



Telecommunications Group

3641-80 / 3648-80
Ethernet Routers
Guide and Web Users Manual
Section 364-180-N02
Equipment Issue 1
1st Printing, April, 2006

Contents

| | | |
|------|--------------------------------------|----|
| 1. | About This Manual | 1 |
| 1.1. | Revision History | 1 |
| 1.2. | Document Organization..... | 1 |
| 1.3. | Glossary of Terms and Acronyms | 1 |
| 2. | General Overview | 3 |
| 3. | Specifications | 5 |
| 4. | Applications | 7 |
| 5. | Installation..... | 9 |
| 5.1. | Preparing Before Installation..... | 9 |
| 5.2. | Installation Procedures | 9 |
| 6. | Web Configuration Tool..... | 11 |
| 6.1. | About the Web Configuration..... | 11 |
| 6.2. | Factory Default Settings..... | 11 |
| 6.3. | TCP/IP Configuration..... | 12 |
| 6.4. | Login to Web Configuration Tool..... | 17 |
| 6.5. | Status Menu | 19 |
| 6.6. | System Menu | 22 |
| | Error Log..... | 22 |
| | Upgrade | 23 |
| | Restart | 25 |
| 6.7. | Configuration Menu | 26 |
| | Save config..... | 27 |
| | Authentication..... | 29 |
| | LAN Connections | 33 |
| | WAN Connections | 36 |
| | IP routes | 52 |
| | DHCP Server..... | 54 |
| | DNS Client..... | 61 |

| | |
|--|-----|
| DNS Relay | 63 |
| Security | 66 |
| VPN Configuration | 88 |
| SNTP client | 105 |
| Syslog | 109 |
| SNMP | 110 |
| Port | 115 |
| 7. CLI Configuration Tool | 117 |
| 7.1. Help Text for Using the CLI Commands..... | 118 |
| 7.2. Download/Upload Configuration File..... | 119 |
| 7.3. Using the <i>source</i> CLI commands | 122 |
| 7.4. CLI Application Examples | 124 |
| Note: After loading the scripts, save the configuration and restart the router | |
| Frame Relay - bridged..... | 124 |
| Frame Relay - routed | 127 |
| PPP - bridged | 129 |
| PPP - routed | 132 |
| 7.5. CLI Commands Group | 135 |
| 7.6. List of CLI Commands..... | 136 |
| Appendix: System Limit..... | 152 |

List of Figures

| | | |
|-------------|---|----|
| Figure 4-1 | Router card point to point application..... | 7 |
| Figure 4-2 | Router card frame relay application..... | 7 |
| Figure 4-3 | Router card VPN application..... | 8 |
| Figure 4-4 | Router card dual gateway application..... | 8 |
| Figure 6-1 | Login Web Configuration Tool..... | 17 |
| Figure 6-2 | Web Tool - Welcome page..... | 18 |
| Figure 6-3 | Web Tool – Status page..... | 20 |
| Figure 6-4 | Web Tool – Error Log page..... | 22 |
| Figure 6-5 | Web Tool – Firmware Upgrade page..... | 23 |
| Figure 6-6 | Web Tool – Firmware Upgrade Complete page..... | 24 |
| Figure 6-7 | Web Tool – Reset Router page..... | 25 |
| Figure 6-8 | Web Tool – Save configuration Confirm page..... | 27 |
| Figure 6-9 | Web Tool – Save configuration completed page..... | 28 |
| Figure 6-10 | Web Tool – Authentication page..... | 29 |
| Figure 6-11 | Web Tool – Authentication: edit user details page..... | 30 |
| Figure 6-12 | Web Tool – Authentication: create user page..... | 31 |
| Figure 6-13 | Web Tool – Authentication: Currently Defined Users page..... | 32 |
| Figure 6-14 | Web Tool – LAN connection page..... | 33 |
| Figure 6-15 | Web Tool – WAN connections page..... | 36 |
| Figure 6-16 | Web Tool – WAN connection: create service page..... | 36 |
| Figure 6-17 | Web Tool - WAN connection: Frame Relay routed page..... | 38 |
| Figure 6-18 | Web Tool – WAN connection: frame relay routed: Edit Service page..... | 39 |
| Figure 6-19 | Web Tool – WAN connection: Edit Frame Relay channel page..... | 40 |
| Figure 6-20 | Web Tool – WAN connection: Edit IP Interface page..... | 41 |
| Figure 6-21 | Web Tool – WAN connection: Edit Rip Versions page..... | 42 |
| Figure 6-22 | Web Tool – WAN connection: Frame Relay bridged page..... | 43 |
| Figure 6-23 | Web Tool – WAN connections page..... | 44 |

| | | |
|-------------|--|----|
| Figure 6-24 | Web Tool – WAN connection: PPP routed page..... | 46 |
| Figure 6-25 | Web Tool – WAN connections page..... | 47 |
| Figure 6-26 | Web Tool – WAN connection: PPP bridged page..... | 50 |
| Figure 6-27 | Web Tool – WAN connections page..... | 51 |
| Figure 6-28 | Web Tool – WAN connection: delete ‘Frame Relay routed’ page..... | 52 |
| Figure 6-29 | Web Tool – IP routes: Create Ip V4Route page..... | 53 |
| Figure 6-30 | Web Tool – IP routes: Edit Routes page..... | 53 |
| Figure 6-31 | Web Tool – DHCP server page..... | 54 |
| Figure 6-32 | Web Tool – DHCP: enable server page..... | 56 |
| Figure 6-33 | Web Tool – DHCP: enable relay agent page..... | 59 |
| Figure 6-34 | Web Tool – DHCP server: DHCP relay enabled page..... | 60 |
| Figure 6-35 | Web Tool – DNS Client page..... | 61 |
| Figure 6-36 | Web Tool – DNS Client page..... | 62 |
| Figure 6-37 | Web Tool – DNS relay page..... | 63 |
| Figure 6-38 | Web Tool – DNS: enable relay page..... | 64 |
| Figure 6-39 | Web Tool – DNS relay enabled page..... | 65 |
| Figure 6-40 | Web Tool – Security page..... | 66 |
| Figure 6-41 | Web Tool – Security: Security Interfaces page..... | 67 |
| Figure 6-42 | Web Tool – Security: Security Interfaces page..... | 68 |
| Figure 6-43 | Web Tool – Security: Advanced NAT Configuration page..... | 69 |
| Figure 6-44 | Web Tool – Security: Firewall Add Global Address Pool page..... | 69 |
| Figure 6-45 | Web Tool – Security: Advanced NAT Configuration page..... | 70 |
| Figure 6-46 | Web Tool – Security: Firewall Delete Global Address Pool page..... | 71 |
| Figure 6-47 | Web Tool – Security: Security Interfaces page..... | 72 |
| Figure 6-48 | Web Tool – Security: Add Reserved Mappings page..... | 72 |
| Figure 6-49 | Web Tool – Security: Firewall Add Reserved Mapping page..... | 73 |
| Figure 6-50 | Web Tool - Security: Reserved Mappings page..... | 74 |
| Figure 6-51 | Web Tool – Security: Firewall Delete Reserved Mappings page..... | 74 |
| Figure 6-52 | Web Tool – Security: Firewall Policy Configuration page..... | 75 |

| | | |
|-------------|---|-----|
| Figure 6-53 | Web Tool – Security: Firewall Add TCP Port Filter page | 76 |
| Figure 6-54 | Web Tool – Security: Firewall Add Raw IP Filter page | 77 |
| Figure 6-55 | Web Tool – Security: Firewall Add Trigger page..... | 81 |
| Figure 6-56 | Web Tool – Security: Firewall Configuration Intrusion Detection page..... | 84 |
| Figure 6-57 | Web Tool – Security: Alerting Configuration for Intrusion page..... | 86 |
| Figure 6-58 | Web Tool – IPsec Configuration page | 93 |
| Figure 6-59 | Web Tool – IPsec: Create New IPsec Endpoint page..... | 94 |
| Figure 6-60 | Web Tool – IPsec: User Certificates page..... | 98 |
| Figure 6-61 | Web Tool – IPsec: Generate Certificate Request page | 99 |
| Figure 6-62 | Web Tool – IPsec: Add new CA certificate page | 100 |
| Figure 6-63 | Web Tool – PPTP Configuration page..... | 102 |
| Figure 6-64 | Web Tool – PPTP: Authentication: create user page..... | 102 |
| Figure 6-65 | Web Tool – SNTP client page | 105 |
| Figure 6-66 | Web Tool – SNTP client: SNTP Synchronization Mode page | 105 |
| Figure 6-67 | Web Tool – SNTP client: Enter Unicast Server IP Address page..... | 107 |
| Figure 6-68 | Web Tool – SNTP client: SNTP Client General Configuration Parameters page | 108 |
| Figure 6-69 | Web Tool – SNTP client: ISOS Clock Setting page..... | 109 |
| Figure 6-70 | Web Tool – Syslog Client Configuration page..... | 109 |
| Figure 6-71 | Web Tool – Snmp page..... | 111 |
| Figure 6-72 | Web Tool – Snmp: select Action page..... | 112 |
| Figure 6-73 | Web Tool – Snmp: Snmp Show Community page | 112 |
| Figure 6-74 | Web Tool – Snmp: Snmp Add Community page | 113 |
| Figure 6-75 | Web Tool – Snmp: Snmp Add Host page | 113 |
| Figure 6-76 | Web Tool – Snmp: Snmp Add Trap page | 114 |
| Figure 6-77 | Web Tool – Snmp: Snmp Show Host page..... | 114 |
| Figure 6-78 | Web Tool – Snmp: Snmp Show Trap page..... | 114 |
| Figure 6-79 | Web Tool – Ports: Ethernet Port Configuration page | 115 |
| Figure 6-80 | Web Tool – Ports: Advanced Ethernet Port Configuration page | 116 |
| Figure 7-1 | Login CLI Configuration Tool | 117 |

List of Tables

| | | |
|-----------|--|-----|
| Table 1-1 | Revision history table | 1 |
| Table 1-2 | Glossary of terms and acronyms..... | 1 |
| Table 3-1 | Router card specifications..... | 5 |
| Table 6-1 | Default user name and password | 29 |
| Table 6-2 | User access levels | 31 |
| Table 6-3 | Syslog severity levels..... | 110 |
| Table 7-1 | Default names of different Interface/Transport/Port..... | 124 |
| Table 7-2 | List of CLI commands | 136 |

1. About This Manual

1.1. Revision History

Table 1-1 Revision history table

| <i>Revision</i> | <i>Date</i> | <i>Description</i> |
|-----------------|-------------|--------------------|
| Issue 1.0 | April, 2006 | Initial release |

1.2. Document Organization

About This Manual, Chapter 1, introduces you to the document.

General Overview, Chapter 2, provides overview and features of the router card.

Specification, Chapter 3, provides the technical specifications.

Applications, Chapter 4, introduces some application examples.

Installation, Chapter 5, provides the installation procedures.

Controls and Indicators, Chapter 6, provides the descriptions of controls and LED activity.

Web Configuration Tool, Chapter 7, provides the details of the web configuration.

CLI Configuration Tool, Chapter 8, introduces the CLI configuration and provides some setting examples.

1.3. Glossary of Terms and Acronyms

Table 1-2 Glossary of terms and acronyms

| <i>Abbreviations</i> | <i>Description</i> |
|----------------------|---|
| CHAP | Challenge-Handshake Authentication Protocol |
| CLI | Command Line Interface |
| DCE | Data Communication Equipment |
| DHCP | Dynamic Host Configuration Protocol |
| DTE | Data Terminal Equipment |
| DNS | Domain Name System |
| IGMP | Internet Group Management Protocol |
| IP | Internet Protocol |
| IPSec | IP Security Protocol |
| LAN | Local Area Network |

| | |
|-------|---------------------------------------|
| L2TP | Layer Two Tunneling Protocol |
| NAT | Network Address Translation |
| PAP | Password Authentication Procedure |
| PPP | Point to Point Protocol |
| PPPoH | PPP over High-Level Data Link Control |
| PPTP | Point to Point Tunneling Protocol |
| PVC | Permanent Virtual Circuit |
| RIP | Routing Information Protocol |
| SNTP | Simple Network Time Protocol |
| SNMP | Simple Network Management Protocol |
| VPN | Virtual Private Networking |
| WAN | Wide Area Network |

2. General Overview

This document supports both the 3641-80 Single Port router and the 3648-80 router which includes an 8 port Ethernet switch. The router cards are Ethernet IP routers, which mounts in a full size card slot. The only difference between the 3641-80 and 3648-80 is that the 3648-80 has an unmanaged Ethernet switch to eliminate the need for an external switch. Therefore the routers will be referred to as 'the router'. The router includes an Ethernet interface to provide data services from the T1/E1 interface. The router can act as a frame relay router, frame relay bridge, firewall, VPN gateway, or IP sharing.

For purposes of understanding, the Ethernet port represents the LAN side of the router and the T1/E1 represents the WAN side of the router.

The router card provides three primary services:

1. Provides a standard T1/E1 gateway function between the customer Ethernet interface and the WAN data service channel on the T1/E1 interface.
2. Provides the possibility for including voice and data over the same T1/E1 line.
3. Provides a flexible programmable data rate $56/64K \times N$ bps where $N = 1 \dots 24$ for T1, $1 \dots 30$ for E1 (i.e. $56K \sim 1.536M$ bps for T1, $56K \sim 1.92M$ bps for E1).

Equipment Features

- Provide one Ethernet port with 10/100 BaseT auto sensing (3641-80)
- Provide Eight Ethernet ports with 10/100 BaseT auto sensing and auto crossover cable sensing (3648-80 only)
- Provide one female RS-232 DCE console port (also referred to as a craft port) for set up and management
- Provide management via CLI (by console port or Telnet) and web browser
- Support SNMP V1/V2c management (maximum 10 SNMP managers and trap recipients are allowed at any one time when using the router Ethernet port)
- Support RIP V1 and V2
- Support NAT and NAPT

- Support DHCP Server / Relay Agent / Client mode
- Support DNS Client / Relay mode
- Support Frame Relay WAN layer 2 protocol
- Support PAP and CHAP
- Support all three types of VPN --- IPSec, PPTP, and L2TP
- Simple firmware update via web-based GUI interface

NOTE: There are certain features that are only accessible through the Web Configuration Tool:

1. Digital signature certificates of IPSec
2. Remote upgrade firmware (by browser http-upload.tar file)
3. Errorlog

There are certain features that are only accessible through the CLI Configuration Tool:

1. Webserver configuration
2. DHCP client parameters configuration (such as reboot time, retry time, backoff time, etc.)
3. Upload/download the configuration file to/from system/PC
4. Local upgrade firmware (via tftp/bootp protocol)
5. Set rip host route and set rip poison

3. Specifications

Table 3-1 Router card specifications

| Parameter | Specification |
|-----------------------|--|
| Dimension: | |
| Height | 1.9 cm |
| Width | 24.45 cm |
| Depth | 23.49 cm |
| Weight | 300 g |
| Operating Environment | (in service) -40°C ~ +65°C < 95% RH |
| Power: | Less than 1 amp. DC input voltage range of - 42V to 56V |
| Console port | Standard DB-9 connector, DCE configured with baud rate 9600, 8 bits of data, no parity, and 1 stop bit |
| Ethernet port | RJ-45 connector with IEEE 802.3 compatible, 10/100BaseT auto sensing (both 3641-80 and 3648-80), and auto crossover cable sensing (3648-80 only) |
| WAN side data rate: | 56K to 1.536 M b/s |
| IP Protocol Support: | |
| TCP | Meet the requirements of RFC 793 |
| UDP | Meet the requirements of RFC 768 |
| ICMP | Meet the requirements of RFC 792/STD 0005 updated with RFC 950/STD 0005. |

| | |
|-------------------|--|
| RIP V1 and V2 | Meet the requirements of RFC 1058 and RFC 2453. |
| IGMP | Meet the requirements of RFC 2236. Supports IGMP Proxy as described in [draft-ietf-idmr-igmp-proxy-03] "IGMP-based Multicast Forwarding (IGMP Proxying)", W. Fenner, July 2000. |
| Static routing | Meet the requirements of RFC 3442 and the current practice defined in RFC 3180/BGP 0053. |
| CIDR | Meet the Best Current Practice defined in RFC 3180/BGP 0053 and the requirements defined in RFC 1517, RFC 1518 and RFC 1519. |
| ARP | Meet the requirements of RFC 826/STD 0037. |
| DHCP | Meet the requirements of RFC 3022 and 3235. |
| PPP Support: | |
| IPCP | Meet the PPP IPCP RFC 1332. |
| BCP | Meet the requirements of IEEE 802.1D MAC Bridging and RFC 1638. |
| LCP | Meet the requirements of RFC 1570. |
| L2TP | Meet the requirements of RFC 3070 and 3438. |
| PPTP | Meet the requirements of RFC 1661/STD0051. |
| Frame Relay: | The system serves as end stations (DTEs) on a public or private Frame Relay network. Meet the requirements of RFC 2427/STD 0055. |
| Security Support: | |
| PAP and CHAP | Meet the current practice defined in RFC1334 for PAP and RFC 1994 for CHAP. |

4. Applications

The router card can act as a frame relay router, frame relay bridge, firewall, VPN gateway, or IP sharing. The following figures are application examples.

Point-to-Point application

Figure 4-1 is for either router or bridge applications.

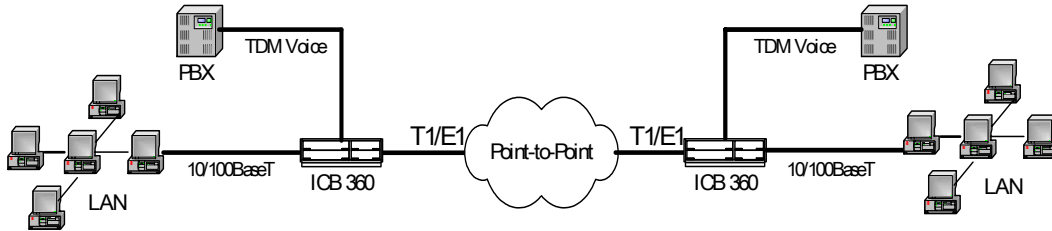


Figure 4-1 Router card point to point application

Frame Relay application

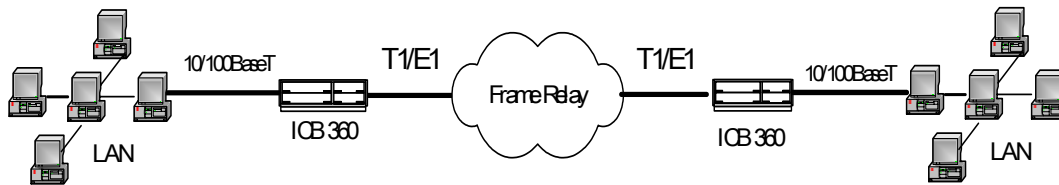


Figure 4-2 Router card frame relay application

VPN application

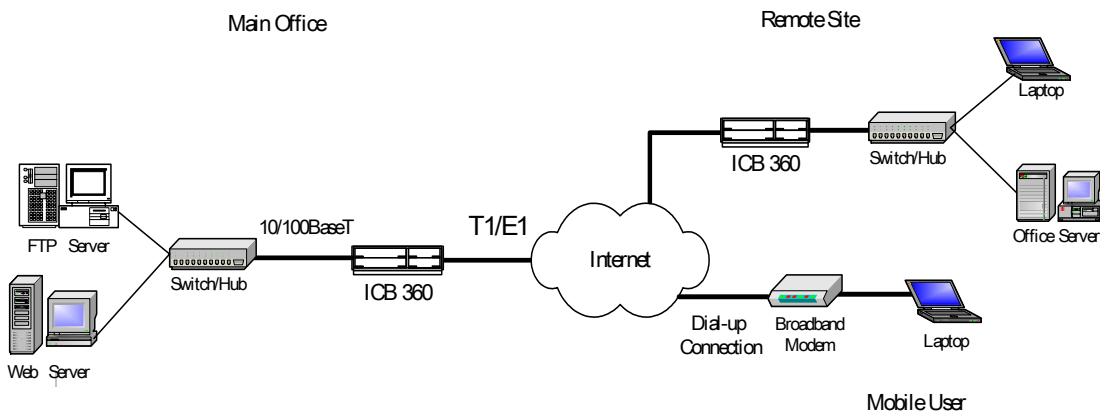


Figure 4-3 Router card VPN application

Dual Gateway application

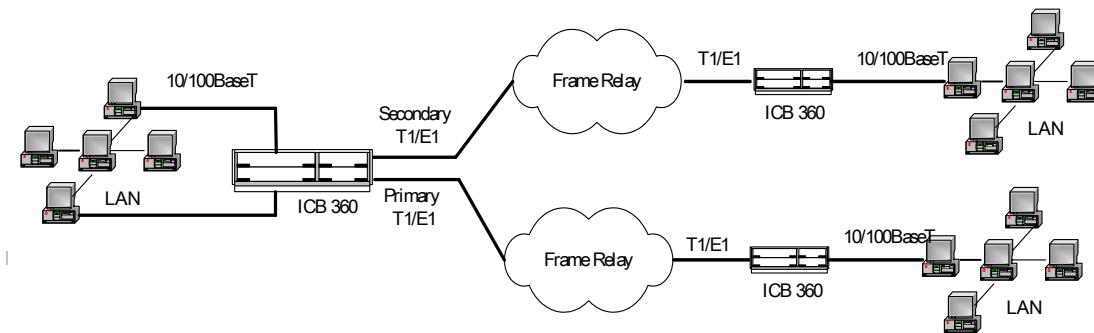


Figure 4-4 Router card dual gateway application

5. Installation

5.1. Preparing Before Installation

The major functions of the Router Card are performed by the Ethernet network interface. Your computer must have an Ethernet Network Interface Card (NIC) installed and set up with the TCP/IP protocol before beginning to use the router. The router also provides a serial console port for monitoring and configuring the router via the built-in command line interface.

You will need to know the Internet Protocol supported by your T1/E1 provider to successfully connect to the Internet. For future troubleshooting or reinstallation, it is important that you retain these details.

Before beginning the hardware installation, please gather the following materials for the setup.

- At least one computer running a supported *operating system, with an Ethernet Network Interface Card (NIC) installed (or more computers if you use an external hub).
- TCP/IP protocol installed for each NIC.
- Ethernet straight connect cable (one for each computer you will be connecting)
- RS-232 serial cable (Optional)

* The router Web Configuration tool supports browsers that operate under Windows 95, 98, 2000, XP and Unix system. Configuration can also be done via telnet, ftp or through an RS-232 RTR MGMT port.

5.2. Installation Procedures

To install the router card, follow the procedure in the router practice (LT364-180-202) or the router installation guide (LT364-180-802).

6. Web Configuration Tool

6.1. About the Web Configuration

The Web Configuration tool provides a series of web pages that you can use to setup and configure your Router card. There are three main menus. You can select each of the following menus from the left frame of the main window:

- **Status Menu:** Information about the current setup and status of the system and system hardware and options..
- **System Menu:** Information about the error log, upgrading the firmware and restarting the system.
- **Configuration Menu:** Information about the current configuration of various system features with options to change the configuration.

NOTE: There are certain features that are only accessible through the Web Configuration Tool:

1. Digital signature certificates of IPSec
2. Remote upgrade firmware (by browser http-upload.tar file)
3. Errorlog

6.2. Factory Default Settings

If your required configuration exactly matches the settings below, the router will work for you as pre-configured. After completing the installation, assigning your static IP address to your computer's TCP/IP settings, you should be able to make a connection to the Internet.

| | |
|---------------------|-----------------------------------|
| LAN Port: | IP Address: 192.168.0.1 |
| | Subnet Mask: 255.255.255.0 |
| DHCP Server: | Disabled |
| Loopback: | IP Address: 127.0.0.1 |

6.3. TCP/IP Configuration

In order to access the router's Web GUI to begin your configuration, you must have the TCP/IP protocol installed and configured properly in your computer's network interface card. Your computer's TCP/IP settings must allow your computer to obtain an IP address automatically.

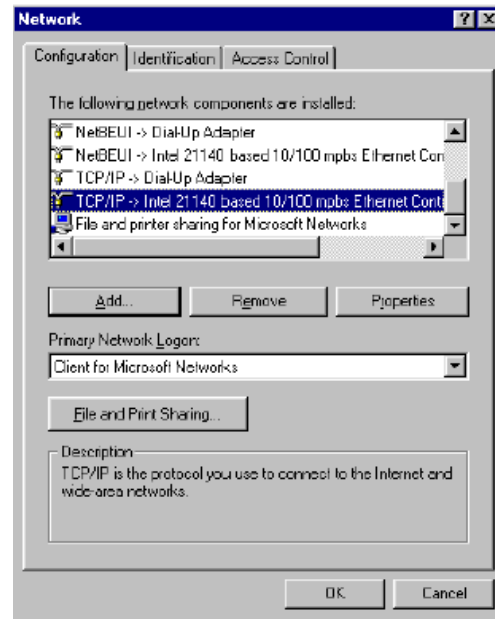
To connect to the Internet or configure the router via Ethernet, the TCP/IP protocol must be installed and configured correctly. Follow the steps below to determine if you have TCP/IP installed and configured correctly for Windows 95/98.

Step 1 - Check if TCP/IP is installed

1. From your computer's desktop, double-click on **My Computer**, then **Control Panel**, and then double-click the **Network** icon.



2. In the "Network" window, choose the *Configuration* tab. Check that TCP/IP is installed and setup for the Ethernet NIC that is installed in your computer. If you see, for example, TCP/IP->Intel 21140 based 10/100mbps Ethernet Controller, that means that TCP/IP has been installed.



- If TCP/IP has not been installed for your NIC, proceed to **Step 2** as below.

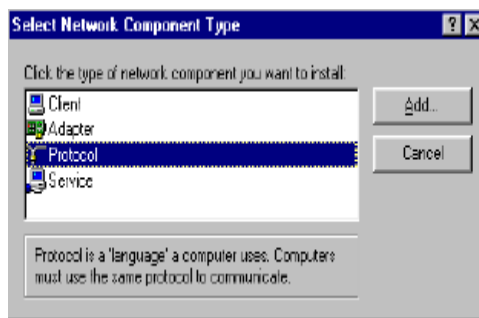
OR –

- *If TCP/IP has been installed for your NIC, continue with **Step 3** - Setup TCP/IP section.*

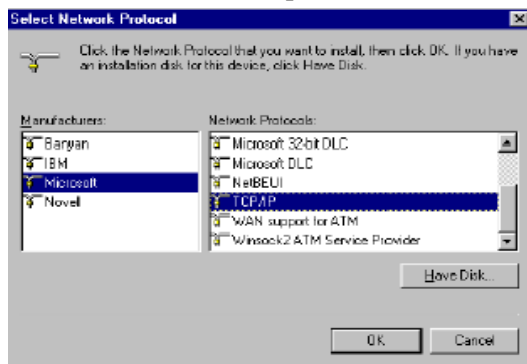
Step 2 - Install TCP/IP, if necessary

Install TCP/IP now if it is not previously installed. You may need the Windows Installation CD-ROM.

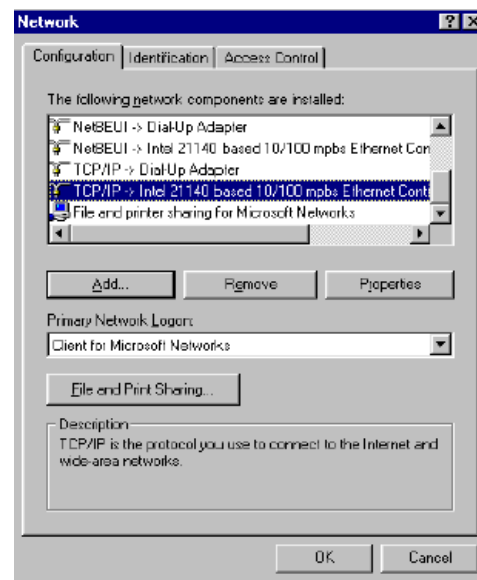
1. Still in the “Network” window, click the **Add** button. The “Select Network Component Type” window will appear. Select *Protocol* by clicking on it once. Then click **Add**.



2. The “Select Network Protocol” window will appear. Choose *Microsoft* in the “Manufacturers” panel and then *TCP/IP* in the “Network Protocols” panel. Click **OK**.

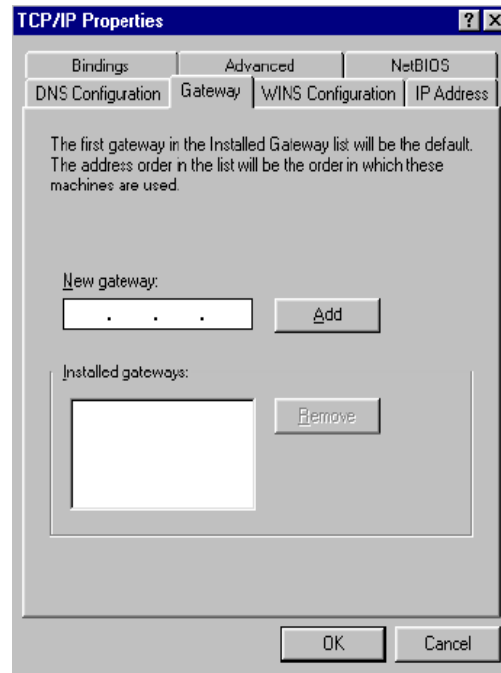
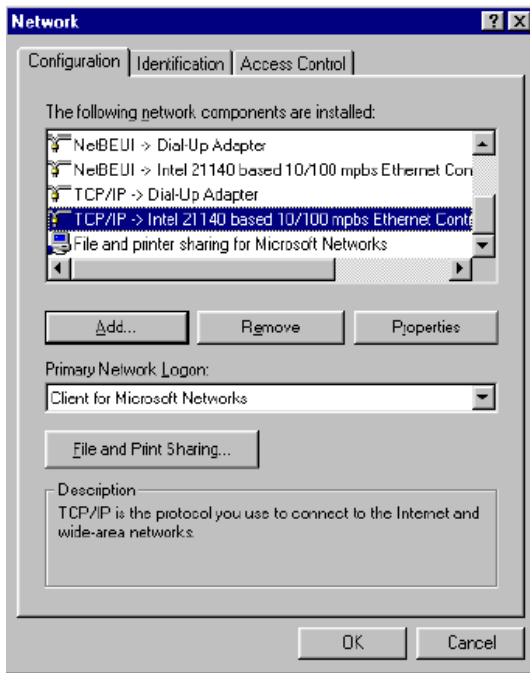


3. Confirm that the TCP/IP protocol has been correctly set up with your Ethernet. Click **OK**.

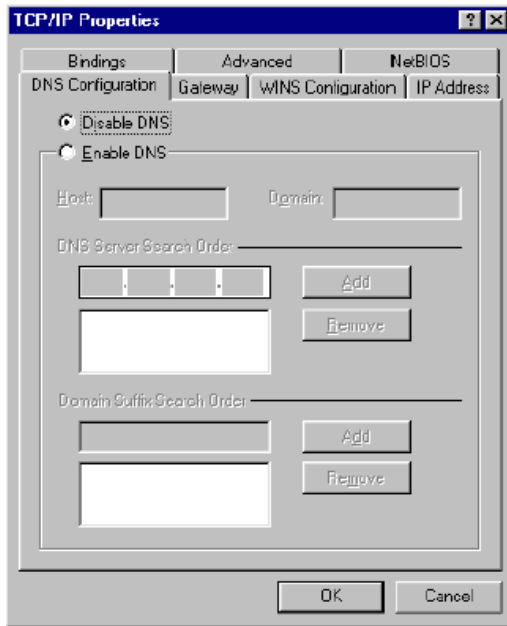


Step 3 - Setup TCP/IP

1. In the “Network” window, choose the *Configuration* tab. Then double-click the **TCP/IP component for your Ethernet NIC** (for example, **TCP/IP->Intel 21140 based 10/100 Mbps Ethernet Controller**).
2. In the “TCP/IP Properties” window, click the Gateway tab. Remove any installed Gateways by selecting them and clicking the Remove button.

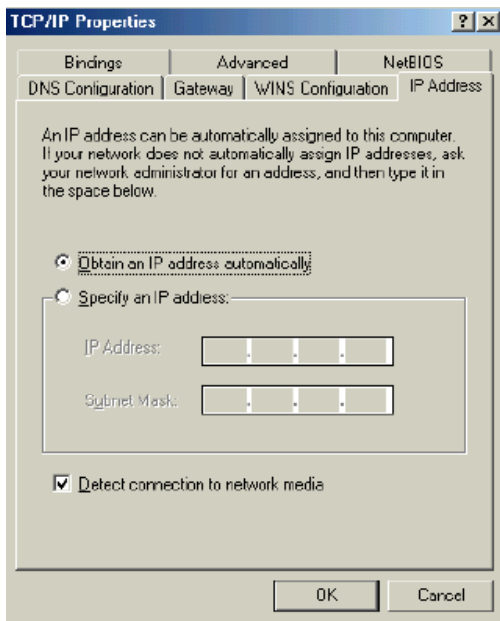


- Click the **DNS Configuration** tab, and then click the **Disable DNS** button.

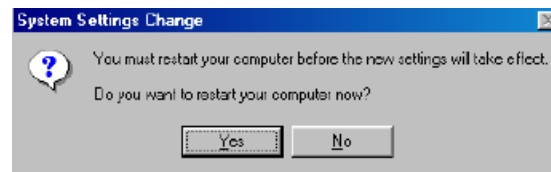


NOTE: If you disable the routers DHCP functions, you will be unable to access the router with the setting shown in step 4. You will need to choose the Specify an IP address option in step 4 and then manually enter an IP address which is on the same subnet as the router and the Subnet Mask. For instance, assuming the router's default IP address is 192.168.0.1, an IP address on the same subnet would be 192.168.0.2 or 192.168.0.13 .

- Click the **IP Address** tab. Choose *Obtain an IP address automatically* and click **OK**.



- The "System Settings Change" window appears. Click Yes to reboot your system.



6.4. Login to Web Configuration Tool

1. Be sure you have configured your computer's TCP/IP settings as described in the section 6.3.
2. Launch a compatible Internet Browser. In your Browser window, type the default IP address of the router, **192.168.0.1** into the URL bar and click **GO** or hit the **Enter** key.
3. You will be prompted to enter a **User Name** and **Password**. The default User Name and Password are:

User Name: **admin**

Password: **admin**

Figure 6-1 Login Web Configuration Tool

1. After logging into your router, the “Welcome!” page will appear on the screen.

| Port | Type | Connected |
|----------|----------|-----------|
| Ethernet | ethernet | ● |
| Hdlc | hdlc | ● |

Figure 6-2 Web Tool - Welcome page

6.5. Status Menu

Login the Web Configuration GUI as described in the previous section. Click the **Status** link from the left frame, then a “Status” page will appear as below.

Status

This page shows the status of your connection

Status

PPPoH Connection: Connection established (open for IP, sent 472, received 471) [Disconnect](#)

Connected time so far: 01:11:26s

WAN IP Address: 10.10.10.6 [▶ WAN Settings...](#)

Local IP Address: 192.168.7.64 [▶ LAN Settings...](#)

Advanced Diagnostics

Port Connection Status

| Port | Type | Connected |
|----------|----------|--------------------------------------|
| Ethernet | ethernet | ● |
| Hdlc | hdlc | ● |

WAN Status

IP Address Type: Dynamic [▶ IP Address Settings...](#)

WAN Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Primary DNS: None [▶ DNS Client Settings...](#)

LAN Status

LAN Subnet Mask: 255.255.0.0

Act as Local DHCP Server: No [▶ DHCP Server Settings...](#)

DHCP Server Address: 192.168.7.64

MAC Address: 00:2D:33:44:55:62

Software Status

Up-Time: 01:15:01s

Current Time: 11:53:07s [▶ Set Time...](#)

Version: 1.7 (v1.7)

Defined Interfaces

| | Upstream / Downstream | |
|------------------|-----------------------|--------------------------------------|
| ppp: | 492 / 471 | ▶ Show Statistics... |
| Ethernet: | 867 / 55902 | ▶ Show Statistics... |

Routing Table

| Destination | Netmask | Gateway | Interface |
|--------------|-----------------|---------|-----------|
| 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | ppp-0 |
| 10.10.10.6 | 255.255.255.255 | 0.0.0.0 | ppp-0 |
| 192.168.7.64 | 255.255.255.255 | 0.0.0.0 | eth0 |

Figure 6-3 Web Tool – Status page

The **Status** Menu contains information about the current configuration of your router. It contains two sections: **Status** and **Advanced Diagnostics**.

The **Status** section displays:

- **WAN IP Address:** Current WAN IP address of your router card.
- **Local IP Address:** Current local IP address of your router card.

The **Advanced Diagnostics** section displays:

- **Port Connection Status:** This section displays the type and connection status of ports. Refer to Table 7-1 for the names of the ports.
- **WAN Status:** This section displays information about your WAN configuration. It also provides two hyperlinks: (1) *IP Address Settings* -- allows you to create, modify or delete your WAN Configuration, (2) *DNS Client Settings* -- allows you to create, modify or delete your DNS Client configuration.
- **LAN Status:** This section displays information about your Local Area Network settings. It also provides a *DHCP Server Settings* hyperlink that allows you to configure your DHCP server status.
- **Software Status:** This section displays information about your software version. It provides a *Set Time* hyperlink that allows you to set the system time.
- **Defined Interfaces:** This section lists frame relay (or ppp) and Ethernet interfaces that have been defined. Each interface listed has a *Show Statistics* hyperlink that will display more detailed information about the IP interface, physical port, frame relay, or ppp connection.
- **Routing Table:** This section displays the current routing table.

6.6. System Menu

The **System** menu contains options that describe the system and allow low-level changes to be made. Login the web configuration GUI (refer to the section 6.1). Click the **System** link from the left frame, and then the following sub-headings will be shown on the left frame.

- **Error Log:** This page display information about recent configuration errors.
- **Upgrade:** This page allows you to upgrade your firmware to your router.

WARNING: Do not upgrade firmware unless you have been specifically instructed to do so. It is unnecessary to upgrade the firmware if your device is working properly. To do so may cause malfunction to your device.

- **Restart:** This page allows you to restart your router. It has the same effect as resetting your router by pressing the front panel RESET button.

Error Log

The Error Log displays any recent configuration errors.

To access the Error Log, simply login to your router. From the left frame, click **System**, and then from the submenu, click **Error Log**. Then the following page will appear.

Error log
This page shows recent configuration errors from your router

Error log (*most recent errors first; times are in seconds since last reboot*):

| When | Process | Error |
|------------|---------|--|
| 1023085899 | im | im:Invalid argument:failed to set the SNTP host to |

Figure 6-4 Web Tool – Error Log page

Upgrade

The remote upgrade firmware can only be accessible through the Web Configuration Tool. The “Firmware Upgrade” page allows you to upgrade the firmware version of your router. You will need to download the new firmware file (the file name is http-upload.tar and you don’t have to uncompress the file) to your computer in order to upgrade successfully.

The router will preserve your installed configuration during a firmware upgrade and reinstall it once the firmware upgrade is complete. In other words, if you have saved a configuration in the router, you will not need to re-configure the router after upgrading the firmware.

1. Log in to your router. From the left frame, click **System** and then **Upgrade**. The “Firmware Upgrade” page will appear. In the “Select Upgrade File” section, enter the path to your new firmware file, or click the **Browse** button and browse to it. When you have found the file, click the **Upgrade** button.

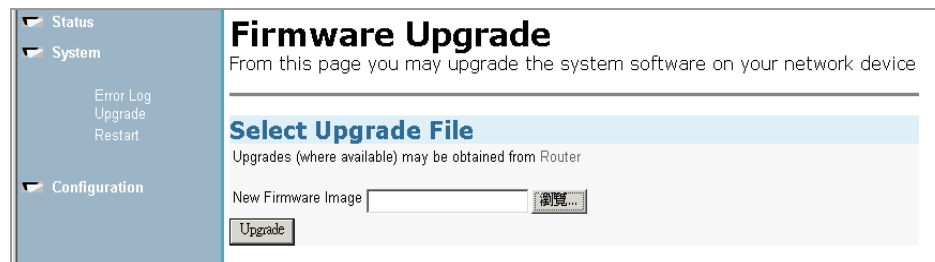


Figure 6-5 Web Tool – Firmware Upgrade page

2. The “Firmware Upgrade” page will refresh and begin installing the new firmware file. It will show a progress bar, indicating how much data has been installed.

3. Once the firmware upgrade is complete, the “Firmware Upgrade” page will refresh and indicate a successful upgrade. You will need to restart in order for the upgrade to take effect. Click the **Restart** button.

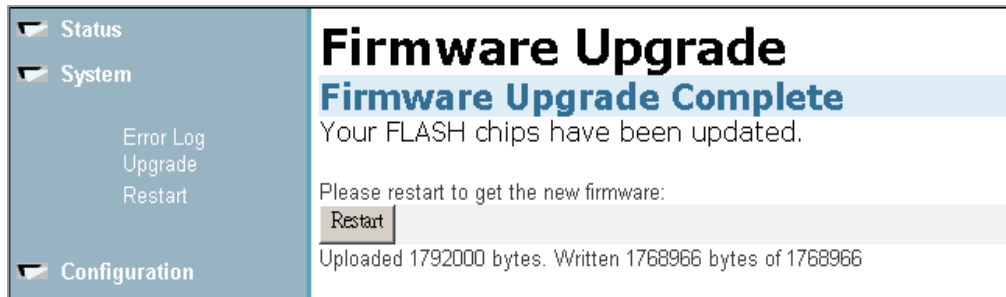


Figure 6-6 Web Tool – Firmware Upgrade Complete page

4. After the router card is restarted, it will receive the clock speed change message “**Change wan port's clock speed require save and restart**” from the primary T1/E1 card (but you won't see the message on the web browser). You have to re-login the web browser, save the configuration (refer to 0) and restart (refer to 0) the router card again.

Warning: Do not disturb or power off the router during the upgrade process. Doing so may corrupt the firmware. Users must be patient to wait the result screen appear when they are doing the firmware upgrade and save configuration. If users interrupt the process arbitrarily, system could not run normally, and users have to re-upgrade again.

Restart

This page allows you to restart your router. Be sure that you have saved your configuration before restarting to preserve your modifications. Restarting the router will restore the last configuration 'saved'.

1. Log in to your router. From the left frame, click System and then Restart. The "Restart Router" page will appear. In the "Restart" section, click the **Restart** button.

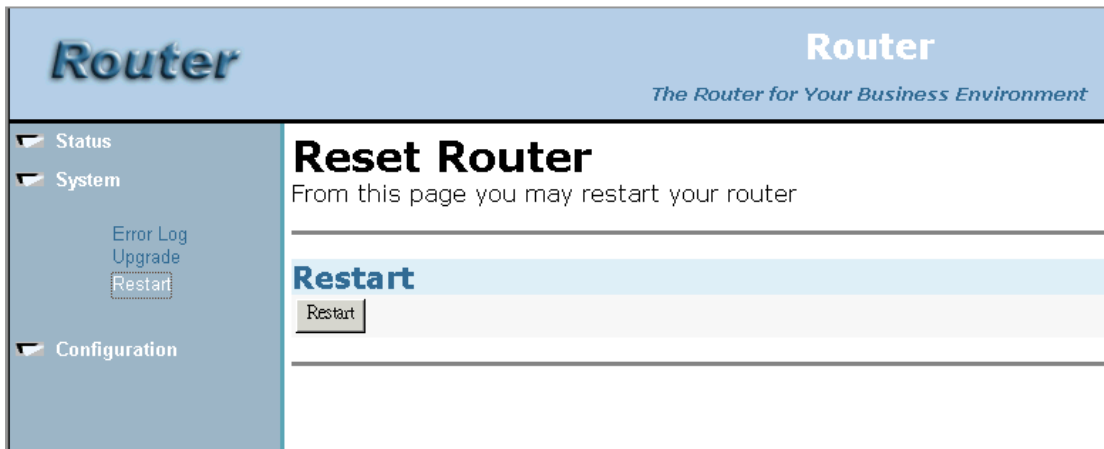


Figure 6-7 Web Tool – Reset Router page

Warning: when you first time login to the Web browser or first time re-login to the Web browser after the router card is restarted, you have to wait for several seconds. During the waiting time, don't restart the router card or pull out the card from the slot. Otherwise, you'll have to reload the firmware into the router card.

6.7. Configuration Menu

The **Configuration** menu contains options for configuring features on the router including basic LAN and WAN connections, DHCP and DNS settings, and VPN settings. There are sixteen sub-headings on the left frame in the configuration menu.

- **Save config:** Allows you to save your current configuration to Flash memory.
- **Authentication:** Allows you to create, edit and delete user accounts for the web configuration tool.
- **LAN connections:** Allows you to edit the LAN port IP address, create and edit a secondary IP address, and modify the RIP options.
- **WAN connections:** Allows you to create, edit, and delete WAN services.
- **IP routes:** Allows you to create, edit, and delete IP routers.
- **DHCP server:** Allows you to enable, disable and configure your DHCP server.
- **DNS client:** Allows you to enable, disable and configure your DNS client.
- **DNS relay:** Allows you to enable, disable and configure your DNS relay.
- **Security:** Allows you to configure Security, Firewall, NAT, and Intrusion Detection.
- **IPSec:** Allows you to configure gateway setting, endpoint, and certificate status.
- **PPTP:** Allows you to configure PPTP IP pool and set users.
- **L2TP:** Allows you to configure L2TP IP pool and set users.
- **SNTP client:** Allows you to set time zone, synchronization time from unicast server, and set the system clock.
- **Syslog:** Allows you to configure minimum severity threshold.
- **SNMP:** Allows you to configure read and write community, IP address, and subnet mask.
- **Ports:** Allows you to configure the Ethernet port available on your router.

For more information, see the following detailed descriptions for each sub-heading.

Save config

After configuring or modifying the configuration of your router, and before powering it off or rebooting it, you must save your configuration to the internal flash memory. Should you power off or reboot the router without saving, you will lose the settings previously configured. Be sure to save after making any change to your configuration.

1. Once you have completed configuring your router, click **Configuration** and then click **Save config** from the left frame. The “Save configuration” page will appear. You will be asked to confirm that you are ready to save. Click the **Save** button. Do not disturb the router while it is writing to the Flash memory, as doing so may corrupt the firmware. Do not turn the power off or disturb the router until the confirmation message has been displayed.



Figure 6-8 Web Tool – Save configuration Confirm page

2. The “Save configuration” page will reload stating that it has saved the configuration.



Figure 6-9 Web Tool – Save configuration completed page

Warning: Users must be patient to wait the result screen appear when they are doing the firmware upgrade and save configuration. If users interrupt the process arbitrarily, system will not run normally.

Authentication

The User Management section allows you to control the access levels of your defined users. The default user name and password for the router is:

Table 6-1 Default user name and password

| User name | Password |
|-----------|----------|
| admin | admin |
| firewall | firewall |
| user | user |

✧ To Edit a User, Change the Password, or Delete a User

1. Login to your router. From the left frame, click **Configuration** and then **Authentication** from the submenu. The “Authentication” page will appear and show the currently defined users. Click the **Edit user** link on the right side of the user which you would like to edit or delete.

Router
The Router for Your Business Environment

▼ Status
▼ System
▼ Configuration

Save config
Authentication
LAN connection
WAN connections
IP routes
DHCP server
DNS client
DNS relay
Security
IPSec
PPTP
L2TP
SNTP client
Syslog
Snmp
▼ Ports

Authentication

This page allows you to control access to your router's console and the pages

Currently Defined Users

| User name | GUI user | Dial-in user | pppLogin | accessLevel | Comment | |
|-----------|----------|--------------|----------|-------------|---------------|----------------|
| user | true | false | none | default | Default guest | Edit user... ▶ |
| firewall | true | false | none | engineer | Default user | Edit user... ▶ |
| admin | true | true | none | superuser | Default admin | Edit user... ▶ |

Create a new user... ▶

Figure 6-10 Web Tool – Authentication page

2. The “Authentication: Edit User ‘username’ ” page will appear. To delete this user, simply click the **Delete this user** button near the bottom of the screen. Or you may edit the settings of your choice for the user. You may enter a new password in the password field, which is recommended for the admin user. Then enter the description about the user, and select the access level using the “Access Level” menu.

Authentication: edit user 'admin'

Details for user 'admin'

Username: **admin**

Password:

GUI user?:

Dial-in user?:

pppLogin:

Access Level:

Comment:

Cancel and return to Authentication Setup Page...
 Cancel and return to Authentication Setup Page... ▶

Figure 6-11 Web Tool – Authentication: edit user details page

- **Username:** the user that you are editing (not editable)
- **Password:** This field contains the default password, which matches the username (see Table 6-1). You may edit this field to be the password of your choice.
- **GUI user?:** Enable or disable GUI users access the router.
- **Dial-in user?:** Enable or disable ppp dial-in users access the router.
- **pppLogin:** Set the ppp authentication protocol. The options are none, chap, or pap.
- **Comment:** You may change the comment field to whatever you wish.
- **Access Level:** This will set the level of access that this user has.

The access level determines what a user can do within the configuration. Table 6-2 is a list of

the functions users can edit based on their access levels:

Table 6-2 User access levels

| Access Level | Functions |
|--------------|--|
| superuser | All configurations |
| engineer | All configurations, except firmware upgrade, and user management |
| default | View status, view error log, system restart |

Finally, click the **Apply** button to apply your new settings.

3. You will be returned to the “**Authentication**” page. You may now edit another user, or create a new one, if needed. See the next subsection for instructions on creating a new user.

✧ **To Create a New User**

1. Login to your router. From the left frame, click **Configuration** and then **Authentication** from the submenu. The “Authentication” page will appear as shown in Figure 6-10. Click the **Create a new user** link to add a new user. The page will appear as follows.

Figure 6-12 Web Tool – Authentication: create user page

2. In the “Authentication: create user” page, the details for a new user includes the following items:
 - **Username:** Enter the new username you want to create
 - **Password:** Enter the password of the new user
 - **GUI user?:** Enable or disable GUI users access the router.
 - **Dial-in user?:** Enable or disable ppp dial-in users access the router.
 - **pppLogin:** Set the ppp authentication protocol. The options are none, chap, or pap.
 - **Access Level:** This will set the level of access that this user has. Refer to Table 6-2 for the access level information.
 - **Comment:** You may edit the comment field to whatever you wish.

After you have entered all the fields, click **Create** button to create a new user.

3. The “Authentication” page will appear again, showing your newly added user in the list of currently defined users. You may edit or delete a user or create a new user at any time.

Authentication

This page allows you to control access to your router's console and the pages

Currently Defined Users

| User name | GUI user | Dial-in user | pppLogin | accessLevel | Comment | |
|-----------------|----------|--------------|----------|-------------|---------------|----------------|
| <i>newuser</i> | false | false | none | default | add user test | Edit user... ▶ |
| <i>user</i> | true | false | none | default | Default guest | Edit user... ▶ |
| <i>firewall</i> | true | false | none | engineer | Default user | Edit user... ▶ |
| <i>admin</i> | true | true | none | superuser | Default admin | Edit user... ▶ |

Create a new user... ▶

Figure 6-13 Web Tool – Authentication: Currently Defined Users page

LAN Connections

The LAN Connections page allows you to change the default and secondary IP address for the LAN port and lets you modify the RIP options.

1. Login to your router. From the left frame, click **Configuration** and then click **LAN connection**. The “LAN connection” page will appear.

LAN connection

This page allows you to change the IP address for the default LAN port

RIP Options

Accept V1:

Accept V2:

Send V1:

Send V2:

Send Multicast:

Enable Password:

Password:

LAN Configuration

Primary IP Address

IP Address:

Subnet Mask:

Secondary IP Address

IP Address:

Subnet Mask:

DHCP Client:

Warning: If you have enabled DHCP Client Option, the router LAN port IP will change. You will then need new LAN port IP address. To return to configuration, enter new IP address in the browser URL and hit Enter

Figure 6-14 Web Tool – LAN connection page

RIP Options:

- **Accept V1:** Set to *true* if you would like to receive version 1 routing information packets.
- **Accept V2:** Set to *true* if you would like to receive version 2 routing information packets.
- **Send V1:** Set to *true* if you would like to send version 1 routing information

packets.

- **Send V2:** Set to *true* if you would like to send version 2 routing information packets.
- **Send Multicast:** Set to *true* if you need to send multicast packets (often used when you obtain your LAN port IP address dynamically). This item is useful only when **Send V2** is set to true.
- **Enable Password:** You may set this to *true* to require incoming packets to have the proper password to be recognized.
- **Password:** Enter your desired password for incoming RIP packets.

<Note: If the router is set in RIP v2 mode, and you still want it to be RIP v1 compatible, you must enable Accept V1, Accept V2, Send V1, Send V2, but disable Send Multicast>

LAN Configuration:

- **Primary IP Address** setting:

IP address and subnet mask details of your primary LAN connection. To edit these details, click in the appropriate text box and type new primary address details. If the IP address is set to the special value *0.0.0.0*, the interface is marked as unconfigured. This value is used when the interface address is obtained automatically.

- **Secondary IP Address** setting:

A secondary address may be used to create an extra IP address on an interface for management purposes, or to allow the IP stack to route between two subnets on the same interface. The functionality of secondary IP addresses depends on several parameters including the type of IP interface and the subnet mask:

If a secondary address is on the same subnet as the primary interface address, you do not need to specify a subnet mask for that secondary address. This applies to all interface types.

If a secondary address is on a different subnet to the primary address, and the interface is Ethernet or a transport using a bridged encapsulation, you must specify the subnet mask. The IP stack will listen on the new address for connections to local services (e.g., for management purposes), and will also route packets to the new subnet.

If a secondary address is on a different subnet to the primary address, and the interface

is a point-to-point interface, specifying a subnet mask is optional.

For the same behavior as described for Ethernet interfaces above, the subnet mask should be specified. If the subnet mask is not specified, the IP address will not be associated with any subnet, but will still be recognized as one of the IP stack's own addresses for local traffic.

- **DHCP Client:** Set to true if you would like to configure the router as a DHCP client.

After entering your RIP and LAN configuration settings, click **Apply**. The "LAN Connection" page will appear stating the changes you have just made.

WAN Connections

The WAN Connections page allows you to create different kinds of WAN services.

Creating or Editing a WAN service:

1. From the left frame, click the **Configuration** link, then click **WAN connections** link.

The “WAN connections” page will appear as below. The page lists all the currently defined connections (services). You can edit or delete the connections, or you can create a new service but only one WAN service can exist at a time).



Figure 6-15 Web Tool – WAN connections page

2. If there's no currently defined service, you will see the following page after you click the **Create a new service** link in the “WAN connections” page:

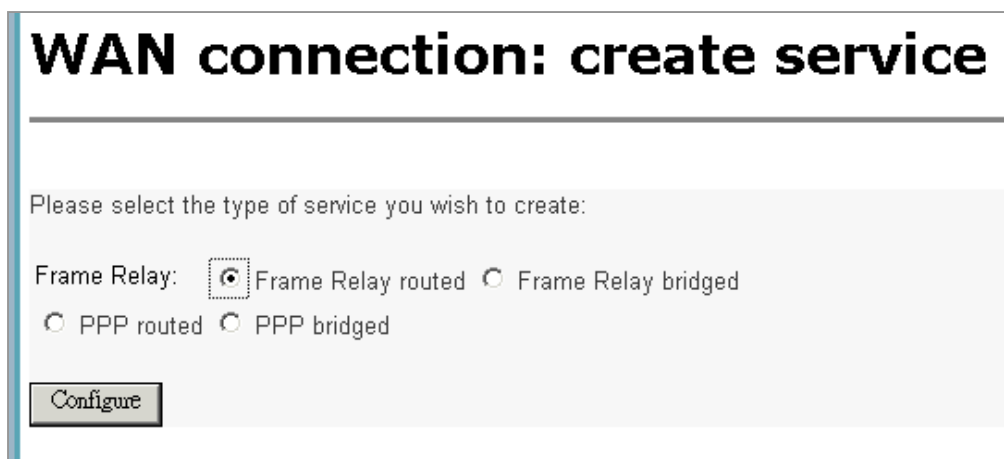


Figure 6-16 Web Tool – WAN connection: create service page

Select the type of service you want to create, and then click the **Configure** button.

✧ **Frame Relay routed**

1. If you select **Frame Relay routed** in the “WAN connection: create service” page, the following page will appear. The option fields include:

Description: Enter a brief description for the service.

DLCI: DLCI (data link connection identifier) sets the identifier for the Frame Relay data link channel that you are using. The range of the DLCI is 16 to 1007.

Encapsulation method: sets the RFC1490 encapsulation method used by Frame Relay. Each DLCI can be multiplexed further if you are using RFC1490 multi-protocol encapsulation. The choices are: Raw, Routed IP.

Use DHCP or WAN IP address: You must choose “Use DHCP” if you want to set the router as a **DHCP client**.

After entering all the fields needed in this page, click **Apply** button.

WAN connection: Frame Relay routed

Description:

DLCI:

Encapsulation method:

Use DHCP

WAN IP address: WAN IP netmask:

Figure 6-17 Web Tool - WAN connection: Frame Relay routed page

Note: The maximum number of Frame Relay DLCI channels that can be created is 14.

2. To edit a currently defined frame relay routed service, click “Edit” link for that connection as in Figure 6-15, then the page will appear as follows.

Figure 6-18 Web Tool – WAN connection: frame relay routed: Edit Service page

To edit the service, click on the links at the top of the edit page. The links include: *Edit ‘Service’, Edit ‘Frame Relay’, Edit ‘Frame Relay Channel’, Edit ‘IP Interface’, Edit ‘Rip Versions’, and Edit ‘Tcp Mss Clamp’.*

In “Edit Service” page, you can edit the creator name and the brief description of the service.

In “Edit Frame Relay Channel” page, the option fields include:

DLCI: sets the DLCI; the identifier for the Frame Relay data link channel that you are using. The range of the DLCI is 16 to 1007.

Rx Max Pdu: sets the maximum Protocol Data Unit (PDU) size that can be received over Frame Relay. The default value is 8192.

Tx Max Pdu: sets the maximum Protocol Data Unit (PDU) size that can be transmitted over Frame Relay. The default value is 8192.

Chnl Segment Size: sets the size of the channel segment used by Frame Relay. The default

value is 0. If you set this to any number other than 0, DLCI level FRF.12 segmentation is enabled. The range of the segment size recommended is 200 to 1500. For more information on FRF.12, see <http://www.frforum.com>.

Port: sets the port that an existing Frame Relay transport uses to transport data. (The port is always fr for frame relay routed.)

| Name | Value |
|--------------------|----------|
| Dlci: | 16 |
| Encaps Type: | RoutedIP |
| Rx Max Pdu: | 8192 |
| Tx Max Pdu: | 8192 |
| Chnl Segment Size: | 0 |
| Port: | fr |

Change Reset

Figure 6-19 Web Tool – WAN connection: Edit Frame Relay channel page

In “*Edit Ip Interface*” page, the Ipaddr, Mask, and Dhcp are the same meaning as in Figure 6-17. The MTU (maximum transmission unit) is the largest size frame that can be sent in transmission. The default MTU is 1500 octets. The Enabled is set to true by default. If the Enabled is set to false, the specified IP interface does not work.

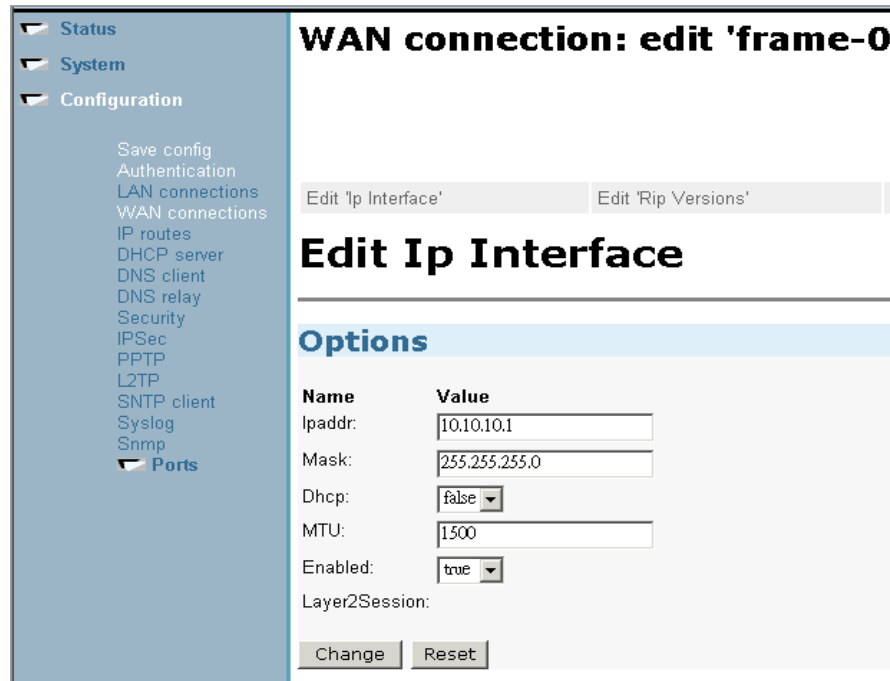


Figure 6-20 Web Tool – WAN connection: Edit IP Interface page

In “Edit Rip Versions” page, you can refer to section 0 for the setting rule of RIP options.

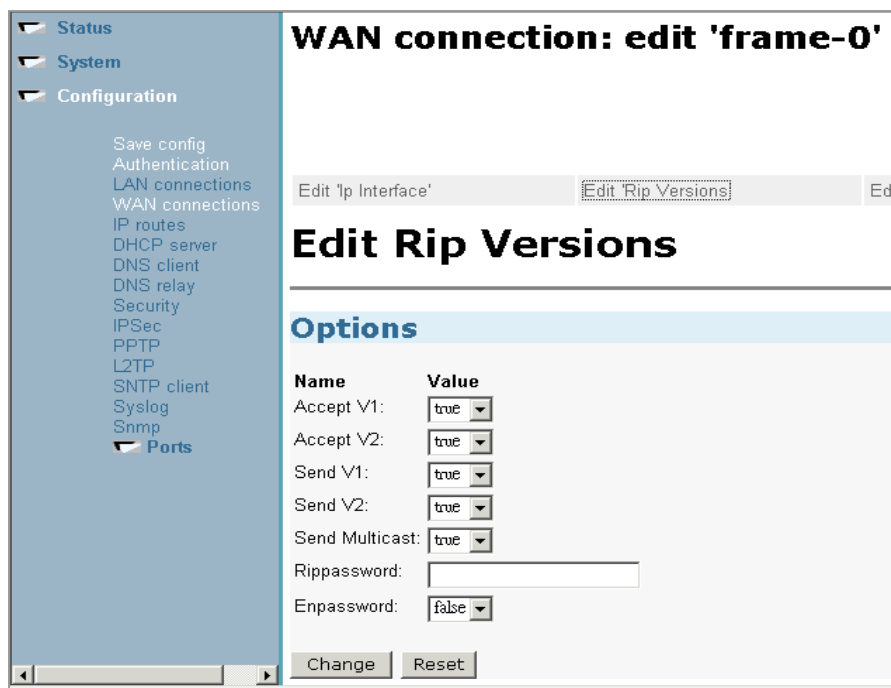


Figure 6-21 Web Tool – WAN connection: Edit Rip Versions page

In “*Edit Tcp Mss Clamp*” page, you can set the Tcp Mss Clamp to true or false. The TCP Maximum Segment Size (MSS) Clamp intercepts TCP synchronization (SYN) packets as the router forwards them. These packets advertise the MSS that the host is prepared to accept.

The clamp modifies the MSS of outgoing packets according to the MTU of the interface on which the packet is transmitted. The MSS is modified so that it is no bigger than the interface MTU minus the IP and TCP header. This ensures that once the connection is established, the data packets will not be large enough to require fragmentation when sent over the link with the smaller MTU.

Note – The TCP MSS clamp should be **used with care**. Allowing the router to change data in the TCP header is against the nature of the protocol stack - the lower IP protocol alters data in the higher level TCP protocol. A TCP stream with IPSec/VPN should **never** be modified by the MSS clamp.

REMEMBER! When you have completely configured your router, please be sure to save your new configuration by clicking the Save config link from the left frame and follow the steps there within. Please see 0 Save config section for more information regarding save procedures.

✧ **Frame Relay bridged**

1. If you select **Frame Relay bridged** in the “WAN connection: create service” page, the following page will appear. The option fields include:

Description: Enter a brief description for the service.

DLCI: DLCI (data link connection identifier) sets the identifier for the Frame Relay data link channel that you are using. The range of the DLCI is 16 to 1007.

Encapsulation method: sets encapsulation method used by Frame Relay bridged. The choices are: Bridged Ethernet, Bridged Ethernet with CRC, and Raw.

After entering all the fields needed in this page, click **Apply** button.

Figure 6-22 Web Tool – WAN connection: Frame Relay bridged page

2. To edit a currently defined frame relay bridged service, click “Edit” link for that connection as in the figure below. Then the edit page will appear.

| Name | Description | Creator | Edit... | Delete... |
|---------|---------------------|----------|---------|-----------|
| frame-0 | Frame relate bridge | WebAdmin | ▶ | ▶ |

Create a new service... ▶

Figure 6-23 Web Tool – WAN connections page

To edit the service, click on the links at the top of the edit page. The links include:

Edit ‘Service’, Edit ‘Frame Relay’, Edit ‘Frame Relay Channel’, Edit ‘Bridge Interface’, and Edit ‘Spanning Bridge Interface’.

In “*Edit Bridge Interface*” page, the option fields include:

Ether Filter Type: The value can be All, Ip, or Pppoe.

Enabled: true or false.

In “*Edit Spanning Bridge Interface*” page, the option fields include:

Enabled: specifies whether or not the bridge is to implement the spanning tree protocol (STP).

Priority: sets the spanning tree protocol priority.

Path Cost: sets the cost of the path from all bridges to the root bridge.

In “*Edit Frame Relay*” page, the option fields include:

DLCI: sets the DLCI; the identifier for the Frame Relay data link channel that you are using. The range of the DLCI is 16 to 1007.

Rx Max Pdu: sets the maximum Protocol Data Unit (PDU) size that can be received over Frame Relay. The default value is 8192.

Tx Max Pdu: sets the maximum Protocol Data Unit (PDU) size that can be transmitted over Frame Relay. The default value is 8192.

Chnl Segment Size: sets the size of the channel segment used by Frame Relay. The default value is 0. If you set this to any number other than 0, DLCI level FRF.12 segmentation is enabled. The range of the segment size recommended is 200 to 1500. For more information on FRF.12, see <http://www.frforum.com>.

Port: sets the port that an existing Frame Relay transport uses to transport data. (The port is always fb for frame relay bridged.)

For the other Edit items, please refer to the descriptions in the **Frame Relay routed** subsection.

Note: The maximum number of Frame Relay DLCI channels that can be created is 14.

✧ **PPP routed**

1. If you select **PPP routed** in the “WAN connection: create service” page, the following page will appear. The option fields include:

Description: enter a brief description for the service.

WAN IP address: enter the WAN IP address of the router card.

WAN IP netmask: enter the WAN IP netmask of the router card.

Listening or not: determines whether the router can accept incoming connections from a remote PPP server. Set to on to accept.

Authentication to log in a remote peer: The choices are None, PAP, and CHAP.

User name: sets the dial-out user name.

Password: sets the dial-out password.

After entering all the fields needed in this page, click **Configure** button.

WAN connection: PPP routed

Description:

WAN IP address: WAN IP netmask:

Listening or not:

Authentication to log in a remote peer:

User name:

Password:

Figure 6-24 Web Tool – WAN connection: PPP routed page

2. To edit the currently defined PPP routed service, click “Edit” link for the connection as in the figure below. Then the edit page will appear.

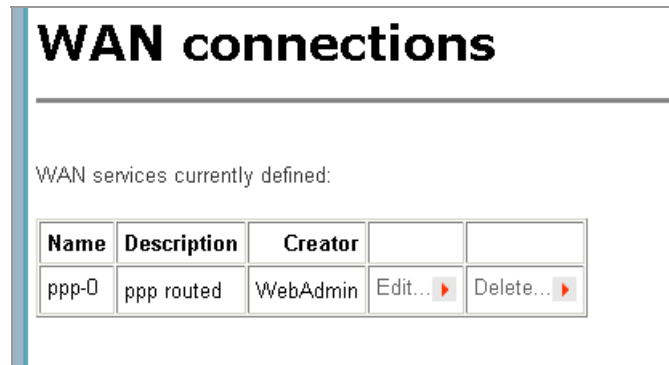


Figure 6-25 Web Tool – WAN connections page

To edit the service, click on the links at the top of the edit page. The links include: *Edit ‘Service’, Edit ‘PPP’, Edit ‘Hdlc Channel’, Edit ‘Ip Interface’, Edit ‘Rip Versions’, and Edit ‘Tcp Mss Clamp’.*

In “Edit PPP” page, the option fields include:

Server: PPP server true or false. If this is set to true, the router card is configured to be a PPP server; if false, the router card is configured to be a PPP client.

Note: The two ends of a PPP link must not be PPP servers at the same time.

Create Route: set to *true*, a route will be created which directs packets to the remote end of the PPP link.

Specific Route: set to *false*.

Subnet Mask: sets the subnet mask used for the local IP interface connected to the PPP transport.

Route Mask: sets the subnet mask used by the route that is created when a PPP link comes up. If it is set to *0.0.0.0*, the subnet mask is determined by the IP address of the remote end of the link.

Lcp Max Configure: sets the Link Control Protocol (LCP) maximum parameter for an existing PPPoH transport.

Lcp Max Failure: sets the Link Control Protocol (LCP) maximum fail parameter for an existing PPPoH transport.

- Lcp Max Terminate:** sets the Link Control Protocol (LCP) maximum terminate parameter for an existing PPPoH transport.
- Dialin Auth:** sets the authentication method that remote PPP clients must use to dialin to the server. The choices are: none, chap, and pap.
- Dialout Username:** sets the dial-out user name.
- Dialout Password:** sets the dial-out password.
- Confirmation Password:** sets the confirmation password.
- Dialout Auth:** sets the authentication protocol used to connect to external PPP servers (dial-out). The choices are: none, chap, and pap.
- Interface ID:** sets the PPP interface ID for an existing PPPoH transport.
- Remote Ip:** sets the IP address supplied to the remote end of the PPP connection during negotiation. If the remote peer doesn't set its IP address for PPP connection, it will use the IP set in this field. But if the remote peer already set its IP address for PPP connection, you must not set the Remote IP or the connection can't be established.
- Local Ip:** tells the PPP process the local IP address to be associated with the local end of the WAN interface after a successful connection.
- Magic Number:** sets the magic number. This option provides a method to detect looped-back links and other Data Link Layer anomalies. For more information, please refer to RFC 1661 section 6.4 Magic-Number.
- MRU:** sets the Maximum Receive Unit.
- Ip Addr From IPCP:** sets to true if you want to get your local IP address from the PPP negotiation or false if you do not want to receive the local IP.
- Discovery Primary DNS:** enables/disables whether the primary DNS server address is requested from a remote PPP peer using IPCP.
- Discovery Secondary DNS:** enables/disables whether the secondary DNS server address is requested from a remote PPP peer using IPCP.
- Give DNS to Relay:** controls whether the PPP Internet Protocol Control Protocol (IPCP) can request the DNS server IP address for a remote PPP Peer.
- Give DNS to Client:** controls whether the PPP Internet Protocol Control Protocol (IPCP) can request a DNS server IP address for a remote PPP peer.
- Remote DNS:** sets the primary local DNS server addresses that will be given to a remote PPP peer when the peer requests a primary DNS server IP address using IPCP.
- Remote Secondary DNS:** sets the secondary local DNS server addresses that will be given

to a remote PPP peer when the peer requests a secondary DNS server IP address using IPCP.

Lcp Echo Every: tells a specified PPP transport to send an LCP echo request frame at specified intervals (in seconds). If no reply to the request is received, the PPP connection is torn down.

Auto Connect: sets to true or false.

Idle Timeout: sets the idle time out (in minutes).

Enabled: enables/disables a PPPoH transport.

In “Edit Hdlc Channel” page, the option fields include:

Port: sets the port that an existing transport uses to transport PPP data. (Currently this can't be edited. The value is always hdlc)

For the other Edit items, please refer to the descriptions in the **Frame Relay routed** subsection.

✧ **PPP bridged**

1. If you select **PPP bridged** in the “WAN connection: create service” page, the following page will appear. The option fields include:

Description: Enter a brief description for the service.

WAN IP address: enter the WAN IP address of the router card.

Listening or not: determines whether the router can accept incoming connections from a remote PPP server. Set to on to accept.

Authentication to log in a remote peer: The choices are None, PAP, and CHAP.

User name: sets the dial-out user name.

Password: sets the dial-out password.

After entering all the fields needed in this page, click **Configure** button.

WAN connection: PPP bridged

Description:

Listening or not:

Authentication to log in a remote peer:

User name:

Password:

Figure 6-26 Web Tool – WAN connection: PPP bridged page

2. To edit the currently defined PPP bridged service, click “Edit” link for the connection as in the figure below. Then the edit page will appear.

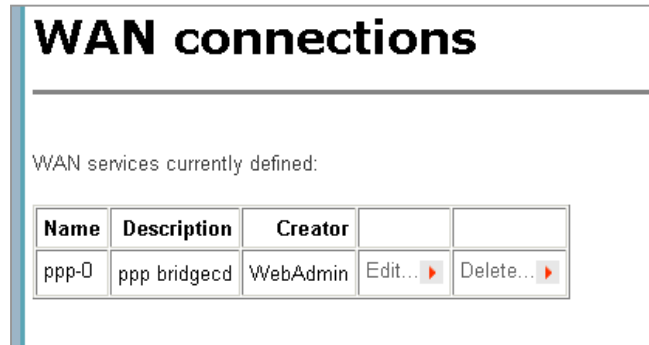


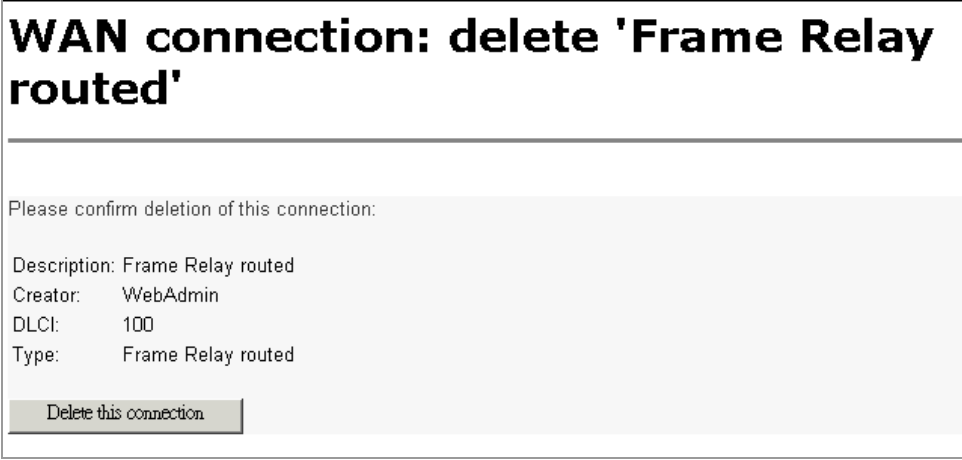
Figure 6-27 Web Tool – WAN connections page

To edit the service, click on the links at the top of the edit page. The links include: *Edit ‘Service’, Edit ‘PPP’, Edit ‘Hdlc Channel’, Edit ‘Bridge Interface’, and Edit ‘Spanning Bridge Interface’.*

For the *Edit ‘PPP’* and *Edit ‘Hdlc Channel’* items, please refer to the descriptions in the **PPP routed** subsection. For the other *Edit* items, please refer to the descriptions in the **Frame Relay bridged** subsection.

Deleting a WAN service:

If you want to delete a currently defined service, click “Delete” link for that service in “WAN connections” page. The following example is to delete a frame relay routed connection ‘frme-0’. After clicking the “Delete” link, a confirm page will appear as follows. Click the **Delete this connection** button to delete the connection.



The screenshot shows a web page titled "WAN connection: delete 'Frame Relay routed'". Below the title, there is a confirmation message: "Please confirm deletion of this connection:". Underneath, the following details are listed: "Description: Frame Relay routed", "Creator: WebAdmin", "DLCI: 100", and "Type: Frame Relay routed". At the bottom of the page, there is a button labeled "Delete this connection".

Figure 6-28 Web Tool – WAN connection: delete ‘Frame Relay routed’ page

IP routes

The IP Route Configuration allows you to create static IP routes to destination addresses via an IP interface name or a Gateway address. IP Routes do not need to be configured for dynamic connections.

1. Log-in to your router. From the left frame, click **Configuration** and then **IP Routes**. The “Edit Routes” page will appear, showing all configured routes, if any. Click **Create New Ip V4Route**, then the page will appear as follows.

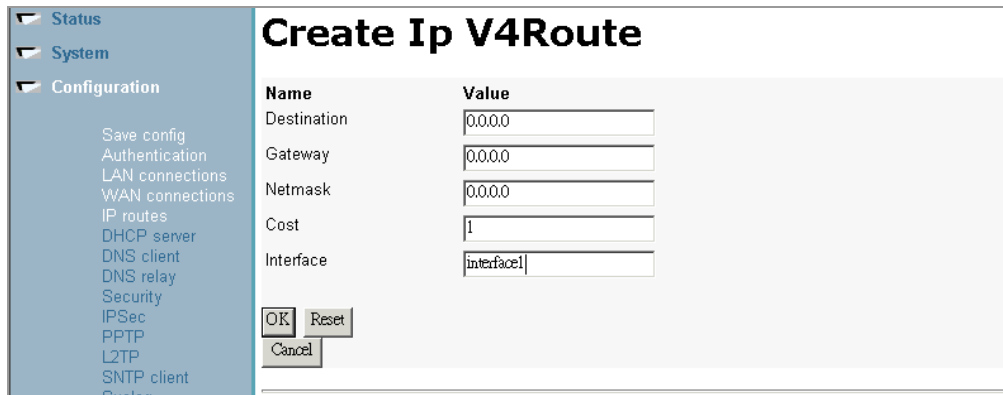


Figure 6-29 Web Tool – IP routes: Create Ip V4Route page

2. Enter the destination, gateway and netmask for your route. You can also specify the cost and the interface to apply it to. Use the name of your WAN or LAN interface. Click **OK**, then the “Edit Routes” page will appear and show the configured route. There is a Valid indicator showing the status of each route. If the LED color is red, the route is invalid because of the wrong interface name or the same Destination/Netmask as some already existing route. If the LED color is green, the route is a valid route.

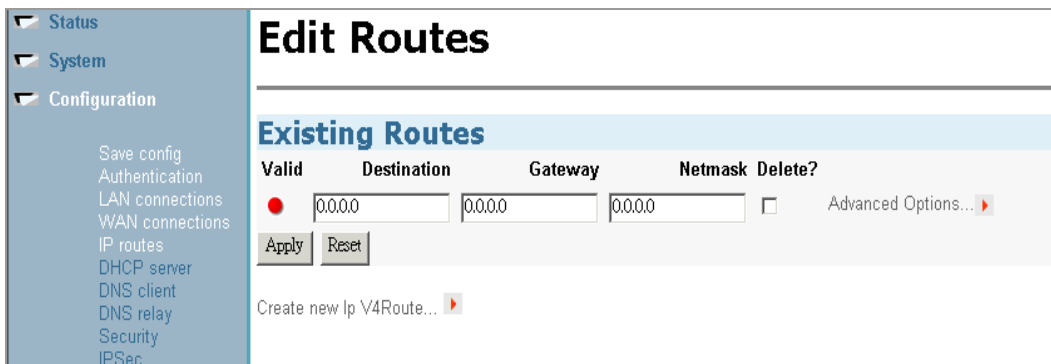


Figure 6-30 Web Tool – IP routes: Edit Routes page

NOTE: To set rip host route or rip poison, you can only do the setting by CLI commands. You cannot access these two IP routes features through Web configuration.

DHCP Server

DHCP is a client-server protocol that replies to requests from a DHCP server and provides configuration information to devices on an IP network (the DHCP clients). The DHCP server provides network addresses from a central pool on an as-needed basis. DHCP is very useful for providing IP addresses to devices connected to the network temporarily or for sharing a limited pool of IP addresses among a group of hosts that do not need permanent IP addresses.

1. Log-in to your router. From the left frame, click **Configuration** and then click **DHCP Server** from the submenu. The “**DHCP Server**” page will appear, showing the current Server status and DHCP Settings. In the **DHCP Server Mode** section, choose Disabled (disable the DHCP function) or DHCP server or DHCP relay agent, then click the **Configure** button to edit the settings. The DHCP server is disabled by default.

DHCP server

DHCP server status:

Default Lease Time: 43200
 Allow Bootp: true
 Max Lease Time: 86400
 Allow Unknown Clients: true
 Enabled: true
 DHCP Server Address: 192.168.0.1

Subnet definitions:

Subnet Value: 192.168.0.0
 Subnet Mask: 255.255.0.0
 Max Lease Time: 86400
 Default Lease Time: 43200
 Host Is Dns Server: true
 Host Is Default Gateway: true
 Subnet From Interface: eth0
 IP range: 192.168.0.2 - 192.168.0.21
 Option: domain-name-servers = 0.0.0.0

DHCP Server Mode

Disabled
 DHCP server
 DHCP relay agent

Configure

Figure 6-31 Web Tool – DHCP server page

✧ DHCP Server mode

1. If you choose **DHCP server** in the DHCP Server Mode section, this will provide IP addresses to computers connected to the router from within the default IP address pool. You can edit your DHCP settings for a custom configuration by clicking the **Configure** button. The “**DHCP: enable server**” page will appear then. Make any changes to the configuration that are needed and then click the **Apply** button. The fields are defined below.

DHCP: enable server

DHCP Server Setup

Please enter details for DHCP server configuration:

Address Range

Note that your LAN interface has IP address 192.168.0.1, with subnet mask 255.255.0.0; the IP address range should be within this subnet.

Use Default Range (192.168.0.2 - 192.168.0.21)

Starting IP Address

Ending IP Address

Lease Times

Default Lease Time seconds

Maximum Lease Time seconds

Domain Name Servers

List here the primary and secondary domain name servers to be provided to LAN clients.

Use Router as DNS Server

Primary DNS Server Address

Secondary DNS Server Address

Default Gateway

Use Router as Default Gateway

Figure 6-32 Web Tool – DHCP: enable server page

Address Range:

- **Use Default Range:** This will enable the use of the router’s default address pool (as shown). Checking this box will override any settings in the following two fields.
- **Starting IP Address:** This field allows you to define the first address of the range of numbers in your custom address pool. The range will span between this number

and the Ending IP Address, defined in the next field.

- **Ending IP Address:** This field allows you to define the last address in the range of numbers in your custom address pool.

Note: The maximum number of DHCP IP addresses supported by the system is 128.

Lease Times:

- **Default Lease Time:** You may specify the default time, in seconds, of a typical DHCP-assigned address.
- **Maximum Lease Time:** You may specify the maximum time, in seconds, that a device can use a DHCP-assigned address.

Domain Name Servers:

- **Use Router as DNS Server:** Checking here will enable the router to act as a DNS server. If this option is checked, you will need to have DNS Relay enabled.
- **Primary DNS Server Address:** This is where the router will go looking for DNS information. Enter your ISP-provided Primary DNS Server Address here.
- **Secondary DNS Server Address:** This is where the router will go looking for DNS information if the primary address is busy or not responding. Enter your ISP-provided Secondary DNS Server Address here.

Default Gateway:

- **Use Router as Default Gateway:** It is recommended that you check this field.

2. The “DHCP Server” page will appear again, showing your new changes. Review your new settings. If you should need to modify the settings further, you may click the **Configure the DHCP Server** button at the bottom of the page.

Note: WINS server configuration cannot be made by web browser. Users can only configure the WINS server by using CLI commands. See the following example:

```
-->dhcpserver subnet 1 add option netbios-node-type 8
-->dhcpserver subnet 1 add option netbios-name-servers 10.10.10.10
-->dhcpserver update
-->dhcpserver subnet 1 list option
options for subnet: LAN
ID | Identifier | Value
----|-----|-----
1 | netbios-name-servers | 10.10.10.10
2 | netbios-node-type | 8
1 | domain-name-servers | 55.55.55.55
-----
```

For details of the above CLI commands, please refer to the *Ethernet Router CLI Manual Section 364-180-C01* manual.

✧ DHCP Relay Agent Mode

If your ISP, or a different server, performs the DHCP server function for your network, then you should configure the router as a DHCP relay agent. When the router receives a request from a computer on your network, it contacts your ISP or the assigned server for the necessary IP information, and then relays the assigned information back to the computer.

1. On the “DHCP Server” page, scroll down to the “DHCP Server Mode” section and select **DHCP Relay Agent**. Then click the **Configure** button. The “DHCP: Enable Relay Agent” page will appear. Enter the IP Address of the DHCP Server you wish to relay to and click the **Apply** button.

The screenshot displays the 'DHCP: enable relay agent' configuration page. On the left is a navigation menu with sections: Status, System, and Configuration. Under Configuration, various options are listed, including 'Ports' which is currently selected. The main content area is titled 'DHCP: enable relay agent' and contains the following information:

DHCP server status:

- Default Lease Time: 43200
- Allow Bootp: true
- Max Lease Time: 86400
- Allow Unknown Clients: true
- Enabled: true
- DHCP Server Address: 192.168.0.1

Subnet definitions:

- Subnet Value: 192.168.0.0
- Subnet Mask: 255.255.0.0
- Max Lease Time: 86400
- Default Lease Time: 43200
- Host Is Dns Server: true
- Host Is Default Gateway: true
- Subnet From Interface: eth0
- IP range: 192.168.0.2 - 192.168.0.21
- Option: domain-name-servers = 0.0.0.0

Below the subnet definitions, there is a section for 'Please enter details for DHCP relay configuration:'. It includes a text input field for 'DHCP server IP address:' with the value '192.168.200.254' entered. At the bottom of the page is an 'Apply' button.

Figure 6-33 Web Tool – DHCP: enable relay agent page

2. The “DHCP Server” page will appear showing the IP Address that DHCP will be relayed to. If you should need to RE-CONFIGURE the DHCP server, you may click the **Configure the DHCP Server** button below the message.

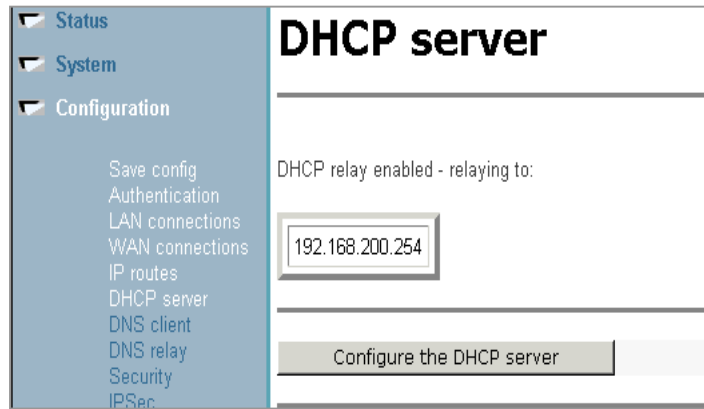


Figure 6-34 Web Tool – DHCP server: DHCP relay enabled page

DNS Client

The DNS Client configuration allows you to specify the Domain Name Server that the router will use for Domain Name resolution.

1. Log-in to your router. From the left frame, click **Configuration** and then **DNS Client**. The “DNS Client” page will appear. Enter your DNS server address into the box in the DNS Servers section and click the **Add** button.

| DNS client | |
|-----------------------------|--------|
| DNS servers: | |
| 200.246.5.87 | Delete |
| 168.95.1.1 | Add |
| Domain search order: | |
| <input type="text"/> | Add |

Figure 6-35 Web Tool – DNS Client page

2. The “DNS Client” page will refresh and show your newly assigned DNS address. You may add another using the procedure from step 1. You may also delete the assigned DNS address at any time by clicking the **Delete** button to the right of the assigned address.

| DNS client | |
|-----------------------------|--------|
| DNS servers: | |
| 168.95.1.1 | Delete |
| 200.246.5.87 | Delete |
| <input type="text"/> | Add |
| Domain search order: | |
| <input type="text"/> | Add |

Figure 6-36 Web Tool – DNS Client page

- 3. Domain search order:** Enter your search order into the box in the Domain search order section and click the **Add** button. The 'DSN Client' page will refresh and show the newly assigned Domain search order. You may make multiple entries in the list by repeating this procedure. You may delete the assigned search order by clicking the **Delete** button to the right of the assigned name. Entering a domain search order will create a list that the DNS client will use to attempt to complete an incomplete domain name. It will append each entry in the search order to the incomplete domain name in an attempt to find a valid domain name.

DNS Relay

DNS Relay forwards packets to request the DNS information from a specified DNS server. It is possible to enter both a primary and secondary DNS server to contact, which is commonly configured. Replies from the DNS are then forwarded back to the originator of the packets that were made for the original request. UDP and TCP traffic are both supported.

NOTE: When using Routed PPP mode, you do not need to configure DNS Relay. It will be automatically configured upon connection to the PPP server.

1. Log-in to your router. From the left frame, click **Configuration** and then **DNS Relay**. The “DNS Relay” page will appear, indicating that the *DNS Relay is disabled*. In the DNS Relay Mode section, choose the *Enabled* button and click the **Configure** button.

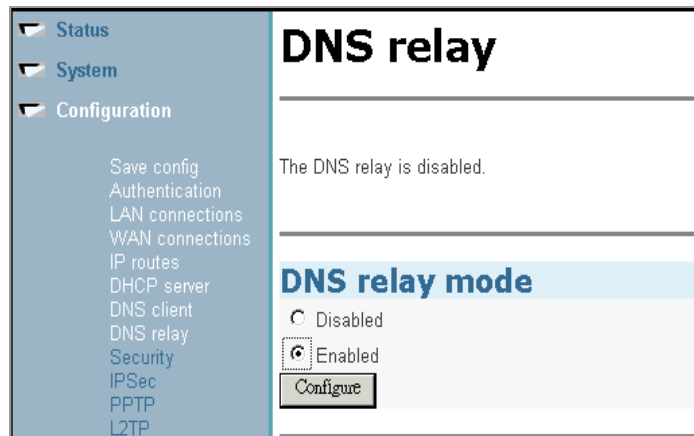


Figure 6-37 Web Tool – DNS relay page

2. The “DNS: Enable Relay” page will appear. In the DNS Relay Settings section, enter the address of your DNS server and click the **Apply** button.

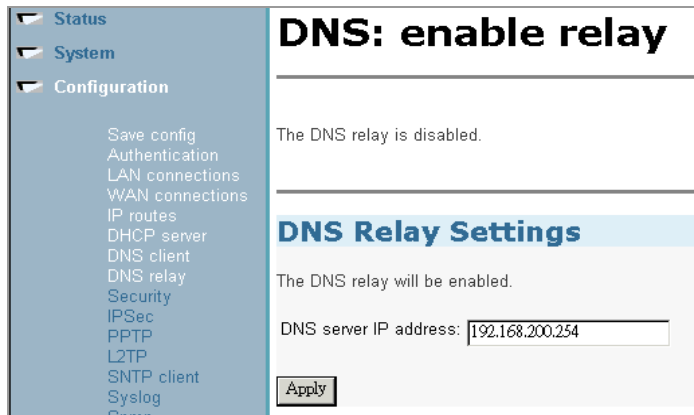


Figure 6-38 Web Tool – DNS: enable relay page

3. The “DNS Relay” page will appear again stating that the relay has been enabled and will show the address the relay is pointing to. If you should need to RE-CONFIGURE the DNS relay, you may click the **Configure the DNS relay** button below the message.

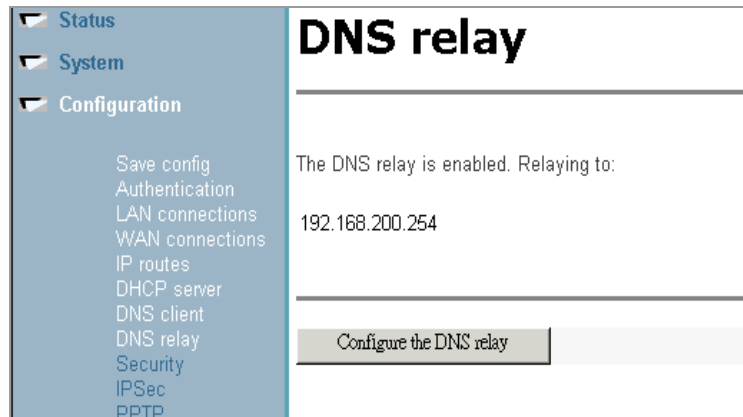


Figure 6-39 Web Tool – DNS relay enabled page

Security

The “Security Interface Configuration” page allows you to set the Firewall Security Level, the NAT configuration, Policies, Triggers and Intrusion Detection. Click **Configuration** from the left frame and then click **Security** link. The following page will be displayed:

Security Interface Configuration

Security State

Security: Enabled

Firewall: Enabled Disabled

Intrusion Detection: Enabled Disabled

Change State

Security Level

Security Level: low Change Level

Security Interfaces

| Name | Type | NAT | |
|---|----------|---|-----------------------|
| eth0 | internal | May be configured on external or DMZ interfaces | Delete Interface... ▶ |
| frame-0 | external | Enable NAT to internal interfaces | Delete Interface... ▶ |
| Advanced NAT Configuration... ▶ (Enable NAT for Advanced Configuration) | | | |

Add Interface... ▶ (all interfaces defined)

Policies, Triggers and Intrusion Detection

Firewall Policy Configuration... ▶

Firewall Trigger Configuration... ▶

Configure Intrusion Detection... ▶

Configure Alerting... ▶

Figure 6-40 Web Tool – Security page

✧ Enabling Security

You must enable Security before you can enable Firewall and/or Intrusion Detection. In the “Security State” section, click on the Security Enabled radio button and then click on **Change State** to update.

✧ Enabling Firewall and/or Intrusion Detection

* Intrusion Detection is for future feature.

You must create a security interface before you can enable Firewall and/or Intrusion Detection. Security interfaces are based on existing LAN services. You must create a LAN service for every security interface that you want to configure (From the “Security Interfaces” section, click on “Add Interface”). If you see any error in the content of the security interfaces table, you must delete the interface first and re-add the interface again. When you add the security interface, the Type setting (internal/external) must follow the default rule (if it is a LAN side interface, the Interface Type should be internal; if it is a WAN side interface, the Interface Type should be external).

After the *Firewall* is enabled, you can set the **Security Level**. In the Security Level section, click the “Security Level” drop-down list. Then click on the level that you want to set. Finally, click on the **Change Level** button.

✧ NAT Configuration

NAT stands for **Network Address Translation**, which is an Internet standard that enables a local-area network to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. NAT, located where the LAN meets the Internet, makes all necessary IP address translations.

1. In the “Security Interfaces” section of the page, you can see the newly created interfaces (see Figure 6-40). To enable NAT, click the **Enable NAT to internal interfaces** button. Then the page will refresh and the button will now read **Disable NAT to internal interfaces**.

| Name | Type | NAT | |
|---------|----------|--|-----------------------|
| eth0 | internal | May be configured on external or DMZ interfaces | Delete Interface... ▶ |
| frame-0 | external | <input type="button" value="Disable NAT to internal interfaces"/> Advanced NAT Configuration... ▶ | Delete Interface... ▶ |

Add Interface... ▶ (all interfaces defined)

Figure 6-41 Web Tool – Security: Security Interfaces page

✧ Global Address Pools

A Global Address Pool is a pool of addresses seen from the outside network. By default, each outside interface creates a Global Address Pool with a single address – the address assigned to that interface. For outbound sessions, an address is picked from a pool by hashing the source IP address for a pool index and then hashing again for an address index. For inbound sessions, it is necessary to create a reserved mapping. See the following subsection “Nat Reserved Mapping”.

NOTE: NAT must be enabled before you can configure global address pools. It is assumed here that you have previously configured NAT.

1. Login to your router. Click **Configuration** and then click **Security** from the left frame. The “Security Configuration” page will appear. In the “Security Interfaces” section, click the **Advanced NAT Configuration** link.

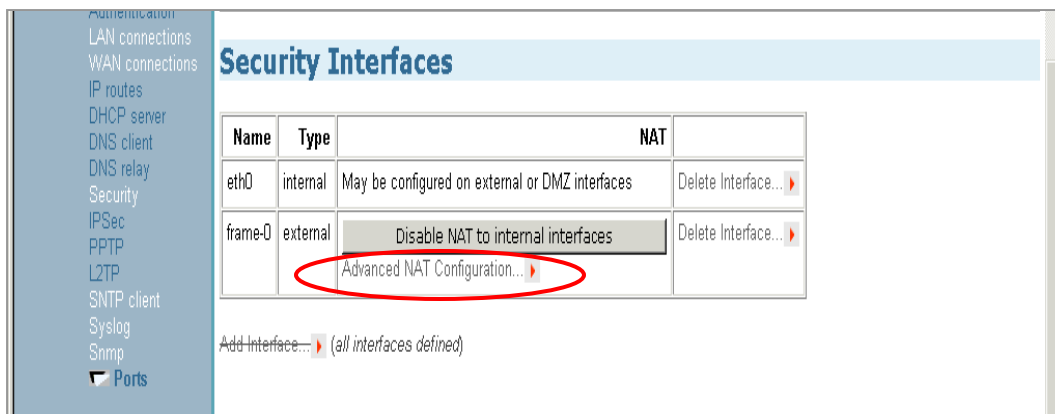


Figure 6-42 Web Tool – Security: Security Interfaces page

- The “Advanced NAT Configuration” page will appear. In the “Global Address Pools” section, click the **Add Global Address Pool** link.

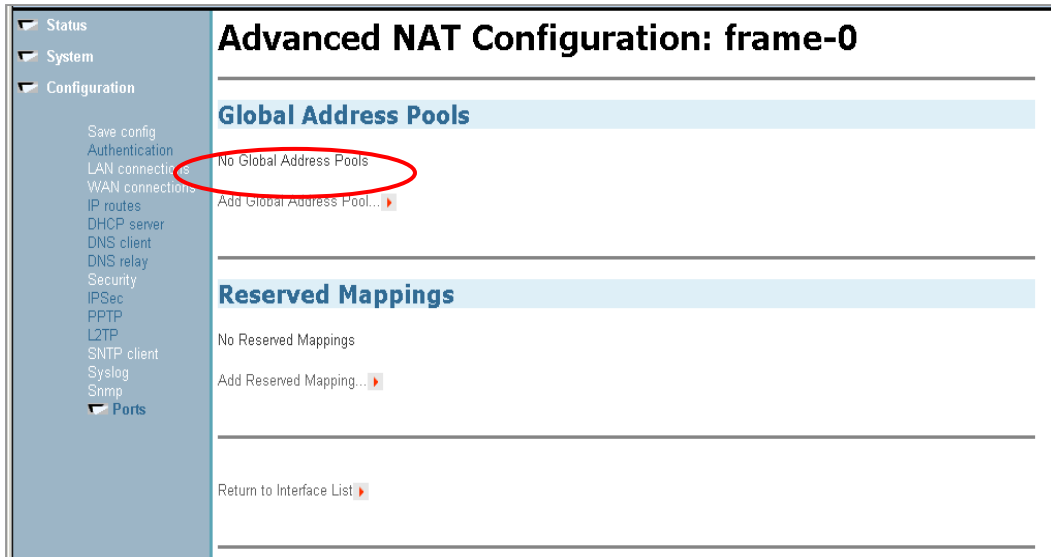


Figure 6-43 Web Tool – Security: Advanced NAT Configuration page

- The “Firewall Add Global Address Pool” page will appear. This page allows you to create a pool of network IP addresses that are visible outside your network. Add values for each of the fields. See the table below for a summary of each field. Click the **Add Global Address Pool** button.

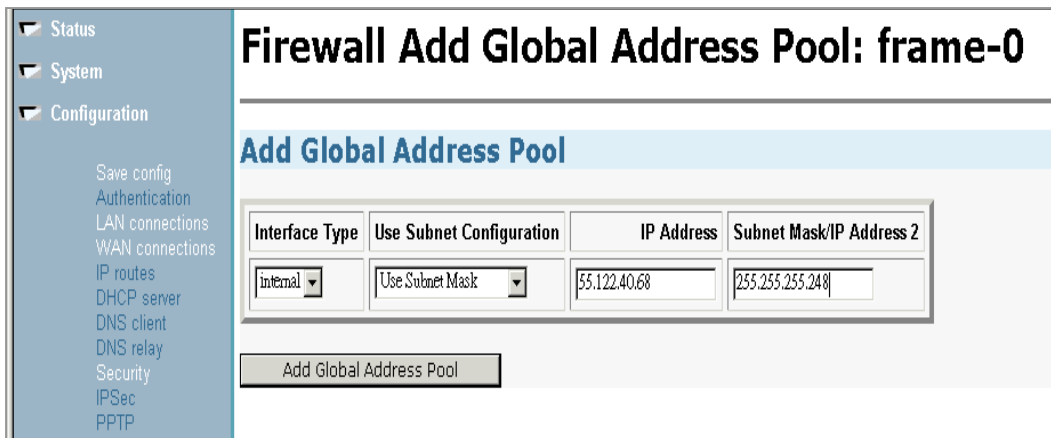


Figure 6-44 Web Tool – Security: Firewall Add Global Address Pool page

GLOBAL ADDRESS POOL FIELDS DEFINED:

Interface type: The internal address type that you want to map your external global IP addresses to. Click on the drop-down list and select an interface type.

Use Subnet Configuration: There are two ways to specify a range of IP addresses. You can either *Use Subnet Mask* (specify the subnet mask address of the IP address) or *Use IP Address Range* (specify the first and last IP address in the range). Click on the drop-down list and select a method.

IP Address: Enter the IP Address that is visible outside the network

Subnet Mask/IP Address 2: The value you specify here depends on the Subnet Configuration that you are using. If you chose *Use Subnet Mask*, type in the subnet mask of the IP address. If you chose *Use IP Address Range*, type in the last IP address in the range of addresses that make up the global address pool.

4. The “Advanced NAT Configuration” page will appear again, showing your newly created Global Address Pool.

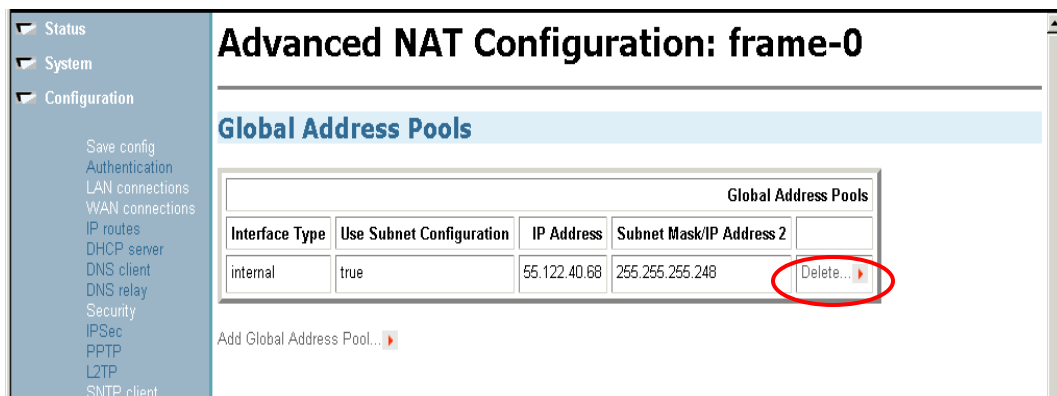


Figure 6-45 Web Tool – Security: Advanced NAT Configuration page

5. To delete a Global Address Pool, click on the **Delete** link on the right side of the Global Address Pool you wish to delete (see Figure 6-45).

6. The “Firewall Delete Global Address Pool” page will appear confirming your deletion. Click the **Delete Global Address Pool** button.

Firewall Delete Global Address Pool: frame-0

Delete Global Address Pool Confirmation

Please confirm deletion of the following Global Address Pool:

| Interface Type | Use Subnet Configuration | IP Address | Subnet Mask/IP Address 2 |
|----------------|--------------------------|--------------|--------------------------|
| internal | true | 55.122.40.68 | 255.255.255.248 |

Figure 6-46 Web Tool – Security: Firewall Delete Global Address Pool page

✧ NAT Reserved Mapping

Reserved mapping is used so that NAT knows where to route packets on inbound sessions. The reserved mapping will map a specific global address and port to an inside address and port. Reserved mappings can also be used so that different inside hosts can share a global address by mapping different ports to different hosts. For example, Host A is an FTP server and Host B is a web server. By mapping the FTP port to Host A and the HTTP port to Host B, both inside hosts can share the same global address. Setting the port number to 65535 for TCP or UDP protocols means that the mapping will apply to all port numbers for that protocol. Reserved mapping allows you to map an outside security interface or an IP address from a global pool to an individual IP address inside the network. Mapping is based on transport type and port number.

NOTE: NAT must be enabled before you can configure reserved mapping. It is assumed that you have previously configured NAT.

1. Login to your router. Click **Configuration** and then click **Security** from the left frame. The “Security Configuration” page will appear. In the “Security Interfaces” section, click the **Advanced NAT Configuration** link.

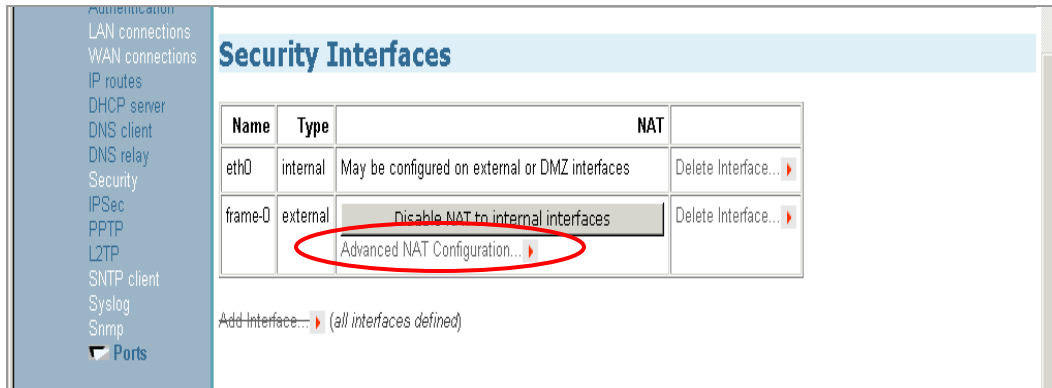


Figure 6-47 Web Tool – Security: Security Interfaces page

2. The “Advanced NAT Configuration” page will appear. Click the **Add Reserved Mapping** link.

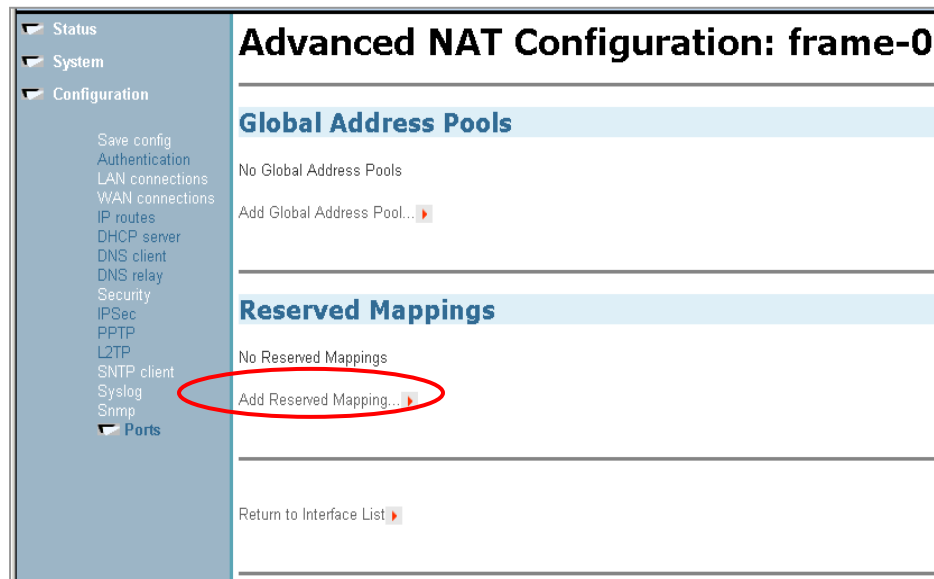


Figure 6-48 Web Tool – Security: Add Reserved Mappings page

3. The “Firewall Add Reserved Mapping” page will appear. You can configure the details of your reserved mapping here. Add specific values in the table and then click the **Add Reserved Mapping** button. The table will refresh and the reserved mapping is added to your NAT

configuration.

| Global IP Address | Internal IP Address | Transport Type | Port Number |
|---|---------------------|----------------|-------------|
| 0.0.0.0 <small>(Set to 0.0.0.0 to use the primary IP address of the interface "frame-0")</small> | 192.168.0.5 | icmp | 21 |

Add Reserved Mapping

[Return to NAT Configuration](#)

[Return to Interface List](#)

Figure 6-49 Web Tool – Security: Firewall Add Reserved Mapping page

NOTE: Setting the port number to 65535 for TCP or UDP protocols means that the mapping will apply to all port numbers for that protocol.

RESERVED MAPPING FIELDS DEFINED:

Global IP Address: If you are mapping from a global IP address, type the address here. If you are mapping from a security interface, type 0.0.0.0.

Internal IP Address: The IP address of an individual host inside your network.

Transport Type: Specify the transport type that you want to map from the outside interface to the inside.

Port Number: The port number that your transport uses.

- The “Advanced NAT Configuration” page will appear showing your newly added reserved mapping. You may click the **Add Reserved Mapping** link to add another mapping if needed.

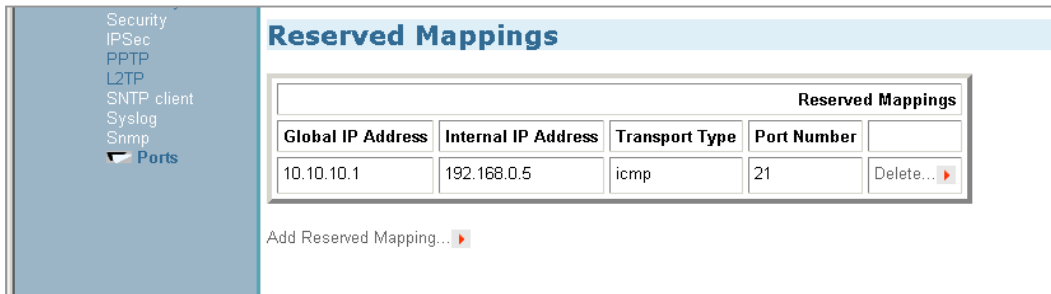


Figure 6-50 Web Tool - Security: Reserved Mappings page

- To delete a Reserved Mappings, click on the **Delete** link on the right side of the Reserved Mappings you want to delete (see Figure 6-50).
- The “Firewall Delete Reserved Mapping” page will appear confirming your deletion. Click the **Delete Reserved Mapping** button.

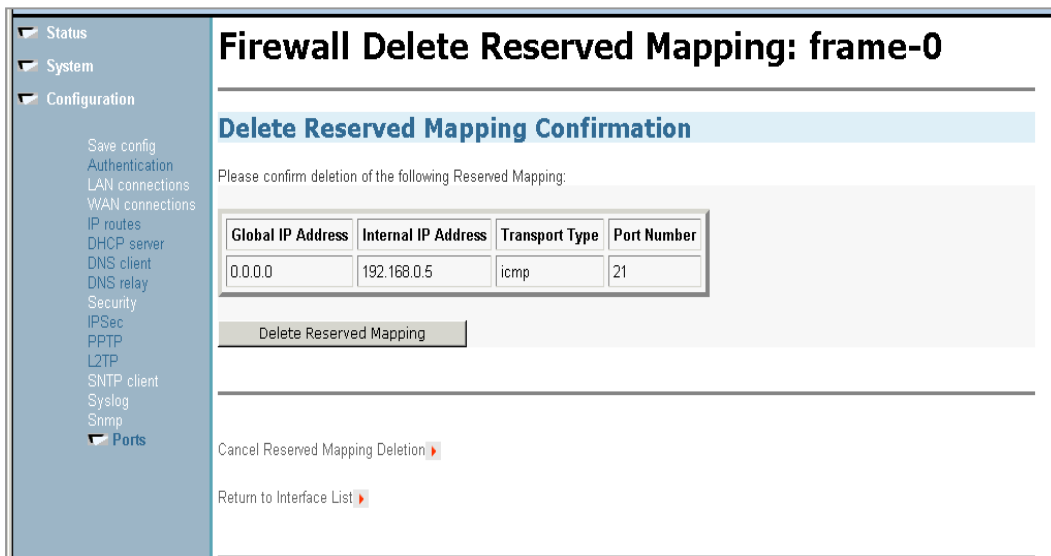


Figure 6-51 Web Tool – Security: Firewall Delete Reserved Mappings page

❖ Configuring Firewall Policy

A policy is the collective term for the rules that apply to incoming and outgoing traffic between two interface types. Before you can create a Firewall policy, you need to enable Firewall.

1. Go to the Polices, Triggers and Intrusion Detection section of the “Security Interface Configuration” page. Click on the “Firewall Policy Configuration” link, The Firewall Policy Configuration page is displayed.

| Interface Type 1 | Interface Type 2 | Validators | Policy Configuration |
|------------------|------------------|---------------------------|----------------------|
| external | internal | Only listed hosts blocked | Port Filters... ▶ |

New Policy... ▶ (All policies defined)

Return to Interface List ▶

Figure 6-52 Web Tool – Security: Firewall Policy Configuration page

2. In the page, you will see the “Current Firewall Policies” table. The table contains details of each Firewall policy. You can now configure the Port Filters.

❖ Configuring Port Filters

A port filter is an individual rule that determines what kind of traffic can pass between two interfaces specified in an existing policy.

1. From the *Current Firewall Policies* table, click on the *Port Filters* link for the policy that you want to configure. The page displayed contains three *Add Filter* hyperlinks that allow you to create three different kinds of port filter. For a TCP port filter click on *Add TCP Filter*. The following page is displayed:

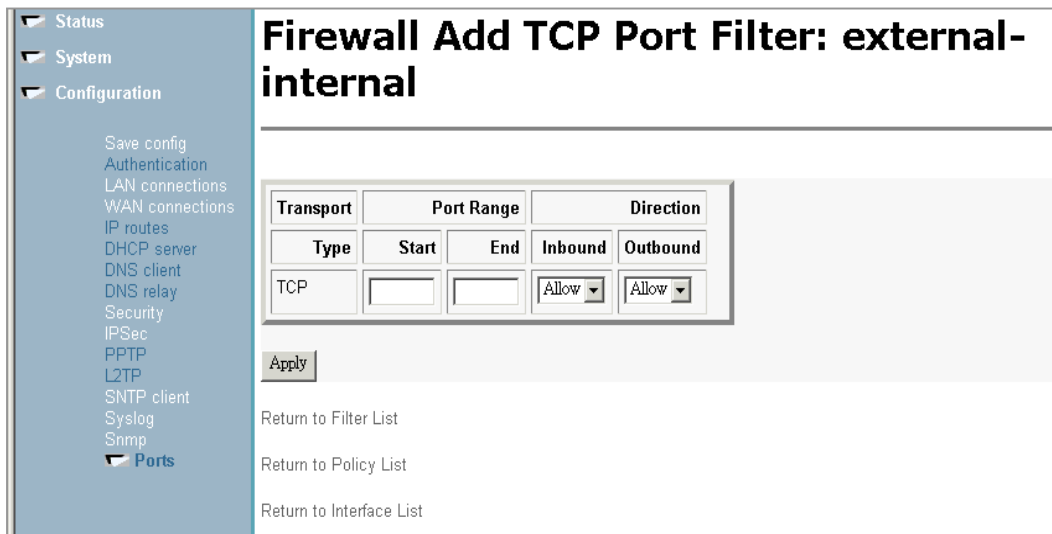


Figure 6-53 Web Tool – Security: Firewall Add TCP Port Filter page

Specify the start and end of the port range for the TCP protocol that you want to filter. Then use the *Direction* drop-down lists to specify whether you want to allow/block inbound traffic, and allow/block outbound traffic. Click on *Apply*. The *Firewall Port Filters* page is displayed, containing details of the TCP portfilter that you have just added.

For a UDP portfilter, click on *Add UDP Filter*. The *Firewall Add UDP Port Filter* page is displayed. For details on how to complete the table, follow the above instructions for adding a TCP portfilter.

For a non-TCP/UDP portfilter, click on *Add Raw IP Filter*. The following page is displayed:

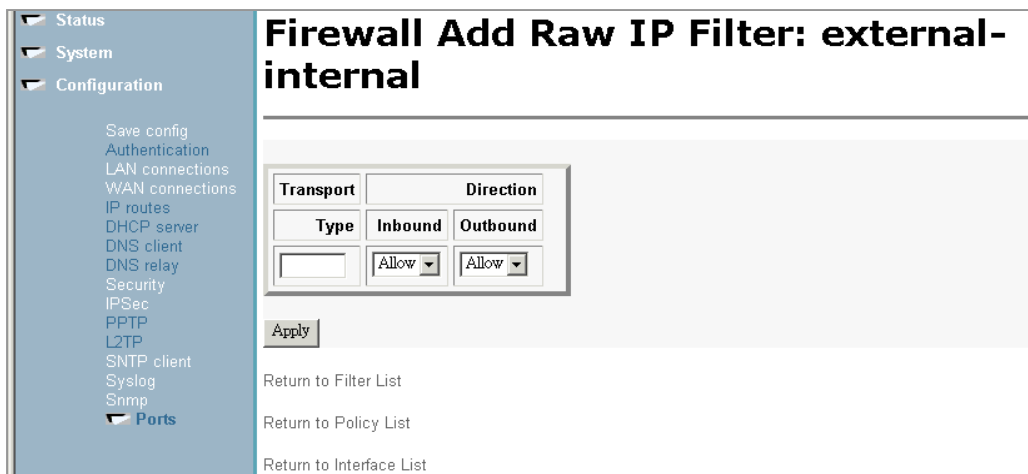


Figure 6-54 Web Tool – Security: Firewall Add Raw IP Filter page

Specify the protocol number in the *Transport Type* text box, for example, for IGMP, enter protocol number 2. For more information on protocol numbers, see <http://www.ietf.org/rfc/rfc1700.txt>. Then use the *Direction* drop-down lists to specify whether you want to allow/block inbound traffic, and allow/block outbound traffic. Click on *Apply*. The *Firewall Port Filters* page is displayed, containing details of the IP portfilter that you have just added.

2. Each portfilter displayed in the *Firewall Port Filters* page has a *Delete* hyperlink assigned to it. To delete a portfilter, click on this link, then at the confirmation page, click on the *Delete* button. The portfilter is removed from the Firewall configuration.

These actions have the same effect as typing the following CLI commands:

```
firewall add portfilter
firewall list portfilters
firewall delete portfilter
```

NOTE: If the firewall is enabled, RIP is by default disabled for the router card. If you want RIP to work when the firewall is enabled, you must add a UDP port filter – Port Range: 520 ~ 520, Inbound/Outbound Allow.

3. Portfilter's default items are different that will be according to the security level.

- **Security Level = low**

--> firewall list portfilters pex_in

Firewall Port Filters:

| ID | Name | Type | Port Range | In | Out | Raw | TCP | UDP |
|----|---------|------|-------------|-------|------|-------|-------|------|
| 1 | ei_rip | 17 | 520 - 520 | true | true | false | false | true |
| 2 | ei_sntp | 17 | 123 - 123 | false | true | false | false | true |
| 3 | ei_l2tp | 17 | 1701 - 1701 | true | true | false | false | true |

| | | | | | | | | | |
|----|------------|----|------|---------|-------|------|-------|-------|-------|
| 4 | ei_pptp | 6 | 1723 | - 1723 | true | true | false | true | false |
| 5 | ei_gre | 47 | 0 | - 0 | true | true | true | false | false |
| 6 | ei_isakmp | 17 | 500 | - 500 | true | true | false | false | true |
| 7 | ei_esp | 50 | 0 | - 0 | true | true | true | false | false |
| 8 | ei_ah | 51 | 0 | - 0 | true | true | true | false | false |
| 9 | lei_ssh | 6 | 22 | - 22 | true | true | false | true | false |
| 10 | lei_tcp_wc | 6 | 0 | - 65535 | false | true | false | true | false |
| 11 | lei_ucp_wc | 17 | 0 | - 65535 | false | true | false | false | true |
| 12 | lei_icmp | 1 | 0 | - 0 | true | true | true | false | false |

- **Security Level = medium**

--> firewall list portfilters pex_in

Firewall Port Filters:

| ID | Name | Type | Port Range | In | Out | Raw | TCP | UDP | |
|----|-------------|------|------------|--------|-------|------|-------|-------|-------|
| 1 | mei_ssh | 6 | 22 | - 22 | true | true | false | true | false |
| 2 | mei_t120 | 6 | 1503 | - 1503 | false | true | false | true | false |
| 3 | mei_h323 | 6 | 1720 | - 1720 | false | true | false | true | false |
| 4 | mei_rav | 17 | 7070 | - 7070 | false | true | false | false | true |
| 5 | mei_nntp | 6 | 119 | - 119 | false | true | false | true | false |
| 6 | mei_webmail | 6 | 5080 | - 5080 | false | true | false | true | false |
| 7 | mei_icq | 6 | 5190 | - 5190 | false | true | false | true | false |
| 8 | mei_msn | 6 | 1863 | - 1863 | false | true | false | true | false |
| 9 | mei_https | 6 | 443 | - 443 | false | true | false | true | false |
| 10 | mei_ils | 6 | 1002 | - 1002 | false | true | false | true | false |
| 11 | mei_ldap | 6 | 389 | - 389 | false | true | false | true | false |
| 12 | mei_imap | 6 | 143 | - 143 | false | true | false | true | false |
| 13 | mei_icmp | 1 | 0 | - 0 | false | true | true | false | false |
| 14 | mei_pop3 | 6 | 110 | - 110 | false | true | false | true | false |
| 15 | mei_smtpt | 6 | 25 | - 25 | false | true | false | true | false |

| | | | | | | | | | |
|----|-----------|----|------|--------|-------|------|-------|-------|-------|
| 16 | mei_tnet | 6 | 23 | - 23 | false | true | false | true | false |
| 17 | mei_ftp | 6 | 21 | - 21 | false | true | false | true | false |
| 18 | mei_tdns | 6 | 53 | - 53 | false | true | false | true | false |
| 19 | mei_dns | 17 | 53 | - 53 | false | true | false | false | true |
| 20 | mei_http | 6 | 80 | - 80 | false | true | false | true | false |
| 21 | ei_ah | 51 | 0 | - 0 | true | true | true | false | false |
| 22 | ei_esp | 50 | 0 | - 0 | true | true | true | false | false |
| 23 | ei_isakmp | 17 | 500 | - 500 | true | true | false | false | true |
| 24 | ei_gre | 47 | 0 | - 0 | true | true | true | false | false |
| 25 | ei_pptp | 6 | 1723 | - 1723 | true | true | false | true | false |
| 26 | ei_l2tp | 17 | 1701 | - 1701 | true | true | false | false | true |
| 27 | ei_snmp | 17 | 123 | - 123 | false | true | false | false | true |

- **Security Level = high**

--> firewall list portfilters pex_in

Firewall Port Filters:

| ID | Name | Type | Port Range | In | Out | Raw | TCP | UDP | |
|----|-------------|------|------------|--------|-------|-------|-------|-------|-------|
| 1 | hei_webmail | 6 | 5080 | - 5080 | false | true | false | true | false |
| 2 | hei_https | 6 | 443 | - 443 | false | true | false | true | false |
| 3 | hei_imap | 6 | 143 | - 143 | false | true | false | true | false |
| 4 | hei_icmp | 1 | 0 | - 0 | false | true | true | false | false |
| 5 | hei_pop3 | 6 | 110 | - 110 | false | true | false | true | false |
| 6 | hei_smtp | 6 | 25 | - 25 | false | true | false | true | false |
| 7 | hei_tnet | 6 | 23 | - 23 | false | true | false | true | false |
| 8 | hei_ftp | 6 | 21 | - 21 | false | true | false | true | false |
| 9 | hei_tdns | 6 | 53 | - 53 | false | true | false | true | false |
| 10 | hei_dns | 17 | 53 | - 53 | false | true | false | false | true |
| 11 | hei_http | 6 | 80 | - 80 | false | true | false | true | false |
| 12 | hei_ssh | 6 | 22 | - 22 | true | false | false | true | false |
| 13 | ei_ah | 51 | 0 | - 0 | true | true | true | false | false |
| 14 | ei_esp | 50 | 0 | - 0 | true | true | true | false | false |

15 | ei_isakmp | 17 | 500 - 500 | true | true | false | false | true
16 | ei_gre | 47 | 0 - 0 | true | true | true | false | false
17 | ei_pptp | 6 | 1723 - 1723 | true | true | false | true | false
18 | ei_l2tp | 17 | 1701 - 1701 | true | true | false | false | true
19 | ei_sntp | 17 | 123 - 123 | false | true | false | false | true

✧ Configuring triggers

A trigger allows an application to open a secondary port in order to transport packets. The most common applications that require secondary ports are FTP and NetMeeting. This section assumes that you have followed the instructions in *Enabling Security*.

To configure a trigger:

1. Go to the *Policies, Triggers and Intrusion Detection* section of the *Security Interface Configuration*. Click on *Firewall Trigger Configuration*. The “Firewall Trigger Configuration” page is displayed. There are no triggers defined at this time. Click on the *New Trigger* link. The following page is displayed:

Figure 6-55 Web Tool – Security: Firewall Add Trigger page

2. Configure the trigger as follows:

Transport Type; select a transport type from the drop-down list, depending on whether you are adding a trigger for a TCP or a UDP application.

Port Number Start; type the start of the trigger port range that the primary session uses.

Port Number End; type the end of the trigger port range that the primary session uses.

Allow Multiple Hosts; select *allow* if you want a secondary session to be initiated to/from different remote hosts. Select *block* if you want a secondary session to be initiated only to/from the same remote host.

Max Activity Interval; type the maximum interval time (in milliseconds) between the uses of secondary port sessions.

Enable Session Chaining; select *Allow* or *Block* depending on whether you want to allow multi-level TCP session chaining.

Enable UDP Session Chaining; select *Allow* or *Block* depending on whether you want to allow

multi-level UDP and TCP session chaining. You must set *Enable Session Chaining* to *Allow* if you want this to work.

Binary Address Replacement; select *Allow* or *Block* depending on whether you want to use binary address replacement on an existing trigger.

Address Translation Type; specify what type of address replacement is set on a trigger. You must set *Binary Address Replacement* to *Allow* if you want this to work.

3. Once you have configured the trigger, click on *Apply*. The *Firewall Trigger Configuration* page is displayed, containing details of the trigger that you have just configured.

4. Each trigger displayed in the *Firewall Trigger Configuration* page has a *Delete* hyperlink assigned to it. To delete a trigger, click on this link, then at the confirmation page, click on the *Delete* button. The *Firewall Trigger Configuration* page is displayed and details of the deleted trigger have been removed. There are two hyperlinks on the page:

a To add a new trigger, click on *New Trigger*.

b To display the *Security Interface Configuration* page, click on *Return to Interface List*.

These actions have the same effect as typing the following CLI commands:

```
security add trigger
```

```
security list triggers
```

```
security set trigger endpoint
```

```
security set trigger startport
```

```
security set trigger multihost
```

```
security set trigger maxactinterval
```

```
security set trigger sessionchaining
```

```
security set trigger security set trigger
```

```
UDPsessionchaining
```

```
security set trigger binaryaddressreplacement
```

```
security set trigger addressreplacement
```

5. Default firewall triggers

Firewall Trigger Configuration

Current Firewall Triggers

| Firewall Triggers | | | | | | | | | |
|-------------------|-------------------|-----------------|----------------------|-----------------------|-------------------------|-----------------------------|----------------------------|--------------------------|--------|
| Transport Type | Port Number Start | 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 | false | 30000 | true | false | true | tcp | Delete |

✧ Configuring Intrusion Detection Settings

Intrusion Detection settings allow you to protect your network from intrusions such as denial of service (DOS) attacks, port scanning and web spoofing. This section assumes that you have followed the instructions in *Enabling Security* and *Enabling Firewall and/or Intrusion Detection*.

To configure Intrusion Detection settings:

1. Go to the *Policies, Triggers and Intrusion Detection* section of the *Security Interface Configuration* page. Click on *Configure Intrusion Detection*. The “Firewall Configure Intrusion Detection” page is displayed:

Figure 6-56 Web Tool – Security: Firewall Configuration Intrusion Detection page

2. Configure Intrusion Detection as follows:

Use Blacklist; select *true* or *false* depending on whether you want external hosts to be blacklisted if the Firewall detects an intrusion from that host. Click on the *Clear Blacklist* button at the bottom of the page to clear blacklisting of an external host. The *Security Interface Configuration* page is displayed.

Use Victim Protection; select *true* or *false* depending on whether you want to protect a victim from an attempted web spoofing attack.

DOS Attack Block Duration; type the length of time (in seconds) that the Firewall blocks suspicious hosts for once a DOS attack attempt has been detected.

Scan Attack Block Duration; type the length of time (in seconds) that the Firewall blocks suspicious hosts for after it has detected scan activity.

Victim Protection Block Duration; type the length of time (in seconds) that the Firewall blocks packets destined for the victim of a spoofing style attack.

Maximum TCP Open Handshaking Count; type in the maximum number of unfinished TCP handshaking sessions (per second) that are allowed by Firewall before a SYN Flood is detected.

Maximum Ping Count; type in the maximum number of pings (per second) that are allowed before the Firewall detects an Echo Storm DOS attack.

Maximum ICMP Count; type in the maximum number of ICMP packets (per second) that are allowed by the Firewall before an ICMP Flood DOS is detected.

3. Once you have configured Intrusion Detection, click on *Apply*. The Intrusion Detection settings are applied to the Firewall, and the *Security Interface Configuration* page is displayed.

These actions have the same effect as typing the following CLI commands:

```
security enable
firewall enable IDS
firewall set IDS blacklist
firewall set IDS victimprotection
firewall set IDS DOSattackblock
firewall set IDS SCANattackblock
firewall set IDS MaxTCPopenhandshake
firewall set IDS MaxPING
firewall set IDS MaxICMP
firewall set IDS blacklist clear
```

✧ Configuring Alerting

Alerting configuration for Intrusion allows you to send email or paging when there's intrusion upon your network. The alerting settings will take effect only when intrusion detection is enabled.

1. Go to the *Policies, Triggers and Intrusion Detection* section of the *Security Interface Configuration* page. Click on *Configure Alerting*. The "Alerting Configuration" page is displayed:

Alerting Configuration for Intrusion

The following settings will take effect only when intrusion detection is enabled:

Email Enabled: false if enabled, open the outbound smtp port (25/tcp) in firewall policy...

Server:

From (Email):

To 1:

Name:

Email:

To 2:

Name:

Email:

Paging Enabled: false if enabled, open the outbound snpp port (444/tcp) in firewall policy...

Server:

You are?:

Receipient 1:

Receipient 2:

[Return to Security Configuration...](#)

Figure 6-57 Web Tool – Security: Alerting Configuration for Intrusion page

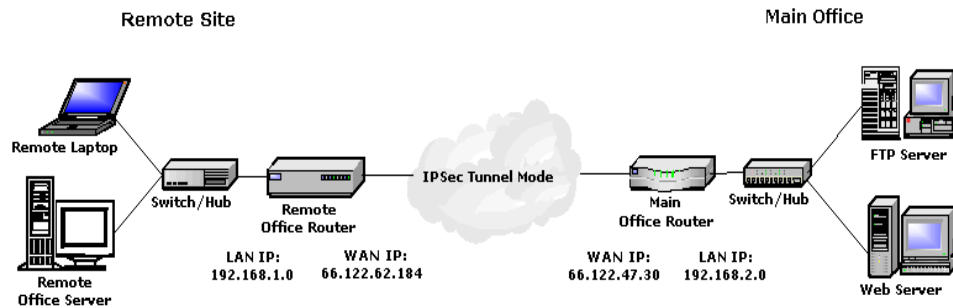
Set Enabled to true if you want to send out email or paging. You have to open the outbound smtp port in the firewall policy if you set Email Enabled to true. You have to open the outbound snpp port in the firewall policy if you set Paging Enabled to true. You can send email to two email

addresses or send paging to two recipients at the same time.

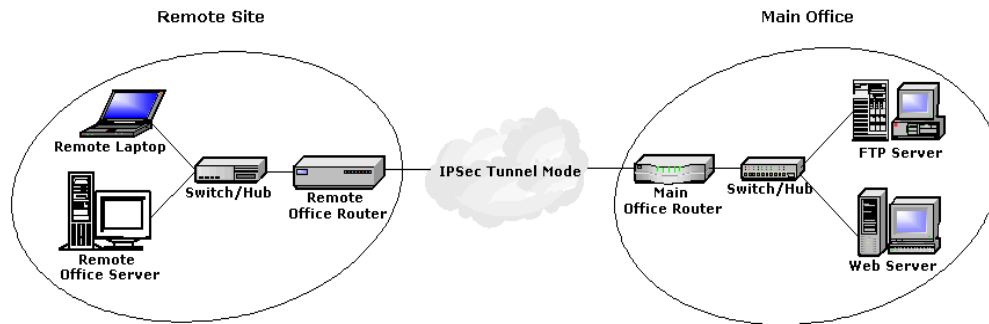
VPN Configuration

Pre-Shared Key

IPSec is defined by the IETF as a standard approach for establishing a secure connection across an IP network.



| IPSec Settings Overview (Example): | |
|---|--|
| LAN/WAN Settings for Branch | Office LAN/WAN Settings for Main Office |
| Negotiation ID: remote@ABCD.com | Negotiation ID: main@ABCD.com |
| Intranet address: 192.168.1.0 | Intranet address: 192.168.2.0 |
| Intranet subnet mask: 255.255.255.0 | Intranet subnet mask: 255.255.255.0 |
| Endpoint ID: main@ABCD.com | Endpoint ID: remote@ABCD.com |
| Termination address: 66.122.47.30 | Termination address: 66.122.62.184 |
| Authentication Method: Pre-shared Key | Authentication Method: Pre-shared Key |
| Tunnel shared key: test | Tunnel shared key: test |
| Tunnel type: Public | Tunnel type: Public |
| IKE life duration: 3600 | IKE life duration: 3600 |
| IKE hash: SHA | IKE hash: SHA |
| IKE encryption: DES | IKE encryption: DES |
| IPSec operation: ESP | IPSec operation: ESP |
| ESP transform: DES | ESP transform: DES |
| ESP AUTH: Null or HMAC_MD5 | ESP AUTH: Null or HMAC_MD5 |



Site to Site VPNs

✧ Site to Site VPNs

Traditionally, connecting two branch offices of the same company required leasing a dedicated private circuit or a frame relay permanent virtual circuit (PVC) between two locations. By using virtual private networking (VPN) to link two offices together, as show above, can offer considerable savings, while offering a competitive alternative to leased lines or PVCs.

✧ Basic Terms and concepts

- **VPN Tunnel:** VPN tunnels are created from site to site pair and secure encrypted connection between two points thru a public or third party network.
- **Encryption:** Is a mathematical operation that transforms data from “clear text” (something that a human or a program can interpret) to “cipher text” (something that cannot be interpreted). Usually the mathematical operation requires that an alphanumeric “key” be supplied along with the clear text. The key and clear text are processed by the encryption operation which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is the mathematical operation that transforms cipher text to clear text. Decryption also requires a key.
- **Authentication:** Before any communication can be called private, each party must know the identity of the other. The same holds true for secure network communication: One network system must make sure that the other network system is the intended correspondent. The process of such identity verification is called authentication.

- **Time to live:** The time to live (TTL) indicates the maximum amount of time this IP packet is allowed to remain in the network. Each router is required to decrement this value as it routes the packet. The packet is dropped if this value reaches 0.
- **Digital Signatures:** Is the electronic analogy to a handwritten signature, and in many ways it is an even stronger device. The key is shared by at least one other party.
- **IKE:** IKE (Internet Key Exchange) is a protocol negotiation and key exchange protocol that is part of the IPSec protocol suite specified by the Internet Engineering Task Force (IETF). IKE allows communicating parties implementing VPNS to automatically negotiate IPSec SAs to facilitate the implementation of VPNs. With IKE, a separate IKE SA is initially created to provide a secure channel for negotiating an IPSec SAs to facilitate the implementation of VPNs.
- **Point-to-Point Protocol (PPP):** Point-to-Point Protocol is the Internet standard for transmission of IP packets over serial lines. It uses a variation of High Level Data Link Control (HDLC) for packet encapsulation.
- **Point-to-Point Tunneling Protocol (PPTP):** A Microsoft-sponsored IETF draft standard for implementing VPNs from the Windows 95/98 operating system to a VPN gateway.
- **Layer 2 Tunneling Protocol (L2TP):** L2TP is refinement of PPTP and Cisco's L2F protocol. L2TP was designed to combine the best features of both PPTP and L2F. L2TP operates, as its name suggests, at Layer 2 in the International Organization for Standardization (ISO) model, and it is a network protocol that creates a tunnel between an L2TP client and an L2TP server, and then encapsulates PPP frames to be sent over tunnel. When using IP as the transport protocol, L2TP can be used as a VPN protocol over the Internet. L2TP has been designed so that it can be used directly over various wide area network (WAN) media (such as Frame Relay) without an IP transport layer, which can extend its usefulness in setting up corporate networks.
- **Private Key:** A digital key code used to decrypt data and verify digital signatures. This key is kept secret, and is known only to its owner.
- **Public key:** A trusted and efficient key and certificate management system.
- **Public key infrastructure:** A trusted and efficient key and certificate management system.
- **Hash algorithm:** When a provider issues a certificate, it is not generally the overall certificate but a cryptographic check sum from the certificate that is signed. The procedure used for calculating the check sum is referred to as a hash algorithm, and the check sum is called the hash value.
- **Security Associations (SA):** An SA defines the kinds of security measures that should be applied to packets based on who is sending the packets, where they are going, and what type of

payload they are carrying.

- **IPSec:** IPSec is a protocol suite defined by the IETF to secure communication at layer 3-the network layer between communicating peers.
- **ESP:** ESP (Encapsulating Security Payload) protocol [RFC2406] can provide confidentiality with authenticity and integrity, or confidentiality only services.
- **Data Encryption Standard (DES):** DES function can be used for both encryption and decryption. DES is the most widely used shared key cryptographic algorithm and is both a U.S. and an international standard.
- **3DES:** An algorithm that uses DES and one, two, or three keys to encrypt/decrypt/encrypt packets of information.
- **Authentication Header (AH):** The Authentication Header is a mechanism for providing strong integrity and authentication for IP packets. Confidentiality and protection from traffic analysis is not provided by the Authentication Header.
- **IP Payload Compression Protocol (IPCOMP):** IP payload compression is a protocol to reduce the size of IP datagrams. IP payload compression is especially useful when encryption is applied to IP datagrams.
- **Phase 1 negotiation:** IKE defines two modes when negotiating a phase 1 SA: **main mode** and **aggressive mode**. There are three negotiating rounds in the IKE phase 1 main mode exchange. In the first round, one ISAKMP entity (the initiator) sends multiple SA proposals to another entity (the responder). The responder chooses one proposal and sends it back to the initiator. In the second round, two peers exchange their key exchange parameters and random use once values called nonces. In the third round, all the exchanged information is authenticated through one of the three authentication mechanisms: shared secret, digital signature, or public key encryption. When shared secret mechanism is employed, the two peers use a secret key derived from a shared secret to create the keyed hash. The keyed hash is then exchanged between two peers and serves as the authenticator. With the second alternative digital signature the authentication between the initiator and the responder is carried out using the digital signature of the negotiation entities. Two peers exchange digitally signed hashes of their identities, public key values, and SA proposals. The third alternative is public key encryption. Here, the two peers exchange the public key encrypted value of their IDs and nonce's, as well as a keyed hash value.
- **Phase 2 Negotiation:** During phase 2, security associations are negotiated on behalf of services such as IPSec or any other service that needs keying material or parameter negotiation. Because a secure channel has already been established in phase 1, the negotiation can be performed more

quickly: thus, it is referred to as quick mode. The identity of the IKE peers has already been verified in phase 1, and the ISAKMP SA already protects exchanges between the IKE peers. Therefore, the identities passed in quick mode are not the identities of the IKE peers but rather the identities of the selectors to be used in the IPsec security policy database. A phase 1 ISAKMP SA is required when negotiating a phase 2 SA. Once established, a phase 2 SA can exist independently of the phase 1 SA that is later destroyed.

- **PKCS #10:** Certificate Request Syntax Standard
- **PKCS #7:** Cryptographic Message Syntax Standard
- **PKCS #11:** Cryptographic Token Interface Standard

✧ IPsec Configuration

1. Log in to your router. From the left frame, click **Configuration** and then click the **IPsec** link. Set your Negotiation ID.

IKE defines two modes when negotiating a phase 1 SA: main mode and aggressive mode.

- For Aggressive Mode use a string like remote@ABCD.com
- or
- For Main Mode use the WAN IP address of your Branch Office (remote) VPN router (our example shows a setup in Aggressive Mode)

IPsec Configuration

Gateway settings
Please specify the IKE negotiation ID for this ipsec gateway to use.

Negotiation ID

Please specify the subnet that this ipsec gateway is protecting.

IP address/Subnet mask

Endpoint Configuration

| Endpoint ID | Termination IP | Target Host | Status | Sent/Received | Actions |
|--|----------------|-------------|--------|---------------|---------|
| Add Endpoint... <input type="button" value="▶"/> | | | | | |

Certificate Configuration

Certificate Authorities

| Name | Actions |
|------|---------|
| | |

Figure 6-58 Web Tool – IPSec Configuration page

2. Next enter the Intranet address. The Intranet address will tell the remote gateway the IP address of the network the local gateway is protecting.
3. Now enter the Intranet subnet mask. The Intranet subnet mask will specify the size of the network it is protecting. A setting of 255.255.255.0 will indicate a Class C network. In our example, we use the Intranet address 192.168.1.0 and a subnet mask of 255.255.255.0.
4. After you enter the Gateway settings, be sure to click the **Change** button.
5. Now, click the “Add Endpoint” link in the “Endpoint Configuration” section. A “Create New IPSec Endpoint” page will appear. Fill out all the required fields. The list below provides details about each field.

- ▼ Status
- ▼ System
- ▼ Configuration
 - Save config
 - Authentication
 - LAN connections
 - WAN connections
 - IP routes
 - DHCP server
 - DNS client
 - DNS relay
 - Security
 - IPSec
 - PPTP
 - L2TP
 - SNTP client
 - Save config
 - Authentication
 - LAN connections
 - WAN connections
 - IP routes
 - DHCP server
 - DNS client
 - DNS relay
 - Security
 - IPSec
 - PPTP
 - L2TP
 - SNTP client
 - Syslog
 - Snmp
 - ▼ Ports

Create New IPSec Endpoint

| | |
|-----------------------------------|--|
| Endpoint ID | <input type="text"/> |
| Termination IP address | <input type="text"/> |
| termination-ip | <input type="text"/> |
| IKE: | |
| authentication method | <input type="text" value="Pre-shared Key"/> |
| pre-shared key | <input type="text"/> |
| encryption algorithm | <input type="text" value="3des"/> |
| hash algorithm | <input type="text" value="sha1"/> |
| SA lifetime (seconds) | <input type="text" value="3600"/> |
| IPSec: | |
| protocol | <input type="text" value="esp"/> |
| ESP transform | <input type="text" value="3des"/> |
| ESP auth | <input type="text" value="sha1"/> |
| AH transform | <input type="text" value="null"/> |
| IPCOMP transform | <input type="text" value="null"/> |
| tunnel type | <input type="text" value="public"/> |
| Target host: | |
| ip range? | <input type="text" value="Subnet"/> |
| ip 1 (ip address / ip address 1) | <input type="text" value="192.168.2.0"/> |
| ip 2 (subnet mask / ip address 2) | <input type="text" value="255.255.255.255"/> |
| | <input type="button" value="Add Endpoint"/> |

Cancel & Return to IPSec Configuration...

Figure 6-59 Web Tool – IPSec: Create New IPSec Endpoint page

- **Endpoint ID:** This must correspond with the remote gateway's Negotiation ID. For instance, the Branch office, with a Negotiation ID of `remote@ABCD.com`, will use a Endpoint ID of `main@ABCD.com` (which is the Negotiation ID of the Main office). Or, in Main Mode, the Endpoint ID will be the WAN IP address of the Main Office VPN Router (in our example, 66.122.47.30).

- **Termination IP address:** the IP address of the external interface of the VPN router.

- **IKE:**

| | |
|------------------------------|--|
| authentication method | Select Pre-shared Key |
| pre-shared key | Both gateways must use the same value. |
| encryption algorithm | The options include: 3des, des, blowfish |
| hash algorithm | The options include: md5, shal |

- **SA lifetime (seconds):** Specifies the time-to-live for the overall security association. When the SA expires, all keys negotiated under the association (AH or ESP) must be renegotiated regardless of the time-to-live remaining for the keys. It is specified as the maximum number of seconds the SA can be used. The default value is 3600.

- **IPSec:**

| | |
|----------------------|--|
| protocol | The options include: ah, esp, ipcomp, ah-esp, ah-ipcomp, esp-ipcomp. |
| ESP transform | The options include: 3des, des, blowfish, ro4, esp-null, null. |
| ESP auth | The options include: md5, shal, des-mac, |

| | |
|-------------------------|---|
| | null. |
| AH transform | The options include: md5, shal, des-mac, null. |
| IPCOMP transform | The options include: lzs, null. |
| tunnel type | The options include: public, private. Public uses the ESP protocol only. Private provides UDP encapsulation for NAT traversal. We are using ports 2787 (ESP), 2788 (AH), and 2845 (IPCOMP). Public should be used for initial testing. |

- **Target host:** Destination of decrypted traffic

| | |
|---|--|
| ip range? | The options include: Subnet, IP Range |
| ip 1(ip address / ip address 1) | The IP address of the target host / The Start IP address of the target host IP range |
| ip 2(subnet mask / ip address 2) | The subnet mask of the target host / The End IP address of the target host IP range |

Note: IKE life duration (SA lifetime)/IKE Hash/IKE Encryption/IPSec Operation (protocol)/ESP transform/ESP auth: When negotiating ABCD VPN IPSec to ABCD VPN IPSec, it is not critical to match up these settings on both servers. The routers have the ability to respond to and initiator's negotiation and handle it accordingly, without detecting a mismatch in policy and rejecting the negotiation. If desired, you may enter the settings shown in our example.

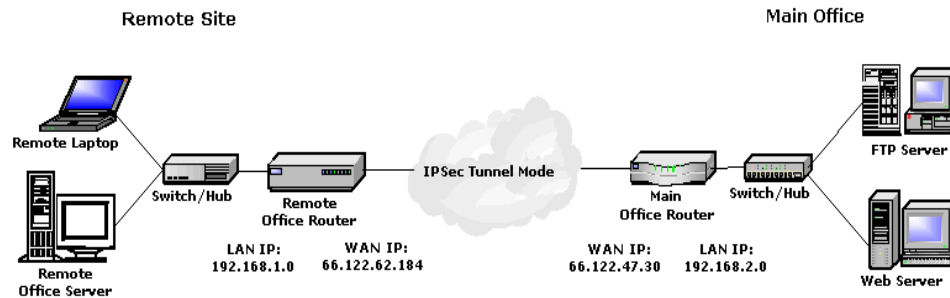
6. When you have finished the settings, scroll to the bottom of the page and click the **Add Endpoint** button. A window will pop up indicating a successful save.

NOTE: You must configure the Main Office VPN Router (main@ABCD.com) as we have configured the Branch Office VPN Router (remote@ABCD.com) above. Once you have configured both sides of the connection, you can test the tunnel using PING. To verify that your tunnel is working, ping the IP address of a computer on the remote network. If you ping the main network, it will only trigger phase 1 and 2 negotiations. You will only receive a reply if you ping an actual IP address on the network, such as the router WAN IP address. You can use Microsoft HyperTerminal to view phase 1 and 2 negotiations.

✧ Digital Signature VPN Configuration

IPSec is defined by the IETF as a standard approach for establishing a secure connection across an IP network. Your router supports all three types of IPSec protocols: AH, ESP, and IPCOMP.

PKCS10 is a Certificate Request Syntax Standard that uses a Digital Signature.



IPSec PKCS10 Settings Overview (Example):

LAN/WAN Settings for Branch Office

Negotiation ID: remote@ABCD.com
 Intranet address: 192.168.1.0
 Intranet subnet mask: 255.255.255.0
 Termination address: 66.122.47.30
 Authentication Method: Digital Signature
 Tunnel shared key: yourvalue

LAN/WAN Settings for Main Office

Negotiation ID: main@ABCD.com
 Intranet address: 192.168.2.0
 Intranet subnet mask: 255.255.255.0
 Termination address: 66.122.62.184
 Authentication Method: Digital Signature
 Tunnel shared key: yourvalue

NOTE: The Digital Signature configuration can only be accessible through the Web Configuration Tool. Before beginning your configuration, it is recommended that you make a serial connection to your router using an RS-232 cable and terminal emulation software, such as Microsoft HyperTerminal. By accessing the router this way, you can verify the actions of the router and web configuration tool.

1. Log in to your Web Configuration tool. From the left frame, click **Configuration** and then click the **IPSec** link. The “IPSec Configuration” page will appear. In the “User Certificates” section, click **Generate New User Certificate** link.

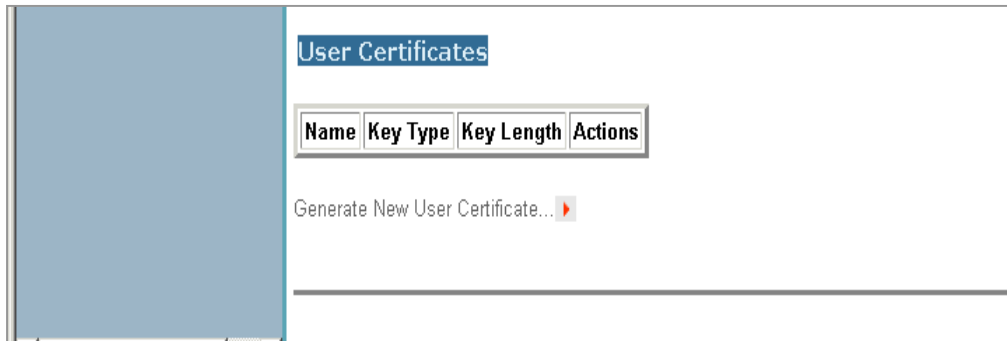


Figure 6-60 Web Tool – IPSec: User Certificates page

2. The page will appear as follows. Fill in the “Common Name” field with any name you would like (in the example, we use “atmosgw”). Remember this, as you will need to enter it again later in the configuration.

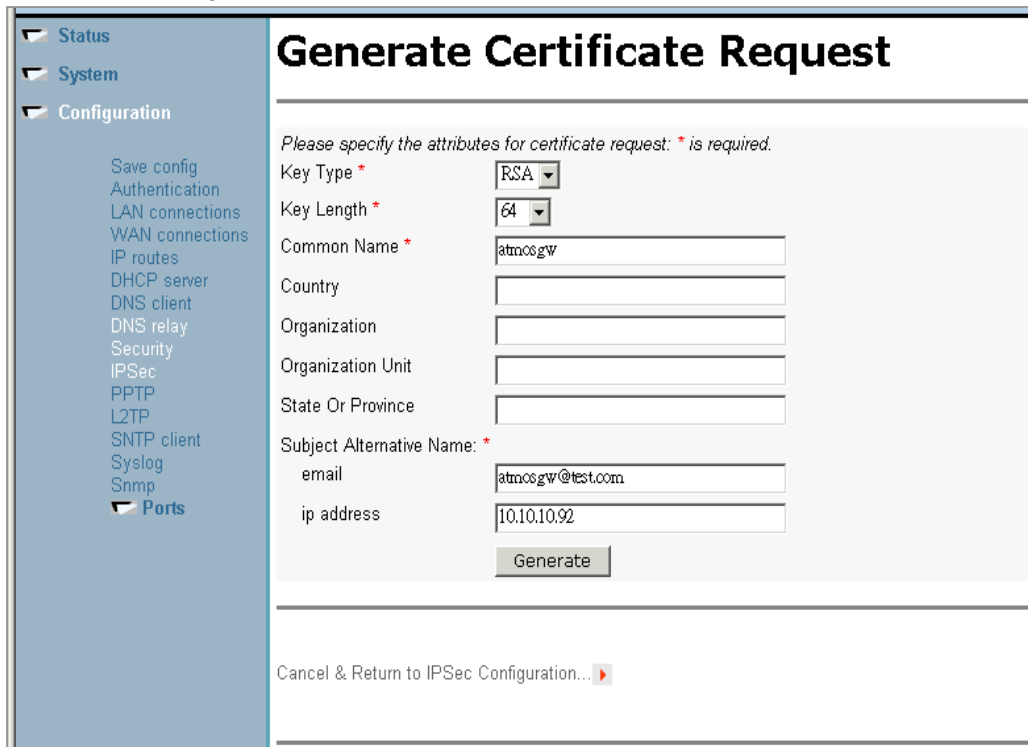


Figure 6-61 Web Tool – IPSec: Generate Certificate Request page

3. From the “Key Type” drop-down menu, choose *RSA* and then from the “Key Length” drop-down menu, select the key length.
4. All remaining fields are optional except for the Subject Alternative Name. Enter the Subject Alternative Name with both an email address and your router’s WAN port IP address.

NOTE: Entering both an IP address and an email address into the Subject Alternative Name field will give you the flexibility for negotiating both Main Mode and Aggressive Mode successfully with certificates. What you enter into the Subject Alternative Name field in the PKCS10 request will be checked against the ID sent for phase 1 Negotiation ID. If the Subject Alternative Name field is left blank when creating this PKCS10 request, negotiations will fail with the remote peer because the ID actually being sent is the Negotiation ID, which does not match the blank ID inside the certificate.

5. Now click the **Generate** button at the bottom of the page. This will send the attributes to the router, which will generate the private key pair and send a user certificate back to the Management Interface in the form of a PKCS10 request. The user certificate will appear. Select all the text shown and copy it.
6. You now need to access a Certificate Authority server of your choice. You can use <http://isakmptest.ssh.fi/cgi-bin/nph-real-cert/cert.pem>, as we do in the example. In a new browser window, enter the URL of your desired server or the one listed above. Paste the user certificate text that you copied in step 5 into the box on the CA server and follow the steps to reach a final certificate. Copy the text of the final certificate.
7. Back in the Web Configuration tool, in the folder list, click the **Certificate Information** link. If not already showing, click the **User Certificate** tab at the top of the window. Click the

- Replace** button. The “Import Certificate” window will pop up. Enter the Common Name, as you entered it in step 2 (it was “atmosgw” in the example). Then paste the text of the final certificate (from step 6) into the text box and click **OK**.
- Back in your browser window that you used to go to the CA server in step 6, enter `http://isakmptest.ssh.fi/certs/ca1.pem` in the address bar and hit enter. This will give you the Root CA in pem format. From the Edit menu in the browser, choose select all. The text will then be highlighted and then, again from the Edit menu, choose Copy.
 - Now switch back to the router’s Web Configuration window. Click the **Add Certificate Authority** link in the “Certificate Authorities” section of the “IPSec Configuration” main page. Paste the Root CA, that you copied in step 8, into the window. Enter “atmosgw” as the common name. Then from the bottom of the page, click the **Add CA Certificate** button.

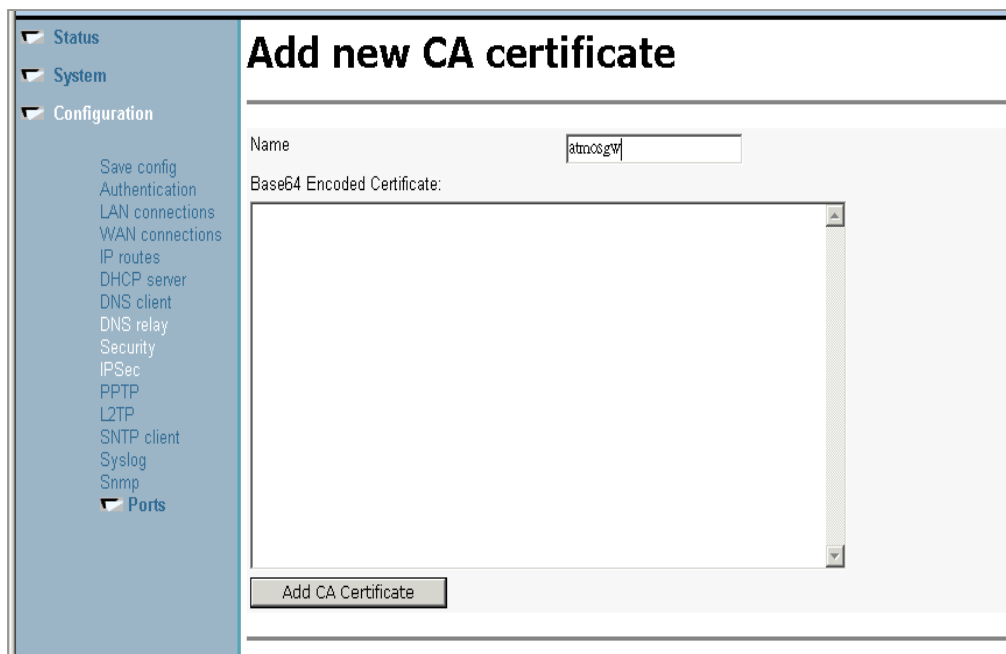


Figure 6-62 Web Tool – IPSec: Add new CA certificate page

NOTE: The CA Certificate for the Main office VPN router must also use “atmosgw” as the common name.

NOTE: If you have HyperTerminal running to confirm your changes, switch to HyperTerminal to verify the save to flashfs.

10. Now, on the top of the “IPSec Configuration” page, enter your Negotiation ID (You must enter what you entered as Subject Alternative Name in Step 4). Also enter your Intranet address and Intranet subnet mask.
11. Next, click the “Add Endpoint” link in the “Endpoint Configuration” section. A page will appear. Enter your Endpoint ID, termination IP address, and choose *Digital Signature* as your “Authentication Method”.

Once you have configured both sides of the connection, you can test the tunnel using PING. To verify that your tunnel is working, ping the IP address of a computer on the remote network. If you ping the main network, it will only trigger phase 1 and 2 negotiations. You will only receive a reply if you ping an actual IP address on the network, such as the router WAN IP address. You can use Microsoft HyperTerminal to view phase 1 and 2 negotiations.

❖ PPTP and L2TP Configuration

1. Log in to your router. From the left frame, click **Configuration** and then click the **PPTP or L2TP** link, depending on your needs. In the *PPTP or L2TP Configuration* page, set the starting and ending IP address of the pptp/l2tp ip pool in the IP Pool section.

PPTP Configuration

IP Pool
Please specify the starting and ending address of the pptp ip pool.

Starting IP Address

Ending IP Address

User Authentication

[Set up users ...](#)

Connected clients

Figure 6-63 Web Tool – PPTP Configuration page

2. From the User Authentication section, click the **Set up users** link. The “Authentication” page will appear. Click the **Create a new user** link, then the “Authentication: Create User” page will appear. .

Authentication: create user

Details for new user

Username:

Password:

GUI user?

Dial-in user?

Comment:

Access Level:

[Cancel and return to Authentication Setup Page...](#)

Figure 6-64 Web Tool – PPTP: Authentication: create user page

3. Enter a new user name and password. Select *true* for the “Dial-in user?” field and then select your access level. The access level determines what a user can do in the configuration (please refer to Table 6-2).
4. Click the **Create** button and then from the left frame, in the Configuration menu, click **Save config** to save the configuration.

✧ **Configuring PPTP or L2TP Client-Initiated Tunneling with VPN Concentrator**

The following configuration is only suitable for the Windows 2000 Client.

1. From the Windows Start Menu, select Settings, then Control Panel, then Network and Dial-Up Connections, and then Make New Connection.
2. The “Network Connection Wizard” will appear. Click **Next**.
3. Select *Connect to a private network through the Internet* and click **Next**.
4. Select *Automatically Dial this Initial Connection* and then select *Virtual Private Connection* from the drop-down menu. Click **Next**.
5. Enter the Destination IP Address (LAN IP address of the main office router) and click **Next**.
6. Select *Add only myself* and then click **Next**.
7. Enter a user name and password for your new connection and then click **Properties**.
8. The “Virtual Private Connection” window will appear. In the *General* tab, enter the IP address of your destination.
9. Select the *Networking* Tab. Choose your desired type of VPN server from the drop-down menu. Then select the *Internet Protocol (TCP/IP)* component by clicking on it, then click the **Properties** button. Be sure that TCP/IP is configured to *Obtain an IP address automatically* and then click the **Advanced** tab. Check the “Use default gateway on remote network” and click **OK**.

NOTE: For L2TP on Windows 2000 computers, you must disable IPSec by modifying the registry. Be sure to take adequate precautions, such as backing up the registry, prior to modifications. You should also refer to the Microsoft website for the correct procedure for modifying the registry. Please refer to Microsoft articles Q258261 - Disabling IPSec Policy Used with L2TP and Q240262- How to Configure a L2TP/IPSec Connection Using a Pre-shared Key.

10. You will be back at the “Connect Virtual Private Connection” window. Click **Connect** to make your connection.

WARNING: If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. It is not guaranteed that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

To add the ProhibitIPSec registry value to your Windows 2000 system, use the application Regedit32.exe to locate the following key in the registry:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters

Add the following registry value to this key:

Value name: ProhibitIPSec

Data Type: REG_DWORD

Value: 1

You must reboot your computer for the changes to take effect.

SNTP client

This section describes the SNTP (Simple Network Time Protocol) client configuration.

1. Login to your router. Click **Configuration** from the left frame, and then click the **SNTP client** link. The “SNTP client” page will appear.

Figure 6-65 Web Tool – SNTP client page

2. In the ‘SNTP Client Mode Configuration Parameters’ section, set the SNTP Synchronization mode. Enable the mode you want and click the **Set Mode** button to set.

Figure 6-66 Web Tool – SNTP client: SNTP Synchronization Mode page

There are three modes to choose from, and each mode has enable and disable options:

- **Unicast** mode

- *Enable* - the mode uses a unicast server and the IP address or hostname in the SNTP server association list is used to synchronize the client time with the server. The SNTP client attempts to contact the specific server in the association in order to receive a timestamp when the *sntpclient sync* command is issued.
- *Disable* - the unicast server is removed from the association list.

- **Broadcast** mode

- *Enable* - allows the SNTP client to accept time synchronization broadcast packets from an SNTP server located on the network, and updated the local system time accordingly.
- *Disable* - stops synchronization via broadcast mode

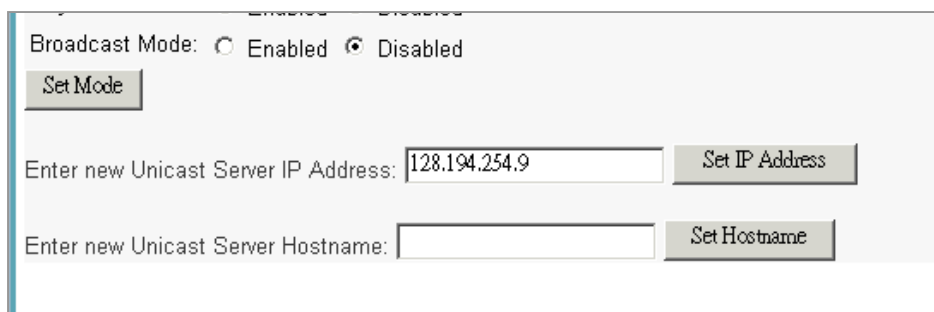
- **Anycast** mode

- *Enable* - the SNTP client sends time synchronized broadcast packets to the network and subsequently expects a reply from a valid timeserver. The client then uses the first reply it receives to establish a link for future sync operations in unicast mode. This server will then be added to the server association list. The client ignores any later replies from servers after the first one is received.

The enabled anycast mode takes precedence over any entries currently in the associations list when the *sntpclient sync* command is issued. The entry will then be substituted for any existing entry in the unicast association list.

- *Disable* - stops synchronization via anycast mode.

If you choose the Unicast mode, you must set the dedicated unicast server for which the SNTP client can synchronize its time. You can set the server either by specifying the IP address or the hostname.

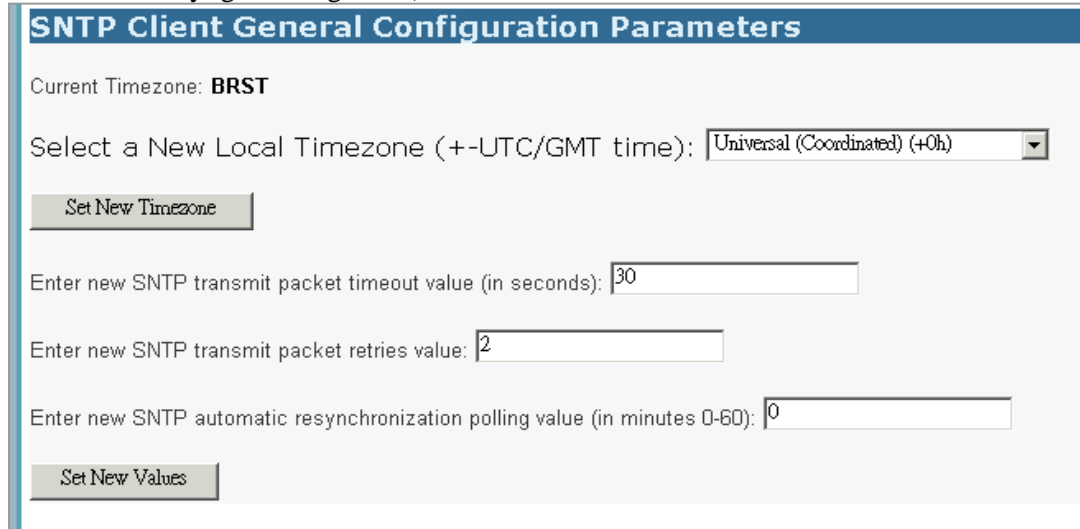


The screenshot shows a configuration window with the following elements:

- Broadcast Mode:** Radio buttons for Enabled and Disabled.
- Set Mode:** A button to apply the selected broadcast mode.
- Unicast Server IP Address:** A text input field containing "128.194.254.9" and a **Set IP Address** button.
- Unicast Server Hostname:** An empty text input field and a **Set Hostname** button.

Figure 6-67 Web Tool – SNTP client: Enter Unicast Server IP Address page

3. In the 'SNTP Client General Configuration Parameters' section, set the Timezone. Sixty-four of the world's most prominent time zones are represented (including those using standard time and summer/daylight savings time).



The screenshot shows a web tool interface titled "SNTP Client General Configuration Parameters". The current timezone is set to "BRST". Below this, there is a dropdown menu for "Select a New Local Timezone (+-UTC/GMT time)" currently showing "Universal (Coordinated) (+0h)". There are three input fields: "Enter new SNTP transmit packet timeout value (in seconds)" with the value "30", "Enter new SNTP transmit packet retries value" with the value "2", and "Enter new SNTP automatic resynchronization polling value (in minutes 0-60)" with the value "0". There are two buttons: "Set New Timezone" and "Set New Values".

Figure 6-68 Web Tool – SNTP client: SNTP Client General Configuration Parameters page

4. Next, in the 'SNTP Client General Configuration Parameters' section (see the figure in previous step), set the:

transmit packet response timeout value (in seconds): sets the received packet response timeout value (in seconds) upon sync request initiation. After timeout, if the transmit packet retries value is set, an attempt will be retried.

transmit packet retries value: sets the number of packet retry attempts when no response is received from a timeserver. The SNTP client will send another packet for synchronization after a timeout.

automatic resynchronization polling value (in minutes 0-60): sets the SNTP client to automatically send a time synchronization request (specific to the mode) to the network at a specific interval. If the poll-interval is set to 0, the polling mechanism will be disabled.

5. In the 'ISOS Clock Setting' section, sets the router card system clock to a specific time and date. This command can be used as an alternative to synchronizing the local system clock via internal or external timeservers.

Figure 6-69 Web Tool – SNMP client: ISOS Clock Setting page

Syslog

1. Login to your router. Click **Configuration** from the left frame, and then click the **Syslog** link. The “Syslog Client Configuration” page will appear.

Figure 6-70 Web Tool – Syslog Client Configuration page

2. Choose your level of severity from the drop-down menu in the Severity Threshold section (See the table below for more information on each severity level). Then set the host name in the Host Name section. Finally enter the IP address of the receiver in the Receiver section and click the **Change** button to enter your settings. The device will now deliver all log files of

corresponding severity to the syslog server.

There are 7 levels of severity. Any messages equal to or of a higher level of severity than what you have selected will be sent to the syslog server. Below is a brief description of each severity level.

Table 6-3 Syslog severity levels

| Severity Level | Description |
|----------------|----------------------------------|
| Emergency | System is unusable |
| Alert | Action must be taken immediately |
| Critical | Critical conditions |
| Error | Error conditions |
| Warning | Warning conditions |
| Notice | Normal but significant condition |
| Informational | Informational messages |

NOTE: You must have a Syslog Client running on the Receiver computer to listen for and log all incoming syslog files. There are many freeware clients available, such as 3CSyslog from 3Com.

SNMP

The Snmp page allows you to do the configuration of SNMP management.

1. Login to your router, click the **Snmp** from the left frame. Then the page will appear as follows.

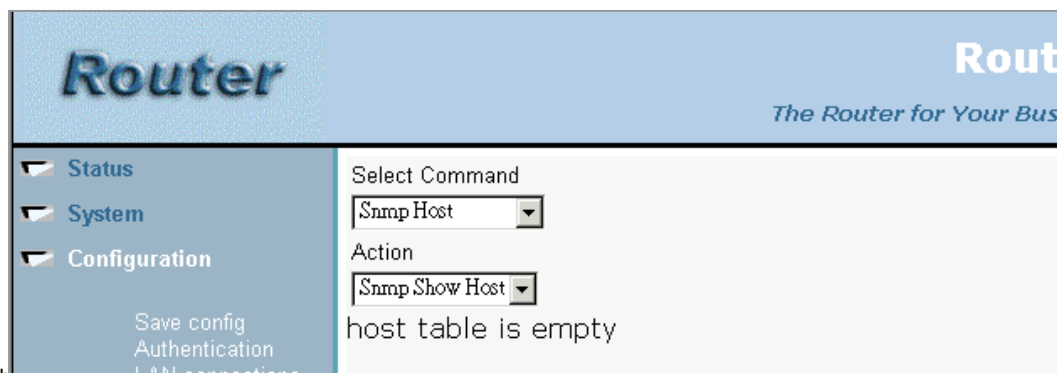


Figure 6-71 Web Tool – Snmp page

- In the **Select Command** field, you can select **Snmp Host**, **Snmp Community**, or **Snmp Trap** to configure. Under each command, you can select “Show”, “Add”, and “Delete” three different actions as the following figure shows.

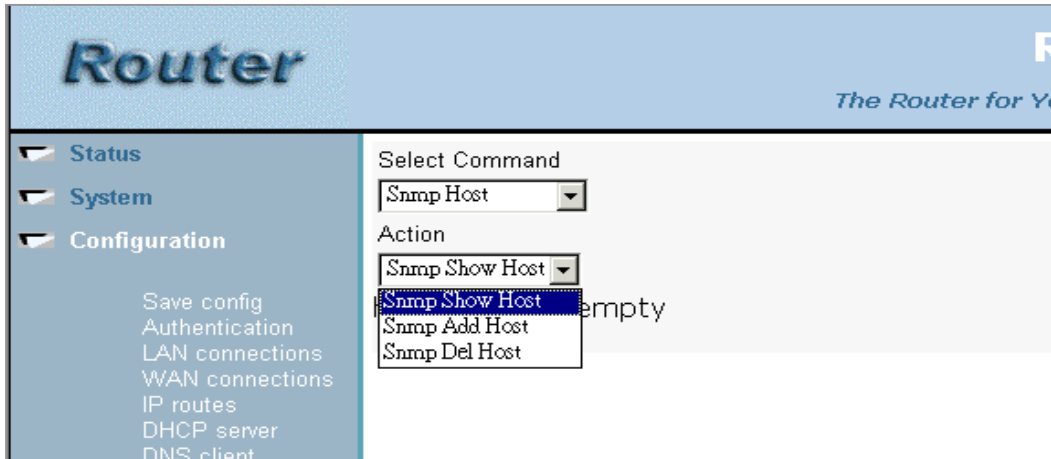


Figure 6-72 Web Tool – Snmp: select Action page

- Show current SNMP Community by selecting **Snmp Community** in Select Command and **Snmp Show Community** in Action.

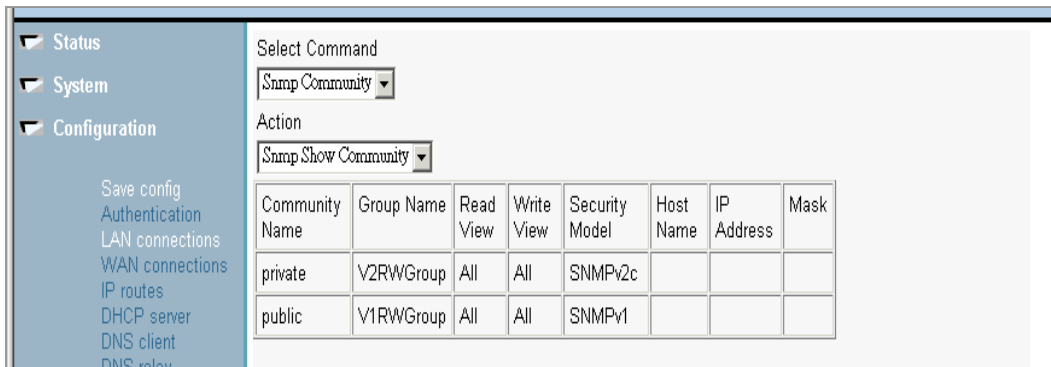


Figure 6-73 Web Tool – Snmp: Snmp Show Community page

If you want to add a new SNMP Community, select **Snm Add Community** in Action. Or if you want to delete a Community, select **Snm Del Community** in Action.

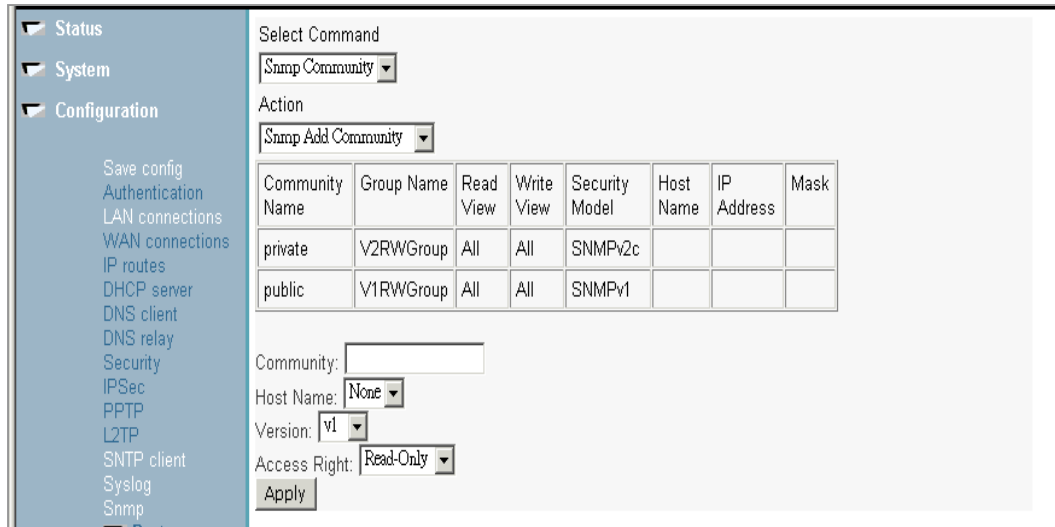


Figure 6-74 Web Tool – Snmp: Snmp Add Community page

- To add a SNMP host, just select **Snm Host** in Select Command and **Snm Add Host** in Action. Enter an already existing SNMP community in the **Community** field.

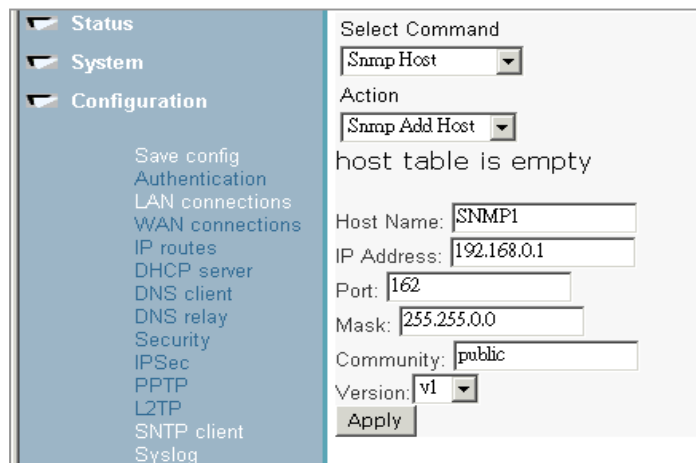


Figure 6-75 Web Tool – Snmp: Snmp Add Host page

5. You can now set the Trap. To add a SNMP Trap, select **Snmp Trap** in Select Command and **Snmp Add Trap** in Action. Enter the Host Name you want the trap to be sent to. The host name must already exist in the host table.

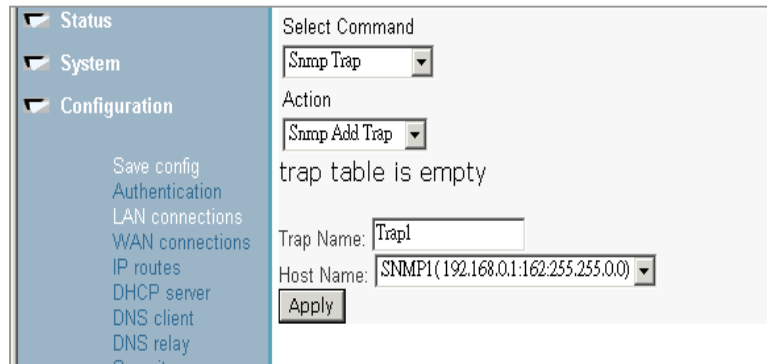


Figure 6-76 Web Tool – Snmp: Snmp Add Trap page

6. You can select **Snmp Show Host** or **Snmp Show Trap** in Action to check the configuration.

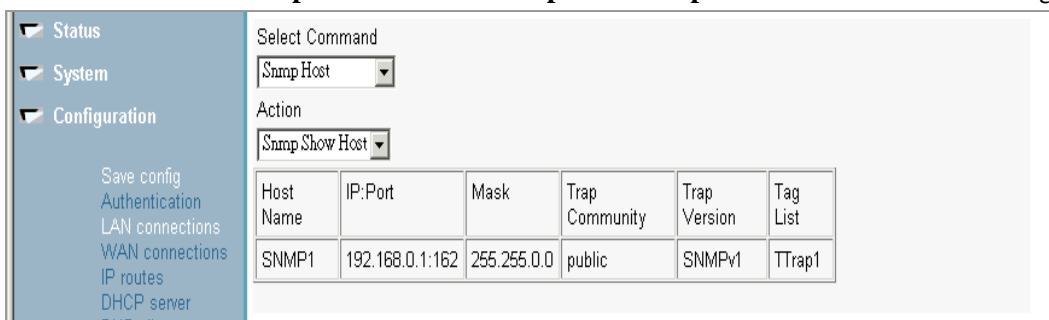


Figure 6-77 Web Tool – Snmp: Snmp Show Host page

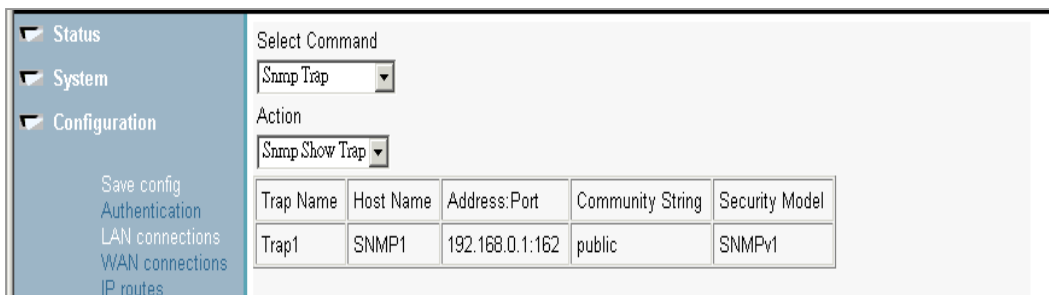


Figure 6-78 Web Tool – Snmp: Snmp Show Trap page

Port

After fully configuring your router card, be sure the proper mode of the Ethernet port, Fr port, Fb port, or Hdlc port has been selected. To check, please follow the steps below.

1. From the GUI left frame, click on **Configuration** and then click on **Ports**. Click on **Ethernet**, **FB**, **FR**, or **Hdlic** and then the chosen “Port Configuration” page will appear (3641-80 only).

Note – For the 3648-80 router which includes the 8 port Ethernet switch, this screen will only display version, connection and a link speed of 1 000 000.

View advanced attributes... ▶

Basic Port Attributes

| Name | Value |
|---------------------|--------|
| Version | 1.01 |
| 100Base | false |
| Auto Neg Ack Ok | false |
| Auto Neg Done | true |
| Connected | true |
| Dis Reconnect Count | 2 |
| Full Duplex | false |
| Jabber | false |
| Jabber Count | 0 |
| Link Speed | 100000 |
| Remote100BTFD | false |
| Remote100BTHD | false |
| Remote10BTFD | false |
| Remote10BTHD | false |
| Remote Fault | false |
| Remote Fault Count | 0 |

Apply Reset

Figure 6-79 Web Tool – Ports: Ethernet Port Configuration page

2. Click on the “View advanced attributes” link to view advanced port attributes (3641-80 only)

Note – For 3648-80 router, this screen will not display any information.

Advanced Ethernet Port Configuration

[Return to basic attribute list...](#)

Advanced Port Attributes

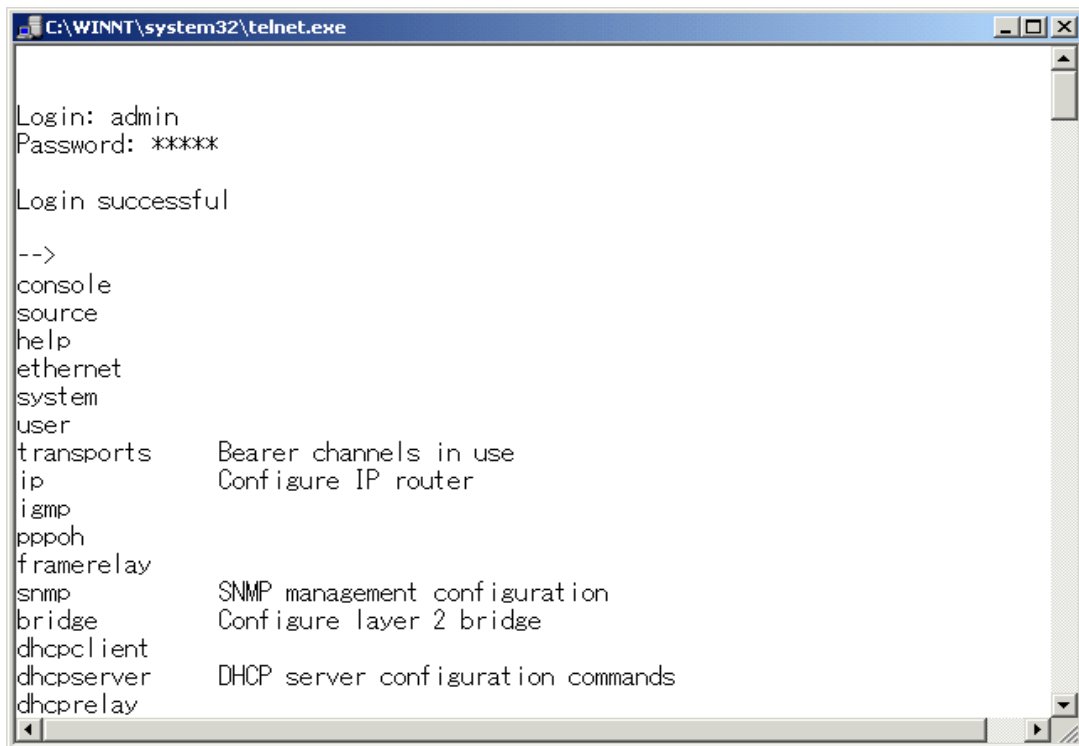
| Name | Value |
|-------------------------|------------------------------------|
| 100Base Full Advert | <input type="text" value="true"/> |
| 100Base Half Advert | <input type="text" value="true"/> |
| 10Base Full Advert | <input type="text" value="true"/> |
| 10Base Half Advert | <input type="text" value="true"/> |
| Auto Negotiation | <input type="text" value="true"/> |
| Auto Negotiate Restart | <input type="text" value="false"/> |
| Enable Duplex Check | <input type="text" value="true"/> |
| Loopback | <input type="text" value="false"/> |
| No Neg100Base Mode | <input type="text" value="true"/> |
| No Neg Full Duplex Mode | <input type="text" value="false"/> |
| Power Down | <input type="text" value="false"/> |
| Reset | <input type="text" value="false"/> |

Figure 6-80 Web Tool – Ports: Advanced Ethernet Port Configuration page

7. CLI Configuration Tool

The router card provides provisioning not only via the web browser but also the craft serial port using Command Line Interface (CLI).

Login to CLI of the router via the serial console port of the router card or any terminal emulation program to connect to the router card over the Ethernet. The default user names and passwords are the same as those previously described in the Web configuration chapter (see Table 6-1).



```
C:\WINNT\system32\telnet.exe

Login: admin
Password: ****

Login successful

-->
console
source
help
ethernet
system
user
transports      Bearer channels in use
ip               Configure IP router
igmp
pppoh
framerelay
snmp             SNMP management configuration
bridge          Configure layer 2 bridge
dhcpclient
dhcpserver      DHCP server configuration commands
dhcprelay
```

Figure 7-1 Login CLI Configuration Tool

There are two types of commands available for use in router card: one is CLI commands, the other is Console commands. Users with appropriate access permissions (superuser) can enter console mode from the CLI by entering the “console enable” command and use the console commands. Most of the console commands are the same with the CLI commands. Basically, users can use “help”, “help all”, “home”, “exit” and etc...to search for help and switch the command mode.

The details of each CLI command are described in the *Ethernet Router CLI Manual Section 364-180-C01* manual. While for Console commands, there are only a few commands described

since the Console commands are mainly for customer support debug. You can also see usage of some of the console commands in the following sections.

NOTE: There are certain features that are only accessible through the CLI Configuration Tool:

1. Webserver configuration
2. DHCP client parameters configuration (such as reboot time, retry time, backoff time, etc.)
3. Upload/download the configuration file to/from system/PC
4. Local upgrade firmware (via tftp/bootp protocol)
5. Set rip host route and set rip poison
6. Reset the router configuration to factory default settings.

7.1. Help Text for Using the CLI Commands

Within the CLI, the following functions can be used:

- * Hitting ? halfway through a word shows all valid completions of that prefix
- * Hitting ? after a word shows a list of the words that can follow it
- * Hitting TAB halfway through a word completes it, if it is unique
- * The UP and DOWN cursor keys move back and forward through the command history
- * LEFT and RIGHT cursor keys can be used for line-editing, and CTRL+A and CTRL+E move the cursor to the start and end of the line respectively

Pressing ? at the top-level prompt will display a list of the command groups available. Typing one followed by a space and then hitting ? will show the subcommands within that group, and so on.

| Task | Command |
|---------------------------------|--|
| List all command groups | ? ex. ? |
| List all commands under a group | <i>command group</i> ? ex. ethernet ? |

7.2. Download/Upload Configuration File

The download/upload configuration file can only be accessible through the CLI and console commands. This cannot be done via the web configuration tool. The configuration file of the router, im.conf, is located in the //flashfs/ directory of the router. Once you want to download/upload the configuration file, you can do this either by FTP or TFTP.

If you want to download a configuration file from Router **A** and upload it to Router **B**:

Using FTP

1. First ftp to Router **A** from your PC by executing the “ftp xxx.xxx.xxx.xxx” command where xxx.xxx.xxx.xxx stands for the IP address of Router **A**. Then get the configuration file back to your PC by entering command “get //flashfs/im.conf im.conf” in the ftp terminal.
2. Similarly, ftp to Router **B** from your PC and put the file from your PC into Router **B** by entering command “put im.conf //flashfs/im.conf”.
3. Restart Router **B**.

Using TFTP

1. You must prepare a PC with TFTP server software, and let Router **A** and **B** be TFTP clients.
2. In the Router **A** CLI, enter the CLI command “tftpc connect xxx.xxx.xxx.xxx” where xxx.xxx.xxx.xxx stands for the IP address of your TFTP server.
3. After Router **A** is connected to the TFTP server, enter CLI command “tftpc put //flashfs/im.conf im.conf” command.
4. Similarly, let Router **B** connects to the TFTP server and gets the configuration file via CLI command “tftpc get im.conf //flashfs/im.conf”.
5. Restart Router **B**.

<For example>:

1. Router Card configurations save to PC the CLI commands bellow:

→tftpc connect 172.16.100.88 (PC IP address: 172.16.100.88)

Successfully connect to 172.16.100.88 (Router Card connect with PC successfully)

→tftpc put //flashfs/im.conf im.conf (Put Router Card configuration to PC. The file name is “im.conf)

PUT 11848 bytes from //flashfs/im.conf (Put Router Card configuration to PC successfully)

2. Router Card configurations get from PC the CLI commands bellow:

→tftp connect 172.16.100.88 (PC IP address: 172.16.100.88)

Successfully connect to 172.16.100.88 (Router Card connect with PC successfully)

→tftp get im.conf //flashfs/im.conf (Get Router Card configuration from PC. The file name is "im.conf")

GET 13029 bytes from im.conf to //flashfs/im.conf (Get Router Card configuration from PC successfully)

→system restart

* For the details of the tftp console commands, please refer to *Ethernet Router CLI Manual Section 364-180-C01*.

Note: When you FTP to the router or use tftp command (CLI or console) in the router, you don't need to change to any other directories. Just get or put the configuration file to the connected directory directly.

You can exit the tftp console command mode by entering the "home" command to return to the root command tree of the console mode. You can exit the console mode back to the CLI mode by entering the "exit" command.

About FlashFS and ISFS

Flash memory is used on the System to store a permanent copy of an image and any configuration data. This data is stored in a non-volatile partitioned filing system known as FlashFS. SDRAM is used on the System to store a temporary copy of some of the files that are stored in FlashFS. This data is stored in a volatile filing system known as ISFS.

ISFS stores a copy of FlashFS files to make them accessible to application processes for storing of configuration data that can subsequently be written back to FlashFS.

For example, setting the IP address of the System and the ARP server it uses is the type of information that would be configured during a session and then saved for future use as configuration data in FlashFS.

7.3. Using the *source* CLI commands

The *source* <filename> command allows you to run a list of predefined commands stored in an existing file. This saves you having to retype lengthy configurations that you will want to use again. Before you can use this command, you need to create a plain text file containing the command list and save it in your ISFS directory (you can do this by the FTP/TFTP method; please refer to the section 7.2). Once you specify the *filename* in the *source* command, the file is located and the commands are executed. For example:

```
--> source //isfs/myconfiguration.txt
Sourcing file '//isfs/myconfiguration.txt'...

--> ethernet clear transports

--> ethernet add transport eth1 ethernet

--> bridge add interface bridge1

--> bridge attach bridge1 eth1

--> framerelay add transport fr1 fr 171

--> framerelay set transport fr1 encapsulation bridgedether

--> bridge add interface bridge2

--> bridge attach bridge2 fr1

--> ethernet list transports

Ethernet transports:

  ID  | Name      | Port
-----|-----|-----
   1  | eth1      | ethernet
-----|-----|-----

--> bridge list interfaces

Bridge Interfaces:
```

| ID | Name | Filter Type | Transport |
|----|---------|-------------|-----------|
| 1 | bridge2 | All | fr1 |
| 2 | bridge1 | All | eth1 |

--> framereelay list transports

Frame Relay Transports:

| ID | Name | Port | DLCI | Encapsulation |
|----|------|------|------|---------------|
| 1 | fr1 | fr | 171 | BridgedEther |

7.4. CLI Application Examples

Before the application examples, you need to understand the following CLI terms.

Transports: A transport is a layer 2 session and everything below it. You can create a transport and attach it to a bridge or router so that data can be bridged or routed via the attached transport.

Interface: bridges and routers both have interfaces. A single transport is attached to a bridge or router via an interface.

Port: A transport is set to run on a certain port.

The table below lists the default names of the different ports or interfaces of the router card.

Table 7-1 Default names of different Interface/Transport/Port

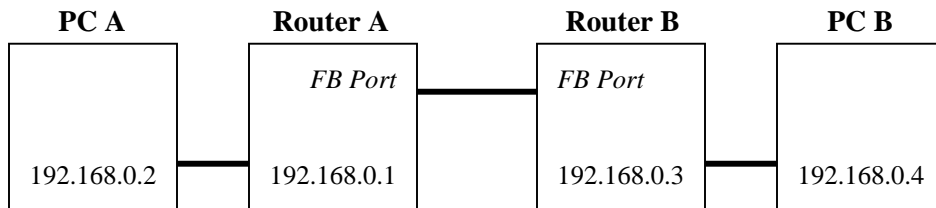
| Type | Name |
|-----------|-----------------------------|
| interface | ip, bridge |
| transport | ethernet, framerelay, pppoh |
| port | ethernet, fr, fb, hdlc |

Note: the port names cannot be changed.

Note: After loading the scripts, save the configuration and restart the router

Frame Relay - bridged

In this example, the router card bridges between Ethernet and Frame Relay. Frame Relay runs between the two routers over an HDLC link.



Configure PC A and PC B

1. Configure PC A as follows:

- IP address: 192.168.0.2
- Subnet mask: 255.255.255.0
- Gateway: None

2. Configure PC B as follows:

- IP address: 192.168.0.4
- Subnet mask: 255.255.255.0
- Gateway: None

Configure Router A using the CLI

1. Clear any existing Bridge interfaces and Ethernet and Frame Relay transports by typing the following command:

```
ip clear routes
ip clear rip
ip clear interfaces
bridge clear interfaces
transports clear
port fr set AutoStart false
port fb set AutoStart false
```

2. Add an Ethernet device to the Bridge. In the following commands, *eth0* is the transport name, *ethernet* is the port name and *bridge1* is the Bridge interface name:

```
ethernet add transport eth0 ethernet
ip add interface eth0 192.168.0.1 255.255.255.0
bridge add interface bridge1
bridge attach bridge1 eth0
```

3. Add a Frame Relay device to the Bridge, with Frame Relay configured to run on port *fr* using DLCI 100. In the following commands, *frame-0* is the transport name and *bridgedether* is the encapsulation method:

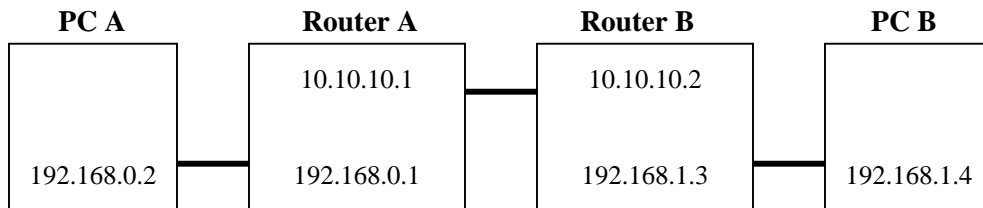
```
framerelay add transport frame-0 fb 100
framerelay set transport frame-0 encapsulation bridgedether
bridge add interface bridge2
bridge attach bridge2 frame-0
ip attachbridge eth0
```

Configure Router B using the CLI

Configure Router B by following the same configuration instructions for Router A except you will need to change the IP address from 192.168.0.1 to 192.168.0.3.

Frame Relay - routed

In this example, the router card routes between Ethernet and Frame Relay. Frame Relay runs between the two routers over an HDLC link.



Configure PC A and PC B

1. Configure PC A as follows:

- IP address: 192.168.0.2
- Subnet mask: 255.255.255.0
- Gateway: 192.168.0.1

2. Configure PC B as follows:

- IP address: 192.168.1.4
- Subnet mask: 255.255.255.0
- Gateway: 192.168.1.3

Configure Router A using the CLI

1. Clear any existing IP interfaces and transports. Clearing the IP interfaces also deletes any existing DHCP client settings on those interfaces. This change to DHCP is not updated in the DHCP client configuration until you enter the *dhcpclient update* command. Type the following commands:

```
ip clear routes
ip clear rip
ip clear interfaces
transports clear
port fr set AutoStart false
port fb set AutoStart false
dhcpclient update
```

2. Add the Ethernet device to the router. In the following command, *eth0* is the name of the

transport, and *ethernet* is the port name.

```
ethernet add transport eth0 ethernet
ip add interface eth1 192.168.0.1 255.255.255.0
ip attach eth1 eth0
```

3. Add a Frame Relay device to the router, with Frame Relay configured to run on port *fr* using DLCI 100. In the following commands, *frame-0* is the transport name and *routedip* is the encapsulation method:

```
framerelay add transport frame-0 fr 100
framerelay set transport frame-0 encapsulation routedip
ip add interface frame-0 10.10.10.1 255.255.255.0
ip attach frame-0 frame-0
```

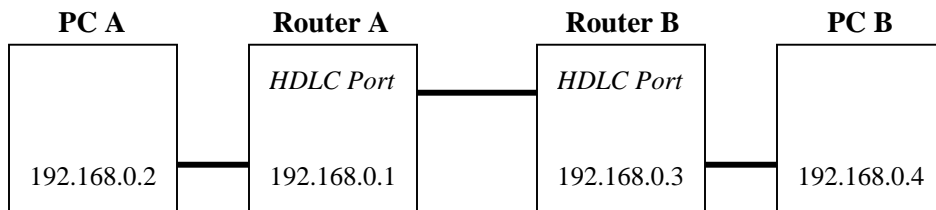
Configure Router B using the CLI

The configuration here is similar to Router A.

```
ip clear routes
ip clear rip
ip clear interfaces
port fr set AutoStart false
port fb set AutoStart false
dhcpclient update
ethernet add transport eth0 ethernet
ip add interface eth1 192.168.1.3 255.255.255.0
ip attach eth1 eth0
framerelay add transport frame-0 fr 100
framerelay set transport frame-0 encapsulation routedip
ip add interface frame-0 10.10.10.2 255.255.255.0
ip attach frame-0 frame-0
```


PPP - bridged

In this example, the router card bridges between Ethernet and PPP over HDLC. Router A will be the dial-out (i.e., client) end of the PPP link, and Router B will be the dial-in (i.e., server) end of the link.



Configure PC A and PC B

1. Configure PC A as follows:

- IP address: 192.168.0.2
- Subnet mask: 255.255.255.0
- Gateway: None

2. Configure PC B as follows:

- IP address: 192.168.0.4
- Subnet mask: 255.255.255.0
- Gateway: None

Configure Router A using the CLI

1. Clear any existing IP interfaces and pppoh transports. Clearing the IP interfaces also deletes any existing DHCP client settings on those interfaces. This change to DHCP is not updated in the DHCP client configuration until you enter the *dhcpclient update* command. Clear any existing Bridge interface. Type the following command:

```
ip clear routes
ip clear rip
ip clear interfaces
bridge clear interfaces
transports clear
port fr set AutoStart false
port fb set AutoStart false
```

dhcpcclient update

2. Add an Ethernet device to the Bridge. In the following commands, *eth1* is the transport name, *ethernet* is the port name and *bridge1* is the Bridge interface name:

```
ethernet add transport eth1 ethernet
ip add interface eth1 192.168.0.1 255.255.255.0
bridge add interface bridge1
bridge attach bridge1 eth1
ip attachbridge eth1
ip list int
```

3. Create the PPP transport. The following commands configure PPP device 1 for dial-out on HDLC port, *ppp1* is the transport name and *1* is the interface id:

```
pppoh add transport ppp1 dialout 1 hdlc
```

4. Configure the PPP transport:

- A. No authentication will be used.

```
pppoh set transport ppp1 wlogin none
```

- B. Ensure that PPP uses the correct IP subnet mask:

```
pppoh set transport ppp1 subnetmask 255.255.255.0
```

5. Add the PPP device to the bridge.

```
Bridge add interface bridge2
Bridge attach bridge2 ppp1
```

Configure Router B using the CLI

The configuration here is similar to Router A.

```
ip clear routes
ip clear rip
ip clear interfaces
transports clear
port fr set AutoStart false
```

```
port fb set AutoStart false
pppoh clear transports
dhcpcclient update
bridge clear interfaces
```

```
ethernet add transport eth1 ethernet
ip add interface eth1 192.168.0.3 255.255.255.0
bridge add interface bridge1
bridge attach bridge1 et1
```

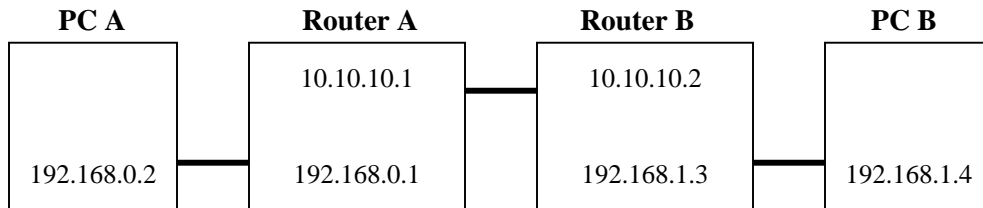
```
pppoh add transport ppp1 dialin 1 hdlc
```

```
pppoh set transport ppp1 theylogin none
pppoh set transport ppp1 subnetmask 255.255.255.0
pppoh list transports
```

```
bridge add interface bridge2
bridge attach bridge2 ppp1
```

PPP - routed

In this example, each router card routes data between Ethernet and PPP over HDLC. Router A will be the dial-out (i.e., client) end of the PPP link, and Router B will be the dial-in (i.e., server) end of the link.



Configure PC A and PC B

1. Configure PC A as follows:

- IP address: 192.168.0.2
- Subnet mask: 255.255.255.0
- Gateway: 192.168.0.1

2. Configure PC B as follows:

- IP address: 192.168.1.4
- Subnet mask: 255.255.255.0
- Gateway: 192.168.1.3

Configure Router A using the CLI

1. Clear any existing IP interfaces and transports. Clearing the IP interfaces also deletes any existing DHCP client settings on those interfaces. This change to DHCP is not updated in the DHCP client configuration until you enter the *dhcpclient update* command. Type the following commands:

```
ip clear routes
ip clear rip
ip clear interfaces
transports clear
port fr set AutoStart false
port fb set AutoStart false
dhcpclient update
```

2. Add the Ethernet device to the router. In the following command, *eth0* is the name of the transport, and *ethernet* is the port name.

```
ethernet add transport eth1 ethernet
ip add interface ip1 192.168.0.1 255.255.255.0
ip attach ip1 eth1
```

3. Create the PPP transport. The following commands configure PPP device 1 for dial-out (client) on HDLC port, *ppp1* is the transport name and *1* is the interface id:

```
pppoh add transport ppp1 dialout 1 hdlc
```

4. Configure the PPP transport:

- A. CHAP authentication will be used; PPP will supply a username of 'admin' and a password of 'admin':

```
pppoh set transport ppp1 username admin
pppoh set transport ppp1 password admin
pppoh set transport ppp1 wlogin chap
```

- B. Ensure that PPP uses the correct IP subnet mask:

```
pppoh set transport ppp1 subnetmask 255.255.255.0
```

- C. By default, the transport creates a default route to the subnet at the remote end of the PPP link. You do not need to configure this.

5. Add the PPP device to the router:

```
ip add interface ip2
ip attach ip2 ppp1
```

Configure Router B using the CLI

1. Clear any existing IP interfaces and transports. Clearing the IP interfaces also deletes any existing DHCP client settings on those interfaces. This change to DHCP is not updated in the DHCP client configuration until you enter the *dhcpclient update* command. Type the following commands:

```
ip clear routes
ip clear rip
ip clear interfaces
transports clear
port fr set AutoStart false
port fb set AutoStart false
dhcpcclient update
```

2. Add the Ethernet device to the router. In the following command, *eth0* is the name of the transport, and *ethernet* is the port name.

```
ethernet add transport eth1 ethernet
ip add interface ip1 192.168.1.3 255.255.255.0
ip attach ip1 eth1
```

3. Create the PPP transport. The following commands configure PPP device 2 for dial-in (server) on HDLC port. CHAP authentication will be used, and PPP will expect the user “admin” to login using the password “admin”.

```
pppoh add transport ppp1 dialin 1 hdlc
ip add interface ip2 10.10.10.2
pppoh set transport ppp1 theylogin chap
pppoh set transport ppp1 remoteip 10.10.10.1
ip attach ip2 ppp1
```

4. On the dial-in end of the link, a route to the other PC will not be added manually. The following command adds a default route using Router A as the gateway:

```
ip add route default 0.0.0.0 0.0.0.0 gateway 10.10.10.1
```

5. Finally, add a dial-in facility for user ‘admin’ using password ‘admin’:

```
pppoh set transport ppp1 username admin
pppoh set transport ppp1 password admin
```

7.5. CLI Commands Group

The CLI commands can be divided into different groups that are listed below:

- Bridge CLI commands
- Console commands
- DHCP Client CLI commands
- DHCP Relay CLI commands
- DHCP Server CLI commands
- DNS Client CLI commands
- DNS Relay CLI commands
- Ethernet CLI commands
- Firewall CLI commands
- Frame Relay CLI commands
- IGMP CLI commands
- IPsec CLI commands
- L2TP CLI commands
- NAT CLI commands
- Port CLI commands
- PPPoH CLI commands
- PPTP CLI commands
- Security CLI commands
- Snmp CLI commands
- SNTP CLI commands
- SyslogClient CLI commands
- System CLI commands
- TCP/IP CLI commands
- Transport CLI commands
- User CLI commands
- Web Server CLI commands

7.6. List of CLI Commands

The notation conventions for the parameter in the CLI commands list are as follows:

- Parameter values enclosed in < > must be specified.
- Parameters enclosed in [] are optional.
- Parameter values are separated by a vertical bar “|” only when one of the specified values can be used.
- Parameter values are enclosed in { } when you must use one of the values specified.

For the details of each CLI command, please look up the *Ethernet Router CLI Manual Section 364-180-C01*.

Table 7-2 List of CLI commands

| Group | Command | Parameter | | |
|---------|-----------|--------------------------------------|------------------------|------------------------------|
| Bridge | bridge | add interface <name> | | |
| | | attach {<name> <number>} <transport> | | |
| | | clear interfaces | | |
| | | delete interface {<name> <number>} | | |
| | | detach {<name> <number>} | | |
| | | list interfaces | | |
| | | set | filterage <filter age> | |
| | | | interface | {<name> <number>} filtertype |
| | | | | {all ip pppoe} |
| | | | spanning | {enabled disabled} |
| | | | | forwarddelay <delay> |
| | | | | hellotime <hellotime> |
| | | | maxage <maxage> | |
| | | priority <priority> | | |
| show | interface | {<name> <number>} | | |
| | console | enable | | |
| Console | console | process <console command> | | |

| | | | | |
|--------------------|------------|-----------------|------------------|---|
| DHCP Client | dhcpclient | add | interfaceconfig | <name><ipinterface> |
| | | clear | interfaceconfigs | |
| | | delete | interfaceconfig | {<name> <number>} |
| | | interfaceconfig | | {<name> <number>} add requested option <option> |
| | | | | {<name> <number>} add required option <option> |
| | | | | {<name> <number>} add sent option <option> <value> |
| | | | | {<name> <number>} clear sent options |
| | | | | {<name> <number>} clear requested options |
| | | | | {<name> <number>} delete requested option <option number> |
| | | | | {<name> <number>} delete sent option <option number> |
| | | | | {<name> <number>} list requested options |
| | | | | {<name> <number>} list sent options |
| | | list | interfaceconfigs | |
| | | set | backoff | <backofftime> |
| | | | interfaceconfig | {<name> <number>} autoip {enabled disabled} |
| | | | | {<name> <number>} clientid <clientid> |
| | | | | {<name> <number>} defaultroute {enabled disabled} |
| | | | | {<name> <number>} dhcpinform {enabled disabled} |
| | | | | {<name> <number>} dhcpserverpoolsize <pool size> |
| | | | | {<name> <number>} dhcpserverinterface <interface name> |

| | | | | |
|--------------------|------------|--------------------|-----------------|---|
| | | | | {<name> <number>} givednstoclient |
| | | | | {enabled disabled} |
| | | | | {<name> <number>} givednstorelay |
| | | | | {enabled disabled} |
| | | | | {<name> <number>} interface |
| | | | | <ipinterface> |
| | | | | {<name> <number>} noclientid |
| | | | | {<name> <number>} requestedleasetime |
| | | | | <requestedleasetime> |
| | | | | {<name> <number>} server <ipaddress> |
| | | | reboot | <reboottime> |
| | | | retry | <retrytime> |
| | | show | | |
| | | | interfaceconfig | <name> |
| | | update | | |
| DHCP Relay | dhcprelay | add | server | <ipaddress> |
| | | clear | servers | |
| | | delete | server | <number> |
| | | {enable disable} | | |
| | | list | servers | |
| | | show | | |
| | | update | | |
| DHCP Server | dhcpserver | add | subnet | <name> <ipaddress> <netmask> [<startaddr> <endaddr>] |
| | | clear | subnets | |
| | | delete | subnet | {<name> <number>} |
| | | {enable disable} | | |
| | | list | options | |
| | | | subnets | |

| | | | |
|--------|----------------------|--|---|
| set | allowunknownclients | {enabled disabled} | |
| | bootp | {enabled disabled} | |
| | defaultleasetime | <defaultleasetime> | |
| | maxleasetime | <maxleasetime> | |
| | subnet | | {<name> <number>} defaultleasetime <defaultleasetime> |
| | | | <{<name> <number>}> |
| | | | hostisdefaultgateway {enabled disabled} |
| | | | {<name> <number>} hostisdnsserver {enabled disabled} |
| | | | {<name> <number>} maxleasetime <maxleasetime> |
| | | | {<name> <number>} subnet <ip address> <netmask> |
| show | | | |
| | subnet | {<name> <number>} | |
| subnet | | {<name> <number>} add iprange <startaddr> <endaddr> | |
| | | {<name> <number>} add option <identifier> <value> | |
| | | {<name> <number>} clear ipranges | |
| | | {<name> <number>} clear options | |
| | | {<name> <number>} delete iprange <range-id> | |
| | | {<name> <number>} delete option <option number> | |
| | | {<name> <number>} list ipranges | |
| | | {<name> <number>} list options | |
| update | | | |
| | DNS Client dnsclient | add | searchdomain <searchstring> |
| | | server <ipaddress> | |
| clear | | searchdomains | |
| | | servers | |

| | | | | |
|------------------|----------|--------|--|---|
| | | delete | searchdomain | <searchstring> |
| | | | server | <number> |
| | | list | searchdomains | |
| | | | servers | |
| DNS Relay | dnsrelay | add | server | <ip-address> |
| | | clear | servers | |
| | | delete | server | <id-number> |
| | | list | servers | |
| Ethernet | ethernet | add | transport | <name> [<port>] |
| | | clear | transports | |
| | | delete | transport | {<name> <number>} |
| | | list | ports | |
| | | | transports | |
| | | set | transport | {<name> <number>} port <port> |
| | | show | transport | {<name> <number>} |
| Firewall | firewall | add | policy | <name> {external-internal externaldmz dmz-internal} [[allowonly-val] {blockonly-val}] |
| | | | portfilter | <name> <policyname> {protocol <number>} {inbound outbound both} <name> <policyname> {tcp udp} <startport> <endport> {inbound outbound both} |
| | | | validator | <name> <policyname> |
| | | | (this command is not useful at present) | {inbound outbound both} <ipaddress> <hostipmask> |
| | | clear | policies | |
| | | | portfilters | <policyname> |
| | | delete | policy | <name> |

| | | |
|--------------------|---|--|
| | portfilter | <name> <policyname> |
| | validator | <name> <policyname> |
| | (this command is not useful at present) | |
| {enable disable} | | |
| | alerting | {email paging} |
| | blockinglog | |
| | IDS | |
| | intrusionlog | |
| | sessionlog | |
| list | policies | |
| | portfilters | <policyname> |
| | protocol | |
| | validators | <policyname> |
| | (this command is not useful at present) | |
| set | alerting | email server <email_server> |
| | | email from <from> |
| | | email recipient1 <email><name> |
| | | email recipient2 <email><name> |
| | | paging server <paging_server> |
| | | paging from <from> |
| | | paging recipient1 <pager><name> |
| | | paging recipient2 <pager><name> |
| | IDS | blacklist {enable disable clear} |
| | | DOSattackblock <duration> |
| | | MaxICMP <max> |
| | | MaxPING <max> |
| | | MaxTCPopenhandshake <max> |
| | | SCANattackblock <duration> |
| | | victimprotection {enable <duration> disable} |

| | | | | |
|--------------------|------------|--------|---|---|
| | | | privhost | <privhost_start_addr> <privhost_end_addr> |
| | | | securitylevel | {none high medium low userdefined <slevel>} |
| | | show | alerting | |
| | | | IDS | |
| | | | policy | <name> |
| | | | portfilter | <name> <policyname> |
| | | | privhost | |
| | | | validator | <name> <policyname> |
| | | | (this command is not useful at present) | |
| | | | status | |
| Frame Relay | framerelay | add | transport | <name> <port> <dlci> |
| | | clear | transports | |
| | | delete | transport | {<name> <number>} |
| | | list | transports | |
| | | set | transport | {<name> <number>} chnlsegmentsize <channel segment size> {<name> <number>} dlci <dlci> {<name> <number>} encapsulation {raw routedip bridgedether} {<name> <number>} port <port> {<name> <number>} rxmaxpdu <rxmaxpdu> {<name> <number>} tcmaxpdu <tcmaxpdu> |
| | | show | transport | {<name> <number>} |
| IGMP | igmp | set | upstreaminterface | {<ip_interface> none} |
| | | show | upstreaminterface | |
| | | | status | |
| IPSec | IPSec | add | endpoint | <endpoint_id> |

| | | | | |
|-------------|----------|--------|---------------|---|
| | | clear | endpoints | |
| | | delete | endpoint | <endpoint_id> |
| | | list | endpoints | |
| | | set | endpoint | <number> endpointid <endpoint_id> |
| | | | | <number> ipaddress <ip_address> |
| | | | | <number> ike auth preshared-key |
| | | | | <number> ike auth digital-signature |
| | | | | <number> ike presharedkey |
| | | | | <preshared_key> |
| | | | | <number> salife <seconds> |
| | | | | <number> ike hash {md5 sha1} |
| | | | | <number> ike encryption |
| | | | | {des blowfish 3des} |
| | | | | <number> IPSec protocol |
| | | | | <protocol_type> |
| | | | | <number> IPSec tunnel_type |
| | | | | <tunnel_type> |
| | | | | <number> IPSec ah <ah_transform> |
| | | | | <number> IPSec esp <esp_transform> |
| | | | | <number> IPSec esp_auth <esp_auth> |
| | | | | <number> IPSec ipcomp <ipcomp_auth> |
| | | | | <number> target_host subnet |
| | | | | <ip_addressss> <subnet_mask> |
| | | | | <number> target_host range |
| | | | | <ip_addressss_start> <ip_addressss_end> |
| | | | intranet | <intranet_addr> <intranet_mask> |
| | | | negotiationid | <negotiation_id> |
| | | show | endpoint | <number> |
| | | | intranet | |
| | | | negotiationid | |
| L2TP | anscl2tp | set | pool | <pool_start_addr> <pool_end_addr> |
| | | show | pool | |

| | | | | |
|--------------|-------|----------|-------------|--|
| | | | clients | |
| NAT | nat | add | globalpool | <name> <interfacename> internal dmz <ipaddress> {subnetmask <mask> endaddress <address>} |
| | | | resvmap | <name> globalip <interfacename> <globalip> <internalip> {tcp <portno> udp <portno> icmp igmp ip egp rsvp ospf ipip all} |
| | | | resvmap | <name> interfacename <interfacename> <internalip> {tcp <portno> udp <portno> icmp igmp ip egp rsvp ospf ipip all} |
| | | clear | globalpools | <interfacename> |
| | | | resvmaps | <interfacename> |
| | | delete | globalpool | <name> <interfacename> |
| | | | resvmap | <name> <interfacename> |
| | | disable | | <name> |
| | | enable | | <name><interfacename> {internal dmz} |
| | | list | globalpools | <interfacename> |
| | | | resvmaps | <interfacename> |
| | | show | globalpool | <name> <interfacename> |
| | | | resvmap | <name> <interfacename> |
| | | status | | |
| Port | port | ethernet | set | <attribute> <value> |
| | | | show | |
| | | fb | set | <attribute> <value> |
| | | | show | |
| | | fr | set | <attribute> <value> |
| | | | show | |
| | | hdlc | set | <attribute> <value> |
| | | | show | |
| PPPoH | pppoh | add | transport | <name> dialin <interface> <port> |

| | | |
|--------|------------|---|
| | transport | <name> dialout <interface> <port> |
| clear | transports | |
| delete | transport | {<name> <number>} |
| list | transports | |
| set | transport | {<name> <number>} createroute {enabled disabled} |
| | | {<name> <number>} dialin |
| | | {<name> <number>} dialout |
| | | {<name> <number>} discoverdns primary {enabled disabled} |
| | | {<name> <number>} discoverdns secondary {enabled disabled} |
| | | {<name> <number>} {enabled disabled} |
| | | {<name> <number>} givedns client {enabled disabled} |
| | | {<name> <number>} givedns relay {enabled disabled} |
| | | {<name> <number>} headers hdlc {enabled disabled} |
| | | {<name> <number>} headers llc {enabled disabled} |
| | | {<name> <number>} interface <interface> |
| | | {<name> <number>} lcpechoevery <interval> |
| | | {<name> <number>} lcpmaxconf <lcp max configure> |
| | | {<name> <number>} lcpmaxfail <lcp max fail> |
| | | {<name> <number>} lcpmaxterm <lcp max terminate> |
| | | {<name> <number>} localip <ip-address> |
| | | {<name> <number>} password <password> |

| | | | | |
|-----------------|----------|--------|------------|--|
| | | | | {<name> <number>} remoteds |
| | | | | <ipaddress> [<ipaddress2>] |
| | | | | {<name> <number>} remoteip |
| | | | | <ip-address> |
| | | | | {<name> <number>} routemask <mask> |
| | | | | {<name> <number>} specificroute |
| | | | | {enabled disabled} |
| | | | | {<name> <number>} subnetmask <mask> |
| | | | | {<name> <number>} theylogin |
| | | | | {none pap chap} |
| | | | | {<name> <number>} username |
| | | | | <username> {<name> <number>} |
| | | | | welogin {none pap chap} |
| | | show | transport | |
| PPTP | anscptp | set | pool | <pool_start_addr> <pool_end_addr> |
| | | show | pool | |
| | | | clients | |
| Security | security | add | interface | <name> {external internal dmz} |
| | | | trigger | <name> {tcp udp} <startport> <endport> <maxactinterval> |
| | | clear | interfaces | |
| | | | triggers | |
| | | delete | interface | <name> |
| | | | trigger | <name> |
| | | | {enable | |
| | | | disable} | |
| | | list | interfaces | |
| | | | triggers | |
| | | set | trigger | <name> addressreplacement {none tcp udp both} |
| | | | | <name> multihost {enable disable} |
| | | | | <name> binaryaddressreplacement {enable disable} |

| | | | | |
|-------------|------------|--------|---------------|---|
| | | | | <name> maxactinterval <interval> |
| | | | | <name> endpoint <portnumber> |
| | | | | <name> startport <portnumber> |
| | | | | <name> sessionchaining {enable disable} |
| | | | | <name> UDPsessionchaining {enable disable} |
| | | show | interface | <name> |
| | | | trigger | <name> |
| | | status | | |
| SNMP | snmp | add | community | <commstr> {v1 v2c} [hostname<hostname>] [rw] |
| | | | host | <hostname> <ipaddr> [port <ipport>] [mask <mask>] [{v1 v2c} <commstr>] |
| | | | trap | <trapname> <hostname> |
| | | config | save | |
| | | delete | community | <commstr> |
| | | | host | <hostname> |
| | | | trap | <trapname> |
| | | show | community | |
| | | | host | |
| | | | trap | |
| SNTP | sntpclient | set | clock | <yyyy:mm:dd:hh:mm:ss> |
| | | | mode | {unicast broadcast anycast} {enable disable} |
| | | | poll-interval | <0-30> |
| | | | retries | <0-10> |
| | | | server | {ipaddress <IP address> hostname <hostname>} |
| | | | timeout | <0-30> |
| | | | timezone | <abbreviation> |
| | | show | association | |

| | | | | |
|---------------|--------------|--|----------------|--|
| | | | status | |
| | | sync | | |
| Syslog | syslogClient | set | hostname | <hostName> |
| | | | receiver | <receiveripaddress> |
| | | | severity | {alert critical emergency error informational notice warning} |
| | | show | hostname | |
| | | | receiver | |
| | | | severity | |
| System | system | add | user | <name> ["comment"] |
| | | config | backup | |
| | | | restore | {backup factory } |
| | | | save | |
| | | delete | user | <name> |
| | | info | | |
| | | list | errors | |
| | | | openfiles | <name> |
| | | | users | |
| | | log | | {nothing warnings info trace entryexit all} |
| | | | enable disable | <module> <category> |
| | | | list | [<module>] |
| | | restart | | |
| set | user | <name> access {superuser engineer default} <name> mayconfigure {enabled disabled} <name> maydialin {enabled disabled} | | |
| TCP/IP | ip | add | interface | <name> [<ipaddress> [<netmask>]] |
| | | | route | <name> <dest_ip> <netmask> [{gateway <gateway_ip>}][interface <interface>] |
| | | | defaultroute | gateway <gateway_ip> interface <interface> |
| | | attach | | {<name> <number>} <transport> |

| | | | |
|--------------|-------------|---|--|
| attachbridge | | {<name> <number>} | |
| clear | interfaces | | |
| | riproutes | | |
| | routes | | |
| delete | interface | {<name> <number>} | |
| | route | {<name> <number>} | |
| detach | interface | {<name> <number>} | |
| interface | | {<name> <number>} add secondaryipaddress <ipaddress> [<netmask>] | |
| | | {<name> <number>} clear secondaryipaddresses | |
| | | {<name> <number>} delete secondaryipaddress <secondaryipaddress number> | |
| | | {<name> <number>} list secondaryipaddresses | |
| | | | |
| | | | |
| | | | |
| list | arpentries | | |
| | connections | | |
| | interfaces | | |
| | riproutes | | |
| | routes | | |
| ping | | <dest-address> | |
| set | interface | {<name> <number>} ipaddress <ipaddress> [<netmask>] | |
| | | {<name> <number>} netmask <netmask> | |
| | | {<name> <number>} mtu <mtu> | |
| | | {<name> <number>} dhcp {enabled disabled} | |
| | | {<name> <number>} rip accept {none v1 v2 all} | |
| | | | |
| | | | |

| | | | |
|------------------|------------|------------|---|
| | | | {<name> <number>} rip multicast |
| | | | {enabled disabled} |
| | | | {<name> <number>} rip send |
| | | | {none v1 v2 all} |
| | | | {<name> <number>} rip password |
| | | | <password> |
| | | | {<name> <number>} rip Auth {enabled disabled} |
| | | | <name> tcpmssclamp {enabled disabled} |
| | rip | | hostroutes {enabled disabled} |
| | | | poison {enabled disabled} |
| | route | | {<name> <number>} destination |
| | | | <dest-network> <netmask> |
| | | | {<name> <number>} gateway <gateway> |
| | | | {<name> <number>} cost <cost> |
| | | | {<name> <number>} interface |
| | | | {<interface> none} |
| | show | | |
| | | interface | {<name> <number>} |
| | | route | {<name> <number>} |
| | | debuginfo | |
| TFTPC | tftpc | connect | <host> |
| | | disconnect | |
| | | get | <src> <dst> |
| | | put | <src> <dst> |
| Transport | transports | clear | |
| | | delete | {<name> <number>} |
| | | list | |
| | | show | {<name> <number>} |
| User | user | logout | |
| | | password | |

| | | | | |
|-------------------|--------------|-----------------------|------------|--------------|
| | | change | | <name> |
| Web Server | webservice | clear | stats | |
| | | {enable disable} | | |
| | set | interface | | <interface> |
| | | managementip | | {ip-address} |
| | | managementipmask | | {netmask} |
| | | port | | <port> |
| | | upnpport | | <port> |
| | show | info | | |
| | | stats | | |
| | Other | help | | |
| Commands | source | | <filename> | |

Appendix: System Limit

Frame Relay:

1. The maximum number of Frame Relay DLCI channels is 14.

Routing Table:

1. The maximum number of dynamic learning routing entries is 256.
2. The maximum number of static route entries is 128.

Bridge:

1. The maximum number of addresses in the MAC address table is 4095.
2. The maximum size of an Ethernet frame allowed is 1536 bytes.

VPN:

1. The maximum number of IPsec VPN tunnels is 4.
2. If you want to add a new endpoint when there already exists an IPsec VPN tunnel, you must restart the router after the new endpoint is added.
3. The maximum data flow rate of IPsec is 500kbps.
4. The maximum data flow rate of PPTP or L2TP tunnel is 64kbps. In fact, it is about 45Kbps excluding the VPN tunnel header.
5. The maximum number of PPTP or L2TP VPN tunnels is 7.
6. The IPsec protocol IPCOMP is not supported by the router card.

DHCP Server:

1. The maximum number of DHCP IP addresses supported by the system is 128.