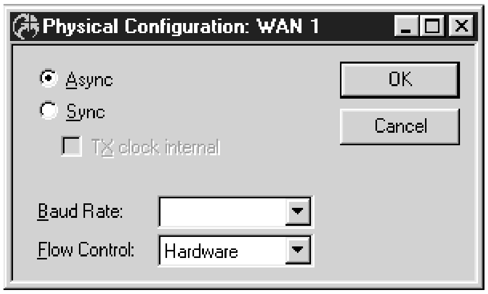
CHAPTER 14

General Configuration Windows

Physical EIA/TIA-232 Configuration: WAN Dialog Box

To access the Physical Configuration dialog box (Figure 14-1), select WAN/Physical Configuration from the Device View.

Figure 14-1 Physical EIA/TIA-232 Configuration: WAN Dialog Box



Physical Configuration: WAN 1

● Async
○ Sync
□ TX clock internal

Baud Rate:
Flow Control: Hardware

Async/Sync

This set of radio buttons determines whether this interface will use the asynchronous or synchronous mode of communication.

- If **Async** is selected, the interface will communicate asynchronously (using start and stop bits) with the device it is connected to. This mode of communication is typically used by modems.
- If **Sync** is selected, the interface will communicate synchronously (using a separate clock) with the device it is connected to. This mode of communication is typically used by CSU/DSUs and ISDN Terminal Adapters.

Interfaces set for asynchronous operation do not use parity, and use one stop bit.

Some high-speed WAN interfaces (i.e. V.35) may only support synchronous communications. This set of radio buttons will not appear in the Manager’s Physical Configuration: WAN dialog box for these interfaces.

Tx Clock Internal (Sync Only)

This parameter determines whether the interface will source a clock signal or expect to receive an external clock.

- If **checked**, the interface will expect to source a clock, and will ignore an external clock signal.
- If **unchecked**, the interface will expect to receive an external clock. This is the default setting.

In addition to this setting, some WAN interfaces require internal hardware jumpers to be changed in order to source a clock signal. Check the Installation Reference Guide for the device.

Baud Rate

This pull-down menu determines the speed of the port's internal clock. In **Async** operation, this value must match the baud rate of the external communications device. In **Sync** operation this value is ignored unless **Tx Clock Internal** is checked, in which case it determines the speed of the clock which is sourced.

Flow Control (Async Only)

This setting determines the type of flow control used on interfaces set for Async operation.

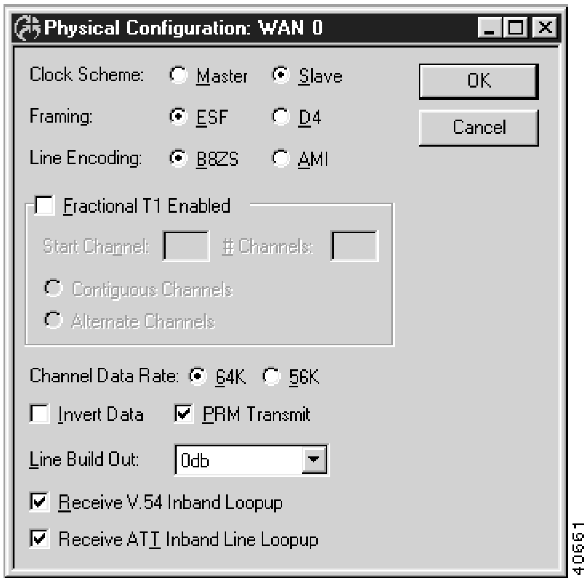
- If **none** is selected, the interface will not pace the rate at which it sends characters.
- If **hardware** is selected, the interface will use the state of the CTS (Clear To Send) line to determine whether characters may be sent. This is the default setting.
- If **XOn/XOff** is selected, the interface will trap XOn and XOff characters to determine whether characters may be sent. This method is also known as "software" flow control.

You may also need to configure your communications device (through switch settings or internal registers) to run with software flow control. Software flow control is **not** recommended at speeds above 9600 Baud.

Physical T1 Configuration: WAN Dialog Box

To access this dialog box (Figure 14-2), select WAN/Physical Configuration from the Device View.

Figure 14-2 Physical T1: WAN Configuration Dialog Box



Clock Scheme: ○ Master ● Slave

Framing: ● ESF ○ D4

Line Encoding: ● B8ZS ○ AMI

☐ Fractional T1 Enabled

Start Channel: # Channels:

○ Contiguous Channels

○ Alternate Channels

Channel Data Rate: ● 64K ○ 56K

☐ Invert Data ☑ PRM Transmit

Line Build Out: 0db

☑ Receive V.54 Inband Loopup

☑ Receive ATT Inband Line Loopup

Since many of the settings for a T1 line are dependent upon the service provided by your ISP or telco, you may need to contact them to find out the appropriate specifications. Unless otherwise noted, both ends of a T1 WAN connection should have the same physical configuration settings.

Clock Scheme

This set of radio buttons determines whether this interface will source clock onto the T1 line (dry line operation) or accept clock from an external source on a T1 line.

- If **Master** is selected, the interface will source clock onto the line.
- If **Slave** is selected, the interface will sync to the clock received on the line. The default setting is Slave.

Units connected to telco lines should always be set for slave mode. Units driving a dry line should have one end set to master and the other set to slave.

Framing

This parameter determines the type of T1 framing to be used on the interface. Both ends of a WAN connection must be configured with the same framing format

- If **ESF** is selected, the interface will expect extended superframe framing on the line. ESF is the preferred format because it offers a Facility Data Link which can provide performance monitoring, error checking and other features. ESF is the default.
- If **D4** is selected, the interface will expect the older D4 superframe framing. D4 may be the only framing format available in some areas.

Line Encoding

This parameter determines the type of T1 encoding to be used on the interface.

- If **B8ZS** is selected, the interface will expect this type of encoding on the line. With B8ZS, the **Channel Data Rate** should be set to 64 Kbps. This is the default setting.
- If **AMI** is selected, the interface will expect this type of encoding. With AMI, the **Channel Data Rate** should be set to 56 Kbps if the line is Full T1 or if **Contiguous** channels are being used on a Fractional T1 line. If **Alternate** channels are being used on a Fractional T1 line, then the **Channel Data Rate** can be set to 64 Kbps.

Fractional T1 Enabled

This checkbox enables fractional T1 operation, where the device's built-in CSU/DSU will not use all of the T1 channels in the T1 data stream.

Start Channel & Number of Channels

This pair of edit boxes determines which T1 channel the internal CSU/DSU will use as the beginning of its T1 fraction, and how many channels it will occupy.

Contiguous Channels or Alternate Channels

This set of radio buttons determine whether the T1 fraction will occupy every channel starting with the requested channel, or every other channel. If more than 12 channels will be used, the Contiguous Channels radio button must be selected.

- If **Contiguous** is selected, the T1 fraction will occupy every channel beginning at the Start Channel. This is the default setting.
- If **Alternate** is selected, the T1 fraction will occupy every other channel beginning at the Start Channel.

Channel Data Rate

These two radio buttons determine whether the internal CSU/DSU will use 64Kbps channels or 56Kbps channels. The default is 64Kbps.

Invert Data

This checkbox instructs the CSU/DSU to invert the data it transmits and to expect to receive inverted data on the line. This is sometimes done to insure ones density on the line. The default setting is unchecked.

PRM Transmit

This checkbox enables sending and receiving of Performance Report Messages (PRM) on the Facility Data Link (FDL). This is only possible when ESF framing has been selected. The default is enabled.

Line Build Out

This pulldown sets the expected signal range for the CSU/DSU's receiver. 0db is the default and will be satisfactory in virtually all telco applications. Other settings may be necessary for dry line applications.

Receive V.54 Inband Loopup

This checkbox instructs the CSU/DSU to respond to V.54 style loopup commands received over the line. The default setting is on.

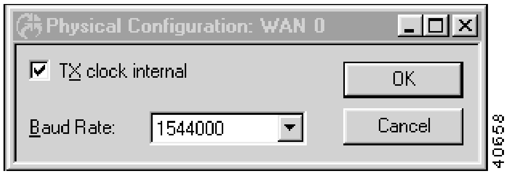
Receive ATT Inband Line Loopup

This checkbox instructs the CSU/DSU to respond to ATT 64211 style loopup commands received over the line. The default setting is on.

Physical V.35 Configuration: WAN Dialog Box

To access this dialog box (Figure 14-3), select WAN/Physical Configuration from the Device View.

Figure 14-3 Physical V.35 Configuration: WAN Dialog Box



Physical Configuration: WAN 0

☑ TX clock internal

Baud Rate: 1544000

Tx Clock Internal

This parameter determines whether the interface will source a clock signal or expect to receive an external clock.

- If **checked**, the interface will expect to source a clock, and will ignore an external clock signal.
- If **unchecked**, the interface will expect to receive an external clock. This is the default setting.

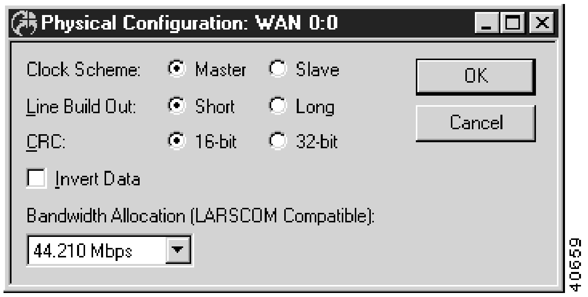
Baud Rate

This pull-down menu determines the speed of the port's internal clock when **Tx Clock Internal** is checked.

Physical DS3 Configuration: WAN Dialog Box

To access this dialog box (Figure 14-4), select WAN/Physical Configuration from the Device View.

Figure 14-4 Physical DS3 Configuration: WAN Dialog Box



Physical Configuration: WAN 0:0

Clock Scheme: ● Master ○ Slave

Line Build Out: ● Short ○ Long

CRC: ● 16-bit ○ 32-bit

□ Invert Data

Bandwidth Allocation (LARSCOM Compatible):

44.210 Mbps

Clock Scheme

These radio buttons set whether the DSU will use its own internal clock or obtain the clock from the network to use for the DSU’s DS3 transmit signal towards the network.

- **Master** means an internal clock will be used.
- **Slave** means the clock derived from the DS3 receive signal will be used. This is the default setting.

Line Build Out

These radio buttons should be set based on the distance between the device and the DS3 terminal located in your building.

- **Short** should be used for cable lengths from 0 - 100 feet.
- **Long** should be used for cable lengths from 101 - 900 feet.

CRC

These radio buttons control whether the DSU will use a 16-bit or 32-bit frame check sequence. Both ends of a DS3 connection must use the same CRC (Cyclical Redundancy Check) setting. The default is **16 bit**.

Invert Data

This checkbox determines whether data will be inverted. Data inversion can be used to meet pulse density requirements. Always leave this unchecked unless otherwise instructed by your ISP.

- If **checked**, data will be inverted. If a DSU at one end of a DS3 line inverts its data, then the DSU at the other end must do the same.
- If **unchecked**, data will not be inverted. This is the default setting.

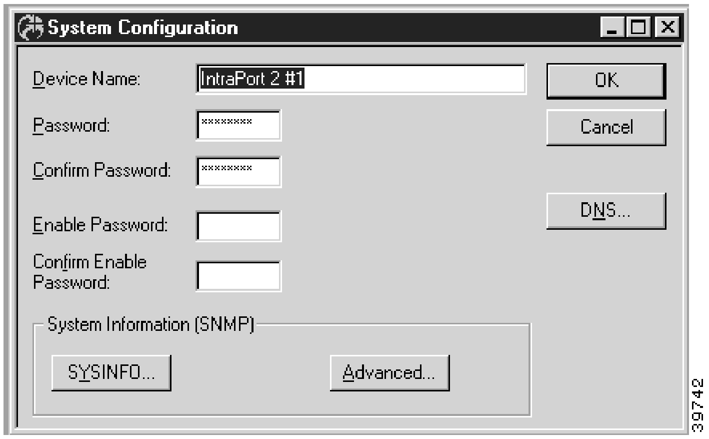
Bandwidth Allocation

This pull-down menu allows you to select the data rate for the CSU/DSU. This can be used to set the throughput to match the bandwidth provided by your NSP (Network Service Provider). The values are specified in megabits per second, using an underscore (_) as the decimal point (e.g., 3_158 is 3.158 Mbps). Both ends of the DS3 connection must have the same rate specified. Unless the remote end is a Larscom CSU/DSU (or equivalent) or another Cisco VPN 5000 series DS3 interface, the default setting of **44_210** must be used.

System Configuration Dialog Box

To access this dialog box (Figure 14-5), select Global/System Configuration from the Device View.

Figure 14-5 System Configuration Dialog Box



Device Name: IntraPort 2 #1

Password: ********

Confirm Password: ********

Enable Password:

Confirm Enable Password:

Device Name

This is the name which is used to advertise this device on both AppleTalk and IPX networks. Thus, it is the name the VPN 5000 Manager displays in the Open - Device screen (accessed from the File menu).

Password

This is the main password used to access the device from the Manager and from the command line (either Telnet or auxiliary port operation). This login level will allow a user to display tables and statistics, but does not permit a user to view or make any changes to the configuration.

If you lose the password for this device, you can enable the default **letmein** password for five minutes by setting the switch marked “Test” or “Mode” on the back of the device to 9 and restarting the device. Make sure you set the switch back to 0 after you have set a new password into the device.

Confirm Password

This box is used to confirm the entered **Password**.

Enable Password

This password will enable supervisor mode for viewing or making changes to a device's configuration. If no **Enable Password** is created, then the **Password** will be used.

Confirm Enable Password

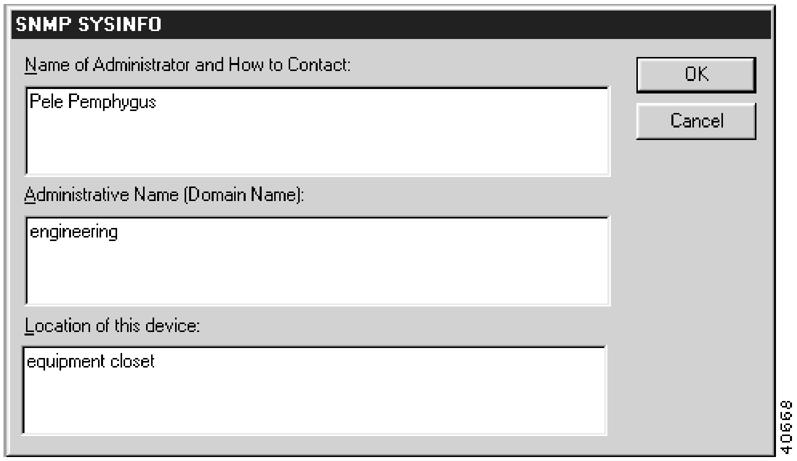
This box is used to confirm the entered **Enable Password**.

SNMP Configuration

SNMP System Info Configuration Dialog Box

To access this dialog box (Figure 14-6), select Global/System Configuration from the Device View, and then select the **SYSINFO** button.

Figure 14-6 SNMP System Info Configuration Dialog Box



SNMP SYSINFO

Name of Administrator and How to Contact: Pele Pemphygus

Administrative Name (Domain Name): engineering

Location of this device: equipment closet

The information in this dialog box is returned by the device in response to SNMP (Simple Network Management Protocol) queries from SNMP consoles for the SNMP MIB-II System Group, as specified in RFC 1213. Each of the entries may be up to 255 characters.

Name of Administrator and How to Contact

This is the name of the contact person for this device, together with information on how to contact the administrator.

Administrative Name

This is the administratively assigned name for this device. By convention, this is the fully qualified domain name for the device.

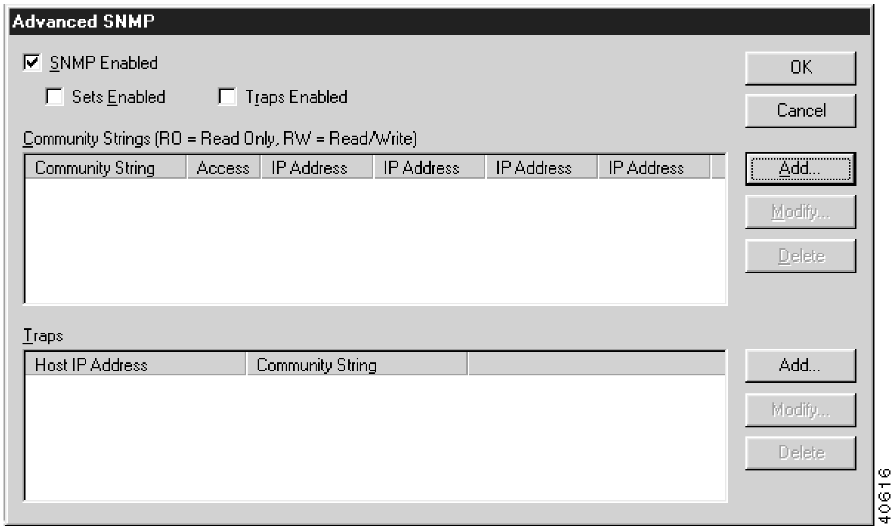
Location of this device

This is the physical location of the device (e.g. telephone closet, 3rd floor).

Advanced SNMP Configuration Dialog Box

To access this dialog box (Figure 14-7), select Global/System Configuration from the Device View, and then select the **SYSINFO** button.

Figure 14-7 Advanced SNMP Configuration Dialog Box



Advanced SNMP

☑ SNMP Enabled

□ Sets Enabled □ Traps Enabled

Community Strings (RO = Read Only, RW = Read/Write)

Community String	Access	IP Address	IP Address	IP Address	IP Address

Traps

Host IP Address	Community String

To access this dialog box, select Global/System Configuration from the Device View, and then select the **ADVANCED** button.

This dialog box displays Community Strings and Traps, but is not used to add or modify the entries.

To add or modify entries, you must access the Community Strings and/or Traps dialog boxes by selecting the **Add...** or **Modify...** buttons in the Advanced SNMP Configuration dialog box.

SNMP Enabled

This checkbox controls whether Advanced SNMP management of the device can be done.

Sets Enabled

This checkbox controls whether SNMP Sets can be done to the device.

Traps Enabled

This setting controls whether SNMP Traps will be done by the device when trap conditions are encountered.

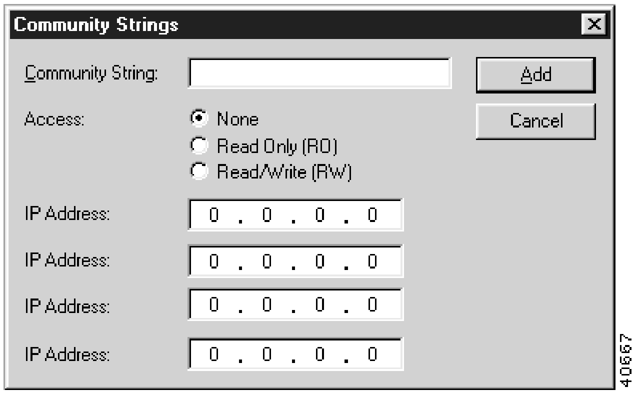
This device supports the following SNMP Traps (as outlined in RFC 1157):

- **coldStart** - this will be generated when a restart to save a configuration or software download is accomplished.
- **warmStart** - this will be generated when a restart event is received.
- **linkDown** - this will be generated from a WAN interface when a link is dropped due to abnormal conditions, such as lost carrier, lost PVC, etc.
- **linkUp** - this will be generated from a WAN interface when a link which was lost due to abnormal conditions comes back up.
- **authenticationFailure** - this will be generated when a protocol message is not properly authenticated.

SNMP Community Strings Configuration Dialog Box

To access this dialog box (Figure 14-8), select **Add** or **Modify** in the Community Strings section of the Advanced SNMP dialog box.

Figure 14-8 SNMP Community Strings Configuration Dialog Box



Community Strings

Community String:

Access: ● None ○ Read Only (RO) ○ Read/Write (RW)

IP Address: 0 . 0 . 0 . 0

IP Address: 0 . 0 . 0 . 0

IP Address: 0 . 0 . 0 . 0

IP Address: 0 . 0 . 0 . 0

Community String

This is the string associated with the administrator(s) who have access to the SNMP console. It is included in every message and is used, along with the IP address(es) configured for access authentication.

Access

This set of radio buttons controls the type of access the administrator(s) within the Community String will have to this device.

- **None** - no access.

- **Read Only (RO)** - receives information such as Traps, but can not do Sets.
- **Read/Write (RW)** - can perform Sets to, and receive Traps from, this device.

IP Address

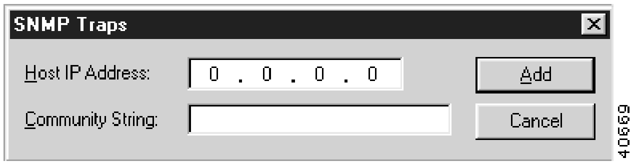
This is the IP address, or addresses, of the SNMP console. The address is used, along with the Community String, for access authentication. Up to four IP addresses may be entered.

They should be entered in standard IP dotted-decimal notation (e.g. 198.41.9.1). An address with all zeros (0.0.0.0) can be used as a wildcard to allow the Community String access from any console.

SNMP Traps Configuration Dialog Box

To access this dialog box (Figure 14-9), select **Add** or **Modify** in the Traps section of the Advanced SNMP dialog box.

Figure 14-9 SNMP Traps Dialog Box



SNMP Traps

Host IP Address: 0 . 0 . 0 . 0

Community String:

Host IP Address

This is the IP address of the SNMP console to which the device will transmit a Trap message whenever one is generated.

It should be entered in standard IP dotted-decimal notation (e.g. 198.41.9.1).

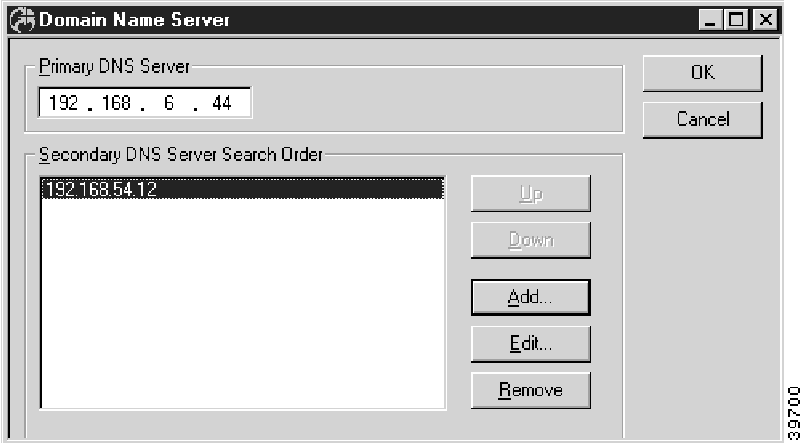
Community String

This is the Community String on the SNMP console to which the Trap message will be sent.

Domain Name Server (DNS) Dialog Box

To access this dialog box (Figure 14-10), select Global/Domain Name Server from the device view.

Figure 14-10 Domain Name Server Dialog Box



Domain Name Server

Primary DNS Server: 192 . 168 . 6 . 44

Secondary DNS Server Search Order: 192.168.54.12

DNS allows the device to report DNS names instead of raw IP addresses when using the **Traceroute** command, and also allows the **Ping** command to be optionally issued with a DNS name.

The Traceroute and Ping commands themselves are not supported from the VPN 5000 Manager. To access these commands, use the command line interface via Telnet or the Console port.

Primary DNS Server

This is the IP address of the DNS server which should be queried first for the identity of a name or an IP address.

This address should be entered directly into the edit box as four decimal numbers separated by periods – for example 198.238.9.1

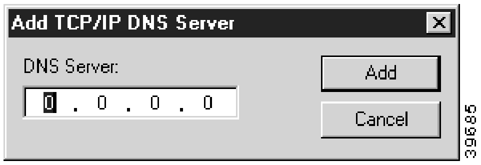
Secondary DNS Server Search Order

These are the IP addresses of other DNS servers which should be queried for the identity of a name or an IP address.

Use the **Move Up** and **Move Down** buttons to manipulate the addresses in this list.

To add or modify this list, click on the appropriate button to access the Add TCP/IP DNS Server dialog box (Figure 14-11).

Figure 14-11 Add TCP/IP DNS Server



Add TCP/IP DNS Server

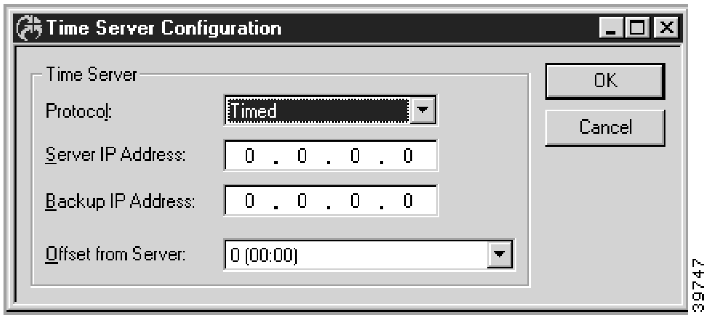
DNS Server: 0 . 0 . 0 . 0

Enter the IP address of other DNS servers which should be queried for the identity of a name or an IP address.

Time Server Dialog Box

To access this dialog box (Figure 14-12), select Global/Time Server Configuration from the Device View.

Figure 14-12 Time Server Configuration Dialog Box



Protocol: Timed

Server IP Address: 0 . 0 . 0 . 0

Backup IP Address: 0 . 0 . 0 . 0

Offset from Server: 0 (00:00)

This dialog box is used to enable the setting of the device's internal clock from a network time server. The device's time server will connect to most UNIX systems running "inetd" using either the time server port (UDP 37) or NTP port (UDP 123). Automatic daylight savings adjustment is not supported.

Protocol

This pulldown identifies the type of time server protocol to use. In most cases, the time server being used will dictate the protocol type. UNIX servers generally use **Timed**. Windows servers generally use **SNTP** (Simple Network Time Protocol). The default is Timed.

Server IP Address

This field is used to specify the IP address of the primary time server. It is recommended that you use a time server which is local to your network.

Backup IP Address

This field is used to specify the IP address of the backup time server. All time requests go to the primary server first. If there is no response the backup will be used. This address is optional.

Offset from Server

Most time servers return GMT. You can use this option to set the device to local time. Accepted values range from -720 to 720 minutes.

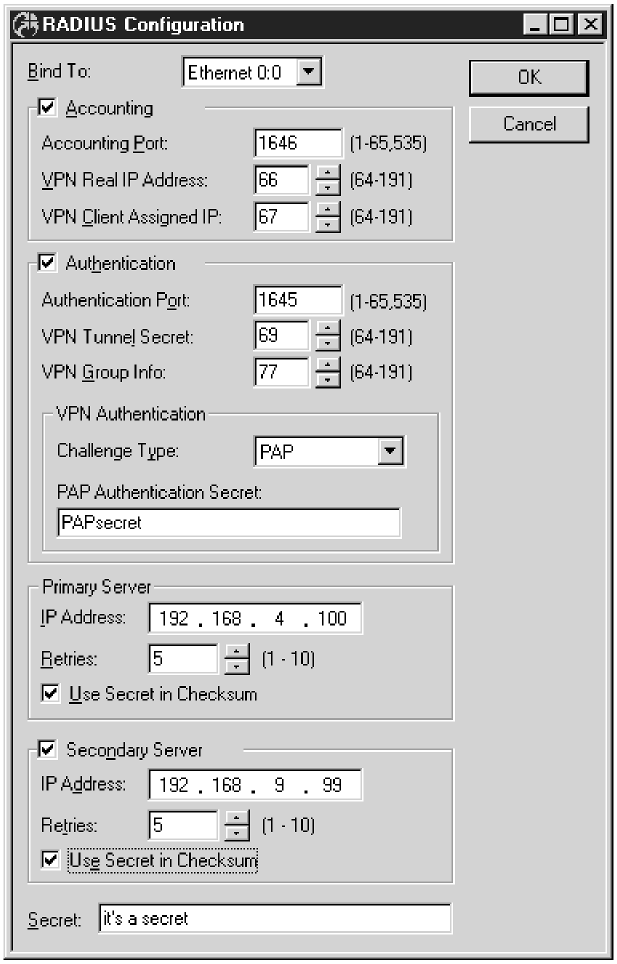
RADIUS Configuration Dialog Box

RADIUS (Remote Authentication Dial In User Service) can be used for remote access authentication using PAP or CHAP and for remote access accounting. The device acts as a client and exchanges packets with a RADIUS server running on an external host computer.

The device can be configured with a primary and a secondary server. If the device is unable to reach the primary server, it will attempt to use the secondary server if one has been configured.

To access this dialog box (Figure 14-13), select Global/RADIUS from the Device View.

Figure 14-13 RADIUS Configuration Dialog Box



RADIUS Configuration

Bind To: Ethernet 0:0

☑ Accounting

Accounting Port: 1646 (1-65,535)

VPN Real IP Address: 66 (64-191)

VPN Client Assigned IP: 67 (64-191)

☑ Authentication

Authentication Port: 1645 (1-65,535)

VPN Tunnel Secret: 69 (64-191)

VPN Group Info: 77 (64-191)

VPN Authentication

Challenge Type: PAP

PAP Authentication Secret: PAPsecret

Primary Server

IP Address: 192 . 168 . 4 . 100

Retries: 5 (1 - 10)

☑ Use Secret in Checksum

☑ Secondary Server

IP Address: 192 . 168 . 9 . 99

Retries: 5 (1 - 10)

☑ Use Secret in Checksum

Secret: it's a secret

RADIUS servers are available in the public domain, and can also be purchased from a variety of commercial suppliers.

Bind To

This pulldown allows the selection of an interface on the device. The interface selected will act as the local end point for the tunnels defined by this configuration.

Accounting

This setting determines whether the device will attempt to exchange user accounting information with a RADIUS server.

- If **checked**, each time a user logs into the device, a record of their login is sent to the RADIUS server where it is catalogued.

Accounting Port

This edit box allows you to set the UDP port on the RADIUS server(s) on which accounting information will be exchanged. The default is 1646.

VPN Real IP Address

This value sets the attribute number for the reporting of the actual IP address of a VPN 5000 concentrator user. This attribute number must also be set up in the RADIUS server's dictionary file. If this number has been set both here and in the RADIUS server's dictionary file, then the actual IP address of a user will be reported by the VPN Client software and will be recorded by the RADIUS server. The value may range between 64 and 191. The default is 66.

VPN Client Assigned IP

This value sets the attribute number for the reporting of the IP address which the concentrator assigns to a concentrator user. This attribute number must also be set up in the RADIUS server's dictionary file. If this number has been set both here and in the RADIUS server's dictionary file, then the assigned IP address will be reported by the VPN Client software and will be recorded by the RADIUS server. The value may range between 64 and 191. The default is 67.

Authentication

This setting determines whether the device will exchange user authentication information with a RADIUS server.

- If **checked**, user authentication information will be exchanged.

Authentication Port

This edit box allows you to set the UDP port on the RADIUS server(s) on which authentication information will be exchanged. The default is 1645.

VPN Tunnel Secret

This value sets the attribute number for the VPN tunnel secret. The tunnel secret is a shared secret between the VPN Client and the RADIUS server which is used for authentication of tunnel connections. This attribute number must also be set up in the RADIUS server's dictionary file. The value may range between 64 and 191. The default is 69.

VPN Group Info

This value sets the attribute number for the VPN group configuration. The group configuration defines tunneling profiles for a group of one or more VPN Client users. This attribute number must also be set up in the RADIUS server's dictionary file. The value may range between 64 and 191. The default is 77.

VPN Authentication

Challenge Type

This pulldown menu sets the authentication protocol to be used for validation of remote VPN Client users to the RADIUS server.

- If **CHAP** is selected, CHAP will be used to validate remote VPN Client users to the RADIUS server.
- If **PAP** is selected, PAP will be used to validate remote VPN Client users to the RADIUS server. This should only be used for an older RADIUS server which does not support CHAP authentication.
- If **Challenge** is selected, The RADIUS server is notified of a login attempt before contacting the client. The RADIUS server is expected to respond with a RADIUS challenge which is passed on to the client.

PAP Authentication Secret

This is the secret used to authenticate and encrypt packets before they are passed on to the RADIUS server. The PAP authentication secret can be a string from 1 to 255 ASCII characters in length.

Primary Server

Primary Server IP Address

The device will attempt to contact this RADIUS server first when it needs to exchange RADIUS information. The address should be entered in dotted-decimal notation (e.g. 198.238.41.7).

Primary Server Retries

The device will try to resend a packet if the primary RADIUS server doesn't acknowledge it within a timeout period. The timeout period for packets 1 through 10 is (in seconds): 1, 1, 2, 2, 3, 3, 4, 4, 5, 5.

If the retry limit is reached and a secondary server is configured, the device will attempt to communicate with the secondary server.

Possible values range between 1 and 10 with a default of 5.

Use Secret in Checksum

Some RADIUS servers calculate packet validation checksums using both the secret value and the packet data. Earlier RADIUS servers typically do not. Check the documentation for your RADIUS server to determine whether this parameter should be set.

- If **checked**, packet checksums will be calculated using both the data and the checksum.

Secondary Server

The device may be configured to use a secondary server if the primary server cannot be contacted.

- If **checked**, a secondary server can be configured and will be used in the event the primary server cannot be contacted.

Secondary Server IP Address

The device will attempt to contact this RADIUS server if the primary server does not respond after the configured number of primary server retries. The address should be entered in dotted-decimal notation (i.e. 198.238.41.7).

Secondary Server Retries

The device will try to resend a packet if the secondary RADIUS server doesn't acknowledge it within a timeout period. The timeout period for packets 1 through 10 is (in seconds): 1, 1, 2, 2, 3, 3, 4, 4, 5, 5.

Possible values range between 1 and 10 with a default of 5.

Use Secret in Checksum

Some RADIUS servers calculate packet validation checksums using both the secret value and the packet data. Earlier RADIUS servers typically do not. Check the documentation for your RADIUS server to determine whether this parameter should be set.

- If **checked**, packet checksums will be calculated using both the data and the checksum.

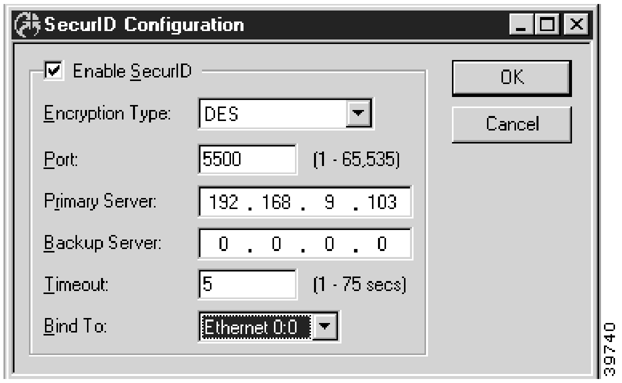
Secret

The secret is the shared secret used by the device and RADIUS server to validate packets exchanged between them. This secret must match the client secret configured in the RADIUS server. It can be from 1 to 31 ASCII characters in length.

SecurID Configuration Dialog Box

To access this dialog box (Figure 14-14), select Global/SecurID from the Device View.

Figure 14-14 SecurID Configuration Dialog Box



☑ Enable SecurID

Encryption Type: DES

Port: 5500 (1 - 65,535)

Primary Server: 192 . 168 . 9 . 103

Backup Server: 0 . 0 . 0 . 0

Timeout: 5 (1 - 75 secs)

Bind To: Ethernet 0:0

All VPN 5000 concentrators and the VPN 5000 Client software are SecurID-ready. SecurID is Security Dynamic's proprietary system which requires ACE/Server software and SecurID tokens to perform dynamic two-factor authentication.

Enable SecurID

This checkbox determines whether SecurID authentication will be performed by the device.

Port

This edit box allows you to set which UDP port on the ACE/Server will be used to exchange information. The default is 5500. The value may range between 1 and 65,535.

Encryption Type

This edit box allows you to select the encryption algorithm for data exchanged between the concentrator and the ACE/Server. **DES** specifies that the DES algorithm will be used to scramble the data in both directions. **SDI** specifies that Security Dynamic's propriety algorithm will be used. The default is **DES**.

Primary Server

The device will attempt to contact this SecurID server first when attempting to authenticate a user. The address should be entered in dotted-decimal notation (i.e. 198.238.41.7).

If the timeout period is reached and a secondary server is configured, the device will attempt to communicate with the backup server.

Backup Server

The device will attempt to contact this SecurID server if the primary server does not respond after the configured timeout period. The address should be entered in dotted-decimal notation (i.e. 198.238.41.7).

Timeout

This is the number of seconds the device will wait before trying the backup ACE/Server. The default is 5. The value may range between 1 and 75.

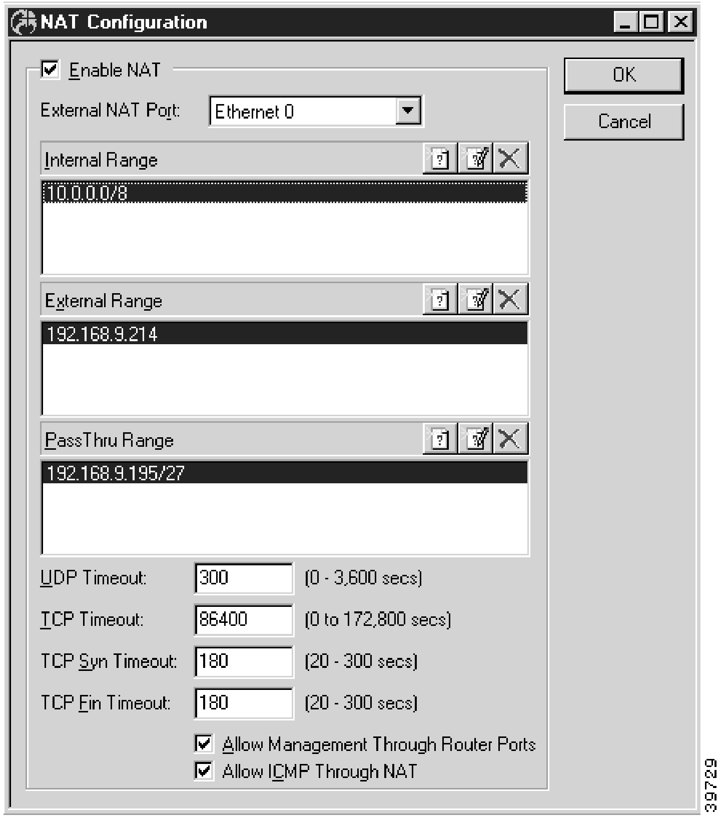
Bind To

This pulldown allows the selection of an interface on the device. The interface selected will act as the local end point for the tunnels defined by this configuration.

NAT Configuration Dialog Box

To access this dialog box (Figure 14-15), select Global/NAT Configuration from the Device View.

Figure 14-15 NAT Configuration Dialog Box



NAT Configuration

☑ Enable NAT

External NAT Port: Ethernet 0

Internal Range: 10.0.0.0/8

External Range: 192.168.9.214

PassThru Range: 192.168.9.195/27

UDP Timeout: 300 (0 - 3,600 secs)

TCP Timeout: 86400 (0 to 172,800 secs)

TCP Syn Timeout: 180 (20 - 300 secs)

TCP Fin Timeout: 180 (20 - 300 secs)

☑ Allow Management Through Router Ports

☑ Allow ICMP Through NAT

NAT allows internal networks which use private IP addresses to be translated into a valid external “global” IP address (or addresses). (See RFC 1918 "Address Allocation for Private Internets" for more information about private IP addresses.) This can allow a private network to provide Internet access through a single "official" IP address. It can also function as a minimal firewall by limiting access to the internal network from external networks while allowing the internal network easy access to the Internet.

Enable NAT

This checkbox enables NAT globally for this device.

External NAT Port

Select the External NAT Port from this pull-down menu.

Internal Range

This is the address range of the internal NAT network. This range will be translated into the range of IP addresses defined by the External Range. Any interface or subinterface on the device which is part of the same network as the Internal Range is considered to be an internal NAT port.

This window displays a list of all entered Internal Range but is not used to add or modify the entries. To add or modify the entries, you must access the NAT Map dialog box by selecting the **New** or **Modify** buttons above the Internal Range window.

External Range

This is the address range of the external NAT network. This range will be translated into the range of IP addresses defined by the Internal Range. The address or range of addresses specified must be a valid, globally recognized Internet address (or addresses) which can be routed on the network.

If only a single Internet IP address is available, then the **External Range** must be the same as the IP address on the IP port communicating with the Internet. In this case, care must be taken not to create a one-to-one translation pair using this IP address in the NAT Mapping dialog box (under Global/Nat Mapping). If a range of addresses is specified, the NAT software makes the decision about which Internet address is assigned to outgoing packets.

This window displays a list of all entered External Range but is not used to add or modify the entries. To add or modify the entries, you must access the NAT Map dialog box by selecting the **New** or **Modify** buttons above the External Range window.

PassThru Range Addresses

This is the address range which may pass through the external NAT port without being translated. This is used when the NAT router has an IP interface (or interfaces), in addition to the NAT internal port and NAT external port, which is connected to part of the local network which is configured with global IP addresses.

If an IP address or range of addresses is included in both the **External Range** and **PassThru Range**, NAT will treat the IP address(es) as being members of the **External Range** only.

This window displays a list of all entered PassThru Range but is not used to add or modify the entries. To add or modify the entries, you must access the NAT Map dialog box by selecting the **New** or **Modify** buttons next to the PassThru Range window.

TCP Timeout

This edit box allows you to set the amount of time to lapse without any IP Network Address Translations using this NAT session before the router removes an active NAT session for TCP. The value may range from 0 to 172,800 seconds (48 hours). A value of zero will cause TCP NAT sessions to never be removed due to inactivity. Extending the amount of time will cause more router memory to be used by the NAT translation session database. The default is 86,400 seconds (24 hours).

UDP Timeout

This edit box allows you to set the amount of time to lapse without any IP Network Address Translations using this NAT session before the router removes an active non-TCP NAT session. The value may range from 0 to 3600 seconds (1 hour). A value of zero will cause non-TCP NAT sessions to never be removed due to inactivity. Extending the amount of time will cause more router memory to be used by the NAT translation session database. The default is 300 seconds (5 minutes).

TCP Syn Timeout

This edit box allows you to set the amount of time to lapse without a response to a SYN TCP packet before the router removes an active NAT session for TCP. The value may range from 20 to 300 seconds. The default is 180 seconds (3 minutes).

TCP Fin Timeout

This edit box allows you to set the amount of time to lapse without a response to a FIN TCP packet before the router removes an active NAT session for TCP. The value may range from 20 to 300 seconds. The default is 180 seconds (3 minutes).

Allow Management Through Router Ports

This checkbox allows communication with the router through the IP addresses of the router's ports. This allows the user to communicate with the router (e.g., establish a telnet session with the router). The default is **checked**.

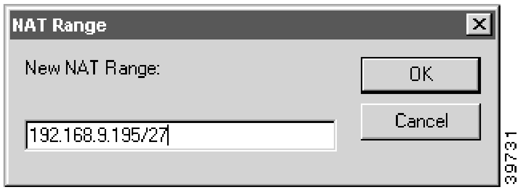
Allow ICMP Through NAT

This checkbox allows external workstations/routers to ping workstations/routers in the internal NAT network if a one-to-one translation pair allowing such a translation has been set using the NAT Mapping dialog box. The default is **checked**. The workstation/router on the internal NAT network will not be allowed to respond to a ping if this parameter is **unchecked**.

NAT Range Dialog Box

To access the NAT Range dialog box (Figure 14-16), select the **New** or **Modify** buttons in the NAT Configuration dialog box (under Global/NAT Configuration).

Figure 14-16 NAT Range Dialog Box



192.168.9.195/27

This dialog box allows you to enter a NAT address range. It can be a single IP address or a range of addresses.

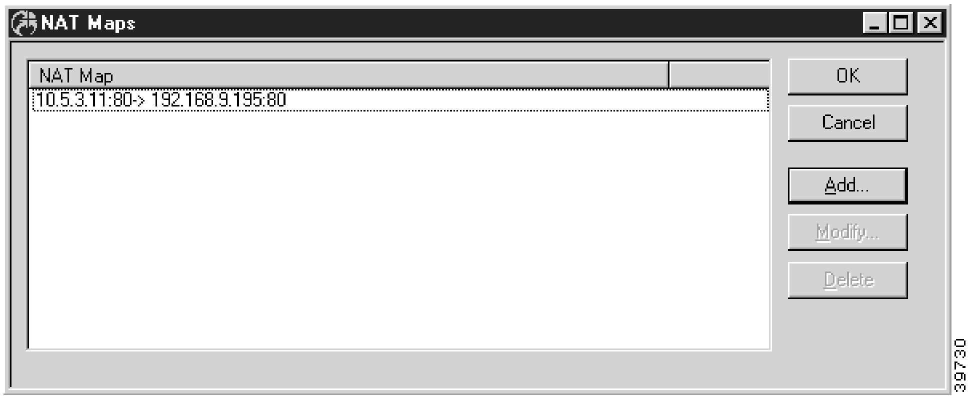
The address range may be specified in several different ways:

- Addresses can be specified in normal dotted-decimal notation. If the rightmost components are 0, they are treated as wild cards (e.g., 128.138.12.0 matches all hosts on the 128.138.12 subnet).
- An inclusive range of addresses can be specified using a "dash notation" in the form of #.#.#.{# -#}. For example, 10.5.3.{1-30} would be parsed as the IP addresses 10.5.3.1, 10.5.3.2,..... 10.5.3.29, and 10.5.3.30 (and every IP address in between). Each of these parsed addresses would have a mask of /32 or 255.255.255.255
- Addresses may also be specified as a hexadecimal number (e.g., 0x82cc0801 matches the host address 130.204.8.1).
- A bit field can also be used to indicate a range of addresses by denoting the top or most significant bits which define the range. For example, an address specified as 192.15.32.0/19 would indicate a range from 192.15.32.1 to 192.15.63.255.

NAT Maps Window

To access the NAT Maps window (Figure 14-17), select Global/NAT Maps from the Device List.

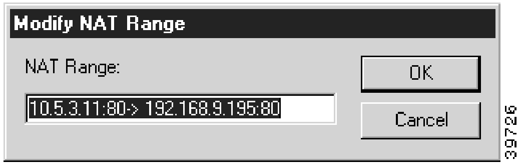
Figure 14-17 NAT Maps Window



NAT Map
10.5.3.11:80-> 192.168.9.195:80

This window displays a list of all entered one-to-one NAT Mapping translation pairs. To add or modify the entries, access the NAT Range dialog box (Figure 14-18) by selecting the **Add...** or **Modify...** buttons.

Figure 14-18 Modify NAT Range Dialog Box



Modify NAT Range

NAT Range: 10.5.3.11:80-> 192.168.9.195:80

These one-to-one translation pairs allow the user to provide access from the internal or external network to selected parts of the NAT internal network, such as a web server.

Each translation pair must be entered using the following syntax:

```
<internal IP address> [ /<bits> | :<port>  ] [ ->  |  = ] <external IP address>  [
/<bits> | :<port> ]
```

<internal IP address>
This is the IP address on the internal network to be mapped to the external IP address. It must be entered first, followed by " -> " or " = " and the external IP address. The *internal IP address* must be within the range (or ranges) of IP addresses defined by the **Internal Range Addresses**. IP addresses must be specified in normal dotted-decimal notation. If the rightmost components are 0, they are treated as wild cards (e.g., 128.138.12.0 includes all devices on the 128.138.12 subnet).

<external IP address>
This is the IP address on the external network to be mapped to the internal IP address. The *external IP address* must be within the range of IP addresses defined by the **External Range Addresses**.

If only a single external IP address is available for the NAT router, do **not** map that IP address to an internal IP address because you will no longer be able to communicate with the router. Mapping single ports of the single external IP address to internal IP address:port combinations (e.g., creating access to a web server in the internal NAT network) is acceptable, however.

:*<port>*

The :*port* option allows an individual socket (IP address and port combination) to be mapped as part of a translation pair.

An IP address:port combination cannot be paired with an IP address range (even if that range is a single IP address). It can only be paired with another IP address:port combination.

/*<bits>*

The */bits* option allows a range of IP addresses to be mapped as part of a translation pair. The *bits* field denotes the top or most significant bits which define the range. For example, an address specified as 192.15.32.0/19 would indicate a range from 192.15.32.1 to 192.15.63.255.

NAT Mapping Translation Pair Examples

The following example shows one IP address being translated into another.

```
[ NAT Mapping ]
10.5.3.20 -> 198.41.9.194
```

The following example shows individual sockets (IP address and port combination) being mapped as a translation pair.

```
[ NAT Mapping ]
10.5.3.10:80 -> 198.41.9.195:80
```

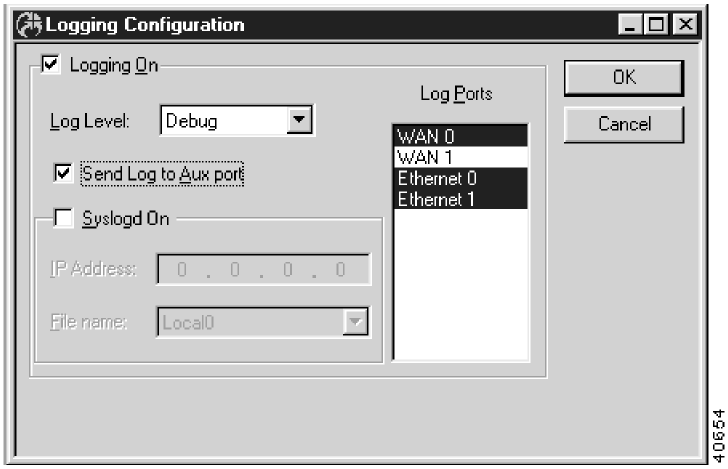
The following example shows a range of IP addresses being mapped as a translation pair.

```
[ NAT Mapping ]
10.5.3.0/29 -> 198.41.9.200/29
```

Logging Configuration Dialog Box

To access this dialog box (Figure 14-19), select Logging from the Device View.

Figure 14-19 Logging Configuration Dialog Box



Logging Configuration

☑ Logging On

Log Level: Debug

☑ Send Log to Aux port

□ Syslogd On

IP Address: 0 . 0 . 0 . 0

File name: Local0

Log Ports

WAN 0
WAN 1
Ethernet 0
Ethernet 1

Logging On

This setting determines whether the internetworking device will output logging information via any of the possible output methods. Logging is on by default.

Log Level

This pull-down menu selects the detail of the logging information provided.

- The **Notice** setting provides information that may be useful on a day-to-day basis by an administrator but generally does not require any response. Examples include login/logout, serial line resets, and LAN-to-LAN connections. This is the default setting and is suitable for most conditions.
- The **Emergency** level means that you will receive logging information only when the system is unusable. These log messages will help indicate the source of the problem.
- The **Alert** level reports only alert and emergency messages. An alert message requires immediate attention.
- The **Critical** level outputs critical, alert, and emergency messages. A critical condition requires imminent action.
- **Error** messages include exception cases pertaining to violations of protocols or other operational rules. Such violations may include illegal packets and improper command syntax.

- If **Warning** messages are repeated, they require a response. Examples of warning-level messages include network number conflicts and resource allocation problems.
- The **Info** option reports routine information, such as WAN network connect and disconnect messages.
- The **Debug** option logs every action of the device and should not be used on a day-to-day basis since it generates a large number of log messages.

Send Log to Aux Port

This checkbox determines whether the auxiliary port will receive logging messages.

Syslogd On

This checkbox determines whether the logging messages will be sent to a UNIX host system running the syslog daemon.

IP Address (Syslogd On Only)

This is the IP address of the UNIX system which is running the syslog daemon, in dotted-decimal notation (i.e. 198.238.41.7).

File (Syslogd On Only)

This pull-down menu determines which syslogd file the device's logging messages will be written into.

Log Ports

This list shows the ports for which logging information will be generated. If an interface is highlighted, logging information will be generated for that interface. To select or deselect more than one interface, press Control while clicking on the interface.

LDAP Configuration

This section configures LDAP (Lightweight Directory Access Protocol) parameters into a device. LDAP can be used to serve configurations to any Cisco VPN 5000 series device. LDAP configuration server settings are set in the LDAP Server dialog box.

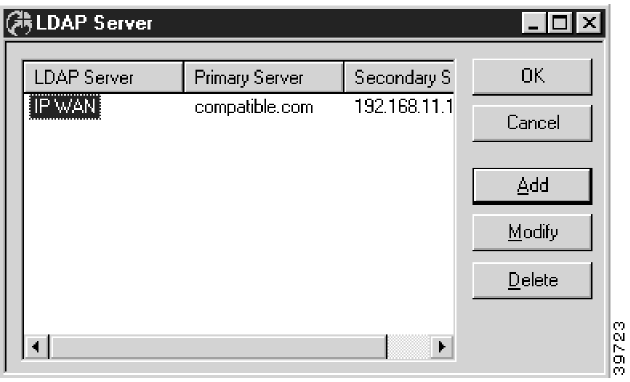
LDAP can also be used for VPN user authentication. LDAP user authentication is configured with the LDAP Authentication dialog box.

LDAP Server Dialog Box

Each LDAP configuration specifies an LDAP server and information about the configuration to be served. The configuration can be a full device configuration, or just a portion of one. When new configurations are added, the device's configuration is rebuilt to include the one that was just added.

This dialog box displays a list of previously defined LDAP configuration servers.To access this dialog box (Figure 14-20), select Global/LDAP Server from the Device View.

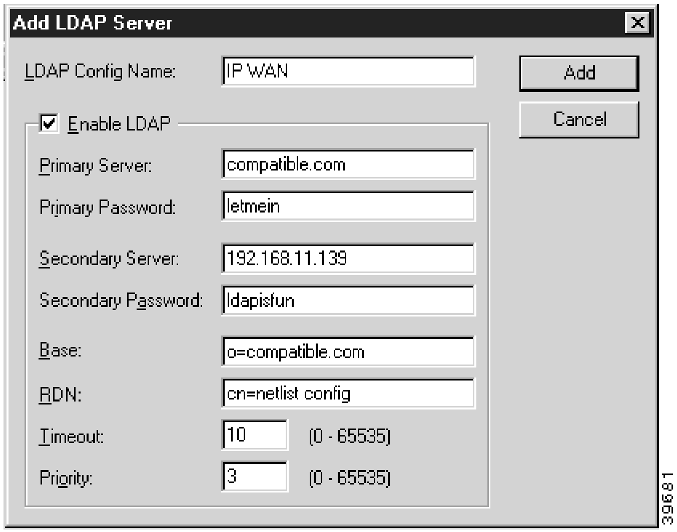
Figure 14-20 LDAP Server Dialog Box



LDAP Server	Primary Server	Secondary S
IP WAN	compatible.com	192.168.11.1

To add to or modify this list, click on the appropriate button to open the Add LDAP Server dialog box (Figure 14-21).

Figure 14-21 Add LDAP Server Dialog Box



LDAP Config Name: IP WAN

☑ Enable LDAP

Primary Server: compatible.com

Primary Password: letmein

Secondary Server: 192.168.11.139

Secondary Password: ldapisfun

Base: o=compatible.com

RDN: cn=netlist config

Timeout: 10 (0 - 65535)

Priority: 3 (0 - 65535)

LDAP Config Name

This specifies a name which uniquely defines this LDAP configuration. It can be up to 16 characters long.

Enable LDAP

This checkbox enables this entire section. If checked, the settings from this section will be used to get a configuration from an LDAP server. If left unchecked, no settings from this section will be used.

Primary Server

This sets the IP address (e.g., 192.168.9.99) or fully qualified domain name (e.g., monkeywrench.com) of the primary LDAP server which contains the configuration.

Primary Password

This string is used to authenticate the device to the primary LDAP server. If this is not set, then the device will attempt an anonymous bid to the server. The Primary Password may be up to 32 characters long.

Secondary Server

This sets the IP address (e.g., 192.168.9.99) or fully qualified domain name (e.g., monkeywrench.com) of the secondary LDAP server which contains the configuration.

Secondary Password

This string is used to authenticate the device to the secondary LDAP server. If this is not set, then the device will attempt an anonymous bid to the server. The Secondary Password may be up to 32 characters long.

Base

This specifies the portion of the LDAP tree where the configuration is located.

RDN

This string specifies the relative distinguished name used in the LDAP server to identify the entry which contains the configuration.

Timeout

This value is the number of seconds the device will wait for a response from the LDAP server.

Priority

This value specifies which configurations take precedence. When new configurations are added, the device’s configuration is rebuilt to include the one that was just added.

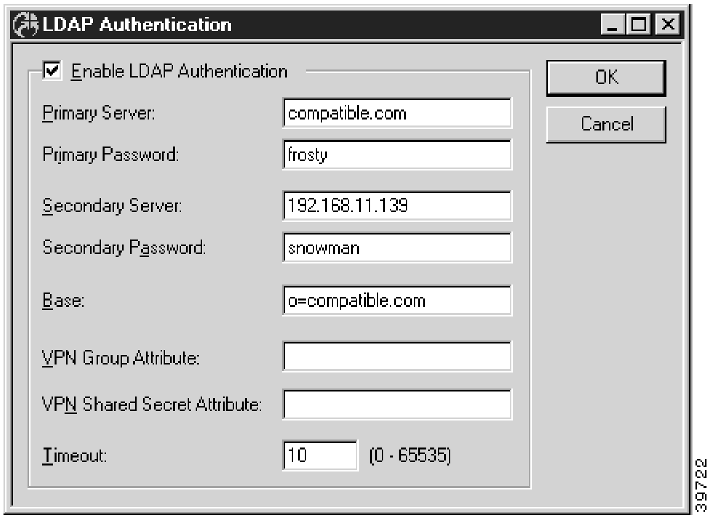
If a new configuration contains a section which contains a higher priority than one already in place, the new configuration (or configuration portion) is added above the one that is already there. This enables higher priority sections to take precedence.

LDAP Authentication Dialog Box

LDAP authentication is done only if the user cannot be found in the VPN User Authentication Database first. The device acts as a client and exchanges packets with an LDAP server.

To access this dialog box, select Global/LDAP Authentication from the Device View.

Figure 14-22 LDAP Authentication Dialog Box



LDAP Authentication

☑ Enable LDAP Authentication

Primary Server:	compatible.com
Primary Password:	frosty
Secondary Server:	192.168.11.139
Secondary Password:	snowman
Base:	o=compatible.com
VPN Group Attribute:	
VPN Shared Secret Attribute:	
Timeout:	10 (0 - 65535)

Enable LDAP Authentication

This checkbox enables this entire section. If checked, the settings from this section will be used to get a VPN user authentication from an LDAP server. If left unchecked, no settings from this section will be used.

Primary Server

This sets the IP address (e.g., 192.168.9.99) or fully qualified domain name (e.g., monkeywrench.com) of the primary LDAP server which contains the authentication information.

Primary Password

This string is used to authenticate the device to the primary LDAP server. If this is not set, then the device will attempt an anonymous bid to the server. The Primary Password may be up to 32 characters long.

Secondary Server

This sets the IP address (e.g., 192.168.9.99) or fully qualified domain name (e.g., monkeywrench.com) of the secondary LDAP server which contains the authentication information.

Secondary Password

This string is used to authenticate the device to the secondary LDAP server. If this is not set, then the device will attempt an anonymous bid to the server. The Secondary Password may be up to 32 characters long.

Base

This specifies the portion of the LDAP tree where the authentication information is located.

VPN Group Attribute

This value specifies the attribute name given to the VPN group attribute which has been defined in the LDAP server. There are no standard attributes defined by LDAP for this attribute, so you must specify one. If this field is left blank, the device will assume the attribute name to be “vpngroupattr”.

VPN Shared Secret Attribute

This value specifies the name given to the VPN shared secret attribute which has been defined in the LDAP server. There are no standard attributes defined by LDAP for this attribute, so you must specify one. If this field is left blank, the device will assume the attribute name to be “sharedsecret”.

Timeout

This value is the number of seconds the device will wait for a response from the LDAP server.