

5 Advanced Configuration

After you complete the proceeding configuration correctly, the VDR824/824g can access all Internet services. This chapter introduces how to configure the advanced functions of the VDR824/824g to enhance the performances, thereby satisfying various demands on network configuration.

5.1 Binding LAN Ports to PVCs

Click [LAN/PVC] to enter the [Attachment Setting] page. You can bind the Ethernet port to a PVC and set the corresponding QoS parameters for PVC.

I. PVC Binding Settings

With the PVC binding function, you can bind any of the four Ethernet ports (LAN ports) to any of the four upstream PVCs. Each PVC bridges data from the bound Ethernet port to the broadband access server (BAS) to accommodate different Internet services through different Ethernet ports. Services such as the Internet accessing, video-on-demand (VOD), and IPTV carried out by different access servers improve security and stability of the system and ease the load of BASs remarkably.

You can also configure an Ethernet port as a management port to manage devices. You can access the configuration management page of your VDR824/824g through a host that is connected to the management port. By default, the four LAN ports of the VDR824/824g are all the management ports.

Figure 5-1 PVC Binding Settings

As Figure 5-1 shows, there are five options for each Ethernet port (LAN1 to LAN4) in the drop-down list: Attached to PVC1/2/3/4 and Attached to Router (Default).

Upon the configuration of these LAN ports, you need to click <Apply> to save your configuration and have it take effect. Then in the [PVC Setting] section set VPIs/VCI for the corresponding PVCs. Values of VPI/VCI are provided by your ISP. Click <Apply> in this section to save your configuration.



Caution:

- You can manage your VDR824/824g only through the PC connected to the management port or the USB port.
- If all the four Ethernet ports are configured to be bound to PVCs, you can still access the configuration management page through the USB port. Refer to section 8 “Appendix - USB Configuration” for more information about the USB port.
- The VPI/VCI values of different PVCs cannot be identical with each other or the same as those on the other configuration pages.

The following example illustrates the configuration upon the assumption:

- Bind a LAN port to PVC 0/35 to access the IPTV Website that your ISP set up. The Website uses DHCP to assign IP addresses dynamically.

- Bind other two LAN ports to PVC 0/100, and the PCs connecting to these ports access the Internet through PPPoE dial-up connections.
- Route the last LAN port to access the Internet and apply NAT-enabled PPPoE service on this port. Bind it to PVC 8/35. The user name and password your ISP assigns are **username** and **myPassword** respectively.

Follow these steps to achieve the settings on your VDR824/824g.

- 1) On the [Ethernet Port Attachment Setting] page (see Figure 5-2), select the **Attached to PVC1** option from the LAN1 drop-down list to bind LAN1 to PVC1 and bind LAN2 and LAN3 to PVC2 in the same way. Leave the LAN4 default setting **Attached to Router** untouched. Click the <Apply> to save your configuration.
- 2) In the [PVC Setting] section, set **0/35** as the VPI/VCI value of PVC1, **0/100** as that of PVC2. Click <Apply> in the [PVC Setting] section to save your settings. Since you do not use PVC3 and PVC4 here, there is no need to specify VPI/VCI values for them.

Attachment Setting

Ethernet Port Attachment Setting

Except the USB port, users CANNOT access the webpages through any LAN ports attached to PVCs. So it that at least one LAN port be reserved as "Attached to Router".

LAN1:	Attached to PVC1
LAN2:	Attached to PVC2
LAN3:	Attached to PVC2
LAN4:	Attached to Router (Default)

PVC Setting

PVC1:	VPI: 0	VCI: 35	QoS Setting...
PVC2:	VPI: 0	VCI: 100	QoS Setting...
PVC3:	VPI: 0	VCI: 37	QoS Setting...
PVC4:	VPI: 0	VCI: 38	QoS Setting...

Figure 5-2 Actual configuration on the Attachment Setting page

- 3) Click <Quick Setup> in the navigation bar and select the PPPoE Login option on the [WAN Connections] page. Set the values of VPI and VCI to **8** and **35** respectively, type **username**, **myPassword**, and **myPassword** in the PPPoE Username, PPPoE Password, and PPPoE Password (confirm) text boxes respectively and then click <Apply> to save your settings.

WAN connections
This page allows you to set up some authentication & login details which may be required

Login Type

☐ No Login / DHCP
☒ PPPoE Login

PPPoE Login Setup

VPI: 8
VCI: 35
PPPoE Username: uerName
PPPoE Password: [masked]
PPPoE Password (confirm): [masked]
PPPoE Access concentrator: [optional]
[Apply] [Reset]

Figure 5-3 Set the PPPoE authentication information

- 4) It takes about two minutes for your settings to take effect. Figure 5-4 depicts these settings. Actual configuration on the WAN connections page Click <Status> in the navigation bar to bring up the [Status] page as shown in Figure 4-48. You can find that the WAN IP Address item is a public IP address instead of the original one 0.0.0.0. Then you can access the Internet through a PC connected to the LAN4 port.

Status

PPPoE Connection: Connection established [Disconnect]

Connected time so far: 00:14:56s

WAN IP Address: 42.42.42.42
Local IP Address: 192.168.1.1
MAC Address: 00:0F:E2:04:1B:85
Primary DNS: 20.2.0.100
Secondary DNS: 10.72.66.36

Figure 5-4 Actual settings on the Status page

- 5) Verify the binding of the LAN ports to the PVCs. Connect a PC which is configured to obtain an IP address automatically to the LAN1 port. You can then access the IPTV Website of your ISP. Similarly, connect PCs to the LAN2 and LAN3 ports and access the Internet by PPPoE connection. After you enter the user name and password, the PC can obtain an IP address quickly and set up a connection with the Website.

II. QoS configuration

For the upstream packets over an ADSL line, your VDR824/824g supports multiple asynchronous transfer mode (ATM) services, such as CBR, VBR-rt, VBR, UBR, and ABR. DR814Q provides different measures, caching space, scheduling priorities, and service shaping to allocate appropriate bandwidth to ATM services of different types. This ensures high-performance QoS.

Click <QoS Setting...> in the [PVC Setting] section as shown in Figure 5-1 to enter the [QoS Config] page of a corresponding PVC as below.

Figure 5-5 QoS Config page

You can set different ATM service types for specified PVCs from the ATM Traffic Class drop-down list and configure QoS parameters for the selected service type. For more information, refer to Table 5-1.

Table 5-1 Description of commonly used ATM service types

Service type	Description
UBR (unspecified bit rate)	Suitable for services that are not real-time-critical and with large burst traffic. UBR demands best-effect services on the network side. When applying for services, you are not required to set QoS parameters except for PCR, which limits the upper rate. The network side does not guarantee QoS for UBR services. UBR cells will be discarded first in a network congestion. Error correction is carried out by upper-layer protocols. Typical applications are FTP and E-mail.

Service type	Description
CBR (constant bit rate)	Suitable for services that require static bandwidth and demand the highest priority. This type of service can provide stable traffic with the minimum burst. Only PCR parameter is needed for CBR service application. The source can transmit cells at a negotiated PCR or a rate lower than it. Typical applications are circuit and emulated voice.
VBR-rt (real-time variable bit rate)	Sensitive to delay and jitter of data flow. Similar to CBR except that they are delay- and jitter-sensitive. VBR-rt services allow limited burst. The transmission rate on source side can be different at different time. The parameters required for VBR-rt service application include PCR, SCR, and MBS or BT. Typical VBR-rt applications are voice and interactive video services and IPTV.
VBR (non-real-time variable bit rate)	Suitable for bursting non-real-time services. Compared to VBR-rt, a distinct feature of VBR services is that demands of real-time are not so crucial, and the priority for service data processed on the network side is also lower than that of VBR-rt. The parameters required by VBR services include PCR, SCR, and MBS (or BT), the same as that of VBR-rt.

Keep 0 unchanged for those options unrelated to the configuration. As shown in Figure 5-5, if **VBR-rt** is selected from the ATM Traffic Class drop-down list, you need to set values for Peak Cell Rate, Max Burst Size, and Sustainable Cell Rate and leave **0** in the Burst Tolerance and Minimum Cell Rate text boxes.

An example is taken to explain how to configure ATM QoS parameters. You must configure to meet the following requirements for the ATM QoS parameters of your VDR824/824g to take effect:

- The digital subscriber line access multiplexer (DSLAM) has a relax control or even no control over the LAN port and PVC upstream rates, entirely depending on the ADSL line. The actual upstream rate of ADSL can be 896 Kbps at most if DSLAM supports ADSL only.
- Multiple PVCs are configured on a single ADSL line.

Suppose that:

The downstream rate of each PVC is strictly specified by the central office (CO), whereas the upstream rates of the PVCs are all configured to 896 Kbps. PVC1 and PVC2 are configured on each ADSL line, among which you use PVC1 to access the Internet and PVC2 to provide video chatting service.

Analysis:

Although an upstream rate of 896 Kbps is configured to PVC1 and PVC2 respectively at the CO, audio and video services carried out over them may still be interfered. For example, an uploading service, which consumes a bandwidth larger than 500 Kbps, bursts on PVC1 when a video conference, which requires a minimum bandwidth of 384 Kbps for both upstream and downstream rates, is carried out over PVC2. This results in

the available bandwidth for PVC2 less than 384 Kbps, thus causing the audio and video service interrupted.

To avoid this, configure the QoS parameters as follows:

- 1) Click <QoS Setting...> in the [PVC Setting] section as shown in Figure 5-1 to enter the [QoS Config] page of PVC2.
- 2) Select the **VBR-rt** option from the ATM Traffic Class drop-down list.
- 3) Set Peak Cell Rate to **2000** (approximately 800 Kbps), Max Burst Size to **6000**, and Sustainable Cell Rate to **1000** (approximately 400 Kbps).
- 4) Click <Apply> to save your settings.

QoS Config

QoS of 'PVC2'

QoS of 'PVC2'

VPI/VCI: 0/36

ATM Traffic Class: VBR-rt

Peak Cell Rate: 2000

Burst Tolerance: 0

Minimum Cell Rate: 0

Max Burst Size: 6000

Sustainable Cell Rate: 1000

Apply **Reset**

Figure 5-6 QoS configuration

For PVC1, keep the default UBR settings unchanged. Thus, PVC1 can occupy all the upstream bandwidth when there is no traffic on PVC2, and PVC2 can always be guaranteed with an average bandwidth of 400 Kbps for audio and video services over it. This ensures normal upload over PVC1 and non-interrupted real-time communication over PVC2.

5.2 Security

Click [Security] in the navigation bar to enter the corresponding page where four tabs are available: Interface, Policy, Trigger and IDS. Click any tab to enter your desired configuration page.

5.2.1 Interface

Every firewall policy is intended for access between security interfaces. This page allows you to enable the security function and configure security interfaces.

Interface Policy Trigger IDS

Security Interface Configuration

Security State

Security: ☒ Enabled ☐ Disabled

Firewall: ☐ Enabled ☒ Disabled

Intrusion Detection: ☒ Enabled ☐ Disabled

[Change State](#)

Security Level

Security Level: n/a (Enable Firewall to set level)

Security Interfaces

Name	Type	NAT	
iplan	internal	May be configured on external or DMZ interfaces	Delete Interface...
ipwan	external	Disable NAT to internal interfaces Advanced NAT Configuration...	Delete Interface...

Figure 5-7 Add a security interface

I. Security state

To enable/disable the security function, select the corresponding **Enabled/Disabled** option, and then click <Change State>.

Likewise, such operation can also be used to enable/disable the firewall and intrusion detection.



Caution:

- You can enable the firewall, intrusion detection and NAT only when the security function is enabled.
- If the security function is disabled, the firewall, intrusion detection and NAT are also necessarily disabled.

II. Security level

After the firewall is enabled, the [Security Level] drop-down list appears in the [Security Level] section as below.

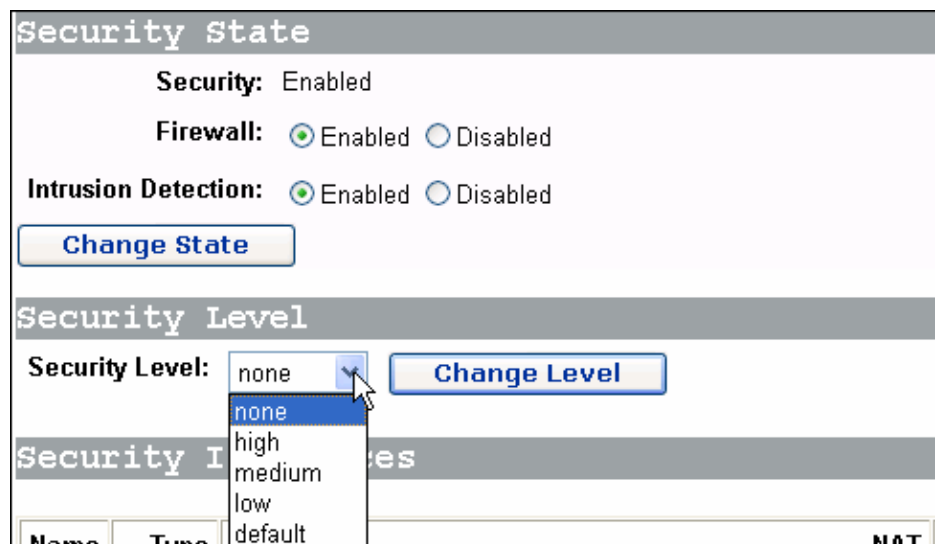


Figure 5-8 Security Level drop-down list

This drop-down list includes the following options:

- none: (default setting) Indicates that the external and internal users have no access right.
- high: Indicates that the internal users have some access rights and the external users have no access right.
- medium: Indicates that the external and internal users have more access rights.
- low: Indicates that the external and internal users have the maximum access rights.
- default: Indicates that the internal users can access all the Internet services, the external users are prevented to access the internal network

To set the corresponding security level, select an option from the drop-down list, and then click <Change Level>.



Caution:

- By default, the **none** security level is not configured with port filtering policies. In this case, internal users cannot access all the Internet services, and the internal network cannot be accessed from the outside, either. To enable the access right to a service, you need to configure the corresponding port policy. For details, refer to section 5.2.2 "Policy".
- The default port filtering policies are configured to the security levels except **none**. After a security level is set, the corresponding policy appears on the port filtering page. You can also configure a policy manually as needed. For details, refer to section 5.2.2 "Policy".

III. Security interface

You can establish the corresponding firewall policy between a group of security interfaces. The security interface table lists the information about existing security interfaces. By default, the VDR824/824g defines all interfaces as security ones and you cannot create a new security interface any more. If you have created a virtual interface (refer to section 4.3.1 "LAN"), <Add Interface...> appear on the page as below.

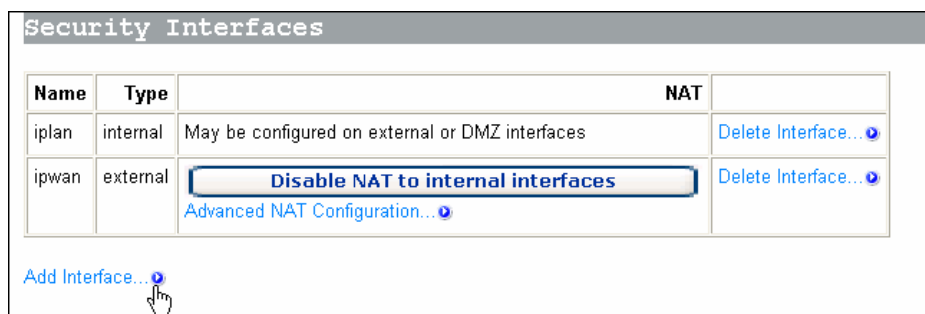


Figure 5-9 Security interface

In this case, you can add a security interface by clicking <Add Interface...> to enter the page as below.

Add Interface

Security: Add Interface

New Interface Setup

Name: item0

Interface Type: dmz

external
internal
dmz

Apply

[Return to Interface List](#)

Figure 5-10 Security – add an interface

Select an interface type, **external**, **internal** or **DMZ** from the [Interface Type] drop-down list, and then click <Apply>. The configured interface has been added to the security interface table on the [Security Interfaces] section as below.

Name	Type	NAT	
iplan	internal	May be configured on external or DMZ interfaces	Delete Interface...
ipwan	external	Disable NAT to internal interfaces Enable NAT to DMZ interfaces Advanced NAT Configuration...	Delete Interface...
item0	dmz	Enable NAT to internal interfaces Advanced NAT Configuration... (Enable NAT for Advanced Configuration)	Delete Interface...

Figure 5-11 Security interface table

To delete a security interface, click the corresponding <Delete Interface...> button, and then click <Delete> on the [Delete Interface] page.

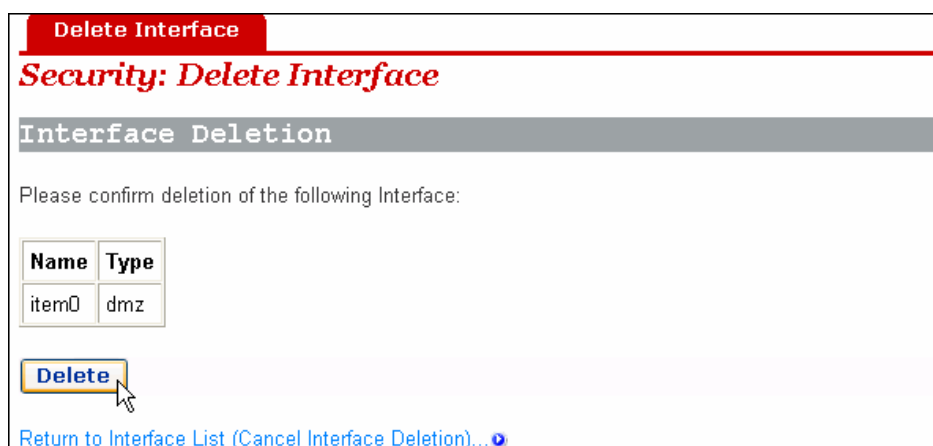


Figure 5-12 Delete a security interface

IV. NAT configuration

The NAT technology can translate an internal private address into a valid public IP address, and thus PCs in the LAN can share a public IP address for network access.

You can click the three buttons on the page as shown in Figure 5-11 to enable/disable NAT between the three types of interfaces. After the NAT is enabled, you can perform advanced NAT configuration. Click <Advanced NAT Configuration...> to enter the configuration page as below.

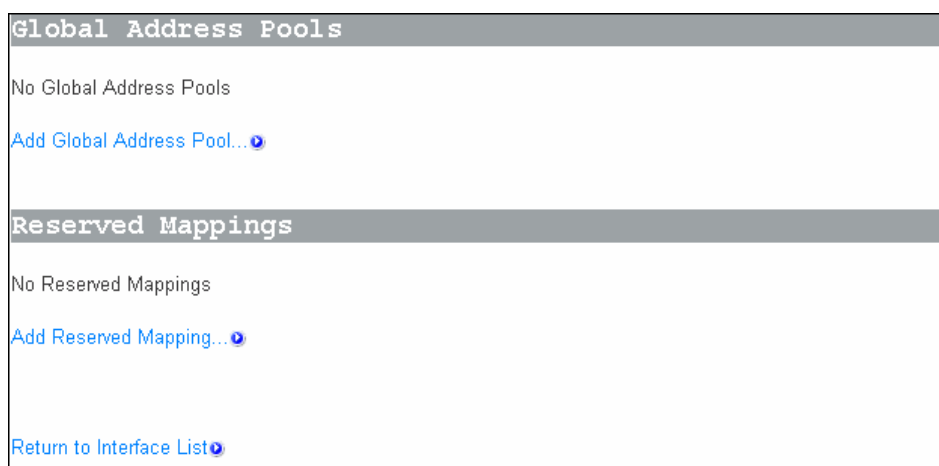


Figure 5-13 Advanced NAT configuration

1) Global address pool

This page allows you to add a public IP address obtained from your ISP to the global address pool. After NAT is enabled, internal addresses are randomly translated to an unused address in this pool.

To add a public IP address or an address pool, click <Add Global Address Pool...> to enter the configuration page as below.

Figure 5-14 Add a global IP address pool

Table 5-2 Description on the items of the global IP address pool

Item	Description
Interface Type	Select the interface type corresponding to a public IP address from the drop-down list.
Use Subnet Configuration	Select the method to specify the address from the drop-down list. The Use Subnet Mask option indicates to specify a network segment. The Use IP Address Range option indicates to specify a range of the IP address.
IP Address	Type in the IP address of a segment if the Use Subnet Mask option is selected. Type in the start IP address if the Use IP Address Range option is selected.
Subnet Mask/IP Address2	Type in the subnet mask of the segment if the Use Subnet Mask option is selected. Type in the end IP address if the Use IP Address Range option is selected.

Click <Add Global Address Pool> after the configuration is complete. This IP address will be added to the address pool.

2) Virtual server

After NAT is enabled, the internal network devices cannot be accessed from the Internet. To provide public services such as Web server, Email and FTP for the outside, a virtual server needs to be configured to make the network computer with private static IP address provide these services. Although the internal service address cannot be accessed by external users directly, the VDR824/824g can identify service requests through port number and forward them to the virtual server.

To configure a virtual server, click <Add Reserved Mapping...> in the [Reserved Mappings] section (see Figure 5-13) to enter the page as below.

Figure 5-15 Virtual server configuration page

Table 5-3 Description on the items of the virtual server

Item		Description
IP Address	Global	The default address, 0.0.0.0, can be reserved which means that the address obtained from the WAN port is used. Or you can type in the address from the global address pool.
	Internal	Type in the IP address of internal PC providing application services.
Transport	Type	Select the protocol type for the application service from the drop-down list.
External Port Range		Most application services forward inbound and outbound packets through the same port. In this case, you can just configure Start and End as this port number. But some application services forward inbound and outbound packets respectively through different ports. In this case, you need to type in the port range used by the inbound packets.
Internal Port Range		Most application services forward inbound and outbound packets through the same port. In this case, you can just configure Start and End as this port number. But some application services forward inbound and outbound packets respectively through different ports. In this case, you need to type in the port range used by the outbound packets.

Click <Add Reserved Mapping> after the configuration is complete.

Example: To configure the PC with the address 192.168.1.100 as a virtual server to provide an FTP service for the outside (with the port number 21), refer to the configuration in Figure 5-16. Thus, all FTP requests from the Internet users will be forwarded to the PC (server) with the fixed IP address 192.168.1.100.

IP Addresses		Transport	External Port Range		Internal Port Range	
Global	Internal	Type	Start	End	Start	End
0.0.0.0 (Set to 0.0.0.0 to use the primary IP address of the interface "ipwan")	192.168.1.100	tcp	21	21	21	21

[Add Reserved Mapping](#)

Figure 5-16 Example of the virtual server configuration

Note:

NAT can work between:

- External interface and internal interface
- External interface and DMZ
- DMZ and internal interface.

5.2.2 Policy

Security policy is a rule set to limit inbound and outbound data between different types of interfaces. The VDR824/824g provides a powerful security module to support the firewall policies configured between external and internal interfaces, between external interface and DMZ, and between DMZ and internal interface respectively, thereby satisfying various demands on network security. The firewall must be enabled before the creation of a policy.

Interface Type 1	Interface Type 2	Validators	Policy Configuration	
external	internal	Only listed hosts blocked	Port Filters...	Host Validators...
external	dmz	Only listed hosts blocked	Port Filters...	Host Validators...
dmz	internal	Only listed hosts blocked	Port Filters...	Host Validators...

[Return to Interface List](#)

Figure 5-17 Security policy configuration

I. Port filter

You can configure the port filtering policy to limit the data transmission of a protocol type.

To configure a group of interfaces (suppose external interface and internal interface) with the port filtering policy, click the corresponding <Port Filters...> button to enter the page as below.

Firewall Port Filters: external-internal

Source Address	Destination Address	IP Protocol	Source Port		Destination Port		Direction		
			Min	Max	Min	Max	Inbound	Outbound	
Any	Any	TCP	0	65535	80	80	false	true	Delete
Any	Any	UDP	0	65535	53	53	false	true	Delete
Any	Any	TCP	0	65535	21	21	false	false	Delete
Any	Any	ICMP	N/A	N/A	N/A	N/A	false	true	Delete

[Add TCP or UDP Filter](#)
[Add Raw IP Filter](#)
[Return to Policy List](#)

Figure 5-18 Firewall port filter

This page lists the currently configured policies. Select different firewall security level to display the corresponding port filtering policies. Other types of packet requests not configured with the policies will be blocked by the firewall.

To delete a policy, click the corresponding <Delete> button, and then click <Delete> to confirm on the popup page.

To add a policy for the port number of the protocol, click <Add TCP or UDP Filter> to enter the page as below.

Firewall Add TCP/UDP Port Filter: external-internal

Source address		Destination address		Protocol	Source port		Destination port		Direction	
									Inbound	Outbound
IP Address: 0.0.0.0		IP Address: 0.0.0.0		TCP	Range Start - End 0 - 65535		Range Start - End 0 - 65535		Allow	Allow
Mask: 0.0.0.0		Mask: 0.0.0.0								

Apply

Figure 5-19 TCP/UDP port filtering policy

Table 5-4 Description on the items of TCP/UDP port filter

Item		Description
Source address	IP Address	Type in the source IP address. The default address 0.0.0.0 indicates any node on the network.
	Mask	Type in the subnet mask of the source. The default mask 0.0.0.0 indicates any node on the network.
Destination address	IP Address	Type in the destination IP address. The default address 0.0.0.0 indicates any node on the network and is usually reserved.
	Mask	Type in the subnet mask of the destination. The default mask 0.0.0.0 indicates any node on the network and is usually reserved.
Protocol		Select a protocol type (TCP or UDP) from the drop-down list and apply the filtering policy to the packets of this type.
Source port	Range Start-End	Type in the port range of the source. The default range from 0 to 65535 indicates any node and is usually reserved.
Destination port	Range Start-End	Type in the port range of the destination. Generally, this parameter needs to be set. For example, to control Web services, type in the corresponding port number 80 . To control FTP services, type in the port number 21 .
Direction	Inbound	The direction of inbound data. Select Allow to permit external hosts to access internal hosts. Select Block to forbid external hosts to access internal hosts.
	Outbound	The direction of outbound data. Select Allow to permit internal hosts to access external hosts. Select Block to forbid internal hosts to access external hosts.

Click <Apply> after the configuration is complete. This policy will be added to the list of port filtering policies.

Example: If you want the internal users to access the external HTTP server (with the port number 80), but do not want the external users to access the internal HTTP server, you can perform the configuration as below.

Firewall Add TCP/UDP Port Filter: external-internal

Source address	Destination address	Protocol	Source port	Destination port	Direction	
					Inbound	Outbound
IP Address: 0.0.0.0	IP Address: 0.0.0.0	TCP	Range Start - End 0 - 65535	Range Start - End 80 - 80	Block	Allow
Mask: 0.0.0.0	Mask: 0.0.0.0					

Figure 5-20 Example of the port filtering configuration

To add a policy for a protocol, click <Add Raw IP Filter> in Figure 5-18 to enter the page as below.

Firewall Add Raw IP Filter: external-internal

Source address	Destination address	IP Protocol	Direction	
			Inbound	Outbound
IP Address: 0.0.0.0	IP Address: 0.0.0.0	Number or name: TCP	Allow	Block
Mask: 0.0.0.0	Mask: 0.0.0.0			

Apply

Figure 5-21 Filtering policy based on the protocol type

Table 5-5 Description on the items of the filtering policy

Item		Description
Source address	IP Address	Type in the source IP address. The default address 0.0.0.0 indicates any node on the network.
	Mask	Type in the subnet mask of the source. The default mask 0.0.0.0 indicates any node on the network.

Item		Description
Destination address	IP Address	Type in the destination IP address. The default address 0.0.0.0 indicates any node on the network and is usually reserved.
	Mask	Type in the subnet mask of the destination. The default mask 0.0.0.0 indicates any node on the network and is usually reserved.
IP Protocol	Number or name	Type in a protocol name or number and apply this filtering policy to the packets of this type. The protocol name can be TCP, UDP or ICMP. For other protocols, you need to type in their protocol numbers. For example, type in 2 for IGMP, and 46 for RSVP.
Direction	Inbound	The direction of inbound data. Select Allow to permit external hosts to access internal hosts. Select Block to forbid external hosts to access internal hosts.
	Outbound	The direction of outbound data. Select Allow to permit internal hosts to access external hosts. Select Block to forbid internal hosts to access external hosts.

Click <Apply> after the configuration is complete. This policy will be added to the list of port filtering policies.

Example: By default, the external hosts are not allowed to ping the WAN port even if the security level is set to **low**. To allow the internal hosts and external hosts to ping each other, you can perform the configuration as below.

Firewall Add Raw IP Filter: external-internal

Source address	Destination address	IP Protocol	Direction	
			Inbound	Outbound
IP Address: 0.0.0.0	IP Address: 0.0.0.0	Number or name: ICMP	Allow	Allow
Mask: 0.0.0.0	Mask: 0.0.0.0			

Figure 5-22 Example of the filtering policy for a protocol (2)

II. Host validators

By specifying the IP address and configuring the corresponding policy, you can restrict the access right of a host or hosts on a network segment.

To configure host validators to a group of interfaces, click the corresponding <Host Validators...> button in the [Current Security Policies] section (see Figure 5-17) to enter the page as below.

Figure 5-23 Host validators page

To add a host validator policy, click <Add Host Validator...> to enter the page as below.

Figure 5-24 Configure a host validator

Table 5-6 Description on the items of the host validator

Item	Description
Host IP Address	Type in the IP address of the host or network segment to be restricted.
Host Subnet Mask	Type in the subnet mask of the host or network segment to be restricted.
Direction	Select the direction of data transmission. Select inbound to block the inbound data only. Select outbound to block the outbound data only. Select both to block both inbound data and outbound data.

Example: To block a host with the IP address 192.168.1.10 in the LAN to access an external network, and permit the external users to access this host, you can perform the configuration as below, and then click <Apply>.

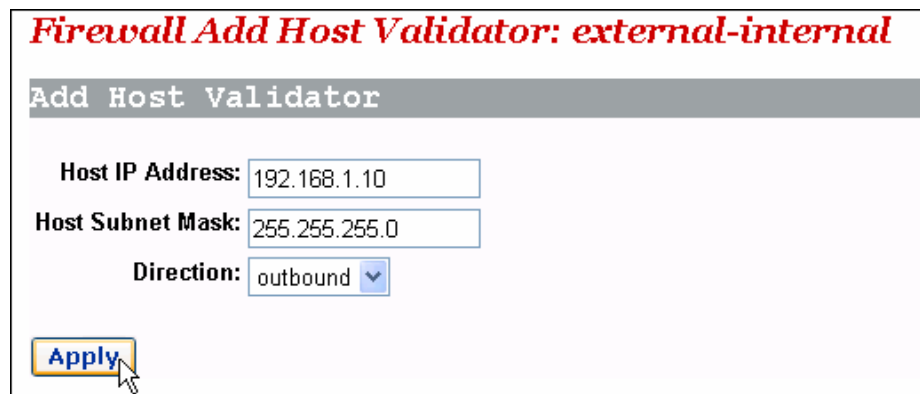


Figure 5-25 Example of the host validator configuration (1)

Example: If you find a suspicious host (with the IP address 10.1.1.2) in an external network, you can set the host validator policy as below to block its attack on the internal host.

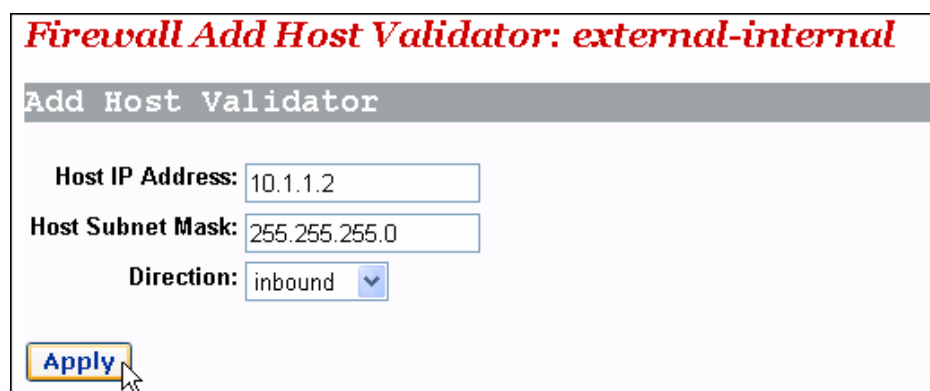


Figure 5-26 Example of the host validator configuration (2)

As shown in Figure 5-26, **inbound** is selected from the [Direction] drop-down list, and thus the device only block the data from the address 10.1.1.2 to the internal host while the internal host can still send data to the address 10.1.1.2.



Caution:

- The host validator can be used to limit the data stream between the WAN and LAN ports.
- The security policy takes effect only when the firewall is enabled.

5.2.3 Trigger

A security trigger is used to deal with application protocols that set up separate sessions. Some application protocols, such as NetMeeting, open the primary sessions and secondary connections at the same time during the normal operations. The trigger tells the security mechanism to handle these secondary sessions and instruct it how to handle them. The trigger handles the situation dynamically, allowing the secondary sessions only when appropriate. These newly triggered sessions are not restricted by the firewall.

Interface

Policy

Trigger

IDS

Security Trigger Configuration

Current Security Triggers

Security Triggers										
Transport Type	Port Number Start	Port Number End	Secondary Port Number Start	Secondary Port Number End	Allow Multiple Hosts	Max Activity Interval	Enable Session Chaining	Enable UDP Session Chaining	Binary Address Replacement	Address Translation Type
tcp	1720	1720	1024	65535	true	3000	true	false	true	tcp
udp	1719	1719	1024	65535	true	3000	true	true	true	udp

New Trigger

Return to Interface List

Figure 5-27 Security trigger

This page allows you to:

- View the information in the current security trigger list.
- Create a new security trigger and add it to the current security trigger list.
- Delete an existing security trigger.

To create a new security trigger, click <New Trigger> to enter the page as below.

Security: Add Trigger

Transport Type	Port Number Start	Port Number End	Secondary Port Number Start	Secondary Port Number End	Allow Multiple Hosts	Max Activity Interval	Enable Session Chaining	Enable UDP Session Chaining	Binary Address Replacement
tcp			1024	65535	Allow		Allow	Allow	Allow

[Return to Trigger List](#)
[Return to Interface List](#)

Figure 5-28 Add a security trigger

Table 5-7 Description on the items of the security trigger

Item	Description
Transport Type	From the drop-down list, select a transport type (TCP or UDP) to which the newly added trigger is specified.
Port Number Start	Type in the start of the trigger port range that the primary session uses.
Port Number End	Type in the end of the trigger port range that the primary session uses.
Secondary Port Number Start	Type in the start of the trigger port range that the secondary session uses.
Secondary Port Number End	Type in the end of the trigger port range that the secondary session uses.
Allow Multiple Hosts	Select Allow if you want a secondary session to be initiated by different remote hosts. Select Block if you want a secondary session to be initiated only by one remote host.
Max Activity Interval	Type in the maximum activity interval (in milliseconds) for secondary port sessions after the primary session starts.
Enable Session Chaining	Select Allow or Block to determine whether the multi-level TCP session chaining is accepted or not.
Enable UDP Session Chaining	Select Allow or Block to determine whether the multi-level UDP session chaining is accepted or not. Before this, you must enable the session chaining.
Binary Address Replacement	Select Allow or Block to determine whether to use the binary address replacement on the current trigger or not.
Address Translation Type	Specify the address replacement type on a trigger. Before this, you must set the binary address replacement to Allow .

Click <Apply> after the configuration is complete. The [Security Trigger Configuration] page is displayed, containing details of the trigger that you have just configured.

To delete an existing security trigger, click the corresponding <Delete> button in Figure 5-27 and then click <Delete>.

Security Delete Trigger

Please confirm deletion of the following Trigger:

Transport Type	Port Number Start	Port Number End	Secondary Port Number Start	Secondary Port Number End	Allow Multiple Hosts	Max Activity Interval	Enable Session Chaining	Enable UDP Session Chaining	Binary Address Replacement	Address Translation Type
udp	1719	1719	1024	65535	true	3000	true	true	true	udp

[Delete](#)

[Cancel Trigger Deletion](#)

[Return to Interface List](#)

Figure 5-29 Delete a security trigger

In fact, the VDR824/824g has provided an Application Level Gateway (ALG) for NetMeeting. NetMeeting applications can be also normal even if the port trigger is not configured. The following example is taken to show how to configure a port trigger if the VDR824/824g does not provide the ALG for NetMeeting.

Suppose your PC is connected to the LAN interface of the VDR824/824g, and you want to use NetMeeting to have an audio/video chat with Internet users, and to apply whiteboard and program sharing.

Analysis:

A NetMeeting call is established on the TCP 1720 port. After the connection is established, NetMeeting needs to re-enable the TCP 1503 port to use whiteboard and program sharing. NetMeeting also needs to enable any port of TCP and UDP protocols within the range of 1024 to 65535 to transmit audio and video signals. After the firewall is enabled, you can configure the port filtering policies and virtual servers of TCP and UDP protocols to all ports within the range. In this way, Internet users can actively call a LAN user during the use of NetMeeting. However, possible omission in configuring the filtering policy and virtual server may cause the failure of the audio/video chat establishment. Moreover, the virtual server configuration exposes almost all the LAN host ports to the Internet, resulting in the insecurity of the host.

To solve these problems, you can perform the configuration as below to make the TCP 1720 port trigger TCP/UDP port within the range of 1024 to 65535.

Security: Add Trigger

Transport Type	Port Number Start	Port Number End	Secondary Port Number Start	Secondary Port Number End	Allow Multiple Hosts	Max Activity Interval	Enable Session Chaining	Enable UDP Session Chaining	Binary Address Replacement	Tr
tcp	1720	1720	1024	65535	Allow	30000	Allow	Block	Allow	to

Figure 5-30 Example of the trigger configuration

In this way, all applications provided by NetMeeting can be used normally after a LAN user calls the Internet user and you can just add the access policy suitable for packets on the TCP 1720 port on the corresponding page (see Figure 5-19). To make the Internet users call LAN users and use NetMeeting normally, you can just configure the virtual server on the TCP 1720 port on the corresponding page (see Figure 5-15) and combine it with the port trigger mentioned previously.

5.2.4 IDS

IDS protects the current network from the following attacks:

- Denial of Service (DoS).
- Port scanning.
- Web spoofing.

IDS also implements the blacklist function. It stops external hosts that try to invade the network from accessing the VDR824/824g within a specific time limit.

Interface
Policy
Trigger
IDS

Firewall Configure Intrusion Detection

Use Blacklist

Use Victim Protection

Victim Protection Block Duration

seconds

DOS Attack Block Duration

seconds

Scan Attack Block Duration

seconds

Scan Detection Threshold

per second

Scan Detection Period

seconds

Port Flood Detection Threshold

per second

Host Flood Detection Threshold

per second

Flood Detection Period

seconds

Maximum TCP Open Handshaking Count

per second

Maximum Ping Count

per second

Maximum ICMP Count

per second

[Return to Interface List](#)

Copyright 2003-2004 Huawei Tech

Figure 5-31 IDS configuration

Table 5-8 Description of the IDS configuration items

Item	Description
Use Blacklist	Select true or false to enable or disable the blacklist function. When the external host attacks (Ascend Kill, Echo Scan, WinNuke, Xmas Tree Scan, IMAP SYN/FIN Scan, SMURF, TCP SYN Flood, Net Bus Scan and Back Orifice Scan) are found, these hosts are put into the blacklist and their packets are filtered out within the set time limit.
Use Victim Protection	Select true or false to enable or disable the Smurf protection which protects the VDR824/824g against attacks caused by pings with a broadcast address. The attacker may broadcast pings with the victim's MAC address as the source MAC address. Without this protection, hosts in LAN will send response packets to the victim when receiving these packets, and even cause the collapse of the victim. With this protection, the VDR824/824g will detect and drop ICMP packets sent by the attacker and continue to do so within a specific time limit.

Item	Description
Victim Protection Block Duration	Block duration of Web Spoofing (Smurf) attacks on the host. If the device detects these attacks, it will filter all the ICMP packets that attack the host and continue to do so within a specific time limit. The default value is 10 minutes.
DOS Attack Block Duration	Block duration of DoS attacks on the host. If the VDR824/824g detects these attacks, it will filter all the packets that attack the host and continue to do so within a specific time limit. The default value is 30 minutes. DoS attacks will prevent legitimate users from accessing normal Internet services. The DoS attacks that the device can detect include Smurf Attack, SYN/FIN/RST Flood, ICMP Flood, Ping Flood, Ascend Kill, WinNuke Attack and Echo Chargen.
Scan Attack Block Duration	Block duration of port scanning attacks on the host. If the VDR824/824g detects these attacks, it will filter all the packets that attack the host and continue to do so within a specific time limit. The default value is 24 hours.
Scan Detection Threshold	Threshold of port scanning packets. When the VDR824/824g detects port scanning packets (such as SYN/ACK, FIN or RST) sent by a host per second and the number of packets reaches the threshold, the device regards them as port scanning attacks. The port scanning attacks that the device can detect include Echo scan, Xmas Tree scan, IMAP scan, TCP SYN ACK scan, TCP FIN RST scan, NetBus scan, Back Orifice scan and SubSeven. Most of port scanning attacks are the Trojan Horse attack.
Scan Detection Period	Statistics duration of port scanning. When the device detects that port scanning continues to reach the set time, the device will block all the packets that attack the host and continue to do so within the time limit set in the [Scan Attack Block Duration] text box. The default value is 60 seconds.
Port Flood Detection Threshold	When the device detects that TCP SYNC packets sent by a host per second to a fixed port exceed this threshold, the device will time the Flood attack. If the timing reaches the limit set in the [Flood Detection Period] text box, the VDR824/824g concludes that the host is making a port flood attack, and starts blocking the packets sent by the host. The default value is 10.
Host Flood Detection Threshold	When the device detects that TCP SYNC packets sent by a host per second exceed this threshold, the device will time the Flood attack. If the timing reaches the limit set in the [Flood Detection Period] text box, the VDR824/824g concludes that the host is making a port flood attack, and starts blocking the packets sent by the host. The default value is 20.

Item	Description
Flood Detection Period	When the VDR824/824g detects that the duration of Flood attack by a host reaches the set detection period, the device starts blocking the packets sent by the host. The default value is 10 seconds.
Maximum TCP Open Handshaking Count	When the open handshaking count that the VDR824/824g receives per second from a host exceeds the set value, the device concludes that the SYN/ACK attack is detected. The default value is 100.
Maximum Ping Count	The attacker may send a number of ping packets to a network. These packets consume too much bandwidth and make normal network services unavailable. When the device detects that the count of ping packets sent by a host per second exceeds the set value, the device concludes that the ping flood attack is detected. The default value is 15.
Maximum ICMP Count	The attacker may send a number of ICMP (non-Echo Request) packets to a network. These packets consume too much bandwidth and make normal network services unavailable. When the device detects that the count of ICMP packets sent by a host per second exceeds the set value, the device concludes that the ICMP Flood attack is detected. The default value is 100.

To modify the current IDS configuration, type in the relevant values of IDS options, and then click <Apply>.

To clear the blacklist, click <Clear Blacklist>.



Caution:

By default, the security mode is enabled.

5.3 DMZ Configuration

The Demilitarized Zones (DMZ) feature of VDR824/824g allows you to configure a DMZ in a LAN. The hosts that are configured on the same segment with this DMZ can perform bi-directional communication with other Internet users or servers. At the same time, you can enable NAT and configure a firewall policy between DMZ interface and internal interface, and between DMZ interface and external interface. This not only provides a security shelter for the hosts in the DMZ, but also satisfies the needs of

server installation in LANs by small and medium-sized enterprises to provide services such as FTP and Web for bi-directional communication with users.

The following figure depicts the steps to configure DMZ:

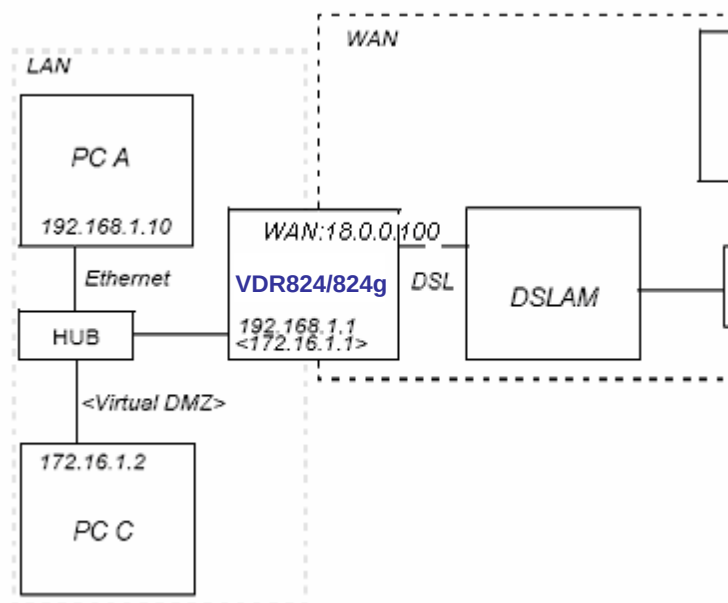


Figure 5-32 DMZ configuration

I. Create a virtual interface

To create a virtual interface, refer to section 4.3.1 "LAN".

Type in the following parameters on the [Create virtual interface] page as below, and then click <Apply>.

Create virtual interface

Create virtual interface

Configure new virtual interface:

IP Address

Netmask

Figure 5-33 Create a virtual interface

The result appears on the [LAN connections] page (see Figure 4-16), showing that a virtual interface named item0 has been added into the list.

II. Add an security interface

Refer to section 5.2.1 III. "Security interface" to add a security interface.

Perform the configuration on the [Add Interface] page as below, and then click <Apply>.

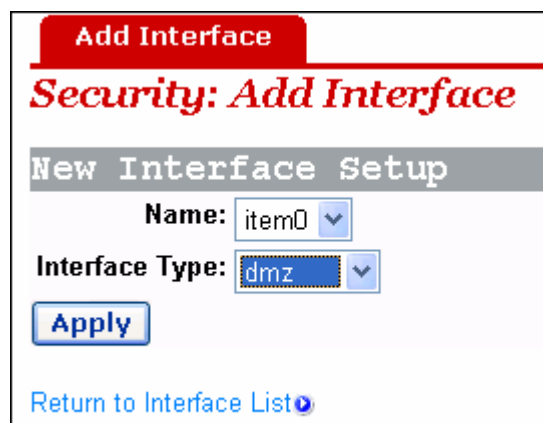


Figure 5-34 Add a security interface

Here, item0 is the virtual interface added previously.

III. Configure the port filtering policy for external-dmz and external-internal interfaces respectively

To configure port filtering policy for external-dmz and external-internal interfaces respectively, refer to section I. "Port filter".

Enter the [Firewall Port Filters: external-dmz] page to configure a policy, ensuring that users can access the Internet services (such as HTTP, FTP, and Telnet) specified by the DMZ zone through the external interface. Meanwhile, enter the [Firewall Port Filters: external-internal] page to configure the port filtering policy, ensuring to disable users under the external interface to access the host services under the internal interface.

IV. Configure a DMZ host in the same segment with a DMZ zone

Make sure that the IP address of the DMZ host is in the same segment as that of the above configured virtual interface. For example, configure the IP address to 172.16.1.100, the mask to 255.255.0.0, and enable the corresponding Internet service, and then connect this DMZ host to the LAN port of the VDR824/824g.

V. Configure the corresponding virtual server

To configure the corresponding virtual server, refer to section 5.2.1 IV. 2) "Virtual server".

Configure the DMZ host as a virtual server to provide the Internet services, such as http, ftp and telnet.

Thus, the entire DMZ is configured completely and securely.

5.4 Route Configuration

The static route configuration makes the VDR824/824g to communicate with PCs on different network segments. This option allows you to create static IP routes to destination addresses by an IP interface name or a gateway address.

To access the VDR824/824g configuration page, follow either of these steps:

- Click [WAN Setup] in the navigation bar to enter the [WAN Connections] page, and then click <Route setup...>.
- Click [LAN Setup] in the navigation bar to enter the [LAN Connections] page, and then click <Route setup...>.
- Click [Status] in the navigation bar to enter the [Status] page, and then click <Route setup...>.

Valid	Destination	Netmask	Gateway	Advertise	Delete?
✓	0.0.0.0	0.0.0.0	192.200.200.1	false	☐

[Advanced Options...](#)

[Apply](#) [Reset](#)

[Create new Ip V4Route...](#)

Figure 5-35 Route configuration

This page allows you to:

- View the information about existing routes
- Modify the route information in the route list
- Add a new route
- Delete an existing route

This page also allows you to view the following information about existing routes:

- Whether the route is valid ✓ or invalid ✗
- Destination IP address (Destination)
- Gateway address (Gateway)
- Network mask (Netmask)
- Whether the route is advertised via RIP (true or false)

To change the destination address, gateway address, netmask and advertise status of a route, change the settings in the relevant text boxes, and then click <Apply>.

To modify the cost or interface settings for the route, click <Advanced Options...> to enter the [Advanced Settings] page. Change the related value, and then click <OK>.

Name	Value
Destination	0.0.0.0
Netmask	0.0.0.0
Gateway	192.200.200.1
Cost	1
Interface	none
Advertise	false

OK Reset Cancel

Figure 5-36 Advanced Settings page

To delete an existing route, select the corresponding [Delete?] check box in Figure 5-35 and click <Apply>.

To add a new route, click <Create new Ip V4Route...> in Figure 5-35 to enter the [IP V4Route] page. Type in the related values of route options, and then click <OK>. Click <Cancel> to cancel the settings and return to the route configuration page.

Name	Value
Destination	0.0.0.0
Netmask	0.0.0.0
Gateway	
Cost	1
Interface	none
Advertise	false

OK Reset Cancel

Figure 5-37 Create a route



Caution:

For DHCP or Static IP services, you must type in the next hop address in the [Gateway] field (you cannot leave it blank), while you can set the [Interface] drop-down list to the default (None) or other value.

For other services (IPoA, PPPoA, and PPPoE), you can specify a value of either the interface or the gateway. If both of them are specified, only the interface value takes effect.

Example: Figure 5-38 illustrates a physical connection that requires static routes.

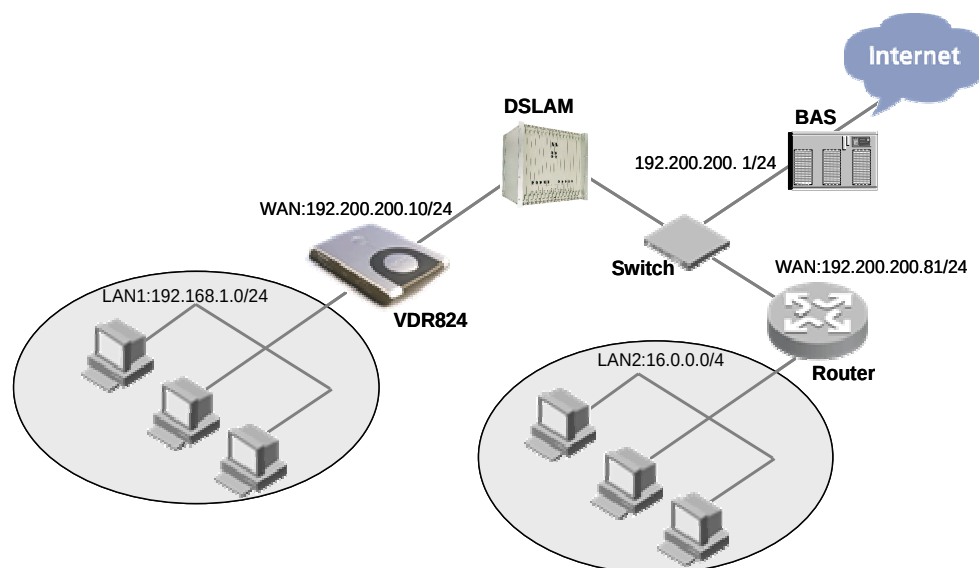
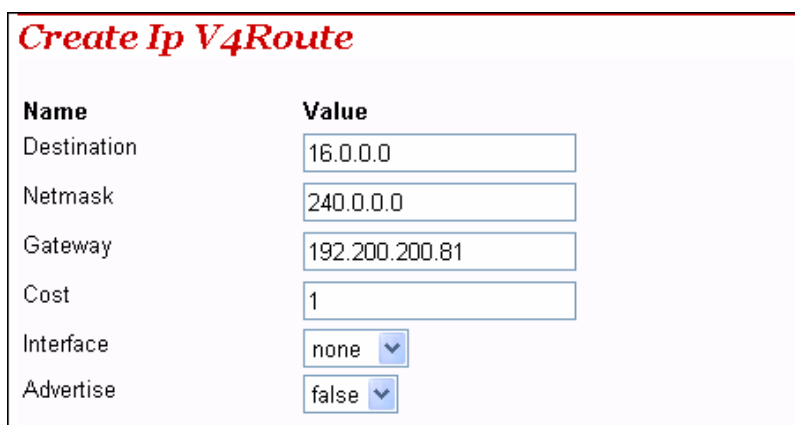


Figure 5-38 Network diagram for the static route configuration

In Figure 5-38, suppose that a DHCP service is configured for the VDR824/824g, the gateway address is 192.200.200.1, and there is a default route to broadband access server (BAS). A router is connected to another network segment, LAN2 (16.0.0.0/4), on the WAN side, and the IP address of the WAN port is 192.200.200.81. To make hosts in LAN1 access hosts in LAN2 normally, you need to create a route as below so that the VDR824/824g can choose routes for packets correctly.



Name	Value
Destination	16.0.0.0
Netmask	240.0.0.0
Gateway	192.200.200.81
Cost	1
Interface	none
Advertise	false

Figure 5-39 Example of the static route configuration

5.5 Service

Two tabs, SNTP and ZIPB, are available on the [Service] page. Click any tab to enter the corresponding configuration page.

5.5.1 SNTP

Configure the VDR824/824g as an SNTP client and thus you can obtain accurate time/date information from the corresponding SNTP server. If your router is not connected to the SNTP server, you can set the time/date on the VDR824/824g instead.

SNTP ZIPB SNMP

Current System Time: **May 08 2005 11:32:09**

Current Time Zone: **CCT**

Current Synchronized NTP Server: **time.nist.gov**

Synchronize Client with NTP Server now! **Synchronize**

Select a Local Timezone (+UTC/GMT time): **China Coast (+8h)** ▼

Set Timezone

SNTP - NTP Server Configuration Parameters

NTP servers:

IP Address | DNS Hostname

time.nist.gov **Delete**

Add NTP Server IP Address: **Add**

Add NTP Server Hostname: **Add**

Copyright 2003-2004 Huawei Tec

Figure 5-40 SNTP configuration

This page allows you to:

- View the current system time configuration
- Set the time zone
- Configure the NTP server on the Internet to make the clock of the VDR824/824g synchronize its internal clock.

To synchronize the local time of the router with the SNTP server, click <Synchronize>.

To set the time zone, select a desired option from the corresponding drop-down list and then click <Set Timezone>.

To add an NTP server, type in the IP Address or the domain name of the SNTP server in the [NTP servers:] field, and then click <Add>.

To delete an existing NTP server, click the corresponding <Delete> button.

5.5.2 ZIPB

ZZIPB (zero installation PPP bridge) can ensure that a SOHO user can obtain a public IP address through the router, and to resolve the problem that all SOHO routers with NAT enabled cause part of the application unable to function normally.

SNTP **ZIPB** SNMP

ZIPB is currently disabled.

[Enable](#)

Choose which computer will use the public IP address:

None ▾

[Apply](#)

ZIPB advanced configuration

Configure the specifics of how you wish ZIPB to operate here. At a minimum, ZIPB must be configured with a LAN interface and one WAN interface. If no interfaces are chosen, ZIPB will automatically use the LAN interface and the first available WAN interface. ZIPB will also do this if you choose an IP interface incorrectly. **Note:** Some settings may require you to disable and re-enable ZIPB.

LAN interface: none ▾

WAN interface: none ▾

[OK](#) [Reset](#)

Figure 5-41 ZIPB configuration

This page allows you to:

- Enable/disable the ZIPB mode
- Specify the ZIPB host
- Perform advanced ZIPB configuration.

If the ZIPB is currently disabled, click <Enable> to enable it. If enabled, click <Disable> to disable it.

Select the PC that will use the public IP address in the current LAN from the drop-down list, and then click <Apply>.

To perform advanced ZIPB configuration, follow these steps:

- Select the LAN interface on which ZIPB will run from the [LAN interface] drop-down list.
- Select the WAN interface on which ZIPB will run from the [WAN interface] drop-down list.

Click <OK> after the ZIPB configuration is complete.



Caution:

- Make ensure that ZIPB is disabled before you change the ZIPB configuration. Change the configuration, and then click <OK>. The new configuration will take effect after you enable ZIPB. Any change on the configuration takes no effect when the ZIPB is enabled.
- Configuration changes on ZIPB will not be saved, and so you need to reconfigure it whenever the router restarts. That is, make the previous ZIPB host obtain the IP address again through DHCP, and then specify a new ZIPB host from the drop-down list
- You can enable ZIPB only for two WAN services: PPPoE and PPPoA.

5.5.3 SNMP

The VDR824/824g supports simple network management protocol (SNMP) proxy function, exchanging SNMP information with the network management sites through SNMP.

community Name	Write Enable	ServerIP	
public	false	0.0.0.0	Delete
password	true	0.0.0.0	Delete
ADSL	true	127.0.0.2	Delete

Add a community:

community

WriteEnable

ServIP

Figure 5-42 SNMP Client Setting page

You can create an SNMP community in Figure 5-42 and this community will be displayed in the community list. The VDR824/824g authenticates the SNMP packets according to the defined information in the list.

To add a community, refer to the following information to perform the settings, and then click <Add>.

- community: Type in the community name, uniquely identifying an SNMP community. The packets mismatching the community name are discarded.
- WriteEnable: Specify the access right for the community. If **Read-Only** is selected, this community can only view the VDR824/824g information; if Read-Write is selected, this community can view or modify the VDR824/824g information.
- ServIP: Specify the IP address of the management site sending SNMP packets. It is recommended that you keep the default setting 0.0.0.0, which indicates the source IP address sending the SNMP packets is not restricted.

To delete the current community, click the corresponding <Delete>.

6 Troubleshooting

This chapter gives solutions to problems you may encounter when installing or using the VDR824/824g, and provides instructions for using several IP utilities to diagnose problems. Contact Customer Support if these suggestions do not resolve the problems.

6.1 VDR824/824g Troubleshooting

Symptom 1: The power LED does not illuminate.

Solution: Check whether:

- The power switch is turned on.
- The power adapter that comes with the VDR824/824g is used.
- The power adapter is securely connected to the VDR824/824g and the power socket.

Symptom 2: The ADSL2+ Link LED does not illuminate after the telephone cable is connected.

Solution: Check whether the telephone cable is securely connected to the ADSL port and the telephone port.

Symptom 3: The LAN LED does not illuminate after the Ethernet cable is connected.

Solution: Check whether:

- The power connection is good.
- The Ethernet cable is securely connected to the port.
- The correct cable is used. To check this, connect two ends of the cable to the LAN ports of the VDR824/824g, observe whether the corresponding LED illuminates. If not, change the cable and follow the steps described in section 2.3 “Device Connection” to set up the connection.
- The PC has an Ethernet NIC installed correctly.

Symptom 4: You forget your password.

Solution: If you have not changed the password, use the default user name (**admin**) and password (**admin**). Press the Reset button for at least five seconds to restore the default settings on the VDR824/824g. Then you can use the default user name and password.



Caution:

Resetting the VDR824/824g removes all the customized settings and restores the default ones.

Symptom 5: Fail to access the Web configuration page.

Solution: Follow the procedures to check whether:

- 1) The version of the Internet Explorer is Microsoft Internet Explorer 5.5 or Netscape 6.0 or later.
- 2) PC and the VDR824/824g are in the same network segment.
- 3) Use the **ping** command in an MS-DOS window to check the network connectivity:
 - Ping 127.0.0.1 to see if the TCP/IP protocol is installed.
 - Ping 192.168.1.1 (the default IP address of the gateway) to check for the connection between the PC and VDR824/824g in the LAN.
- 4) If the physical connections are normal, but you still cannot access the Web configuration pages of the VDR824/824g, make sure the proxy server and the dialup connection are disabled.

Symptom 6: Fail to access the Internet with your PC.

Solution: Follow the procedure:

- 5) Check whether the ADSL2+ Link LED is solid ON. If not, check the ADSL line connection.
- 6) Check whether the IP address is obtained and you can ping the IP address of the VDR824/824g's LAN port if you configure the PC to obtain the IP addresses of the host and the DNS server automatically (recommended). Refer to section 6.2.1 "Ping" for instructions on how to use the ping utility. If you cannot ping the port, check if the Ethernet cable is correct.
- 7) When the current PC is specified with a private IP address, make sure that: The PC resides in the same segment as that of the VDR824/824g's LAN port. The IP address of the gateway is specified as that of the DVDR824/824g's LAN port. The IP address of the DNS is specified as that of the VDR824/824g's LAN port or the DNS Server the ISP allocates. The host is able to ping the IP address of the VDR824/824g's LAN port.

- 8) When the host can communicate with the VDR824/824g normally, but cannot connect to the Internet, log into the [Status] page of the VDR824/824g (refer to section 4.7 "Status") first, and check to see if the WAN port of the VDR824/824g has obtained the Internet IP address and if the default route exists.

Symptom 7: You cannot access the Web pages through the PC in the LAN.

Solution: Follow the procedure to check:

- 9) The DNS server IP address specified on the PC is correct. If you specify the PC to obtain the DNS server address dynamically, verify with your ISP that the address configured on the VDR824/824g is correct, and then you can use the ping utility to test the connectivity with your ISP's DNS server.
- 10) Generally, if a host can ping the Internet IP address, but cannot open the Web pages, the DNS server of the ISP is experiencing a failure temporarily. In this case, you can choose either of the following to solve the problem: Manually change your PC's DNS IP address to the address of a normally functioning DNS server. Log into the Web page of the VDR824/824g and manually modify the configuration for DNS Relay (refer to section 4.2.2 "DNS Relay"), and then check by the **nslookup** command as instructed in section 6.2.2 "Nslookup".

Symptom 8: Fail to save the changes made on the Web configuration pages.

Solution: Make sure that you click <Apply> to confirm every change you have made. After completing all the settings, enter the [Save Configuration] page to save them, thus making them take effect when the VDR824/824g is powered on next time.

Symptom 9: You can access most of the websites, but sometimes connection to some websites times out. When you set the VDR824/824g to operate in the bridge mode and your PC to establish a dialup connection, you can access the websites normally. How does this problem come?

Solution: This problem is due to the MTU value from the client to the VDR824/824g. It is set too large. To solve the problem, enter the specific editing page (refer to section 4.2.1 "WAN") to change the MTU value to a smaller one, such as 1440, and then select **true** from the [TCP MSS Clamp] drop-down list.

In addition, if you fail to send an E-mail in the LAN, but succeed when you change an SMTP server, or you fail to transfer files by the point-to-point communication software, but succeed in transferring photos with other friends, this may be caused by the settings of the MTU for the LAN interface if you are sure the server functions well. Enter the [LAN Connections] tab page (refer to section 4.3.1 "LAN") to change the MTU value to a smaller one, such as 1440, and then select **true** from the [TCP MSS Clamp] drop-down list.

Symptom 10: Some services are unavailable once the firewall is enabled.

Solution: As the firewall rules of the VDR824/824g are very strict, it is recommended someone familiar with the WAN services and router configuration enable the firewall

and configure the firewall rules. Before the creation of firewall rules, you must be clear about the Internet service deployment. It is recommended that you disable the firewall.

6.2 Diagnosis Tools

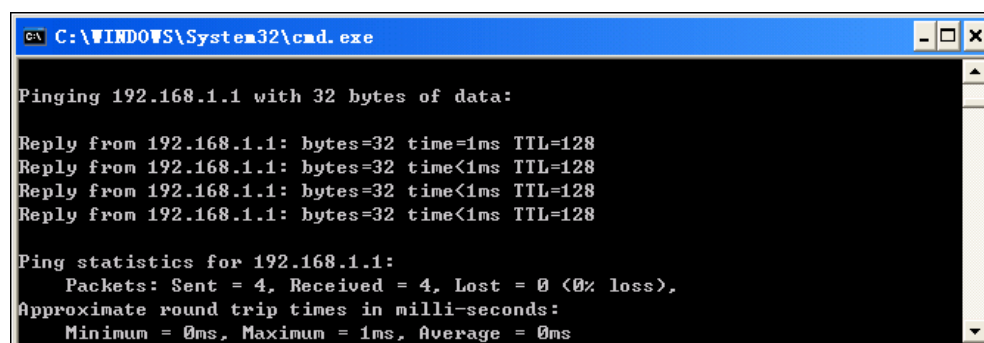
6.2.1 Ping

Use the **Ping** command to check whether your PC can recognize other computers on the network. A **ping** command sends messages to the specified computer. If the computer receives the messages, it replies with the response message. Before using the command, you must know the IP address of the destination host with which your PC is trying to communicate.

At the DOS prompt, enter the following command:

ping 192.168.1.1

If the destination host receives the packet, the command prompt window displays the contents as shown in Figure 6-1.



```
C:\WINDOWS\System32\cmd.exe

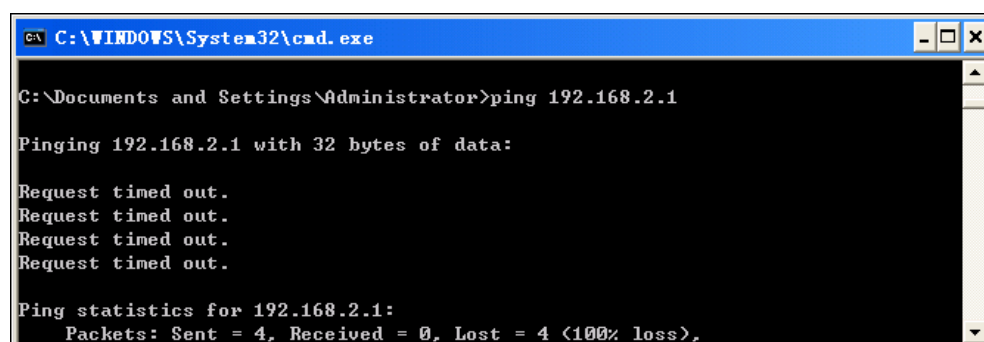
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure 6-1 Use the **ping** command – the ping succeeds

If the destination PC is not reachable, the Request timed out message is displayed as follows:



```
C:\WINDOWS\System32\cmd.exe

C:\Documents and Settings\Administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 6-2 Use the **ping** command – the ping fails

To check the connectivity with the VDR824/824g, use the **Ping** command with the default IP address of the LAN port (192.168.1.1) or the address you assign.

To check the connectivity with the Internet, enter an Internet domain name, such as **www.yahoo.com** (216.115.108.243). If you want to look up the IP address of a website, use the nslookup command as instructed in section 6.2.2 “Nslookup” for details.

For other operating systems running the IP protocol, you can enter the same ping command at a command prompt or through a system administration utility.

6.2.2 Nslookup

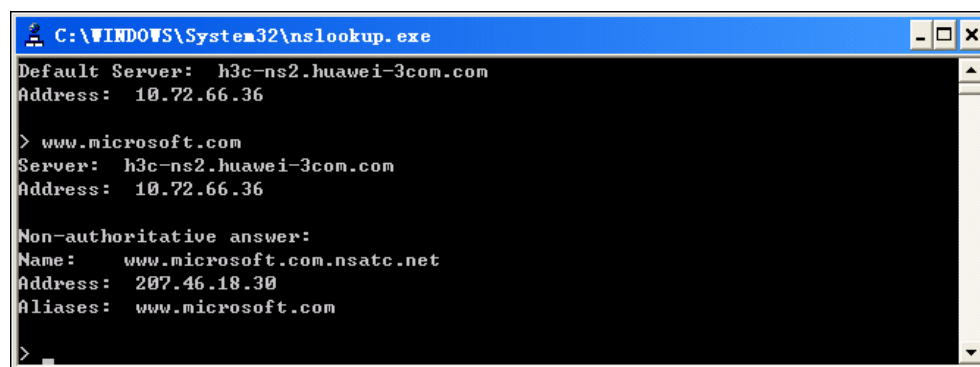
The **nslookup** command is used to query the IP address associated with a domain name. You can specify the common domain name and use the **nslookup** command to look up in the DNS server (usually located through your ISP). If that name is not in your ISP's DNS table, the request is then sent to a higher-level server until the name is found. The server then returns the associated IP address.

On Windows-based computer, you can execute the **nslookup** command from the [Start] menu. Choose [Start/Run] and in the open text box type the following:

nslookup

Click <OK> and a command prompt window appears. The [Command Prompt – nslookup] window is displayed with a bracket prompt (>). At the prompt, type the domain name of the desired Website, for example **www.microsoft.com**.

The window displays the associated IP address as shown below.



```
C:\WINDOWS\System32\nslookup.exe
Default Server:  h3c-ns2.huawei-3com.com
Address:  10.72.66.36

> www.microsoft.com
Server:  h3c-ns2.huawei-3com.com
Address:  10.72.66.36

Non-authoritative answer:
Name:    www.microsoft.com.nsatc.net
Address:  207.46.18.30
Aliases:  www.microsoft.com

>
```

Figure 6-3 Use the **nslookup** command

Some websites with heavy traffic use multiple servers to carry the same information. So it is common to have several IP addresses associated with one Internet domain name.

To exit from the nslookup utility, enter **exit**.

7 Appendix - TCP/IP Protocol

7.1 Installing TCP/IP

The PC through which you configure your VDR824/824g must have the TCP/IP installed. If you are not sure whether TCP/IP is installed, follow these steps.



Caution:

By default, TCP/IP is installed on Windows 2000/XP. The following steps are described for the Windows 98/ME/NT.

- 1) Choose [Start/Settings/Control Panel].
- 2) Double-click the Network Connection icon to open the [Network] dialog box and select the [Configuration] tab (see Figure 7-1).
- 3) Check the list on the [Configuration] tab page to see if the item that contains both the TCP/IP and the name of the NIC you are currently using exists. If not, click <Add> to open the [Select Network Component Type] dialog box (see Figure 7-1).

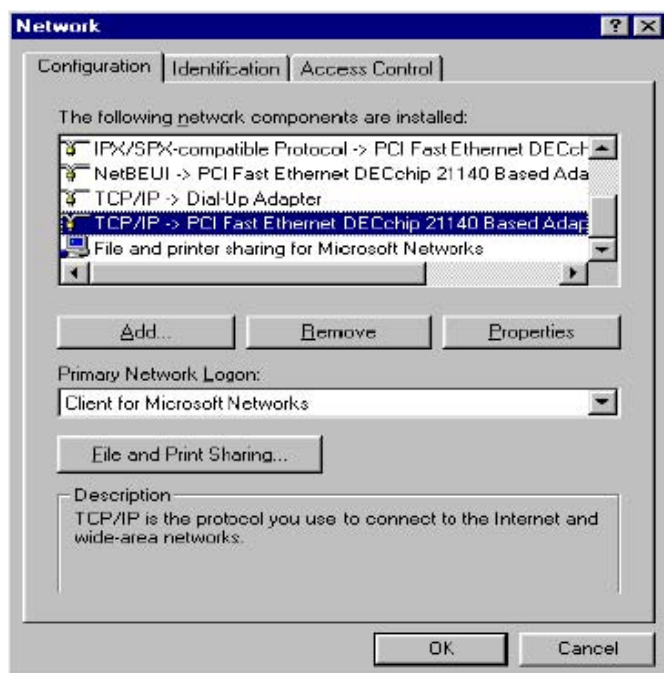


Figure 7-1 Network dialog box

- 4) Double-click **Protocol** from the list of [Select Network Component Type] dialog box (or click **Protocol** and then click <Add...>) to open the [Select Network Protocol] dialog box (see Figure 7-2).

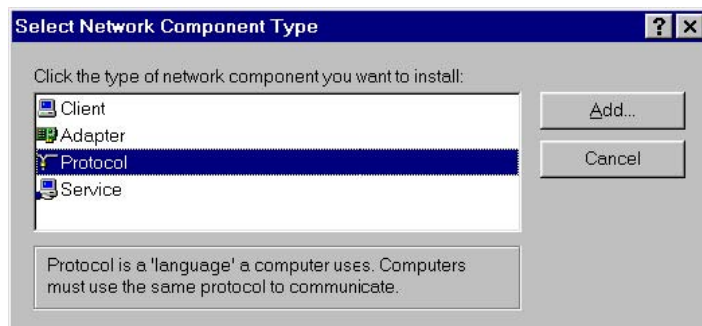


Figure 7-2 Select Network Component Type dialog box

- 5) Select **Microsoft** from the Manufacturers list in the [Select Network Protocol] dialog box, double-click **TCP/IP** in the Network Protocols list (or click **TCP/IP**, and then click <OK>) to return to the [Network] dialog box. Then you can see the TCP/IP item in the section listing the installed network components.

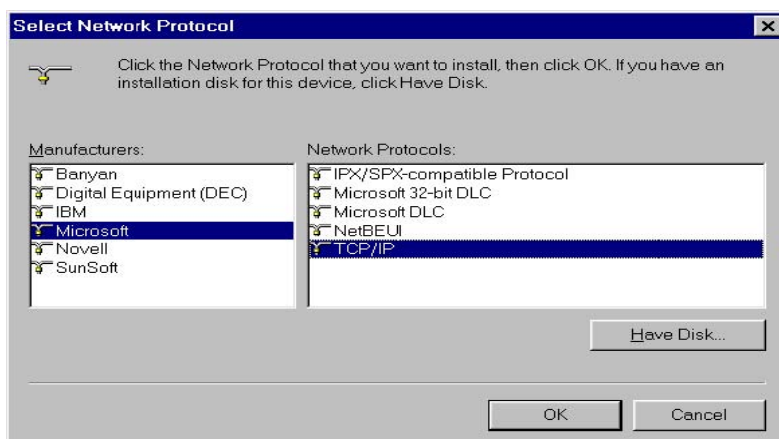


Figure 7-3 Select Network Protocol dialog box

- 6) Click <Properties> in the [Network] dialog box to open the [TCP/IP Properties] dialog box (see Figure 7-4). Select the [IP address] tab and select the **Obtain an IP address automatically** option. Click <OK> and restart your PC to complete the TCP/IP installation.

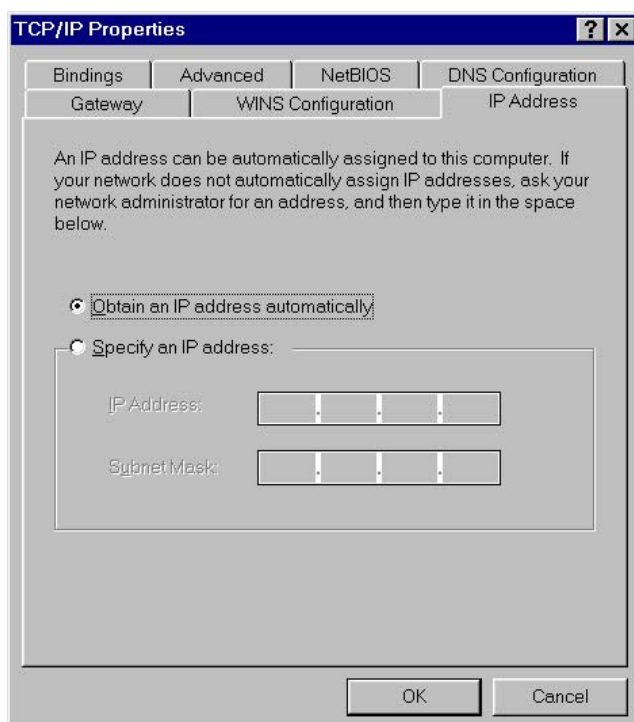


Figure 7-4 TCP/IP Properties dialog box

7.2 Configuring TCP/IP

7.2.1 Specifying to Obtain an IP Address Automatically

If you are running Windows 98/ME/NT, refer to those described in section Figure 7-3 to specify to obtain an IP address automatically. If you are running Windows 2000/XP, perform the following operation.

- 1) Choose [Start/Settings/Control Panel] to open the [Control Panel] dialog box. Double-click the Network Connection icon to open the [Network Connection] dialog box and then double-click the Local Connection icon to open the [Local Area Connection Status] dialog box (see Figure 7-5).

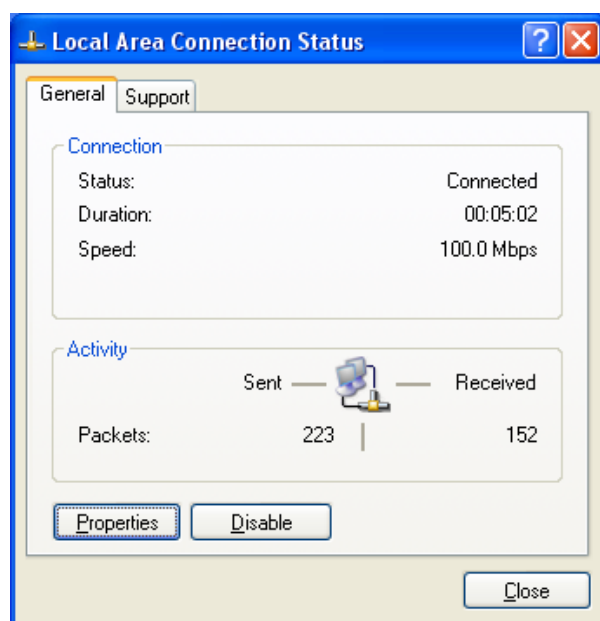


Figure 7-5 Local Area Connection Status dialog box

- 2) Click <Properties> to open the [Local Area Connection Properties] dialog box (see Figure 7-6). Select the [General] tab and select **Internet Protocol (TCP/IP)** in the [This connection uses the following items:] section, and then click <Properties> to open the [Internet Protocol (TCP/IP) Properties] dialog box as shown in Figure 7-7.

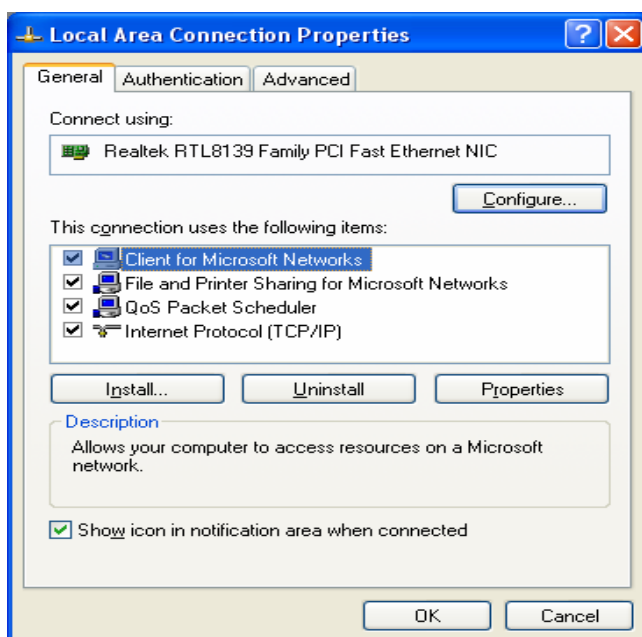


Figure 7-6 Local Area Connection Properties

- 3) On the [General] tab page of the [Internet Protocol (TCP/IP) Properties] dialog box select the **Obtain an IP address automatically** option and click <OK>.

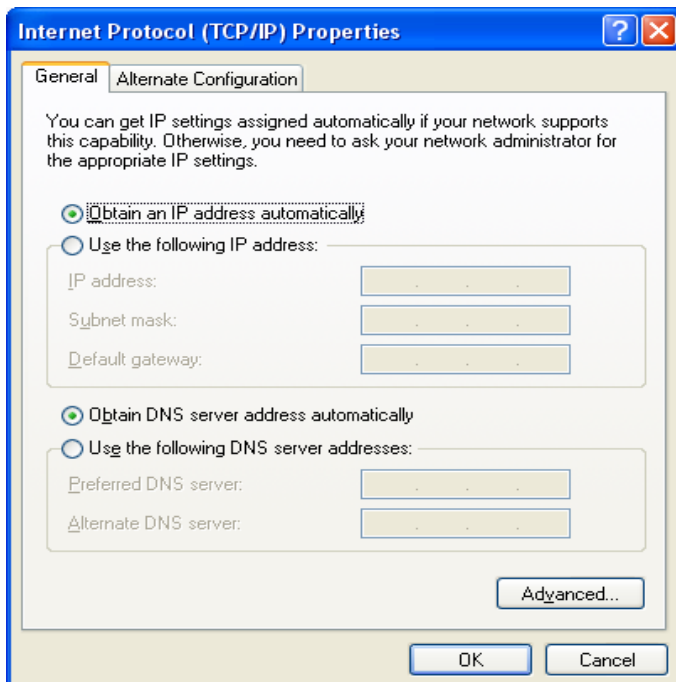


Figure 7-7 Internet Protocol (TCP/IP) Properties dialog box

7.2.2 Specifying a Fixed IP Address

Since the VDR824/824g enables the DHCP by default, the PCs in the LAN can obtain related information dynamically, thus there is no need to assign static IP addresses for PCs in the LAN. But in some cases you still need to configure network settings for some or even all the PCs on a network.

By default, the IP address of the Ethernet port of VDR824/824g is 192.168.1.1. Choose any from 192.168.1.2 to 192.168.1.254 to make your PC in the same segment with 192.168.1.1/24. Follow the procedure suitable for your operating system to specify IP addresses.

- 1) Specify the IP address of your PC.
 - Windows 98/ME/NT: In the [TCP/IP Properties] dialog box (see Figure 7-4), select the [IP Address] tab and select the Specify an IP address option.
 - Windows 2000/XP: In the [Internet Protocol (TCP/IP) Properties] dialog box (see Figure 7-7) select the [General] tab, and then the **Use the following IP address** option. Type in the IP address and subnet mask in the corresponding fields and click <OK>.
- 2) Specify the IP address of the gateway.
 - Windows 98/ME/NT: In the [TCP/IP Properties] dialog box (see Figure 7-4) select the [Gateway] tab. Type in the default IP address of your VDR824/824g (**192.168.1.1**) in the [New gateway] text box and click <Add>.
 - Windows 2000/XP: In the [Internet Protocol (TCP/IP) Properties] dialog box (see Figure 7-7), select the [General] tab. Type in the default IP address of your VDR824/824g (**192.168.1.1**) in the [Default gateway] text box and click <OK>.
- 3) Specify the IP address of the DNS server.
 - Windows 98/ME/NT: In the [TCP/IP Properties] dialog box (see Figure 7-4), select the [DNS configuration] tab and type in the default IP address of your VDR824/824g (**192.168.1.1**) as the DNS server IP address in the corresponding field.
 - Windows 2000/XP: In the [Internet Protocol (TCP/IP) Properties] dialog box (see Figure 7-7) click <Advanced...> to open the [Advanced TCP/IP Configuration] dialog box. Select the [DNS] tab and click <Add...>. Type in the default IP address of the VDR824/824g (**192.168.1.1**) in the [DNS server] field and click <Add>.
- 4) Making the settings take effect.
 - Windows 98/ME/NT: Click <OK> and restart your PC for the above settings to take effect.
 - Windows 2000/XP: Click <OK> to make the above settings to take effect.

8 Appendix - USB Configuration

8.1 Installing USB Driver

Make sure the USB function of your PC operates properly.

The Microsoft Windows 98/98 SE/ME/2000/XP supports USB driver. The following installation procedure is based on Windows XP. Use it for reference when running any other operating system.

I. Insert the driver CD into the CD-ROM of your PC.

The CD that comes with the VDR824/824g contains the USB driver.

II. Plug one end of the USB cable into the USB port of the VDR824/824g, and the other into the USB port of your PC.

The USB cable has a rectangular Type A connector on one end and a square Type B connector on the other end. Connect the Type A to your PC and the Type B to the VDR824/824g.

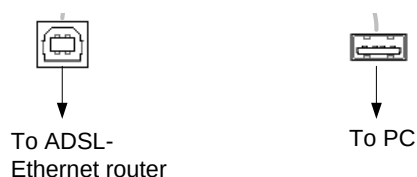


Figure 8-1 USB cable connector

III. The [Found New Hardware Wizard] dialog box appears (see Figure 8-2).
Select the **Install the software automatically (Recommended)** option and
click **<Next>** to proceed.

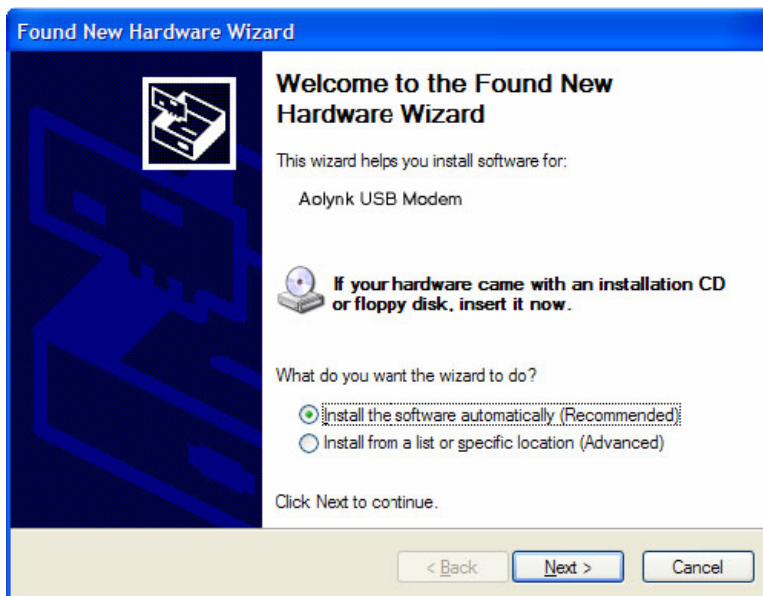


Figure 8-2 Find new hardware

IV. The PC searches the CD for the driver configuration file. When this file is found, the PC begins to install the driver.

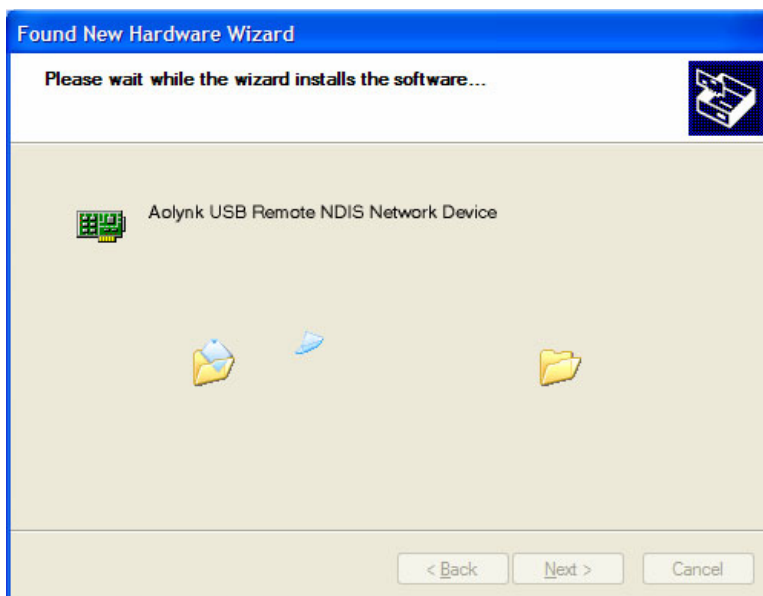


Figure 8-3 Install software

The dialog box (see Figure 8-4) appears during installation, warning that the device is not compatible with Windows XP. Just click <Continue Anyway> to proceed. Microsoft logo test

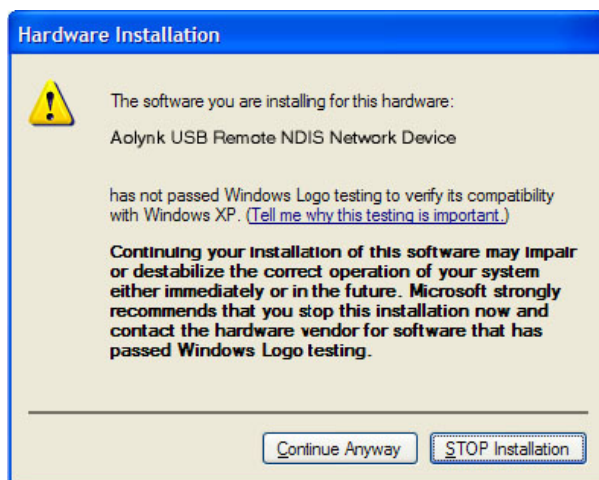


Figure 8-4 Microsoft logo test

V. The dialog box (see Figure 8-5) indicates the installation is complete. Click <Finish> to exit the installation.

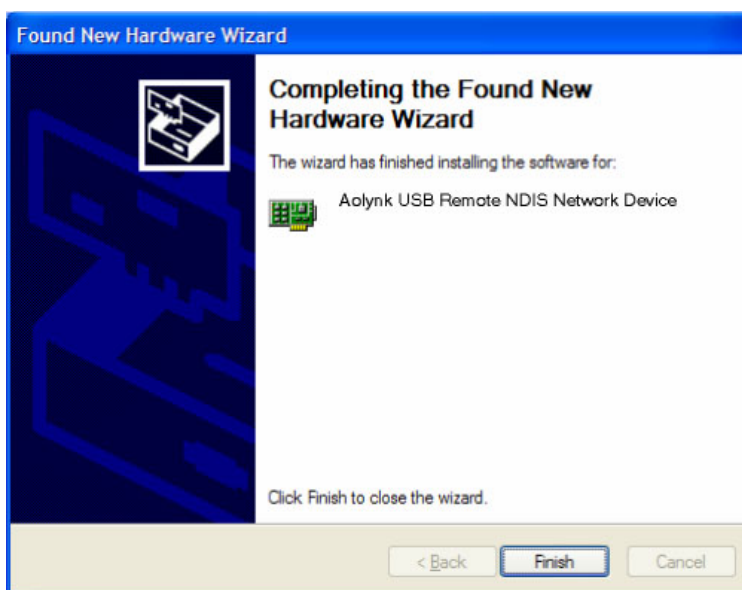


Figure 8-5 Complete the installation

8.2 Configuring IP Properties

After the USB driver installation is complete, you must configure the PC to place it in the same subnet as the VDR824/824g USB port. Two options are available to configure the IP properties:

- Your VDR824/824g can be a DHCP server to assign IP addresses to PCs in the LAN, so you can specify your PC to obtain IP address automatically. Refer to section 7.2.1 "Specifying to Obtain an IP Address Automatically" for detailed information.
- If you want to specify a fixed IP address to the PC, follow the instructions in section 7.2.2 "Specifying a Fixed IP Address" and use the following information..

The USB port on the VDR824/824g is preconfigured with these properties:

IP address: 192.168.1.1

Subnet mask: 255.255.255.0

Therefore, your PC should be configured as the following:

IP address: 192.168.1.n (n is an integer ranging from 2 to 254)

Subnet mask: 255.255.255.0

9 Appendix - IP Address and Subnet Mask

9.1 IP Address

Note:

- This section refers to the IP address of IPv4 (version 4 of the Internet Protocol) only and the IP address of IPv6 is not covered.
 - This section describes the basic knowledge of binary numbers, bits, and bytes.
-

An IP address, like the telephone number on the Internet, is used to identify the individual node (a PC or network device) on the Internet. Every IP address contains four sets of numbers, each from 0 to 255 and separated by dots, for example 20.56.0.211. These numbers are called, from left to right, field 1, field 2, field 3, and field 4.

The representation of four sets of digits separated by dots for IP address is called dotted decimal notation.

9.1.1 Structure of the IP Address

Like a telephone number, the IP address contains two components. For instance, the first three digits of a seven-digit telephone number identify a group with thousands of telephone lines, while the last four digits identify a specific line in this group.

Similarly, an IP address contains two components:

- Network ID

Identify a specific network segment on the Internet or the intranet.

- Host ID

Identify a specific PC or device on the segment.

The starting part of every IP address is the network ID and the rest is the host ID. The length of the network ID depends on the class of the network (refer to section 9.1.2 “Classes of IP Addresses”). Table 9-1 describes the structure of the IP address.

Table 9-1 Structure of the IP address

Class	Field 1	Field 2	Field 3	Field 4
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

The following are some valid IP address examples:

Class A: 10.30.6.125 (network ID = 10, host ID = 30.6.125)

Class B: 129.88.16.49 (network ID = 129.88, host ID = 16.49)

Class C: 192.60.201.11 (network ID = 192.60.201, host ID = 11)

9.1.2 Classes of IP Addresses

Three common IP addresses are of Class A, B, and C. (Class D is for special use and is beyond the scope of this discussion.) These classes have different uses and characteristics.

The class A network is the largest on the Internet. This allows at least 16 million hosts per network. Such 126 class A networks can hold at least two billion PCs. These enormous networks are quite suitable for the LAN or Internet fundamental organizations such as Internet service provider (ISP).

The class B network is relatively smaller than the class A network, but it still allows 16,384 class B networks and 65,000 hosts in each class B network. This kind of network is suitable for the large organizations such as enterprises and governments.

The class C network is the smallest one. It allows over two million (2,097,152 exactly) class C networks and 254 hosts in each class C network. The LANs connecting to the Internet are usually of this class networks.

Following are the key points about the IP address:

- The easiest way to determine the class of an IP address is to look at its number in the field 1:

Class A: The number is from 1 to 126.

Class B: The number is from 128 to 191.

Class C: The number is from 192 to 223.

(The numbers for special use are not given here.)

- Not all the fields of a host ID can be 0s or 255s as these numbers are reserved for special use.

9.2 Subnet Mask

Note:

A network mask looks like a regular IP address and a subnet mask can tell the division of the network ID and the host ID: A bit set to 1 means this bit is part of the network ID and a bit set to 0 means this bit is part of the host ID.

Subnet masks are used to define subnets (subnets are smaller segments of a large one). A subnet number is a number of bits borrowed from the host portion of IP address. For example, to divide a Class C address 192.168.1.1 into two subnets, you need to set the subnet mask as follows:

255.255.255.128

It is much more straightforward to define the address in binary notation.

11111111. 11111111. 11111111.10000000

For any Class C address, all the bits in the field 1 through field 3 are part of the network ID, but note how the mask specifies that the first bit in field 4 is also included. Since this extra bit has only two values (0 and 1), this means there are two subnets. Each subnet uses the remaining 7 bits in field 4 for its host IDs, which range from 1 to 126 hosts (instead of the usual 0 to 255 for a Class C address).

Similarly, to divide a class C network into four subnets, set the mask as follows:

255.255.255.192 or 11111111. 11111111. 11111111.11000000

The two extra bits in field4 can have four values (00, 01, 10, and 11), so there are four subnets. Each subnet uses the remaining six bits in field 4 for its host IDs, ranging from 1 to 62.

 Note:

Sometimes a subnet mask does not specify any additional network ID bits, and thus no subnets exist. Such a mask is called a default subnet mask. These masks are:

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

They are so called because they are used for an initially configured network without subnets.

10

Appendix - Technical Specifications

Table 10-1 Technical specifications

Item	Description
Ports and buttons	Four 10/100Base-TX Ethernet ports Two phone ports One ADSL port One USB port One console port One Reset button to restore the factory default settings One power switch
Power consumption	< 12W
Power supply (external)	12 VDC, 1 A
Physical dimensions (H x W x D)	<37 x 250 x 150 mm (1.5 x 9.8 x 6.0 in.)
Weight	Approximately 510g (11 oz)
Operating temperature	0°C to 40°C (32°F to 104°F)
Storage temperature	- 10°C to +70°C (14°F to 158°F)
Operating humidity (noncondensing)	20% to 85%
Storage humidity (noncondensing)	10% to 90%
Certification	FCC Class B CE

11 Appendix - Glossary

100Base-TX

Category 5 twisted pair cable with the maximum transmission distance of 100 meters (328 ft) and maximum transmission rate of 100 Mbps.

10Base-T

Category 3/4/5 twisted pair cable with the maximum transmission distance of 150 meters (492 ft) and the maximum transmission rate of 10 Mbps.

ADSL

Asymmetric digital subscriber line. The most popular flavor of DSL for home users. The term asymmetrical refers to its unequal data rates for download and upload (the download rate is higher than the upload rate). The asymmetrical rate benefits home users because they typically download much more data from the Internet than they upload.

ATM

Asynchronous transfer mode. A technology that uses fixed length packets, called cells, for the packet-switched network. The cell, consisting of a cell header and the text, are switched over a public or private ATM network. The individual ATM segments in the ATM switch cross connect to each other, forming the end-to-end connection.

Binary

The binary number system just uses two digits, 0 and 1, to represent all the numbers. In this system, the decimal digit 1 is represented by 1, 2 by 10, 3 by 11, 4 by 100, and so on. Although it is convenient to express numbers in decimal, the IP addresses actually use binary numbers. For instance, the IP address 209.191.4.240 is converted into 11010001.10111111.00000100.11110000 in binary.

Bridging

The data is sent from your network to your ISP and in return your ISP sends the data to the devices on the network by the physical addresses. Compared with routing, bridging

makes it more intelligent to transfer data by using network addresses. VDR824/824g can perform both routing and bridging. When both functions are enabled, the VDR824/824g routes IP data and bridges all the other types of data.

Broadcast

A technology used to send data to all the computers on a network.

DHCP

Dynamic host configuration protocol. DHCP automates IP address assignment and management. When a PC connects to the LAN, DHCP assigns it an IP address from a shared address pool, and after a specified period, DHCP returns the address to the pool.

DHCP server

Dynamic host configuration protocol server. A DHCP server is a computer responsible for assigning IP addresses to the computers in a LAN.

DNS

Domain name system. The DNS translates domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among the computers called DNS servers. For example, **www.yahoo.com** is the domain name associated with the IP address 216.115.108.243. When you start to access a website, a DNS server looks up the requested domain name and searches for its corresponding IP address. If the DNS server cannot find the IP address, it communicates with higher-level DNS servers to determine the IP address.

Domain name

A domain name is a user-friendly name in place of its associated IP address. A domain name must be unique and is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). A domain name is a key element of a URL which identifies a specific file at a website.

DSL

Digital subscriber line. A technology that allows both digital data and analog voice signals to travel over the existing copper telephone lines.

Ethernet

The most commonly installed computer network technology, usually using the twisted pair cables. The Ethernet data rates are 10 Mbps and 100 Mbps.

Firewall

A firewall can protect your computer or LAN from malicious attacks and other unexpected accesses. Unauthorized users may attempt to attack your network in order to prevent you or others on your LAN from the services.

Using the firewall, you can block certain types of IP traffic commonly used by hackers to protect your network. You can also restrict the types of IP traffic sent from your network to the outside. Some firewall protection can be provided by packet filtering and network address translation services.

FTP

File transfer protocol. A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a Web server, and downloading files from a Web server.

HTTP

Hypertext transfer protocol. It is the main protocol used to transfer data between websites so that it can be displayed by Web browser.

Hub

A hub receives the data from devices and forwards them. It usually performs the switching function by connecting a device such as an Ethernet bridge or a router to a group of computers in a LAN and allowing communication between those devices.

ICMP

Internet control message protocol. An Internet protocol used to report errors and other network-related information. The **ping** command makes use of ICMP.

IEEE

Institute of Electrical and Electronics Engineers. It is a technical professional society that fosters the development of standards that often become national and international standards.

IP address

Internet protocol address. The address of a host (computer) on the Internet, consisting of four decimal numbers, each from 0 to 255, separated by dots, such as 209.191.4.240. An IP address consists of a network ID that identifies the particular network the host belongs to, and a host ID uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead.

ISP

Internet service provider. A company that provides Internet access and charges the customers for services.

LAN

Local area network. A network limited to a small geographic area, such as a home, office, or small building.

MAC

Media access control address. It is the permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of two hexadecimal digits, separated by hyphens, such as 00-0F-1F-80-65-25.

MTU

Maximum transmission unit. It is the largest frame size that is transmitted over the physical network.

NAT

Network address translation. This enables computers in a LAN to access the Internet by sharing the same IP address. When a computer accesses the Internet, its private IP address is translated into a public address of the WAN port.

Network mask

A network mask is a sequence of bits applied to an IP address to select the network ID. Select the bit set to 1 and ignore the bit set to 0. For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1.

NIC

Network interface card. An adapter provides the physical interface for your network cabling. The Ethernet NIC usually has an RJ-45 connector.

Packet

Data that consists of units transmitted on a network are called packets. Each packet consists of a header, which contains the information about the source and destination addresses of the packet, and a data field.

Ping

A program used to check whether the host associated with an IP address can connect to the network. It can also be used to reveal the IP address for a given domain name.

Port

A physical access point on a device such as a computer or router, through which data flows into and out of the device.

PPP

Point-to-point protocol. It is a communication protocol for data transmission between devices over the standard telephone line. The WAN port on the VDR824/824g uses two types of the PPP, that is, PPPoA and PPPoE.

PPPoA

Point-to-point protocol over ATM. One of the two types of PPP interfaces. The other type is PPPoE. You can specify only one PPPoA interface for each VC.

PPPoE

Point-to-point protocol over Ethernet. One of the two types of PPP interfaces. The other type is PPPoA. You can specify multiple PPPoE interfaces for each VC.

Protocol

A set of rules to govern the data transmission. The two connected ends must obey these rules to transmit data.

Remote

A geographically separated location. For example, an employee on travel who logs into the company's intranet is a remote user.

RJ-11

The standard connector used to connect telephones, fax machines, and Modems to a telephone port. It is a 6-pin connector usually holding four wires.

RJ-45

The 8-pin connector used for transmitting data over the telephone lines. Straight-through cables are usually the connector of this type.

Routing

Forwarding data between the local network and the Internet through the most efficient path, based on the data's destination IP address and current network conditions. A device that performs routing is called a router.

SNMP

Simple network management protocol (SNMP), a network management standard, is widely used in the TCP/IP network. SNMP provides a way to manage the network

nodes from the host located in the center of the network, such as the server, work station, router, bridge, and hub. It usually performs the management through the distributed structure administration and proxy.

Subnet

A subnet is a separate part of a network. The subnet mask is used to break a large network into pieces by adding additional bits to the host portion of IP address. A host in a subnet is physically connected to its host in the network, however, each of them is in an individual division of network.

TCP/IP

Transmission control protocol/internet protocol.

It defines a suite of the basic protocols, not just the TCP/IP protocol, for the network communication.

Telnet

An interactive, character-based program used to access a remote computer. The HTTP and FTP only allow you to download files from a remote computer, while Telnet allows you to log into and use a computer from a remote location.

Twisted pair

A common copper cable used for the telephony application. It contains one or more cable pairs twisted together to minimize the interference and the noise. In an Ethernet LAN, category 3 cable is used for the 10Base-T network while the category 5 cable, the higher level, is used for the 100Base-T network.

Upstream

The upstream flows from users to the Internet.

USB

Universal serial bus. A serial interface that attaches the devices such as printers and scanners to the computer. The VDR824/824g provides a USB port to connect a computer.

VC

Virtual circuit. A connection from the DSL router to the ISP.

VCI

Virtual channel identifier. Together with the virtual path identifier (VPI), the VCI uniquely identifies a virtual circuit (VC). The ISP provides the VCI value for each VC.

VPI

Virtual channel identifier. Together with the virtual path identifier (VPI), the VCI uniquely identifies a virtual circuit (VC). The ISP provides the VPI value for each VC.

WAN

Wide area network. A network covering a large area such as a country or a continent is called a WAN. With respect to the ADSL router, WAN refers to the Internet.

Web browser

A software program that uses hypertext transfer protocol (HTTP) to download information from (and upload to) websites, and displays the information consisting of text, graphic images, audio, and video. The popular Web browsers are Netscape Navigator and Microsoft Internet Explorer.

Web page

A website file typically containing text, graphic images and hyperlinks to the other pages. When you access a website, the first displayed page is called the home page.

ZIPB

Zero installation PPP bridge. This technology ensures that a home user obtains a public IP address through the Modem, and access the Internet without configuring NAT on the Modem or installing the PPP client on the Scathe ZIPB mode becomes active when it is enabled, IPCP negotiation is complete over the WAN PPP link, and a DHCPDISCOVER is received on the Modem LAN interface.