ip6 ntp

This command allows you to set IPv6 settings for NTP (Network Time Protocols) server.

Syntax

ip6 ntp –h

ip6 ntp –v

ip6 ntp –p [0/1]

Syntax Description

Parameter	Description
–h	It is used to display the usage of such command.
-v	It is used to show the NTP state.
-p <0/1>	It is used to specify NTP server for IPv6. 0 – Auto 1 – First Query IPv6 NTP Server.

Example

```
> ip6 ntp -p 1
% Set NTP Priority: IPv6 First
```

Telnet Command: ip6 lan

This command allows you to set IPv6 settings for LAN interface.

Syntax

ip6 lan -l n *[-<l:w:d:D:m:o:s> <parameter> | ...]*

Syntax Description

Parameter	Description
–h	It is used to display the usage of such command.
-l n	It means to selete LAN interface to be set. n= 1: LAN1 n= 2: LAN2, ... x: LANx. Default is LAN1
-w n	It means to selete WAN interface to be primary interface. n= 0: None, n=1: WAN1 , n=2: WAN2, ... x: WANx.
-d <server>	It means to set 1st DNS Server IP. <server>= IPv6 Address
-D <server>	It means to set 2nd DNS Server IP. <server>= IPv6 Address
-m n	It means to set ipv6 LAN management. n=0:OFF n=1:SLAAC. Default is SLAAC n=2:DHCPv6
-o n	It means to enable Other option(O-bit) flag. (O-bit is redundant

	when management is DHCPv6) n=0: Disable n=1: Enable.
-e n	It means to add an extension WAN. n: 1: WAN1, 2: WAN2, … x: WANx.
-E n	It means to delete an extension WAN. n: 1: WAN1 ,2: WAN2, … x: WANx.
-b map	It means to set bit map(decimal) for extension WAN. map: bit 0: WAN1 bit 1: WAN2, … bit n: WAN(n+1).
-f n	It means to disable IPv6. n= 1: Disable IPv6, n=0: Enable IPv6.
-R n	It means to enable /disable RIPng. n=1: Enable RIPng, n=0: Disable RIPng.
-s n	It means to show IPv6 LAN setting. n=0:show all. Default is show all. n=1: LAN1 n=2: LAN2, … 4: LAN4, n=5: DMZ.

Example

```
> ip6 lan -l 1 -w 1 -d 2001:4860:4860::8888 -o 1 -f 0 -s 2
%   Set primary WAN1!

%  Set 1st DNS server 2001:4860:4860::8888

%   Set Other Option Enable!

%   [LAN1] support ipv6!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.

% [LAN2] setting:
%  Primary WAN    : WAN1
%  Management     : SLAAC
%  Other Option   : Disable
%  WAN Exten      : None
%  Subnet ID      : 2
%  Static IP(0)   : ::/0
%                 [ifno: 0, enable: 0]
%  Static IP(1)   : ::/0
```

```
%                [ifno: 0, enable: 0]
%  Static IP(2)  : ::/0
%                [ifno: 0, enable: 0]
%  Static IP(3)  : ::/0
%                [ifno: 0, enable: 0]
%  DNS1          : 2001:4860:4860::8888
%  DNS2          : 2001:4860:4860::8844
%  ULA Type      : OFF
%  RIPng         : Enable
```

Telnet Command: ip6 session

This command allows you to set sessions limit for IPv6 address.

Syntax

ip6 session *[on/off/default num/status/show]*

ip6 session *[add/del] [IP1-IP2] [num]*

Syntax Description

Parameter	Description
on	It means to turn on session limit for each IP.
off	It means to turn off session limit for each IP.
default <num>	It means to set the default number of session num limit.
status	It means to display the current settings.
show	It means to display all IP range session limit settings.
add	It means to add the session limit for an IPv6 range. <IP1-IP2> - Specify a range for IPv6 addresses.
del	It means to delete the session limit for an IPv6 range by first IP (IP1) or 'del all'.

Example

```
> ip6 session on
> ip6 session add 2100:ABCD::2-2100:ABCD::10 100
> ip6 session status

  IPv6 range:
    2100:ABCD::2 - 2100:ABCD::10 : 100

  Current ip6 session limit is turn on

  Current default session number is 100
```

Telnet Command: ip6 bandwidth

This command allows you to set IPv6 settings

Syntax

ip6 Bandwidth [*on/off/default tx_rate rx_rate/status/show]*

ip6 Bandwidth *[add/del] [IP1-IP2] [tx][rx][shared]*

Syntax Description

Parameter	Description
on	It means to turn on bandwidth limit for each IP.
off	It means to turn off bandwidth limit for each IP.
default <tx> <rx>	It means to set the default transmission (tx), receiving (rx) rate of bandwidth limit (0-30000 Kbps/Mbps).
status	It means to display the current settings.
show	It means to display all IP range bandwidth limit settings.
add	It means to add the bandwidth limit for an IPv6 range. <IP1-IP2> - Specify a range for IPv6 addresses.
del	It means to delete the bandwidth limit for an IPv6 range by first IP (IP1) or 'del all'.

Example

```
> ip6 bandwidth on
> ip6 bandwidth add 2001:ABCD::2-2001:ABCD::10 512 5M shared
> ip6 bandwidth status

  IPv6 range:
    2001:ABCD::2 - 2001:ABCD::10 : Tx:512K Rx:5M shared

  Current ip6 Bandwidth limit is turn on


  Current default ip6 Bandwidth rate is Tx:2000K Rx:8000K bps
```

Telnet Command: ipf view

IPF users to view the version of the IP filter, to view/set the log flag, to view the running IP filter rules.

Syntax

ipf view *[-VcdhrtzZ]*

Syntax Description

Parameter	Description
-V	It means to show the version of this IP filter.
-c	It means to show the running call filter rules.
-d	It means to show the running data filter rules.
-h	It means to show the hit-number of the filter rules.
-r	It means to show the running call and data filter rules.
-t	It means to display all the information at one time.
-z	It means to clear a filter rule's statistics.
-Z	It means to clear IP filter's gross statistics.

Example

```
> ipf view -V -c -d
ipf: IP Filter: v3.3.1 (1824)
```

```
Kernel: IP Filter: v3.3.1
Running: yes
Log Flags: 0x80947278 = nonip
Default: pass all, Logging: available
```

Telnet Command: ipf set

This command is used to set general rule for firewall.

Syntax

ipf set *[Options]*

ipf set *[SET_NO] rule [RULE_NO] [Options]*

Syntax Description

Parameter	Description
Options	There are several options provided here, such as *-v*, *-c [SET_NO], -d [SET_NO],… and etc.*
SET_NO	It means to specify the index number (from 1 to 12) of filter set.
RULE_NO	It means to specify the index number (from 1 to 7) of filter rule set.
-v	Type “-v” to view the configuration of general set.
-c [SET_NO]	It means to setup Call Filter, e.g., **-c 2**. The range for the index number you can type is “0” to “12” (0 means “disable).
-d [SET_NO]	It means to setup Data Filter, e.g., *-d 3*. The range for the index number you can type is “0” to “12” (0 means “disable).
-I [VALUE]	It means to setup Log Flag, e.g., *-I 2* Type “0” to disable the log flag. Type “1” to display the log of passed packet. Type “2” to display the log of blocked packet. Type “3” to display the log of non-matching packet.
- p [VALUE]	It means to setup actions for packet not matching any rule, e.g., *-p 1* Type “0” to let all the packets pass; Type “1” to block all the packets.
-M [P2P_NO]	It means to configure IM/P2P for the packets not matching with any rule, e.g., *-M 1* Type “0” to let all the packets pass; Type “1” to block all the packets.
-U [URL_NO]	It means to configure URL content filter for the packets not matching with any rule, e.g., *-U 1* Type “0” to let all the packets pass; Type “1” to block all the packets.
-a [AD_SET]	It means to configure the advanced settings.
-f [VALUE]	It means to accept large incoming fragmented UDP or ICMP packets.
-E [VALUE]	It means to set the maximum count for session limitation.
-F [VALUE]	It means to configure the load-balance policy.
-Q [VALUE]	It means to set the QoS class.

Example

```
> ipf set -c 1  #set call filter start from set 1
```

```
Setting saved.

> ipf set -d 2  #set data filter start from set 2
Setting saved.
> ipf set -v

Call Filter: Enable (Start Filter Set = 1)
Data Filter: Enable (Start Filter Set = 2)
Log Flag   : None

Actions for packet not matching any rule:
  Pass or Block    : Pass
  CodePage        : ANSI(1252)-Latin I
  Max Sessions Limit: 60000
  Current Sessions  : 0
  Mac Bind IP      : Non-Strict
  QOS Class       : None
  APP Enforcement   : None
  URL Content Filter: None
  Load-Balance policy : Auto-select
  ------------------------------------------------------------
  CodePage               : ANSI(1252)-Latin I
  Window size             : 65535
  Session timeout          : 1440
  DrayTek Banner           : Enable
  ------------------------------------------------------------
  Apply IP filter to VPN incoming packets          : Enable
  Accept large incoming fragmented UDP or ICMP packets: Enable
  ------------------------------------------------------------
  Strict Security Checking
    [ ]APP Enforcement
>
```

Telnet Command: ipf rule

This command is used to set filter rule for firewall.

Syntax

ipf rule *s r [-<command> <parameter>* | *...*

ipf rule s r -v

Syntax Description

Parameter	Description
s	Such word means Filter Set, range form 1~12.
r	Such word means Filter Rule, range from 1~7.
<Command><parameter>	The following lists all of the available commands with parameters.
-e	It means to enable or disable the rule setting. 0- disable 1- enable
-s o:g <obj>	It means to specify source IP object and IP group.

	o - indicates “object”. g - indicates “group”. obj - indicates index number of object or index number of group. Available settings range from 1-192. For example, “-s g 3" means the third source IP group profile.
–s u <Address Type> <Start IP Address> <End IP Address> | <Address Mask>	It means to configure **source** IP address including address type, start IP address, end IP address and address mask. u – It means “user defined”. *Address Type* - Type the number (representing different address type). 0 - Subnet Address 1 - Single Address 2 - Any Address 3 - Range Address Example: Set Subnet Address => -s u 0 192.168.1.10 255.255.255.0 Set Single Address => -s u 1 192.168.1.10 Set Any Address => -s u 2 Set Range Address => -s u 3 192.168.1.10 192.168.1.15
–d u <Address Type> <Start IP Address> <End IP Address> | <Address Mask>	It means to configure **destination** IP address including address type, start IP address, end IP address and address mask. u – It means “user defined”. *Address Type* - Type the number (representing different address type). 0 - Subnet Address 1 - Single Address 2 - Any Address 3 - Range Address Example: Set Subnet Address => -d u 0 192.168.1.10 255.255.255.0 Set Single Address => -d u 1 192.168.1.10 Set Any Address => -d u 2 Set Range Address => -d u 3 192.168.1.10 192.168.1.15
-d o:g <obj>	It means to specify destination IP object and IP group. o – indicates “object”. g – indicates “group” <obj>– indicates index number of object or index number of group. Available settings range from 1-192. For example, “-d g 1" means the first destination IP group profile.
-S o:g <obj>	It means to specify Service Type object and IP group. o – indicates “object”. g – indicates “group” <obj> – indicates index number of object or index number of group. Available settings range from 1-96. For example, “-S 0 1" means the first service type object profile.
-S u <protocol> <source_port__value> <destination_port_vale>	It means to configure advanced settings for Service Type, such as protocol and port range. u – it means “user defined”. <protocol> – It means TCP(6),UDP(17), TCP/UDP(255). <source_port__value> – 1 – Port OP, range is 0-3. 0:= =, 1:!=, 2:>, 3:< 3 – Port range of the Start Port Number, range is 1-65535. 5 – Port range of the End Port Number, range is 1-65535.

	<destination_port_value>: 2 – Port OP, range is 0-3, 0:==, 1:!=, 2:>, 3:< 4 – Port range of the Start Port Number, range is 1-65535. 6 – Port range of the End Port Number, range is 1-65535.
-F	It means the Filter action you can specify. 0 –Pass Immediately, 1 – Block Immediately, 2 – Pass if no further match, 3 – Block if no further match.
-q	It means the classification for QoS. 1– Class 1, 2 – Class 2, 3 – Class 3, 4 – Other
-l	It means load balance policy. Such function is used for "debug" only.
-E	It means to enable APP Enforcement.
-a<index>	It means to specify which APP Enforcement profile will be applied. <index> – Available settings range from 0 ~ 32. "0" means no profile will be applied.
-u<index>	It means to specify which URL Content Filter profile will be applied. <index> – Available settings range from 0 ~ 8. "0" means no profile will be applied.
-c	It means to set code page. Different number represents different code page. 0. None 1. ANSI(1250)-Central Europe 2. ANSI(1251)-Cyrillic 3. ANSI(1252)-Latin I 4. ANSI(1253)-Greek 5. ANSI(1254)-Turkish 6. ANSI(1255)-Hebrew 7. ANSI(1256)-Arabic 8. ANSI(1257)-Baltic 9. ANSI(1258)-Viet Nam 10. OEM(437)-United States 11. OEM(850)-Multilingual Latin I 12. OEM(860)-Portuguese 13. OEM(861)-Icelandic 14. OEM(863)-Canadian French 15. OEM(865)-Nordic 16. ANSI/OEM(874)-Thai 17. ANSI/OEM(932)-Japanese Shift-JIS 18. ANSI/OEM(936)-Simplified Chinese GBK 19. ANSI/OEM(949)-Korean 20. ANSI/OEM(950)-Traditional Chinese Big5
-C <Windows Size> <Session_Timeout>	It means to set Window size and Session timeout (Minute). <Windows Size> - Available settings range from 1 ~ 65535. <Session_Timeout> - Make the best utilization of network resources.
-v	It is used to show current filter/rule settings.

Example

```
> ipf rule 2 1 -e 1 -s "o 1" -d "o 2" -S "o 1" -F 2
> ipf rule 2 1 -v

Filter Set 2 Rule 1:

Status  : Enable
Comments: xNetBios -> DNS
Index(1-15) in Schedule Setup: <null>, <null>, <null>, <null>

Direction    : LAN -> WAN
Source IP    : Group1,
Destination IP: Group2,
Service Type  : TCP/UDPGroup1,
Fragments    : Don't Care

Pass or Block           : Block Immediately
Branch to Other Filter Set: None
Max Sessions Limit       : 32000
Current Sessions         : 0
Mac Bind IP             : Non-Strict
Qos Class               : None
APP Enforcement          : None
URL Content Filter       : None
Load-Balance policy      : Auto-select
Log                     : Disable
----------------------------------------------------------------
CodePage                : ANSI(1252)-Latin I
Window size              : 65535
Session timeout          : 1440
DrayTek Banner           : Enable
----------------------------------------------------------------
  Strict Security Checking
    [ ]APP Enforcement
```

Telnet Command: ipf flowtrack

This command is used to set and view flowtrack sessions.

Syntax

ipf flowtrack set *[-re]*

ipf flowtrack view *[-f]*

ipf flowtrack *[-i][-p][-t]*

Syntax Description

Parameter	Description
-r	It means to refresh the flowtrack.

-e	It means to enable or disable the flowtrack.
-f	It means to show the sessions state of flowtrack. If you do not specify any IP address, then all the session state of flowtrack will be displayed.
-b	It means to show all of IP sessions state.
- i [IP address]	It means to specify IP address (e.g,, -i 192.168.2.55).
-p[value]	It means to type a port number (e.g., -p 1024). Available settings are 0 ~ 65535.
-t [value]	It means to specify a protocol (e.g., -t tcp). Available settings include: *tcp* *udp* *icmp*

Example

```
>ipf flowtrack set -r
Refresh the flowstate ok
> ipf flowtrack view -f
Start to show the flowtrack sessions state:

ORIGIN>>  192.168.1.11:59939 ->       8.8.8.8:   53 ,ifno=0
REPLY >>      8.8.8.8:   53 ->   192.168.1.11:59939 ,ifno=3
      proto=17, age=93023180(3920), flag=203
ORIGIN>>  192.168.1.11:15073 ->       8.8.8.8:   53 ,ifno=0
REPLY >>      8.8.8.8:   53 ->   192.168.1.11:15073 ,ifno=3
      proto=17, age=93025100(2000), flag=203
ORIGIN>>  192.168.1.11: 7247 ->       8.8.8.8:   53 ,ifno=0
REPLY >>      8.8.8.8:   53 ->   192.168.1.11: 7247 ,ifno=3
      proto=17, age=93020100(7000), flag=203
End to show the flowtrack sessions state
> ipf flowtrack set -e
Current flow_enable=0
> ipf flowtrack set -e
Curretn flow_enable=1
```

Telnet Command: ipf flowtest

This command is used to for RD debug in firewall diagnose.

Syntax

ipf flowtest mode *[<command><parameter>|…]*

ipf flowtest set *[index][option]*

ipf flowtest send

ipf flowtest view

ipf flowtest reset

Syntax Description

Parameter	Description
mode	

[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-m [value]	It means to set ICMP, UDP or TCP as flowtest mode. Value – 1, 2 or 3. In which, 1: ICMP 2: UDP 3: TCP
-d [value]	It means to set the original direction Value – 1 or 2. In which, 1: LAN to WAN 2: WAN to LAN
-v [value]	It means to choose IP version. Value – 4 or 6. In which, 4: IPv4 6: IPv6
-i [value]	It means to specify IPv4 address of LAN device (e.g., 192.168.1.10).
-j [value]	It means to specify IPv4 address of WAN divice (e.g., 8.8.8.8).
-l [value]	It means to specify IPv6 address of LAN device (e.g., 2001:5678:0000:0000:1319:8a2e:0370:7343).
-w [value]	It means to specify IPv6 address of WAN divice (e.g., 2001:1234:0000:0000:1319:8a2e:0370:7344).
-p [value]	It means to set port number of LAN device (e.g., 65535)
-q [value]	It means to set port number of WAN device (e.g., 53).
-e [value]	It means to set MAC address of LAN device (e.g., AA:BB:CC:11:22:33).
set	
[index]	Index: 1 to 5.
-e [value]	It means to enable /disable the test packet. Value – 1 or 0. In which, 1: enable 0: disable
-w [value]	It means to set direction of this packet. Value – 1 or 2. In which, 1: LAN to WAN 2: WAN to LAN
-y [value]	It means to set the payload type of this packet. Value – 1 to 7. In which, 1: Customize 2: Echo Request 3: Echo Reply 4: Destination Unreachable 5: Ping Request 6: Pin Reply

	7: Traceroute 8: DNS Query 9: Http Get
-a [value]	It means set payload data depending to payload type. Value – host name (e.g, www.draytek.com) or hex. stream (e.g., "6162636465666768696a6b6c6d6e6f70")
-f [value]	It means to set TCP flag of this packet. Value – SYN ACK PSH FIN RST URG
send	It means to start a test by sending each packet out.
view	It means to view the test information and the test result.
reset	It means to clear all configuration for flowtest.

Example

```
> ipf flowtest mode -m 2 -v 4 -d 1 -i 192.168.1.111 -j 8.8.8.8 -p 57005
-q 53 -e 60:E3:27:02:CB:B1
> ipf flowtest set 1 -e 1 -w 1 -y 8 -a www.draytek.com
> ipf flowtest send
Send TEST Packet

>
> ipf flowtest view
Test Info
Mode:UDP Direction:LAN->WAN
LAN>> IP:192.168.1.111 Port:57005 WAN>> IP:8.8.8.8 Port:53
LAN MAC 60:E3:27:02:CB:B1

Test Result
ORIGIN>>  192.168.1.111:57005 ->       8.8.8.8:   53 ,ifno=0
nat=49969 td_state=1
REPLY >>       8.8.8.8:   53 -> 192.168.200.104:38445 ,ifno=3
nat=49969 td_state=1
Status:Pass Packet:2 Set:13 Rule:1
all_app_flag:1f7f8 send_out:2 wan_num:3

Packet:1
Status:Pass dir:LAN->WAN is_p:17
flowflag:9 appflag:80 accflag:1e5b8
fr_flags:2 set:13 rule:1

> ipf flowtest reset
Reset TEST
```

Telnet Command: Log

This command allows users to view log for WAN interface such as call log, IP filter log, flush log buffer, etc.

Syntax

log *[-cfhiptwx?] [-F a| c | f | w]*

Syntax Description

Parameter	Description
-c	It means to show the latest call log.
-f	It means to show the IP filter log.
-F	It means to show the flush log buffer. a: flush all logs c: flush the call log f: flush the IP filter log w: flush the WAN log
-h	It means to show this usage help.
-p	It means to show PPP/MP log.
-t	It means to show all logs saved in the log buffer.
-w	It means to show WAN log.
-x	It means to show packet body hex dump.

Example

```
> log -w
25:36:25.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
       Relay agent IP = 0.0.0.0
25:36:33.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
       Relay agent IP = 0.0.0.0
25:36:41.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
       Relay agent IP = 0.0.0.0
25:36:49.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
       Relay agent IP = 0.0.0.0
25:36:57.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: ldap user

This command is used to configure the LDAP profile.

Syntax

ldap user *[INDEX][OPTION]*

Syntax Description

Parameter	Description
INDEX	Specify the index number (1 to 8) of the LDAP profile.
OPTION	
-n VALUE	Setup Profile Name.
-b VALUE	Setup Base Distinguished Name.
-a VALUE	If you have added containers to be published, you may need to specify additional LDAP filters for each class of objects included in these containers. Creating LDAP filters is a fairly complex task that should be performed by advanced users only. LDAP filters must be RFC2254-compliant. For example, to exclude from publication all users who either belong to the HR department of your company or are members of the HR Group. For example: >ldap user 1 -a "(!(|(department=HR)(memberOf=CN=HRGroup,OU=Groups, DC=acme,DC=com)))" Additional Filter has been updated.
-g VALUE	Setup Group Distinguished Name.
-c VALUE	Setup Common Name Identifier.
-v	View detail information of the LDAP profile.

Example

```
>ldap user 1 -n LD_user_test1
Profile Name has been updated!
> ldap user 1 -v
Profile Index:1
Profile Name:LD_user_test1
Common Name Identifier:
Base Distinguished Name:
Additional Filter:
Group distinguished Name:
>ldap user 1 -b ou=People,dc=example,dc=com
```

Telnet Command: ldap set

This command is used to set general settings (e.g., IP address, port number) for LDAP server.

Syntax

ldap set *[Options][Value]*

Syntax Description

Parameter	Description
enable [0-1]	Enable or disable LDAP function. 0 – Disable the function. 1 – Enable the function.
type [0-2]	Set the bind type as Simple(0),Anonymous(1), and Regular(2).
ssl [0-1]	Enable or disable LDAP function via SSL tunnel. 0 – Disable the function. 1 – Enable the function.

IP <VALUE>	Set IP address for LDAP server.
port <VALUE>	Set port number for LDAP server.
dn <VALUE>	Set Regular DN value
PWD <VALUE>	Set Regular password value.

Example

```
>ldap set enable 1
>ldap enabled.
> ldap set ssl 1
LDAP with SSL has been enabled!
> ldap set IP 192.168.100.155
LDAP Server IP has been setting.
> ldap set port 389
LDAP Server Port has been setting.
> ldap set dn dc=example,dc=com
LDAP Regular DN has been setting.
> ldap set PWD 123456
LDAP Regular Password has been setting.
```

Telnet Command: ldap view

This command is used to check current status of LDAP settings configuration.

Syntax

ldap view

Example

```
> ldap view ?
LDAP Enable:Disabled.
LDAP Bind Type:Simple
LDAP with SSL:Disabled
LDAP Regular DN:
LDAP Regular Password:
LDAP Server IP:
LDAP Server Port:389
```

Telnet Command: tacacsplus set

This command allows users to configure general settings for TACACS+ server

Syntax

tacacspluse set *[Options][Value]*

Syntax Description

Parameter	Description
enable [0-1]	Disable (0)/enable(1) the TACACS+ server.
IP <VALUE>	Set the IP address of TACACS+ server.
port <VALUE>	Set the port number of TACACS+ server.
shared_secret <VALUE>	Set the Shared Secret value of TACACS+ Server.

Example

```
> tacacsplus set enable 1
TACACS+ enabled!
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.

> tacacsplus set IP 192.168.1.59
TACACS+ Server IP has been setting.
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> tacacsplus view
TACACS+ Enable:Enable.
TACACS+ Server IP:192.168.1.59
TACACS+ Server Port:49
TACACS+ Type:ASCII
TACACS+ Shared Secret:
```

Telnet Command: tacacsplus view

This command allows users to check the general settings for TACACS+ server

Syntax

tacacspluse view

Example

```
> tacacsplus view
TACACS+ Enable:Enable.
TACACS+ Server IP:192.168.1.59
TACACS+ Server Port:49
TACACS+ Type:ASCII
TACACS+ Shared Secret:
```

Telnet Command: mngt ftpport

This command allows users to set FTP port for management.

Syntax

mngt ftpport *[FTP port]*

Syntax Description

Parameter	Description
FTP port	It means to type the number for FTP port. The default setting is 21.

Example

```
> mngt ftpport 21
% Set FTP server port to 21 done.
```

Telnet Command: mngt httpport

This command allows users to set HTTP port for management.

Syntax

mngt httpport *[Http port]*

Syntax Description

Parameter	Description
Http port	It means to enter the number for HTTP port. The default setting is 80.

Example

```
> mngt httpport 80
% Set web server port to 80 done.
```

Telnet Command: mngt httpsport

This command allows users to set HTTPS port for management.

Syntax

mngt httpsport *[Https port]*

Syntax Description

Parameter	Description
Https port	It means to type the number for HTTPS port. The default setting is 443.

Example

```
> mngt httpsport 443
% Set web server port to 443 done.
```

Telnet Command: mngt telnetport

This command allows users to set telnet port for management.

Syntax

mngt telnetport *[Telnet port]*

Syntax Description

Parameter	Description
Telnet port	It means to type the number for telnet port. The default setting is 23.

Example

```
> mngt telnetport 23
% Set Telnet server port to 23 done.
```

Telnet Command: mngt sshport

This command allows users to set SSH port for management.

Syntax

mngt sshport *[ssh port]*

Syntax Description

Parameter	Description
ssh port	It means to type the number for SSH port. The default setting is 22.

Example

```
> mngt sshport 23
% Set ssh port to 23 done.
```

Telnet Command: mngt noping

This command is used to pass or block Ping from LAN PC to the internet.

Syntax

mngt noping *[on]*

mngt noping *[off]*

mngt noping *[viewlog]*

mngt noping *[clearlog]*

Syntax Description

Parameter	Description
on	All PING packets will be forwarded from LAN PC to Internet.
off	All PING packets will be blocked from LAN PC to Internet.
viewlog	It means to display a log of ping action, including source MAC and source IP.
clearlog	It means to clear the log of ping action.

Example

```
> mngt noping off
No Ping Packet Out is OFF!!
```

Telnet Command: mngt defenseworm

This command can block specified port for passing through the router.

Syntax

mngt defenseworm *[on]*

mngt defenseworm *[off]*

mngt defenseworm *[add port]*

mngt defenseworm *[del port]*

mngt defenseworm *[viewlog]*

mngt defenseworm *[clearlog]*

Syntax Description

Parameter	Description

on	It means to activate the function of defense worm packet out.
off	It means to inactivate the function of defense worm packet out.
add port	It means to add a new TCP port for block.
del port	It means to delete a TCP port for block.
viewlog	It means to display a log of defense worm packet, including source MAC and source IP.
clearlog	It means to remove the log of defense worm packet.

Example

```
> mngt defenseworm add 21
Add TCP port 21
Block TCP port list: 135, 137, 138, 139, 445, 21
> mngt defenseworm del 21
Delete TCP port 21
Block TCP port list: 135, 137, 138, 139, 445
```

Telnet Command: mngt rmtcfg

This command can allow the system administrators to login from the Internet. By default, it is not allowed.

Syntax

mngt rmtcfg *[status]*

mngt rmtcfg *[enable]*

mngt rmtcfg *[disable]*

mngt rmtcfg *[http/https/ftp/telnet/ssh/tr069] [on/off]*

Syntax Description

Parameter	Description
status	It means to display current setting for your reference.
enable	It means to allow the system administrators to login from the Internet.
disable	It means to deny the system administrators to login from the Internet.
http/https/ftp/telnet/ssh/tr069	It means to specify one of the servers/protocols for enabling or disabling.
on/off	on – enable the function. off – disable the function.

Example

```
> mngt rmtcfg ftp on
Enable server fail
Remote configure function has been disabled
please enable by enter mngt rmtcfg enable

> mngt rmtcfg enable
%% Remote configure function has been enabled.
> mngt rmtcfg ftp on
```

```
%% FTP server has been enabled.
```

Telnet Command: mngt lanaccess

This command allows users to manage accessing into Vigor router through LAN port.

Syntax

mngt lanaccess *-e [0/1] –s [value] –i [value]*

mngt lanaccess *–f*

mngt lanaccess *–d*

mngt lanaccess *–v*

mngt lanaccess *–h*

Syntax Description

Parameter	Description
-e[0/1]	It means to enable/disable the function. 0-disable the function. 1-enable the function.
-s[value]	It means to specify service offered. Available values include: FTP, HTTP, HTTPS, TELNET, SSH, None, All
-i[value]	It means the interface which is allowed to access. Available values include: LAN2~LAN6, DMZ, IP Routed Subnet, None, All **Note**: LAN1 is always allowed for accessing into the router.
-f	It means to flush all of the settings.
-d	It means to restore the factory default settings.
-v	It means to view current settings.
-h	It means to get the usage of such command.

Example

```
> mngt lanaccess -e 1
> mngt lanaccess -s FTP,TELNET
> mngt lanaccess -i LAN3
>> mngt lanaccess -v
Current LAN Access Control Setting:
* Enable:Yes
* Service:
   - FTP:Yes
   - HTTP:No
   - HTTPS:No
   - TELNET:Yes
   - SSH:No
* Subnet:
   - LAN 2: disabled
   - LAN 3: enabled
   - LAN 4: disabled
   - LAN 5: disabled
   - LAN 6: disabled
   - DMZ: disabled
```

```
   - IP Routed Subnet: disabled

Note: the settings do NOT apply to LAN1, LAN1 is always allowed to access
the router
```

Telnet Command: mngt echoicmp

This command allows users to reject or accept PING packets from the Internet.

Syntax

mngt echoicmp *[enable]*

mngt echoicmp *[disable]*

Syntax Description

Parameter	Description
enable	It means to accept the echo ICMP packet.
disable	It means to drop the echo ICMP packet.

Example

```
> mngt echoicmp enable
%% Echo ICMP packet enabled.
```

Telnet Command: mngt accesslist

This command allows you to specify that the system administrator can login from a specific host or network. A maximum of three IPs/subnet masks is allowed.

Syntax

mngt accesslist *list*

mngt accesslist *add [index][ip addr][mask]*

mngt accesslist *remove [index]*

mngt accesslist *flush*

Syntax Description

Parameter	Description
list	It can display current setting for your reference.
add	It means adding a new entry.
index	It means to specify the number of the entry.
ip addr	It means to specify an IP address.
mask	It means to specify the subnet mask for the IP address.
remove	It means to delete the selected item.
flush	It means to remove all the settings in the access list.

Example

```
> mngt accesslist add 1 192.168.1.89 255.255.255.0
%% Set OK.
> mngt accesslist list
```

```
%% Access list :
  Index IP address     Subnet mask
========================================
  1    192.168.1.89    255.255.255.0
```

Telnet Command: mngt snmp

This command allows you to configure SNMP for management.

Syntax

mngt snmp *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-e <1/2>	1: Enable the SNMP function. 2: Disable the SNMP function.
-g<Community name>	It means to set the name for getting community by typing a proper character. (max. 23 characters)
-s <Community name>	It means to set community by typing a proper name. (max. 23 characters)
-m <IP address>	It means to set one host as the manager to execute SNMP function. Please type in IPv4 address to specify certain host.
-t <Community name>	It means to set trap community by typing a proper name. (max. 23 characters)
-n <IP address>	It means to set the IPv4 address of the host that will receive the trap community.
-T <seconds>	It means to set the trap timeout <0~999>.
-V	It means to list SNMP setting.

Example

```
> mngt snmp -e 1 -g draytek -s DK -m 192.168.1.1 -t trapcom -n 10.20.3.40
-T 88
 SNMP Agent Turn on!!!
 Get Community set to draytek
 Set Community set to DK
 Manager Host IP set to 192.168.1.1
 Trap Community set to trapcom
 Notification Host IP set to 10.20.3.40
 Trap Timeout set to 88 seconds
```

Telnet Command: mngt bfp

This command allows you to configure brute force protect (BFP) for system management.

Syntax

mngt bfp *[<command><parameter>|…]*

Syntax Description

Parameter	Description

[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-e 0/1	Enable / disable the BFP function. 0 – Disable 1 – Enable
-s [service]	It means to enable different service. service - Available types are FTP, HTTP, HTTPS, TELNET, TR069, SSH, None and All.
-l [failure]	It means to set login failure retry times. failure - Available number is from 1 to 255.
-p [penalty]	It means to set penalty time for BFP. The unit is sec.
-v	It means to view current settings.

Example

```
> mngt bfp -e 1
> mngt bfp -s FTP
> mngt bfp -l 10
> mngt bfp -v
Current Brute Force Protection Setting:
* Enable: yes
* Service:
 - FTP:        yes
 - HTTP:       no
 - HTTPS:      no
 - TELNET:     no
 - TR069:      no
 - SSH:        no
* Maximum login failures: 10
* Penalty period: 0
```

Telnet Command: msubnet switch

This command is used to configure multi-subnet.

Syntax

msubnet switch *[2/3/4/5][On/Off]*

Syntax Description

Parameter	Description
2/3/4/5	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5
On/Off	On means turning on the subnet for the specified LAN interface. Off means turning off the subnet.

Example

```
> msubnet switch 2 On
% LAN2       Subnet On!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet addr

This command is used to configure IP address for the specified LAN interface.

Syntax

msubnet addr *[2/3/4/5][IP address]*

Syntax Description

Parameter	Description
2/3/4/5	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5
IP address	Type the private IP address for the specified LAN interface.

Example

```
> msubnet addr 2 192.168.5.1
% Set LAN2 subnet IP address done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet nmask

This command is used to configure net mask address for the specified LAN interface.

Syntax

msubnet nmask *[2/3/4/5][IP address]*

Syntax Description

Parameter	Description
2/3/4/5	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5
IP address	Type the subnet mask address for the specified LAN interface.

Example

```
> msubnet nmask 2 255.255.0.0
% Set LAN2 subnet mask done !!!
```

```
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet status

This command is used to display current status of subnet.

Syntax

msubnet status *[2/3/4/5]*

Syntax Description

Parameter	Description
2/3/4/5	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5

Example

```
> msubnet status 2
% LAN2       Off: 0.0.0.0/0.0.0.0, PPP Start IP: 0.0.0.60
% DHCP server: Off
% Dhcp Gateway: 0.0.0.0, Start IP: 0.0.0.10, Pool Count: 50
```

Telnet Command: msubnet dhcps

This command allows you to enable or disable DHCP server for the subnet.

Syntax

msubnet dhcps *[2/3/4/5][On/Off]*

Syntax Description

Parameter	Description
2/3/4/5	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5
On/Off	On means enabling the DHCP server for the specified LAN interface. Off means disabling the DHCP server.

Example

```
> msubnet dhcps 3 off
% LAN3       Subnet DHCP Server disabled!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet nat

This command is used to configure the subnet for NAT or Routing usage.

Syntax

msubnet nat *[2/3/4/5] [On/Off]*

Syntax Description

Parameter	Description
2/3/4/5	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5
On/Off	On – It means the subnet will be configured for NAT usage. Off **-** It means the subnet will be configured for Routing usage.

Example

```
> > msubnet nat 2 off
% LAN2 Subnet is for Routing usage!
%Note: If you have multiple WAN connections, please be reminded to setup
a Load-Balance policy so that packets from this subnet will be forwarded
to the right WAN interface!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet gateway

This command is used to configure an IP address as the gateway used for subnet.

Syntax

msubnet gateway *[2/3/4/5] [Gateway IP]*

Syntax Description

Parameter	Description
2/3/4/5	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5
Gateway IP	Specify an IP address as the gateway IP.

Example

```
> msubnet gateway 2 192.168.1.13
% Set LAN2 Dhcp Gateway IP done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet ipcnt

This command is used to defined the total number allowed for each LAN interface.

Syntax

msubnet ipcnt *[2/3/4/5] [IP counts]*

Syntax Description

Parameter	Description
2/3/4/5	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5
IP counts	Specify a total number of IP address allowed for each LAN interface. The available range is from 0 to 220.

Example

```
> msubnet ipcnt 2 15
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet talk

This command is used to establish a route between two LAN interfaces.

Syntax

msubnet talk *[1/2/3/4/5] [1/2/3/4/5] [On/Off]*

Syntax Description

Parameter	Description
1/2/3/4/5	It means LAN interface. 1=LAN1 2=LAN2 3=LAN3 4=LAN4 5=LAN5
On/Off	On – It means Off **-** It means

Example

```
> msubnet talk 1 2 on
% Enable routing between LAN1       and LAN2      !

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> msubnet talk ?
% msubnet talk <1/2/3/4/5> <1/2/3/4/5> <On/Off>
% where 1:LAN1, 2:LAN2, 3:LAN3, 4:LAN4, 5:LAN5
% Now:
```

```
%              LAN1   LAN2   LAN3   LAN4   LAN5
% LAN1          V
% LAN2                 V
% LAN3                        V
% LAN4                               V
% LAN5                                      V
>
```

Telnet Command: msubnet startip

This command is used to configure a starting IP address for DCHP.

Syntax

msubnet startip *[2/3/4/5] [Gateway IP]*

Syntax Description

Parameter	Description
2/3/4/5	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5
Gateway IP	Type an IP address as the starting IP address for a subnet.

Example

```
> msubnet startip 2 192.168.2.90
%Set LAN2 Dhcp Start IP done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> msubnet startip ?
% msubnet startip <2/3/4/5/6> <Gateway IP>
% Now: LAN2 192.168.2.90; LAN3 192.168.3.10; LAN4 192.168.4.10; LAN5
192.168.5.1
0; LAN6 192.168.6.10
```

Telnet Command: msubnet pppip

This command is used to configure a starting IP address for PPP connection.

Syntax

msubnet pppip *[2/3/4/5] [Start IP]*

Syntax Description

Parameter	Description
2/3/4/5	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5
Start IP	Type an IP address as the starting IP address for PPP connection.

Example

```
> msubnet pppip 2 192.168.2.250
% Set LAN2 PPP(IPCP) Start IP done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.

> msubnet pppip ?
% msubnet pppip <2/3/4/5/6> <Start IP>
% Now: 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
```

Telnet Command: msubnet nodetype

This command is used to specify the type for node which is required by DHCP option.

Syntax

msubnet nodetype *[2/3/4/5][count]*

Syntax Description

Parameter	Description
2/3/4/5	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5
count	Choose the following number for specifying different node type. 1= B-node 2= P-node 4= M-node 8= H-node 0= Not specify any type for node.

Example

```
> msubnet nodetype ?
% msubnet nodetype <2/3/4/5> <count>
% Now: LAN2 0; LAN3 0; LAN4 0; LAN5 0

% count: 1. B-node 2. P-node 4. M-node 8. H-node

>  msubnet nodetype 2 1
% Set LAN2 Dhcp Node Type done !!!

> msubnet nodetype ?
% msubnet nodetype <2/3/4/5> <count>
% Now: LAN2 1; LAN3 0; LAN4 0; LAN5 0

% count: 1. B-node 2. P-node 4. M-node 8. H-node
```

Telnet Command: msubnet primWINS

This command is used to configure primary WINS server.

Syntax

msubnet primWINS *[2/3/4/5/6] [WINS IP]*

Syntax Description

Parameter	Description
2/3/4/5/6	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6
WINS IP	Type the IP address as the WINS IP.

Example

```
> msubnet primWINS 2 192.168.3.5
% Set LAN2 Dhcp Primary WINS IP done !!!

> msubnet primWINS ?
% msubnet primWINS <2/3/4/5/6> <WINS IP>
% Now: 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
```

Telnet Command: msubnet secWINS

This command is used to configure secondary WINS server.

Syntax

msubnet secWINS *[2/3/4/5/6] [WINS IP]*

Syntax Description

Parameter	Description
2/3/4/5/6	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5 6=LAN6
WINS IP	Type the IP address as the WINS IP.

Example

```
> msubnet secWINS 2 192.168.3.89
% Set LAN2 Dhcp Secondary WINS IP done !!!

> msubnet secWINS ?
```

```
% % msubnet secWINS <2/3/4/5/6> <WINS IP>
% Now: 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
```

Telnet Command: msubnet tftp

This command is used to set TFTP server for multi-subnet.

Syntax

msubnet tftp *[2/3/4/5] [TFTP server name]*

Syntax Description

Parameter	Description
2/3/4/5	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4 5=LAN5
TFTP server name	Type a name to indicate the TFTP server.

Example

```
> msubnet tftp ?
% msubnet tftp <2/3/4/5> <TFTP server name>
% Now: LAN2
      LAN3
      LAN4
      LAN5
      LAN6

> msubnet tftp 2 publish
% Set LAN2 TFTP Server Name done !!!

> msubnet tftp ?
% msubnet tftp <2/3/4/5> <TFTP server name>
% Now: LAN2 publish
      LAN3
      LAN4
      LAN5
```

Telnet Command: msubnet mtu

This command allows you to configure MTU value for LAN/DMZ/IP Routed Subnet.

Syntax

msubnet mtu *[interface][value]*

Syntax Description

Parameter	Description
interface	Available settings include LAN1~LAN6, IP_Routed_Subnet, and DMZ.
value	1000 ~ 1508 (Bytes), default: 1500 (Bytes)

Example

```
> msubnet mtu ?
Usage:

  >msubnet mtu <interface> <value>

  <interface>: LAN1~LAN5,IP_Routed_Subnet,DMZ
  <value>:    1000 ~ 1496 (Bytes), default: 1500 (Bytes)

  e.x: >msubnet mtu LAN1 1492

Current Settings:

   LAN1 MTU:           1500 (Bytes)
   LAN2 MTU:           1500 (Bytes)
   LAN3 MTU:           1500 (Bytes)
   LAN4 MTU:           1500 (Bytes)
   LAN5 MTU:           1500 (Bytes)
   DMZ MTU:            1500 (Bytes)
   IP Routed Subnet MTU: 1500 (Bytes)
```

Telnet Command: msubnet leasetime

This command allows you to set leasetime for DHCP server. It is helpful to manage the IP address(es) assigned by DHCP server.

Syntax

msubnet leasetime *[1/2/3/4/5/6/dmz][Lease Time (sec.)]*

Syntax Description

Parameter	Description
[1/2/3/4/5/6/dmz]	1 – 6 represent LAN1 to LAN6.
Lease Time (sec.)	Range from 1 to 259200. If no value specified here, Vigor router system will use the maximum value, 259200, as the leasetime.

Example

```
> msubnet leasetime 1 80800
Set LAN1 lease time: 80800
> msubnet leasetime 1
% Set LAN1 lease time: 259200
```

Telnet Command: object ip obj

This command is used to create an IP object profile.

Syntax

object ip obj setdefault

object ip obj *INDEX -v*

object ip obj *INDEX -n NAME*

object ip obj *INDEX -i INTERFACE*

object ip obj *INDEX -s INVERT*

object ip obj I*NDEX -a TYPE [START_IP] [END/MASK_IP]*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified object profile.
-v	It means to view the information of the specified object profile. Example: *object ip obj 1 -v*
-n NAME	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: *object ip obj 9 -n bruce*
-i INTERFACE	It means to define an interface for the IP object. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: *object ip obj 8 -i 0*
-s INVERT	It means to set invert seletion for the object profile. INVERT=0, means disableing the function. INVERT=1, means enabling the function. Example: *object ip obj 3 -s 1*
-a TYPE	It means to set the address type and IP for the IP object profile. TYPE=0, means Mask TYPE=1, means Single TYPE=2, means Any TYPE=3, means Rang Example: *object ip obj 3 -a 2*
[START_IP]	When the TYPE is set with 2, you have to type an IP address as a starting point and another IP address as end point. Type an IP address.
[END/MASK_IP]	Type an IP address (different with START_IP) as the end IP address.

Example

```
> object ip obj 1 -n marketing
> object ip obj 1 -a 1 192.168.1.45
> object ip obj 1 -v
 IP Object Profile 1
 Name   :[marketing]
 Interface:[Any]
 Address type:[single]
 Start ip address:[192.168.1.45]
 End/Mask ip address:[0.0.0.0]
 Invert Selection:[0]
```

Telnet Command: object ip grp

This command is used to integrate several IP objects under an IP group profile.

Syntax

object ip grp setdefault

object ip grp *INDEX -v*

object ip grp *INDEX -n NAME*

object ip grp *INDEX -i INTERFACE*

object ip grp *INDEX -a IP_OBJ_INDEX*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified group profile.
-v	It means to view the information of the specified group profile. Example: *object ip grp 1 -v*
-n NAME	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: *object ip grp 8 -n bruce*
-i INTERFACE	It means to define an interface for the IP group. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=2, means WAN Example: *object ip grp 3 -i 0*
-a IP_OBJ_INDEX	It means to specify IP object profiles for the group profile. Example: *:object ip grp 3 -a 1 2 3 4 5* The IP object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```
> object ip grp 2 -n First
 IP Group Profile 2
 Name   :[First]
 Interface:[Any]
 Included ip object index:
 [0:][0]
 [1:][0]
 [2:][0]
 [3:][0]
 [4:][0]
 [5:][0]
 [6:][0]
 [7:][0]

> object ip grp 2 -i 1
> object ip grp 2 -a 1 2
 IP Group Profile 2
```

```
Name   :[First]
Interface:[Lan]
Included ip object index:
[0:][1]
[1:][2]
[2:][0]
[3:][0]
[4:][0]
[5:][0]
[6:][0]
[7:][0]
```

Telnet Command: object ipv6 obj

This comman is used to create an IP object profile.

Syntax

object ip obj setdefault

object ip obj *INDEX -v*

object ip obj *INDEX -n NAME*

object ip obj *INDEX -i INTERFACE*

object ip obj *INDEX -s INVERT*

object ip obj I*NDEX -a TYPE [START_IP] [END/MASK_IP]*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified object profile.
-v	It means to view the information of the specified object profile. Example: *object ip obj 1 -v*
-n NAME	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: *object ip obj 9 -n bruce*
-i INTERFACE	It means to define an interface for the IP object. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=3, means WAN Example: *object ip obj 8 -i 0*
-s INVERT	It means to set invert seletion for the object profile. INVERT=0, means disableing the function. INVERT=1, means enabling the function. Example: *object ip obj 3 -s 1*
-a TYPE	It means to set the address type and IP for the IP object profile. TYPE=0, means Mask TYPE=1, means Single TYPE=2, means Any TYPE=3, means Rang Example: *object ip obj 3 -a 2*
[START_IP]	When the TYPE is set with 2, you have to type an IP address as a starting point and another IP address as end point. Type an IP address.
[END/MASK_IP]	Type an IP address (different with START_IP) as the end IP address.

Example

```
> object ip obj 1 -n marketing
> object ip obj 1 -a 1 192.168.1.45
> object ip obj 1 -v
 IP Object Profile 1
 Name   :[marketing]
```

```
 Interface:[Any]
 Address type:[single]
 Start ip address:[192.168.1.45]
 End/Mask ip address:[0.0.0.0]
 Invert Selection:[0]
```

Telnet Command: object ipv6 grp

This command is used to integrate several IP objects under an IP group profile.

Syntax

object ip grp setdefault

object ip grp *INDEX -v*

object ip grp *INDEX -n NAME*

object ip grp *INDEX -i INTERFACE*

object ip grp *INDEX -a IP_OBJ_INDEX*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified group profile.
-v	It means to view the information of the specified group profile. Example: *object ip grp 1 -v*
-n NAME	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: *object ip grp 8 -n bruce*
-i INTERFACE	It means to define an interface for the IP group. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=2, means WAN Example: *object ip grp 3 -i 0*
-a IP_OBJ_INDEX	It means to specify IP object profiles for the group profile. Example: *:object ip grp 3 -a 1 2 3 4 5* The IP object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```
> > object ip grp 2 -n First
 IP Group Profile 2
 Name   :[First]
 Interface:[Any]
 Included ip object index:
 [0:][0]
 [1:][0]
 [2:][0]
 [3:][0]
 [4:][0]
 [5:][0]
 [6:][0]
```

```
 [7:][0]
 [8:][0]
 [9:][0]
 [10:][0]
 [11:][0]

Set ok!
```

Telnet Command: object service obj

This command is used to create service object profile.

Syntax

object service obj setdefault

object service obj *INDEX -v*

object service obj *INDEX -n NAME*

object service obj *INDEX -p PROTOCOL*

object service obj *INDEX -s CHK [START_P] [END_P]*

object service obj *INDEX -d CHK [START_P] [END_P]*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified service object profile.
-v	It means to view the information of the specified service object profile. Example: *object service obj 1 -v*
-n NAME	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: *object service obj 9 -n bruce*
-i PROTOCOL	It means to define a PROTOCOL for the service object profile. PROTOCOL =0, means any PROTOCOL =1, means ICMP PROTOCOL =2, means IGMP PROTOCOL =6, means TCP PROTOCOL =17, means UDP PROTOCOL =255, means TCP/UDP Other values mean other protocols. Example: *object service obj 8 -i 0*
CHK	It means the check action for the port setting. 0=equal**(=)**, when the starting port and ending port values are the same, it indicates one port; when the starting port and ending port values are different, it indicates a range for the port and available for this service type. 1=not equal**(!=)**, when the starting port and ending port values are the same, it indicates all the ports except the port defined here; when the starting port and ending port values are different, it indicates that all the ports except the range defined here are available for this service type. 2=larger**(>)**, the port number greater than this value is available.. 3=less**(<)**, the port number less than this value is available for this

	profile.
-s CHK [START_P] [END_P]	It means to set souce port check and configure port range (1~65565) for TCP/UDP. END_P, type a port number to indicate source port. Example: *object service obj 3 -s 0 100 200*
-d CHK [START_P] [END_P]	It means to set destination port check and configure port range (1~65565) for TCP/UDP. END_P, type a port number to indicate destination port. Example: *object service obj 3 -d 1 100 200*

Example

```
> object service obj 1 -n limit
> object service obj 1 -p 255
> object service obj 1 -s 1 120 240
> object service obj 1 -d 1 200 220
> object service obj 1 -v
 Service Object Profile 1
 Name   :[limit]
 Protocol:[255]
 Source port check action:[!=]
 Source port range:[120~240]
 Destination port check action:[!=]
 Destination port range:[200~220]
```

Telnet Command: object service grp

This command is used to integrate several service objects under a service group profile.

Syntax

object service grp setdefault

object service grp *INDEX -v*

object service grp *INDEX -n NAME*

object service grp *INDEX -a SER_OBJ_INDEX*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified group profile.
-v	It means to view the information of the specified group profile. Example: *object service grp 1 -v*
-n NAME	It means to define a name for the service group. NAME: Type a name with less than 15 characters. Example: *object service grp 8 -n bruce*
-a SER_OBJ_INDEX	It means to specify service object profiles for the group profile. Example: *:object service grp 3 -a 1 2 3 4 5* The service object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```
>object service grp 1 -n Grope_1
 Service Group Profile 1
 Name   :[Grope_1]
 Included service object index:
 [0:][0]
 [1:][0]
 [2:][0]
 [3:][0]
 [4:][0]
 [5:][0]
 [6:][0]
 [7:][0]

> object service grp 1 -a 1 2
 Service Group Profile 1
 Name   :[Grope_1]
 Included service object index:
 [0:][1]
 [1:][2]
 [2:][0]
 [3:][0]
 [4:][0]
 [5:][0]
 [6:][0]
 [7:][0]
```

Telnet Command: object kw

This command is used to create keyword profile.

Syntax

object kw obj setdefault

object kw obj show PAGE

object kw obj *INDEX -v*

object kw obj *INDEX -n NAME*

object kw obj *INDEX -a CONTENTS*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
show PAGE	It means to show the contents of the specified profile. PAGE: type the page number.
show	It means to show the contents for all of the profiles.
INDEX	It means the index number of the specified keyword profile.
-v	It means to view the information of the specified keyword profile.
-n NAME	It means to define a name for the keyword profile. NAME: Type a name with less than 15 characters.

-a CONTENTS	It means to set the contents for the keyword profile. Example: *object kw obj 40 -a test*

Example

```
> object kw obj 1 -n children
 Profile 1
 Name   :[children]
 Content:[]
> object kw obj 1 -a gambling
 Profile 1
 Name   :[children]
 Content:[gambling]

> object kw obj 1 -v
 Profile 1
 Name   :[children]
 Content:[gambling]
```

Telnet Command: object fe

This command is used to create File Extension Object profile.

Syntax

object fe show

object fe setdefault

object fe obj *INDEX -v*

object fe obj *INDEX -n NAME*

object fe obj *INDEX -e CATEGORY|FILE_EXTENSION*

object fe obj *INDEX -d CATEGORY|FILE_EXTENSION*

Syntax Description

Parameter	Description
show	It means to show the contents for all of the profiles.
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number (from 1 to 8) of the specified file extension object profile.
-v	It means to view the information of the specified file extension object profile.
-n NAME	It means to define a name for the file extension object profile. NAME: Type a name with less than 15 characters.
-e	It means to enable the specific CATEGORY or FILE_EXTENSION.
-d	It means to disable the specific CATEGORY or FILE_EXTENSION
CATEGORY|FILE_EXTENSION	CATEGORY: Image, Video, Audio, Java, ActiveX, Compression, Executation Example: *object fe obj 1 -e Image* FILE_EXTENSION: ".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", ".sit", ".zip", ".bas", ".bat", ".com", ".exe", ".inf", ".pif", ".reg", ".scr" Example: *object fe obj 1 -e .bmp*

Example

```
> object fe obj 1 -n music
> object fe obj 1 -e Audio
> object fe obj 1 -v
Profile Index: 1
Profile Name:[music]

----------------------------------------------------------------------
Image category:
 [ ].bmp   [ ].dib   [ ].gif   [ ].jpeg  [ ].jpg   [ ].jpg2  [ ].jp2   [ ].pct
 [ ].pcx   [ ].pic   [ ].pict  [ ].png   [ ].tif   [ ].tiff
----------------------------------------------------------------------
Video category:
 [ ].asf   [ ].avi   [ ].mov   [ ].mpe   [ ].mpeg  [ ].mpg   [v].mp4   [ ].qt
 [ ].rm    [v].wmv   [ ].3gp   [ ].3gpp  [ ].3gpp2 [ ].3g2
----------------------------------------------------------------------
Audio category:
 [v].aac   [v].aiff  [v].au    [v].mp3   [v].m4a   [v].m4p   [v].ogg   [v].ra
 [v].ram   [v].vox   [v].wav   [v].wma
----------------------------------------------------------------------
Java category:
 [ ].class [ ].jad   [ ].jar   [ ].jav   [ ].java  [ ].jcm   [ ].js    [ ].jse
 [ ].jsp   [ ].jtk
----------------------------------------------------------------------
ActiveX category:
 [ ].alx   [ ].apb   [ ].axs   [ ].ocx   [ ].olb   [ ].ole   [ ].tlb   [ ].viv
 [ ].vrm
----------------------------------------------------------------------
Compression category:
 [ ].ace   [ ].arj   [ ].bzip2 [ ].bz2   [ ].cab   [ ].gz    [ ].gzip  [ ].rar
 [ ].sit   [ ].zip
----------------------------------------------------------------------
Executation category:
 [ ].bas   [ ].bat   [ ].com   [ ].exe   [ ].inf   [ ].pif   [ ].reg   [ ].scr
```

Telnet Command: object sms

This command is used to create short message object profile.

Syntax

object sms show
object sms setdefault
object sms obj *INDEX -v*
object sms obj *INDEX -n NAME*
object sms obj *INDEX -s Service Provider*
object sms obj *INDEX -u Username*

object sms obj *INDEX -p Password*
object sms obj *INDEX -q Quota*
object sms obj *INDEX -i Interval*
object sms obj *INDEX -I URL*

Syntax Description

Parameter	Description
show	It means to show the contents for all of the profiles.
setdefault	It means to return to default settings for all profiles.
[INDEX]	It means the index number (from 1 to 10) of the specified SMS object profile.
-v	It means to view the information of the specified SMS object profile.
-n [NAME]	It means to define a name for the SMS object profile. NAME: Type a name with less than 15 characters.
-s [Service Provider]	It means to specify the number of the service provider which offers the service of SMS. Different numbers represent different service provider. 0 : kotsms.com.tw (TW) 2 : textmarketer.co.uk (UK) 4 : messagemedia.co.uk (UK) 5 : bulksms.com (INT) 6 : bulksms.co.uk (UK) 7 : bulksms.2way.co.za (ZA) 8 : bulksms.com.es (ES) 9 : usa.bulksms.com (US) 10 : bulksms.de (DE) 11 : www.pswin.com (EU) 12 : www.messagebird.com (EU) 13 : www.lusosms.com (EU) 14 : www.vibeactivemedia.com (UK)
-u [Username]	It means to define a user name for the SMS object profile. Type a user name that the sender can use to register to selected SMS provider.
-p [Password]	It means to define a password for the SMS object profile. Type a password that the sender can use to register to selected SMS provider.
-q [Quota]	Type the number of the credit that you purchase from the service provider. Note that one credit equals to one SMS text message on the standard route.
-I [Interval]	It means to set the sending interval for the SMS to be delivered. Type the shortest time interval for the system to send SMS.
-I [URL]	It means to set the URL for Custom 1 and Custom 2 profiles. The profile name for Custom 1 and Custom 2 are defined in default and can not be changed.

Example

```
> object sms obj 1 –n CTC
> object sms obj 1 -n CTC
> object sms obj 1 -s 0
> object sms obj 1 -u carrie
> object sms obj 1 -p 19971125cm
> object sms obj 1 -q 2
> object sms obj 1 -i 50
> object sms obj 1 -v
Profile Index: 1
Profile Name:[CTC]
SMS Provider:[kotsms.com.tw (TW)]
Username:[carrie]
Password:[******]
Quota:[2]
Sending Interval:[50(seconds)]
```

Telnet Command: object mail

This command is used to create mail object profile.

Syntax

object mail show
object mail setdefault
object mail obj *INDEX -v*
object mail obj *INDEX -n Profile Name*
object mail obj *INDEX -s SMTP Server*
object mail obj *INDEX -l Use SSL*
object mail obj *INDEX -m SMTP Port*
object mail obj *INDEX -a Sender Address*
object mail obj *INDEX -t Authentication*
object mail obj *INDEX -u Username*
object mail obj *INDEX -p Password*
object mail obj *INDEX -i Sending Interval*

Syntax Description

Parameter	Description
show	It means to show the contents for all of the profiles.
setdefault	It means to return to default settings for all profiles.
[INDEX]	It means the index number (from 1 to 10) of the specified mail object profile.
-v	It means to view the information of the specified mail object profile.
-n [Profile Name]	It means to define a name for the mail object profile. *Profile Name*: Type a name with less than 15 characters.
-s [SMTP Server]	It means to set the IP address of the mail server.
-l [Use SSL]	It means to use port 465 for SMTP server for some e-mail server uses https as the transmission method. 0 – disable 1 – enable to use the port number.
-m [SMTP Port]	It means to set the port number for SMTP server.
-a [Sender Address]	It means to set the e-mail address (e.g., johnwash@abc.com.tw) of the sender.
-t Authentication	The mail server must be authenticated with the correct username and password to have the right of sending message out. 0 – disable 1 – enable to use the port number.
-u Username	Type a name for authentication. The maximum length of the name you can set is 31 characters.
-p Password	Type a password for authentication. The maximum length of the password you can set is 31 characters.
-i Sending Interval	Define the interval for the system to send the SMS out. The unit is second.

Example

```
> object mail obj 1 –n buyer
> object mail obj 1 -n buyer
> object mail obj 1 -s 192.168.1.98
> object mail obj 1 -m 25
> object mail obj 1 -t 1
> object mail obj 1 -u john
> object mail obj 1 -p happy123456
> object mail obj 1 -i 25
> object mail obj 1 -v
Profile Index: 1
Profile Name:[buyer]
SMTP Server:[192.168.1.98]
SMTP Port:[25]
Sender Address:[]
Use SSL:[disable]
Authentication:[enable]
Username:[john]
```

```
Password:[******]
Sending Interval:[25(seconds)]
```

Telnet Command: object noti

This command is used to create notification object profile.

Syntax

object noti show
object noti setdefault
object noti obj *INDEX -v*
object noti obj *INDEX -n Profile Name*
object mail obj *INDEX –e Category Status*
object mail obj *INDEX –d Category Status*

Syntax Description

Parameter	Description
show	It means to show the contents for all of the profiles.
setdefault	It means to return to default settings for all profiles.
[INDEX]	It means the index number (from 1 to 8) of the specified notification object profile.
-v	It means to view the information of the specified notification object profile.
-n [Profile Name]	It means to define a name for the notification object profile. *Profile Name*: Type a name with less than 15 characters.
–e	It means to enable the status of specified category.
-d	It means to disable the status of specified category.
[Category]	Available categories are: 1: WAN; 2: VPN Tunnel; 3: Temperature Alert; 4: WAN Budget; 5: CVM; 6: High Availability
[status]	For WAN – 1: Disconnected; 2: Reconnected. For VPN Tunnel - 1: Disconnected; 2: Reconnected. For Temperature Alert – 1: Out of Range. For WAN Budget – 1: Limit Reached. For CVM – 1: CPE Offline; 2: Backup Fail; 3: Restore Fail; 4: FW Update Fail; 5: VPN Profile Setup Fail. For High Availability – 1: Failover Occurred, Config Sync Fail, and Router Unstable

Example

```
> object noti obj 1 –n markbei
> object noti obj 1 –e 1 1
> object noti obj 1 –e 2 1
> object noti obj 1 –e 5 3
> object noti obj 1 –v
> object noti obj 1 -e 1 1
> object noti obj 1 -e 2 1
> object noti obj 1 -e 5 3
> object noti obj 1 -v
Profile Index: 1
Profile Name:[]
    Category                  Status
  WAN                 [v]Disconnected     [ ]Reconnected
  VPN Tunnel          [v]Disconnected     [ ]Reconnected
  Temperature Alert [ ]Out of Range
  WAN Budget Alert    [ ]Limit Reached
  CVM Alert           [ ]CPE Offline
                      [ ]CPE Config Backup Fail
                      [v]CPE Config Restore Fail
                      [ ]CPE Firmware Fpgrade Fail
                      [ ]CPE VPN Profile Setup Fail
```

```
  High Availability   [ ]Failover Occurred
                          Config Sync Fail
                          Router Unstable
```

Telnet Command: object schedule

This command is used to create schedule object profile.

Syntax

object schedule set *INDEX option*
object schedule view
object schedule setdefault

Syntax Description

Parameter	Description
set	It means to set the schedule profile.
[INDEX]	It means the index number (from 1 to 15) of the specified object profile.
option	Available options for schedule includes: -e
-e [value]	It means to enable the schedule setup. 0 – disable 1 – enable
-c [comment]	It means to set brief description for the specified profile. The length range of the comment: 1 ~ 32 characters.
-D [year][month][day]	It means to set the starting date of the profile. [year] – Must be between 2000-2049. [month] - Must be between 1-12. [day] - Must be between 1-31. For example: To set Start Date 2015/10/6, type *> object schedule set 1 -D "2015 10 6"*
-T [hour][minute]	It means to set the starting time of the profile. [hour] - Must be between 0-23. [minute] - Must be between 0-59. For example: To set Start Time 10:20, type *> object schedule set 1 -T "10 20"*
-d [hour][minute]	It means to set the duration time of the profile. [hour] - Must be between 0-23. [minute] - Must be between 0-59. For example: To set Duration Time 3:30, type *> object schedule set 1 -d "3 30"*
-a [value]	It means to set the action used for the profile. [value] – 0:Force On, 1:Force Down, 2:Enable Dial-On-Demand, 3:Disable Dial-On-Demand
-I [value]	It means to set idle time. [value] – Must be between 0-255(minute). The default is 0.
-h [option] [day]	Set how often the schedule will be applied. [option] – 0: Once, 1: Weekdays [day] – Sun, Mon, Tue, Wed, Thu, Fri, Sat If the [option] set Weekdays, then must select which days of Week. example: To select Sunday, Monday, Thursday, type *> object schedule set 1 -h "1 Sun Mon Thu"*
view [INDEX]	It means to show the content of the profile.
setdefault	It means to return to default settings for all profiles.

Example

```
> object schedule set 1 –e 1
> object schedule set 1 –c Working
> object schedule set 1 –D “2016 11 8”
> object schedule set 1 –T “8 1”
> object schedule set 1 –d “2 30”
> object schedule set 1 –a 0
> object schedule set 1 –h “1 Mon Wed”
```

```
> object schedule view 1
Index No.1

-------------------------------------------------
[v] Enable Schedule Setup
       Comment [ Working ]
       Start Date (yyyy-mm-dd) [ 2016 ]-[ 11 ]-[  8 ]
       Start Time (hh:mm)      [  8 ]:[  1 ]
       Duration Time (hh:mm)       [  2 ]:[ 30 ]
       Action                  [ Force On ]
       Idle Timeout            [ 0 ] minute(s).(max. 255, 0 for
                               default)
       ---------------------------------------------------------------
       How Often
        [ ] Once
        [v] Weekdays
           [ ]Sun  [v]Mon  [ ]Tue  [v]Wed  [ ]Thu  [ ]Fri  [ ]Sat
>
```

Telnet Command: port

This command allows users to set the speed for specific port of the router.

Syntax

port *[1, 2, 3, 4, wan1, wan2, all] [AN, 1000F, 100F, 100H, 10F, 10H, status]*

port*[enable,disable] [1, 2, 3, 4, all] [*

port status

port sniff *[on,off,port,txrx,restart,status]*

port 802.1x*[enable,disable,status,addport,delport]*

port jumbo

port wanfc

port spoof *[on, off, stat]*

port mac_flush

Syntax Description

Parameter	Description
1, 2, 3, 4, 5, wan1, wan2, all	It means the number of LAN port and WAN port.
AN… 10H	It means the physical type for the specific port. AN: auto-negotiate. 1000F: 1000M Full Duplex. 100F: 100M Full Duplex. 100H: 100M Half Duplex. 10F: 10M Full Duplex. 10H: 10M Half Duplex.
status	It means to view the Ethernet port status.
wanfc	It means to set WAN flow control.
spoof	It means to enable /disable spoofing detection. Stat – Display current spoofing status (on or off).

Example

```
> port 1 100F
```

```
%Set Port 1 Force speed 100 Full duplex OK !!!
```

Telnet Command: portmaptime

This command allows you to set a time of keeping the session connection for specified protocol.

Syntax

portmaptime *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-t <sec>	It means “TCP” protocol. <sec>: Type a number to set the TCP session timeout.
-u <sec>	It means “UDP” protocol. <sec>: Type a number to set the UDP session timeout.
-i <sec>	It means “IGMP” protocol. <sec>: Type a number to set the IGMP session timeout.
-w <sec>	It means “TCP WWW” protocol. <sec>: Type a number to set the TCP WWW session timeout.
-s <sec>	It means “TCP SYN” protocol. <sec>: Type a number to set the TCP SYN session timeout.
-f	It means to flush all portmaps (useful for diagnostics).
-l <List>	List all settings.

Example

```
> portmaptime -t 86400 -u 300  -i 10
> portmaptime -l
------ Current setting ------
TCP Timeout   : 86400 sec.
UDP Timeout   : 300 sec.
IGMP Timeout  : 10 sec.
TCP WWW Timeout: 60 sec.
TCP SYN Timeout: 60 sec.
```

Telnet Command: ppa

This command allows you to configure PPA mode.

ppa *[-<command> <parameter> | ...]*

ppa n *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-m <mode>	Specify a mode.

	1=auto 2=manual(traffic) 3=manual(qos) 4=manual(specific hosts) 0=disable
-p <proto>	Specify a protocol. proto - 1-TCP; 2-UDP; 3-Both.
-b 1/0	Enable/disable TWO-way hardware acceleration.
-M enable/disable	Enable/disable the multicast hardware acceleration.
-v	Show PPA_WAN_Table and PPA_LAN_Table for reference.
-c	Clean all settings.
ppa n – used in QoS or specific host	
-l <rule>	Specify an index number of rule profile for QoS mode.
-h <host>	Type an IP address for Specific Host mode.
-s <start port>	Specify a starting port number for Specific Host mode.
-e <end port>	Specify an ending port number for Specific Host mode

Example

```
> ppa -m 1 -p 1 -b 0
 Set ok! The PPA mode is Auto

% You need to set the Manual mode first !

%TWO way accleration is disable

> ppa -v
% PPA mode is Auto
%PPA Protocol TCP 1, UDP 0
%PPA two way disable
%PPA time  is 10
%PPA range is 192
%PPA LAN entries 0
%PPA WAN entries 0
```

Telnet Command: prn

This command allows you to view current status (interface and driver) of USB printer.

Syntax

prn status

prn debug

Example

```
> prn status
Interface: USB bus 2.0
Printer: NotReady

> prn debug
conn[0] :
```

```
none
conn[1] :
none
conn[2] :
none
conn[3] :
none
LPD_data_total=0

usblp_ptr=0
UsbPrintReady=0, UsbIsPrinting=0
```

Telnet Command: qos setup

This command allows user to set general settings for QoS.

Syntax

qos setup *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-h	Type it to display the usage of this command.
-m <mode>	It means to define which traffic the QoS control settings will apply to and eable QoS control. 0: disable. 1: in, apply to incoming traffic only. 2: out, apply to outgoing traffic only. 3: both, apply to both incoming and outgoing traffic. Default is enable (for outgoing traffic).
-i <bandwidth>	It means to set inbound bandwidth in kbps (Ethernet WAN only) The available setting is from 1 to 100000.
-o <bandwidth>	It means to set outbound bandwidth in kbps (Ethernet WAN only). The available setting is from 1 to 100000.
-r <index:ratio>	It means to set ratio for class index, in %.
-u <mode>	It means to enable bandwidth control for UDP. 0: disable 1: enable Default is disable.
-p <ratio>	It means to enable bandwidth limit ratio for UDP.
-t <mode>	It means to enable/disable Outbound TCP ACK Prioritize. 0: disable 1: enable
-V	Show all the settings.
-D	Set all to factory default (for all WANs).
[…]	It means that you can type in several commands in one line.

Example

```
> qos setup -m 3 -i 9500 -o 8500 -r 3:20 -u 1 -p 50 -t 1

 WAN1 QOS mode is both
 Wan 1 is XDSL model ,don,t need to set up
 Wan 1 is XDSL model ,don,t need to set up
 WAN1 class 3 ratio set to 20
 WAN1 udp bandwidth control set to enable
 WAN1 udp bandwidth limit ratio set to 50
 WAN1 Outbound TCP ACK Prioritizel set to enable
QoS WAN1 set complete; restart QoS
>
```

Telnet Command: qos class

This command allows user to set QoS class.

Syntax

qos class -c *[no] –[a|e|d] [no][-<command> <parameter> | …]*

Syntax Description

Parameter	Description
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-h	Type it to display the usage of this command.
-c <no>	Specify the inde number for the class. Available value for <no> contains 1, 2 and 3. The default setting is class 1.
-n <name>	It means to type a name for the class.
-a	It means to add rule for specified class.
-e <no>	It means to edit specified rule. <no>: type the index number for the rule.
-d <no>	It means to delete specified rule. <no>: type the index number for the rule.
-m <mode>	It means to enable or disable the specified rule. 0: disable, 1: enable
-I <addr>	Set the local address. *Addr1* – It means Single address. Please specify the IP address directly, for example, "*-I 172.16.3.9*". *addr1:addr2* – It means Range address. Please specify the IP addresses, for example, "*-I 172.16.3.9: 172.16.3.50*." *addr1:subnet* – It means the subnet address with start IP address. Please type the subnet and the IP address, for example, "*-I 172.16.3.9:255.255.0.0".0* *any* – It means Any address. Simple type "*-I*" to specify any address for this command.
-r <addr>	Set the remote address. *addr1* – It means Single address. Please specify the IP address

	directly, for example, "*-I 172.16.3.9*". *addr1:addr2* – It means Range address. Please specify the IP addresses, for example, "*-I 172.16.3.9: 172.16.3.50*." *addr1:subnet* – It means the subnet address with start IP address. Please type the subnet and the IP address, for example, "*-I 172.16.3.9:255.255.0.0".0* *any* – It means Any address. Simple type "*-I*" to specify any address for this command.
-p <DSCP id>	Specify the ID.
-s <Service type>	Specify the service type by typing the number. The available types are listed as below: 1:ANY 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:NEWS 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
-S <d/s>	Show the content for specified DSCP ID/Service type.
-V <1/2/3>	Show the rule in the specified class.
[…]	It means that you can type in several commands in one line.

Example

```
> qos class -c 2 -n draytek -a -m 1 -l 192.168.1.50:192.168.1.80

 Following setting will set in the class2
 class 2 name set to draytek
 Add a rule in class2
 Class2 the 1 rule enabled
 Set local address type to Range, 192.168.1.50:192.168.1.80
```

Telnet Command: qos type

This command allows user to configure protocol type and port number for QoS.

Syntax

qos type *[-a <service name> | -e <no> | -d <no>]***.**

Syntax Description

Parameter	Description
-a <name>	It means to add rule.
-e <no>	It means to edit user defined service type. "no" means the index number. Available numbers are 1~40.
-d <no>	It means to delete user defined service type. "no" means the index number. Available numbers are 1~40.
-n <name>	It means the name of the service.
-t <type>	It means protocol type. 6: tcp(default) 17: udp 0: tcp/udp <1~254>: other
-p <port>	It means service port. The typing format must be [start:end] (ex., 510:330).

-l	List user defined types. “no” means the index number. Available numbers are 1~40.

Example

```
> qos type -a draytek -t 6 -p 510:1330

 service name set to draytek
 service type set to 6:TCP
 Port type set to Range
 Service Port set to 510 ~ 1330
>
```

Telnet Command: qos voip

This command allows user to enable or disable the QoS for VoIP and RTP.

Syntax

qos voip *[on/off]*

Syntax Description

Parameter	Description
on/off	On – Enable the QoS for VoIP. Off – Disable th QoS for VoIP.

Example

```
> qos voip off
QoS for VoIP: Disable; SIP Port: 5060
```

Telnet Command: quit

This command can exit the telnet command screen.

Telnet Command: show lan

This command displays current status of LAN IP address settings.

Example

```
> show lan
The LAN settings:
         ip            mask       dhcp  star_ip         pool   gateway
-------------------------------------------------------------------------
-----
[V]LAN1  192.168.1.1   255.255.255.0   [V]  192.168.1.10      200
192.168.1.1
[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]Route 192.168.0.1   255.255.255.0   [V]  0.0.0.0     0  192.168.0.1
```

Telnet Command: show dmz

This command displays current status of DMZ host.

Example

```
> show dmz
%     WAN1 DMZ mapping status:
 Index  Status  WAN1 aux IP    Private IP
-----------------------------------------------------
   1    Disable 172.16.3.221
   2    Disable 192.168.1.65
```

Telnet Command: show dns

This command displays current status of DNS setting

Example

```
> show dns
%%     Domain name server settings:
%            Primary DNS: [Not set]
%            Secondary DNS: [Not set]
```

Telnet Command: show openport

This command displays current status of open port setting.

Example

```
> show openport
%%     Openport settings:
Index   Status  Comment        Local IP Address
*****************************************************
                 No data entry.
```

Telnet Command: show nat

This command displays current status of NAT.

Example

```
> show nat
 Port Redirection Running Table:

Index  Protocol  Public Port   Private IP       Private Port
 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
16           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
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
```

Telnet Command: show portmap

This command displays the table of NAT Active Sessions.

Example

```
> show portmap
-------------------------------------------------------------------------
  Private_IP:Port Pseudo_IP:Port Peer_IP:Port [Timeout/Protocol/Flag]
-------------------------------------------------------------------------
```

Telnet Command: show pmtime

This command displays the reuse time of NAT session.

Level0: It is the default setting.

Level1: It will be applied when the NAT sessions are smaller than 25% of the default setting.

Level2: It will be applied when the NAT sessions are smaller than the eighth of the default setting.

Example

```
> show pmtime
  Level0 TCP=86400001 UDP=300001 ICMP=10001
  Level1 TCP=600000 UDP=90000 ICMP=7000
  Level2 TCP=60000 UDP=30000 ICMP=5000
```

Telnet Command: show session

This command displays current status of current session.

Example

```
> show session
% Maximum Session Number: 10000
% Maximum Session Usage: 49
% Current Session Usage: 0
% Current Session Used(include waiting for free): 0
% WAN1 Current Session Usage: 0
```

Telnet Command: show status

This command displays current status of LAN and WAN connections.

Example

```
> show status
System Uptime:71:2:7
LAN Status
Primary DNS:8.8.8.8          Secondary DNS:8.8.4.4
IP Address:192.168.1.1       Tx Rate:61614    Rx Rate:45219

WAN 1 Status: Disconnected
Enable:Yes      Line:Ethernet    Name:
Mode:PPPoE      Up Time:0:00:00    IP:---          GW IP:---
TX Packets:0         TX Rate:0   RX Packets:0         RX Rate:0


WAN 2 Status: Disconnected
Enable:Yes      Line:Ethernet    Name:
Mode:DHCP Client Up Time:0:00:00    IP:---          GW IP:---
TX Packets:0         TX Rate:0   RX Packets:0         RX Rate:0

WAN 3 Status: Disconnected
Enable:Yes      Line:USB        Name:
Mode:---        Up Time:0:00:00    IP:---          GW IP:---
TX Packets:0         TX Rate:0   RX Packets:0         RX Rate:0
```

Telnet Command: show traffic

This comman can display traffic graph for WAN1, WAN2, transmitted bytes, receivied bytes and sessions.

Syntax

show traffic *[wan1/wan2] [tx/rx] [weekly]*

show traffic session *[weekly]*

Example

```
> show traffic session weekly0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,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 ,1 ,3 ,0 ,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 ,0 ,0
> show traffic wan1 tx weekly0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
```

```
,0 ,0 ,0 
```

0, 0, 0,

Telnet Command: show statistic

This command displays statistics for WAN interface.

Syntax

show statistic

show statistic reset *[interface]*

Syntax Description

Parameter	Description
reset	It means to reset the transmitted/received bytes to Zero.
interface	It means to specify WAN1 ~WAN5 (including multi-PVC) interface for displaying related statistics.

Example

```
> show statistic
 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
 >
```

Telnet Command: smb setting

This command is used to configure file sharing settings for SMB server.

Syntax

smb setting *[enable/disable]*

smb setting *show status*

smb setting *set workgroup [Workgroup name]*

smb setting *set host [host name]*

smb setting *set access [LAN or LANWAN]*

Syntax Description

Parameter	Description
enable/disable	Enable or disable the SMB service.
show status	Display current status of SMB service.
Set workgroup [Workgroup name]	Set a name of workgroup for SMB service.
set host [host name]	Set a name of the host for SMB service.
set access [LAN or LANWAN]	Allow to access into SMB server by LAN or borth LAN and WAN.

Example

```
> smb setting enable
SMB service is enabled.

> smb setting set access LAN
```

```
Allow SMB access from LAN only.
>
```

Telnet Command: srv dhcp dhcp2

This command is used to enable DCHP2 server.

Syntax

srv dhcp dhcp2 *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-l<enable>	It menas to enable the LAN port to public DHCP. 0: Disenable 1: Enable
-m<enable>	It menas to enable MAC address to public DHCP. 0: Disenable 1: Enable
-e<id>	It menas to turn on the flag of LAN port 1/2/3/4.
-d<id>	It menas to turn off the flag of LAN port 1/2/3/4.
-v	It menas to view current status.

Example

```
> srv dhcp dhcp2 -l 1 -e 1
> srv dhcp dhcp2 -v
 2nd DHCP server flag status --
   Server works on specified MAC address: ON
   Server works on specified LAN port: ON
   Port 1 flag: ON
   Port 2 flag: ON
   Port 3 flag: OFF
   Port 4 flag: OFF
```

Telnet Command: srv dhcp public

This command allows users to configure DHCP server for second subnet.

Syntax

srv dhcp public *start [IP address]*

srv dhcp public *cnt [IP counts]*

srv dhcp public *status*

srv dhcp public *add [MAC Addr XX-XX-XX-XX-XX-XX]*

srv dhcp public *del [MAC Addr XX-XX-XX-XX-XX-XX/all/ALL]*

Syntax Description

Parameter	Description
start	It means the starting point of the IP address pool for the DHCP

	server.
IP address	It means to specify an IP address as the starting point in the IP address pool.
cnt	It means the IP count number.
IP counts	It means to specify the number of IP addresses in the pool. The maximum is 10.
status	It means the execution result of this command.
add	It means creating a list of hosts to be assigned.
del	It means removing the selected MAC address.
MAC Addr	It means to specify MAC Address of the host.
all/ALL	It means all of the MAC addresses.

Example

```
Vigor> ip route add 192.168.1.56 255.255.255.0 192.168.1.12 3 default
Vigor> srv dhcp public status
Index   MAC Address
```

Telnet Command: srv dhcp dns1

This command allows users to set Primary IP Address for DNS Server in LAN.

Syntax

srv dhcp dns1 *[?]*

srv dhcp dns1 *[DNS IP address]*

Syntax Description

Parameter	Description
?	It means to display current IP address of DNS 1 for the DHCP server.
DNS IP address	It means the IP address that you want to use as DNS1. **Note:** The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns1 168.95.1.1
% srv dhcp dns1 <DNS IP address>
% Now: 168.95.1.1
(IP Routed Subnet dns same as NAT Subnet dns)
```

Telnet Command: srv dhcp dns2

This command allows users to set Secondary IP Address for DNS Server in LAN.

Syntax

srv dhcp dns2 *[?]*

srv dhcp dns2 *[DNS IP address]*

Syntax Description

Parameter	Description
?	It means to display current IP address of DNS 2 for the DHCP server.
DNS IP address	It means the IP address that you want to use as DNS2. **Note:** The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns2 10.1.1.1
% srv dhcp dns2 <DNS IP address>
% Now: 10.1.1.1
(IP Routed Subnet dns same as NAT Subnet dns)
```

Telnet Command: srv dhcp frcdnsmanl

This command can force the router to invoke DNS Server IP address.

Syntax

srv dhcp frcdnsmanl *[on]*

srv dhcp frcdnsmanl *[off]*

Syntax Description

Parameter	Description
?	It means to display the current status.
on	It means to use manual setting for DNS setting.
Off	It means to use auto settings acquired from ISP.

Example

```
> srv dhcp frcdnsmanl on
% Domain name server now is using manual settings!
> srv dhcp frcdnsmanl off
% Domain name server now is using auto settings!
```

Telnet Command: srv dhcp gateway

This command allows users to specify gateway address for DHCP server.

Syntax

srv dhcp gateway *[?]*

srv dhcp gateway *[Gateway IP]*

Syntax Description

Parameter	Description
?	It means to display current gateway that you can use.
Gateway IP	It means to specify a gateway address used for DHCP server.

Example

```
> srv dhcp gateway 192.168.2.1
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: srv dhcp ipcnt

This command allows users to specify IP counts for DHCP server.

Syntax

srv dhcp ipcnt *[?]*

srv dhcp ipcnt *[IP counts]*

Syntax Description

Parameter	Description
?	It means to display current used IP count number.
IP counts	It means the number that you have to specify for the DHCP server.

Example

```
> srv dhcp ipcnt ?
% srv dhcp ipcnt <IP counts>
% Now: 150
```

Telnet Command: srv dhcp off

This function allows users to turn off DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: srv dhcp on

This function allows users to turn on DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: srv dhcp relay

This command allows users to set DHCP relay setting.

Syntax

srv dhcp relay servip *[server ip]*

srv dhcp relay subnet *[index]*

Syntax Description

Parameter	Description
server ip	It means the IP address that you want to used as DHCP server.
Index	It means subnet 1 or 2. Please type 1 or 2. The router will invoke this function according to the subnet 1 or 2 specified here.

Example

```
> srv dhcp relay servip 192.168.1.46
> srv dhcp relay subnet 2
>srv dhcp relay servip ?
% srv dhcp relay servip <server ip>
% Now: 192.168.1.46
```

Telnet Command: srv dhcp startip

Syntax

srv dhcp startip *[?]*

srv dhcp startip *[IP address]*

Syntax Description

Parameter	Description
?	It means to display current used start IP address.
IP address	It means the IP address that you can specify for the DHCP server as the starting point.

Example

```
> srv dhcp startip 192.168.1.53
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: srv dhcp status

This command can display general information for the DHCP server, such as IP address, MAC address, leased time, host ID and so on.

Example

```
> srv dhcp status
DHCP server: Relay Agent
Default gateway: 192.168.1.1
Index   IP Address     MAC Address           Leased Time     HOST ID
1      192.168.1.113   00-05-5D-E4-D8-EE      17:20:08       A1000351
```

Telnet Command: srv dhcp leasetime

This command can set the lease time for the DHCP server.

Syntax

srv dhcp leasetime *[?]*

srv dhcp leasetime *[Lease Time (sec)]*

Syntax Description

Parameter	Description
?	It means to display current leasetime used for the DHCP server.
Lease Time (sec)	It means the lease time that DHCP server can use. The unit is second.

Example

```
> srv dhcp leasetime ?
% srv dhcp leasetime <Lease Time (sec.)>
% Now: 86400
>
```

Telnet Command: srv dhcp nodetype

This command can set the node type for the DHCP server.

Syntax

srv dhcp nodetype <*count*>

Syntax Description

Parameter	Description
count	It means to specify a type for node. 1. B-node 2. P-node 4. M-node 8. H-node

Example

```
> srv dhcp nodetype 1
> srv dhcp nodetype ?
%% srv dhcp nodetype <count>
%% 1. B-node 2. P-node 4. M-node 8. H-node
% Now: 1
```

Telnet Command: srv dhcp primWINS

This command can set the primary IP address for the DHCP server.

Syntax

srv dhcp primWINS *[WINS IP address]*

srv dhcp primWINS clear

Syntax Description

Parameter	Description
WINS IP address	It means the IP address of primary WINS server.
clear	It means to remove the IP address settings of primary WINS server.

Example

```
> srv dhcp primWINS 192.168.1.88
> srv dhcp primWINS ?
%% srv dhcp primWINS <WINS IP address>
%% srv dhcp primWINS clear
% Now: 192.168.1.88
```

Telnet Command: srv dhcp secWINS

This command can set the secondary IP address for the DHCP server.

Syntax

srv dhcp secWINS *[WINS IP address]*

srv dhcp secWINS clear

Syntax Description

Parameter	Description
WINS IP address	It means the IP address of secondary WINS server.
clear	It means to remove the IP address settings of second WINS server.

Example

```
> srv dhcp secWINS 192.168.1.180
> srv dhcp secWINS ?
%% srv dhcp secWINS <WINS IP address>
%% srv dhcp secWINS clear
% Now: 192.168.1.180
```

Telnet Command: srv dhcp expired_RecycleIP

This command can set the time to check if the IP address can be assigned again by DHCP server or not.

Syntax

srv dhcp expRecycleIP <*sec time*>

Syntax Description

Parameter	Description
sec time	It means to set the time (5~300 seconds) for checking if the IP can be assigned again or not.

Example

```
Vigor> srv dhcp expRecycleIP 250
% DHCP expired_RecycleIP = 250
```

Telnet Command: srv dhcp tftp

This command can set the TFTP server as the DHCP server.

Syntax

srv dhcp tftp <*TFTP server name*>

Syntax Description

Parameter	Description
TFTP server name	It means to type the name of TFTP server.

Example

```
> srv dhcp tftp TF123
> srv dhcp tftp ?
%% srv dhcp tftp <TFTP server name>
% Now: TF123
```

Telnet Command: srv dhcp tftpdel

This command can remove the name defined for the TFTP server.

Syntax

srv dhcp tftpdel

Example

```
> srv dhcp tftp TF123
> srv dhcp tftp ?
%% srv dhcp tftp <TFTP server name>
% Now: TF123
> srv dhcp tftpdel
 % The TFTP Server Name had been deleted !!!
```

Telnet Command: srv dhcp option

This command can set the custom option for the DHCP server.

Syntax

srv dhcp option *-h*

srv dhcp option *-l*

srv dhcp option *-d [idx]*

srv dhcp option *-e [1 or 0] -c [option number] -v [option value]*

srv dhcp option *-e [1 or 0] -c [option number] -a [option value]*

srv dhcp option -*e [1 or 0] -c [option number] -x [option value]*

srv dhcp option *-u [idx unmber]*

Syntax Description

Parameter	Description
-h	It means to display usage of this command.
-l	It means to display all the user defined DHCP options.
-d[idx]	It means to delete the option number by specifying its index number.
-e [1 or 0]	It means to enable/disable custom option feature. 1:enable 0:disable
-c	It means to set option number. Available number ranges from 0 to 255.
-v	It means to set option number by typing string.
-a	It means to set the option value by specifying the IP address.
-x	It means to set option number with the format of Hexadecimal characters.
-u	It means to update the option value of the sepecified index.

idx number	It means the index number of the option value.

Example

```
> srv dhcp option -e 1 -c 18 -v /path
> srv dhcp option -l
% state   idx interface        opt type    data



% enable  1   ALL LAN          18  ASCII   /path
```

Telnet Command: srv nat dmz

This command allows users to set DMZ host. Before using this command, please set WAN IP Alias first.

Syntax

srv nat dmz n m *[-<command> <parameter> | …]*

Syntax Description

Parameter	Description
n	It means to map selected WAN IP to certain host. 1: wan1 2: wan2
m	It means the index number of the DMZ host. Default setting is "1" (WAN 1). It is only available for Static IP mode. If you use other mode, you can set 1 ~ 8 in this field. If WAN IP alias has been configured, then the number of DMZ host can be added more.
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-e	It means to enable/disable such feature. 1:enable 0:disable
-i	It means to specify the private IP address of the DMZ host.
-r	It means to remove DMZ host setting.
-v	It means to display current status.

Example

```
> srv nat dmz 1 1 -i 192.168.1.96
> srv nat dmz -v
%     WAN1 DMZ mapping status:
 Index  Status  WAN1 aux IP    Private IP
-----------------------------------------------------
   1    Disable 0.0.0.0 192.168.1.96
```

Telnet Command: srv nat ipsecpass

This command allows users to enable or disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.

Syntax

srv nat ipsecpass *[options]*

Syntax Description

Parameter	Description
[options]	The available commands with parameters are listed below.
on	It means to enable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
off	It means to disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
status	It means to display current status for checking.

Example

```
> srv nat ipsecpass status
%% Status: IPsec ESP pass-thru and IKE src_port:500 preservation is
OFF.
```

Telnet Command: srv nat openport

This command allows users to set open port settings for NAT server.

Syntax

srv nat openport n m *[-<command> <parameter> | …]*

Syntax Description

Parameter	Description
n	It means the index number for the profiles. The range is from 1 to 20.
m	It means to specify the sub-item number for this profile. The range is from 1 to 10.
[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-a <enable>	It means to enable or disable the open port rule profile. 0: disable 1:enable
-c <comment>	It means to type the description (less than 23 characters) for the defined network service.
-i <local ip>	It means to set the IP address for local computer. Local ip: Type an IP address in this field.
-w <idx>	It means to specify the public IP. 1: WAN1 Default, 2: WAN1 Alias 1, …and so on.
-p <protocol>	Specify the transport layer protocol. Available values are TCP, UDP and ALL.

-s<start port>	It means to specify the starting port number of the service offered by the local host. The range is from 0 to 65535.
-e<end port>	It means to specify the ending port number of the service offered by the local host. The range is from 0 to 65535.
-v	It means to display current settings.
-r <remove>	It means to delete the specified open port setting. remove: Type the index number of the profile.
-f <flush>	It means to return to factory settings for all the open ports profiles.

Example

```
> srv nat openport 1 1 -a 1 -c games -i 192.168.1.100 -w 1 -p TCP -s
23 -e 83
> srv nat openport -v
%% Status: Enable
%% Comment: games
%% Private IP address: 192.168.1.100
Index   Protocal       Start Port     End Port
**************************************************************
  1.    TCP            23             83

%% Status: Disable
%% Comment:
%% Private IP address: 0.0.0.0
Index   Protocal       Start Port     End Port
**************************************************************

%% Status: Disable
%% Comment:
%% Private IP address: 0.0.0.0
Index   Protocal       Start Port     End Port
**************************************************************
>
```

Telnet Command: srv nat portmap

This command allows users to set port redirection table for NAT server.

Syntax

srv nat portmap *add [idx][serv name][proto][pub port][pri ip][pri port][wan1/wan2]*

srv nat portmap *del [idx]*

srv nat portmap *disable [idx]*

srv nat portmap *enable [idx] [proto]*

srv nat portmap *flush*

srv nat portmap *table*

Syntax Description

Parameter	Description
Add[idx]	It means to add a new port redirection table with an index number.

	Available index number is from 1 to 10.
serv name	It means to type one name as service name.
proto	It means to specify TCP or UDP as the protocol.
pub port	It means to specify which port can be redirected to the specified Private IP and Port of the internal host.
pri ip	It means to specify the private IP address of the internal host providing the service.
pri port	It means to specify the private port number of the service offered by the internal host.
wan1/wan2	It means to specify WAN interface for the port redirection.
del [idx]	It means to remove the selected port redirection setting.
disable [idx]	It means to inactivate the selected port redirection setting.
enable [idx]	It means to activate the selected port redirection setting.
flush	It means to clear all the port mapping settings.
table	It means to display Port Redirection Configuration Table.

Example

```
> srv nat portmap add 1 game tcp 80 192.168.1.11 100 wan1
> srv nat portmap table

NAT Port Redirection Configuration Table:

Index  Service Name   Protocol  Public Port  Private IP     Private
Port ifno
 1    game            6         80   192.168.1.11        100
-1
 2                    0          0                    0     -2
 3                    0          0                    0     -2
 4                    0          0                    0     -2
 5                    0          0                    0     -2
 6                    0          0                    0     -2
 7                    0          0                    0     -2
 8                    0          0                    0     -2
 9                    0          0                    0     -2
10                    0          0                    0     -2
11                    0          0                    0     -2
12                    0          0                    0     -2
13                    0          0                    0     -2
14                    0          0                    0     -2
15                    0          0                    0     -2
16                    0          0                    0     -2
17                    0          0                    0     -2
18                    0          0                    0     -2

19                    0          0                    0     -2

20                    0          0                    0     -2
```

```
Protocol: 0 = Disable, 6 = TCP, 17 = UDP
```

Telnet Command: srv nat status

This command allows users to view NAT Port Redirection Running Table.

Example

```
> srv nat status
NAT Port Redirection Running Table:

Index  Protocol  Public Port   Private IP       Private Port
 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
16          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

--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: srv nat showall

This command allows users to view a summary of NAT port redirection setting, open port and DMZ settings.

Example

```
>  srv nat showall ?
Index   Proto   WAN IP:Port              Private IP:Port          Act
**************************************************************************
****
R01     TCP     0.0.0.0:80               192.168.1.11:100         Y

O01     TCP     0.0.0.0:23~83             192.168.1.100:23~83       Y

D01     All     0.0.0.0                  192.168.1.96             Y

R:Port Redirection, O:Open Ports, D:DMZ
```

Telnet Command: switch -i

This command is used to obtain the TX (transmitted) or RX (received) data for each connected switch.

Syntax

switch -i *[switch idx_no] [option]*

Syntax Description

Parameter	Description
switch idx_no	It means the index number of the switch profile.
option	The available commands with parameters are listed below. *cmd* *acc* *traffic [on/off/status/tx/rx]*
cmd	It means to send command to the client.
acc	It means to set the client authentication account and password.
traffic [on/off/status/tx/rx]	It means to turn on/off or display the data transmission from the client.

Example

```
>  switch -i 1 traffic on
External Device NO. 1 traffic statistic function is enable
```

Telnet Command: switch status

This command is used to display current status for external devices.

Example

```
> switch status
External Device auto discovery status : Disable

 No Respond to External Device : Enable
```

Telnet Command: switch not_respond

This command is used to detect the external device automatically and display on this page.

Syntax

switch not_respond 0

switch not_respond 1

Syntax Description

Parameter	Description
0	Disable the option of "No Respond to External Device packets".
1	Enable the option of "No Respond to External Device packets".

Example

```
> switch not_respond 1
slave not respond!
>
```

Telnet Command: switch on

This command is used to turn on the auto discovery for external devices.

Example

```
>  switch on
Enable Extrnal Device auto discovery!
```

Telnet Command: switch off

This command is used to turn off the auto discovery for external devices.

Example

```
>  switch off
Disable External Device auto discovery!
```

Telnet Command: switch list

This command is used to display the connection status of the switch.

Example

```
> switch list?
No.      Mac             IP         status   Dur Time   Model_Name
-------------------------------------------------------------------
---------
[1]  00-50-7f-cd-07-48  192.168.1.3    On-Line   00:01:01
Vigor2920 Series
```

Telnet Command: switch clear

This command is used to reset the switch table and reboot the router.

Syntax

switch clear *[idx]*

Syntax Description

Parameter	Description
idx	It means the index number of each item shown on the table. The range is from 1 to 8.
-f	It means to clear all of the data.

Example

```
> switch clear 1
Switch Data clear successful

> switch clear -f
Switch Data clear successful
```

Telnet Command: switch query

This command is used to enable or disable the switch query.

Example

```
> switch query on
Extern Device status query is Enable
> switch query off
Extern Device status query is Disable
```

Telnet Command: sys admin

This command is used for RD engineer to access into test mode of Vigor router.

Telnet Command: sys adminuser

This command is used to create user account and specify LDAP server. The server will authenticate the local user who wants to access into the 網頁使用者介面 of Vigor router.

Syntax

sys adminuser *[option]*

sys adminuser edit *[index] username password*

Syntax Description

Parameter	Description
option	Available options includes: Local [0-1] LDAP [0-1] edit [INDEX] delete [INDEX] view [INDEX]
Local [0-1]	0 – Disable the local user. 1 – Enable the local user.
LDAP [0-1]	0 – Disable the LDAP. 1 – Enable the LDAP.
edit [INDEX] username password	Edit an existed user account or create a new local user account. [INDEX] – 1 ~8. There are eight profiles to be added / edited. Username – Type a new name for local user. Password – Type a password for local user.
delete [INDEX]	Delete a local user account.
view [INDEX]	Show the user account/password detail information.

Example

```
> sys adminuser Local 1
Local User has enabled!
> sys adminuser LDAP 1
LDAP has enabled!
>> sys adminuser edit 1 carrie test123
Updated!
>> sys adminuser view 1
```

```
Index:1
User Name:carrie
User Password:test123
```

Telnet Command: sys board

This command is used to turn on or turn off the function of physical factory reset button, WLAN button, LEDs, and / or the USB ports on Vigor router.

Syntax

sys board button def *[on/off]*

sys board button wlan *[on/off]*

sys board led control *[on/off]*

sys board led sleepMode *[on/off]*

sys board led sleepMode time *[minute]*

sys board usb p1/p2 *[on/off]*

Syntax Description

Parameter	Description
button def [on/off]	on – It is the default value (Enabled). off – Disable the reset function of the factory reset button.
button wlan [on/off]	on – It is the default value (Enabled). off - Disable the ability of the Wireless button to control WLAN and WPS functions.
led control [on/off]	on – It is the default value (Enabled). The LEDs on the front panel is always on. off – The LEDs on the front panel is always off.
led sleepMode [on/off]	The function of SleepMode will be available only when LED control is set to "On". on – Enable the function of sleep mode. off – Disable the function of sleep mode.
led sleepMode time [minute]	Set the countdown time for the LEDs to sleep. [minute] – Enter a value (e.g., 1, 2, 3 and etc.)
usb p1/p2 [on/off]	on – It is the default value (Enabled). off – Disable the USB port 1 or 2.

Example

```
> sys board button ?
 sys board button [def/wlan [on/off]]
 The button will be invalid after turn it off.
 - default button is on now.
 - wlan   button is on now.
> sys board button def off
 default button is off now.
> sys board button def on
 default button is on now.
> sys board usb p2 off
 USB port2 power is off now.
> sys board led sleepMode ?
```

```
Usage:
 sys board led sleepMode [on/off]
                      [time] [minute]
Current Setting:
 LEDs Sleep Mode is off now.
 Sleep Countdown Time : 1 minute(s)
> sys board led sleepMode on
 LEDs Sleep Mode is on now.
> sys board led sleepMode time 3
 Sleep Countdown Time set as 3 minute(s).
```

Telnet Command: sys bonjour

This command is used to disable/enable and configure the Bonjour service.

Syntax

sys bonjour *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
-e <enable>	It is used to disable/enable bonjour service (0: disable, 1: enable).
-h <enable>	It is used to disable/enable http (web) service (0: disable, 1: enable).
-t <enable>	It is used to disable/enable telnet service (0: disable, 1: enable).
-f <enable>	It is used to disable/enable FTP service (0: disable, 1: enable).
-s <enable>	It is used to disable/enable SSH service (0: disable, 1: enable).
-p <enable>	It is used to disable/enable printer service (0: disable, 1: enable).
-6 <enable>	It is used to disable/enable IPv6 (0: disable, 1: enable).

Example

```
> sys bonjour -s 1
>
```

Telnet Command: sys cfg

This command reset the router with factory default settings. When a user types this command, all the configuration will be reset to default setting.

Syntax

sys cfg default

sys cfg status

Syntax Description

Parameter	Description
default	It means to reset current settings with default values.
status	It means to display current profile version and status.

Example

```
> sys cfg status
Profile version: 3.0.0   Status: 1 (0x491e5e6c)
> sys cfg default
>
```

Telnet Command: sys cmdlog

This command displays the history of the commands that you have typed.

Example

```
> sys cmdlog
% Commands Log: (The lowest index is the newest !!!)
    [1] sys cmdlog
    [2] sys cmdlog ?
    [3] sys ?
    [4] sys cfg status
    [5] sys cfg ?
```

Telnet Command: sys ftpd

This command displays current status of FTP server.

Syntax

sys ftpd *on*

sys ftpd *off*

Syntax Description

Parameter	Description
on	It means to turn on the FTP server of the system.
off	It means to turn off the FTP server of the system.

Example

```
> sys ftpd on
% sys ftpd turn on !!!
```

Telnet Command: sys domainname

This command can set and remove the domain name of the system when DHCP mode is selected for WAN.

Syntax

sys domainname *[wan1/wan2] [Domain Name Suffix]*

sys domainname *[wan1/wan2] clear*

Syntax Description

Parameter	Description
wan1/wan2	It means to specify WAN interface for assigning a name for it.
Domain Name Suffix	It means the name for the domain of the system. The maximum number of characters that you can set is 40.
clear	It means to remove the domain name of the system.

Example

```
> sys domainname wan1 clever
> sys domainname wan2 intellegent
> sys domainname ?
```

```
% sys domainname <wan1/wan2> <Domain Name Suffix (max. 40 characters)>
% sys domainname <wan1/wan2> clear
% Now: wan1 == clever, wan2 ==intelligent
>
```

Telnet Command: sys iface

This command displays the current interface connection status (UP or Down) with IP address, MAC address and Netmask for the router.

Example

```
> sys iface
Interface 0 Ethernet:
Status: UP
IP Address: 192.168.1.1      Netmask: 0xFFFFFF00 (Private)
IP Address: 0.0.0.0          Netmask: 0xFFFFFFFF
MAC: 00-50-7F-00-00-00
Interface 4 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-02
Interface 5 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-03
Interface 6 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-04
Interface 7 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-05
Interface 8 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-06

Interface 9 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-07
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
>
```

Telnet Command: sys name

This command can set and remove the name for the router when DHCP mode is selected for WAN.

Syntax

sys name *[wan1] [ASCII string]*

sys name *[wan1]* **clear**

Syntax Description

Parameter	Description
wan1	It means to specify WAN interface for assigning a name for it.
ASCII string	It means the name for router. The maximum character that you can set is 20.

Example

```
> sys name wan1 drayrouter
> sys name ?
% sys name <wan1/wan2> <ASCII string (max. 20 characters)>
% sys name <wan1/wan2> clear
% Now: wan1 == drayrouter, wan2 ==
```

Note: Such name can be used to recognize router's identification in SysLog dialog.

Telnet Command: sys passwd

This command allows users to set password for the administrator.

sys passwd *[ASCII string]*

Syntax Description

Parameter	Description
ASCII string	It means the password for administrator. The maximum character that you can set is 23.

Example

```
> sys passwd admin123
>
```

Telnet Command: sys reboot

This command allows users to restart the router immediately.

Example

```
> sys reboot
>
```

Telnet Command: sys autoreboot

This command allows users to restart the router automatically within a certain time.

Syntax

sys autoreboot *[on/off/hour(s)]*

Syntax Description

Parameter	Description
on/off	On – It means to enable the function of auto-reboot. Off – It means to disable the function of auto-reboot.
hours	It means to set the time schedule for router reboot. For example, if you type "2" in this field, the router will reboot with an **interval** of two hours.

Example

```
> sys autoreboot on
 autoreboot is ON
> sys autoreboot 2
 autoreboot is ON
 autoreboot time is 2 hour(s)
```

Telnet Command: sys commit

This command allows users to save current settings to FLASH. Usually, current settings will be saved in SRAM. Yet, this command will save the file to FLASH.

Example

```
> sys commit
>
```

Telnet Command: sys tftpd

This command can turn on TFTP server for upgrading the firmware.

Example

```
> sys tftpd
% TFTP server enabled !!!
```

Telnet Command: sys version

This command can display current version for the system.

Example

```
> sys version
Router Model: Vigor2926Vn+   Version: 3.7.4.1 English
Profile version: 3.0.0   Status: 1 (0x49165e6c)
Router IP: 192.168.1.1   Netmask: 255.255.255.0
Firmware Build Date/Time: Mar 20 2014 14:09:50
Router Name: drayrouter
Revision: 40055 2860_374
VDSL2 Firmware Version: 05-04-08-00-00-06
```

Telnet Command: sys qrybuf

This command can display the system memory status and leakage list.

Example

```
> sys qrybuf
System Memory Status and Leakage List

Buf sk_buff  ( 200B), used#: 1647, cached#:   30
Buf KMC4088  (4088B), used#:    0, cached#:    8
Buf KMC2552  (2552B), used#: 1641, cached#:   42
Buf KMC1016  (1016B), used#:    7, cached#:    1
Buf KMC504   ( 504B), used#:    8, cached#:    8
Buf KMC248   ( 248B), used#:   26, cached#:   22
Buf KMC120   ( 120B), used#:   67, cached#:   61
Buf KMC56    (  56B), used#:   20, cached#:   44
Buf KMC24    (  24B), used#:   58, cached#:   70
Dynamic memory: 13107200B; 4573168B used; 190480B/0B in level 1/2
cache.

FLOWTRACK Memory Status
# of free = 12000
# of maximum = 0
# of flowstate = 12000
# of lost by siganture = 0
# of lost by list = 0
```

Telnet Command: sys pollbuf

This command can turn on or turn off polling buffer for the router.

Syntax

sys pollbuf *[on]*

sys pollbuf *[off]*

Syntax Description

Parameter	Description
on	It means to turn on pulling buffer.
off	It means to turn off pulling buffer.

Example

```
> sys pollbuf on
% Buffer polling is on!

> sys pollbuf off
% Buffer polling is off!
```

Telnet Command: sys britask

This command can improve triple play quality.

Syntax

sys britask *[on]*

sys britask *[off]*

Syntax Description

Parameter	Description
on	It means to turn on the bridge task for improving the triple play quality.
off	It means to turn off the bridge task.

Example

```
> sys britask on
% bridge task is ON, now
```

Telnet Command: sys tr069

This command can set CPE settings for applying in VigorACS.

Syntax

sys tr069 get *[parm] [option]*

sys tr069 set *[parm] [value]*

sys tr069 getnoti *[parm]*

sys tr069 setnoti *[parm] [value]*

sys tr069 log

sys tr069 debug *[on/off]*

sys tr069 save

sys tr069 inform *[event code]*

sys tr069 port *[port num]*

sys tr069 cert_auth *[on/off]*

Syntax Description

Parameter	Description
get [parm] [option]	It means to get parameters for tr-069. option=<nextlevel>: only gets nextlevel for GetParameterNames.
set [parm] [value]	It means to set parameters for tr-069.
getnoti [parm]	It means to get parameter notification value.
setnoti [parm] [value]	It means to set parameter notification value.
log	It means to display the TR-069 log.
debug [on/off]	on: turn on the function of sending debug message to syslog. off: turn off the function of sending debug message to syslog.
save	It means to save the parameters to the flash memory of the router.
Inform [event code]	It means to inform parameters for tr069 with different event codes.

	[event code] includes: 0-"0 BOOTSTRAP", 1-"1 BOOT", 2-"2 PERIODIC", 3-"3 SCHEDULED", 4-"4 VALUE CHANGE", 5-"5 KICKED", 6-"6 CONNECTION REQUEST", 7-"7 TRANSFER COMPLETE", 8-"8 DIAGNOSTICS COMPLETE", 9-"M Reboot"
port [port num]	It means to change tr069 listen port number.
cert_auth [on/off]	on: turn on certificate-based authentication. off: turn off certificate-based authentication.

Example

```
> sys tr069 get Int. nextlevel
Total number of parameter is 24
Total content length of parameter is 915
InternetGatewayDevice.LANDeviceNumberOfEntries
InternetGatewayDevice.WANDeviceNumberOfEntries
InternetGatewayDevice.DeviceInfo.
InternetGatewayDevice.ManagementServer.
InternetGatewayDevice.Time.
InternetGatewayDevice.Layer3Forwarding.
InternetGatewayDevice.LANDevice.
InternetGatewayDevice.WANDevice.
InternetGatewayDevice.Services.
InternetGatewayDevice.X_00507F_InternetAcc.
InternetGatewayDevice.X_00507F_LAN.
InternetGatewayDevice.X_00507F_NAT.
InternetGatewayDevice.X_00507F_Firewall.
InternetGatewayDevice.X_00507F_Bandwidth.
InternetGatewayDevice.X_00507F_Applications.
InternetGatewayDevice.X_00507F_VPN.
InternetGatewayDevice.X_00507F_VoIP.
InternetGatewayDevice.X_00507F_WirelessLAN.
InternetGatewayDevice.X_00507F_System.
InternetGatewayDevice.X_00507F_Status.

InternetGatewayDevice.X_00507F_Diagnostics.
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: sys sip_alg

This command can turn on/off SIP ALG (Application Layer Gateway) for traversal.

Syntax

sys sip_alg *[1]*

sys sip_alg *[0]*

Syntax Description

Parameter	Description
1	It means to turn on SIP ALG.
0	It means to turn off SIP ALG.

Example

```
> sys sip_alg ?
usage: sys sip_alg [value]
 0 - disable SIP ALG
 1 - enable SIP ALG
 current SIP ALG is disabled
```

Telnet Command: sys rtsp_alg

This command is used to configure settings (e.g., listen port) for ALG with the protocol of RTSP.

Syntax

sys rtsp_alg *[<command> <parameter>]*

Syntax Description

Parameter	Description
-e [1/0]	Enable / disable the function of RTSP ALG. 0 – Disable. 1 – Enable.
-p [value]	Set your listening port for RTSP ALG.
-u [1/0]	Enable / disable listen along UDP path. 0 – Disable. 1 – Enable.
-t [1/0]	Enable / disable listen along TCP path. 0 – Disable. 1 – Enable.
-v	Display RTP and RTSP portmap information of RTSP ALG.

Example

```
> sys rtsp_alg -e 1
 Auto enable ALG Master Switch

 Enable RTSP ALG

> sys rtsp_alg -p 375
```

```
 Current listening RTSP Port: 375

> sys rtsp_alg -v
 Current Open PortMap Number of RTSP ALG: 0
```

Telnet Command: sys license

This command can process the system license.

Syntax

sys license *licmsg*

sys license *licauth*

sys license *regser*

sys license *licera*

sys license *licifno*

sys license *lic_wiz [set/reg/qry]*

sys license *dev_chg*

sys license *dev_key*

Syntax Description

Parameter	Description
licmsg	It means to display license message.
licauth	It means the license authentication time setting.
regser	It means the license register server setting.
licera	It means to erase license setting.
licifno	It means license and signature download interface setting.
lic_wiz [set/reg/qry]	It means the license wizard setting. qry: query service support status set [idx] [trial] [service type] [sp_id] [start_date] [License Key] reg: register service in portal
dev_chg	It means to change the device key.
dev_key	It means to show device key.

Example

```
> sys license licifno

License and Signature download interface setting:
licifno [AUTO/WAN#]

Ex: licifno wan1

Download interface is "auto-selected" now.
```

Telnet Command: sys fr_log

This command is used for displaying log information related to web syslog.

Syntax

sys fr_log

Example

```
> sys fr_log ?

------------------------------------------------------------------

Note: This command shows the same log information with
Diagnostics>>Syslog Explo
rer. If you don't see any log information, go to the Web Interface and
make sure Diagnostics>>Syslog Explorer is enabled.
```

Telnet Command: sys diag_log

This command is used for RD debug.

Syntax

sys diag_log *[status| enable| disable| flush| lineno [w] | level [x] | feature [on|off] [y]| log]*

Syntax Description

Parameter	Description
status	It means to show the status of diagnostic log.
enable	It means to enable the function of diag_log.
disable	It means to disenable the function of diag_log.
flush	It means the flush log buffer.
lineno [w]	It means the total lines for displaying message. w - Available value ranges from 100 to 50000.
level[x]	It determines the level of data displayed. x – Available value ranges from 0 to 12. The larger the number is, the detailed the data is displayed.
feature [on/off][y]	It is used to specify the function of the log. Supported features include SYS and DSL (Case-Insensitive). Default setting is “on” for “DSL”.
voip_feature [on/off][vf_name]	It means VoIP feature. Type on to enable the feature or type off to disable the feature. vf_name: available settings include DRVTAPI, DRVVMMC, DRVMPS, DRVFXO, DRVHAL, PSMPHONE, PSMSUPP, PSM, FXO, PSMISDN, DTMFPSER, CALLERID (Case-Insensitive).
log	It means the dump log buffer.

Example

```
> sys diag_log status
 Status:
```

```
 diag_log is Enabled.
 lineno : 10000.
 level : 3.
 Enabled feature: SYS DSL
> sys diag_log log
0:00:02   [DSL] Current modem firmware: AnnexA_548006_544401
0:00:02   [DSL] Modem firmware feature: 5, ADSL_A, VDSL2
0:00:02   [DSL] xtseCfg=04 00 04 00 0c 01 00 07
0:00:02   [DSL] don't have last showtime mode!! set next mode to VDSL!!
0:00:02   [DSL] Status has changed: Stopped(0) -> FwWait(3)
0:00:02   [DSL] Status has changed: FwWait(3) -> Starting(1)
0:00:02   [DSL] Status has changed: Starting(1) -> Running(2)
0:00:02   [DSL] Status was switched: firmwareReady(3) to Init(5)
0:00:02   [DSL] Status was switched: Init(5) to Restart(10)
0:00:02   [DSL] Status was switched: Restart(10) to
FirmwareRequest(1)
0:00:02   [DSL] Line state has changed: 00000000 -> 000000FF
0:00:02   [DSL] Entering VDSL2 mode
0:00:03   [DSL] modem code: [05-04-08-00-00-06]
0:00:05   [DSL] Status was switched: FirmwareRequest(1) to
firmwareReady(3)
0:00:05   [DSL] Status was switched: firmwareReady(3) to Init(5)
0:00:05   [DSL] >> nXtseA=0d, nXtseB=00, nXtseV=07, nFwFeatures=5
0:00:05   [DSL] >> nHsToneGroupMode=0, nHsToneGroup=106,
nToneSet=43, nCamState
=2
0:00:05   [DSL] Line state has changed: 000000FF -> 00000100
0:00:05   [DSL] Line state has changed: 00000100 -> 00000200
0:00:05   [DSL] Status was switched: Init(5) to Train(6)
```

Telnet Command: sys arp_AutoReq

This command is used to enable / disable the function that Vigor router sends ARP request to the connected device(s) periodically.

Syntax

sys arp_AutoReq -d *[value]*

Syntax Description

Parameter	Description
-d [value]	Disable the function of ARP auto request. 0 – Enable 1 – Disable

Example

```
> sys arp_AutoReq -d 0
  Arp auto-request enable.
```

Telnet Command: sys daylightsave

This command is used to configure daylight save setting.

Syntax

sys daylightsave *[-<command> <parameter> | …]*

Syntax Description

Parameter	Description
[<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-v	Display the daylight saving settings.
-r	回復出廠預設值(Set to Factory Default) setting.
-e [1/0]	Enable (1) / disable (0) daylight saving.
-t [0/1/2]	Specify the saving type for daylight setting. 0 – Default 1 – Time range 2 - Yearly
-s <year> <month> <day> <hour>	Set the detailed settings of the starting day for time range type. year – must be the year after 2013. month - 1 ~ 12 day – 1 ~ 31 hour – 0 ~ 23 e.g., sys daylightsave -s 2014 3 10 12
-d <year> <month> <day> <hour>	Set the detailed settings of the ending day for time range type. year – After 2013. month - 1 ~ 12 day – 1 ~ 31 hour – 0 ~ 23 e.g., sys daylightsave -d 2014 9 10 12
-y <month> <th weekday> <day in week> <hour>	Set the detailed settings of the starting day for yearly type. month - 1 ~ 12 th weekday – 1 ~ 5, 9: last week day in week - 0:Sun, 1:Mon, 2:Tue, 3:Wed, 4:Thu, 5: Fri, 6:Sat hour – 0 ~ 23 e.g, sys daylightsave -y 9 1 0 14
-z <month> <th weekday> <day in week> <hour>	Set the detailed settings of the ending day for yearly type. month - 1 ~ 12 th weekday – 1 ~ 5, 9: last week day in week - 0:Sun, 1:Mon, 2:Tue, 3:Wed, 4:Thu, 5: Fri, 6:Sat hour – 0 ~ 23 e.g, sys daylightsave -z 3 1 6 14

Example

```
> sys daylightsave -y 9 1 0 14
% Start: Yearly on Sep 1th Sun 14:00
```

Telnet Command: sys dnsCacheTbl

This command is used to configure TTL settings which will be displayed in DNS Cache table.

Syntax

sys dnsCacheTbl *[<command><parameter>|…]*

Syntax Description

Parameter	Description
[<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-l	Display DNS IPv4 entry in the DNS cache table.
-s	Display DNS IPv6 entry in the DNS cache table.
-v	Display the TTL limit value in the DNS cache table.
-t < 0/n >	Set the TTL limit value in the DNS cache table. 0- No limit N – Greater than or equal to 5.
-c	Clear the DNS cache table.

Example

```
> sys dnsCacheTbl -l
%DNS Cache Table List
> sys dnsCacheTbl -t 65
% Set TTL limit: 65 seconds.
% When TTL larger than 65s , delete the DNS entry in the router's DNS cache
tabl
e.
>
```

Telnet Command: sys syslog

This command is used to configure

Syntax

sys syslog *-a <enable> [-<command> <parameter> | …]*

Syntax Description

Parameter	Description
[<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-a <1/0>	Enable (1) or disable (0) Syslog Access Setup.
-s <1/0>	Enable (1) or disable (0) Syslog Save to Syslog Server.
-i <IP address>	Define the IP address of the Syslog server.
-d <port number>	Define the port number (1 ~ 65535) as the destination port.
-u <1/0>	Enable (1) or disable (0) Syslog Save to USB Disk.
-m <1/0>	Enable (1) or disable (0) Mail Syslog.
-f <1/0>	Enable (1) or disable (0) Filewall Log.
-v <1/0>	Enable (1) or disable (0) VPN Log.

-e <1/0>	Enable (1) or disable (0) User Access Log.
-c <1/0>	Enable (1) or disable (0) Call Log.
-w <1/0>	Enable (1) or disable (0) WAN Log.
-r <1/0>	Enable (1) or disable (0) Router/DSL Information.
-t <1/0>	Enable (1) or disable (0) AlertLog Setup.
-o <port number>	Define the port number (1 ~ 65535) for AlertLog.

Example

```
> sys syslog -a 1 -s 1 -i 192.168.1.25 -d 514
>
```

Telnet Command: sys mailalert

This command is used to configure settings for syslog mail alert.

Syntax

sys mailalert *[-<command> <parameter>]*

Syntax Description

Parameter	Description
[<command><parameter>]	The available commands with parameters are listed below.
-e [0/1]	Enable/disable Mail Alert. 0 – Disable. 1 – Enable.
-i [SMTP Server IP]	Set IP Address for SMTP server.
-o [SMTP Server Port]	Set port number for SMTP server..
-a [Mail Address]	Set E-maiil address for alert mail reciver.
-r [Mail Address]	Set E-mail Address for mail return.
-s [0/1]	Enable/disable the function of Use SSL. 0 – Disable. 1 – Enable.
-h [0/1]	Enable/disable SMTP Authentication. 0 – Disable. 1 – Enable.
-u [Username]	Set username for SMTP Authentication.
-p [Password]	Set password for SMTP Authentication.
-l [type][0/1]	Enable / disable mail alert for different types. Number 0 ~ 6 represent different types. "0 <0/1>" : Enable/Disable Mail Alert of the DoS Attack. "1 <0/1>" : Enable/Disable Mail Alert of the APPE. "2 <0/1>" : nable/Disable Mail Alert of the VPN Log. "3 <0/1>" : Enable/Disable Mail Alert of the APPE Signature. "6 <0/1>" : Enable/Disable Mail Alert of the Reboot Debug Log. In which, 0 – Disable. 1 – Enable.
-f	Reset Mail Alert setting to factory default.
-v	Show current Mail Alert setting.
-R [0/1]	Set Mail Alert Reboot debug log mode. 0: Limited Mode 1: Unlimited Mode.

Example

```
> sys mailalert -e 1
Set Enable Mail Alert.
> sys mailalert -v
------ Current setting for Mail Alert ------
Mail Alert: Enable
SMTP Server IP Address: 0.0.0.0
SMTP Server Port: 25
Alert Mail Reciver E-maiil Address:
Mail Return E-mail Address:
Use SSL: Disable
SMTP Authentication: Disable
Username for SMTP Authentication:
Password for SMTP Authentication:
Mail Alert for DoS Attack: Enable.
Mail Alert for APPE: Enable.
Mail Alert for VPN Log: Enable.
Mail Alert for APPE Signature: Disable.
Mail Alert for Reboot Debug Log: Disable, Mode: Limited.
-------------------------------------------
```

Telnet Command: sys time

This command is used to configure system time and date.

Syntax

sys time server *[domain]*

sys time inquire

sys time show

sys time zone [index]

Syntax Description

Parameter	Description
domain	Type the domain name of the time server. The maximum length is 39 characters.
index	Different number means different time zone. 1 - GMT-12:00 Eniwetok, Kwajalein 2 - GMT-11:00 Midway Island, Samoa 3 - GMT-10:00 Hawaii 4 - GMT-09:00 Alaska 5 - GMT-08:00 Pacific Time (US & Canada) 6 - GMT-08:00 Tijuana 7 - GMT-07:00 Mountain Time (US & Canada) 8 - GMT-07:00 Arizona 9 - GMT-06:00 Central Time (US & Canada) 10 - GMT-06:00 Saskatchewan 11 - GMT-06:00 Mexico City, Tegucigalpa 12 - GMT-05:00 Eastern Time (US & Canada) 13 - GMT-05:00 Indiana (East) 14 - GMT-05:00 Bogota, Lima, Quito 15 - GMT-04:00 Atlantic Time (Canada) 16 - GMT-04:00 Caracas, La Paz 17 - GMT-04:00 Santiago 18 - GMT-03:30 Newfoundland 19 - GMT-03:00 Brasilia 20 - GMT-03:00 Buenos Aires, Georgetown 21 - GMT-02:00 Mid-Atlantic

	22 - GMT-01:00 Azores, Cape Verde Is. 23 - GMT Greenwich Mean Time : Dublin 24 - GMT Edinburgh, Lisbon, London 25 - GMT Casablanca, Monrovia 26 - GMT+01:00 Belgrade, Bratislava 27 - GMT+01:00 Budapest, Ljubljana, Prague 28 - GMT+01:00 Sarajevo, Skopje, Sofija 29 - GMT+01:00 Warsaw, Zagreb 30 - GMT+01:00 Brussels, Copenhagen 31 - GMT+01:00 Madrid, Paris, Vilnius 32 - GMT+01:00 Amsterdam, Berlin, Bern 33 - GMT+01:00 Rome, Stockholm, Vienna 34 - GMT+02:00 Bucharest 35 - GMT+02:00 Cairo 36 - GMT+02:00 Helsinki, Riga, Tallinn 37 - GMT+02:00 Athens, Istanbul, Minsk 38 - GMT+02:00 Jerusalem 39 - GMT+02:00 Harare, Pretoria 40 - GMT+03:00 Volgograd 41 - GMT+03:00 Baghdad, Kuwait, Riyadh 42 - GMT+03:00 Nairobi 43 - GMT+03:00 Moscow, St. Petersburg 44 - GMT+03:30 Tehran 45 - GMT+04:00 Abu Dhabi, Muscat 46 - GMT+04:00 Baku, Tbilisi 47 - GMT+04:30 Kabul 48 - GMT+05:00 Ekaterinburg 49 - GMT+05:00 Islamabad, Karachi, Tashkent 50 - GMT+05:30 Bombay, Calcutta 51 - GMT+05:30 Madras, New 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 Singapore 58 - GMT+08:00 Taipei 59 - GMT+08:00 Perth 60 - GMT+09:00 Seoul 61 - GMT+09:00 Osaka, Sapporo, Tokyo 62 - GMT+09:00 Yakutsk 63 - GMT+09:30 Darwin 64 - GMT+09:30 Adelaide 65 - GMT+10:00 Canberra, Melbourne, Sydney 66 - GMT+10:00 Brisbane 67 - GMT+10:00 Hobart 68 - GMT+10:00 Vladivostok 69 - GMT+10:00 Guam, Port Moresby 70 - GMT+11:00 Magadan, Solomon Is. 71 - GMT+11:00 New Caledonia 72 - GMT+12:00 Fiji, Kamchatka, Marshall Is. 73 - GMT+12:00 Auckland, Wellington

Example

```
> sys time zone 8
  Set Time Zone OK

> sys time show
  ***************  System Time  ***************
  Current System Time: [2000 Jan 01 Sat 02:09:29]
  Time Server: [pool.ntp.org]
  Time Zone Index: [8]. GMT-07:00
  ******************************************
```

Telnet Command: sys eap_tls

This command is used to disable or enable EAP-TLS.

You might have to enable EAP-TLS compatibility to avoid compatibility issues with some operating systems. But, please note that enabling EAP-TLS compatibility will lower down the connection security level.

Syntax

sys eap_tls set *[0/1]*

Syntax Description

Parameter	Description
0	Disable EAP-TLS compatibility!
1	Enable EAP-TLS compatibility!

Example

```
> sys eap_tls set 1
Enable EAP_TLS compatibility!
```

Telnet Command: sys dashboard

This command is used to display / hide items (such as System Information, Interface…) on dashboard.

Syntax

sys dashboard *[-<command> <value> | …]*

sys dashboard show

Syntax Description

Parameter	Description
[<command> <value>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several parameters in one line. <command> "0 ~ 9" and "a" represent different sections to be displayed on the dashboard. 0 : Front Panel 1 : System Information 2 : IPv4 LAN Information 3 : IPv4 Internet Access 4 : IPv6 Internet Access 5 : Interface 6 : Security 7 : System Resource 8 : LTE Status 9 : Quick Access a : VoIP <value> 1 : Enable 0 : Disable
show	Display current status (enabled /disabled) for each item.

Example

```
> sys dashboard -0 1
  Front Panel enabled
> sys dashboard show
  Front Panel enabled
  System Information enabled
  IPv4 LAN Information enabled
  IPv4 Internet Access enabled
  IPv6 Internet Access enabled
  Interface enabled
  Security enabled
  System Resource enabled
  LTE Status enabled
  Quick Access enabled
  VoIP enabled
```

Telnet Command: testmail

This command is used to display current settings for sending test mail.

Example

```
> testmail
Send out test mail
 Mail Alert:[Disable]
 SMTP_Server:[0.0.0.0]
 Mail to:[]
 Return-Path:[]
```

Telnet Command: upnp off

This command can close UPnP function.

Example

```
>upnp off
UPNP say bye-bye
```

Telnet Command: upnp on

This command can enable UPnP function.

Example

```
>upnp on
UPNP start.
```

Telnet Command: upnp nat

This command can display IGD NAT status.

Example

```
> upnp nat ?
******************  IGD NAT Status  ****************
```

```
((0))
InternalClient >>192.168.1.10<<, RemoteHost >>0.0.0.0<<
InternalPort >>21<<, ExternalPort >>21<<
PortMapProtocol >>TCP<<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
Ftp Example [MICROSOFT]
((1))
InternalClient >>0.0.0.0<<, RemoteHost >>0.0.0.0<<
InternalPort >>0<<, ExternalPort >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
0<<

--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

Telnet Command: upnp service

This command can display the information of the UPnP service. UPnP service must be enabled first.

Example

```
> upnp on
UPNP start.

> upnp service
>>>>> SERVICE TABLE1 <<<<<
  serviceType urn:schemas-microsoft-com:service:OSInfo:1
  serviceId   urn:microsoft-com:serviceId:OSInfo1
  SCPDURL    /upnp/OSInfo.xml
  controlURL  /OSInfo1
  eventURL    /OSInfoEvent1
  UDN        uuid:774e9bbe-7386-4128-b627-001daa843464

>>>>> SERVICE TABLE2 <<<<<
  serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
  serviceId   urn:upnp-org:serviceId:WANCommonIFC1
  SCPDURL    /upnp/WComIFCX.xml
  controlURL  /upnp?control=WANCommonIFC1
  eventURL    /upnp?event=WANCommonIFC1
  UDN        uuid:2608d902-03e2-46a5-9968-4a54ca499148
.
.
.
```

Telnet Command: upnp subscribe

This command can show all UPnP services subscribed.

Example

```
> upnp on
UPNP start.
> upnp subscribe
Vigor> upnp subscribe
>>>> (1) serviceType urn:schemas-microsoft-com:service:OSInfo:1

  ----- Subscribtion1 -------

    sid = 7a2bbdd0-0047-4fc8-b870-4597b34da7fb

    eventKey =1, ToSendEventKey = 1

    expireTime =6926

    active =1

    DeliveryURLs
=<http://192.168.1.113:2869/upnp/eventing/twtnpnsiun>

>>>> (2) serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1

  ----- Subscribtion1 -------

    sid = d9cd47a5-d9c9-4d3d-8043-d03a82f27983

    eventKey =1, ToSendEventKey = 1
.
.
.
```

Telnet Command: upnp tmpvs

This command can display current status of temp Virtual Server of your router.

Example

```
Vigor> upnp tmpvs
******************  Temp virtual server status  ****************

((0))
real_addr  >>192.168.1.10<<, pseudo_addr >>172.16.3.229<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>TCP<<
time >>0<<

((1))
```

```
real_addr  >>0.0.0.0<<, pseudo_addr >>0.0.0.0<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>0<<
time >>0<<
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: upnp wan

This command is used to specify WAN interface to apply UPnP.

Syntax

upnp wan *[n]*

Syntax Description

Parameter	Description
n	It means to specify WAN interface to apply UPnP. n=0, it means to auto-select WAN interface. n=1, WAN1 n=2, WAN2 …….

Example

```
> upnp wan 1
use wan1 now.
```

Telnet Command: usb list

This command is use to display the information about the brand name and model name of the USB modems which are supported by Vigor router.

Example

```
> usb list ?
Brand      Module             Standard
-----------------------        --------
Aiko       Aiko 83D            3.5G                Y
BandRich    Bandluxe C170        3.5G                Y
BandRich    Bandluxe C270        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
Huawei     Huawei E169u         3.5G                Y
Huawei     Huawei E220          3.5G                Y
Huawei     Huawei E303D         3.5G                Y
Huawei     Huawei E392          3.5G                Y
Huawei     Huawei E398          3.5G                Y
Sony Erics  Sony Ericsson MD30     3.5G                Y
TP-LINK    TP-LINK MA180         3.5G                Y
TP-LINK    TP-LINK MA260         3.5G                Y
Vodafone    Vodafone K3765-Z      3.5G                Y
```

```
Vodafone    Vodafone K4605         3.5G                 Y
ZTE         ZTE MF626             3.5G                 Y
ZTE         ZTE MF627 plus         3.5G                 Y
ZTE         ZTE MF633             3.5G                 Y
ZTE         ZTE MF636             3.5G                 Y

SpinCom     SpinCom GPRS Modem     3.5G                 Y
- MORE - ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] -
```

Telnet Command: usb user

This command is used to set profiles for FTP/SMB users.

Syntax Description

usb user add *[Index] [Username] [Password] [Permission] [Home path]*

usb user rm *[Index]*

usb user enable *[Index]*

usb user disable *[Index]*

usb user list

Syntax Description

Parameter	Description
add	Add a new user profile.
Rm	Delete an existed user profile.
enable	Enable a user profile.
disable	Disable a user profile.
list	Display all of the user profile.
index	It means the index number of the user profile. There are 16 profiles allowed to be configured. So the range of such option is 1 ~ 16.
Username	Type a text (maximum 11 characters) as the username for the user profile.
Password	Type a text (maximum 11 characters) as the password for the user profile.
Permission	Specify the action (RWDLCR) permitted. If one of the actions is not allowed, simple type "-" instead. R – Read File. W – Write File. D – Delete File. L – List directory. C – Create directory. R – Remove selected directory.
Home path	Set the path (maximum 159 characters) for the USB user profile.

Example

```
> usb user add 1 root 1234 R-DLCR /usr
```

Telnet Command: vigbrg set

This command is to configure specified WAN as bridge mode.

Syntax Description

vigbrg set *-v [IP version] -w [WAN_idx] -l [LAN_idx] -e [0/1] -f [0/1]*

Syntax Description

Parameter	Description
-v [IP version]	Indicate the IP version for the IP address. 4 – IPv4. 6 – IPv6.
-w [WAN_idx]	WAN_idx – Indicate the WAN interface. 1 – WAN1 2 – WAN2 3 – WAN3 4 – WAN4
-l [LAN_idx]	LAN_idx – Indicate the LAN interface. 1 – LAN1 2 – LAN2 3 – LAN3 4 – LAN4
e [0/1]	Enable (1) or disable (0) the Vigor Bridge for WAN or/and LAN.
f [0/1]	Enable (1) or disable (0) the firewall functions.

Example

```
> vigbrg set -v 4 -w 1 -l 1 -e 1
[WAN1] IPv4 bridge is enable. Set subnet[LAN1]
```

Telnet Command: vigbrg status

This command can show whether the Vigor Bridge Function is enabled or disabled.

Example

```
> vigbrg status
%Vigor Bridge Function is enable!

%Wan1 management is disable!
```

Telnet Command: vigbrg cfgip

This command allows users to transfer a bridge modem into ADSL router by accessing into and adjusting specified IP address. Users can access into Web UI of the router to manage the router through the IP address configured here.

Syntax

vigbrg cfgip *[IP Address]*

Syntax Description

Parameter	Description
IP Address	It means to type an IP address for users to manage the router.

Example

```
> vigbrg cfgip 192.168.1.15
> vigbrg cfgip ?
% Vigor Bridge Config IP,
% Now: 192.168.1.15
```

Telnet Command: vigbrg wanstatus

This command can display the existed WAN connection status for the modem (change from ADSL router into bridge modem), including index number, MAC address, Stamp Time, PVC, VLAN port for Vigor Bridge Function..

Example

```
> vigbrg wanstatus
Vigor Bridge: Running
WAN mac table:
Index  MAC Address          Stamp Time      PVC         VLan
    Port
```

Telnet Command: vigbrg wlanstatus

This command can display the existed WLAN connection status for the modem (change from router into bridge modem), including index number, MAC address, Stamp Time, PVC, VLAN port for Vigor Bridge Function.

Example

```
> vigbrg wlanstatus
Vigor Bridge: Running
WAN mac table:
Index  MAC Address          Stamp Time      PVC     VLan    Port
```

Telnet Command: vlan group

This command allows you to set VLAN group. You can set four VLAN groups. Please run *`vlan restart`* command after you change any settings.

Syntax

vlan group *id [set/set_ex] [p1/p2/p3/p4/s1/s2/s3/s4*

Syntax Description

Parameter	Description
id	It means the group 0 to 7 for VLAN.
set	It indicates each port can join more than one VLAN group.
set_ex	It indicates each port can join one VLAN group at one time.
p1/p2/p3/p4	It indicates LAN port 1 to LAN port 4. To group LAN1, LAN2, LAN3 and/or LAN4 under one VLAN group, please type the port number(s) you want.
s1/s2/s3/s4	It is only available for WALN models.

Example

```
> vlan group 3 set p1 s3 s4
 VLAN   p1   p2   p3   p4   s1   s2   s3   s4
 ---------------------------------------------
   3    V                         V    V
>
```

Telnet Command: vlan off

This command allows you to disable VLAN function.

Syntax

vlan off

Example

```
> vlan off
 VLAN is Disable!
 Force subnet LAN2/3/4 to be disabled!!
```

Telnet Command: vlan on

This command allows you to enable VLAN function.

Syntax

vlan on

Example

```
> vlan on
 VLAN is Enable!
```

Telnet Command: vlan pri

This command is used to define the priority for each VLAN profile setting.

Syntax

vlan pri *n pri_no*

Syntax Description

Parameter	Description
n	It means VLAN ID number. n=VLAN ID number (from 0 to 7).

pri_no	It means the priority of VLAN profile. pri_no=0 ~7 (from none to highest priority).

Example

```
> vlan pri 1 2
 VLAN1: Priority=2
```

Telnet Command: vlan restart

This command can make VLAN settings restarted with newest configuration.

Syntax

vlan restart

Example

```
> vlan restart ?
 VLAN restarts!!!
```

Telnet Command: vlan status

This command display current status for VLAN.

Syntax

vlan status

Example

```
> vlan status
VLAN  is Enable :
-----------------------------------------------------
VLAN Enable VID  Pri   p1 p2 p3 p4 s1 s2 s3 s4  subnet
-----------------------------------------------------
 0    OFF    0   0                          1:LAN1
 1    OFF    0   2                          1:LAN1
 2    OFF    0   0                          1:LAN1
 3    OFF    0   0   V              V  V   1:LAN1
 4    OFF    0   0                          1:LAN1
 5    OFF    0   0                          1:LAN1
 6    OFF    0   0                          1:LAN1
 7    OFF    0   0                          1:LAN1
-----------------------------------------------------
 Note: they are only untag for s1/s2/s3/s4, but they can join tag vlan
with lan
ports.
 Permit untagged device in P1 to access router: ON.
```

Telnet Command: vlan subnet

This command is used to configure the LAN interface used by the VLAN group.

Syntax

vlan subnet group_id *[1/2/3/4/5/6]*

Syntax Description

Parameter	Description
[1/2/3/4/5/6]	It means interfaces, LAN1 ~ LAN4.

Example

```
> vlan subnet group_id 2
% Vlan Group-0 using LAN2      !

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: vlan submode

This command changes the VLAN encapsulation mechanisms in the LAN driver.

Syntax

vlan submode *[on|off|status]*

Syntax Description

Parameter	Description
on	It means to enable the promiscuous mode.
off	It means to enable the normal mode.
status	It means to display if submode is normal mode or promiscuous mode.

Example

```
> vlan submode status
% vlan subnet mode : normal mode
> vlan submode on
% vlan subnet mode modified to promiscuous mode.
> vlan submode status
% vlan subnet mode : promiscuous mode
```

Telnet Command: vlan tagged

This command is used to enable or disable the incoming of untagged packets.

Syntax

vlan tagged *[n] [on/off]*

vlan tagged *[unlimited] [on/off]*

vlan tagged *[p1_untag] [on/off]*

Syntax Description

Parameter	Description
n	It means VLAN channel. The ranage is from 0 to 7.
on/off	It means to enable/disable the tagged VLAN.
[unlimited] [on/off]	unlimited on: It allows the incoming of untagged packets even all VLAN are tagged. unlimited off: It does not allows the incoming of untagged packets.

[p1_untag] [on/off]	P1_untag on: It allows the incoming of untagged packets form LAN port 1. P1_untag off: It does not allow the incoming of untagged packets from LAN port 1.

Example

```
> vlan tagged unlimited on
 unlimited mode is ON
```

Telnet Command: vlan vid

This command is used to configure VID number for each VLAN channel.

Syntax

vlan vid *n vid_no*

Syntax Description

Parameter	Description
n	It means VLAN channel. The ranage is from 0 to 7.
vid_no	It means the value of VLAN ID. Type the value as the VLAN ID number. The range is form 0 to 4095.

Example

```
> vlan vid 1 4095
 VLAN1, vid=4095
```

Telnet Command: vlan sysvid

This command is used to modify and show the scope (reserved 78) of the VLAN IDs used internally by the system.

Syntax

vlan sysvid *[show | n]*

Syntax Description

Parameter	Description
show	It means to show the scope of VLAN ID used internally.
n	It means the value to be set as VLAN ID. The range is from 0 to 4018.

Example

```
> vlan sysvid 100
 You have set system VLAN ID to range: 100 ~ 177,
 We recommend that you reboot the system now.

> vlan sysvid 200
 You have set system VLAN ID to range: 200 ~ 263,
 We recommend that you reboot the system now.
> vlan sysvid show
 The system VLAN ID is in range: 200 ~ 263
```

Telnet Command: voip debug

This command can display debug message on the screen.

Syntax

voip debug *[flush]*

voip debug *[showmsg]*

Syntax Description

Parameter	Description
flush	It means to clear current log.
showmsg	It means to show current log.

Example

```
> voip debug showmsg
-->Send Message to 192.168.1.2:5060 <02:35:16>
INVITE sip:192.168.1.2 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.1:5060;branch=z9hG4bK-YMa-3630;rport
From:  <sip:change_me@192.168.1.1>;tag=WLJ-11782
To: <sip:192.168.1.2>
Call-ID: PbU-25312@192.168.1.1
CSeq: 1 INVITE
Contact: <sip:change_me@192.168.1.1>
Max-Forwards: 70
supported: 100rel, replaces
User-Agent: DrayTek UA-1.2.3 DrayTek Vigor2910
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, INFO, REFER, NOTIFY, PRACK
Content-Type: application/sdp
Content-Length:   264

v=0
o=change_me 5972727 56415 IN IP4 192.168.1.1
```

Telnet Command: voip dialplan

This command allows users to set phone book settings.

Syntax

voip dialplan block *n [-<command><parameter>]*

voip dialplan phonebook *n [-<command><parameter>]*

voip dialplan region *[-<command><parameter>]*

voip dialplan local *[1/0]*

Syntax Description

Parameter	Description
voip dialplan block	
n	It means the index number of the VoIP settings. n=1 ~ 20
-<command><parameter>	The available commands with parameters are listed below.
-m 0/1	It means to enable or disable the block mode.

	0 – Disable 1 - Enable
-p <path>	Determines the block path. 1:in_url, 2:in_number 3:out_url, 4:out_number 5:(in & out)_url, 6:(in & out)_number))
-n <number>	Determines the block number (maximum 29 characters).
-d <domain>	Block the specified domain.
-i <inf>	Block the specified interface(s) or All interfaces.
-s <Schedule>	Specify schedule profiles by indicating the index number of the schedule profile. Four schedule profiles can be used at one time.
-w	Delete the selected entry. N=null (clear all)
-v	List current settings.
voip dialplan phonebook	
n	It means the index number of the VoIP settings. n=1 ~ 60
-<command><parameter>	The available commands with parameters are listed below.
-d <number>	Specify the speed dial number.
-c <url>	Contact SIP URL l(max. 59 characters)
-n <name>	Contact name (max. 23 characters)
-a <enable>	Enable/disable the specify entry.
-m <mode>	Specify backup number mode. 0 – none 2 - PSTN
-b <number>	Spedify the backup number.
-o <acc num>	Specify the dial out account. 0 – default 1 - acc1, 2 - acc2... ~ 12:=acc12
-z <enable>	Enable/disable ZRTP/SRTP VoIP security. 1 – enable 0 - disable
-l	Delete the specify entry.
-V	List current VoIP settings.
voip dialplan region	
-e	Dnable or disable the regional function. 1 – enable 0 - disable
-m <number>	Return the last miss call.
-l <number>	Return the last incoming call.
-o <number>	Return the last outgoing call.
-F <number>	Hotkey to enable call forwarding (all) function.
-f <number>	Hotkey to enable call forwarding (busy) function.

-C <number>	Hotkey to enable call forwarding (no answer) function.
-c <number>	Hotkey to disable call forwarding function.
-W <number>	Hotkey to enable call waiting function.
-w <number>	Hotkey to disable call waiting function.
-H <number>	Hotkey to enable hide caller ID function.
-h <number>	Hotkey to disable hide caller ID function.
-D <number>	Hotkey to enable DND function.
-d <number>	Hotkey to disable DND function.
-A <number>	Hotkey to enable block anonymous calls function.
-a <number>	Hotkey to disable block anonymous calls function.
-U <number>	Hotkey to enable block unknow domain calls function.
-u <number>	Hotkey to disable block unknow domain calls function.
-P <number>	Hotkey to disable block IP calls function.
-p <number>	Hotkey to disable block IP calls function.
-I <number>	Hotkey to block last incoming call.
-v	List current status for Regional settings.
voip dialplan local	
enable/disable	Enable or disable the local calls. 1 – enable 0 - disable

Example

```
> voip dialplan phonebook 1 -d 1125
> voip dialplan region -l 8
> voip dialplan region -v
 Your Setting for Regional
 Regional Function is: Enable
 Return the Last Miss Call: 20
 Return the Last Incoming Call: *12
 Return the Last Outgoing Call: 1
 Hotkey to enable call forwarding (all) function: 0
 Hotkey to enable call forwarding (busy) function: *90
 Hotkey to enable call forwarding (no answer) function: *92
 Hotkey to disable call forwarding function: 12
 Hotkey to Enable Call Waiting Function: *56
 Hotkey to Disable Call Waiting Function: *57
 Hotkey to Enable Hide Caller ID Function: *67
 Hotkey to Disable Hide Caller ID Function: *68
 Hotkey to Enable DND Function: *78
 Hotkey to Disable DND Function: *79
 Hotkey to Enable Block Anonymous Calls Function: *77
 Hotkey to Disable Block Anonymous Calls Function: *87
 Hotkey to Enable Block Unknow Domain Calls Function: *40
 Hotkey to Disable Block Unknow Domain Calls Function: *04
 Hotkey to Enable Block IP Calls Function: *50
 Hotkey to Disable Block IP Calls Function: *05
 Hotkey to Disable Block The Last Incoming Call Function: 8
```

Telnet Command: voip dsp

Syntax

voip dsp countrytone *[channel] [value]*

voip dsp dialtonepwr *[channel] [AbsoluteValue]*

voip dsp EchoCanceller *[type] [w_size] [nlp]*

voip dsp cidtype *[channel] [value]*

voip dsp micgain *[channel] [value/(1~10)]*

voip dsp spkgain *[channel] [value/(1~10)]*

voip dsp jitterBuffer *[port] [mode] [value]*

voip dsp dtmfDetset *[nLevel] [nTwist]*

voip dsp dtmftonepwr *[Level]*

voip dsp cwtonepwr *[ch] [value]*

voip dsp pstnringfxs *[1|2] [on|off]*

voip dsp relaydbounce *[on|off]*

voip dsp setRingPat *[ring_pattern_index] [patten_num]*

voip dsp setDtmfCidlevel –l [value]

voip dsp setDtmfCidlevel –h [value]

voip dsp setDtmfCidlevel –r 0

voip dsp cidplusdigit [1/0] [channel] [value]

Syntax Description

Parameter	Description
voip dsp countrytone	
[channel] [value]	This command allows users to set the region for the tone settings. Different regions usually need different tone settings. Channel – 1 or 2. Value – displayed as follows: [2] UK, [3] USA, [4] Denmark, [5] Italy, [6] Germany, [7] Netherlands, [8] Portugal, [9] Sweden, [10] Australia, [11] Slovenia, [12] Czech, [13] Slovakia, [14] Hungary, [15] Switzerland , [16] France , [17] Malta
voip dsp dialtonepwr	
channel	This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting. Channel - Available channel number: 1 – 2
AbsoluteValue	AbsoluteValue - In -1 dB increments, with 1 corresponding to 6 dBm. Range - 1 to 30
voip dsp EchoCanceler	
type	This command is used to set the type of echo reduction. 0 - Disable the LEC processing. 1 - Cancel using the fixed window. 2 - Cancel using the fixed and moving window. 3 - Cancel using fixed window + Echo Suppressor.

w_size	The Line Echo Canceller (LEC) window size is 4, 6, 8 or 16 (ms).
nlp	Nlp - Non-linear processing (NLP) for more smooth transitions. 1 - disable 0 - enable
voip dsp cidtype	
channel	Set the caller ID type for FXS 1 (Channel 1) or FXS 2 (Channel 2). 1 – FXS 1 2 – FXS 2
value	Each number (1 to 6) represents different type. 1 – FSK_ETSI 2 - FSK_ETSI(UK) 3 - FSK_BELLCORE(US/AU) 4 - DTMF 5 - DTMF(Dk) 6 - DTMF(SE,NL,FIN) For example : Vigor> voip dsp cidtype 2 6 channel=2, current cidType: 6 That means the caller ID type for FXS2 (Channel2) is DTMF (SE, NL, FIN).
voip dsp micgain	
channel	Adjust the volume of microphone by entering number from 1- 10 for FXS 1 or FXS 2. 1 – FXS 1 2 – FXS 2
value/(1~10)	The larger the number is, the louder the volume will be.
voip dsp spkgain	
channel	Adjust the volume of speaker by entering number from 1- 10 for FXS 1 or FXS 2. 1 – FXS 1 2 – FXS 2
value/(1~10)	The larger the number is, the louder the volume will be.
voip dsp jb	
port	Set the size of jitter buffer. Available settings are 0 (FXS1) and 1 (FXS2).
mode	Available settings are **Fixed** and **Adaptive** (default setting).
value	Available settings are 1 ~ 180 (unit: msec). e.g., Vigor> voip dsp jb 1 FIXED 100
voip dsp timer	
[Timer]	Set the waiting time for dialing out. It means to set the timer settings. The unit is mini-second. The range is from 1 to 255. Value “1” is corresponding to 500ms. That is to say, Value “6” is corresponding 3000ms (i.e., 3 seconds) Timer: 1 ~ 20. Vigor> voip dsp timer 20 Set the timer:20
Voip dsp debugMsg	
?	Avaible settings include:

	clrev - clear phone hook status. getev - get phone hook status. clrfskcid - clear fsk data for caller-ID from PSTN line. getfskcid - get fsk data for caller-ID from PSTN line. clrdtmfcid - clear dtmf data for caller-ID from PSTN line. getdtmfcid - get dtmf data for caller-ID from PSTN line. voicebuf - get message for available voice buffer pool. clrint - clear status for interrupt. getint - get status for interrupt. Vigor> voip dsp debugMsg getint the interrupt status for ad0 = 21 the interrupt status for ad1 = 0 the interrupt status for vc = 0
voip dsp dtmfDetset	
nLevel	Set minimal signal level in dB, for DTMF detection. Range – (-96 ~ -1)
nTwist	Maximum allowed signal twist in dB, for DTMF detection. Range – (0 ~ 12)
voip dsp dtmftonepwr	
Level	Set power level for DTMF frequency. Level – 0 ~ 100. Power level for dtmf frequency in 0.3 dB steps. 0 map to 0dB 1 map to -0.3dB .... 100 map to -30dB
voip dsp cwtonepwr	
ch	Set the call waiting tone power level. 1 – FXS 1 2 – FXS 2.
value	1 ~ 30, in -1 dB increments, with 1 corresponding to 8 dBm.
voip dsp pstnringfxs	
1|2	Enable or disable PSTN ring on FXS 1/FXS 2. 1 meansFXS1; 2 means FXS2.
on|off	On means enable; off means disable.
voip dsp relaydbounce	
on|off	on: Enable relay filter noise. But it maybe ignore the caller-id!!! off: Disable relay filter noise. But the noise will cause the relay to switch to PSTN!!!
voip dsp setRingPat	
ring_pattern_index	This command can change the ring pattern at Index(2)~Index(6). ring_pattern_index – Index (1) was locked for your country.
patten_num	It's the ring pattern number (1~12) for a country. ---------- *patten_num=1 Australia Ring Pattern:* *cadenceOneOn=400, cadenceOneOff=200* *cadenceTwoOn=400, cadenceTwoOff=2000* *patten_num=2 Denmark Ring Pattern:* *cadenceOneOn=1000, cadenceOneOff=4000* *.....*
voip dsp setFaxECmode -s	

ch	Set the FAX error correction mode. ch : range (0 ~ 1)
mode	mode : EC(error correction) ch(x) mode(0) : REDUNDANCY EC(error correction) ch(x) mode(1) : FEC
voip dsp setDtmfCidlevel –l / voip dsp setDtmfCidlevel –h [value] *voip dsp setDtmfCidlevel –r 0*	
value	"setDtmfCidLevel" is used to configure the signal strength for transferring to FXS DTMF caller ID. value - 0 ~ 64 voip dsp setDtmfCidLevel -l [value] voip dsp setDtmfCidLevel -h [value] voip dsp setDtmfCidLevel -r 0/1 r - reset low/high DTNF level to default setting. 0 means Disable; 1 means Enable. Note: This function is supported only by special mode.
voip dsp setfxoCY	
value	It is used to apply FXO country settings. 0: "use system country" 1: "Taiwan" 2: "Germany" 3: "Sweden" 4: "France" 5: "Switzerland" 6: "Holland" 7: "Finland" 8: "Denmark" 9: "UK" 10: "Australia" 12: "Italy" 14: "Red_China" 15: "Singapore" 17: "Spain" 18: "Portugal" 20: "Poland" 21: "Czech" 22: "Hungary" 23: "Slovenia" 25: "Slovakia" 37: "Brasil" 61: "US"
voip dsp setfxoringl	
value	It is used to configure detection ring voltage threshold to apply to FXO. Available setting include: 0 : use driver default value 1 : Minimum voltage threshold: 25V 2 : Minimum voltage threshold: 35V 3 : Minimum voltage threshold: 45V Note: This function is supported only by special mode.
voip dsp setfxoCid	
value	Set FXO detect caller ID type. It is available only for the model with FXO port.
voip dsp cidplusdigit	
[1/0] [channel] [value]	Set the substitution (0~9) for '+' digit in caller ID. 1 – enable the substitution.

	0 – disable the substitution. channel – 0 (FXS 1) -1 (FXS 2) value – 0 – 9
voip dsp setRingThres	
port	Set the threshold for ring signal. Port setting is “0” only.
value	Available settings 0-250. Unit is ms. The time is an approximate value.
voip dsp setCidDetGain	
tx|rx gain	Set the gain value of caller ID detected. Tx gain – Available settings -24 ~ 12. Default is 0. Rx gain – Available settings -24 ~ 12. Default is -6.

Example

```
> voip dsp countrytone ?
VoIP has been disable. Please enable VoIP first.
> voip sip misc –D 0
System reboot now!
> voip dsp countrytone ?
> Vigor> voip dsp countrytone?
usage:
 voip dsp countrytone [channel][value]
 [channel]: 1-2
 [value]: ( [2] UK, [3] USA, [4] Denmark, [5] Italy, [6] Germany, [7] Netherland
s, [8] Portugal, [9] Sweden, [10] Australia, [11] Slovenia, [12] Czech, [13]
Slovakia, [14] Hungary, [15] Switzerland , [16] France , [17] Malta)
============  Channel=1  ====================
 current country tone: user defined

----------- ( Dial tone ) --------------------
 Feq1=425, Feq2=0, OneOn=0, Off=0, TwoOn=0, TwoOff=0
----------- ( Ringing tone ) -----------------
 Feq1=425, Feq2=0, OneOn=1500, OneOff=3000, TwoOn=0, TwoOff=0
----------- ( Busy tone ) --------------------
 Feq1=425, Feq2=0, OneOn=200, OneOff=200, TwoOn=0, TwoOff=0

============  Channel=2  ====================
 current country tone: user defined
> voip dsp dialtonepwr 1 20
Current power level of dialtone:20 (-13 db), channel=1
> voip dsp setCidDetGain tx 1
 Current CID Detect Tx Gain [1], Rx Gain [-6]
> voip dsp setCidDetGain rx 3
 Current CID Detect Tx Gain [1], Rx Gain [3]
```

Telnet Command: voip rtp

Syntax

voip rtp codec *[sip acc index][type|size|vad|one][value]*

voip rtp dtmf *[index] [mode|payloadtype][value]*

voip rtp port *[start|end] [value]*

voip rtp symmetric *[value]*

voip rtp tos ?

Syntax Description

Parameter	Description
voip rtp codec	
[sip acc index][type|size|vad|one][value]	Set the voice coding. sip acc index –SIP account index number. Available number, 1 ~ 12. type – Available settings include 0. G.711MU 1. G.711A 2. G.729A/B 3. G.723 4. G.726_32 size - Five options, 0 means 10ms 1 means 20ms 2 means 30ms 3 means 40ms 5 means 60ms Vad - 0 means to Disable the function of Voice Active Detector (vad); 1 means to Enable the function of Voice Active Detector (vad). One – 0 means to Disable the function of single codec; 1 means to Enable the function of single codec.
voip rtp dtmf	
[index] [mode | payloadtype][value]	Set the DTMF mode and Payload type for DTMF. Index – SIP account index number. Available number, 1 ~ 12. Mode – Four options to be selected. 0. Inband 1. Outband 2. SIP INFO (cisco) 3. SIP INFO (nortel) Payloadtype – Available settings 96~127. Value – Type 0~3 or 96~127 based on the mode specified. For example, > voip rtp dtmf 1 mode 1
voip rtp port	
start|end	Specifies the start/end port for RTP stream.
value	The default value is 10050/15000.
voip rtp symmetric	
value	Make the data transmission going through on both ends of local router and remote router not misleading due to IP lost. 1 – Enable 0 - Disable
voip rtp tos	
value	Set the type of service (TOS) setting for RTP packets. For example, > voip rtp tos 0x899 Set TOS: 0x899

Example

```
> voip rtp codec 1 type 3
> voip rtp dtmf 2 mode 3
> voip rtp port start 10070 end 14400
Set start port: 10070
> voip rtp port end 14400
Set end port: 14400
> voip rtp symmetric 1
Set symmetric rtp to Enable
```

Telnet Command: voip sip

This command allows users to set SIP account.

Syntax

voip sip acc n *[-<command> <parameter> | ...]*

voip sip calllog

voip sip ep n *[-<command> <parameter> | ...]*

voip sip misc*[-<command> <parameter> | ...]*

voip sip nat *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
voip sip acc - Allows users to set SIP account.	
n	n = 1 to 12 It means the index number of the VoIP settings.
-P [profile]	It means the name of the account profile (maximum 11 characters).
-r [reg mode]	Set registration mode for SIP account. 0 – none 1 – auto 2 - wan1 only 3 - wan2 only 4 - lan/vpn 5 – PVC 6 - wan3 only 7 - wan4 only 8 - wan1 first 9 - wan2 first 10 - wan3 first 11 - wan4 first
-o [port]	Set the port number for sending/receiving SIP message for building a session. The default value is 5060.
-d [domain]	Set the domain name or IP address of the SIP Registrar server. The maximum is 63 characters.
-y [proxy]	Set domain name or IP address of SIP proxy server. The maximum is 63 characters.
-b [enable]	Enable / disable outbound proxy by SIP account. 0 – disable 1 - enable
-s [enable]	Enable / disable to locate SIP server (rfc 3263).

	0 – disable 1 - enable
-N [name]	Set SIP account display name. Name - max. 23 characters.
-n [number]	Set SIP account number. Number - max. 63 characters.
-a [id]	Set SIP authentication ID. Id - max. 63 characters.
-A [enable]	Enable /disable to use SIP authentication ID. 0 – disable 1 - enable
-p [passwd]	Set SIP account password (max. 63 characters).
-e [sec]	Set expiry time (default 3600) for SIP account.
-w [enable]	Enable to make phone call without registering.
-m [mode]	Set NAT traversal mode. 0 – disable 1 – stun 2 – manual 3 - nortel
-F [mode]	Set call forwarding mode. 0 – disable 1 – always 2 – busy 3 - no answer 4 - busy or no answer
-u [url]	Set SIP URL for call forwarding (max. 63 characters).
-t [sec]	Set call forwarding timer. For example, voip sip acc 1 –t 30
-g [port]	Set the ring port for incoming call. For example, Port - r1 means FXS1; r2 means FXS2.
-z [pattern]	Set account ring pattern (1 ~ 6).
-i [enable]	Remove all bindings while they are un-registered. 0 means Disable; and 1 means Enable.
-B <enable>	Enable / disable the function of Broadsoft Call Control. 0 – disable 1 - enable
-S [idx]	Enable and use alias IP to register. idx - 1 to 31. If 0 is used, such function will be disabled.
-k [num1 num2…]	Set backup wan list (first wan, second wan…). range: 1 to 4.
-v	View current status for account settings.
Voip sip calllog	Display current status for SIP call log.
voip sip ep	
n	The index number of the VoIP settings. n – 1, 2.
-o [acc]	Available dial out account (1 ~ 12).
-L [url]	Set SIP URL (max. 63 characters) for hot line.

-l [enable]	Enable / disable the function of hot line. 0 – disable 1 - enable
-W [enable]	Enable / disable the function of warm line. 0 – disable 1 - enable
-w [enable]	Enable / disable the function of call waiting enable. 0 – disable 1 - enable
-E [enable]	Enable / disable the function of call waiting enable but only remind one time. 0 – disable 1 - enable
-x <enable>	Enable / disable the function of call transfer. 0 – disable 1 - enable
-d [enable]	Enable / disable the function of DND (Do Not Disturb) 0 – disable 1 - enable
-s [id]	Indicate DND schedule. Id - s1, s2, s3, s4 (max. 4 schedule)
-h [enable]	Enable / disable the function of calling line identification restriction (CLIR). 0 – disable 1 - enable
-u [mode]	Set CLIR mode. 0 - means “draft-ietf-sip-privacy” 1 – means “rfc 3323/3325)”
-z [enable]	Enable / disable playing dial tone when registered on sip server. 0 – disable 1 - enable
-n [enable]	Enable / disable session timer. 0 – disable 1 - enable
-m [sec]	Set the value for session timer (unit: sec).
-R [min,max]	Set the flash hook time range 100~2000 (unit: ms).
-8 [enable]	Enable or disable T.38 fax relay feature. 0 – disable 1 - enable
-v	View current settings.
voip sip misc - Allows users to set miscellaneous settings for the device.	
-c [enable]	Enable compact header to shorten the packet (0: disable, 1: enable).
-s [enable]	Change “#” into digit number. 0 - disable 1 - enable
-e [enable]	Enable Europe style flash hook operation mode. 0 - disable

	1 - enable
-h [enable]	Enable/disable call hold mode based on protocol RFC2543 (0: disable, 1:enable).
-i [enable]	Enable CODEC change without Re-INVITE. 0 - disable 1 - enable
-p [enable]	Enable PRACK message. 0 – Not support PRACK. 1 – Support PRACK.
-P [enable]	Enable IP Call. 0 – Disable IP call. 1 – Enable IP call.
-H [enable]	SIP INFO packet will be sent out when encounting hook flash event. 0 - disable 1 - enable
-t [val]	Set the mode of User-Agent (e.g., phone, software, and device) for SIP packet. 0 - Hide SIP header "User-Agent". 1 - Show SIP header "User-Agent". 2 - Use default "User-Agent" value. 3 - Use user-defined "User-Agent" value.
-u UAValue	For every SIP user agent identifies itself with a string, this command allows you to set the value (e.g, IP address, phone number, e-mail address) of User-Agent. The length of the string must be less than 64 characters.
-D [disable]	Disable VoIP Service. 1 – disable VoIP service. 0 – enable VoIP service. System will automatic reboot to activate voip service
-v	View current status for miscellaneous settings.
voip sip nat - Allows users to set NAT Traversal Setting.	
-s [server]	Set the IP address for STUN server.
-t [sec]	Set ping interval for SIP account. Sec – 6 ~ 600
-i [ip]	Indicate external IP address.
-v	View current settings for SIP NAT.

Example

```
> voip sip misc -t 1
includes User-Agent header

> voip sip misc -u 91704688carrie
user-defined User-Agent:91704688carrie
> voip sip acc 1 -P carrie_1 -r 1 -d 172.16.3.133
> voip sip acc 1 -t 30
> voip sip misc -h 1
> voip sip acc 1 -v
index       :  1
profile     :  carrie_1
```

```
reg mode    :  1 | reg. [No]
alias_ip_idx    :  0
backup list     :
domain      :  172.16.3.133
proxy       :   | outbound [No] | DNS-SRV [No]
noreg call  :  No
disp. Name  :
acc number  :  ---
auth. ID    :   | [disable]
expiry      :  3600
NAT mode    :  0
ring ports  :  0
ring pat.   :  1
call fwd mode   :  0
call fwd url    :
call fwd timer  :  30
Broadsoft   :  disable
Italian ITSP modification: disable
```

Telnet Command: voip secure

This command allows users to enable or disable secure phone feature, and SAS voice prompt.

Syntax

voip secure general *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
voip secure general -e	Enable / disable secure phone feature. 0 - disable 1 - enable
voip secure general -p	Enable /disable SAS voice prompt. 0 - disable 1 - enable
voip secure general -v	view only secure phone general settings

Example

```
> voip secure general -v
secure phone feature is disabled
SAS voice prompt is enabled
> voip secure general -p  0
SAS voice prompt is disabled
```

Telnet Command: vpn l2lset

This command allows users to set advanced parameters for LAN to LAN function.

Syntax

vpn l2lset *[list index]* **peerid** *[peerid]*

vpn l2lset *[list index]* **localid** *[localid]*

vpn l2lset *[list index]***main** *[auto/proposal index]*

vpn l2lset *[list index]* **aggressive** *[g1/g2]*

vpn l2lset *[list index]***pfs** *[on/off]*

vpn l2lset *[list index]* **phase***1[lifetime]*

vpn l2lset *[list index]* **phase2***[lifetime]*

Syntax Description

Parameter	Description
list index	It means the index number of L2L (LAN to LAN) profile.
peerid	It means the peer identity for aggressive mode.
localid	It means the local identity for aggressive mode.
main	It means to choose proposal for main mode.
auto index	It means to choose default proposals.
proposal index	It means to choose specified proposal.
aggressive	It means the chosen DH group for aggressive mode
pfs	It means "perfect forward secrete".
on/off	It means to turn on or off the PFS function.
phase1	It means phase 1 of IKE.
lifetime	It means the lifetime value (in second) for phase 1 and phase 2.
phase2	It means phase 2 of IKE.

Example

```
> VPN l2lset 1 peerid 10226
```

Telnet Command: vpn dinset

This command allows users to configure setting for remote dial-in VPN profile.

Syntax

vpn dinset <*list index*>

vpn dinset <*list index*> <*on/off*>

vpn dinset <*list index*> **motp** <*on/off*>

vpn dinset <*list index*> **pin_secret** <*pin*> <*secret*>

Syntax Description

Parameter	Description
<*list index*>	It means the index number of the profile.
<*on/off*>	It means to enable or disable the profile. on – Enable. off – Disable.
motp <*on/off*>	It means to enable or disable the authentication with mOTP function. on – Enable.

	off – Disable.
pin_secret<pin> <secret>	It means to set PIN code with secret. <*pin*> **-** Type the code for authentication (e.g, 1234). <*secret*> - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6)

Example

```
> vpn dinset 1

Dial-in profile index 1

Profile Name: ???
Status: Deactive

Mobile OTP: Disabled

Password:

Idle Timeout: 300 sec

> vpn dinset 1 on
% set profile active

> vpn dinset 1 motp on
% Enable Mobile OTP mode!>
> vpn dinset 1 pin_secret 1234 e759bb6f0e94c7ab4fe6
> vpn dinset 1

Dial-in profile index 1

Profile Name: ???
Status: Active

Mobile OTP: Enabled

PIN: 1234

Secret: e759bb6f0e94c7ab4fe6

Idle Timeout: 300 sec
```

Telnet Command: vpn subnet

This command allows users to specify a subnet selection for the specified remote dial-in VPN profile.

Syntax

vpn subnet *[index] [1/2/3/4/5/6]*

Syntax Description

Parameter	Description
<*index*>	It means the index number of the VPN profile.
<*1/2/3/4/5/6*>	1 – it means LAN1 2 – it means LAN2. 3 – it means LAN3 4 – it means LAN4. 5 – it means LAN5. 6 – it means LAN6.

Example

```
> vpn subnet 1 2
>
```

Telnet Command: vpn setup

This command allows users to setup VPN for different types.

Syntax

Command of PPTP Dial-Out

vpn setup <*index*> <*name*> **pptp_out** <*ip*> <*usr*> <*pwd*> <*nip*> <*nmask*>

Command of IPSec Dial-Out

vpn setup <*index*> <*name*> **ipsec_out** <*ip*> <*key*> <*nip*> <*nmask*>

Command of L2Tp Dial-Out

vpn setup <*index*> <*name*> **l2tp_out** <*ip*> <*usr*> <*pwd*> <*nip*> <*nmask*>

Command of Dial-In

vpn setup <*index*> <*name*> **dialin** <*ip*> <*usr*> <*pwd*> <*key*> <*nip*> <*nmask*>

Syntax Description

Parameter	Description
For PPTP Dial-Out	
<*index*>	It means the index number of the profile.
<*name*>	It means the name of the profile.
<*ip*>	It means the IP address to dial to.
<*usr*> <*pwd*>	It means the user and the password required for the PPTP connection.
<*nip*> <*nmask*>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 pptp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
For IPsec Dial-Out	
<*index*>	It means the index number of the profile.
<*name*>	It means the name of the profile.
<*ip*>	It means the IP address to dial to.
<*key*>	It means the value of IPsec Pre-Shared Key.
<*nip*> <*nmask*>	It means the remote network IP and the mask. e.g.,

	vpn setup 1 name1 ipsec_out 1.2.3.4 1234 192.168.1.0 255.255.255.0
For L2TP Dial-Out	
<*index*>	It means the index number of the profile.
<*name*>	It means the name of the profile.
<*ip*>	It means the IP address to dial to.
<*usr*> <*pwd*>	It means the user and the password required for the L2TP connection.
<*nip*> <*nmask*>	It means the remote network IP and the mask. e.g.,, vpn setup 1 name1 l2tp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
For Dial-In	
<*index*>	It means the index number of the profile.
<*name*>	It means the name of the profile.
<*ip*>	It means the IP address allowed to dial in.
<*usr*> <*pwd*>	It means the user and the password required for the PPTP/L2TP connection.
<*key*>	It means the value of IPsec Pre-Shared Key.
<*nip*> <*nmask*>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0 255.255.255.0

Example

```
> vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0
255.255.255.0
% Profile Change Log ...

% Profile Index : 1
% Profile Name : name1
% Username : vigor
% Password : 1234
% Pre-share Key : abc
% Call Direction : Dial-In
% Type of Server :  ISDN PPTP IPSec L2TP
% Dial from : 1.2.3.4
% Remote NEtwork IP : 192.168.1.0
% Remote NEtwork Mask : 255.255.255.0
>
```

Telnet Command: vpn option

This command allows users to configure settings for LAN to LAN profile.

Syntax

vpn option <*index*> <*cmd1*>=<*param1*> [<*cmd2*>=<*para2*> | *…]*

Syntax Description

Parameter	Description
<index>	It means the index number of the profile. Available index numbers: 1 ~ 32
For Common Settings	
<index>	It means the index number of the profile.
pname	It means the name of the profile.
ena	It means to enable or disable the profile. on – Enable off - Disable
thr	It means the way that VPN connection passes through. Available settings are wlf, wlo, w2f, and w2o. w1f – WAN1 First. w1o – WAN1 Only. w2f – WAN2 First. w2o – WAN2 Only.
nnpkt	It means the NetBios Naming Packet. on – Enable the function to pass the packet. off – Disable the function to block the packet.
dir	It means the call direction. Available settings are b, o and i. b – Both o – Dial-Out i – Dial-In.
idle=[value]	It means Always on and Idle Time out. Available values include: -1 – it means always on for dial-out. 0 – it means always on for dial-in. Other numbers (e.g., idle=200, idle=300, idle=500) mean the router will be idle after the interval (seconds) configured here.
palive	It means to enable PING to keep alive. -1 – disable the function. 1,2,3,4 – Enable the function and PING IP 1.2.3.4 to keep alive.
For Dial-Out Settings	
ctype	It means “Type of Server I am calling”. “ctype=t” means PPTP. “ctype=s” means IPSec. “ctype= l” means L2TP(IPSec Policy None). “ctype= l1” means L2TP(IPSec Policy Nice to Have). “ctype= l2” means L2TP(IPSec Policy Must).
dialto	It means Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89).
ltype	It means Link Type. “ltype=0” means “Disable”. “ltype=1” means “64kbps”. “ltype=2” means “128kbps”. “ltype=3” means “BOD”.
oname	It means Dial-Out Username. “oname=admin” means to set Username = admin.
opwd	It means Dial-Out Password

	"opwd=1234" means to set Password = 1234.
pauth	It means PPP Authentication. "pauth=pc" means to set PPP Authentication = PAP&CHAP. "pauth=p" means to set PPP Authentication = PAP Only
ovj	It means VJ Compression. "ovj=on/off" means to enable/disable VJ Compression.
okey	It means IKE Pre-Shared Key. "okey=abcd" means to set IKE Pre-Shared Key = abcd.
ometh	It means IPSec Security Method. "ometh=ah/" means AH. "ometh=espd/espda/" means ESP DES without/with Authentication. "ometh=esp3/esp3a/" means ESP 3DES without/with Authentication. "ometh=espa/espaa" means ESP AES without/with Authentication.
sch	It means Index(1-15) in Schedule Setup. sch=1,3,5,7 Set schedule 1->3->5->7
rcallb	It means Require Remote to Callback. "rcallb=on/off" means to enable/disable Set Require Remote to Callback.
ikeid	It means IKE Local ID. "ikeid=vigor" means Set Local ID = vigor.
For Dial-In Settings	
itype	It means Allowed Dial-In Type. Available settings include: "itype=t" means PPTP. "itype=s" means IPSec. "itype=L1"means L2TP (None). "itype=L1" means L2TP(Nice to Have). "itype=l2" means L2TP(Must).
peer	It means specify Peer VPN Server IP for Remote VPN Gateway. Type "203.12.23.48" means to allow VPN dial-in with IP address of 203.12.23.48. Type "off" means any remote IP is allowed to dial in.
peerid	It means the peer ID for Remote VPN Gateway. Type "draytek" means the word is used as local ID.
iname	It means Dial-in Username. "iname=admin" means to set username as "admin".
ipwd	It means Dial-in Password. "ipwd=1234" means to set password as "1234".
ivj	It means VJ Compression. "ivj=on/off" means to enable /disable VJ Compression.
ikey	It means IKE Pre-Shared Key. "ikey=abcd" means to set IKE Pre-Shared Key = abcd.
imeth	It means IPSec Security Method "imeth=h" means "Allow AH". "imeth=d" means "Allow DES". "imeth=3" means "Allow 3DES". "imeth=a" means "Allow AES.
For TCP/IP Settings	

mywip	It means My WAN IP. “mywip=1.2.3.4” means to set My WAN IP as “1.2.3.4”.
rgip	It means Remote Gateway IP. “rgip=1.2.3.4” means to set Remote Gateway IP as “1.2.3.4”.
rnip	It means Remote Network IP. “rnip=1.2.3.0” means to set Remote Network IP as “1.2.3.0”.
rnmask	It means Remote Network Mask. “rnmask=255.255.255.0” means to set Remote Network Mask as “255.255.255.0”.
rip	It means RIP Direction. “rip=d” means to set RIP Direction as “Disable”. “rip=t” means to set RIP Direction as “TX”. “rip=r” means to set RIP Direction as “RX”. “rip=b” means to set RIP Direction as “Both”.
mode	It means the option of “From first subnet to remote network, you have to do”. “mode=r” means to set Route mode. “mode=n” means to set NAT mode.
droute	It means to Change default route to this VPN tunnel (Only single WAN supports this). droute=on/off means to enable/disable the function.

Example

```
> vpn option 1 idle=250
% Change Log..

% Idle Timeout = 250
```

Telnet Command: vpn mroute

This command allows users to list, add or delete static routes for a certain LAN to LAN VPN profile.

Syntax

vpn mroute <*index*> **list**

vpn mroute <*index*> **add** <*network ip*>/<*mask*>

vpn mroute <*index*> **del** <*network ip*>/<*mask*>

Syntax Description

Parameter	Description
list	It means to display all of the route settings.
add	It means to add a new route.
del	It means to delete specified route.
<*index*>	It means the index number of the profile. Available index numbers: 1 ~ 32
<*network ip*>/<*mask*>	Type the IP address with the network mask address.

Example

```
> vpn mroute 1 add 192.168.5.0/24
% 192.168.5.0/24
% Add new route 192.168.5.0/24 to profile 1
```

Telnet Command: vpn list

This command allows users to view LAN to LAN VPN profiles.

Syntax

vpn list <*index*> **all**

vpn list <*index*>**com**

vpn list<*index*>**out**

vpn list <*index*> **in**

vpn list<*index*>**net**

Syntax Description

Parameter	Description
all	It means to list configuration of the specified profile.
com	It means to list common settings of the specified profile.
out	It means to list dial-out settings of the specified profile.
in	It means to list dial-in settings of the specified profile.
net	It means to list Network Settings of the specified profile.
<*index*>	It means the index number of the profile. Available index numbers: 1 ~ 32

Example

```
> vpn list 32 all
% Common Settings

% Profile Name            : ???
% Profile Status          : Disable
% Netbios Naming Packet   : Pass
% Call Direction          : Both
% Idle Timeout            : 300
% PING to keep alive      : off

% Dial-out Settings

% Type of Server          : PPTP
% Link Type:              : 64k bps
% Username                : ???
% Password                :
% PPP Authentication      : PAP/CHAP
% VJ Compression          : on
% Pre-Shared Key          :
% IPSec Security Method   : AH
% Schedule                : 0,0,0,0
% Remote Callback         : off
```

```
% Provide ISDN Number     : off
% IKE phase 1 mode        : Main mode
% IKE Local ID            :


% Dial-In Settings

--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
> vpn list 1 com
% Common Settings

% Profile Name          : ???
% Profile Status        : Disable
% Netbios Naming Packet : Pass
% Call Direction        : Both
% Idle Timeout          : 300
% PING to keep alive    : off
>
```

Telnet Command: vpn remote

This command allows users to enable or disable *PPTP/IPSec/L2TP* VPN service.

Syntax

vpn remote *[PPTP/IPSec/L2TP] [on/off]*

Syntax Description

Parameter	Description
PPTP/IPSec/L2TP	There are four types to be selected.
on/off	on – enable VPN remote setting. off – disable VPN remote setting.

Example

```
> vpn remote PPTP on
Set PPTP VPN Service : On

Please restart the router!!
```

Telnet Command: vpn 2ndsubnet

This command allows users to enable second subnet IP as VPN server IP.

Syntax

vpn 2ndsubnet *on*

vpn 2ndsubnet *off*

Syntax Description

Parameter	Description
on/off	It means to enable or disable second subnet.

Example

```
> vpn 2ndsubnet on
%Enable second subnet IP as VPN server IP!
```

Telnet Command: vpn trunk

This command allows users to configure VPN Backup, VPN load balance, GRE over IPsec, and Binding tunnel policy.

vpn trunk show_usable

vpn trunk backup *<add/del> <name> <Member#1> <Member#2>*

vpn trunk backup more_syslog *<ON/OFF>*

vpn trunk backup ERD *<name> <Normal/Recover/Resume><second>*

vpn trunk lb *<add/del> <name> <Member#1> <Member#2>*

vpn trunk lb more_syslog *<ON/OFF>*

vpn trunk lb algorithm *<name> <RR>*

vpn trunk lb algorithm *<name><W-RR><Auto> <AccordingRatio> <Member1:Member2>*

vpn trunk lb algorithm *<name><Fastest>*

vpn trunk bind usage *<BindIndex>*

vpn trunk bind show *<LoadBalanceName>*

vpn trunk bind reset_default

vpn trunk bind more_syslog *<ON/OFF>*

vpn trunk bind set *<BindIndex> <ACT> <TrunkName> <Member> <SrcIp:A~B> <DstI p:A~B> <DstPort:A~B> <Proto> <Frag>*

vpn trunk bind insert *<After_BindIndex> <ACT> <TrunkName> <Member> <SrcIp:A~B> <DstIp:A~B> <DstPort:A~B> <Proto> <Frag>*

vpn trunk SetGre show *<Dialout_Index>*

vpn trunk SetGre
<Active/In-active><Dialout_Index><GRE_MyIP><GRE_PeerIP><Logical_Traffic>

vpn trunk An_Gre GreIPsecAnalyze *<ON/OFF>*

Syntax Description

Parameter	Description
show_usable	Display a list of LAN to LAN dial out profiles.
backup <add/del> <name> <Member#1> <Member#2>	Set multiple VPN tunnels (LAN to LAN profiles) as backup tunnel. add/del - Add or delete a profile for used in VPN Trunk. name – Specify the name of the VPN trunk. Member#1 – Indicate the first LAN to LAN profile. Member#2 – Indicate the second LAN to LAN profile.
backup more_syslog <ON/OFF> *Ib more_syslog <ON/OFF>* *bind more_syslog <ON/OFF>*	These commands are used for RD debug.
backup ERD <name> <Normal/Recover/Resume>< second>	ERD means Environment Recovers Detection. name – Specify the name of the VPN trunk. Normal – Indicate the Normal mode. All dial-out VPN TRUNK backup

	profiles will be activated alternatively. Recover – Indicate the duration of VPN backup operation. Resume – When VPN connection breaks down or disconnects, Member 1 will be the top priority for the system to do VPN connection. Second – "0" means to dial each six seconds automatically. "60 ~ 2147483647" means to early handle for less than 30 seconds within designated time.
lb <add/del> <name> <Member#1> <Member#2>	It means to create VPN trunk with load balance. add/del - Add or delete a profile for used in VPN Trunk. name – Specify the name of the VPN trunk. Member#1 – Indicate the first LAN to LAN profile. Member#2 – Indicate the second LAN to LAN profile.
lb algorithm <name> <RR/W-RR/Fastest>	Set multiple VPN tunnels for using as traffic load balance tunnel. Such command is to configure the algorithm (with round robin mode) of Load Balance. name – Specify the name of the VPN trunk. RR – It means round robin mode. All of the dial-out profiles will be taken turns equally.
lb algorithm <name><W-RR><Auto> <AccordingRatio> <Member1:Member2>	Such command is to configure the algorithm (with round robin mode) of Load Balance. name – Specify the name of the VPN trunk. W-RR – It means weighted round robin mod based on speed ratio. ● *Auto - the speed must be based on Lay2.* ● *AccordingRatio – the speed must be based on given ratio.* Member#1 – Inidcate the first LAN to LAN profile. Member#2 – Indicate the second LAN to LAN proifle.
lb algorithm <name><Fastest>	Such command is to configure the algorithm (with fastest mode) of Load Balance. Most of traffics will be led to the channel with the fastest connection. name – Specify the name of the VPN trunk.
bind usage <BindIndex>	Display detailed information for VPN Load Balance Tunnel Bind. BindIndex – Indicate the index number of the tunnle bind.
bind show <LoadBalanceName>	Display the bind information for VPN Load Balance profile. LoadBalanceName – type the name of VPN Load Balance profile
bind reset_default	Reset the bind tunnel for VPN load balance to factory reset settings.
bind set <BindIndex> <ACT> <TrunkName> <Member> <SrcIp:A~B> <DstI p:A~B> <DstPort:A~B> <Proto> <Frag>	Set the binding tunnel policy. BindIndex – Indicate the index number (1 ~ 64) for the tunnel to be bound. `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 OFF` ACT – Specify the action. "y" means active; "n" means inactive or delete. TrunkName - TrunkName - Specify the name of the VPN trunk created by using "vpn trunk lb" command. Member – Specify the index number of the LAN to LAN (dial-out) profile to be bound. SrcIp:A~B – Specify the source IP range (e.g., 192.168.10.0~192.168.10.255. DstI p:A~B - Specify the destination IP range (e.g., 192.168.1.0~192.168.1.255. DstPort:A~B – Specify the destination port range (1~65535). Proto – Specify the protocol.

	0 – any 1 – ICMP 2 – IGMP 6 – TCP 17 – UDP 255 – TCP/UDP Frag – "ON" means to bind the fragmented packet; "OFF" means not to care. It is the default setting.
bind insert <After_BindIndex> <ACT> <TrunkName> <Member> <SrcIp:A~B> <DstIp:A~B> <DstPort:A~B> <Proto> <Frag>	It is used to insert additional load balance policy into an existing policy. After_BindIndex – Specify an index number that new additional policy should be inserted before. See the following example: *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 OFF* ACT – Specify the action. "y" means active; "n" means inactive or delete. TrunkName - Specify the name of the VPN trunk. Member – Specify the index number of the LAN to LAN (dial-out) profile to be bound. SrcIp:A~B – Specify the source IP range (e.g., 192.168.10.0~192.168.10.255. DstI p:A~B - Specify the destination IP range (e.g., 192.168.1.0~192.168.1.255. DstPort:A~B – Specify the destination port range (1~65535). Proto – Specify the protocol. 0 – any 1 – ICMP 2 – IGMP 6 – TCP 17 – UDP 255 – TCP/UDP Frag – "ON" means to bind the fragmented packet; "OFF" means not to care. It is the default setting.
SetGre show <Dialout_Index>	Display the GRE over IPSec settings in specified LAN to LAN profile. Dialout_Index – Index number of the LAN to LAN (dial-out) profile.
SetGre <Active/In-active><Dialout_Index><GRE_MyIP><GRE_PeerIP><Logical_Traffic>	Active/In-active - Specify the action. "y" means active; "n" means inactive. Dialout_Index – Index number of the LAN to LAN (dial-out) profile. GRE_MyIP –Type the virtual IP for router itself for verified by peer. GRE_PeerIP –Type the virtual IP of peer host for verified by router. Logical_Traffic - Specify the action for RFC2890. "y" means active; "n" means inactive.
An_Gre GreIPsecAnalyze *<ON/OFF>*	These commands are used for RD debug.

Example

```
> vpn setup 1 name1 pptp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
% Profile Change Log ...

% Profile Index : 1
% Profile Name : name1j
% Username : vigor
% Password : 1234
% Call Direction : Dial-Out
% Type of Server : PPTP
```

```
% Dial to : 1.2.3.4
% Remote NEtwork IP : 192.168.1.0
% Remote NEtwork Mask : 255.255.255.0
> vpn setup 2 market pptp_out 5.6.7.8 vigor 5678 192.168.1.31 255.255.255.0
% Profile Change Log ...

% Profile Index : 2
% Profile Name : market
% Username : vigor
% Password : 5678
% Call Direction : Dial-Out
% Type of Server : PPTP
% Dial to : 5.6.7.8
% Remote NEtwork IP : 192.168.1.31
% Remote NEtwork Mask : 255.255.255.0
> vpn trunk lb add comp 1 2
%% Combination VPN Load Balance profile list :
  <Index>   <    Name    >     <    Member1(Active)Type    >    <
Member2(Act
ive)Type    >
    1        comp                   1(YES)PPTP                    2(YES)P
PTP

%% Note: <Active: NO> The LAN-to-LAN Profile is disable or under Dial-In(Call
Di
rection) at present.
==========================================================================

%  Setting 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 OFF
% VPN Load Balance Tunnel Bind Table Index[1] detail:
============================================================
 Action              = ACTIVE
 Trunk Profile(000) Name= comp
 Binding Dial Out Index = 2
 Binding Src IP        = 192.168.10.1 ~ 192.168.10.2
 Binding Dest IP       = 192.168.99.1 ~ 192.168.99.254
 Binding Dest Port      = 1 ~ 65535
 Binding Fragmented     = NO
 Binding Protocol       = ANY Protocol
>
```

Telnet Command: vpn NetBios

This command allows users to enable or disable NetBios for Remote Access User Accounts or LAN-to-LAN Profile.

Syntax

vpn NetBios set <*H2I/L2I*> <*index*> <*Block/Pass*>

Syntax Description

Parameter	Description
<*H2I/L2I*>	H2I means Remote Access User Accounts. L2I means LAN-to-LAN Profile. Specify which one will be applied by NetBios.
<*index*>	The index number of the profile.
<*Block/Pass*>	**Pass** – Have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Block** – When there is conflict occurred between the hosts on both

	sides of VPN Tunnel in connecting, set it block data transmission of Netbios Naming Packet inside the tunnel.

Example

```
> vpn NetBios set H2l 1 Pass
% Remote Dial In Profile Index [1] :
% NetBios Block/Pass: [PASS]
```

Telnet Command: vpn mss

This command allows users to configure the maximum segment size (MSS) for different TCP types.

Syntax

vpn mss show

vpn mss default

vpn mss set *<connection type> <TCP maximum segment size range>*

Syntax Description

Parameter	Description
show	It means to display current setting status.
default	TCP maximum segment size for all the VPN connection will be set as 1360 bytes.
set	Use it to specify the connection type and value of MSS.
<connection type>	1~4 represent various type. 1 – PPTP 2 – L2TP 3 – IPSec 4 – L2TP over IPSec
<TCP maximum segment size range>	Each type has different segment size range. PPTP – 1 ~ 1412 L2TP – 1 ~ 1408 IPSec – 1 ~ 1381 L2TP over IPSec – 1 ~ 1361

Example

```
>vpn mss set 1 1400
% VPN TCP maximum segment size (MSS) :
  PPTP  = 1400
  L2TP  = 1360
  IPSec = 1360
  L2TP over IPSec  = 1360
>vpn mss show
 VPN TCP maximum segment size (MSS) :
 PPTP  = 1400
 L2TP  = 1360
 IPSec = 1360
 L2TP over IPSec  = 1360
```

Telnet Command: vpn ike

This command is used to display IKE memory status and leakage list.

Syntax

vpn ike -q

Example

```
> vpn ike -q
IKE Memory Status and Leakage List

# of free L-Buffer=95, minimum=94, leak=1
# of free M-Buffer=529, minimum=529 leak=3
# of free S-Buffer=1199, minimum=1198, leak=1
# of free Msgid-Buffer=1024, minimum=1024
```

Telnet Command: vpn Multicast

This command allows users to pass or block the multi-cast packet via VPN**.**

Syntax

vpn Multicast set <*H2l/L2l*> <*index*> <*Block/Pass*>

Syntax Description

Parameter	Description
<*H2l/L2l*>	H2l means Host to LAN (Remote Access User Accounts). L2l means LAN-to-LAN Profile.
<*index*>	The index number of the profile.
<*Block/Pass*>	Set Block/Pass the Multicast Packets. The default is Block.

Example

```
> vpn Multicast set L2l 1 Pass
% Lan to Lan Profile Index [1] :
% Status Block/Pass: [PASS]
```

Telnet Command: vpn pass2nd

This command allows users to determine if the packets coming from the second subnet passing through current used VPN tunnel.

Syntax

vpn pass2nd*[on]*

vpn pass2nd *[off]*

Syntax Description

Parameter	Description
on/off	on – the packets can pass through NAT.

	off – the packets cannot pass through NAT.

Example

```
> vpn pass2nd on
% 2nd subnet is allowed to pass VPN tunnel!
```

Telnet Command: vpn pass2nat

This command allows users to determine if the packets passing through by NAT or not when the VPN tunnel disconnects.

Syntax

vpn pass2nat *[on]*

vpn pass2nat *[off]*

Syntax Description

Parameter	Description
on/off	on – the packets can pass through NAT. off – the packets cannot pass through NAT.

Example

```
> vpn pass2nat on
% Packets would go through by NAT when VPN disconnect!!
```

Telnet Command: vpn sameSubnet

This command allows users to build VPN between clients via virtual subnet.

Syntax

vpn sameSubnet *-i [value]*

vpn sameSubnet *–E [0/1]*

vpn sameSubnet *–e[value]*

vpn sameSubnet*-I [xxx.xxx.xxx.xxx]*

vpn sameSubnet *-o [add/del]*

vpn sameSubnet *-v*

Syntax Description

Parameter	Description
-i [value]	Specify the index number of VPN profile.
–E [0/1]]	Enable or disable the IPsec with the same subnet. 1 – enable. 0 – disable.
-e [value]	Translate specified LAN to virtual subnet. 1 – LAN1 2 – LAN2

	3 – LAN3 ...
-I [xxx.xxx.xxx.xxx]	Set the virtual subnet (e.g., 172.16.3.250).
-v	Display current status of virtual subnet.

Example

```
> vpn sameS  -i 1 -e 1 -E 1 -e 1 -I 10.10.10.0 -o add
> vpn sameS -v
IPsec with the same subnet:
VPN profile 1 enable,
 % translated LAN1 to Virtual subnet: 10.10.10.0
```

Telnet Command: wan ppp_mru

This command allows users to adjust the size of PPP LCP MRU. It is used for specific network.

Syntax

wan ppp_mru <*WAN interface number*> <*MRU size* >

Syntax Description

Parameter	Description
<*WAN interface number*>	Type a number to represent the physical interface. For Vigor130, the number is 1 (which means WAN1).
<*MRU size* >	It means the number of PPP LCP MRU. The available range is from 1400 to 1600.

Example

```
>wan ppp_mru 1 ?
% Now: 1492

> wan ppp_mru 1 1490
>
> wan ppp_mru 1 ?
% Now: 1490

> wan ppp_mru 1 1492
> wan ppp_mru 1 ?
% Now: 1492
```

Telnet Command: wan mtu / wan mtu2

This command allows users to adjust the size of MTU for WAN1/WAN2.

Syntax

wan mtu *[value]*

wan mtu2 *[value]*

Syntax Description

Parameter	Description

value	It means the number of MTU for PPP. The available range is from 1000 to 1500. For Static IP/DHCP, the maximum number will be 1500. For PPPoE, the maximum number will be 1492. For PPTP/L2TP, the maximum number will be 1460.

Example

```
> wan mtu 1100
> wan mtu ?
Static IP/DHCP (Max MSS: 1500)
PPPoE(Max MSS: 1492)
PPTP/L2TP(Max MSS: 1460)
% wan ppp_mss <MSS size: 1000 ~ 1500>
% Now: 1100
```

Telnet Command: wan dns

This command allows users to configure primary and / or secondary DNS server.

Syntax

wan dns *[wan_no][dns_select][ipv4_addr]*

Syntax Description

Parameter	Description
wan_no	Select WAN interface. 1 - WAN1 2 - WAN2
dns_select	Specify primary and / or secondary DNS server. pri – It means primary DNS server. sec – It means secondary DNS server.
ipv4_addr	Type the IP address of DNS server.

Example

```
> wan dns 1 pri 168.95.1.1
% Set WAN1 primary DNS done.
% Now: 168.95.1.1
```

Telnet Command: wan DF_check

This command allows you to enable or disable the function of DF (Don't fragment)

Syntax

wan DF_check *[on]*

wan DF_check *[off]*

Syntax Description

Parameter	Description
on/off	It means to enable or disable DF.

Example

```
> wan DF_check on
%DF bit check enable!
> wan DF_check off
%DF bit check disable (reset DF bit)!
```

Telnet Command: wan disable

This command allows you to disable WAN connection.

Example

```
> wan disable WAN
%WAN disabled.
```

Telnet Command: wan enable

This command allows you to disable wan connection.

Example

```
> wan enable WAN
%WAN1 enabled.
```

Telnet Command: wan forward

This command allows you to enable or disable the function of WAN forwarding. The packets are allowed to be transmitted between different WANs.

Syntax

wan forward *[on]*

wan forward *[off]*

Syntax Description

Parameter	Description
on/off	It means to enable or disable WAN forward.

Example

```
> wan forward ?
%WAN forwarding is Disable!

> wan forward on
%WAN forwarding is enable!
```

Telnet Command: wan status

This command allows you to display the status of WAN connection, including connection mode, TX/RX packets, DNS settings and IP address.

Example

```
> wan status
WAN1: Offline, stall=N
 Mode: ---, Up Time=00:00:00
 IP=---, GW IP=---
 TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0
 Primary DNS=0.0.0.0, Secondary DNS=0.0.0.0
```

```
PVC_WAN3: Offline, stall=N
 Mode: ---, Up Time=00:00:00
 IP=---, GW IP=---
 TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0

PVC_WAN4: Offline, stall=N
 Mode: ---, Up Time=00:00:00
 IP=---, GW IP=---
 TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0

PVC_WAN5: Offline, stall=N
 Mode: ---, Up Time=00:00:00
 IP=---, GW IP=---
 TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0
```

Telnet Command: wan modem / wan modem2

This command, wan modem, allows you to configure 3G/4G USB Modem (PPP mode) of WAN3.

The command, wan modem2, allows you to configure 3G/4G USB Modem (PPP mode) of WAN4.

Syntax

wan modem *[init/init2/dial/pin][string]*

wan modem paponly *[on/off]*

wan modem backup_wait *[value]*

wan modem pipe *[Int][Din][Dout] (for USB WAN3 only)*

wan modem wakeup *[on/off/value] (for USB WAN3 only)*

wan modem vid *[id]*

wan modem pid *[id]*

wan modem status

Syntax Description

Parameter	Description
init	Set initial modem AT command (default value is "AT&FE0V1X1&D2&C1S0=0").
Init2	Set the second initial modem AT command.
dial	Set dial modem AT command (default value is "ATDT*99#").
pin	Set PIN code for SIM card. "0":disable
paponly	It means PAP Only. Set the PPP authentication of the USB WAN. on: None. off: PAP or CHAP.
backup_wait	Set waiting time after boot if USB WAN is in backup mode. This waiting time is reserved for the dial of main WANs so that the backup USB WAN will not go up first. Available setting is from 1 to 255. Unit is second.
pipe	It is for RD debug only. Please don't use it without our advice.

wakeup [on/off]	It is for RD debug only. Please don't use it without our advice.
vid	Set VID of VID/PID match to bind the USB modem to specify WAN interface. By default, this match is not set (0x0/0x0) and the router specifies WAN interface by USB port.
pid	Set PID of VID/PID match to bind the USB modem to specify WAN interface. By default, this match is not set (0x0/0x0) and the router specifies WAN interface by USB port.
status	Display current status of USB modem.

Example

```
> wan modem pin 0000
> wan modem status
 Modem Link Speed=0
 Current Signal Strength=0
 Last Fail Message:
 Current Connect Stage:
```

Telnet Command: wan wimax

This command allows you to enable or disable WAN 3G/4G DHCP mode for Vigor router.

Syntax

wan wimax *[on/off]*

Syntax Description

Parameter	Description
On	It means to enable WAN 3G/4G DHCP mode.
off	It means to disable WAN 3G/4G DHCP mode.

Example

```
> wan wimax ?
 Current status is wimax OFF
> wan wimax on
>
```

Telnet Command: wan lte

This command allows you to configure LTE WAN (for L model only).

Syntax

wan lte auth *[0/1]*

wan lte band

wan lte del *[index #/all]*

wan lte pass *[string]*

wan lte quota *[-<command><parameter>|...]*

wan lte read *[index #/all]*

wan lte reboot *[-<command><parameter>|...]*

wan lte reply *[-<command><parameter>|...]*

wan lte send *[number][message]*

wan lte stus

wan lte tag *[index #/all]*

wan lte user *[string]*

wan lte wms *[send[cdma/gwpp]/recv[cdma/gwgw]/setting]*

Syntax Description

Parameter	Description
auth [0/1]	Set PPP authentication of LTE WAN. 0: None. 1: PAP or CHAP.
band	Display working band information for LTE network connection.
del [index #/all]	Delete an SMS from the LTE SIM card by specifying the index number. Use “all” to delete all.
pass	Set the password of LTE WAN.
quota [-<command><parameter>|...]	Set settings of SMS Quota Limit function. Available commands with parameter are listed below: [...] means that you can type in several commands in one line. -a <0/1>: Set whether to send an e-mail alert when SMS quota exceeded. (0: no 1: yes) -c <cycle>: Set the order of today in refresh cycle. -d <day>: Set the refresh day. -e <0/1>: Enable or disable SMS Quota Limit function. (0: disable 1: enable) -h <hour>: Set the refresh hour. -m <0/1/2>: Set SMS quota refresh mode. (0: None 1: monthly 2: periodically) -n <number>: Set SMS quota. The avaible number is between 1 and 1000000. -s <0/1>: Set whether to stop sending SMS after SMS quota exceeded. (0: no 1: yes)
read	Display information of an SMS in the LTE SIM card by specifying the index number. Use "all" to display all.
reboot	Set settings of Reboot on SMS Message function. <command> <parameter>	... The available commands with parameters are listed below. [...] means that you can type in several commands in one line. -a <0/1>: Enable or disable Access Control List. (0: disable 1: enable) -e <0/1>: Enable or disable Reboot on SMS Message function. (0: disable 1: enable) -p <password>: Set the Password / PIN. This setting is necessary if this function is enabled. -x <number>: Set the first phone number in Access Control List. -y <number>: Set the second phone number in Access Control List. -z <number>: Set the third phone number in Access Control List.
reply	Set settings of Reply with Router Status Message function. <command> <parameter>	... The available commands with parameters are listed below.

	[…] means that you can type in several commands in one line. -a <0/1>: Enable or disable Access Control List. (0: disable 1: enable) -c <0/1>: Set whether to reply with MAC address. (0: no 1: yes) -e <0/1>: Enable or disable Reboot on SMS Message function. (0: disable 1: enable) -f <0/1>: Set whether to reply with WAN1 IP address. (0: no 1: yes) -g <0/1>: Set whether to reply with WAN2 IP address. (0: no 1: yes) -h <0/1>: Set whether to reply with LTE WAN IP address. (0: no 1: yes) -i <0/1>: Set whether to reply with WAN4 IP address. (0: no 1: yes) -j <0/1>: Set whether to reply with WAN1 data usage. (0: no 1: yes) -k <0/1>: Set whether to reply with WAN2 data usage. (0: no 1: yes) -l <0/1>: Set whether to reply with LTE WAN data usage. (0: no 1: yes) -m <0/1>: Set whether to reply with WAN4 data usage. (0: no 1: yes) -n <0/1>: Set whether to reply with Router name. (0: no 1: yes) -p <password>: Set the Password / PIN. This setting is necessary if this function is enabled. -u <0/1>: Set whether to reply with Router system uptime. (0: no 1: yes) -v <0/1>: Set whether to reply with Router firmware version. (0: no 1: yes) -x <number>: Set the first phone number in Access Control List. -y <number>: Set the second phone number in Access Control List. -z <number>: Set the third phone number in Access Control List.
send	Send an SMS message to the specified phone number through the LTE SIM card.
stus	Display status of LTE connection.
tag	Set an SMS in the LTE SIM card as read state by specifying the index number. Use "all" to set all SMS as read state.
user	Set the UserName of LTE WAN.
wms	This command is for RD debug only. We use it to test new USB modems. Please don't use it without our advice.

Example

```
> wan lte band

Access technology : LTE
Access band information : E-UTRA Op Band 3
Interfere with 2.4G WLAN : NO
Active channel: 1725
>wan lte stus
Status: Operational. (Online)
Access Tech: LTE
Band: E-UTRA Op Band 3
ISP: Chunghwa
MCC: 466, MNC: 92, LAC: 65534, Cell ID: 81023501
Max Channel TX Rate: 50000000 bps
Max Channel RX Rate: 100000000 bps
IMEI: 356318040749422
IMSI: 466924200859808
RSSI: -61 dBm
Unread SMS: 4
SMSC address: +886932400821
```

```
SMS service status : Ready
Number of SMS sent : 0
```

Telnet Command: wan detect

This command allows you to configure WAN connection detection. When Ping Detection is enabled (for Static IP or DHCP or PPPoE mode), Router pings specified IP addresses to detect the WAN connection.

Syntax

wan detect *[wan1/wan2][on/off/always_on]*

wan detect *[wan1/wan2]* **target** *[ip addr]*

wan detect *[wan1/wan2]* **target2***[ip addr]*

wan detect *[wan1/wan2]* **target_gw** *[1/0]*

wan detect *[wan1/wan2]* **ttl** *[value]*

wan detect *[wan1/wan2]* **interval** *[interval]*

wan detect *[wan1/wan2]* **retry** *[retry]*

wan detect status

Syntax Description

Parameter	Description
on	Enable ping detection. The IP address of the target shall be set.
off	Enable ARP detection (default).
always_on	Disable link detect, always connected(only support static IP)
target	Set the ping target.
Target2	Set the secondary ping target.
Target_gw	Set whether to use gateway as ping target. (1: yes 0: no) Note that USB WAN (PPP mode) cannot support PING gateway
ip addr	It means the IP address used for detection. Type an IP address in this field.
ttl	It means to set the ping TTL value (work as trace route) If you do not set any value for ttl here or just type 0 here, the system will use default setting (255) as the ttl value.
interval [interval]	Set the interval between each ping operation. Available setting is between 1 and 3600. The unit is second. *[interval]:* Type a value.
retry [retry]	Set how many ping operations are retried before the Router judges that the WAN connection is disconnected. Available setting is between 1 and 255. The unit is times. [retry] : Type a number.
status	It means to show the current status.

Example

```
> wan detect status
 WAN1: always on
 WAN2: off
 WAN3: off
```

```
 WAN4: off
 WAN5: off
> wan detect wan1 target 192.168.1.78
 Set OK

> wan detect wan1 on
 Set OK

> wan detect status
 WAN1: on, Target=192.168.1.78, TTL=255
 WAN2: off
 WAN3: off
 WAN4: off
 WAN5: off
>
```

Telnet Command: wan lb

This command allows you to Enable/Disable for each WAN to join auto load balance member.

Syntax

wan lb *[wan1/wan2/...] on*

wan lb *[wan1/wan2/...] off*

wan lb status

Syntax Description

Parameter	Description
wan1/wan2	Specify which WAN will be applied with load balance.
on	Make WAN interface as the member of load balance.
off	Cancel WAN interface as the member of load balance.
status	Show the current status.

Example

```
> wan lb status
 WAN1: on
 WAN2: on
 WAN3: on
 WAN4: on
 WAN5: on
 WAN6: on
 WAN7: on
```

Telnet Command: wan mvlan

This command allows you to configure multi-VLAN for WAN and LAN. It supports pure bridge mode (modem mode) between Ethernet WAN and LAN port 2~4.

Syntax

wan mvlan *[pvc_no/status/save/enable/disable] [on/off/clear/tag tag_no] [service type/vlan priority] [px ...]*

wan mvlan *keeptag[pvc_no][on/off]*

Syntax Description

Parameter	Description
pvc_no	It means index number of PVC. There are 10 PVC, 0(Channel-1) to 9(Channel-9) allowed to be configured. However, bridge mode can be set on PVC number 2 to 9.
status	It means to display the whole Bridge status.
save	It means to save the configuration into flash of Vigor router.
enable/disable	It means to enable/disable the Multi-VLAN function.
on/off	It means to turn on/off bridge mode for the specific channel.
clear	It means to turn off/clear the port.
tag tag_no	It means to tag a number for the VLAN. -1: No need to add tag number. 1-4095: Available setting numbers used as tagged number.
service type	It means to specify the service type for VLAN. 0: Normal. 1: IGMP.
vlan priority	It means to specify the priority for the VALN setting. Range is from 0 to 7.
px	It means LAN port. Available setting number is from 2 to 4. Port number 1 is locked for NAT usage.
keeptag	It means Multi-VLAN packets will keep their VLAN headers to LAN.

Example

PVC 7 will map to LAN port 2/3/4 in bridge mode; service type is Normal. No tag added.

```
> > wan mvlan 7 on p2 p3 p4
PVC  Bridge  p1 p2 p3 p4 p5 p6   Service Type    Tag     Priority    Keep Tag
 ---------------------------------------------------------------------
   7  ON     0  0  1  1  0  0     Normal      0(OFF)     0       OFF
>
```

Telnet Command: wan multifno

This command allows you to specify a channel (in Multi-PVC/VLAN) to make bridge connection to a specified WAN interface.

Syntax

wan multifno *[channel #] [WAN interface #]*

wan multifno *status*

Syntax Description

Parameter	Description
channel #	There are 4 (?) channels including VLAN and PVC. Available settings are: 1=Channel 1 3=Channel 3 4=Channel 4 5=Channel 5
WAN interface #	Type a number to indicate the WAN interface. *1=WAN1* *2=WAN2*
status	It means to display current bridge status.

Example

```
> wan multifno 5 1
% Configured channel 5 uplink to WAN1
> wan multifno status
> wan multifno status
% Channel 5 uplink ifno: 3
% Channel 6 uplink ifno: 3
% Channel 7 uplink ifno: 3
% Channel 8 uplink ifno: 3
% Channel 9 uplink ifno: 3
>
```

Telnet Command: wan vlan

This command allows you to configure the VLAN tag of WAN1 or WAN2.

Syntax

wan vlan wan *[#]* **tag** *[value]*

wan vlan wan *[#] [enable/disable]*

wan vlan stat

Syntax Description

Parameter	Description
wan [#]	Specify which WAN interface will be tagged.
tag [value]	Type a number for tagging on WAN interface.
enable/disable	Enable: Specified WAN interface will be tagged. Disable: Disable the function of tagging on WAN interface.
stat	Display current VLAN status.

Example

```
> wan vlan stat

% Interface    Pri     Tag    Enabled
% ====================================
% WAN1 (ADSL)   0      0
% WAN1 (VDSL)   0      0
% WAN2         0      0
```

Telnet Command: wan phyvlan

This command is used to set VLAN tag insertion for outer tag (service) for WAN interface.

WAN interfaces must be configured first before setting VLAN encapsulation.

Syntax

wan phyvlan wan *[#]* **tag** *[value]*

wan phyvlan wan *[#]* **pri** *[value]*

wan phyvlan wan *[#] [enable|disable]*

wan phyvlan stat

Syntax Description

Parameter	Description
[#]	It means WAN interface. 1 – WAN1 2 – WAN2
tag [value]	It means to tag a value onto the selected WAN interface.
pri [value]	It means to set value for priority for such VLAN tag.
[enable|disable]	It means to enable / disable the VLAN tag.
stat	Display the setting status.

Example

```
> wan phyvlan wan 1 tag 22
% Set physical port tag to 22 for WAN1
% Set physical port tag to 22 for WAN1
% You need to reboot router making config effective
DrayTek> wan phyvlan stat ?
% Interface    Pri     Tag    Enabled
% ====================================
% WAN1         0       22
% WAN2         0        0
```

Telnet Command: wan budget

This command allows you determine the data *traffic volume* for each WAN interface respectively to prevent from overcharges for data transmission by the ISP.

Syntax

wan budget wan *[#] rdate [day] [hour]*

wan budget wan *[#] [enable|disable]*

wan budget wan *[#]* **thres** *[budget limit (MB)]*

wan budget wan *[#]* **gthres** *[budget limit (GB)]*

wan budget wan *[#]* **mode** *[monthly|periodic|none]*

wan budget wan *[#]* **psday** *[th day in periodic]*

wan budget wan *[#]* **action** *[action bitmap]*

wan budget status

Syntax Description

Parameter	Description

wan[#]	Specify the WAN interface.
rdate	Specify the WAN budget refresh time. day – Available settings are from 1 to 30. hour – Available settings are from 1 to 23. E.g., `wan budget wan 1 rdate 5 10` If monthy mode is selected: WAN budget will be refreshed on 5th day at 10:00 in each month If periodic mode is selected: WAN budget will be refreshed every 5 days and 10 hours
enable/disable	enable - Enable the function of wan budget. disable - Disable the function of wan budget.
thres [budget limit (MB)]	Specify the maximum value for WAN budget limit. (Unit: MB) budget limit – Type a number.
gthres [budget limit (GB)]	Specify the maximum value of wan budget limit. (Unit: GB) budget limit – Type a number.
mode [monthly|periodic|none]	Specify the calculation mode (monthly, periodically, or none) for WAN budget.
psday [th day in periodic]	It is used only when mode is set with "periodic". Specify the order of "today" in the cycle. E.g., `wan budget wan 5 psday` → It means "today" is the 5th day in the billing cycle.
action [action bitmap]	Determine the action to be performed when it reaches the WAN budget limit. *action bitmap* – Type a total number of actions to be executed. Different numbers represent different actions. 1: shotdown wan 2: send mail alert 4: send sms alert For example, if you type "5" (5=1+4), the system will send SMS alert when WAN shotdown is detected.
status	Display current configuration status of WAN budget.

Example

```
> wan budget wan 1 action 5
% WAN 1 budget action set to 5
> wan budget wan 1 gthres 10
% WAN 1 budget limit set to 10 GB
```

Telnet Command: wan detect_mtu

This command allows you to run a WAN MTU Discovery. The user can specify an IPv4 target to ping and find the suitable MTU size of the WAN interface.

Syntax

wan detect_mtu -w *[number]* **-i** *[Host/IP address]* **-s** *[base_size]* **-d** *[decrease_size] (-c [count])*

Syntax Description

Parameter	Description
-w [number]	Specify the WAN interface. Value: Type the number of WAN interface. 1: WAN1; 2:WAN2….and etc.
-I [Host/IP address]	Specify the IPv4 target to detect. If can be an IPv4 address or domain name. Host/IP address: Type the IP address/domain name of the target.
-s [base_size]	Set the MTU size base for Discovery. base_size: Available setting is 1000 ~ 1500.
-d [decrease size]	Set the MTU size to decrease between detections. decrease size: Available setting is 1 ~ 100.

-c [count]	Set the maximum times of ping failure during a Discovery. count: Available settings are 1 ~ 10. Default value is 3.

Example

```
> wan detect_mtu -w 2 -i 8.8.8.8 -s 1500 -d 30 -c 10
 detecting  mtu size:1500!!!

 mtu size:1470!!!
```

Telnet Command: wan detect_mtu6

This command allows you to run a WAN MTU Discovery. The user can specify an IPv6 target to ping and find the suitable MTU size of the WAN interface.

Syntax

wan detect_mtu6 -w *[number]* **-i** *[IPv6 address]* **-s** *[base_size]*

Syntax Description

Parameter	Description
-w [number]	Specify the WAN interface number: Type the number of WAN interface. 1: WAN1; 2:WAN2….and etc.
-I [IPv6 address]	Specify the IPv6 target to detect. It must be an IPv6 IP address. IPv6 address: Type the IPv6 address of the target.
-s [base_size]	Specify the size of MTU. base_size: Available setting is 1000 ~ 1500.

Example

```
> wan detect_mtu6 -w 2 -i 2404:6800:4008:c06::5e -s 1500
>
```

Telnet Command: failover

This command is used to configure failover WAN.

Syntax

wan failover off *[index]*

wan failover on *[1][2][3][4][5][6]*

wan failover show *[index]*

Syntax Description

Parameter	Description
failover off [index]	Set specified WAN interface to always on. index – Ranges from 1 to 4.
failover on [1][2][3][4][5][6]	There are six fields which represent different options. Field 1 – Specify WAN interface as failover WAN by typing 1 to 4. Field 2 – Enable / disable the action for the failover WAN. Such action is “Active When selected WAN [disconnect/reached traffic threshold]”. 0 – Disable 1 - Enable Field 3 - Enable / disable the action for the failover WAN. Such action is “Active When [any/all] of selected WAN disconnect or reached traffic threshold”.

	0 – Disable 1 - Enable Field 4 – Specify main WAN by typing 1 to 4. The main WAN will be set to always on. Field 5 – Specify traffic threshold [Download threshold(Kbps)]. Field 6 - Specify traffic threshold [Upload threshold (Kbps)]. For example, WAN 2 will be set as failover, and will be active when any of selected WANs has reached traffic threshold. WAN 4 is the selected WAN. Download threshold : 50 Kbpsl; Upload threshold : 20 Kbps. You can type as follows: *wan failover on 2 1 0 4 50 20*
show [index]	Display parameters settings for WAN interface. index – Ranges from 1 to 4.

Example

```
> wan failover on 2 1 0 4 50 20
> wan failover show 2
  wan2 Active Mode : Failover
       Active when : Any of the selected WANs reached the Traffic Threshold
       Traffic Download Threshold : 50 Kbps
       Traffic Upload Threshold   : 20 Kbps
> wan failover show 3
  wan3 Active Mode : Always ON.
```

Telnet Command: hsportal setup

This command is used to configure a profile (Hotspot Web Portal) with specified URL for accessing into or display a message when a wireless/LAN user connects to Internet through this router.

Syntax

hsportal -p <*profile*> *[-l <lan>] [-s <ssid>] …*

hsportal -p <*profile*> *-c*

Syntax Description

Parameter	Description
-p	Indicate available profile to be configured. Number of profile: 1 /2 /3 / 4.
-l	Apply to LAN interfaces. E.g., apply LAN1 and LAN2: -l 1, 2.
-s	Apply to WLAN interfaces. E.g., apply SSID1 and SSID2: -s 1, 2.
-a	Apply to WLAN5G interfaces. E.g., apply SSID1 and SSID2: -s 1, 2.
-m	Select login mode. 0:skip 1:click 2:social 3:pin 4:social or pin
-f	Configure facebook login. 0: disable. 1: enable.
-g	Configure google login. 0: disable. 1: enable.

-h	Enable HTTPS redirection. 0: disable. 1: enable.
-v	Enable portal detection. 0: disable. 1: enable.
-i	Configure APP id. For example, to configure facebook APP id, you can type: >hsportal -p 1 -f -i this_is_app_id Profile 1 set facebook login disabled … [OK]
-k	Configure app key. For example, to configure google APP key, you can type: > hsportal -p 1 -g -i this_is_app_key Profile 1 set google login disabled … [OK]
-r	Configure landing page mode. 0: fixed URL. 1: user request. 2: bulletin. E.g. > hsportal -p 1 -r 0 Profile 1 set landing page mode 0 … [OK]
-e	Enable the specified profile.
-d	Disable the specified profile.
-c	Reset the specified profile. Number of profile: 1 /2 /3 / 4.
-o	Clear profiles for all clients.

Example

```
> hsportal -p 1 -c
Reset profile 1 ... [OK]
> hsportal -p 1 -r 0
Profile 1 set landing page mode 0 ... [OK]
> hsportal -p 2 -g 1 -k app_key_google
Profile 2 set google login enabled ... [OK]
Profile 2 set API KEY   ... [OK]
>
```

Telnet Command: hsportal info

This command is used to enable /disable database, notification, specify object profile for information related to hotspot web portal users.

Syntax

hsportal info -e *[0/1]*

hsportal info -c

hsportal info -n *[0/1]*

hsportal info -a *[0/1]*

hsportal info -m *[1~10]*

hsportal info -s *[1~10]*

Syntax Description

Parameter	Description
-e [0/1]	Enable database to record information. 0 - disable 1 – enable
-c	Clear user information database.
-n [0/1]	Enable notification for user information.

	0 - disable 1 – enable
-a [0/1]	Enable auto backup and start a new record for user information. 0 - disable 1 – enable
-m [1~10]	Set email notigication object. [1~10]- Index number of object profile.
-s [1~10]	Set SMS notigication object. [1~10]- Index number of object profile.

Example

```
> hsportal info -e 1
Enabled database to record information ... [OK]
> hsportal info -a 1
Enabled auto backup and start a new record for user information ... [OK]
```

Telnet Command: wl acl

This command allows the user to configure wireless access control settings.

Syntax

wl acl enable *[ssid1 ssid2 ssid3 ssid4]*

wl acl disable *[ssid1 ssid2 ssid3 ssid4]*

wl acl add *[MAC] [ssid1 ssid2 ssid3 ssid4] [isolate]*

wl acl del *[MAC]*

wl acl mode *[ssid1 ssid2 ssid3 ssid4] [white/black]*

wl acl show

wl acl showmode

wl acl clean

Syntax Description

Parameter	Description
enable [ssid1 ssid2 ssid3 ssid4]	It means to enable the settings for SSID1, SSID2, SSID3 and SSID4.
disable [ssid1 ssid2 ssid3 ssid4]	It means to disable the settings for SSID1, SSID2, SSID3 and SSID4.
add [MAC] [ssid1 ssid2 ssid3 ssid4] [isolate]	It means to associate a MAC address to certain SSID interfaces' access control settings. The isolate setting will limit the wireless client's network capabilities to accessing the wireless LAN only. [MAC] format: xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx or xx.xx.xx.xx.xx.xx
del [MAC]	It means to delete a MAC address entry defined in the access control list.
mode [ssid1 ssid2 ssid3 ssid4] [white/black]	It means to set white/black list for each SSID.
wl acl show	It means to show access control status.
wl acl showmode	It means to show the mode for each SSID.

wl acl clean	It means to clean all access control setting.

Example

```
> > wl acl showmode
 ssid1: none
 ssid2: none
 ssid3: none
 ssid4: none
> wl acl add 00-50-70-ff-12-70
 Set Done !!
> wl acl add 00-50-70-ff-12-70 ssid1 ssid2 isolate
 Set Done !!
> wl acl show
 ----------Enable Mac Address Filter---------
 ssid1: dis   ssid2: dis   ssid3: dis   ssid4: dis
 ----------MAC Address Filter----------
 Index   Attribute      MAC Address        Associated SSIDs
   0                  00:50:70:ff:12:70   ssid1 ssid2 ssid3 ssid4
   1       s          00:50:70:ff:12:70   ssid1 ssid2

 s: Isolate the station from LAN
>
```

Telnet Command: wl config

This command allows users to configure general settings and security settings for wireless connection.

Syntax

wl config mode *[value]*

wl config mode show

wl config channel *[number]*

wl config preamble *[enable]*

wl config txburst *[enable]*

wl config ssid *[ssid_num enable ssid_name [hidden_ssid]]*

wl config security *[SSID_NUMBER] [mode]*

wl config ratectl *[ssid_num enable upload download]*

wl config isolate *[ssid_num lan member]*

Syntax Description

Parameter	Description
mode[value]	It means to select connection mode for wireless connection. Available settings are: "11bgn", "11gn", "11n", "11bg", "11g", or "11b".
mode show	It means to display what the current wireless mode is.
channel [number]	It means the channel of frequency of the wireless LAN. The available settings are 0,1,2,3,4,5,6,7,8,9,10,11,12 and 13. number=0, means Auto number=1, means Channel 1

	…. number=13, means Channel 13.
preamble [enable]	It means to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. 0: disable to use long preamble. 1: enable to use long preamble.
txburst [enable]	It means to enhance the performance in data transmission about 40%* more (by enabling **Tx Burst**). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. 0: disable the function. 1: enable the funciton.
ssid[ssid_num enable ssid_name [hidden_ssid]]	It means to set the name of the SSID, hide the SSID if required. *ssid_num:* Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *ssid_name*: Give a name for the specified SSID. *hidden_ssid*: Type 0 to hide the SSID or 1 to display the SSID
Security [SSID_NUMBER] [mode][key][index]	It means to configure security settings for the wirelesss connection. *SSID_NUMBER*: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *mode*: Available settings are: disable: No security. wpa1x: WPA/802.1x Only wpa21x: WPA2/802.1x Only wpamix1x: Mixed (WPA+WPA2/802.1x only) wep1x: WEP/802.1x Only wpapsk: WPA/PSK wpa2psk: WPA2/PSK wpamixpsk: Mixed (WPA+WPA2)/PSK wep: WEP *key, index*: Moreover, you have to add keys for *wpapsk, wpa2psk, wpamixpsk* and *wep*, and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8~63 ASCII text string or 64 Hexadecimal digit format.
ratectl [ssid_num enable upload download]	It means to set the rate control for the specified SSID. *ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *enable*: It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable. *upload*: It means to configure the rate control for data upload. The unit is kbps. *download*: It means to configure the rate control for data download. The unit is kbps.
isolate [ssid_num lan member]	It means to isolate the wireless connection for LAN and/or Member. *lan* – It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other. *member* – It can make the wireless clients (stations) with the same SSID not accessing for each other.

Example

```
> wl config mode 11bgn
```

```
 Current mode is 11bgn
% <Note> Please restart wireless after you set the channel
> wl config channel 13
 Current channel is 13
% <Note> Please restart wireless after you set the channel.
> wl config preamble 1
 Long preamble is enabled
% <Note> Please restart wireless after you set the parameters.
> wl config ssid 1 enable dray
 SSID  Enable  Hide_SSID  Name
 1     1       0         dray
% <Note> Please restart wireless after you set the parameters.
> wl config security 1 wpa1x
%% Configured Wlan Security Setting:
% SSID1
%%  Mode: wpa1x
%% Wireless card must be reset for configurations to take effect
%% (Telnet Command: wl restart)
```

Telnet Command: wl set

This command allows users to configure basic wireless settings.

Syntax

wl set *[SSID] [CHAN[En]]*

wl set txburst *[enable]*

Syntax Description

Parameter	Description
SSID	It means to type the SSID for the router. The maximum character that you can use is 32.
CHAN[En]	It means to specify required channel for the router. *CHAN:* The range for the number is between 1 ~ 13. *En*: type *on* to enable the function; type *off* to disable the function.
txburst [enable]	It means to enhance the performance in data transmission about 40%* more (by enabling **Tx Burst**). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. 0: disable the function. 1: enable the function.

Example

```
> wl set MKT 2 on
% New Wlan Setting is:
% SSID=MKT
% Chan=2
% Wl is Enable
```

Telnet Command: wl act

This command allows users to activate wireless settings.

Syntax

wl act *[En]*

Syntax Description

Parameter	Description
En	It means to enable or disable the function of VPN isolation. 0: diable 1: enable

Example

```
> wl act on
% Set Wlan to Enable.
```

Telnet Command: wl scan

This command allows users to perform AP scanning.

Syntax

wl scan *[start]*

wl scan *set [wlist/blist/stime][MAC]*

wl scan *del [wlist/blist] [MAC]*

wl scan *filter [ssid/channel/mac]*

wl scan *show [0/1/2/3]*

Syntax Description

Parameter	Description
start	It means to start AP scanning.
set [wlist/blist/stime] [MAC]	Set white list/block list/scan time. *wlist* – It means to set white list for passing. MAC address must be added in the end. e.g., *wl scan set wlist 001122aabbcc* *blist* – It means to set black list for blocking. MAC address must be added in the end. *stime* – It means to set scanning time. Time value (2~5 second) must be added in the end. e.g., *wl scan set time 5*
del	Remove white list/block list. e.g., *wl scan del wlist 001122aabbcc*
filter	Set which filter you want. *ssid* – scanning the AP based on SSID setting. *channel* - scanning the AP based on channel setting. *mac* - scanning the AP based on MAC address setting..
show [0/1/2/3]	It is used to show AP list. 0 - display white list 1 - display block list,

	2 - display gray/unknown list, 3 - display all list

Example

```
> wl scan set wlist 001122aabbcc
> wl scan start
> wl scan show 3
>
```

Telnet Command: wl stamgt

This command is used to configure connection time and reconnection time for each SSID that wireless client used for accessing into Internet.

Syntax

wl stamgt *[enable/disable] [ssid_num].*

wl stamgt *[show] [ssid_num].*

wl stamgt set *[ssid_num] [c] [r]*

wl stamgt reset *[ssid_num].*

Syntax Description

Parameter	Description
enable/disable	It means to enable/disable the station management control.
ssid_num	It means channel selection. Available channel for 2.4G: 0/1/2/3 Available channel for 5G: 4/5/6/7.
show	It means to display status or configuration of the selected channel.
c	It means connection time. The unit is minute.
r	It means reconnection time. The unit is minute.

Example

```
> wl stamgt enable 1
% Station Management Status: enabled
> wl stamgt set 1 60 60
> wl stamgt show 1
NO. SSID           BSSID              Connect time  Reconnect time
1.  Draytek     00:11:22:aa:bb:cc  0d:0:58:26     0d:0:0
```

Telnet Command: wl iso_vpn

This command allows users to activate the function of VPN isolation.

Syntax

wl iso_vpn *[ssid] [En]*

Syntax Description

Parameter	Description
ssid	It means the number of SSID.

	1: SSID1 2: SSID2 3: SSID3 4: SSID4
En	It means to enable or disable the function of VPN isolation. 0: disable 1: enable

Example

```
> wl iso_vpn 1 on
% ssid: 1 isolate vpn on :1
```

Telnet Command: wl wpa

This command allows you to configure WPA wireless settings.

Syntax

wl wpa *1/2/3*

Syntax Description

Parameter	Description
wl wpa	Type 1/2/3 to represent different WPA modes. 1 – means WPA+WPA2 2 – means WPA2 Only 3 – means WPA Only

Example

```
> wl wpa 1
>
```

Telnet Command: wl wmm

This command allows users to set WMM for wireless connection. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs).

Syntax

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 enable *SSID0 SSID1 SSID2 SSID3*

wl wmm apsd *value*

wl wmm show

Syntax Description

Parameter	Description
ap	It means to set WMM for access point.
bss	It means to set WMM for wireless clients.
ack	It means to map to the Ack policy settings of AP WMM.

enable	It means to enable the WMM for each SSID. 0: disable 1: enable
Apsd [value]	It means to enable / disable the ASPD(automatic power-save delivery) function. 0: disable 1: enable
show	It displays current status of WMM.
QueIdx	It means the number of the queue which the WMM settings will be applied to. There are four queues, best effort, background, voice, and video.
Aifsn	It controls how long the client waits for each data transmission.
Cwmin/ Cwmax	**CWMin** means contention Window-Min and **CWMax** means contention Window-Max. Specify the value ranging from 1 to 15.
Txop	It means transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It can restrict stations from using specific category class if it is enabled. 0: disable 1: enable

Example

```
> wl wmm ap 0 3 4 6 0 0
 QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
> wl wmm enable 1 0 1 0
 WMM_SSID0 =1, WMM_SSID1 =0,WMM_SSID2 =1,WMM_SSID3 =0
> wl wmm show
 Enable 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
```

Telnet Command: wl ht

This command allows you to configure wireless settings.

Syntax

wl ht bw *value*

wl ht gi *value*

wl ht badecline *value*

wl ht autoba *value*

wl ht rdg *value*

wl ht msdu *value*

wl ht txpower *value*

wl ht antenna *value*

wl ht greenfield *value*

Syntax Description

Parameter	Description
wl ht bw value	The value you can type is 0 (for BW_20) and 1 (for BW_40).
wl ht gi value	The value you can type is 0 (for GI_800) and 1 (for GI_4001)
wl ht badecline value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht autoba value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht rdg value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht msdu value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht txpower value	The value you can type ranges from 1 – 6 (level).
wl ht antenna value	The value you can type ranges from 0-3. 0: 2T3R 1: 2T2R 2: 1T2R 3: 1T1R
wl ht greenfield value	The value you can type is 0 (for mixed mode) and 1 (for green field).

Example

```
> wl ht bw value 1
 BW=0
 <Note> Please restart wireless after you set new parameters.
> wl restart
 Wireless restart.................
```

Telnet Command: wl restart

This command allows you to restart wireless setting.

Example

```
> wl restart
 Wireless restart.............
```

Telnet Command: wl wds

This command allows you to configure WDS settings.

Syntax

wl wds mode *[value]*

wl wds security *[value]*

wl wds ap *[value]*

wl wds hello *[value]*

wl wds status

wl wds show

wl wds mac *[value]*

wl wds flush

Syntax Description

Parameter	Description
mode [value]	It means to specify connection mode for WDS. [value]: Available settings are : d: Disable b: Bridge r: Repeapter
security [value]	It means to configure security mode with encrypted keys for WDS. *mode*: Available settings are: disable: No security. wep: WEP wpapsk [key]: WPA/PSK wpa2psk [key]: WPA2/PSK *key*: Moreover, you have to add keys for *wpapsk, wpa2psk,* and *wep*, and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8~63 ASCII text string or 64 Hexadecimal digit format. e.g., *wl dual wds security disable* *wl dual wds security wep 12345* *wl dual wds security wpa2psk 12345678*
ap [value]	It means to enable or disable the AP function. Value: 1 – enable the function. 0 – disable the function.
hello [value]	It means to send hello message to remote end (peer). Value: 1 – enable the function.

	0 – disable the function.
status	It means to display WDS link status for 2.4GHz connection.
show	It means to display current WDS settings.
mac add [index addr]	add *[index addr]* – Add the peer MAC entry in Repeater/Bridge WDS MAC table.
mac clear/disable/enable [index/all]	clear/disable/enable *[index/all]*- Clear, disable, enable the specifed or all MAC entries in Repeater/Bridge WDS MAC table. e.g, `wl dual wds mac enable 1`
flush	It means to reset all WDS setting.

Example

```
> wl wds status
Please enable WDS hello function first.

> wl wds hello 1
% <Note> Please restart router after you set the parameters.

> wl wds status
```

Telnet Command: wl apcli

This command allows users to configure AP client mode for wireless connection (2.4GHz).

Syntax

wl apcli show

wl apcli enable *[1/0]*

wl apcli security *[mode]*

wl apcli ssid *[ssid_name]*

wl apcli bssid *[mac address]*

Syntax Description

Parameter	Description
show	Display current status of wireless AP client.
enable [1/0]	It means to enable wireless 2.4GHz AP client mode. 1 – enable 0 – disable
security [mode]	There are several modes to be selected: Disable – disable the security settings. wpapsk [key] – WPA Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8~63 ASCII string or 64 Hexadecimal digit format. wpa2psk [key] – WPA2 Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8~63 ASCII string or 64 Hexadecimal digit format. wpamixpsk [key] – WPA Mixed Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8~63 ASCII string or 64 Hexadecimal digit format. wep [key] [index] – WEP key will be used. You need to type the key

	string and specify the index number of the profile to be applied. WEP keys must be in 5/13 ASCII string or 10/26 Hexadecimal digit format.
ssid [ssid_name]	Specify the SSID for wireless 2.4GHz AP client.
bssid	Type the MAC address for wireless 2.4GHz AP client.

Example

```
> wl apcli enable 1
Wireless AP-Clinet is enabled
> wl apcli show
% Wireless AP-Clinet is enabled
% Current SSID is test
%%  Security Mode: disable
% Wireless client is disconnected
%% data rate=---, mode=---, signal=0%
```

Telnet Command: wl btnctl

This command allows you to enable or disable wireless button control.

Syntax

wl btnctl *[value]*

Syntax Description

Parameter	Description
value	0: disable 1: enable

Example

```
> wl btnctl 1
Enable wireless botton control
Current wireless botton control is on
>
```

Telnet Command: wl iwpriv

These command is reserved for RD debug. Do not use it.

Telnet Command: wl stalist

This command is used to display the wireless station which accessing Internet via Vigor router.

Syntax

wl stalist

Example

```
> wl stalist
wl stalist show    : show station list
wl stalist num     : show number of stations
wl stalist neighbor : show neighbor station list
```

Telnet Command: wl set8021x

This command allows you to configure the external or internal server used by Vigor router for wireless authentication.

Syntax

wl set8021x -t *[0/1]*

wl set8021x -v

Syntax Description

Parameter	Description
-t	Specify the type (external or internal) of wireless authentication server. 0 – Indicate the external RADIUS server. 1- Indicate the local 802.1x server.
-v	View the settings of 802.1x.

Example

```
> wl set8021x -t 1
% <Note> Please restart wireless after you set the parameters.
> wl set8021x -v
 802.1X type is : Local 802.1X
>
```

Telnet Command: wl bndstrg

This command allows users to configure settings for Band Steering (2.4GHz).

Syntax

wl bndstrg show

wl bndstrg enable *[1/0]*

wl bndstrg chk_time *[value]*

Syntax Description

Parameter	Description
show	Display current status for Band Steering function.
enable [1/0]	It means to enable wireless 2.4GHz AP client mode. 1 – enable 0 – disable
chk_time [value]	If the wireless station does not have the capability of 5GHz network connection, the system shall wait and check for several seconds (15 seconds, in default) to make the 2.4GHz network connection. Specify the time limit for Vigor router to detect the wireless client. *[value] – 1 to 60 seconds.*

Example

```
> wl bndstrg show
band steering: disable
chk_time: 15 sec
```

```
> wl bndstrg chk_time 50 30
argv[0]:chk_time, argv[1]:50, argv[2]:30

%% Wireless card must be reset for configurations to take effect
%% (Telnet Command: wl restart)
```

Telnet Command: wl artfns

This command allows users to configure airtime fairness function for wireless (2.4GHz) connection.

Syntax

wl artfns enable *[value]*

wl artfns trg_num *[value]*

wl artfns show

Syntax Description

Parameter	Description
enable [value]	It means to enable wireless airtime fairness function. 1 – enable 0 – disable
Trg_num [value]	Set a threshold when the active station number achieves this number, the airtime fairness function will be applied. Available values will be 2 to 64.
show	Display current status (enable or disable) and triggering client number for airtime fairness function.

Example

```
> wl artfns enable 1
> wl artfns trg_num 3
> wl artfns show
airtime fairness: enable
trg_num: 3
>
```

Telnet Command: wl drayrs

This command allows the user to configure settings for Roaming for wireless clients.

Syntax

wl drayrs *set [mode] [rs_low] [rs_low_security] [delta]*

wl drayrs *restart*

wl drayrs *show*

Syntax Description

Parameter	Description
set [mode] [rs_low] [rs_low_security] [delta]	Select a mode for roaming. 0 - disable 1 - Strictly Minimum RSSI 2 - Minimum RSSI

	rs_low – Set a value of Strictly Minimum RSSI (62~86). rs_low_security – Set a value of Minimum RSSI (62~86). delta – Set a value of Adjacent AP RSSI (1~20).
restart	Restart to activate roaming function.
show	Dispaly current configuration of roaming function.

Example

```
> wl drayrs show
% Mode : Disable
%  rs_low         : -73
%  rs_low_secure  : -66
%  delta          : 5
>
```

Telnet Command: wl_dual acl

This command allows the user to configure wireless (5GHz) access control settings.

Syntax

wl dual acl enable *[ssid1 ssid2 ssid3 ssid4]*

wl dual acl disable*[ssid1 ssid2 ssid3 ssid4]*

wl dual acl add *[MAC][ssid1 ssid2 ssid3 ssid4][isolate]*

wl dual acl del *[MAC]*

wl dual acl mode *[ssid1 ssid2 ssid3 ssid4] [white/black]*

wl dual acl show

wl dual acl showmode

wl dual acl clear

Syntax Description

Parameter	Description
enable [ssid1 ssid2 ssid3 ssid4]	It means to enable the settings for SSID1, SSID2, SSID3 and SSID4.
disable [ssid1 ssid2 ssid3 ssid4]	It means to disable the settings for SSID1, SSID2, SSID3 and SSID4.
add [MAC] [ssid1 ssid2 ssid3 ssid4] [isolate]	It means to associate a MAC address to certain SSID interfaces' access control settings. The isolate setting will limit the wireless client's network capabilities to accessing the wireless LAN only. [MAC] format: xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx or xx.xx.xx.xx.xx.xx
isolate	It means to isolate the wireless connection of the wireless client (identified with the MAC address) from LAN.
del[MAC]	It means to delete a MAC address entry defined in the access control list. [MAC] format: xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx or xx.xx.xx.xx.xx.xx
mode [ssid1 ssid2 ssid3 ssid4] [white/black]	It means to set white/black list for each SSID.

show	It means to display current status of access control.
showmode	It means to show the mode for each SSID.
clear	It means to clear all of the access control settings.

Example

```
> wl_dual acl showmode
 SSID1: None
 SSID2: None
 SSID3: None
 SSID4: None
>wl_dual acl add 00-50-70-ff-12-80
> wl_acl add 00-50-70-ff-12-80 ssid1 ssid2 isolate
 Set Done !!
> wl_acl show
 ----------Enable Mac Address Filter---------
 ssid1: dis   ssid2: dis   ssid3: dis   ssid4: dis
 ----------MAC Address Filter----------
 Index   Attribute      MAC Address        Associated SSIDs
   0       s          00:50:70:ff:12:80   ssid1 ssid2

 s: Isolate the station from LAN
```

Telnet Command: wl_dual apscan

This command is used to scan Access Point installed near the location of Vigor router.

Syntax

wl_dual apscan *start*

wl_dual apscan *show*

Syntax Description

Parameter	Description
start	It means to execute the AP scanning.
show	It means to display the content of the AP list.

Example

```
> wl_dual apscan start
> wl_dual apscan show
 AP scan is ongoing.
> wl_dual apscan ?
% wl_dual apscan [start/show]
% start: do AP scan
% show: show AP list

> wl_dual apscan show
5G Access Point List :
BSSID            Channel   SSID
```

Telnet Command: wl_dual cardmac

Example

```
> wl_dual cardmac
Card MAC: 54:2a:a2:37:00:ef
```

Telnet Command: wl_dual config

This command allows users to configure general settings and security settings for wireless connection (5GHz).

wl_dual config enable *[value]*

wl dual config enable show

wl_dual config mode *[value]*

wl_dual config mode show

wl_dual config channel *[number]*

wl_dual config channel show

wl_dual config preamble *[enable]*

wl_dual config preamble show

wl_dual config ssid *[ssid_num enable ssid_name]*

wl_dual config ssid hide *[ssid_num enable]*

wl_dual config ssid show

wl_dual config ratectl *[ssid_num enable upload download]*

wl_dual config ratectl show

wl_dual config isolate lan *[ssid_num enable]*

wl_dual config isolate member *[ssid_num enable]*

wl_dual config isolate vpn *[ssid_num enable]*

wl_dual config isolate show

Syntax Description

Parameter	Description
enable[value]	It means to enable/disable the 5GHz wireless function. 1: enable 0: disable
show	It means to display if 5G wireless function is enabled or not.
mode[value]	It means to select connection mode for wireless connection. Available settings are: "11a", "11n_5g", "11n" and "11an".
mode show	It means to display what the current wireless mode is.
channel [number]	It means the channel of frequency of the wireless LAN. The available settings are: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 and 140. number=0, means Auto number=36, means Channel 36 …. Number=52, means Channel 52.
channel show	It means to display what the current channel is.

preamble [enable]	It means to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. 0: disable to use long preamble. 1: enable to use long preamble.
preamble show	It means to display if preamble is enabled or not.
ssid[ssid_num enable ssid_name]	It means to set the name of the SSID, hide the SSID if required. *ssid_num:* Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *ssid_name*: Give a name for the specified SSID.
ssid hide [ssid_num enab le]	It means to hide the name of the SSID if required. *ssid_num:* Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. enable: Type 0 to hide the SSID or 1 to display the SSID.
ssid show	It means to display a table of SSID configuration.
ratectl [ssid_num enable upload download]	It means to set the rate control for the specified SSID. *ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *enable*: It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable. *upload*: It means to configure the rate control for data upload. The unit is kbps. *download*: It means to configure the rate control for data download. The unit is kbps. (example: *wl dual config ratectl 1 1 25 25*)
ratectl show	It means to display the data transmission rate (upload and download) for SSID1, SSID2, SSID3 and SSID4.
isolate lan [ssid_num enable]	It means to isolate the wireless connection from LAN. It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other. *ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *enable*: It means to enable such function. 0: disable and 1:enable
isolate member [ssid_num enable]	It means to isolate the wireless connection from Member. It can make the wireless clients (stations) with the same SSID not accessing for each other. *ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *enable*: It means to enable such function. 0: disable and 1:enable.
isolate vpn [ssid_num enable]	It means to isolate the wireless connection from VPN. *ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *enable*: It means to enable such function. 0: disable and 1:enable.
isolate show	It means to display the status of wireless isolation.

Example

```
> wl_dual config mode 11a
 Current mode is 11a
% <Note> Please restart 5G wireless after you set the channel
> wl_dual config channel 60
 Current channel is 60
% <Note> Please restart 5G wireless after you set the channel.
```

```
> wl_dual config preamble 1
Long preamble is enabled
% <Note> Please restart 5G wireless after you set the parameters.
> wl_dual config ssid 1 enable dray
SSID  Enable  Hide_SSID  Name
 1    1      0         dray
% <Note> Please restart 5G wireless after you set the parameters.
> wl_dual config ssid show
 SSID  Enable  Hide_SSID  Name
 1    1      0         dray
 2    0      0         DrayTek_5G_Guest
 3    0      0
 4    0      0
```

Telnet Command: wl_dual restart

This command allows you to restart wireless setting (5GHz).

Example

```
> wl_dual restart
 5G wireless restart.................
```

Telnet Command: wl_dual security

This command allows users to configure security settings for the wireless connection (5GHz).

Syntax

wl_dual security*[SSID_NUMBER] [mode][key][index]*

wl_dual security show

Syntax Description

Parameter	Description
Security [SSID_NUMBER] [mode][key][index]	*SSID_NUMBER*: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *mode*: Available settings are: disable: No security. wpa1x: WPA/802.1x Only wpa21x: WPA2/802.1x Only wpamix1x: Mixed (WPA+WPA2/802.1x only) wep1x: WEP/802.1x Only wpapsk: WPA/PSK wpa2psk: WPA2/PSK wpamixpsk: Mixed (WPA+WPA2)/PSK wep: WEP *key, index*: Moreover, you have to add keys for *wpapsk, wpa2psk, wpamixpsk* and *wep*, and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8~63 ASCII text string or 64 Hexadecimal digit format.
show	It means to display current mode selection for each SSID.

Example

```
> wl_dual security 1 wpa2psk 123456789e
% <Note> Please restart 5G wireless after you set the parameters.

> wl_dual security show
%% 5G Wireless LAN Security Settings:
% SSID1
%%  Mode: WPA2/PSK
% SSID2
%%  Mode: Disable
% SSID3
%%  Mode: Disable
% SSID4
%%  Mode: Disable
```

Telnet Command: wl_dual stalist

This command is used to display the wireless station which accessing Internet via Vigor router.

Syntax

wl dual stalist

Example

```
> wl_dual stalist
5G Wireless Station List :

Index  Status  IP Address       MAC Address       Associated with


Status Codes :
C: Connected, No encryption.
E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control.
N: Connecting.
F: Fail to pass WPA/PSK authentication.
```

Telnet Command: wl_dual wds

This command allows users to configure WDS for wireless connection (5GHz).

Syntax

wl_dual wds mode *[value]*

wl_dual wds security *[value]*

wl_dual wds ap *[value]*

wl_dual wds hello *[value]*

wl_dual wds status

wl_dual wds show

wl_dual wds mac add *[index addr]*

wl_dual wds mac clear/disable/enable *[index/all]*

wl_dual wds flush

Syntax Description

Parameter	Description
mode *[value]*	It means to specify connection mode for WDS. [value]: Available settings are : d: Disable b: Bridge r: Repeapter
security *[value]*	It means to configure security mode with encrypted keys for WDS. *mode*: Available settings are: disable: No security. wep: WEP wpapsk [key]: WPA/PSK wpa2psk [key]: WPA2/PSK *key*: Moreover, you have to add keys for *wpapsk, wpa2psk,* and *wep*, and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8~63 ASCII text string or 64 Hexadecimal digit format. e.g., *wl_dual wds security disable* *wl_dual wds security wep 12345* *wl_dual wds security wpa2psk 12345678*
ap *[value]*	It means to enable or disable the AP function. Value: 1 – enable the function. 0 – disable the function.
hello *[value]*	It means to send hello message to remote end (peer). Value: 1 – enable the function. 0 – disable the function.
status	It means to display WDS link status for 5GHz connection.
show	It means to display current WDS settings.
mac add *[index addr]*	**add** *[index addr]* – Add the peer MAC entry in Repeater/Bridge WDS MAC table.
mac clear/disable/enable *[index/all]*	**clear/disable/enable** *[index/all]*- Clear, disable, enable the specifed or all MAC entries in Repeater/Bridge WDS MAC table. e.g, *wl_dual wds mac enable 1*
flush	It means to reset all WDS setting.

Example

```
> wl_dual wds status
Please enable WDS hello function first.

> wl_dual wds hello 1
% <Note> Please restart router after you set the parameters.
```

```
> wl dual wds mode b
> wl dual wds security wep
>
>
> wl_dual wds show
5G Wireless WDS Setting

Mode : Bridge
Security : WEP
AP Function : Enable
Send Hello Function : Enable

Bridge :
Index  Enable  MAC Address
  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

Repeater :
Index  Enable  MAC Address
  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
% <Note> Please restart router after you set the parameters.
```

Telnet Command: wl_dual wps

This command allows users to configure WPS for wireless connection (5GHz).

Syntax

wl_dual wps enable *[value]*

wl dual wps pbc

wl_dual wps pin *[code]*

wl_dual wps show

Syntax Description

Parameter	Description
enable [value]	It means to enable WPS. 1 – enable 0 – disable
pbc	It means to start WPS by pressing the WLAN ON/OFF WPS button on Vigor router.
pin [code]	It means to start WPS by using client PIN code. [code]: Client PIN code (digit number).
show	It means to display current WPS settings.

Example

```
> wl_dual wps enable 1
 WPS is enabled.
> wl_dual wps pin 88563337
 WPS has triggered by PIN code.
 The AP will wait for WPS request from your client for 2 minutes...
```

Telnet Command: wl_dual set8021x

This command allows you to configure the external or internal server used by Vigor router for wireless authentication (5GHz).

Syntax

wl_dual set8021x -t *[0/1]*

wWl_dual set8021x -v

Syntax Description

Parameter	Description
-t	Specify the type (external or internal) of wireless authentication server. 0 – Indicate the external RADIUS server. 1- Indicate the local 802.1x server.
-v	View the settings of 802.1x.

Example

```
> wl_dual set8021x -t 1
% <Note> Please restart 5G wireless after you set the parameters.
> wl_dual set8021x -v
 802.1X type is : Local 802.1X
>
```

Telnet Command: wl_dual apcli

This command allows users to configure AP client mode for wireless connection (5GHz).

Syntax

wl_dual apcli show

wl_dual apcli enable *[value]*

wl_dual apcli security *[mode]*

wl_dual apcli ssid *[ssid_name]*

wl_dual apcli bssid

Syntax Description

Parameter	Description
show	Display current status of wireless AP client.
enable [value]	It means to enable wireless 5GHz AP client mode. 1 – enable 0 – disable
Security [mode]	There are several modes to be selected:

	Disable – disable the security settings. wpapsk [key] – WPA Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8~63 ASCII string or 64 Hexadecimal digit format. wpa2psk [key] – WPA2 Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8~63 ASCII string or 64 Hexadecimal digit format. wpamixpsk [key] – WPA Mixed Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8~63 ASCII string or 64 Hexadecimal digit format. wep [key] [index] – WEP key will be used. You need to type the key string and specify the index number of the profile to be applied. WEP keys must be in 5/13 ASCII string or 10/26 Hexadecimal digit format.
ssid [ssid_name]	Specify the SSID for wireless 5GHz AP client.
bssid	Type the MAC address for wireless 5GHz AP client.

Example

```
> wl_dual apcli enable 1
Wireless 5G AP-Clinet is enabled
Vigor> wl_dual apcli show
% Wireless 5G AP-Clinet is enabled
% Current SSID is
%%  Security Mode: disable
% Wireless 5G client is disconnected
%% data rate=---, mode=---, signal=0%
> wl_dual apcli ssid carrie
% <Note> Please restart wireless 5g after you set the parameters.
 Current SSID is carrie
```

Telnet Command: wl_dual artfns

This command allows users to configure airtime fairness function for wireless (5GHz) connection.

Syntax

wl_dual artfns enable *[value]*

wl_dual artfns trg_num *[value]*

wl_dual artfns show

wl_dual artfns status

Syntax Description

Parameter	Description
enable [value]	It means to enable wireless airtime fairness function. 1 – enable 0 – disable
Trg_num [value]	Set a threshold when the active station number achieves this number, the airtime fairness function will be applied. Available values will be 2 to 64.

show	Display current status (enable or disable) and triggering client number for airtime fairness function.
status	Display whether the function of airtime fairness is enabled or disabled.

Example

```
> wl_dual artfns show
airtime fairness for 5G: disable
trg_num: 2
> wl_dual artfns status
airtime fairness for 5G is disabled !!!

> wl_dual artfns enable 0
> wl_dual artfns trg_num 2
> wl_dual artfns show
airtime fairness for 5G: disable
trg_num: 2
> wl_dual artfns status
airtime fairness for 5G is disabled !!!
```

Telnet Command: wl_dual drayrs

This command allows the user to configure settings for Roaming for wireless clients.

Syntax

wl_dual drayrs *set [mode] [rs_low] [rs_low_security] [delta]*

wl_dual drayrs *restart*

wl_dual drayrs *show*

Syntax Description

Parameter	Description
set [mode] [rs_low] [rs_low_security] [delta]	Select a mode for roaming. 0 - disable 1 - Strictly Minimum RSSI 2 - Minimum RSSI rs_low – Set a value of Strictly Minimum RSSI (62~86). rs_low_security – Set a value of Minimum RSSI (62~86). delta – Set a value of Adjacent AP RSSI (1~20).
restart	Restart to activate roaming function.
show	Dispaly current configuration of roaming function.

Example

```
> wl_dual drayrs show
% Mode : Disable
%  rs_low         : -73
%  rs_low_secure  : -66
%  delta          : 5
>wl_dual drayrs set 1 68 66 2
```

```
> wl_dual drayrs show
% Mode : Strictly Minimun RSSI
%  rs_low        : -68
%  rs_low_secure  : -66
%  delta         : 2
```

Telnet Command: radius

This command allows you to configure detailed settings for RADIUS server

Syntax

radius enable *[0/1]*

radius authport *[port number]*

radius set_auth_method *[method idx]*

radius client *[add] [idx] -i [address] -m [mask] -p [prefix] -l [length] -s [secret]*

radius client *[del] [idx]*

radius show

radius set_dot1x_phase1 -e *[method_idx]*

radius set_dot1x_phase1 -d *[method_idx]*

radius set_dot1x_phase2 -e *[method_idx]*

radius set_dot1x_phase2 -d *[method_idx]*

Syntax Description

Parameter	Description
enable[0/1]	Enable (1) or disable (0) the RADIUS server.
authport [port number]	Configure the port number for authentication. Port number: Available range is from 0 to 65535. Default value is “1812”.
set_auth_method [method idx]	Specify which method will be used for authentication. Method idx: “0” is “Only PAP”; “1” is “PAP/CHAP/MS-CHAP/MS-CHAPv2”.
client add	Specify a client to be authenticated by RADIUS server by typing required information as follows: -i [address]: client IPv4 address(domain) -m [mask]: client IPv4 mask -p [prefix]: client IPv6 prefix -l [length]: client IPv6 prefix length -s [secret]: shared secret ex: radius client add 1 -i 192.168.1.1 -m 255.255.255.0 -s 123
client [del] [idx]	*del* - Delete related settings for selected client. *Idx* - Specify the index number of client profiles.
show	Display the status of RADIUS server.
enable_dot1x [0/1]	Enable (1) or disable (0) the 802.1X Authentication function of RADIUS Server. Default is disabled.
set_dot1x_phase1 [method_idx]	Set the phase1 method for 802.1X authentication of RADIUS server. *method_idx* - Specify which method will be used. At present, dot1x_phase1 can only support PEAP now. So only “1” can be used for it.
set_dot1x_phase2	Set the phase2 method for 802.1X authentication of RADIUS server.

[method_idx]	*method_idx* - Specify which method will be used. Dot1x_phase2 can only support MS-CHAPv2 now. So only "1" can be used for it.
-e	Set method for dot1x_phase1 or dot1x_phase2.
-d	Delete method for dot1x_phase1 or dot1x_phase2.

Example

```
> radius client add 1 -i 192.168.1.1 -m 255.255.255.0 -s 123
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: local_8021x

The command is used to configure general settings for Local 802.1X server built in Vigor router.

Syntax

local_8021x enable *[0/1]*

local_8021x set_localdot1x_phase1 options…

local_8021x set_localdot1x_phase2 options…

local_8021x show

Syntax Description

Parameter	Description
enable	Enable or disable the configuration. 0: disable. 1: enable.
set_localdot1x_phase1	Only support PEAP now. The method_idx for such phase1 is "1".
set_localdot1x_phase2	Only support MS-CHAPv2 now. The method_idx for such phase2 is "1".
options	-e [method_idx]: set method. e.g, local_8021x set_localdot1x_phase1 -e 1 -d: delete mehod. e.g, local_8021x set_localdot1x_phase1 -d
show	Display current settings of local 802.1x server.

Example

```
> local_8021x show
% Local 802.1X enable: enable
% phase1 support method: [PEAP]
% phase2 support method: [None]
```

Telnet Command: wol

This command allows Administrator to set the white list of WAN IP addresses/Subnets, that the magic packet from these IP addresses/Subnets will be eligible to pass through NAT and wake up the LAN client. You also need to set NAT rule for LAN client.

Syntax

wol up *[MAC Address]/[IP Address]*

wol fromWan *[on/off/any]*

wol fromWan_Setting *[idx][ip address][mask]*

Syntax Description

Parameter	Description
MAC Address	It means the MAC address of the host.
IP address	It means the LAN IP address of the host. If you want to wake up LAN host by using IP address, be sure that that IP address has been bound with the MAC address (IP BindMAC).
on/off/any	It means to enable or disable the function of WOL from WAN. on: enable off: disable any: It means any source IP address can pass through NAT and wake up the LAN client. This command will allow the user to choose whether WoL packets can be passed from the Internet to the LAN network from a specific WAN interface.
[idx][ip address] [mask]	It means the index number (from 1 to 4). These commands will allow the user to configure the LAN clients that the user may wake up from the Internet through the use of the WoL packet. *ip address* - It means the WAN IP address. *mask* - It means the mask of the IP address.

Example

```
> wol fromWan on
> wol fromWan_Setting 1 192.168.1.45 255.255.255.0
>
```

Telnet Command: user

The command is used to create new user account profiles.

Syntax

sser set *[-e|-d|-c|-l|-o|-a|-r|-b]*

user edit *[PROFILE_IDX] [-e|-d|-n|-p|-t|-u|-i|-q|-r|-w|-s|-m|-x|-v]*

user account *[USER_NAME] [-t|-d|-q|-r|-w]*

Syntax Description

Parameter	Description
set	It means to configure general setup for the user management.
edit	It means to modify the selected user profile.
account	It means to set time and data quota for specified user account.
User Set	
-e	Enable User management function.
-d	Disable User management function.
-a[Profile idx][User name][IP_Address]	It means to pass an IP Address. *Profile idx*- type the index number of the selected profile. *User name*- type the user name that you want it to pass. *IP_Address*- type the IP address that you want it to pass.
-l all *-l userl* *-l ip*	Show online user. *all* – all of the users will be displayed on the screen. *user name* – type the user name that you want to view on the screen. *ip* – type the IP address that you want to view on the screen.
-o	It means to show user account information. e.g.,*-o*
-c[user name] *-c all*	Clear the user record. *user name* – type the user name that you want to get clear corresponding record. *all* – all of the records will be removed.
-buser [user name] *-b ip [ip address]*	Block specifies user or IP address. *user name* – type the user name that you want to block. *ip address* — type the IP address that you want to block.
-u user [user name] *-u ip [ip address]*	Unblock specifies user or IP address. *user name* – type the user name that you want to unblock. *ip address* — type the IP address that you want to unblock.
-r [user name | all]	Remove the user record. *user name* – type the name of the user profile. *all* – all of the user profile settings will be removed.
-q	It means to trigger the alert tool to do authentication.
-s	It means to set login service. 0:HTTPS 1:HTTP e.g.,*-s 1*
User edit	

PROFILE_IDX	Type the index number of the profile that you want to edit.
-e	Enable User profile function.
-d	Disable User profile function.
-n	It means to set a user name for a profile. e.g.,*-n fortest*
-p	It means to configure user password. e.g., *-p 60fortest*
-t	It means to enable /disable time quota limitation for user profile 0:Disable 1:Enable
-u	It means to enable /disable data quota limitation for user profile 0:Disable 1:Enable
-i	It means to set idle time. e.g., *-i 60*
-q	set time quota It means to set time quota of the user profile. e.g., *-q 200*
-r	It means to set data quota. e.g., *-r 1000*
-w	It means to specify the data quota unit (MB/GB). e.g., -w MB
-s	It means to set schedule index. Available settings are" sch_idx1,sch_idx2,sch_idx3, and sch_idx4.
-m	It means to set the maximum login user number. e.g., *-m 200*
-x	It means to set external server authentication 0: None 1: LDAP 2: Radius 3: TACAS e.g., *-x 2*
-v	It means to view user profile(s).
User account	
USER_NAME	It means to type a name of the user account.
-d	It means to enable /disable data quota limitation for user account. 0:Disable 1:Enable
-q	It means to set account time quota. e.g., *-q 200*
-r	It means to set account data quota. e.g., *-r 1000*
-t	It means to enable /disable time quota limitation for user account. 0:Disable 1:Enable
-w	It means to set data quota unit (MB/GB).

Example

```
> user account admin -d 1
 Enable the [admin] data quota limited
```

Telnet Command: appqos

The command is used to configure QoS for APP.

Syntax

appqos view

appqos enable *[0/1]*

appqos traceable *[-v | -e AP_INDEX CLASS | -d AP_INDEX]*

appqos untraceable *[-v | -e AP_INDEX CLASS | -d AP_INDEX]*

Syntax Description

Parameter	Description
view	It means to display current status of APP QoS.
enable[0/1]	It means to enable or disable the function of APP QoS.
traceable/ untraceable	The APPs are divided into traceable and untraceable based on their properties.
-v	It means to view the content of all traceable APs. Use “appqos traceable –v” to display all of the traceable APS with speficed index number. Use “appqos untraceable –v” to display all of the untraceable APS with speficed index number.
-e	It menas to enable QoS for application(s) and assign QoS class.
AP_INDEX	Each index number represents one application. Index number: 50, 51, 52, 53, 54, 58, 60, 62, 63, 64, 65, 66, 68 are used for 13 traceabel APPs. Index number: 0~49, 55~59, 61, 67, 69, and 70~123 are used for 125 untraceable AP.
CLASS	Specifies the QoS class of the application, from 1 to 4 1:Class 1, 2:Class 2, 3:Class 3, 4:Other Class
-d	It means to disable QoS for application(s).

Example

```
> appqos enable 1

APP QoS set to Enable.
> appqos traceable -e 68 2

TELNET: ENABLED, QoS Class 2.
```

Telnet Command: nand bad /nand usage

"NAND usage" is used to display NAND Flash usage; "nand bad" is used to display NAND Flash bad blocks.

Syntax

nand bad

nand usage

Example

```
>nand usage
Show NAND Flash Usage:
Partition    Total          Used           Available      Use%
cfg          4194304        7920           4186384         0%
bin_web      33554432       11869493       21684939        35%
cfg-bak      4194304        7920           4186384         0%
bin_web-bak 33554432       11869493       21684939        35%
> nand bad
Show NAND Flash Bad Blocks:
Block   Address        Partition
1020    0x07f80000     unused
1021    0x07fa0000     unused
1022    0x07fc0000     unused
1023    0x07fe0000     unused
```

Telnet Command: apm enable / disable/ show /clear/discover/query

The apm command(s) is use to display, remove, discover or query the information of VigorAP registered to Vigor2926.

Syntax

apm enable

apm disable

apm show

apm clear

apm discover

apm query

Syntax Description

Parameter	Description
enable/disable	Enable /disable APM function.
show	It displays current information of APM profile.
clear	It is used to remove all of the APM profile.
discover	It is used to search VigorAP on LAN.
query	It is used to query any VigorAP which has been registered to APM (Central AP Management) in Vigor2926. Information related to the registered AP will be send back to Vigor2926 for updating the web page of Central AP Management.

Example

```
> apm clear ?
Clear all clients ... done
```

Telnet Command: apm profile

This command allows to configure wireless profiles to be used in Central AP Management.

Syntax

apm profile clone *[from index][to index][[new name]*

apm profile del *[index]*

apm profile reset

apm profile summary

apm profile *[show [profile index]]*

apm profile *apply [profile index] [client index1 [index2 .. index5]]*

Syntax Description

Parameter	Description
clone	It is used to copy the same parameters settings from one profile to another APM profile.
del	It is used to delete a specified APM profile. The default (index #1) should not be deleted.
reset	It is used to reset to factory settings for WLAN profile.
summary	It is used to list all of the APM profiles with required information.
show	It is used to display specified APM profile.
apply	It is used to apply the selected APM profile onto specified VigorAP.
from index	Type an index number in this field. It is the original APM profile to be cloned to other APM profile.
to index	Type an index number in this file. It is the target profile which will clone the parameters settings from an existed APM profile.
new name	Type a name for a new APM profile.
profile index	Type the index number of existed profile.
client index1/2/3/4/5	It is useful for applying the selected APM profile to the specified VigorAP.

Example

```
> apm profile clone 1 2 forcarrie
(Done)

> apm profile summary
# Name           SSID           Security    ACL    RateCtrl(U/D)
- --------------- ---------------- ------------ ------- ------
0 Default       DrayTek-LAN-A   WPA+WPA2/PSK x          - /    -
                DrayTek-LAN-B   WPA+WPA2/PSK x          - /    -

1 -              -              -           -               -
2 forcarrie       DrayTek         Disable     x          - /    -
```

```
3 -             -             -             -             -
4 -             -             -             -             -
```

Telnet Command: apm cache

This command is used to display or remove the information of registered VigorAP, including MAC address, name, and authentication. Up to 30 entries of registered information can be stored and displayed.

Syntax

apm cache *[show]*

apm cache clear

Syntax Description

Parameter	Description
show	It means to display the information related to VigorAP registered Vigor2926.
clear	It means to remove the information related to VigorAP registered Vigor2926.

Example

```
> apm cache show
MAC         Name               Auth
------------ ------------------- -------------------

>
```

Telnet Command: apm lbcfg

This command allows to set parameters related to AP management control.

Syntax

apm lbcfg *[set] [value]*

apm lbcfg*[show]*

Syntax Description

Parameter	Description
set	It means to set the load balance configuration file for APM.
Show	It shows the configuration value.
[value]	You need to type 10 numbers in this field. Each number represents different setting value. [1] – The first number means the load balance function. Type 1 – enable load balance, 0 – disable load balance. [2] – The second number means the station limit function. Type 1 –enable station limit, 0 – disable station limit. [3] – The third number means the traffic limit function. Type 1 – enable traffic limit, 0 – disable traffic limit.

	[4] – The forth number means the limit num of station. Available range is 3~64. [5] – The fifth number means the upload limit function. Type 1 – enable upload limit, 0 – disable upload limit. [6] – The sixth number means the download limit function. Type 1 – enable download limit, 0 – disable download limit. [7] – The seventh number means disassociation by idle time. Type 1 – enable disassociation, 0 – disable disassociation. [8] – The eighth number means to enable or disable disassociation by signal strength. Type 1 – enable disassociation, 0 – disable disassociation. [9] – The ninth number means to determine the unit of traffic limit (for upload) 1 – Mbps 0 – kbps [10] – The tenth number means to determine the unit of traffic limit (for download) 1 – Mbps 0 – kbps

Example

```
> apm lbcfg show
apm LoadBalance Config :
1. Enable LoadBalance : 0
2. Enable station limit : 0
3. Enable traffic limit : 0
4. limit Number : 64
5. Upload limit : 0
6. Download limit : 0
7. Enable disassociation by idle time : 0
8. Enable disassociation by Signal strength : 0
9. Traffic limit unit (upload)   : 0
10.Traffic limit unit (download) : 0
flag : 0
> apm lbcfg set 1 1 0 15 0 0 0 0 1 1
> apm lbcfg show
apm LoadBalance Config :
1. Enable LoadBalance : 1
2. Enable station limit : 1
3. Enable traffic limit : 0
4. limit Number : 15
5. Upload limit : 0
6. Download limit : 0
7. Enable disassociation by idle time : 0
8. Enable disassociation by Signal strength : 0
9. Traffic limit unit (upload)   : 1
```

```
10.Traffic limit unit (download) : 1
flag : 49
```

Telnet Command: apm apdetect

This command is used to enable/disable AP detection function.

Syntax

apm apdetect *[get]*

apm apdetect *[set] [enable/disable AP Detection 1/0][Refresh Time].*

Syntax Description

Parameter	Description
get	It is used to get AP detection data from VigorAP (e.g., AP900).
set	It allows to set detect configuration to VigorAP.
enable/disable AP Detection 1/0	It is used to enable or disable the AP detection function. 0 – disable the function. 1 – enable the function.
Refresh Time	Available values are 1, 3 or 5 (minutes).

Example

Note: To check the scanning result of AP detection, use the command of "*wl scan show*".

```
> apm napdetect set 1 1
> wl scan show 3
Sta Ch SSID          BSSID           BssType  Security Siganl(%)  Beacon
Period First Detected  Last Detected
11 DrayTek-LAN-B    02:1d:aa:4c:bd:a8  AP     Mixed      26      100
11 DrayTek-LAN-A    00:1d:aa:4f:bd:a8  AP     Mixed      42      100
Dec 09,10:35:44 Dec 09,10:35:44
```

Telnet Command: apm apsyslog

This command is used to display the AP syslog data coming form VigorAP.

Syntax

apm apsyslog *[AP_Index]*

Syntax Description

Parameter	Description
AP_Index	Specify the index number which represents VigorAP.

Example

```
> apm apsyslog 1
8d 02:46:09  syslog: [APM] Send Rogue AP Detection data.
8d 02:53:04  syslog: [APM] Run AP Detection / Discovery.
8d 02:56:09  syslog: [APM] Send Rogue AP Detection data.
8d 03:00:42  kernel: 60:fa:cd:55:f5:ea had disassociated.
8d 03:03:12  syslog: [APM] Run AP Detection / Discovery.
8d 03:06:09  syslog: [APM] Send Rogue AP Detection data.
8d 03:13:21  syslog: [APM] Run AP Detection / Discovery.
```

```
8d 03:16:10  syslog: [APM] Send Rogue AP Detection data.
8d 03:16:41  kernel: 60:fa:cd:55:f5:ea had associated successfully
8d 03:16:55  kernel: 60:fa:cd:55:f5:ea had disassociated.
```

Telnet Command: apm syslog

This command is used to display related syslog data from central AP management.

Syntax

apm syslog

Example

```
> apm syslog
"2015-11-04 12:24:21", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP"
2015-11-04 12:24:56", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP Success"
2015-11-04 12:34:21", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP"
2015-11-04 12:34:57", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP Success"
```

Telnet Command: apm stanum

This command is used to display the total number of the wireless clients, no matter what mode of wireless connection (2.4G WLAN or 5G WLAN) used by wireless clients to access into Internet through VigorAP.

Syntax

apm stanum *[AP_Index]*

Syntax Description

Parameter	Description
AP_Index	Specify the index number which represents VigorAP.

Example

```
> apm stanum

% Show the APM AP Station Number data.
% apm stanum AP_Index.
%     ex : apm stanum 1
%          Idx Nearby(2.4/5G) Conn(2.4/5G)
%           1   2   5          0   0
%           2   2   5          1   0
%           3   2   5          1   0
```

Telnet Command: ha set

This command can be used to configure HA settings for Vigor routers.

Syntax

ha set *[-<command> <parameter>| …]*

Syntax Description

Parameter	Description

[<command> <parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several parameters in one line.
-e <1/0>	1: Enable the function of High Availability (HA). 0: Disable the function of High Availability (HA).
-l <1/0>	1: Enable the function of recording the operation record of HA in Syslog. 0: Disable the function of recording the operation record of HA in Syslog.
-M <1/0>	Specify the Redundancy Method for HA. 1: Active-Standby 0: Hot-Standby
-v <1-255>	Specify the group ID (VHID) 1- 255: Setting range.
-R	Set HA settings to Factory Default.
-p <1-30>	Specify the Priority ID. 1-30: Setting range.
-k <key>	Specify the Authentication Key. Key: Max. 31 Characters.
-u <1/0>	Enable or disable the function of Update DDNS. 1: Enable. When a router changes HA status to primary, it will update DDNS automatically. 0: Disable.
-m <interface>	Specify the management interface. Interface: LAN1 ~ LAN6, DMZ.
-s	It means to get the newest status of other router (except the local router).
-y	It means sync local config to other router. Primary can executes this command. Secondary can not execute this commad.
-c <1/0>	Enable or disable the function of Config Sync. 1: Enable. 0: Disable.
-I -[M|H|D] <interval>	Set the Config Sync Interval for HA. Minimum interval is 15 minutes. -M: Minute. Setting range is 0/15/30/45. (e.g., ha set -I -M 30) -H: Hour. Setting range is from 0 to 23. (e.g., ha set -I -H 12) -D: Day. Setting range is from 0 to 30. (e.g., ha set -I -D 15)
-h -<4/6><Subnet> [<Virtual IP>]	Enable and set virtual IP to the subnet. 4: IPv4; 6: IPv6. Subnet: LAN1 to LAN6, DMZ. Virtual IP: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.1.0) For example, to enable a virtual IP to the sunet, simply type: *ha set –h LAN1 192.168.1.5*
-d -<4/6><Subnet>	Disable a virtual IP to the subnet. 4: IPv4; 6: IPv6. Subnet: LAN1 to LAN6, DMZ. For example, to disable a virtual IP to the subnet, just type: *ha set –h LAN1*
-o <1/0>	Run DARP protocol on IPv4 or IPv6. 0: IPv4 1: IPv6

Example

```
> > ha set -h -4 LAN1 192.168.1.1
% Enable IPv4 Virtual IP on LAN1
% Virtual IP can not be same as router IP (192.168.1.1)!!!
>
```

Telnet Command: ha show

This command can be used to show the *settings information* about config sync and general setup.

Syntax

ha show –c

ha show –g

Syntax Description

Parameter	Description
-c	Show the settings of config sync.
-g	Show the settings of general setup.

Example

```
> ha show -g
%  High Availability   : Disable
%  Redundancy Method   : Active-Standby
%  Group ID           : 1
%  Priority ID        : 10
%  Preempt Mode       : Enable
%  Update DDNS        : Disable
%  Management Interface : LAN1
%  Authentication Key  : draytek
%  Syslog             : OFF
%
%  [ Index | Enable | Virtual IP ]
%    LAN1   On      192.168.1.0
%    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
%    DMZ    -       0.0.0.0
%  [ Index | Enable | Virtual IPv6 ]
%    LAN1    On     FE80::200:5EFF:FE00:101
%    LAN2    On     FE80::200:5EFF:FE00:101
%    LAN3    On     FE80::200:5EFF:FE00:101
%    LAN4    On     FE80::200:5EFF:FE00:101
%    LAN5    On     FE80::200:5EFF:FE00:101
%    LAN6    On     FE80::200:5EFF:FE00:101
%    DMZ     On     FE80::200:5EFF:FE00:101
>
```

Telnet Command: ha status

This command is used to display *HA status information*.

Syntax

ha status –a *[Detail Level]*

ha status –m *[Detail Level]*

Syntax Description

Parameter	Description

-a	Show the status for all of the routers in HA group.
-m	Show the status of local router only.
Detail Level	0: Important status. 1: Important status, plus some information. 2: Show settings

Example

```
> ha status -m 2
%   [Local Router] DrayTek
%   IP               : 192.168.1.1 (FE80::21D:AAFF:FEC6:4C50)
%   Status           : !
%   High Availability   : ! Disable
%   Redundancy Method   : Active-Standby
%   Group ID          : 1
%   Priority ID       : 10
%   Update DDNS       : Disable
%   Protocol          : IPv4
%   Management Interface: LAN1
%   Authentication Key  : draytek
%   Virtual IP: (Max. 7 Virtual IPs)
%     ON       LAN1  192.168.1.0
%   Virtual IPv6: (Max. 7 Virtual IPv6s)
%     ON       LAN1  FE80::200:5EFF:FE00:101
%     ON       LAN2  FE80::200:5EFF:FE00:101
%     ON       LAN3  FE80::200:5EFF:FE00:101
%     ON       LAN4  FE80::200:5EFF:FE00:101
%     ON       LAN5  FE80::200:5EFF:FE00:101
%     ON       LAN6  FE80::200:5EFF:FE00:101
%     ON       DMZ   FE80::200:5EFF:FE00:101
%   Config Sync            : Disable
%   Config Sync Interval    : 0 Day 0 Hour 15 Minute
%   Cached Time       : 0 (s)

>
```

Telnet Command: swm show

This command is used to display general setting of of VigorSwitch which connecting to Vigor router in LAN.

Syntax

swm show *[LAN_port]*

Syntax Description

Parameter	Description
LAN_port	Specify the LAN port number (1 to 5).

Example

```
> swm show

** If you connected a VigorSwitch but does not display here.
** Please check the LLDP is enabled and VLAN ID is matched on VigorSwitch.
********************************************************************************
LAN Port Model Name MAC IP Address Con Port
-------- ---------------- ------------ --------------- ---------
1 G1241 00507FF105FD 192.168.1.10 23
--------------------------------------------------------------------------------
Internal VLAN is [Enable]
Only show P1 related VLAN settings here.
VLAN Subn Tag VID Pri LAN WLAN(2.4G) WLAN(5G)
---- ---- --- ---- --- ------------------ ------------ ------------
0 LAN1 Off 0 0 P1,P2,P3,P4,P5,P6 none none
1 LAN1 On 20 0 P1,P2,P3,P4,P5,P6 none none
2 LAN1 On 100 0 P1,P2,P3,P4,P5,P6 none none
```

Telnet Command: swm get

This command is used to **get** configuration information of VigorSwitch which connecting to Vigor router in LAN. Before using such command, make sure VigorSwitch has been managed under Vigor router (refer to Telnet Command: swm profile for adding a VigorSwitch device onto Vigor router).

Syntax

swm get *[MAC]*

Syntax Description

Parameter	Description
MAC	Specify the MAC address of the switch.

Example

```
> swm get 00507ff0c33c
Start get cfg from 00507ff0c33c external switch

Please wait a few seconds...

Result: [OK].
```

Telnet Command: swm post

This command is used to transfer switch configuration to VigorSwitch which connecting to Vigor router in LAN.

Syntax

swm post *[MAC]*

Syntax Description

Parameter	Description
MAC	Specify the MAC address of the switch.

Example

```
> swm post 00507ff0c33c
Start post cfg to 00507ff0c33c external switch with correct settings.

Please wait a few seconds...

Result: [OK].>
```

Telnet Command: swm auth

This command is used to display or remove the authentication record for external switch.

Syntax

swm auth *[show/clear]*

Syntax Description

Parameter	Description
show	Display recorded external switch MAC address list.
clear	Clear specific index of authentication record table.

	Index range: (1 - 30)

Example

```
> swm auth show
===== SWM Auth Records List=====
Index  Model   Mac
-----  ------  --------------
1      G2261   00507ff0c33c
================================
```

Telnet Command: swm extvlan

This command is used to configure port VLAN of VigorSwitch. Before using such command, make sure you have configured VLAN settings well.

Syntax

swm extvlan *[LAN_Port][VLAN_idx][Port_Description]*

Syntax Description

Parameter	Description
LAN_Port	Setting range is from 1 to 5.
VLAN_idx	Type the enabled internal VLAN number. Index number range for VLAN is from 0 to 7.
Port_Description	Setting range is from 1 to 24.

Example

```
> swm extvlan 1 1 13
Set OK.
> swm post 1
Start post cfg to LAN (1) external switch with currect settings.//post cfg
Please wait a few seconds...
Result: [OK].
```

System will cover the original VLAN settings on your VigorSwitch. Please backup the configuration file before you run this function.

System also will select the physical connect port as trunk port and let it join each VLAN group.

Before using such command, please use [swm show] to check valid VLAN index firstly.

Telnet Command: swm enable

This command is used to enable central management for VigorSwitch.

Syntax

swm enable

Telnet Command: swm disable

This command is used to disable central management for VigorSwitch.

Syntax

swm disable

Telnet Command: swm group

This command is used to gather several VigorSwitch devices as a group.

Syntax

swm group set *[IDX][NAME][1][PASSWD]*

swm group set *[IDX][NAME][0]*

swm group show

swm group add *[IDX][MAC]*

swm group delete *[IDX][MAC]*

Syntax Description

Parameter	Description
IDX	Type the number to specify the index number of the group profile.
NAME	Type a name for VigorSwitch group.
PASSWD	Specify a password.
1,0	1 – Set group name and password. 0 - Set group name without password.
MAC	Type the MAC address of the VigorSwitch.
add/delete	Add – Make the selected switch (by specifying MAC address) to be grouped as VLAN.

Example

```
> swm group set 1 switchvlan 1 123456
> swm group show
Index    Group Name      Passwd Flag    Member Switch
-------- ------------------- -----------  -----------------------------------
1       switchvlan          1      P2261(192.168.1.226),
2                          0
3                          0
4                          0
5                          0
6                          0
7                          0
8                          0
9                          0
10                         0

Name            IP Address      MAC
--------------- --------------- ------------
P2261           192.168.1.226    00507ff0c33c
>
```

Telnet Command: swm profile

This command is used to set switch profile for adding it to be managed by Vigor router, or removing it from Vigor router.

Syntax

swm profile add/delete *[MAC]*

swm profile show

swm profile enable_all/disable_all *[MAC]*

Syntax Description

Parameter	Description
Add	Make the specified switch to be managed by Vigor router by typing the MAC address.
delete	Remove the specified switch from Vigor router by typing the MAC address.

show	Display all the switch devices managed under Vigor router.
Enable_all	Enable all of the switch devices.
Disable_all	Disable all of the switch devices.
MAC	Type the MAC address of the VigorSwitch.

Example

```
> swm profile show
Name            IP Address      MAC          Model  Group
--------------- --------------- ------------  ------ -------------------------
P2261           192.168.1.226   00507ff0c33c P2261   switchvlan,

IP Address      MAC          Model
--------------- ------------  ------
```

Telnet Command: swm detail

This command is used to configure detailed information for VigorSwitch.

Syntax

swm detail comment *[MAC][COMMENT]*

swm detail name *[MAC][NAME]*

swm detail passwd *[MAC][PASSWD]*

swm detail config *[MAC][config]*

swm detail show

swm detail port show *[MAC]*

swm detail port *[MAC][PORT][FLAG][SCHED1][SCHED2][DESCRIPTION]*

Syntax Description

Parameter	Description
[MAC][COMMENT]	Modify the comment of VigorSwitch. MAC - Type the MAC address of the switch. COMMENT – Type a description for the switch.
[MAC]{NAME}	Modify the name of VigorSwitch. MAC - Type the MAC address of the switch. NAME – Type a name for the switch.
[MAC][PASSWD]	Modify the password of VigorSwitch. MAC - Type the MAC address of the switch. *PASSWD* – Type the password for the switch.
[MAC][config]	Modify the config file of VigorSwitch. MAC - Type the MAC address of the switch. *config* – Type the config name of the switch.
show	Display all of the switches' status.
[MAC][PORT][FLAG][SCHED1] [SCHED2][DESCRIPTION]	Modify the port description for specific switch.

Example

```
> swm detail show
Idx  Name            MAC         Comment         Config        Status
---- --------------- ------------  --------------- ------------ --------
1    P2261          00507ff0c33c justfortest     1  None         Connect
```

Telnet Command: swm maintain

This command is used to reboot, reset VigorSwitch or display the status of VigorSwitch.

Syntax

swm maintain reboot *[MAC]*

swm maintain reset *[MAC]*

swm maintain show

Syntax Description

Parameter	Description
Reboot [MAC]	Type the MAC address of the VigorSwitch that you want to reboot.
Reset [MAC]	Type the MAC address of the VigorSwitch that you want to reset.
show	Display the switch status (including name, IP address, MAC and model)

Example

```
> swm maintain show
Name           IP Address      MAC          Model
---------------- ---------------- ------------  ------
P2261          192.168.1.226    00507ff0c33c P2261
> swm maintain reset 00507ff0c33c
Preparing to reset.
Please wait for few minutes and do not turn off power.
```

Telnet Command: swm search

This command is used to searh VigorSwitch managed by Vigor router.

Syntax

swm search mac *[MAC]*

swm search ip *[IP]*

swm search description *[Input]*

Syntax Description

Parameter	Description
Mac [MAC]	Type the MAC address of the VigorSwitch for searching.
IP [IP]	Type the IPv4 address of the VigorSwitch for searching.
Description [Input]	Type a brief description of the VigorSwitch for searching.

Example

```
> swm search ip 192.168.1.11
Type    IP Address      MAC             Description / Name        Lan Port
 UpLink Port     Level   Port
------- ---------------- ----------------- ---------------------------- --------
 ---------------- ----- -------
```

Telnet Command: swm db

This command is used to set corresponding actions (for database) while encountering alert event.

Syntax

swm db ctl en /dis

swm db ctl show

swm db alert notify *[N/S]*

swm db alert action *[S/B]*

swm db alert sms *[IDX]*

swm db alert mail *[IDX]*

Syntax Description

Parameter	Description
ctl en / dis	It means to enable / disable the database for recording switch management information.
ctl show	It means to display the database control status.
alert notify [N/S]	It means to send notification or take no action for database while ecountering alert event. N - Don't send notification S - Send notification
alert action [S/B]	Set the action for (stop or backup) database while ecountering alert event. S - Stop recording urser information. B - Backup and clean up all user info, and start a new record.
alert sms [IDX]	Set object for SMS alert notification. IDX – It menas the index number of availabe object profile. Range is 1 ~ 64.
alert mail [IDX]	Set object for mail alert notification. IDX – It menas the index number of availabe object profile. Range is 1 ~ 64.

Example

```
> swm db ctl en
Enable database to recoard SWM information.

DrayTek> swm db ctl show
Record SWM information: Enable.
Notification :
Dont't send notification.
action : Stop recording user information.
```

Telnet Command: swm alert

This command is used to configure settings for alert and log for VigorSwitch management.

Syntax

swm alert enable/disable

swm alert show

swm alert en/dis *[Idx]*

swm alert set *[Idx]* **log** *[e/d]*

swm alert set *[Idx]* **name** *[name]*

swm alert set *[Idx]* **color** *[O/R/N]*

swm alert set *[Idx]* **notif** *[e/d]*

swm alert set *[Idx]* **obj** *[object idx] [object value]*

swm alert display

swm alert en/dis *[sw/port] [mac]*

swm alert sw show *[mac]*

swm alert set sw *[mac] [incident idx] [level idx]*

swm alert port show *[mac]*

swm alert set port *[mac] [port num][incident idx] [level idx]*

Syntax Description

Parameter	Description
enable/disable	Enable/disable alert mechanism.
show	Display all alert setup information.
en/dis [Idx]	Enable/disable alert action for certain profile. Idx – Indicate profile to be configured; available range: 1 – 8.
set [idx] log [e/d]	Enable/disable log action for certain profile. Idx – Indicate profile to be configured; available range: 1 – 8. 8. e/d – Enable/disable the profile.
set [idx] name [name]	Set level name which can represent different severiy level. Idx – Indicate profile to be configured; available range: 1 – 8. name – Type a string to indicate the severity level.
set [idx] color [O/R/N]	Set color for alert for certain profile. Idx – Indicate profile to be configured; available range: 1 – 8. *O/R/N – O means orange; R means red; N means white*
set [idx] notif [e/d]	Enable/disable the notification action for certain profile. Idx – Indicate profile to be configured; available range: 1 – 8. e/d - Enable/disable the mechanism for sending the notification.
set [idx] obj [object idx] [object value]	Set notifiction by SMS or E-mail thorugh the object profile selelcted for specified profile. Idx – Indicate profile to be configured; available range: 1 – 8. object idx - Available range: 1 – 4 object value – Available range: 1 – 20
swm alert display	Display all switch and port alert state.
en/dis [sw/port][mac]	Enable/disable Switch/Port Action. sw/port – Type a port number for VigorSwitch. mac – Type MAC address of the VigorSwitch.
sw show [mac]	Display VigorSwitch Incident Alert
set sw [mac] [incident idx] [level idx]	Set incident alert for VigorSwitch. mac- Type MAC address of the VigorSwitch. level idx – Available range: 1 – 8. Each number represents different severity level.
port show [mac]	Display the incident alert setting for all LAN ports of certain VigorSwitch (specified by MAC address). Mac – Type the MAC address of the VigorSwitch.
set port [mac] [port num][incident idx][level idx]	Set incident alert for each Ethernet port of VigorSwitch. mac- Type MAC address of the VigorSwitch. port num – Type a port number for VigorSwitch.

	Incident id – Type an index number of the incident. level idx – Available range: 1 – 8. Each number represents different severity level.

Example

```
> swm alert set 5 obj 1
> swm alert display
Name           IP Address       Model Sw-Alert Port-Alert
---------------- ---------------- ------ -------- ----------
G2260          192.168.1.11    G2260  En      En
> DrayTek> swm alert set port 000854123456 5 1 2
DrayTek> swm alert port show 000854123456
Port      (1)Reconnect      (2)Disconnect      (3)Schedule on/off  (4)Shutdown En/Dis
--------  ----------------  -----------------  ------------------  ------------------
1         No Alert          No Alert           No Alert            No Alert
2         No Alert          No Alert           No Alert            No Alert
3         No Alert          No Alert           No Alert            No Alert
4         No Alert          No Alert           No Alert            No Alert
5         Minor Alert       No Alert           No Alert            No Alert
6         No Alert          No Alert           No Alert            No Alert
7         No Alert          No Alert           No Alert            No Alert
8         No Alert          No Alert           No Alert            No Alert
9         No Alert          No Alert           No Alert            No Alert
10        No Alert          No Alert           No Alert            No Alert

DrayTek> swm alert sw show 000854123456
Idx En/Dis   Level        Color    Create Log   Send Notification(1-4)
----- ------ ------------ -------- ------------ ----------------------
1     En     No Alert     No Color     Disable  Disable      0  , 0  , 0  , 0
2     En     Minor Alert  No Color     Enable   Disable      0  , 0  , 0  , 0
3     En     Moderate Alert Orange       Enable   Disable      1  , 1  , 1  , 1
4     En     Major Alert  Red          Enable   Disable      1  , 1  , 1  , 1
5     Dis                 No Color     Disable  Disable      1  , 1  , 1  , 1
6     Dis                 No Color     Disable  Disable      1  , 1  , 1  , 1
7     Dis                 No Color     Disable  Disable      1  , 1  , 1  , 1
8     Dis                 No Color     Enable   Disable      1  , 1  , 1  , 1

Name             IP Address
---------------- ----------------
Switch           192.168.1.11

Index Incident             Type
----- -------------------- ----------------
1     Cold Start           Major Alert
2     Warm Start           Major Alert
3     Disconnect           Major Alert
```

Telnet Command: swm log

This command is used to configure settings for VigorSwitch and display VigorSwitch's log,

Syntax

swm log show filter

swm log show day

swm log show week

swm log set level *[idx] on/off*

swm log set type *[idx] on/off*

swm log set switch *[mac] on/off*

Syntax Description

Parameter	Description
show filter	Display log settings including index number, on /off status, alert level, enabling / disabling, alert type, device name, MAC address and etc. for VigorSwitch.

show day	Display day Log for VigorSwitch.
show week	Display week Log for VigorSwitch.
set level [idx] on/off	Enable / disable the alert with different severity. Idx- Range 1 to 4. 1 means No Alert; 2 means Minor Alert; 3 means Moderate Alert; 4 means Major Alert. On – Enable Off - Disable
set type [idx] on/off	Enable / disable the Port Alert / Switch Alert. Idx- 1 means Port Alart; 2 means Switch Alert. On – Enable Off - Disable
set switch [mac] on/off	Enable (on) or disable (off) the log recorded mechanism for specified VigorSwitch. mac- Type MAC address of the VigorSwitch.

Example

```
> swm log set type 1 on
> swm log set level 1 on
> swm log show weekTotal Logs:0
> swm log show filter
Index Status Level         En/Dis
----- ------ --------------- --------
1    on    No Alert       En
2    off   Minor Alert    En
3    off   Moderate Alert  En
4    off   Major Alert    En
5    off                Dis
6    off                Dis
7    off                Dis
8    off                Dis

Index Status Type
----- ------ -------------
1    on    Port Alert
2    off   Switch Alert

Index Status Switch Name    Model  Mac Address
----- ------ --------------- ------ --------------
```

Telnet Command: swm snmp

This command is used to display information about SNMP.

Syntax

swm snmp sys *[MAC]*

swm snmp iftbl *[MAC][port_num]*

swm snmp poe *[MAC]*

Syntax Description

Parameter	Description
sys [MAC]	Type the MAC address of the VigorSwitch to display the SNMP system information.

Iftbl[MAC][port_num]	Type the MAC address and the port number of the VigorSwitch to display SNMP port interface information.

Example

```
> swm snmp sys 00507ff0c33c
sysDescr:20-Port 10/100/1000Base-T + 4 TP/(100/1G) SFP Combo + 2 (100/1G) SFP
Po
E+ L2 Plus Managed Switch
sysObjectID:1.3.6.1.4.1.5205.2.61
sysUpTime:24 hr 8 m 46 s
sysContact:
sysName:P2261
sysLocation:
sysServices:3
ifNumber:26
```

索引

3

3G/4G USB Modem, 52

3G/4G USB Modem (DHCP mode), 72, 74

6

6rd Mode, 85

6rd Prefix, 86

6rd Prefix Length, 86

8

802.1x ports, 129

A

Accelerate heaviest traffic sessions, 131

Access Control, 258

Access List, 460

Access Mode, 61

Access Mode - Ethernet, 60

Access Mode - LTE, 60

Access Mode - USB, 60

Access Tech, 243

Account Number, 288

Activation, 469

Active Directory/LDAP, 166

Active Mode, 55, 56

Active When, 57, 59

Active-Standby, 179

Additional Filter, 168

Address Mapping, 205, 222

Administrator Password, 441

Advance Mode, 382

Advanced Mode, 238

Advanced Setting, 266

Aggregation MSDU, 266

AH, 328

Airtime Fairness, 271

Always On, 59, 66, 76, 78, 79, 80, 81, 82, 84, 86, 89

Analyze, 396

Anonymous, 166

Antenna Installation, 3

AP Discovery, 270

AP Maintenance, 568, 576

AP Map, 568, 577

APN Name, 71, 73, 74

APP Enforcement, 379

APP Enforcement Filter, 401

APP Enforcement Profile, 402

APP QoS, 485

APPE Module Version, 406

APPE Signature Upgrade, 406

Applications, 146

Apply the Class Rule, 131

APSD Capable, 267

ARP Cache Table, 659

ARP Detect, 63, 66, 71, 73, 75

ARP Table, 126

Auth Type, 151

Authentication, 75, 164

Authentication Information, 676

Authentication Key, 180

Authentication Mode, 261

Authentication Port, 163

Authentication Type, 129

Auto Adjustment, 269

Auto Logout, 22

Auto Weight, 55

Auto-Update interval, 149

Aux. WAN IP, 141

B

Backup, 126

Backup Mode, 349

Backup MX, 151

Backup Phone Number, 292

Band Steering, 273

Bandwidth Limit, 472, 476

Bandwidth Management, 269
Barring Type, 296
Base Distinguished Name / Group Distinguished Name, 168
Beacon Period, 582
Bind IP to MAC, 125
Bind to WAN, 357
Bind Type, 166
Block Anonymous, 298
Block IP Calls, 298
Block Unknown Domain, 298
Bogus DNS Reply, 157
Bonjour, 175
Bridge, 262, 265
Bridge mode, 91
Bridge Mode, 66, 81, 83
Bridge Subnet, 66, 83
Brute Force Protection, 458

C

Cache, 413
Call Barring, 295
Call Direction, 296, 331
Call Filter, 374
Call Forward, 297
Call Forwarding, 289
Call Transfer, 300
Call Waiting, 298
Certificate Backup, 372
Certificate Management, 365
Change the TTL value, 64, 67
Channel, 87, 250, 254
Channel Bandwidth, 266
Choose IP, 139
CLIR, 300
Codepage, 379
Comment, 126, 141
Common Name Identifier, 168
Config Backup, 29
Config Sync, 180
Configuration Backup, 448
Configure via Client PinCode, 261
Configure via Push Button, 261
Connection Management, 349
Connection Type, 151
Connectivity, 51
Country Code, 267
CPE Management, 550
CSM, 401
CSV file, 612, 615
Current System Time, 159

D

Dashboard, 24, 569
Data Coding Scheme, 240
Data Filter, 374
Data Flow Monitor, 665
Data Quota, 503
DataType, 61
Daylight Saving, 454
Days in a week, 160
Default Lifetime, 115
Default MAC Address, 64, 67
Default Preference, 115
Default Rule, 378
Destination IP, 213
Destination Port, 162
Details - PPPoE, 62
Details Page, 61
Details-3G/4G USB Modem (DHCP mode), 74
Details-3G/4G USB Modem(PPP mode), 70
Details-IP Routed Subnet, 110
Details-IPv6-6in4 Static Tunnel, 84
Details-IPv6-6rd, 85
Details-Ipv6-AICCU, 79
Details-IPv6-DHCPv6 Client, 81
Details-IPv6-Offline, 76
Details-IPv6-PPP, 76
Details-IPv6-Static IPv6, 82
Details-IPv6-TSPC, 77
Details-LAN-DMZ, 108
Details-LAN-Ethernet, 106
Details-PPTP/L2TP, 68
Details-Static IP or Dynamic IP, 65
Determine Real WAN IP, 151
DFS Restrictions, 248

DHCP, 40
DHCP Client Identifier, 67
DHCP Server Configuration, 107, 109, 111
DHCP Server IP Address, 107, 109
DHCP Table, 661
DHCPv6 (Stateful), 113
DHCPv6 Server, 114
Diagnose, 158, 217
Diagnostics, 656, 657
Dial-out Triggering, 657
DialPlan, 291
Digit Map, 293
Digital Signature, 313, 328
Display Name, 56, 58, 61
DMZ Host, 138
DNS Cache Table, 663
DNS Filter, 379
DNS Filter Profile, 416
DNS Security, 157
DNS Server, 158
DNS Server IP Address, 67, 107, 110
DNS Server IPv6 Address, 114
Do Not Disturb, 297
Domain, 158
Domain Diagnose, 158
Domain Name, 67, 150, 216
DoS Defense, 375, 391
DoS Flood Table, 677, 679
Download Limit, 269
DrayTek Banner, 389
DTMF, 302
Dynamic DNS, 146, 148
Dynamic DNS Account, 150, 152

E

Each / Shared, 477
Enable PING to keep alive, 65
End IPv6 Address, 114
End Port, 142
ESP, 328
Event Code, 439
Event Log, 584
Extension WAN, 115
External Devices, 607
External RADIUS, 161
External TACACS+, 164

F

Failover, 56, 59
Failover to/Failback, 205
File Explorer, 646
File Extension Object, 626
Filter Setup, 381
Firewall, 374
Firmware Upgrade, 467
Fixed IP, 64, 69, 89
Force NAT /Force Routing, 214
Force Update, 149
Fragment Length, 267
Function Support List, 586

G

Gateway IP Address, 67, 107, 109
General Mode, 349
General Setup, 54
Get Community, 455
Google Map, 556
GRE, 336
Green Field, 266
Group, 598
Group ID, 171, 180
Guard Interval, 266
GUI Map, 27

H

Hardware Acceleration, 130
Hardware Installation, 12
Hide caller ID, 298
Hide SSID, 255
High Availability, 178
High Availability Status, 673
Host Name, 41
Hot-Standby, 179

I

IAID, 81
ICMP, 346
Idle Timeout, 64, 89, 327
IGMP, 170
IGMP Proxy, 170
IGMP Snooping, 170
IKE Authentication Method, 335
IM, 403
Incoming Port, 145
Incoming Protocol, 144
Indicators and Connectors, 2, 10
Installation, i
Inter-LAN Routing, 106
Internal RADIUS, 162
Internal Service User List, 471
Internet Access, 60
Internet Access - Advanced, 61
IP (Internet Protocol), 52
IP Address, 67, 69, 106, 109, 111
IP Address Assignment Method (IPCP), 64
IP Address Assignment Method(IPCP), 69
IP Address List, 155
IP Based, 55
IP Bind List, 126
IP Call, 285
IP Filters, 374
IP Object, 611
IP Pool Counts, 107, 109, 111
IP Routed Subnet, 476
IPsec General Setup, 323
IPsec Tunnel, 327
IPsec VPN Settings, 549
IPTV, 89
IPv4 Border Relay, 86
IPv4 Mask Length, 86
IPv6 Address, 82
IPv6 Gateway Address, 82
IPv6 Group, 618
IPv6 Neighbour Table, 660
IPv6 Object, 616
IPv6 TSPC Status, 672
Isolate, 255
ISP Access Setup, 62, 68
ISP Name, 89

K

keep alive, 331
Keep Alive Period, 439
Keep WAN Connection, 65
Keyword Group, 625
Keyword Object, 623

L

LAN, 102
LAN DNS / DNS Forwarding, 146, 154
LAN- General Setup, 104
LAN Port Mirror, 128
LAN Routed Prefix, 84
LAN to LAN, 329
Landing Page, 498, 502
Last Call Return, 297
LDAP, 166
LDAP /Active Directory Setup, 146
Lease Time, 107, 109, 111
Line Speed, 55, 56, 58
Load Balance, 59, 585
Load Balance for AP, 568
Load Balance Mode, 55
Load-Balance, 220
Load-Balance /Route Policy, 212
Local 802.1X, 471
Local 802.1X General Setup, 183
Local Certificate, 313, 366
Local ID, 328
Local IP Address, 141
Log, 410
Log & Alert, 558
Login, 48
Login Name, 151
Login Page Greeting, 446
Login Page Logo, 498
Login Password, 596
Logout, 29
Long Preamble, 266

Loop through, 292
LTE, 44, 234
LTE hardware version, 75
LTE Status, 243

M

Mail Alert, 174
Mail Extender, 151
Mail Service, 174
Main Screen, 22
Maintenance, 600
Management, 433, 457
Management Interface, 180
Max User Login, 501
Mic Gain, 302
Min/Max Interval Time, 115
Mirror Port, 128
Mode, 250, 256
Modem Code Upgrade, 468
Modem Dial String, 71
Modem Initial String, 71
Modem Initial String2, 71
Modem Support List, 70, 72, 650
mOTP, 327, 359
MPPE, 321
MTU, 63, 66, 68, 73, 75, 115
Multicast via VPN, 327, 359
Multiple SSID, 246
multiple-WAN, 54
Multi-VLAN, 87
MyVigor, 46, 412

N

Name Link, 25
NAT, 133
NAT Sessions Table, 662
NAT Traversal, 169, 284, 288
Neighbor AP Detection, 581
NetBios Name Service, 644
Netbios Naming Packet, 327
Network Configuration, 106, 109, 111
Network Interface, 211
Network Mode, 73, 74
Notification Object, 633
NS Detect, 81

O

Objects Settings, 610
Online Statistics, 479
OP Number, 294
Open Ports, 141
Operation Mode, 266
Option Number, 61

P

P2P, 404
PAP, 322
Password, 62, 67, 68, 75, 78, 79, 89
Password Strength, 257, 443
Path MTU Discovery, 63, 66, 68, 73, 75
Peer ID, 319
Peer-to-Peer, 281
Per Station Limit, 269
Phone Book, 291
Phone Settings, 299
Physical Connection, 30
Physical Members, 91
Physical Mode, 55, 56, 58, 61
Physical Type, 55, 56
PIN Code, 359
Ping Detect, 63, 66, 71, 73, 76, 78, 80, 81, 82, 84, 86
Ping Diagnosis, 664
Ping Gateway IP, 63, 66, 71, 73, 75
Ping Interval, 63, 66, 71, 73, 75
PING Interval, 65
Ping IP/Hostname, 76, 78, 80, 81, 82, 84, 86
Ping Retry, 63, 66, 71, 73, 75
Policy, 501
Polling Interval, 549
Port Redirection, 134
Port Triggering, 143, 145
Port-based Bridge, 88
Port-Based VLAN, 121
PPP Authentication, 64, 69, 71, 89

PPP General Setup, 321
PPP Password, 71
PPP Setup, 69
PPP Username, 71
PPP/MP Setup, 64
PPPoE, 34
PPPoE Pass-through, 63
PPTP, 327
PPTP/L2TP, 37
Prefer Codec, 289
Prefix Len, 210
Prefix Length, 82
Pre-shared Key, 265
Pre-Shared Key (PSK), 257
Primary DNS Sever, 114
Primary IP Address, 107, 110
Primary/Secondary Ping IP, 63, 66, 71, 73, 75
Printer Server, 644
Priority, 57, 91, 123, 205, 217
Priority ID, 180
Private IP, 136
Private IP Address, 52
Private Port, 136
Production Registration, 48
Protocol, 180, 404
Protocol Processing Engine (PPE), 130
Provider Host, 150
Psec Peer Identity, 324
PSTN Setup, 298
Public IP Adderss, 52
Public Port, 136

Q

QoS Setting Example, 491
Quality of Service, 472, 478
Quick Access, 26
Quick Start Wizard, 33
Quota Limit, 93

R

RADIUS/TACACS+, 146, 161
Rate Control, 103
Reboot System, 466
Recipient, 173
Recipient Number, 240
Redundancy Method, 179
Regional, 297
Registering Vigor Router, 48
Regular DN, 167
Regular Mode, 166
Regular Password, 167
Relay Agent, 107, 109
Remote Access Control, 320
Remote Dial-in User, 326
Remote Endpoint IPv4 Address, 84
Repeater, 262, 265
Replace, 293
Restore, 126
Ring Pattern, 289
Ring Port, 289
RIP Protocol, 66
RIPng Protocol, 77, 81, 115
Rogue AP Detection, 581
Rogue APs, 583
Root CA, 370
Route Policy, 205
Router Advertisement Configuration, 115
Router Commands, 241
Router Name, 67, 451
Routing, 205
Routing Information Protocol, 103
Routing Table, 658
RTP, 284
RTP TOS, 284
RTS Threshold, 267
Rule-Based, 497

S

SAS Voice Prompt, 284
Scan, 270
Schedule, 146, 159, 255
Secondary DNS Server, 114
Secondary IP Address, 107, 110
Secure Phone, 284
Security, 256, 373

Security Key, 250
Self-signed, 357
Self-Signed Certificate, 464
Send SMS, 240
Sensor, 648
Server Address, 68
Server Certificate, 357
Server IP Address, 162
Server Response, 151
Service, 144
Service Activation Wizard, 46
Service API, 150
Service Name, 71, 136
Service Provider, 150, 152, 629
Service Type, 150
Service Type Group, 621
Service Type Object, 619
Sesseion Based, 55
Sessions Control, 378
Sessions Limit, 472, 474
Set Community, 455
回復出廠預設值(Set to Factory Default), 148, 159, 206
Setup Query Server, 413
Shared Secret, 162, 163, 165
SIM card, 234
SIM PIN code, 70, 74
Simple Mode, 166, 237
SIP, 280
SIP Accounts, 286
SLAAC(stateless), 113
Smart Bandwidth Limit, 477
SMB, 644, 645
SMB Client Support List, 651
SMS / Mail Alert Service, 173
SMS Alert, 173
SMS Inbox, 237
SMS Provider, 173
SMS Quota Limit, 235
SMS/Mail Service Object, 628
SNMP, 455
Source IP, 136, 142, 144, 213
Speaker Gain, 302
Specific Hosts, 131
Specify Remote Node, 327
SPI, 375
SSID, 251
SSL Tunnel, 327
SSL VPN, 356
Start IP Address, 107, 109, 111
Start IPv6 Address, 114
Start Port, 142
Static IP, 39
Static Route, 103, 206
Static Route for IPv6, 210
Station Control, 268
Station List, 247, 277, 278
Station Number, 585
Stations (STA), 246
Status, 570
Strict Bind, 125
Strict Security Checking, 389
Strict Security Firewall, 377
String Object, 635, 636
Strip, 293
STUN Settings, 439
Subnet, 122
Subnet Mask, 67, 69, 106, 109, 111
Subnet Prefix, 79
Support List, 601, 605, 606
Switch, 591
Switch Hierarchy, 594
Switch Status, 591
Sync User Profile, 183
Syslog Alarm, 649
Syslog Explorer, 671
Syslog/Mail Alert, 451
System Maintenance, 434
System Status, 436
System time set, 159

T

T.38 Fax, 300
TACACS+, 363
Tag value, 57
Tagged VLAN, 121
TCP, 346

Temperature Sensor, 648
Time and Date, 454
Time Quota, 502
Time Schedule, 477
Time Server, 454
Time Zone, 454
Tone Power Level, 302
Total Traffic, 584
TR-069, 438
Trace Route, 670
Traceable, 485
Traffic Graph, 580, 668
Traffic Threshold, 56, 59
Trap Community, 456
Triggering Port, 144
Triggering Protocol, 144
Troubleshooting, 655
Trusted CA, 371
Trusted CA Certificate, 370
TSPC, 77
TTL (Time to Live), 63, 66, 73, 75, 76, 78, 80, 81, 82, 84, 86
Tunnel Broker, 78, 79
Tunnel ID, 79
Tunnel TTL, 84
TX Power, 267

U

UDP, 346
Unique Local Address (ULA), 113
Update DDNS, 180
Upload Limit, 269
UPnP, 147, 169
URL Access Control, 410
URL Content Filter, 379, 401
URL Content Filter Profile, 408
USB, 42
USB Application, 642
USB Device Status, 647
USB General Settings, 643
USB User Management, 644
User Account, 358
User Group, 362, 504
User Management, 496
User Online Status, 505
User Password, 443
User Profile, 164, 183, 499
User-Based, 497
Username, 62, 67, 68, 78, 79, 89
UserName, 75

V

VID, 123
View SMS Outbox Cache, 240
Virtual LAN, 103
Virtual Panel, 25
Virtual WAN, 32
VLAN, 121
VLAN Applications, 692
VLAN Configuration, 124
VLAN Tag, 87, 91, 123
VLAN Tag insertion, 57
Voice Active Detector, 290
VoIP, 279
VoIP Wizard, 282
Volume Gain, 302
VPN, 307, 547
VPN and Remote Access, 308
VPN Backup, 340
VPN Client Wizard, 309
VPN Dial-Out Through, 313
VPN Graph, 669
VPN Load Balance, 340
VPN Management, 557
VPN Server Wizard, 316
VPN Trunk Management, 340

W

Wake by IP Address, 172
Wake on LAN, 147, 172
WAN, 52
WAN Budget, 92
WAN Budget-Custom, 93
WAN Budget-Cycle duration, 93
WAN Budget-Status, 94

WAN Connection Detection, 63, 66, 71, 73, 75, 76, 78, 80, 81, 82, 84, 86
WAN Failure, 56
WAN Inbound Bandwidth, 480
WAN Interface, 136, 141, 150, 152
WAN IP Alias, 64, 67, 69
WAN IP Network Settings, 67, 69
WAN Outbound Bandwidth, 480
WAN Setup, 89
WAN Type, 87, 89, 91
WCF, 2
WDS, 262
Web Console, 28
Web Content Filter, 379, 401
Web Content Filter Profile, 412
Web Feature, 411
WEP, 247, 257
white/black list, 258
Wildcard, 151
Wired 802.1x, 129
Wireless LAN, 245
Wireless Wizard, 249
Wizard Mode, 382
WLAN Isolation, 247
WLAN Profile, 571
WMM Capable, 267
WPA, 247, 257
WPS, 248, 259

Z

ZRTP+SRTP, 292