Version 4.0

Part No. 311643-D Rev 00
December 2001

600 Technology Park Drive
Billerica, MA 01821-4130

Reference for the Contivity VPN Switch

NORTEL NETWORKS™

Copyright © 2001 Nortel Networks

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and Contivity are trademarks of Nortel Networks.

Acrobat, Acrobat Reader, and Adobe are trademarks of Adobe Systems Incorporated.

SPECTRUM is a trademark of Cabletron Systems, Inc.

FireWall-1 is a trademark of Check Point Software Technologies Ltd.

Cisco and Cisco Systems are trademarks of Cisco Technology, Inc.

Entrust is a trademark of Entrust Technologies Inc.

OpenView is a trademark of Hewlett-Packard Company.

NetView is a trademark of International Business Machines Corporation (IBM).

Microsoft, MS-DOS, Windows, and Windows NT are trademarks of Microsoft Corporation.

NDS is a trademark of Novell, Inc.

ACE Server and SecurID are trademarks of RSA Security Inc.

Java is a trademark of Sun Microsystems, Inc.

VeriSign is a trademark of VeriSign Incorporated.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Nortel Networks Inc. software license agreement

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Figures

Tables

Preface

This book is intended for Nortel Networks* Contivity* VPN Switch managers. It provides reference information for each Web browser configuration screen.

Before you begin

This guide is for network managers who are responsible for setting up and managing the Contivity VPN Switch. This guide assumes that you have the following background:

- Experience with windowing systems or graphical user interfaces (GUIs)
- Familiarity with network management

This guide refers to the Contivity VPN Switch as “the switch.”

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is `ping <ip_address>`, you enter `ping 192.32.10.12`
arrow (→)	Shows menu paths. Example: Protocols→IP identifies the IP option on the Protocols menu.

`bold Courier text`	Indicates command names and options and text that you need to enter. Example: Use the **`ping`** command.
braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is `show ip {alerts|routes}`, enter either `show ip alerts` or `show ip routes`, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is `show ip interfaces [-alerts]`, you can enter either `show ip interfaces` or `show ip interfaces -alerts`.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is `ethernet/2/1 [<parameter> <value>]...`, you enter `ethernet/2/1` and as many parameter-value pairs as needed.
italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is `show at <valid_route>`, *`valid_route`* is one variable and you substitute one value for it.

`plain Courier text`	Indicates command syntax and system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is `show ip {alerts|routes}`, you enter either `show ip alerts` or `show ip routes`, but not both.

Related publications

For more information about using the Contivity VPN Switch, refer to the following publications:

- Release notes for the switch (part number 301459-V Rev 00) and the client (part number 311773-E Rev 00) provide the latest information, including brief descriptions of the new features, problems fixed in the release, and known problems and workarounds.
- *Configuring the Contivity VPN Switch* (part number 311642-D Rev 00) provides instructions for configuring, maintaining, and troubleshooting the switch.
- *Reference for the Contivity VPN Switch Command Line Interface* (part number 311645-C Rev 00) describes the commands that you can use from the command line interface.

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

You can purchase selected documentation sets, CDs, and technical publications through the Internet at the www1.fatbrain.com/documentation/nortel/ URL.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

Additional information about the Nortel Networks Technical Solutions Centers is available from the www.nortelnetworks.com/help/contact/global URL.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www130.nortelnetworks.com/cgi-bin/eserv/common/essContactUs.jsp URL.

Chapter 1
System

The System menu provides access to screens for configuring various system level settings.

Figure 1 System menu

System Identity

Each Contivity VPN Switch is uniquely identified by the system's address and domain name system (DNS) name. The DNS name can be used instead of the IP address to identify the switch and launch its management interface through a Web browser.

The System Identity screen allows you to optionally change your switch management IP address and provide the DNS host name and domain name. Additionally, you can assign up to three DNS addresses to resolve IP address name resolution requests.

You can also reset the switch management IP address values using the serial interface.

Figure 2 System Identity

System Identity

Management IP Address

Enter a management IP address for the system. You need this address to contact all system services, such as HTTP, FTP, and SNMP. To be accessible, the management IP address must map to the same network as one of the private interfaces.

For example, if you plan to assign IP address 10.2.3.3 with the subnet mask 255.255.0.0 to the private physical interface, the management IP address must reside in the 10.2.*x*.*x* network.

Changing IP addresses

If you configure the switch on one network and plan to move it to another network, change the management IP address and private LAN interface addresses before you move the switch. Then, communicate with the switch using the new management IP address from your browser's URL address field.

Domain Identity

DNS Host Name

Enter a name to identify the system. Enter the same name that is used by the DNS server to identify the management address of the switch that is located on your private network. You can enter up to 64 characters.

DNS Domain Name

Enter the name of the Internet domain into which this system is being placed. Enter the same Internet domain specified as the System Name in the Domain Name System (DNS) server.

A domain is a part of the Internet naming hierarchy that refers to general groupings of networks that are based on organization type or geography. For example, mycompany.com is the domain name for a commercial (.com) enterprise.

DNS Server Address

Primary

Enter the address of the DNS server that is located on your private network. The DNS server translates textual host names into IP addresses. For example, DNS can translate the fully qualified host name www.mycompany.com to its IP address, 192.19.2.33.

The primary DNS server is the first one addressed for servicing name resolution requests that are needed by the system; if the primary DNS server is unavailable, service is requested of the secondary DNS server.

Management tools use DNS server entries to resolve names in configurations. Always use the IP address for setting a DNS server host instead of a domain name.

Note: If no DNS servers are specified, management requests that use names instead of network addresses fail.

Secondary

Enter an address for the secondary Domain Name System (DNS) server. If the primary DNS server is unavailable, service is requested of the secondary DNS server (if present).

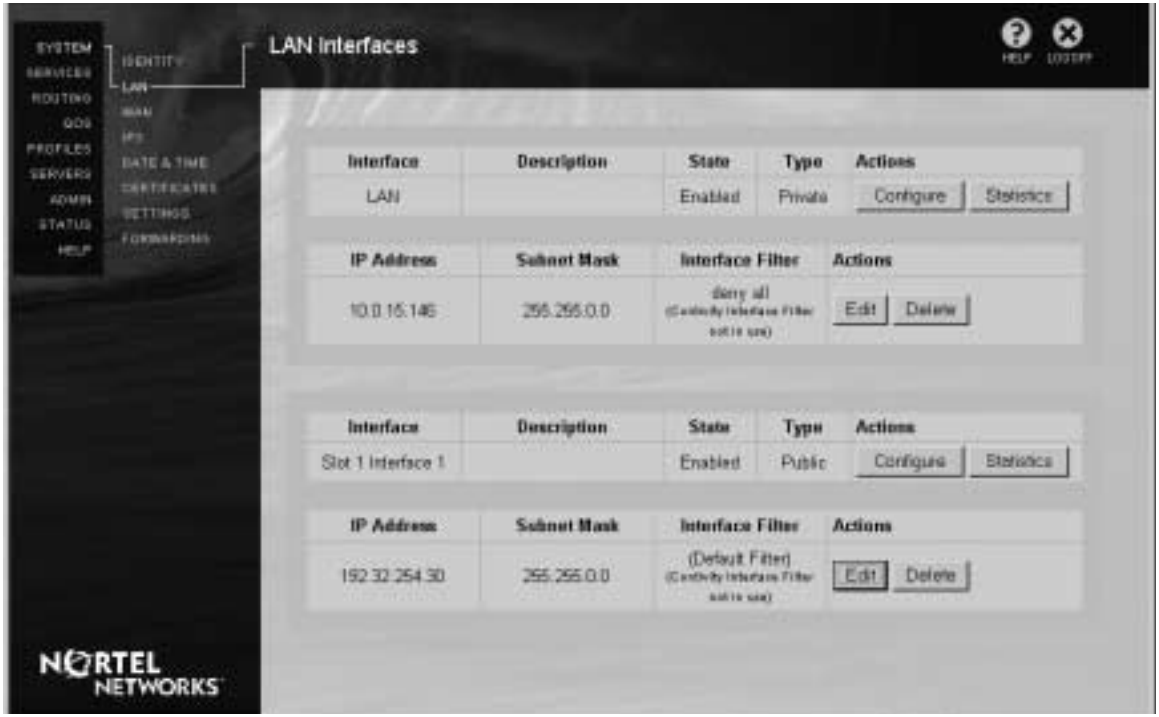
Tertiary

Enter an address for the tertiary Domain Name System (DNS) server. If the primary and secondary DNS servers are unavailable, service is requested of the tertiary DNS server (if present).

LAN Interfaces

The LAN Interfaces screen shows the interfaces that have been detected in the switch. The screen provides information about the interfaces, including the current state and type (private or public). In addition, it shows the IP address, the status of the Contivity Firewall, the interface filters that are being used, and the status of RIP on the interface. You can also configure the interface or view statistics on it from this screen.

Figure 3 LAN Interfaces



LAN/WAN IP Addressing

The private LAN interface and the management IP address must be on the same network; the public LAN interface should be on a different network, both physically and logically.

If your switch has a single network interface and you want to position the switch behind the firewall and router, then you should set the switch's interface type to Private.

Interface

LAN represents the Ethernet interface on the system board, which is installed on every switch.

Slot *n* Interface *n* represents an optional local area network card in expansion Slot *n* using Interface *n*.

Description

Shows the interface description (for example, the Private Interface), if one has been provided on the Interface Configuration screen (for example, a site, location, address, user name, or configuration tag). This can be helpful for network administrators working with the switch after it has been configured.

State

Enabled

This LAN interface is currently available.

Disabled

This LAN interface is currently unavailable.

Type

Public

Indicates that this interface is attached to a public data network like the Internet. The switch rejects nontunneled protocols and only accepts tunneled protocols like IPSec, PPTP, L2TP, L2F, and the diagnostic protocol PING on a Public interface.

A host can send only enough packets to a Public interface to establish a tunnel connection. If the tunnel is not established before a preset maximum number-of-packets-allowed counter is reached, then the packets from that host are discarded.

Private

Indicates that this interface is attached to the Private network and it can accept nontunneled networking protocols such as TCP/IP, FTP, and HTTP. The Private interface also accepts tunneled protocols (for example, IPSec, PPTP, L2TP, L2F) that can be used for secure management access to the switch.

Note: The private LAN interface and the management IP address should be on the same network, and the public LAN interface should be on a different network, both physically and logically.

If you have one network only and want to position the switch behind the firewall and router, then you should use a private LAN interface only (do not use a public LAN interface).

Actions

Configure

Click to modify the interface characteristics.

Statistics

Click to view the Link Statistics.

Edit

Click to change any of the LAN Interface attributes for the associated device.

Delete

Click to remove the listed IP address and associated information attached to the interface. You cannot delete the management IP address from the switch.

IP Address

Shows the current IP Address that is assigned to the interface.

Subnet Mask

The Subnet Mask defines which bits of the IP address represent the network the device is on and which bits represent the host's ID on the network.

The device uses the Subnet Mask to determine which IP addresses are directly reachable on the network and which must be routed through a gateway. A sample IP address is 10.2.3.3 with a Subnet Mask of 255.255.0.0. This indicates that all hosts with addresses 10.2.*n.n* are directly reachable.

Interface Filter

Shows whether the Contivity Firewall is in use on this LAN interface (this reflects the selection on the Services→Firewall screen).

This entry also shows the interface filter that is currently being used by the Contivity Firewall. This is the interface filter that is selected on the System→LAN Interfaces→Edit IP Address screen. If no interface filter has been selected, the default of Deny All is used.

Edit LAN Interface

The Configure button on the LAN Interfaces screen (System→LAN Configure) allows you to provide optional information for the LAN Interfaces, such as a description. This information then appears on the System→LAN screen. Additional fields appear on the Edit LAN Interface screen for optional network cards.

Figure 4 Edit LAN Interface

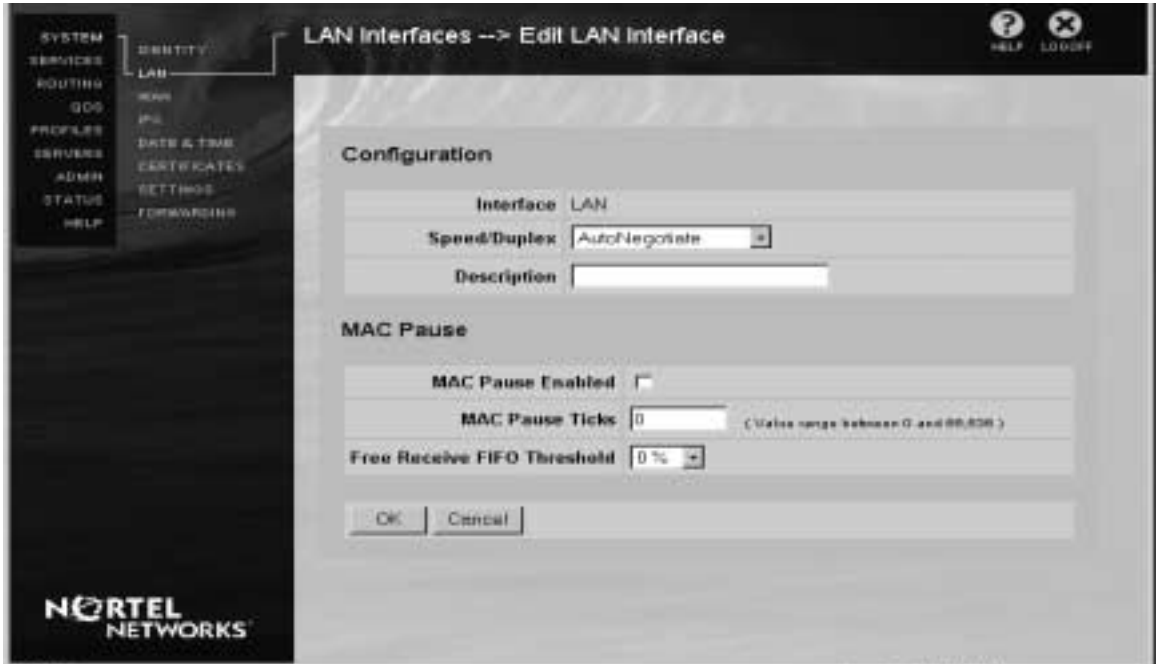
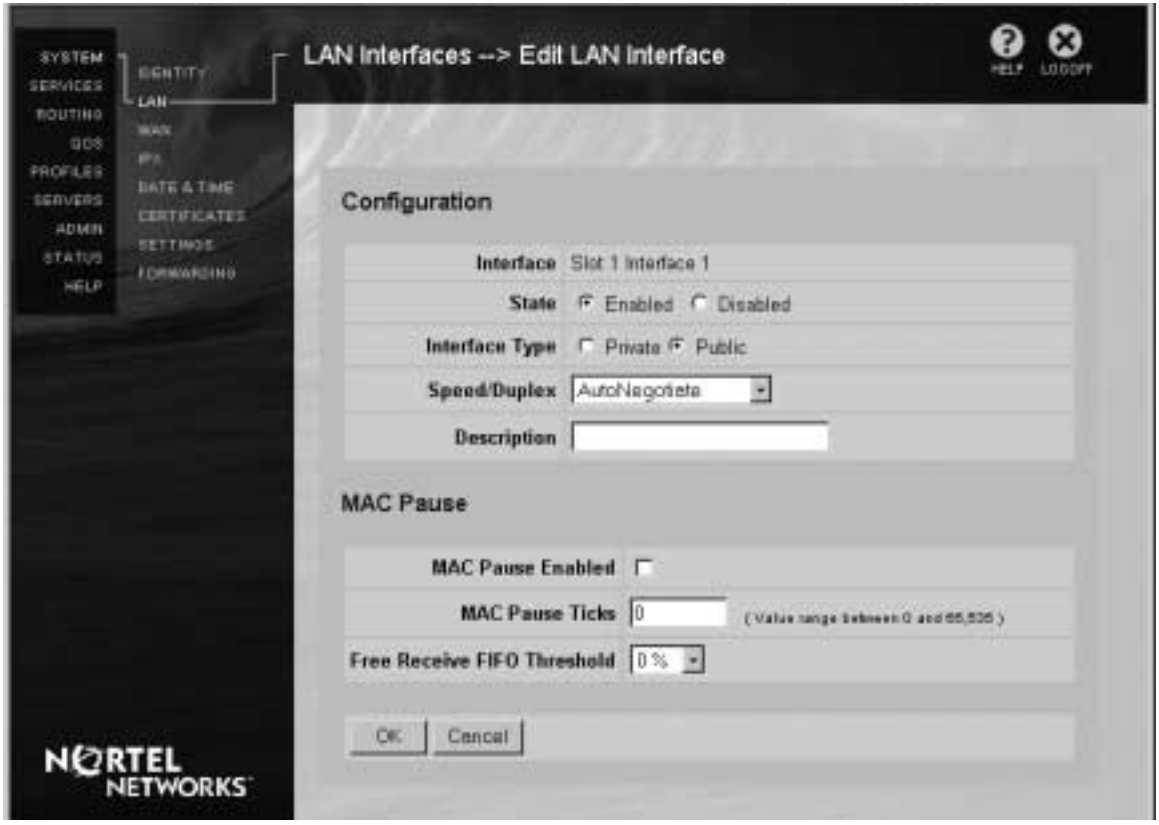


Figure 5 Edit LAN Interface – Slot *n* Interface *n*



Configuration

Interface

LAN represents the physical port interface to which you assign an IP address.

Slot *n* Interface *n* represents an optional LAN card in expansion Slot *n* using Interface *n*.

Speed/Duplex

Use the Speed/Duplex field to automatically or manually configure the LAN interface's port speed and mode.

Note: You can also use the Interface selection on the switch's Serial Port menu to set autonegotiation.

Select Auto-Negotiate to specify that the switch automatically set the port speed and mode to match the best service provided by the connected station, up to 100 Mbps in full-duplex mode. Auto-Negotiate is the default selection, and complies with the IEEE 802.3u autonegotiating standard.

Select one of the following selections to manually set the LAN interface's port speed and mode to match the speed and mode used by the connected station.

- 100Mbs/Full duplex
- 100Mbs/Half duplex
- 10Mbs/Full duplex
- 10Mbs/Half duplex

Note: You might not be able to connect to the remote system if the system is not using autonegotiation or if it uses an incompatible form of autonegotiation. If this occurs, manually set your switch's speed and mode settings to match those used by the remote system.

Description

An optional description that you can provide for the LAN Interface. The description appears on the LAN Interfaces screen.

MAC Pause

MAC Pause (Ethernet packet flow control) enables the switch to automatically adjust and control the flow of incoming and/or outgoing packets from any standard speed LAN device.

MAC Pause Enable

Check to enable MAC Pause (Frame-based flow control) on the selected interface port. When enabled, specify the appropriate Pause parameters to be set in the hardware.

MAC Pause Ticks

Specify a value for MAC Pause Ticks.

Free Receive FIFO Threshold

Select a value from the list. The default is 0.

State

The State field appears on the screen for an optional LAN card in expansion Slot *n* using Interface *n*. Click to enable or disable the card.

Interface Type

The Interface Type field appears on the screen for an optional LAN card in expansion Slot *n* using Interface *n*. Click to specify whether the interface is public or private.

Add IP Address and Edit IP Address

The Add IP address screen (System→LAN Add) allows to you assign an IP Address and Subnet Mask to the interface. Use the Edit IP Address screen (System→LAN Edit) to modify the information.

Figure 6 Edit IP Address – LAN Interface

Figure 7 Edit IP Address – Slot *n* Interface *n*

Interface

LAN - Represents the physical port interface to which you assign an IP address.

Slot *n* Interface *n* - Represents an optional LAN card in expansion Slot *n* using Interface *n*.

Obtaining IP Address

This section specifies whether to use a Static, assigned IP address, or a DHCP assigned address.

Static

Check the Static button to assign a static, unchanging IP Address.

IP Address

The IP Address for the interface. The IP Address consists of 32 bits, which are written as four octets (8-bit bytes) in dotted-decimal format. For example:

```
192.168.34.21
```

Subnet Mask

The Subnet Mask defines how many bits of the IP Address represent the network the device is on and how many bits represent the host's ID on the network.

The device uses the Subnet Mask to determine which IP Addresses are directly reachable on the network and which must be routed through a gateway. A sample IP Address is 10.2.3.3 with a Subnet Mask of 255.255.0.0. This indicates that all hosts with addresses 10.2.*n.n* are directly reachable.

DHCP

Check the DHCP button to have the IP address assigned by a DHCP server.

Cost

Enter a cost. The default is 10.

Interface Filter

Shows whether or not the Contivity Firewall is in use (this reflects the selection on the Services→Firewall screen).

This entry also shows the interface filter that is currently being used by the Contivity Firewall. Use the dropdown menu to show a list of all interface filters that have been set up on the switch (on the Profiles→Filters screen), and to select a different filter for the Contivity Firewall.

Note: If you change the interface filter setting, a message informs you that you must restart your switch before the new interface filter is used. If the Contivity Firewall is not enabled, the new selection has no effect.

Use the New Interface Filter link to go to the Profiles→Filters screen and create a new filter.

The default Interface Filter setting is Deny All.

LAN Interface Statistics screen

This screen (System→LAN Statistics) provides key counters and can help you diagnose and troubleshoot problems with your LAN interfaces.

Table 1 Description of fields

LAN Device	Description
Tx good frames	Good frames transmitted.
Tx MAXCOL errors	The number of frames not transmitted because the frame reached the maximum allowable collision threshold.
Tx LATECOL errors	The number of frames not transmitted because they experienced a late collision during transmission.
Tx underrun errors	The number of frames not transmitted because the hardware transmitter experienced a buffer underrun during transmission.
Tx lost CRS errors	The number of frames not transmitted because carrier sense was lost during transmission.
Tx deferred	The number of times a frame was deferred due to a collision during transmission.
Tx single collisions	The number of times a single collision occurred during a frame transmission.
Tx multiple collisions	The number of times multiple collisions occurred during frame transmissions.
Tx total collisions	Total collisions that occurred during frame transmission.
Rx good frames	Good frames received.
Rx CRC errors	The number of received frames discarded due to an invalid cyclic redundancy check error.
Rx alignment errors	The number of received frames discarded due to invalid frame alignment.
Rx resource errors	The number of frames discarded because a buffer was not available to receive the frame.

Table 1 Description of fields (continued)

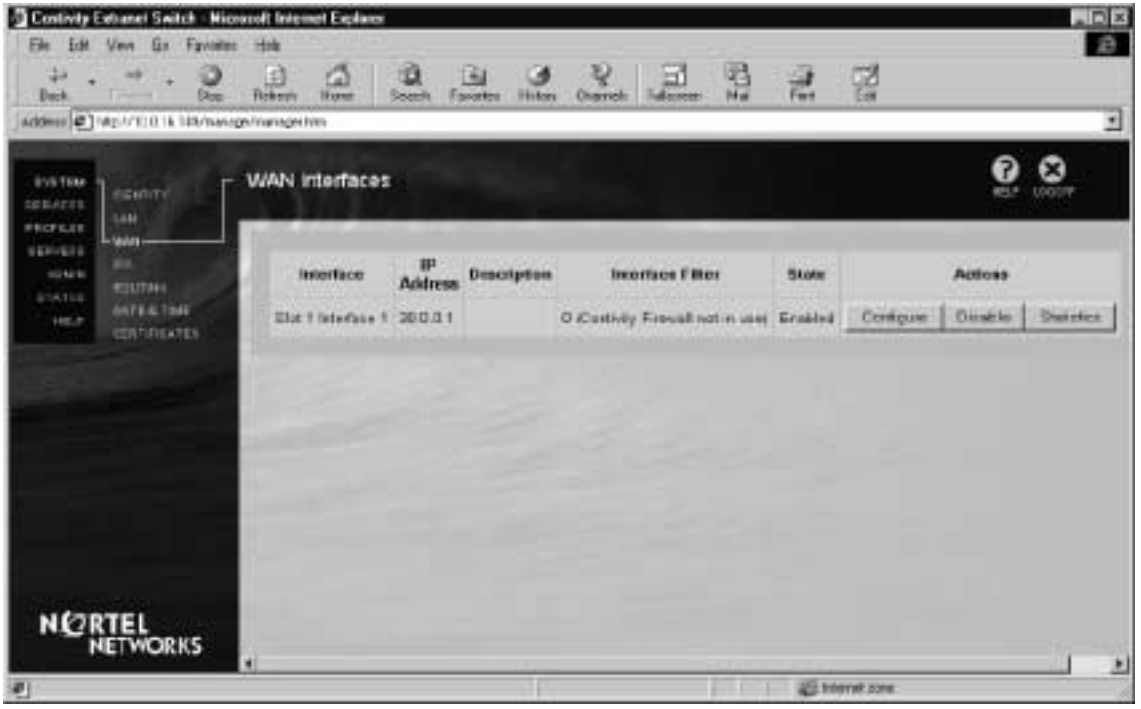
Rx overrun errors	The number of received frames discarded because the hardware receiver experienced an overrun error during reception.
Rx collision detect errors	The number of received frames discarded due to a collision error during reception.
Rx short frame errors	The number of received frames discarded because they didn't meet the minimum frame length.

Table 2 Software-level packet data

Software-level packet data	**Description**
IP Fragments Received	IP fragments received.
IP Routing Filter Drops	Routing filter drops occur when packets are filtered because no access rights are permitted to the resources specified by the designated filters.
IP Local System Filter Drops	Local system filter drops occur when packets are destined to the management interface but are dropped due to lack of authorization access.
IP Local Interface Filter Drops	Local interface filter drops occur when packets are destined to a physical interface but are dropped due to lack of authorization access.
IP PAT Drops	Public Address Table (PAT) drops represent the number of packets dropped prior to being authenticated and having a tunnel established on a public interface.
IP Header Error Drops	IP header error drops occur whenever there is an error in the IP header.
RX MAC Pause Frames received	(Unsigned integer number)
TX MAC Pause Frames transmitted	(Unsigned integer number)

The WAN interfaces screen (System→WAN) shows the WAN interfaces currently installed in the switch, the slot in which the cards reside, an interface description (if one has been provided), and the current state. It also indicates whether the Contivity Firewall is active and the interface filter that is in use. From this screen, you can move to another screen to configure or disable a WAN card, or view statistics.

Figure 8 WAN Interfaces screen



Interface

Slot *n* Interface *n* represents an optional wide area network (WAN) card in expansion Slot *n* using Interface *n*.

IP Address

The IP Address for the interface.

Note: To change the IP address of a WAN link, you must disable the interface, change the address and re-enable the interface. This automatically disables static routes for the interface. If you change the IP address back to the original address, you must manually re-enable static routes.

Description (Optional)

A description that you can optionally provide. For example, a site, location, address, user name, or configuration tag. This can be helpful for network administrators working with the switch after it has been configured.

Interface Filter

Shows whether the Contivity Firewall is in use on this WAN interface (this reflects the selection on the Services→Firewall screen).

This entry also shows the interface filter that is currently being used by the Contivity Firewall. This is the interface filter that is selected on the System→WAN Interfaces→Edit IP Address screen. If no interface filter has been selected, the default of Deny All is used.

State

Enable

This WAN interface is currently enabled. An asterisk (*) means that the Interface Debug option on the WAN PPP Advanced Configuration screen is enabled.

Disable

This WAN interface is currently unavailable.

Actions

Configure

Click to configure a new IP address for the associated device, add or modify PPP advanced and authentication settings. The Configure WAN Interfaces screen appears.

Enable/Disable

Click to toggle between Enable (on) and Disable (off).

Statistics

Click to view Statistics for the interface.

WAN Statistics

This screen (System→WAN Statistics) provides counters that can help you diagnose and troubleshoot problems with your WAN interfaces. Fields on this screen are described in the following tables.

Table 3 WAN statistics

Field	Description
WAN Slot 2 Interface 2	The slot and interface numbers
PHY	The state of the physical link is either up or down
Administrative State	The Administrative state is either enabled or disabled
PPP	The state of the Point-to-Point Protocol (PPP)
Interface	The physical interface type
Link Protocol	The link protocol type
Clocking	The switch relies on the channel service unit/digital service unit (CSU/DSU) to provide the signaling clock at the T1 physical level.
In	Packets received over this link
Out	Packets sent over this link
In Errors	Errors while receiving packets over this link
Out Errors	Errors while sending packets over this link
Cof Errors	Counter overflow errors
Bof Errors	Buffer overflow errors
WD Errors	Watchdog errors
DSR	Data set ready signal
DCD	Data carrier detect signal

Table 3 WAN statistics (continued)

CTS	Clear-to-send signal
RXE	Receive signal
TXE	Transmit signal

Table 4 Packet data statistics

Software-Level Packet Data	**Description**
IP Fragments Received	IP fragments received
Routing Filter Drops	Routing filter drops occur when packets are filtered because no access rights are permitted to the resources specified by the designated filters.
IP Local System Filter Drops	Local system filter drops occur when packets are destined to the management interface but are dropped due to lack of authorization access.
IP Local Interface Filter Drops	Local interface filter drops occur when packets are destined to a physical interface but are dropped due to lack of authorization access.
IP PAT Drops	Public Address Table (PAT) drops pertain to the number of packets dropped prior to being authenticated and having a tunnel established on a public interface.
IP Header Error Drops	IP Header Error Drops occur whenever there is an error in the IP header.

Configure WAN Interface Settings

The Configure WAN Interface Settings screen (System→WAN Configure) allows you to configure WAN devices with local and remote IP addresses and PPP-related settings. When you click the PPP Authentication or Advanced Settings configuration buttons, the associated configuration screen appears. You also use this screen to specify the interface filter that is used for the optional Contivity Firewall on this interface.

The addresses set on this screen are used by the IP Control Protocol (IPCP), which communicates IP addresses to peer connections over PPP. Many of these values are provided to you by your Internet Service Provider (ISP).

Figure 9 Configure WAN Interface Settings screen

Interface

This is the type, slot number, and interface to which this IP address is assigned. The module slots on the back of the switch are labeled Slot 1 through Slot 4, from left to right. Slot 4 is not supported.

Description (Optional)

Provide a brief interface description. For example, a site, location, address, user name, or configuration tag. This can be helpful for network administrators working with the switch after it has been configured.

Interface IP Address

You must enter an Interface IP Address to allow IP traffic to pass over a PPP connection. This is the switch's IP address as seen from a Public network. This IP address is normally provided to you by the ISP. A sample Interface IP Address is 192.19.2.33.

Note: The interface IP address and the remote IP addresses must be different.

Remote IP Address

Accept Negotiated Address

This option informs the peer connection (for example, your Internet Service Provider) that you accept the IP Address that it assigns itself.

This checkbox is **Enabled** by default.

Specify Remote Address

Enter a Remote IP Address to allow IP traffic to pass over a PPP connection. This is the IP address of the router that is connected to the switch. This address is used if you do not check Accept Negotiated Address above. This IP address is normally negotiated between the switch and the ISP. A sample Remote IP Address is 192.19.2.30.

Note: The Remote and Local IP addresses must be different.

Interface Filter

Shows whether or not the Contivity Firewall is in use (this reflects the selection on the Services→Firewall screen).

This entry also shows the interface filter that is currently being used by the Contivity Firewall. Use the dropdown menu to show a list of all interface filters that have been set up on the switch (on the Profiles→Filters screen), and to select a different filter for the Contivity Firewall.

Note: If you change the interface filter setting, a message informs you that you must restart your switch before the new interface filter is used. If the Contivity Firewall is not enabled, the new selection has no effect.

Use the New Interface Filter link to go to the Profiles→Filters screen and create a new filter.

The default Interface Filter setting is Deny All.

PPP Authentication Settings

Click Configure to set PPP Authentication Settings, including Local PAP and CHAP User IDs and Passwords.

PPP Advanced Settings

Click Configure to set PPP Advanced Settings, including Link Control Protocol (LCP) and IP Control Protocol (IPCP) Settings.

CSU/DSU Settings

Click Configure to set the T-1 with an integrated CSU/DSU Settings, including extended superframe (ESF) framing parameters and adding fractional T-1 channels.

T-1 with Integrated CSU/DSU

You can configure your T-1 interface with an integrated CSU/DSU from the System→WAN screen or the serial interface. Following is a list of screens that either allow you to configure or view status for the T-1 interface with an integrated CSU/DSU:

- System→WAN
- System→WAN→Configure
- Admin→Health Check
- Status→Statistics→WAN Status

Newer T-1 services use extended superframe (ESF) framing, which uses out-of-band signaling. The configuration parameters with ESF are:

- Line framing is ESF.
- Line coding is B8ZS.
- HDLC polarity is normal.
- Performance report message value is determined by the T-1 service provider.

Older T-1 services use superframe (SF) framing, which uses in-band signaling. The configuration parameters with SF are:

- Line framing is SF.
- Line coding is AMI.
- HDLC polarity is inverted.
- Performance report message should be set to “none” as it has no effect in SF framing.

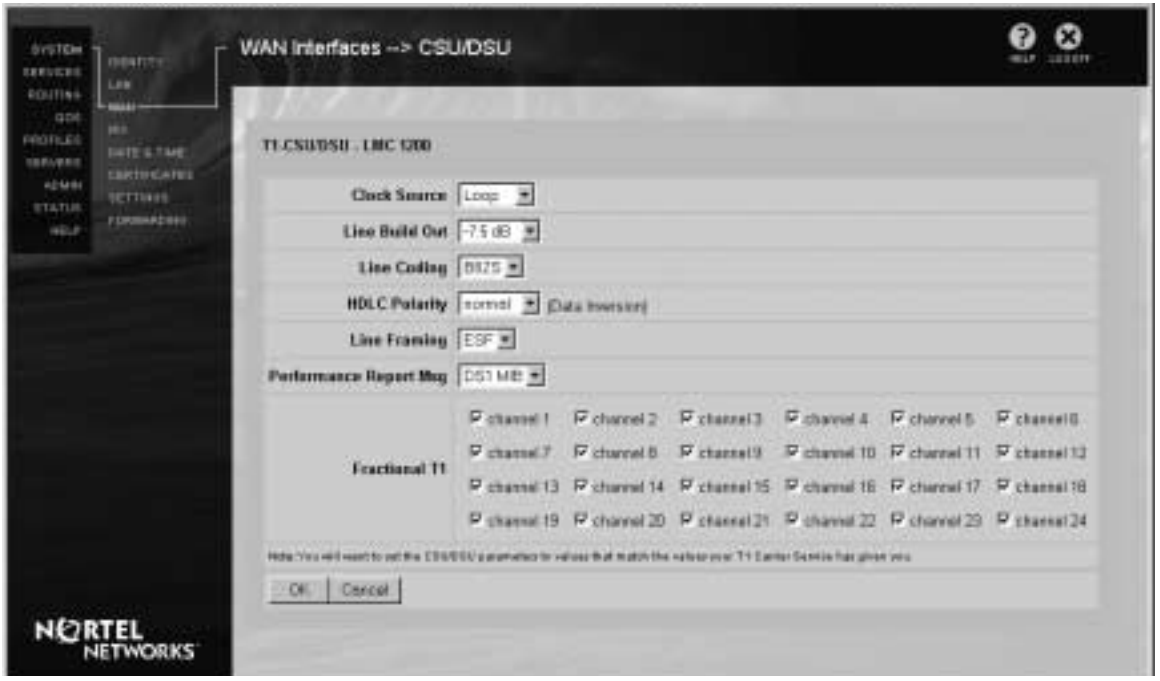
Because SF framing uses in-band signaling, the data can generate a false yellow alarm. These false yellow alarms can be eliminated by setting one fractional T-1 channel to “off.” If you have the option of using SF or ESF framing, Nortel Networks recommends ESF framing because it provides better diagnostics and does not generate false yellow alarms.

Initial configuration takes place when you install the card, and configuration changes are necessary when adding additional fractional T-1 channels.

Note: You must restart the switch after adding a T-1 card or after enabling a fractional T-1 line.

All of the CSU/DSU commands can be configured through the Web interface or the serial interface.

Figure 10 CSU/DSU



T1-CSU/DSU - LMC 1200

Clock Source

This field sets where the timing is being determined, from the switch (Internal) or from the T-1 service provider (Loop). The clock source is usually set to Loop when connected to a live T-1 service. Internal clocking is used for local or test applications only.

Line Build Out (dB)

The line build out value is a power level that is set based on the distance from the CSU/DSU to the T-1 service provider's switch. If the CSU/DSU card is close by, the switch requires less power and the line build out value is lower; if the card is far away, the switch requires more power and the line build out value is higher. This setting is determined by the T-1 service provider. Valid options are:

- 0.0
- -7.5
- -15.0
- -22.5

Line Coding

This field sets the method of encoding binary digits on the line. The line coding value is supplied by the T-1 service provider. Valid options are AMI and B8ZS.

HDLC Polarity

This field determines whether or not the user data is inverted. This field must be synchronized with the AMI line coding; otherwise, you might violate the AMI specification. Both the local and the remote CSU/DSU must terminate the T-1 data circuit with the same setting: either both using Normal or both using Inverted. Valid options are Normal and Inverted.

Line Framing

This field determines the low-level protocol between the T-1 service provider and the switch. It determines how the data is encapsulated and it handles the signaling for alarms and loopbacks. The newer ESF framing uses out-of-band signaling, while the older SF framing uses in-band signaling. The line framing value is supplied by the T-1 service provider. Valid options are SF and ESF.

Performance Report Mesg

The Performance Report Message parameter is a part of the ANSI T-1 specification. It generates messages that state how many errors there are per second. This value is used with ESF framing only. When using SF framing, this parameter has no effect but should be set to None to avoid any confusion. The Performance Report Message value is supplied by the T-1 service provider and are None and ANSI.

Fractional T-1

A T-1 service consists of up to 24 channels. Typically, you purchase the number of necessary channels from the service provider, and you can add additional channels (up to 24) as growth requires. When you add a fractional T-1 channel, you must enable it through this parameter and restart the system. Valid options for each of the 24 DS-0 channels are On (checked) and Off (unchecked).

Local Authentication

The WAN Interfaces Local Authentication screen (System→WAN Configure PPP Authentication) allows you to configure Local Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) User IDs and Passwords, and other details.

The ISP providing the WAN connection to the switch might require a user ID and password. Select the appropriate authentication method, PAP or CHAP, as required by the ISP. If authentication is not required, then select None.

Figure 11 Local Authentication

None

Click None (default) to allow a connection without authentication on this interface.

PAP

Click to enable the Password Authentication Protocol (PAP). PAP is a simple method for a peer (the switch) to establish its identity during link setup. After establishing the identity, the ID and Password are transmitted repeatedly by the peer until the server acknowledges authentication or the connection is ended.

PAP is a lightweight authentication method, and the passwords are transmitted in clear text form (not encrypted). This leaves open the possibility for someone to trace the PPP setup and learn the WAN interface UID and passwords.

Most administrators do not consider the link setup as a possible security issue, and most ISPs use the link authentication described here for accounting purposes.

The PAP User ID and Password are used by the switch to authenticate with the service provider's T1 connection. They are provided to you by your ISP.

CHAP

Click to enable the Challenge Handshake Authentication Protocol (CHAP), which is the default setting.

CHAP uses a handshake to verify the identity of a peer. During link setup, the server (authenticator or ISP) sends a challenge message to the peer (the switch). CHAP depends on a “secret” that is known only by the server and the peer. The peer responds with a calculated value based on the secret. The server matches the calculated value against its own calculation. If the values match, the peer is successfully authenticated.

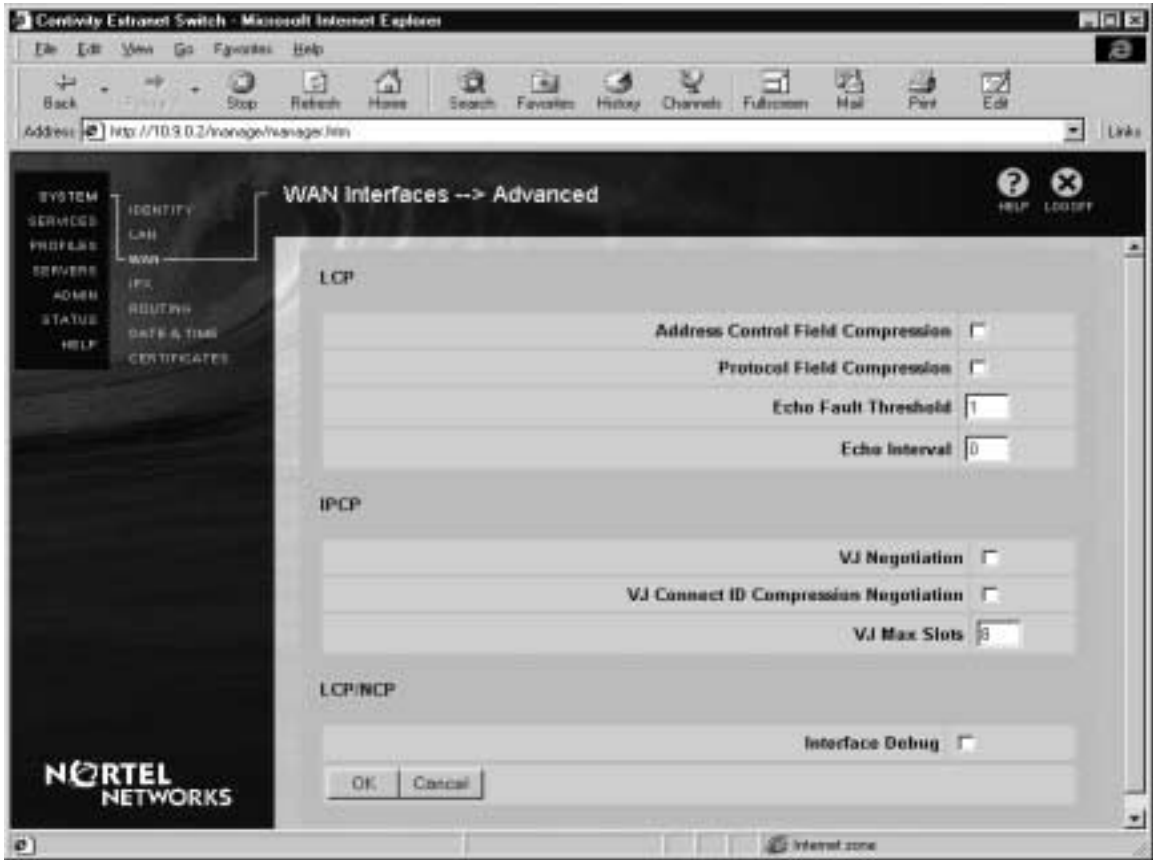
CHAP is a stronger authentication method than PAP. The clear-text secret is never transmitted over the communications link. Therefore, a trace of the session would not reveal the passwords.

The CHAP User ID and Password you assign are used by the switch to authenticate with the service provider's T1 connection. They are provided to you by your ISP.

WAN Interface Advanced Settings

The WAN Interface Advanced Settings screen (System→WAN Configure PPP Advanced) allows you to configure various connection options between the ISP and the switch, and to specify certain dial-up networking attributes, including Link Control Protocol (LCP) and IP Control Protocol (IPCP) Settings.

Figure 12 WAN Interface Advanced Settings



LCP Settings

The Link Control Protocol (LCP) session negotiates various link options between the switch and the ISP.

Address Control Field Compression

Click to enable Address Control Field Compression, which then compresses the Address Control Field and reduces packet overhead by one byte. Address Control Field compression is Disabled by default.

Protocol Field Compression

Click to enable Protocol Field Compression, which then compresses the Protocol Field and reduces packet overhead by one byte. Protocol Field Compression is disabled by default.

Echo Fault Threshold

You can set the number of times LCP attempts an Echo request without receiving a reply. The link is dropped when the number of echo requests exceeds the number in the Echo Fault Threshold box.

The possible range is 0 to 255 (0 indicates disabled); default is 1.

Echo Interval

You can set the Echo request Interval in seconds. Use this interval along with the value of the Echo Fault Threshold box to determine if a link has been disconnected.

The possible range is 0 to 255; default is 0 (Disabled).

IPCP Settings

The IP Control Protocol (IPCP) settings allow you to specify certain dial-up networking attributes. Typically, IPCP handles address assignment and configuration of domain name system (DNS) or windows Internet naming service (WINS) server settings.

The switch allows you to manipulate header compression options that can help optimize data transfers between systems.

VJ Negotiation

Click to enable Van Jacobson (VJ) Compression Negotiation. VJ Compression compresses the TCP/IP header fields on a per TCP/IP flow basis and reduces packet overhead. VJ Negotiation is disabled by default.

VJ Connect ID Compression Negotiation

Click to enable Van Jacobson (VJ) Connect ID Compression, which then further reduces the VJ compression header and increases packet transmission performance. This option is used only when a single TCP/IP flow is active at any single time over the link. VJ-style TCP/IP header compression identification is **Disabled** by default.

VJ Max Slots

This is the Maximum number of concurrent VJ-compressed TCP/IP flows. The range is from 2 to 16; default is 8.

LCP/NCP

Interface Debug

This option, under the Link Control Protocol/Network Control Protocol, sends PPP control packets to the Event log. This is a Nortel Networks internal Customer Support utility that helps diagnose and troubleshoot WAN interface problems.

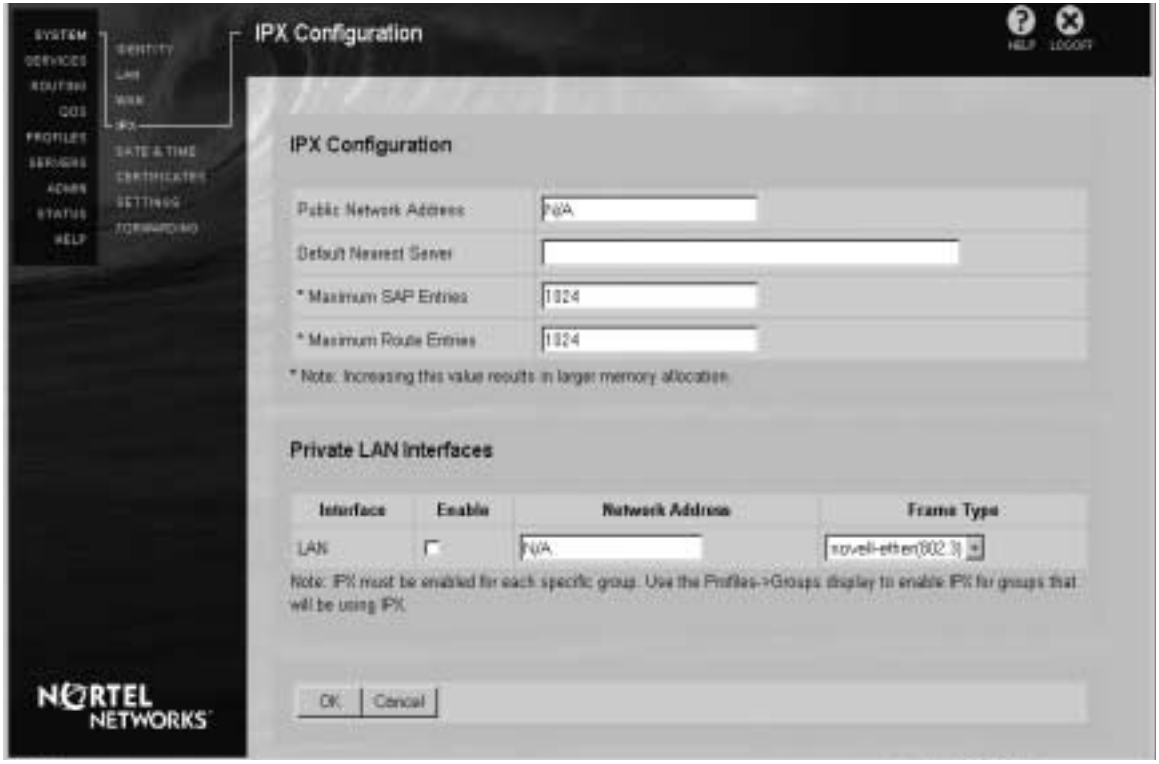
IPX (Internetwork Packet Exchange)

The Internetwork Packet Exchange (IPX) protocol is the Novell adaptation of the Xerox Networking System (XNS) protocol.

IPX Configuration

Click System→IPX to configure IPX support.

Figure 13 System→IPX Configuration



Public Network Address

Enter the IPX Public Network Address. This is the network address that is assigned to clients tunneling into the switch. The Public Network Address is a 4-byte hexadecimal number that must be unique (it cannot match any other IPX network address). A sample Public Network Address is 4F1A3BC2.

The Public Network Address also consists of a node address that is dynamically assigned by the switch to each tunneled-in client system. The Node Address is a randomly allocated number that cannot be overwritten or changed in any way.

Note: Leaving the Public Network Address blank disables IPX on the switch.

Caution: You must restart the system from the Admin→Shutdown screen for Public Network Address changes to take effect.

Default Nearest Server

Enter the name of the server that you want to be the Default Nearest Server. The Default Nearest Server name can consists of up to 48 ASCII characters. When a remote system establishes an IPX connection with the switch, the system sends a Get Nearest Server packet to the switch. In response to a Get Nearest Server request, the switch returns the name and IPX address of the server specified here. This assumes that the server is available; otherwise, the switch returns the name and IPX address of the server that is topologically closest to the requesting system.

Maximum SAP Entries

Shows the largest number of SAP (Service Advertising Protocol) entries that the switch handles concurrently. SAP is a Novell protocol that provides a means for servers to advertise their services to routers, switches, and other servers.

Each SAP entry that you allocate requires about 100 bytes of memory (10,000 entries requires about 1 MB of memory). Therefore, you should keep the number of entries slightly greater than the number of servers that you support to allow for future growth. The default value is 1024 entries; the range is from 10 to 10,000 entries.

Maximum Route Entries

Shows the largest number of IPX route entries that the switch handles concurrently. A route entry is required for each reachable IPX network that is learned through the IPX RIP protocol.

Each route entry that you allocate requires about 100 bytes of memory (10,000 entries requires about 1 MB of memory). Therefore, you should keep the number of entries slightly greater than the number of routes that you support to allow for future growth. The default value is 1024 entries; the range is from 10 to 10,000 entries.

Private LAN Interfaces

Interface

LAN represents the Ethernet interface on the system board, which is installed on every switch.

Slot *n* Interface *n* represents an optional local or wide area network card in expansion Slot *n* using Interface *n*.

Enable

Click to enable the interface for IPX support.

Network Address

Enter the IPX interface Network Address. The IPX Network Address that you configure on this interface must be the IPX Network Address of the LAN.

Frame Type

Click the drop-down list box to select an IPX Frame Type. The IPX Frame Type that you select on this interface must be the IPX Frame Type being used on the LAN.

The switch can forward the following IPX packet types:

- 802.3 (Raw) refers to 802.3 framing without the 802.2 link layer control (LLC).
- 802.2 frame includes 802.3 and 802.2 logical link control (LLC) frames.
- SNAP Sub Network Access Protocol (SNAP) is like 802.2 with expanded link layer control (LLC) capabilities.
- Ethernet II frame type is also similar to 802.2, yet it has a type field rather than a length field. It does not use a link layer control (LLC) header in its data field.

Hardware Encryption Accelerator

The hardware accelerator screen shows the operational status that the switch reports on the hardware accelerator card and allows you to enable automatic recovery in case the card stops running. When the switch detects a recoverable failure, all sessions fail-over and are then handled by the software until the hardware resets and comes back on line.

Figure 14 Hardware Accelerator

You must have Administrator privileges to configure the card, and you must restart the switch after configuring it.

The accelerator supports a maximum of 1024 tunnels. A tunnel consists of two sessions, one each for incoming and outgoing traffic. Each session comprises a set of logical characteristics and parameters that are associated with a single communication path in a tunnel that renders a full-duplex connection. Thus, the number of tunnels supported by an accelerator is exactly half the maximum session count.

Following is a listing of the switch's configuration, status, and monitoring paths related to the hardware accelerator:

- System →Accelerator→Hardware Accelerator: Configure
- Status→Health Check
- Status→Statistics→Hw Accel Stats
- Status→Statistics→Hw Accel Info

- Status→Event Log

The Hardware Accelerator screen shows the operational status that the switch reports for the card.

Figure 15 Hardware Accelerator Configuration

Bulk Accelerator

Auto Recovery Enabled

This selection gives the operator control of what happens when if the card fails and the failure is recoverable. When enabled, the card automatically resets and restarts, when a recoverable failure is encountered.

Auto Recovery is the only configurable parameter. By default it is enabled and it maintains this state through a restart

Description

A description of the device vendor, device type, and serial number (if applicable).

Operational Status

Status can be viewed on the Status→Health Check and the Status→Statistics: HwAccelInfo screens. The operational status can be:

- Disabled means that the card is disabled.
- Active means that the card is attached and is active.
- Shutdown means that in this state you can manually reenable the card after a recoverable failure has been detected (when Auto Recovery Enabled is Off).
- Failed means that the card is not operating properly. Contact Nortel Networks Customer Support for additional information.

Administrative States

The card is either Enabled or Disabled. It is enabled by default.

Note: You can disable the card at any time, even when it is processing tunnel traffic. In this case, the tunnels are processed in software. When the card is subsequently enabled, any tunnels that had been running on the hardware when it was disabled, revert to running on the hardware.

Protocols

Shows the protocol running on the card: IPSEC_ESP.

Algorithms

Shows the encryption and authentication protocols that the card supports:

- DES Data Encryption Standard
- 3DES Triple Data Encryption Standard

- NULL_CRYPT – IPSec ESP authentication and compression only; encryption is turned off. You can use this setting as a troubleshooting mechanism.
- LZS – Lempel/Ziv/Stac, which is a de facto standard for IPSec compression.
- HMAC MD5 – Header Message Authentication Code with Message Digest, which provides integrity that detects packet modifications.
- HMAC SHA – Header Message Authentication Code Secure Hash Algorithm**,** which produces a 160-bit hash. SHA is regarded by cryptographers as being more resistant to attacks than MD5. It does not encrypt data.

Crypto Strength

Shows the available cryptographic strength, which is either 3DES (triple DES) or DES, depending upon the maximum key length.

Boots

Shows the number of times the card has been restarted.

Uptime

Shows the current duration that the switch has been running (days:hours:minutes:seconds).

Context Memory Size

Shows the amount of context memory on the card: 512 kbytes.

Max Sessions

Shows the maximum number of sessions. When you divide this number by two you get the number of tunnels (2048 sessions represents 1028 tunnels).

POST Results

Shows the passing and failure indications for each power-on self test (POST) type. This field displays when there is a POST failure only.

Statistics

You can view statistics for the hardware accelerator on the Status→Statistics HwAccelCounters screen. Byte counters are all 64-bit integers:

- Total packets on egress
- Total bytes on egress
- Total packets on ingress
- Total bytes on ingress
- Corrupt bytes (see explanation)
- Corrupt packets
- Expanded bytes (see explanation)
- Expanded packets

Corrupt bytes and packets counts reflect packets that were not processed because they were corrupted in transit. Indications of a corrupt packet include: no LZS end marker, mismatch MAC.

Expanded bytes and packets counts reflect packets that expanded when compressed by the LZS algorithm. These counters are important because they indicate a heavier load on the accelerator since packets which expand must be sent a second time to the accelerator with compression disabled. If there are many sessions transporting incompressible traffic (such as a video stream), the overall performance of the switch is degraded relative to its performance when all sessions carry compressible data (such as FTP of text files).

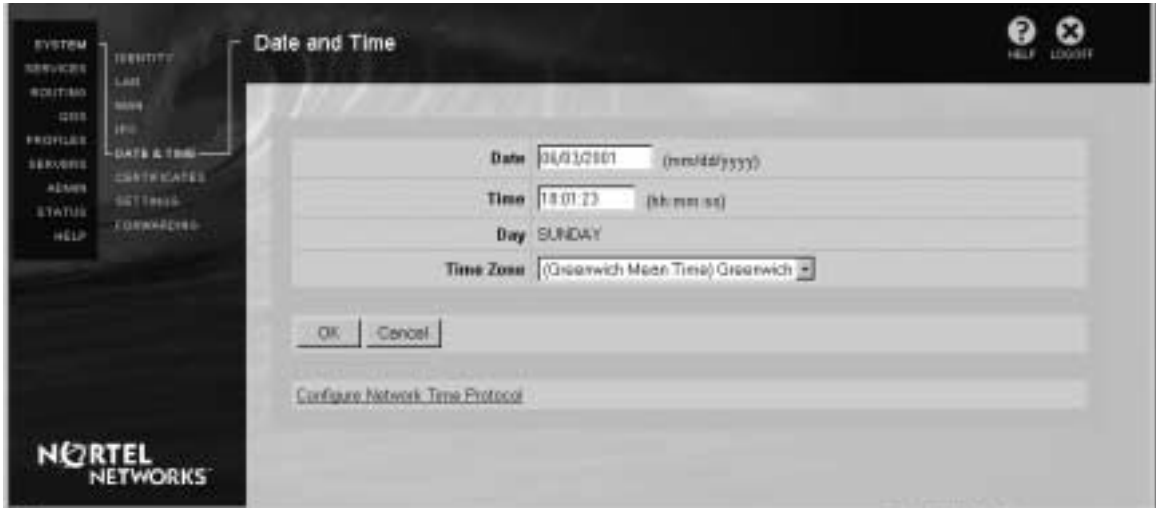
Most of these statistics are maintained for debugging and tuning purposes.

Date and Time

This screen shows the current Date, Time, and Day of the week for the switch. You can change the time based on your time zone, or make daylight savings time adjustments, as necessary.

To change either the Date or Time values, select the fields and enter the new values.

Figure 16 Date and Time



Date

Shows the current month, day, and year (mm/dd/yyyy).

Time

Shows the current hour, minute, and seconds (hh:mm:ss) as displayed by a 24-hour clock (00:00:00 to 23:59:59).

Day

Shows the current day of the week. The day is based on the month, date, and year, and it cannot be changed manually.

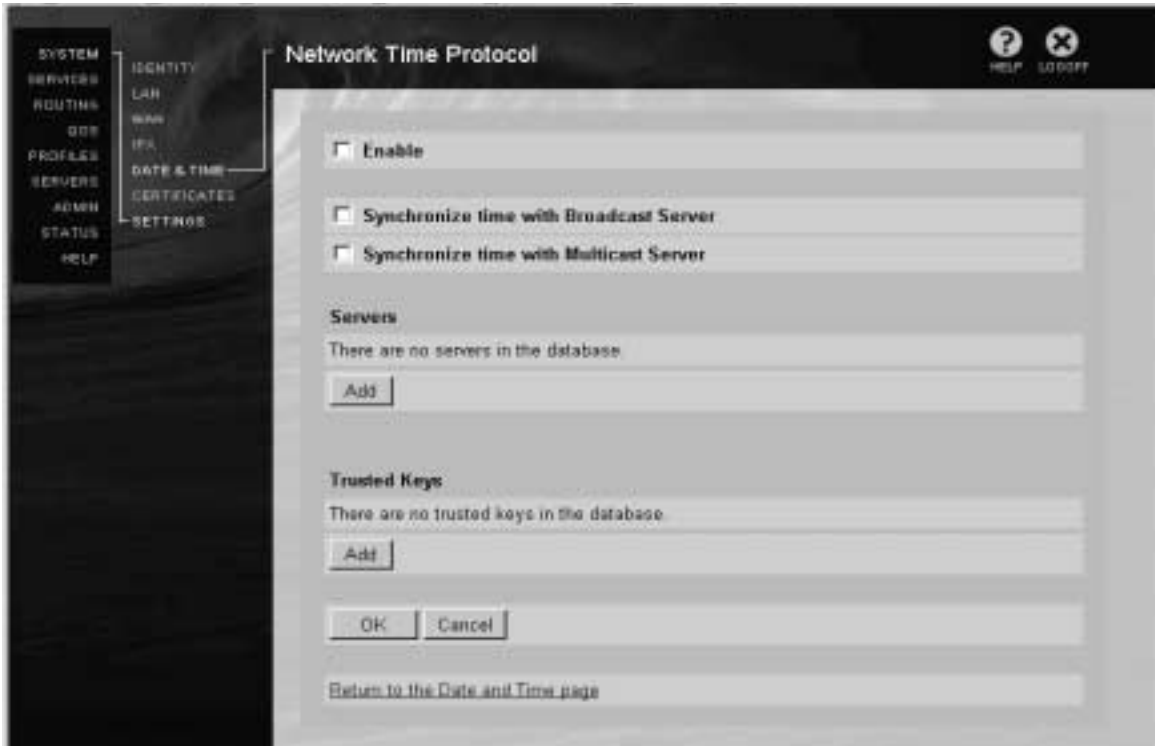
Time Zone

Click the drop-down list box to select the appropriate time zone. Time zones can be a critical factor in the usage of digital certificates.

Configure Network Time Protocol (NTP)

The System→Date and Time→Network Time Protocol screen allows you to set up the Network Time Protocol (NTP) on the switch. NTP synchronizes the clocks of various devices across networks. It also automatically adjusts the time of network devices so that they are synchronized within milliseconds. The switch receives NTP updates from an NTP time server and continuously synchronizes its clock to universal standard time. The switch supports up to eight NTP (unicast) servers and broadcast, multicast servers.

Figure 17 Network Time Protocol



Check the Enable NTP check box to enable NTP on the switch.

If you want the switch to listen for and respond to broadcast messages, check the Synchronize time with NTP Broadcast Server box. If you want the switch to listen for and respond to multicast messages, check the Synchronize time with NTP Multicast Server box. The IP multicast address is 224.0.1.1 for NTP.

NTP listens for both broadcast and multicast messages at the group address of the global network. To avoid disruption in multicast mode, both the client and servers should use authentication and the same trusted key and key identifier.

Servers

The switch lists any existing NTP servers.

Server IP Address

IP address of the NTP (unicast) server.

Interface

For security, you can specify either a Private or Public interface. The private interface is the management IP address. When adding a public interface, you can choose from a list of public interfaces. If you are using the Contivity Firewall, you need to configure an interface filter to add NTP.

Key ID

Specifies the Key ID for Message Digest (MD5) authentication. In authentication mode, each packet transmitted has a 32-bit Key ID and a 64/128-bit cryptographic checksum using MD5 algorithms. With MD5, the receiving peer recomputes the checksum and compares it with the one in the packet. They must share at least one MD5 key (trusted key) and must associate the shared key with the same Key ID.

Bursting

Specifies to send a burst of eight packets at each poll interval.

Version

NTP version number (1, 2, 3, or 4) used on the NTP server. The default is 3.

Actions

Edit

To edit an existing NTP server, click on the edit button in the Action column.

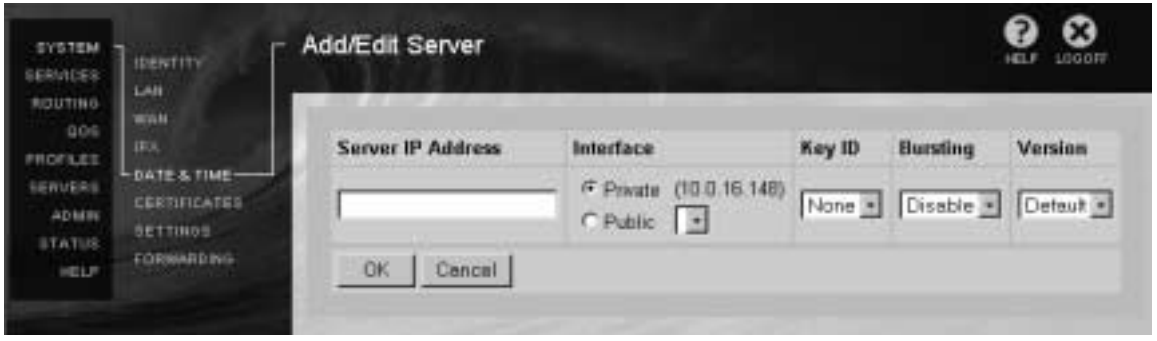
Delete

Click on the Delete button to delete an NTP server.

Add

You can add an NTP server by clicking on the Add button. The switch displays the Add/Edit Server screen. If you are adding an NTP server, enter the appropriate information as described above.

Figure 18 Add/Edit NTP server screen



Trusted Keys

Key ID

Specifies the Key ID for MD5 authentication.

Actions

Edit

To edit an existing key ID, click on the edit button in the Action column.

Delete

Click on the Delete button to delete the trusted key.

Add

You can edit an existing area key ID by clicking on the Edit button. The switch displays the Add/Edit Trusted Key screen. Enter the key Id, the password and the password confirmation.

Click on the Return to the Date and Time page link to return to the previous page.

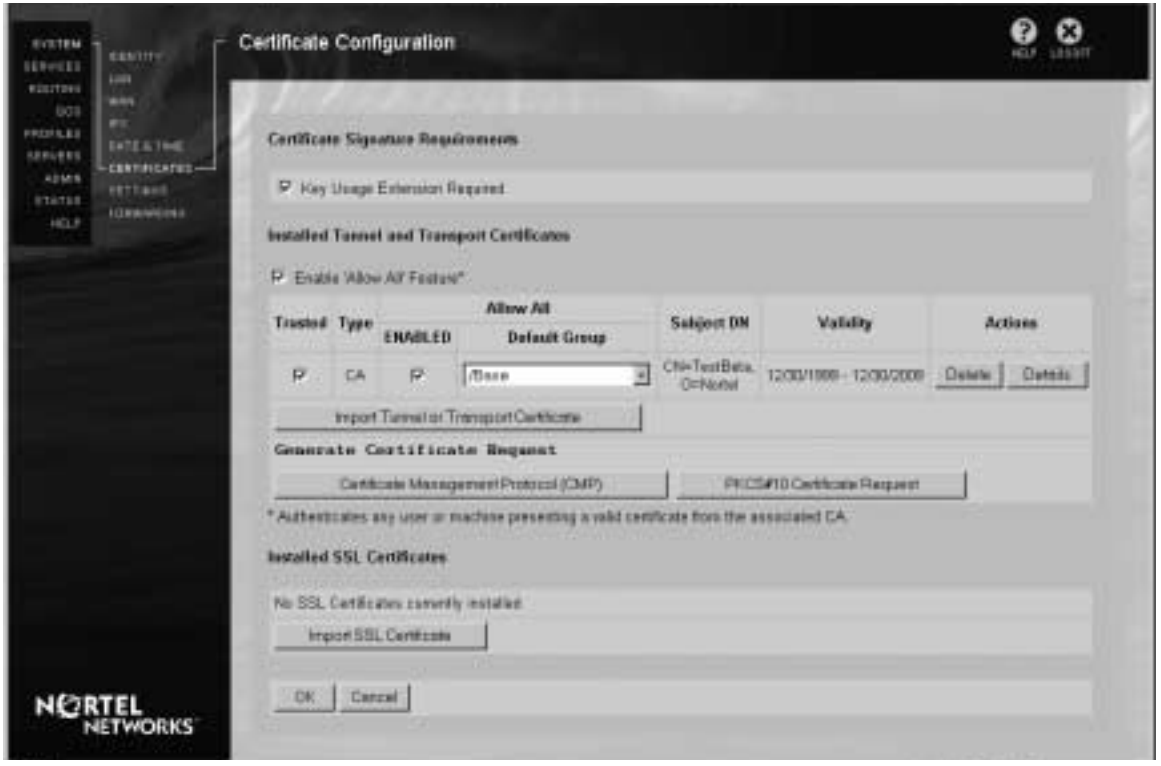
Certificates

This screen allows you to import both tunnel and SSL certificates to the switch and generate a certificate request for a server tunnel certificate. When you have added certificates to the switch, this screen lists the available certificates.

Tunnel Certificates are used to authenticate IPSec tunnel connections. SSL Certificates are used to secure connections with LDAP servers.

A Certificate is an electronic “document” that identifies an entity such as a Certification Authority. You should trust a certificate only if you trust the person or organization that issued it (an approved Certificate Authority).

Figure 19 Certificate Configuration



Key Usage Extensions Required

Enable this option to require key usage extensions to be present in certificates that are presented via a tunnel request. This option is enabled by default.

Enable Allow All Feature

Click the Enable button to allow all clients attempting to authenticate against a CA Certificate, without an explicit user entry, the ability to do so.

Note: Branch Office connections do not support the CA Certificate Allow All feature. Therefore, you must configure an explicit Branch Office connection.

Trusted

Check to designate this certificate as Trusted (you have previously verified that this certificate is authorized and has been validated).

Type

Shows the certificate type, whether it is a Certificate Authority (CA) or a Server Certificate.

Allow All

The Allow All feature must be Enabled for each CA Certificate against which you want to permit authentication without an explicit user entry. This allows anyone with a valid certificate from the particular CA to establish a tunnel connection.

Also, you must associate a Default Group with that certificate. The client authenticating with the Allow All feature then uses the attributes associated with that group.

Subject DN (Distinguished Name)

Shows the certificates Subject Distinguished Name components; for example, Common Name, Organizational Unit, Organization, and Country.

Validity

Shows the dates through which the certificate is valid (for example, 01/29/98 to 01/29/99).

Actions

Delete

Click to Delete the selected certificate. A delete confirmation dialog box then asks you to confirm the deletion.

Details

Click to view the specific details of the Certificate owner and issuer. This screen also shows the certificate's fingerprint, which is important in verifying the authenticity of a CA certificate, especially when first imported.

Import Tunnel or Transport Certificate

Click to display the PKCS certificate import screen. When importing a PKCS#7 encoded certificate, verify the fingerprint of the resulting imported certificate with the fingerprint supplied from the CA. It is important to obtain the fingerprint through some out-of-band mechanism (phone, postal mail, and so forth) to guarantee the supplied certificate is genuine.

Generate Certificate Request

The process for getting a certificate for your server requires the server to generate a public key pair and to send the public key to the CA for inclusion in the certificate. You will need to select a password to protect the private keys the first time that you generate a certificate request on a Contivity VPN Switch.

Certificate Management Protocol (CMP)

Click to display the Certificate Management Protocol (CMP) Certificate Request screen, which allows you to create a key and a certificate request.

PKCS#10 Certificate Request

Click to display the PKCS#10 Create New Key and Certificate Request screen, which allows you to create a key and a certificate request.

Import SSL Certificate

Click to display the certificate import screen. When importing a PKCS#7 encoded certificate, verify the fingerprint of the resulting imported certificate with the fingerprint supplied from the CA. It is important to obtain the fingerprint through some out-of-band mechanism (phone, postal mail, and so forth) to guarantee the supplied certificate is genuine.

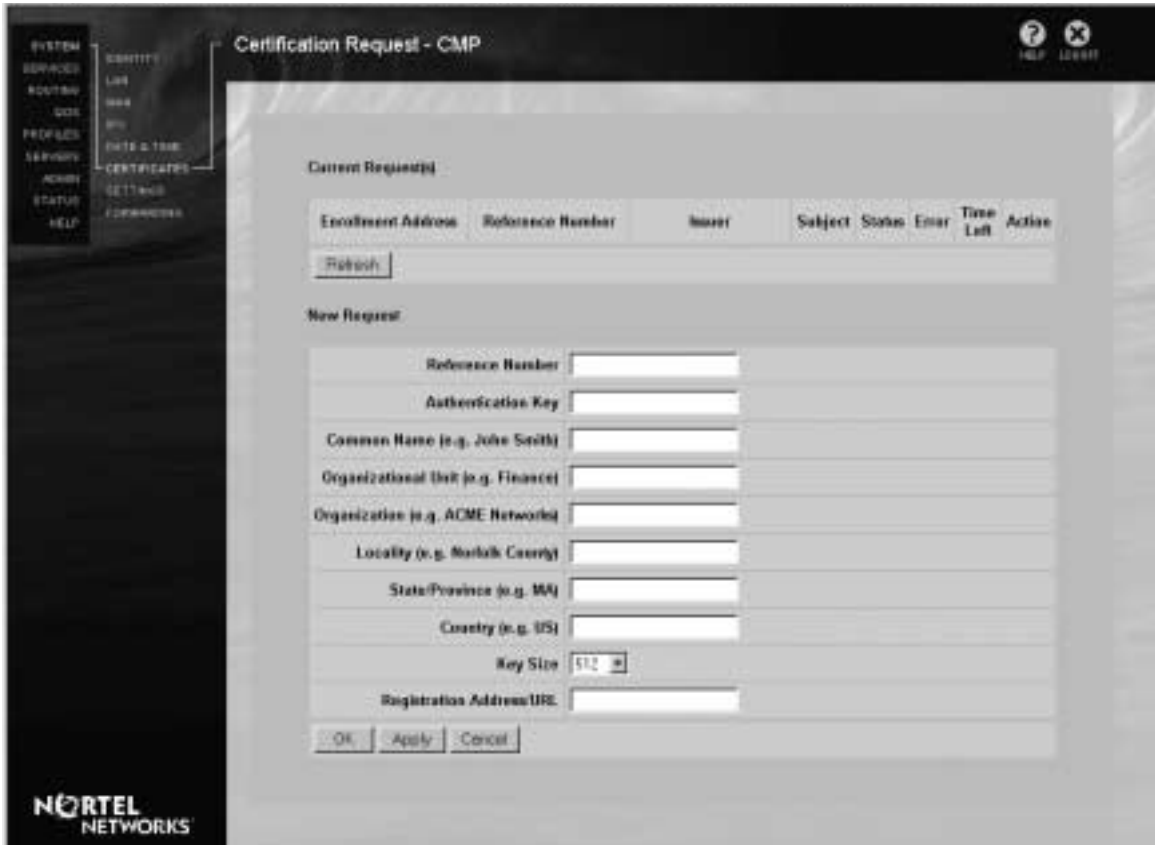
Generate Certificate Requests

Certificate Management Protocol (CMP)

The Certificate Management Protocol (CMP) Certificate Request screen allows you to create a CMP compliant certificate request. CMP is derived from the Entrust PKI management protocol. It includes management functions for the entire certificate and key life cycle. CMP uses CRMF to define message formats.

For the authentication purpose, the CA issues a secret value (initial authentication key) and reference value (used to identify the secret value).

Figure 20 Certificates→Certificate Management Protocol



Reference Number

Enter the reference value (used to identify the secret value), provided by the CA.

Authentication Key

Enter the Authentication key supplied by the CA.

Common Name

Enter the Common Name with which the switch is associated.

Organizational Unit

Enter the Organizational Unit with which the switch is associated.

Organization

Enter the Organization with which the switch is associated.

Locality

Enter the Locality in which the switch resides.

State/Province

Enter the State/Province in which the switch resides.

Country

Enter the Country in which the switch resides.

Public Key Size

Click the drop-down list to select one of the following exportable Public Key Sizes in bits (generally, larger keys are more secure):

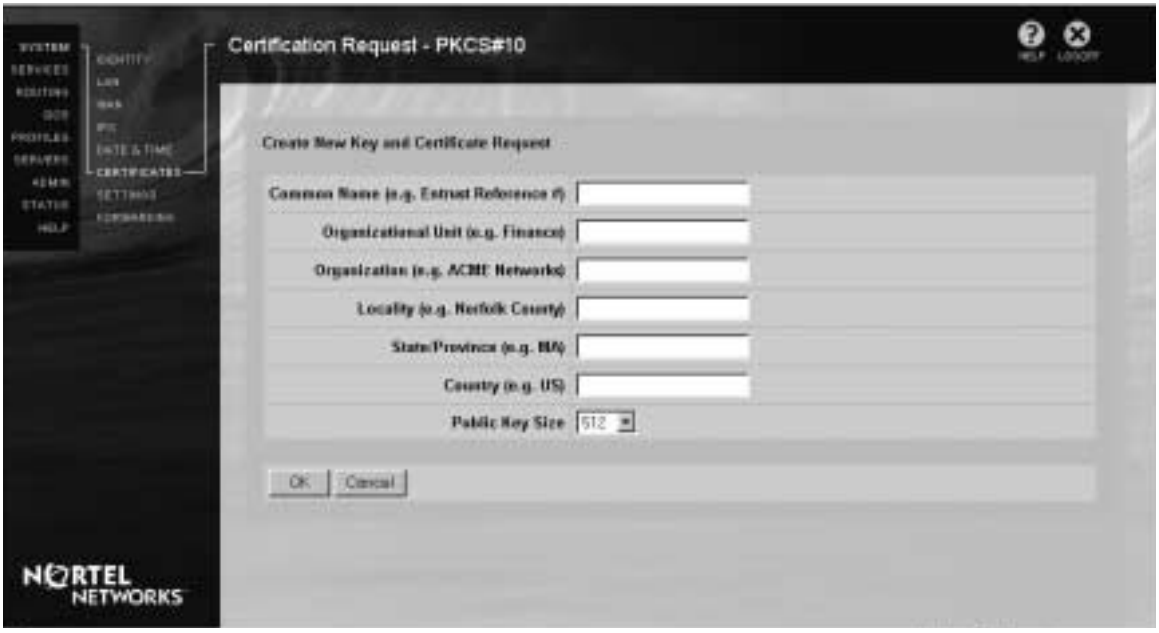
- 512
- 768
- 1024
- 2048 (US only)

Registration Address/URL

Enter the enrollment URL or destination (host name or IP address).

PKCS#10 Certificate Request

Figure 21 Certificates→PKCS#10 Certificate Request



Common Name

Enter the Common Name with which the switch is associated. For an Entrust PKI environment, this must be a valid Entrust Reference Number.

Organizational Unit

Enter the Organizational Unit with which the switch is associated.

Organization

Enter the Organization with which the switch is associated.

Locality

Enter the Locality in which the switch resides.

State/Province

Enter the State/Province in which the switch resides.

Country

Enter the Country in which the switch resides.

Public Key Size

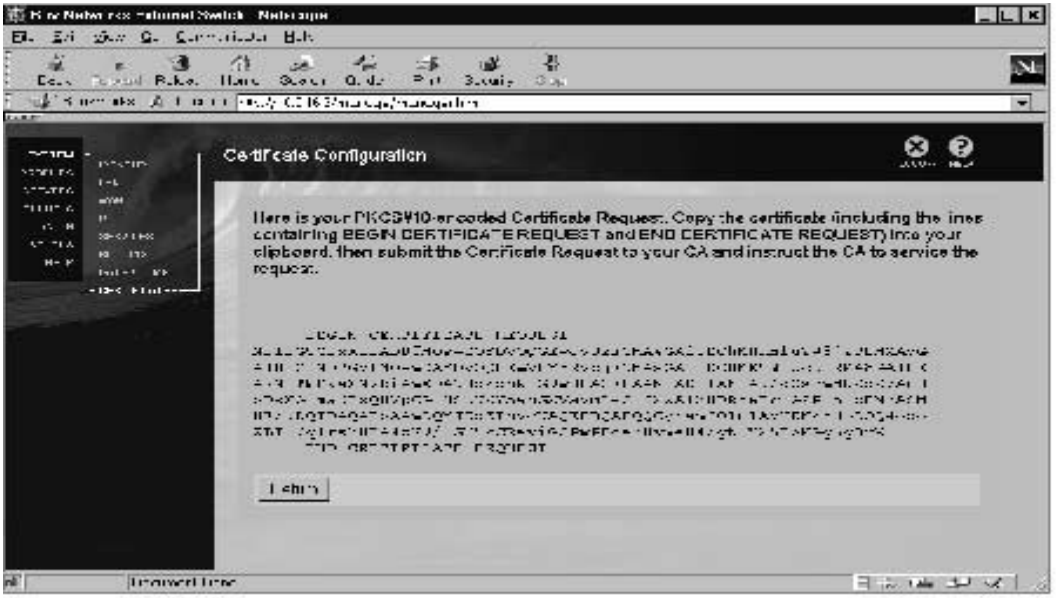
Click the drop-down list to select one of the following exportable Public Key Sizes in bits (generally, larger keys are more secure):

- 512
- 768
- 1024
- 2048 (US only)

PKCS #10-Encoded Certificate Request

The Generate Certificate Request button returns the following sample PKCS (Public Key Cryptography Standard) #10-encoded Certificate request. Copy the contents of the certificate request into your Web browser's copy buffer. Submit the request to the applicable CA by pasting the encoding into the CA's request screen, following the instructions provided by the CA.

Figure 22 Generated PKCS#10-encoded Certificate Request



Server Certificate

Click Server Certificate to indicate you are importing a Server Certificate. Importation of a Server Certificate must correspond to a previous Server Certificate request.

Trusted CA Certificate

Click Trusted CA Certificate to indicate you are importing a Trusted CA Certificate.

Pasting a PKCS #7 Certificate

Copy the Public Key Cryptography Standard (PKCS) #7 ASCII text that is returned by the Create New Key and Certificate Request into the dialog box. Typically, a Certificate Authority provides this text to you.

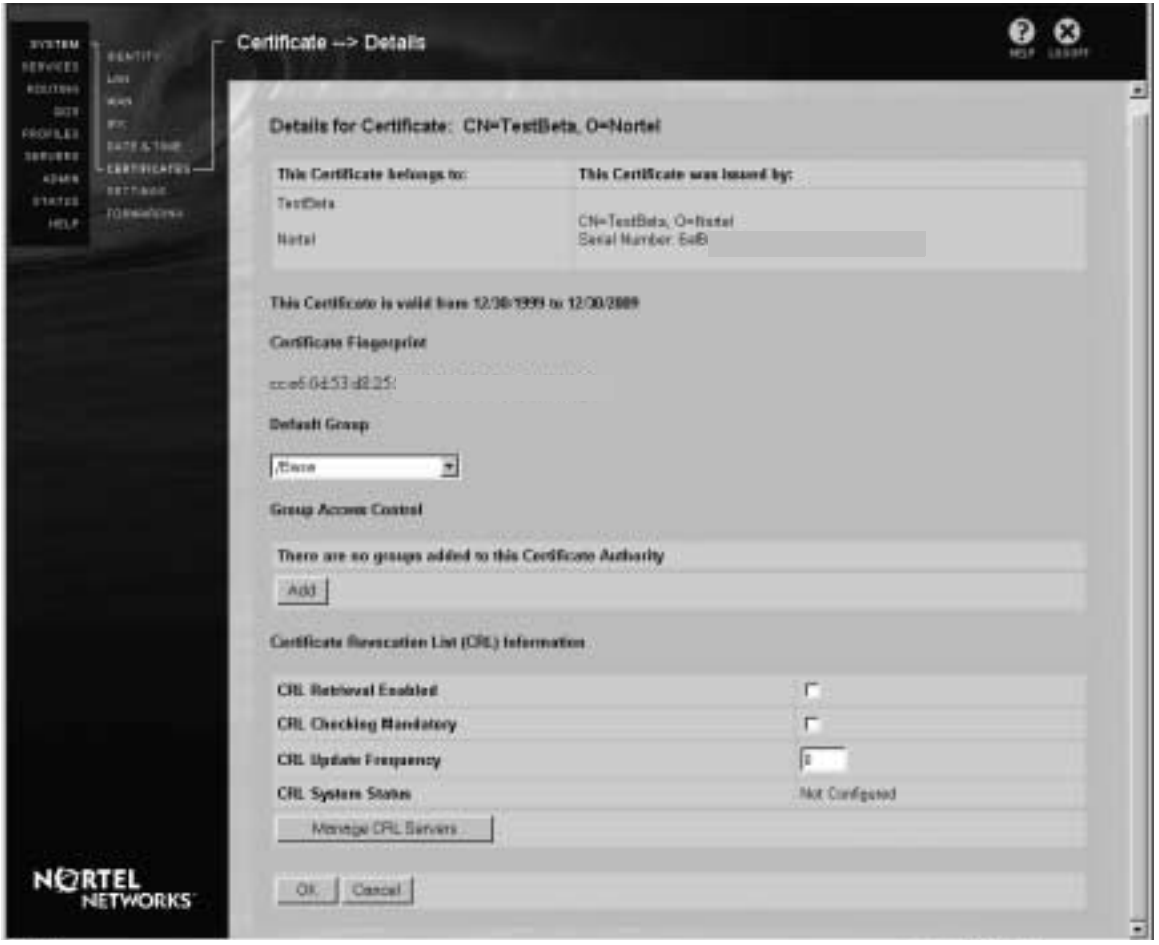
OK

Click OK to generate a certificate and store it on the switch.

Certificate Details

This screen provides the certificate details, including the owner of the certificate and who issued the certificate. Additionally, this screen provides the validity dates, the certificate fingerprint and, if a CA Certificate, the certificate revocation list details.

Figure 23 Certificate Details



This Certificate Belongs To

Shows the certificate owner's X.500 distinguished name.

This Certificate Was Issued By

Shows the issuer of the Certificate (the Certificate Authority). In addition to the main attributes, this field also shows the issuer's Certificate's serial number.

Validity Dates

The starting and ending Dates through which the certificate is valid (for example, 01/29/98 to 01/29/99).

Certificate Fingerprint

The unique identifier that is derived from MD5 hashing the certificates. The identifier should be compared with the fingerprint supplied directly from the certificate's issuer (for example, a CA). If the fingerprints do not match exactly, the certificate has been forged or modified.

Default Group

Drop-down list of the existing default groups.

Association of Certificate Subject DN with groups

For each trusted CA, shows a set of associations between certificates' subject DNs and group profiles. You can edit or delete existing associations by clicking on the appropriate buttons. You can also click on the Add button to add an association between the subject DN and a group profile.

Certificate Revocation List Information

CRL Checking Enabled

Click to enable the Certificate Revocation List (CRL) feature.

CRL usage is enabled on the switch on a per CA basis. To enable the use of CRLs for a CA, select the Details button on the main System→Certificates screen. The section labeled Certificate Revocation List Information is used to configure the necessary information. The Enabled check box turns on CRL checking of certificates for the particular CA. The Search Base, Host, Connection, and Update frequency values must be set for proper access to the CRL LDAP directory store.

CRL Checking Mandatory

This setting determines if a CRL must be present when an IPSec tunnel is established to a particular CA. If checked, when the connection is made, a CRL for that CA must be present. If no CRL is present, the tunnel is not established. This setting has no effect unless "CRL Enabled" is checked.

CRL Update Frequency

Enter a value in minutes that represents the frequency with which the switch should query the CA's LDAP server for a newly published CRL. The default value 0 indicates that this switch does not update any CRLs. This is useful when many switches share an LDAP database, but you want only one switch to actually perform the update operation. To minimize the load on an external LDAP server, it is important to make sure only 1 or 2 switches are updating a shared CRL entry in a multiple switch, shared external LDAP environment.

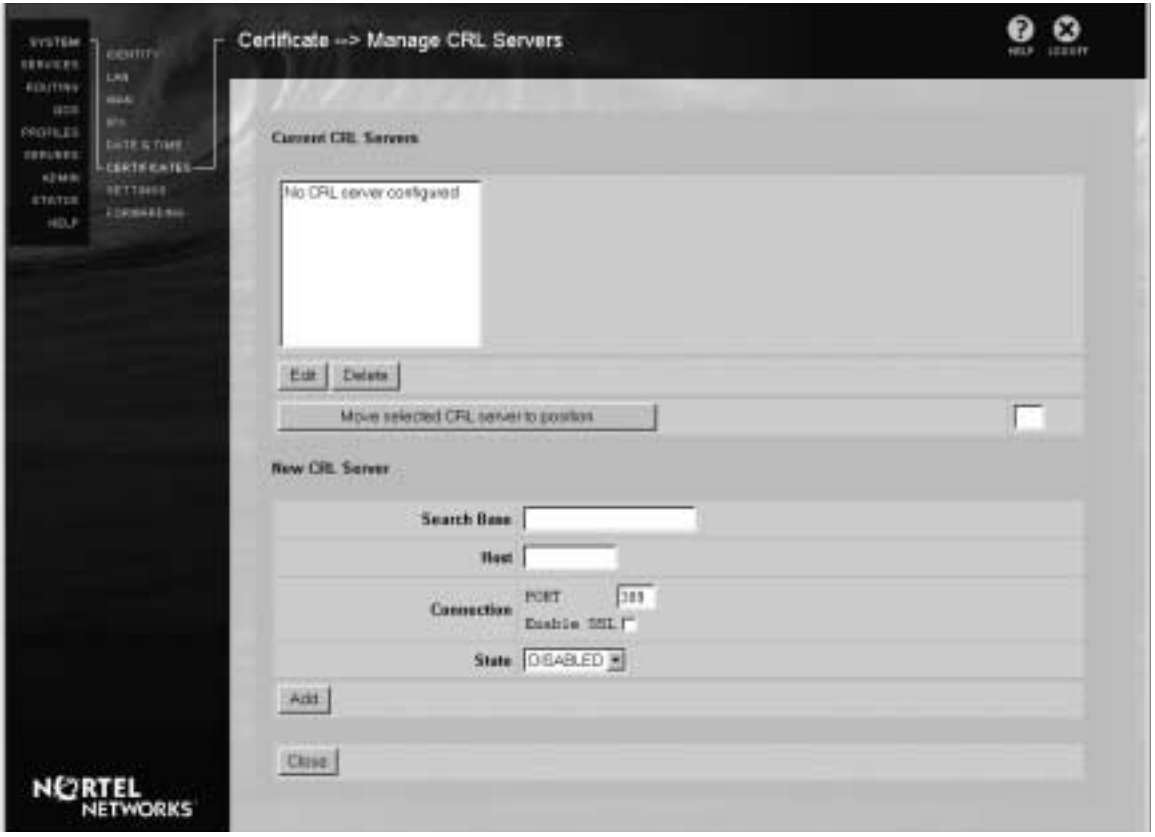
CRL System Status

The status field is read-only and is automatically updated by the switch to reflect the CRL updating activity.

Manage CRL Servers

The Manage CRL Servers button accesses the Manage CRL Servers screen. Use this screen to configure and manage CRL servers.

Figure 24 System→Certificates→Details→Manage CRL Servers



Current CRL Servers

Shown at the top of this screen is a list of currently configured CRL servers for the CA.

Edit

To edit a server, select it and click on the Edit button. After making your changes, click on the OK button to save the changes.

Delete

To delete a server, select it and click on the Delete button.

Move selected server to position

To move a server to a different position, select it, enter the desired position number in the field next to the button, and then click on the Move selected server to position button.

New CRL Server

Use this section of the Manage CRL Servers screen to configure and add a new CRL server.

Search Base

The search base represents the portion of the X.500 directory where the CA stores certificate revocation lists. Following is a sample search base entry:

```
ou=Engineering, o=Nortel Networks, c=US
```

Host

This field contains the host name or IP address of the LDAP-accessible directory server that is storing the published CRLs. This host must be reachable via one of the switch's private interfaces, and if a host name is used in place of an IP address, then one or more DNS servers must be configured on the switch’s System Identity screen.

Connection

Enter the port number that is associated with the LDAP server. Optionally, enable the use of the Secure Socket Layer (SSL) to secure the connection with the LDAP server. SSL is not required in general for handling CRLs since a CRL is signed and is therefore protected against modification and spoofing.

State

Enable or disable the CRL server by selecting the desired state from the list box.

Add

Click on the Add button to add a new CRL server.

To add a new server, enter the Search base, host, and connection fields, choose enabled or disabled, and then click on the Add button.

Switch Settings

The System→Settings screen lets you configure Safe Boot mode, the serial port and the Log file.

Figure 25 System→Switch Settings

Safe Mode Configuration

The switch can be booted in one of the two system modes: Safe Mode or Normal Mode. Each mode has its own software image, configuration files, and LDAP database.

A system booted in Safe Mode is only allowed to accept secured management tunnel establishment. When the secured management tunnel is established, Telnet, HTTP, and FTP traffic are allowed to come into the switch; no other VPN traffic is allowed through the secured management tunnel or the switch.

In Normal Mode, the system operates with the normal software and configuration and transports both VPN traffic and management traffic.

Enable Safe Mode

Use this check box to enable and disable Safe Mode.

Safe Mode Duration

The Safe Mode Duration setting determines how the long the system operates in Safe Mode before attempting to reboot in Normal Mode.

Serial Port Configuration

The Serial Port Configuration section of the System-Settings screen provides options for configuring the switch's serial port. The parameters that you must set to enable your switch to communicate via the serial port are described below.

Whenever you change from either serial menu mode to PPP mode, or vice versa, you must restart the switch for the change to take effect.

Menu Access Level

The Menu Access Level setting determines which commands are available in a serial console port menu.

- Unrestricted - All commands are available to the user (default).

- Restricted 1 - System Reset commands plus the commands to change interface IP address and mask.
- Restricted 2 - Only Reset commands are available.

Mode

Select one of the following Modes of operation:

- Serial Menu (default)
- PPP
- Auto Detect

Serial Menu

In this mode, a standard menu interface is presented. You can use an application such as Hyper Terminal, when directly connected to the switch, to access the menu interface. The switch uses the COM port for a serial menu terminal session. The switch's serial port baud rate is 9600 by default. When you change the serial interface baud rate, you must press the Reset button.

PPP

You can set up the switch to use the Point-to-Point Protocol (PPP) over the serial port. This feature allows you to manage the switch from a remote location using PPP and the serial interface. If the switch were to become unreachable over the Internet, you could still dial up and manage it through the serial interface menu.

This feature allows you to access all of the management services (HTTP, Telnet, FTP, SNMP) through the Web interface. When a session is established through PPP, the serial interface acts as a private WAN interface with an internal IP address (0.0.1.35).

Auto Detect

This feature automatically detects whether the switch is using PPP or serial menu mode at startup. It cannot determine the switch's baud rate, nor can it determine a change from PPP to serial menu mode, except upon startup.

Auto Detect checks the mode each time the switch is restarted. When performing its Auto Detect check, the switch sends out AT command set characters to configure a modem if one is attached.

When the switch is in Auto Detect mode, and if a terminal session is connected and the terminal baud rate is the same as the switch's, the terminal displays the AT command sets on the screen. Simply press Enter more than five times before a serial menu session is started.

Baud Rate

Select one of the following Baud Rates to match the baud rate of your terminal:

- 57600
- 38400
- 19200
- 9600 (default)

Modem Initialization

Enter the modem initialization string. Refer to the manufacturer's documentation to learn the vendor-specific character initialization string. Preconfiguring the modem and using the switch's default initialization string (ATZ) provide the best results.

A sample 3Com/US Robotics 56K modem initialization string to instruct the external modem to connect at 19,200 Kbps follows:

```
ATZ&B1AT&N10
```

Reset Serial Port

When you select the baud rate, you must click the Reset button to change the port to the new baud rate.

Log File Configuration

The Log File Configuration sets the life time of the log files. The default log file life time is 60 days.

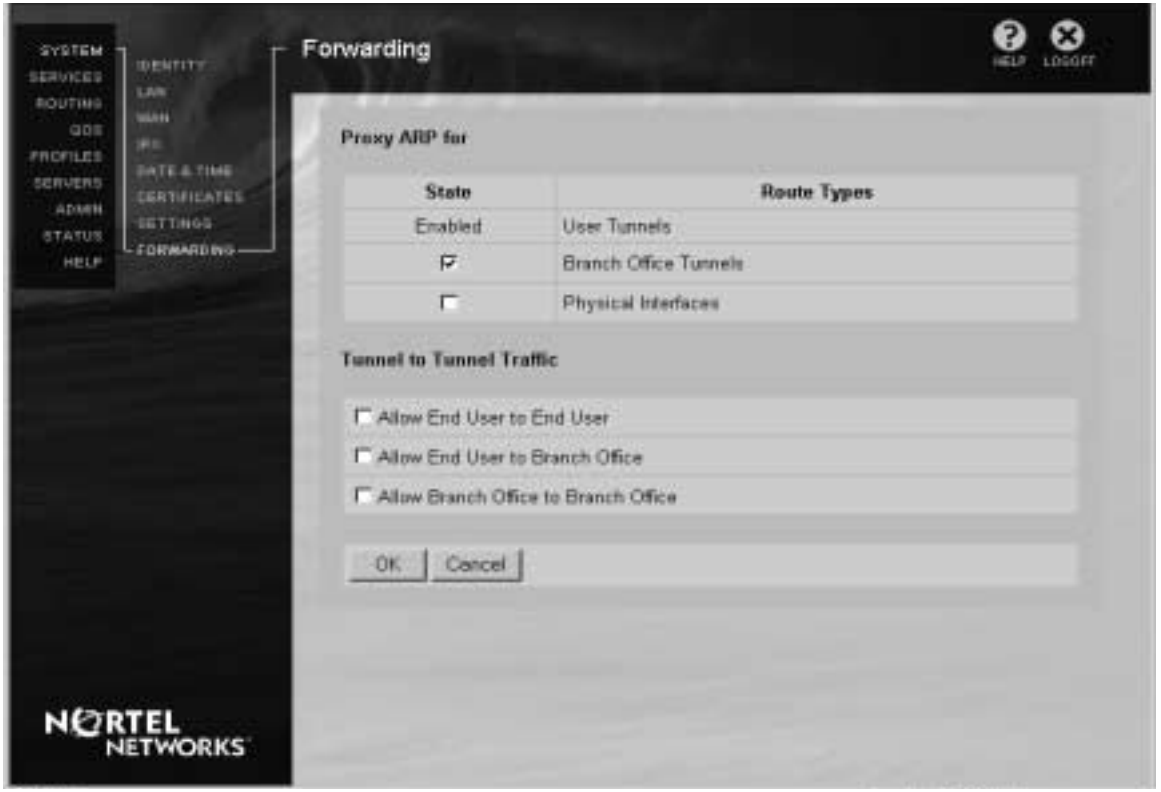
Log File Life Time

Select a value for the log file life time from the list.

Forwarding

The System→Forwarding page allows you to configure Proxy ARP settings and Tunnel to Tunnel traffic settings.

Figure 26 System Forwarding



Proxy ARP for

The Contivity VPN Switch can be configured to respond to ARP requests on any of the physical interfaces. The switch responds to the following types of routes:

- User Tunnels are routes created for user tunnels. This entry is enabled by default and cannot be changed.
- Branch Office Tunnels are routes available through branch office connections. This option is disabled by default.
- Physical Interfaces are routes available through physical interfaces. This option is disabled by default.

Tunnel to Tunnel Traffic

Click the appropriate check boxes to enable the different types of tunnel-to-tunnel traffic. All of these options are **disabled** by default for security reasons.

Allow End User to End User

Click to allow a remote user who is tunneled into the corporate switch to access other remote users that are also tunneled into the switch.

Allow End User to Branch Office

Click to allow a remote user who is tunneled into the corporate switch to access the resources of branch offices that are connected to the switch.

Allow Branch Office to Branch Office

Click to allow users who are on one branch office connected to your switch to access resources on other branch offices that are connected to your switch.

Chapter 2
Services

When you click on the Services menu, the list of services appears in the top left column.

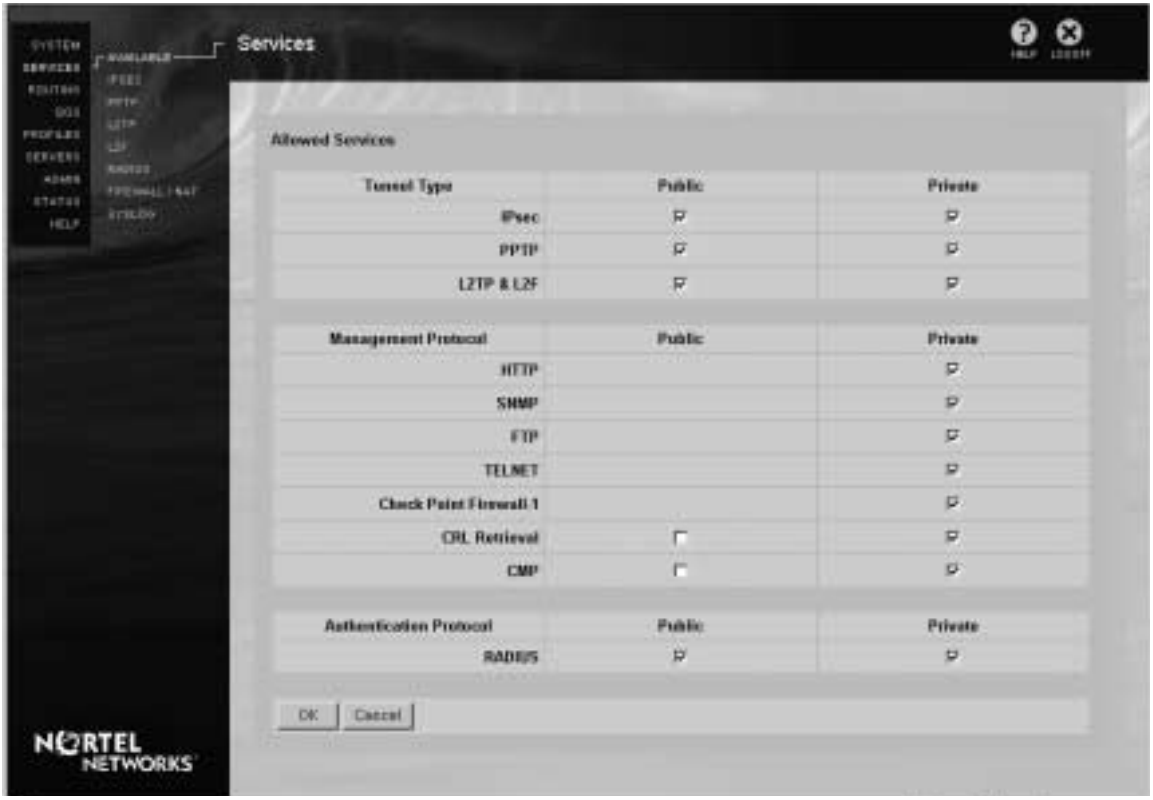
The Services menu allows you to manage the available services, control the type of tunnel access to the switch, and configure how the RADIUS service and the Firewall service are used. You can also specify the management and service protocols that can be used by the switch.

Figure 27 Services menu

Available Services

The Available Services include Tunnel Types, Management Protocols, and Authentication Protocol.

Figure 28 Available Services



Allowed Services

The Allowed Services include Tunnel Types, Management Protocols, and Authentication Protocol.

Tunnel Types

The Tunnel Type portion of this screen allows you to control each of the supported tunneling protocols on Private and Public interfaces. All tunneling protocols are enabled on the Public and Private networks by default. Since data in tunnels is encrypted, this default setting guarantees that all interactions with the switch are private. To prevent tunnel connections of a particular type (for all users including Administrators), you can simply disable the tunnel type here.

For example, if you want to use IPSec as your only Public tunneling protocol, then disable the Public selection (remove the checkmark) for PPTP, L2TP, and L2F. By leaving IPSec, PPTP, L2TP, and L2F enabled on the Private side, you can establish tunneled connections to the switch using any of the tunnel types from within your corporation (Private).

Management Protocols

Management related protocols are used on the switch's Private Interfaces. Use the Available Services screen to control which management protocols can be accessed directly from a private LAN. Enabling Management Protocols allows you to access the switch for management purposes in a nontunneled environment, if the filter permits.

As network administrator, you might decide to deny access to the HTTP or SNMP protocols coming through private nontunneled connections. This ensures that switch management can be accomplished through tunneling only.

Caution: Make sure that the tunneling features are working properly before you disable the local HTTP management option. Otherwise, you cannot manage the switch.

Similarly, you might want to prohibit the ability to transfer files to or from the system using FTP for security reasons.

Note: After your initial system configuration, you might want to disable Private HTTP access and restrict access to Tunneled connections only.

Table 5 Management protocols

Management Protocol	Description
HTTP	HyperText Transfer Protocol is the software protocol that allows Web servers and clients to communicate (it allows for an HTML management interface).
SNMP	Simple Network Management Protocol is the Internet standard that allows you to manage devices and receive traps on an IP network. Due to security reasons, the switch supports SNMP MIB II get commands only.

Table 5 Management protocols (continued)

FTP	File Transfer Protocol is a TCP/IP protocol that allows you to transfer files between systems over a network.
Telnet	Telnet is the virtual terminal protocol that allows users on one device to access and manage a remote device. Telnet is used by Nortel Networks Customer Support personnel strictly for maintenance purposes. Telnet has direct access to the switch System Services and therefore should normally be disabled for security reasons. Telnet must be enabled in order to use the CLI via Telnet.
FIREWALL	The FireWall-1* management protocol that is used for communication between the FireWall-1 Management Station and the CheckPoint FireWall-1 running on the switch.
CRL Retrieval	Enables retrieval of CRLs through the selected interface type. Both interfaces can be enabled at the same time. Refer to “SSL and Digital Certificates” for information about Digital Certificates.
CMP	Enables CMP (Certificate Management Protocol) through the selected interface type. Both interfaces can be enabled at the same time. CMP defines messages used for interactions between CAs and clients or between CAs that cross-certify each other.

Note: In order to provision a Contivity VPN Switch that has been reset to factory defaults with a file produced by the CLI command `show running config`, the Contivity VPN Switch must have an IP Management address assigned and must have the FTP management protocol enabled on the Services→Available screen.

Authentication Protocols

RADIUS

Use the RADIUS check boxes to permit RADIUS requests on the public and private interfaces of the switch. If you enable RADIUS traffic on this screen, the settings on the Services→RADIUS screen are used (RADIUS must also be enabled on that screen).

IPSec Settings

The IP Security (IPSec) standard defines a set of security protocols that:

- Authenticate IP connections.
- Add data confidentiality and integrity to IP packets.
- Are transparent to applications and the underlying network infrastructure.

IPSec supports multiple encryption and authentication protocols so that your security policy can dictate levels of data privacy and authentication. IPSec also supports load balancing and fail-over.

IPSec allows for multivendor interoperability. It uses a flexible key management scheme called the Internet Security Association Key Management Protocol (ISAKMP), which enables peer connections to quickly and dynamically agree on compatible security and connection parameters (keys, encryption, and authentication).

Note: To allow RADIUS authentication with the IPSec client you must enable the RADIUS server on the Profiles→Groups→Edit→IPSec screen.

Figure 29 IPSec Settings

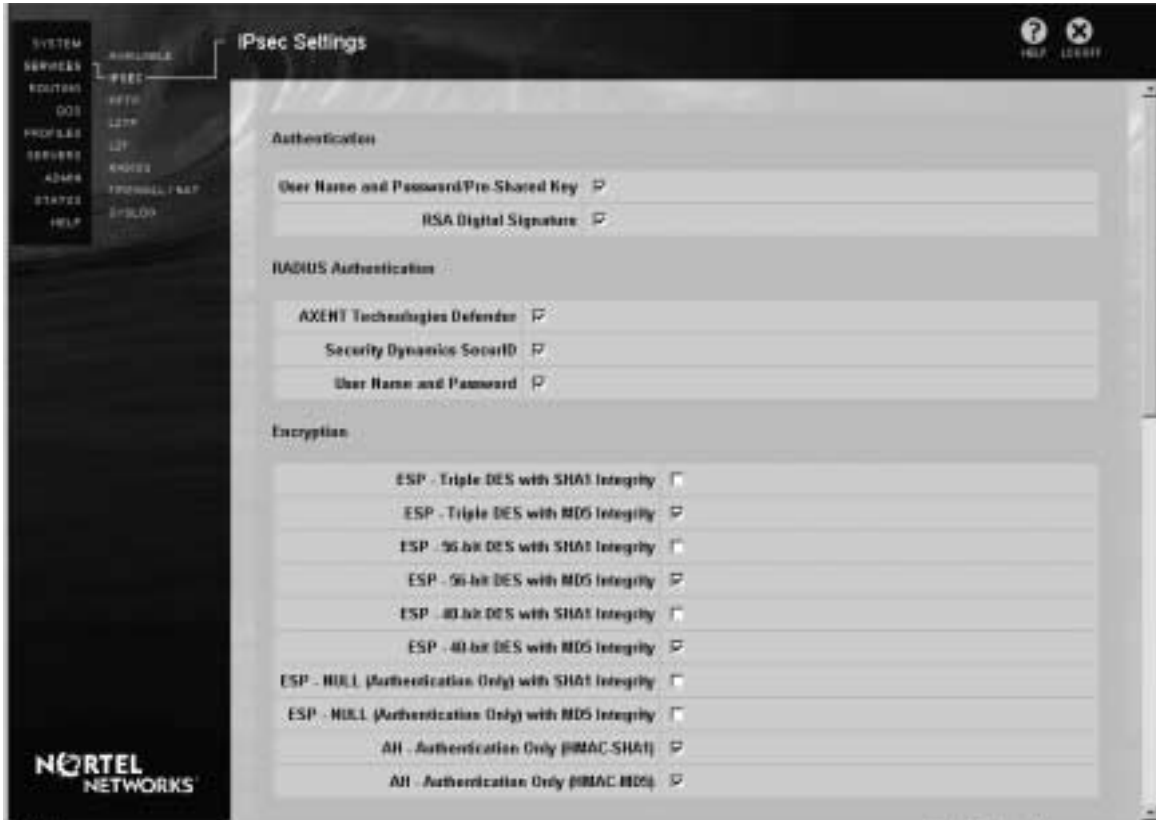
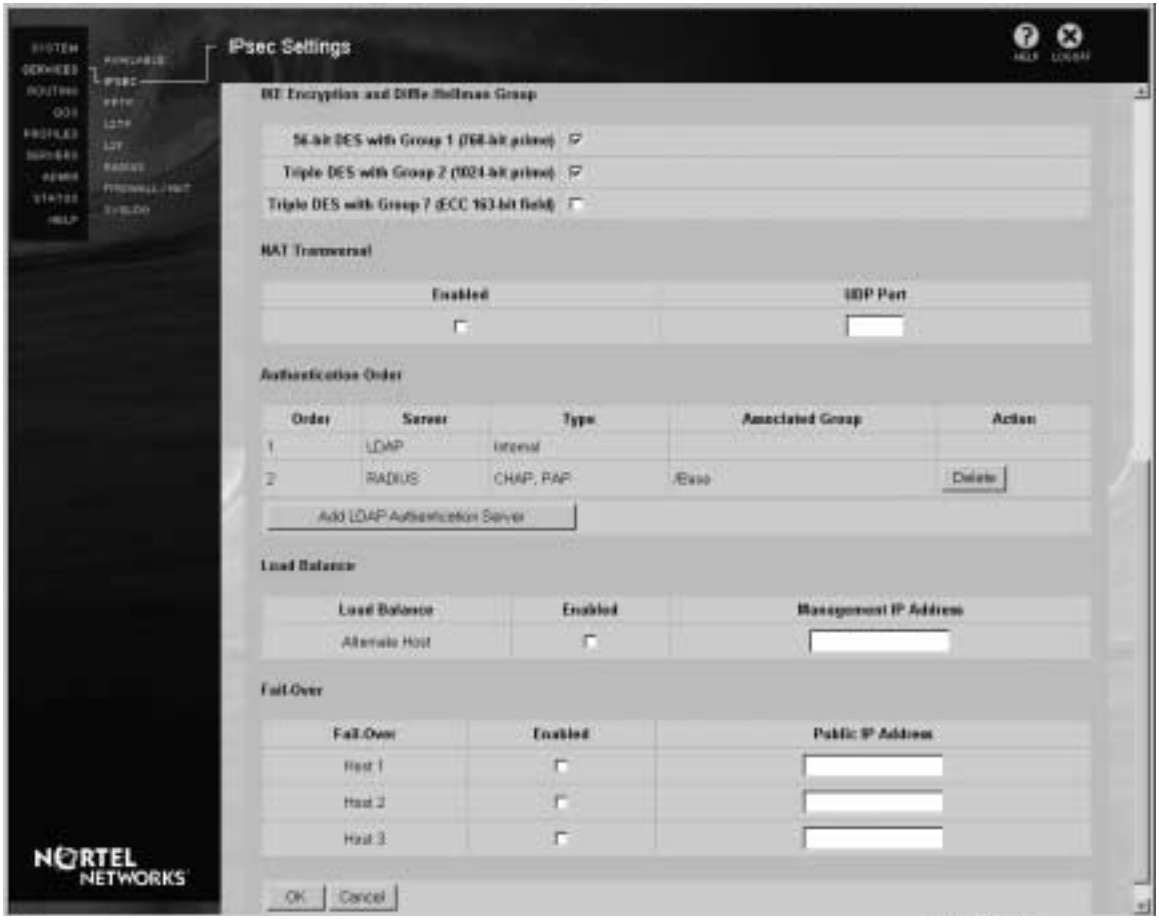


Figure 30 IPSec Settings



Authentication

User Name and Password/Pre-Shared Key

Click to enable authentication with a username and password.

RSA Digital Signature

Click to enable authentication with an RSA Digital Signature.

RADIUS Authentication

Click to Enable support for the authentication types that your RADIUS Server supports and that you expect to use:

- AXENT Technologies Defender--AXENT OmniGuard/Defender authentication.
- Security Dynamics SecurID--Security Dynamics SecurID authentication.
- User Name and Password--Username and password authentication; the username and password are encrypted.

Encryption

Click the appropriate checkbox to either enable or disable the supported Encryption methods for this group.

Note: Using higher-level encryption, such as Triple DES, decreases performance.

The encryption methods are shown on the screen in order of strength, from strongest to weakest. All of the encryption methods ensure that the packet came from the original source at the secure end of the tunnel. Some of the encryption types do not appear on non-US models that are restricted by US Domestic export laws.

If two devices have different encryption settings (due to either US export laws or administrative configuration), the two devices negotiate downward until they agree on a compatible encryption capability. For example, if a switch in the US attempts to negotiate Triple DES encryption with a switch in Australia that is using 56-bit DES, then the Australian switch rejects Triple DES encryption in favor of the 56-bit DES.

The following table shows a comparison of the security provided by the available encryption and authentication methods.

Table 6 Comparing encryption and authentication methods

Method		Encryption of IP packet payload	Authentication of IP packet payload	Authentication of entire IP packet
ESP	Triple DES SHA1	Yes	Yes	No
	Triple DES MD5	Yes	Yes	No
	56-bit DES SHA1	Yes	Yes	No
	56-bit DES MD5	Yes	Yes	No
	40-bit DES SHA1	Yes	Yes	No
	40-bit DES MD5	Yes	Yes	No
	NULL SHA1	No	Yes	No
	NULL MD5	No	Yes	No
AH	HMAC SHA1	No	No	Yes
	HMAC MD5	No	No	Yes

The following topics describe important aspects and terminology to aid you in selecting the appropriate encryption method for your tunnel server.

Types of Integrity Checks

The switch uses the following two types of integrity checks:

- SHA1

  The Secure Hash Algorithm (SHA1) produces a 160-bit hash. It is regarded by cryptographers as being more resistant to attacks than MD5. It does not encrypt data.

- MD5

  The Message Digest 5 Algorithm (MD5) is used to confirm the authenticity of a packet. It produces a 128-bit hash. It does not encrypt data. Also, MD5 provides integrity that detects packet modifications.

- HMAC

  The Hashed Message Authentication Code (HMAC) is a technique that uses a secret key and a message digest function to create a secret message authentication code. The HMAC method strengthens the SHA1 and MD5 technique.

Encapsulating Security Payload (ESP)

The Encapsulating Security Payload (ESP) provides confidentiality for IP datagrams by encrypting the payload data to be protected. Data Encryption Standard (DES) is an encryption block cipher algorithm. The switch supports the following variants of the DES algorithm:

- Triple DES uses a 168-bit key. It uses the DES encryption algorithm three times. The first 56 bits of the key is used to encrypt the data, then the second 56 bits is used to decrypt the data. Finally, the data is encrypted once again with the third 56 bits, which triples the algorithm's complexity.
- 56-bit DES and 40-bit DES use their respective 56-bit or 40-bit key (with 8 bits of parity) over a 64-bit block. The 56 or 40 bits of the key are transformed and combined with a 64-bit message through a complex process of 16 steps.
- Both 56- and 40-bit DES require the same processing demands, so you should use 56-bit DES unless local encryption laws prohibit doing so.
- The Null specification provides authentication only. No encryption is done.

Authentication Header (AH)

Authentication Header (AH) provides data integrity and source authentication. The AH method does *not* encrypt data.

The use of a NAT device in the tunnel path can sometimes cause the AH method to report a security violation.

IKE Encryption and Diffie-Helman Group

On this screen, you set the global IKE encryption and Diffie-Helman group for IPSec. If you select both 56-bit DES with Group 1 and Triple DES with Group 2 option, you can edit this field on the Profiles→Branch Office→Edit→IPSec screen or the Profiles→Groups→Edit→IPSec screen.

From the drop-down list, select one of the following:

- Both 56-bit DES with Group 1 and Triple DES with Group 2
- Triple DES with Group 2 (1024-bit prime)
- 56-bit DES with Group 7 (768-bit prime)

NAT Traversal

NAT (Network Address Translation) Traversal allows a number of devices on a private network to access the Internet simultaneously without each requiring its own external IP address. Most hotels and airports that provide Internet connectivity use NAT to connect to the Internet.

To use NAT Traversal, a UDP port must be defined. It is used for all client connections to the switch. This port must be a unique and unused UDP port within the private network.

By default, NAT Traversal is disabled and no UDP port is defined.

Enabled

Check the Enabled box to enable the NAT Traversal feature.

UDP Port

Specify the UDP Port to be used for NAT Traversal. The supported range is 1025-49151.

Authentication Order

The IPSec, PPTP, L2TP, and L2F tunnel types each have an Authentication Order table, which lists the corresponding servers, authentication types, associated groups, and actions. The LDAP server is always queried first, then RADIUS, if applicable. The Authentication Order descriptions that follow are the same for each tunnel type.

Order

Shows the order of authentication preference.

Server

The switch supports LDAP and RADIUS authentication servers. The switch always attempts to authenticate a remote user against the LDAP database. If a User ID (UID) and password are found, the switch uses the attributes that are defined for that user's group.

The switch can also authenticate against a RADIUS database. When using RADIUS for authentication, you can assign LDAP groups to users in the RADIUS database to take advantage of different profiles, or you can simply assign all RADIUS users into a single "default" group. The default RADIUS group is stored in the LDAP database. Refer to "RADIUS Authentication Class Attribute Values" for additional information on RADIUS Authentication Class Attributes and their relationship to an LDAP database.

Type

LDAP can be either an Internal or External server.

The types of RADIUS authentication currently associated with the server are:

- AXENT--This is AXENT OmniGuard/Defender challenge response token security authentication. The AXENT OmniGuard/Defender uses a personal identification number (PIN) and password, coupled with a challenge response security dialog box, to authenticate user identity.
- SecurID--This is Security Dynamics SecurID token security authentication. The SecurID uses a PIN and the current code generated by a token assigned to the user to authenticate user identity.
- CHAP--This is the Challenge Handshake Authentication Protocol (CHAP).
- MS-CHAP--This is a Microsoft variant of CHAP that includes data encryption.
- PAP--This is Password Authentication Protocol.

Associated Group

This is the Group from which authorization and operational settings are taken if a group attribute is not found in the authentication database.

Action

Delete--Click to remove the configured server. You are prompted to confirm your deletion request.

Add--Click to add an authentication type.

Load Balance

Click to enable Load Balancing of one switch with an alternate switch. Load Balancing is a protocol between two switches that exchanges information about the number of sessions of each connection priority and the CPU utilization. When a connection is being established, the first switch determines which of the two switches should service the session. The switch and the alternate switch must be in the same location (they must be in communication via the private interface).

Management IP Address

Enter the private management IP address of the switch that you want to serve as the alternate switch for Load Balancing.

Fail-Over

Click to enable Fail-over of the selected switch. A Fail-over condition is detected in approximately two minutes. If a connection is somehow terminated or lost, the client then attempts to connect to the first-listed Fail-over switch. It tries each switch in succession and if no connection is established, it stops.

The switch IP addresses (do not use domain names) must be public interfaces if the switches are in remote locations. Also, alternate switches should mirror the same configuration as the primary switch; otherwise, the connection information on the client does not match and results in authentication failures.

Public IP Address

Enter the public IP address of the switches to which you want to Fail-over in case the primary switch connection terminates.

PPTP Settings

The Point-to-Point Tunneling Protocol (PPTP) is supported by Nortel Networks, Microsoft, and other vendors. The PPTP client is available for Windows 95 and is built-in to Windows 98 and Windows NT®. Third-party vendors have developed PPTP clients for Windows 3.1 and the Macintosh operating system.

Figure 31 PPTP Server

Authentication

PPTP settings allow you to select a specific authentication server type; for example, RADIUS. Each server type allows you to specify an authentication scheme: MS-CHAP, CHAP, or PAP.

Note: Not all RADIUS servers support all forms of authentication. Failure to match PPP authentication methods with RADIUS server capabilities results in user-authentication failures. Check your vendor's RADIUS documentation for additional information.

Authentication Order

The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions. The LDAP server is always queried first, then RADIUS, if applicable. Refer to "Authentication Order" for a description of the Authentication Order table.

Add LDAP Authentication Server

Click on the Add LDAP Authentication Server to add an LDAP server to be used for authentication.

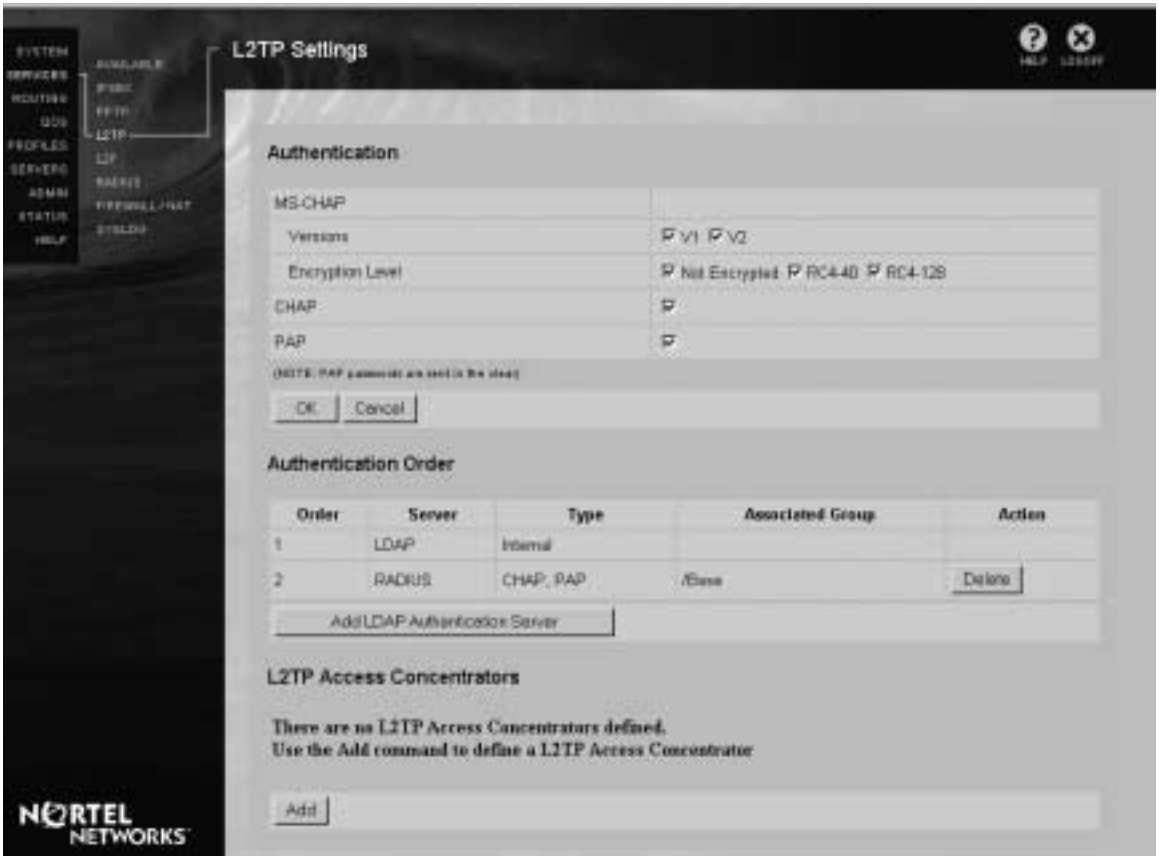
Swap Servers 2 and 3

The Swap Servers 2 and 3 button allows you to toggle the order in which the RADIUS and external LDAP servers authenticate.

L2TP Settings

The Layer 2 Tunneling Protocol (L2TP) is supported by Nortel Networks, Cisco Systems, Microsoft, and other vendors.

Figure 32 L2TP Server



Authentication

L2TP settings allow you to select a specific authentication server type; for example, RADIUS. Each server type allows you to specify an authentication scheme: MS-CHAP, CHAP, or PAP.

Note: Not all RADIUS servers support all forms of authentication. Failure to match PPP authentication methods with RADIUS server capabilities results in user-authentication failures. Check your vendor's RADIUS documentation for additional information.

Authentication Order

The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions. The LDAP server is always queried first, then RADIUS, if applicable. Refer to "Authentication Order" for a description of the Authentication Order table.

Add LDAP Authentication Server

Click on the Add LDAP Authentication Server to add an LDAP server to be used for authentication.

Swap Servers 2 and 3

The Swap Servers 2 and 3 button allows you to toggle the order in which the RADIUS and external LDAP servers authenticate.

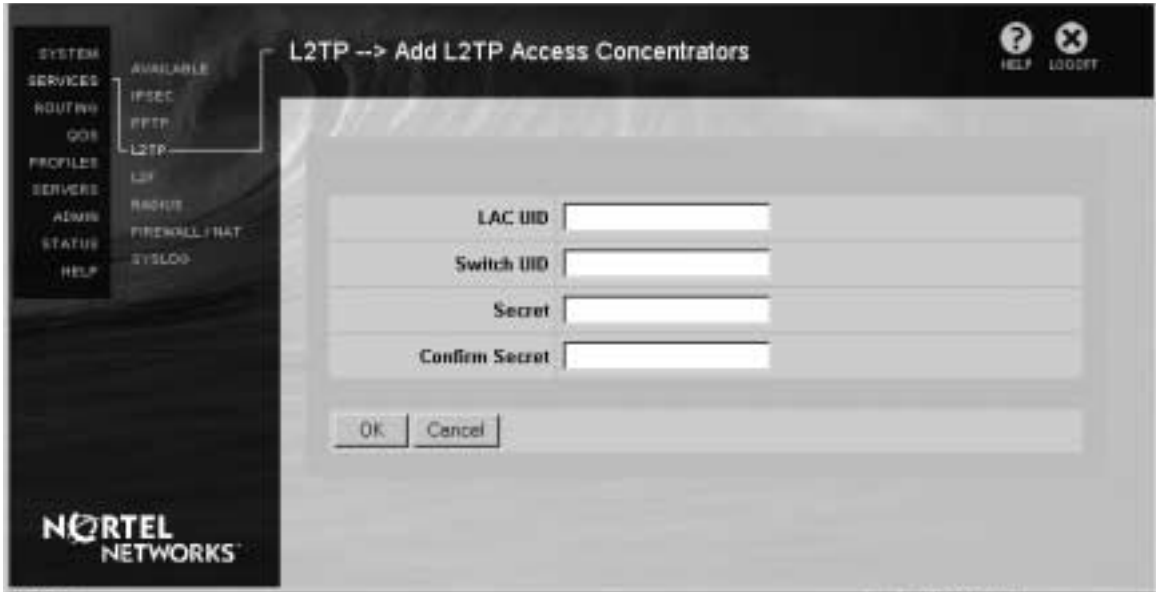
L2TP Access Concentrators

- Delete–Click to remove the configured concentrator. You are prompted to confirm your deletion request.
- Add–Click to go to the Add L2TP Access Concentrator.
- Edit–Click to go to the Edit L2TP Access Concentrator screen and modify the settings of an existing concentrator.

L2TP Add or Edit Access Concentrators

The L2TP Add Access Concentrators screen allows you to configure the authentication between the switch and the NAS. Use the Edit Access Concentrators screen to modify the information for an existing concentrator.

Figure 33 L2TP Add or Edit Access Concentrators



LAC/Switch

LAC/Switch UIDs

Enter the agreed upon User IDs (UIDs) for the LAC (L2TP Access Concentrator) and the switch. UIDs must be coordinated between you and the NAS provider.

Secret

Enter the agreed upon Secret (password) for the LAC (L2TP Access Concentrator) and the switch. Secrets must be coordinated between you and the LAC provider.

Confirm Secrets

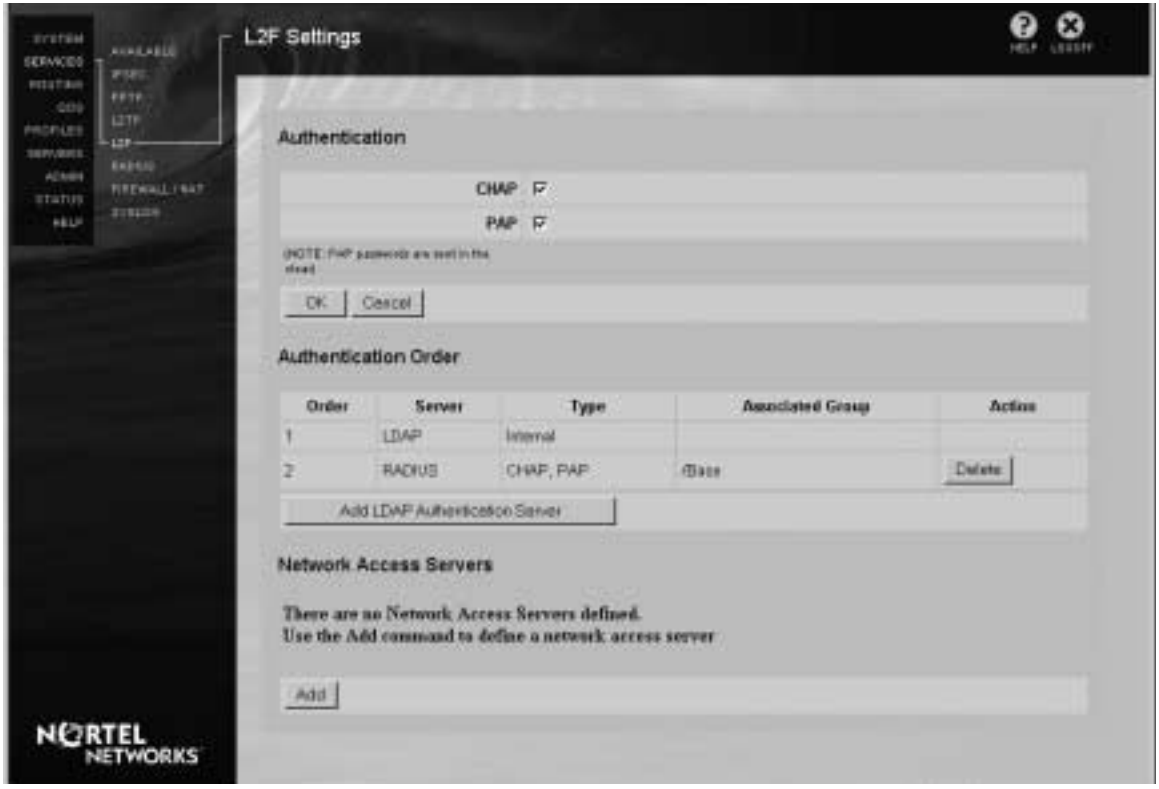
Reenter the assigned Secret (password) to verify that you have typed the intended Secret correctly.

L2F Settings

The L2F (Layer 2 Forwarding) is a tunneling protocol supported by Nortel Networks, Cisco Systems, Shiva, and other vendors. L2F tunneling provides remote access to corporate networks across the public Internet. L2F tunnels are generally established between the network access server (NAS) at the Internet service provider (ISP) and the switch.

In addition to user authentication, L2F requires you to provide NAS and switch user IDs and passwords.

Figure 34 L2F Settings



Authentication

L2F allows you to add a RADIUS server for authentication. The Authentication portion of this screen allows you to specify an authentication scheme or either CHAP or PAP.

Authentication Order

The Authentication Order table lists the corresponding servers, authentication types, associated groups, and actions. The LDAP server is always queried first, then RADIUS, if applicable. Refer to "Authentication Order" for a description of the Authentication Order table.

Add LDAP Authentication Server

Click on the Add LDAP Authentication Server to add an LDAP server to be used for authentication.

Swap Servers 2 and 3

The Swap Servers 2 and 3 button allows you to toggle the order in which the RADIUS and external LDAP servers authenticate.

Network Access Servers

This table provides the UIDs for the network access servers (NAS) and switch, and the possible Actions you can take. The NAS acts like a middleman between the remote user and the switch. It authenticates each side, and once validation is complete, a tunnel is formed. The user has a standard connection (for example, PPP) to the NAS, but an L2F tunnel is formed between the NAS and the switch.

NAS/Switch UIDs

Names/Passwords

UIDs allow the NAS and the switch to mutually authenticate each other. The NAS UID is used by the NAS to log into the switch, and the switch ID is used by the switch to log into the NAS.

Action

Delete–Click to remove an existing NAS entry. You are prompted to confirm your deletion request.

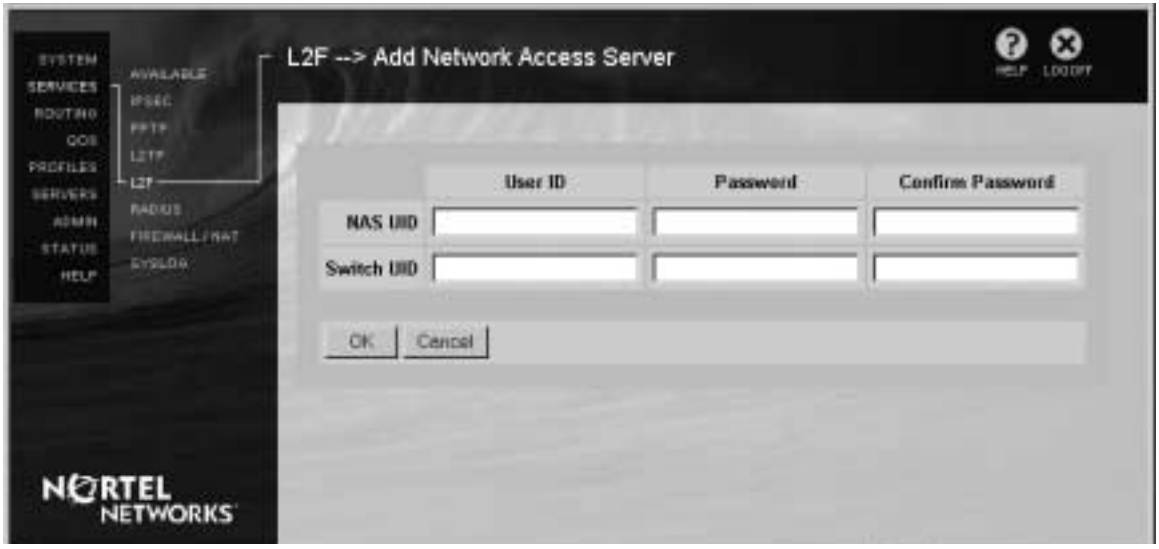
Add–Click to go to the Add Network Access Server screen.

Edit–Click to go to the Edit L2TP Access Concentrator screen and modify the settings of an existing NAS.

L2F Add or Edit Network Access Server

The L2F Add Network Access Server screen allows you to configure the authentication between the switch and the network access server (NAS). Use the L2F Edit Network Access Server screen to modify the information for an existing server.

Figure 35 L2F Add Network Access Server



NAS/Switch

NAS/Switch UIDs

Enter the agreed upon user IDs (UIDs) for the NAS and the switch. UIDs must be coordinated between you and the NAS provider.

Passwords

Enter the agreed upon Passwords for the NAS and the switch. Passwords must be coordinated between you and the NAS provider.

Confirm Passwords

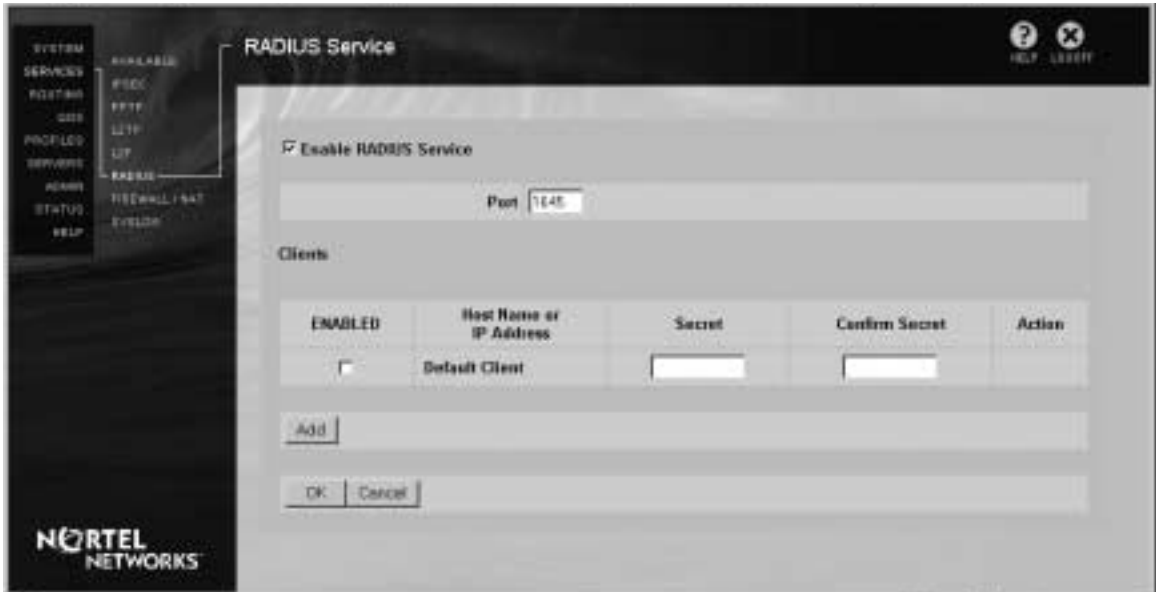
Reenter the assigned password to verify that you have typed the intended password correctly.

RADIUS Service

The RADIUS Service feature allows the switch to function as a simple RADIUS server.

For users with multiple user accounts, RADIUS Service attempts to authenticate against each account type. If the given username/password matches any of the user's accounts, the authentication succeeds. The authentication is done in this order: PPTP, IPSec, L2F, L2TP.

Figure 36 RADIUS Service



Enable RADIUS Service

Click to enable RADIUS Service. The switch now listens on the specified port for authentication requests from remote RADIUS clients.

Note: You must also have RADIUS enabled as an available service on the Services→Available screen. Refer to "Authentication Protocol" for details.

Port

Enter the Port number on which the switch listens for authentication requests from remote RADIUS clients. Port 1645 is the default port number, which is commonly used. However, port 1812 is the port number specified by the RADIUS RFC.

Clients

The Clients section is used to specify the names of the remote hosts that are permitted to send or forward authentication requests to your switch.

Note: Do not confuse the use of the term “Clients” on this screen with a remote Contivity VPN Client, such as an IPSec tunnel client. Clients on this screen denotes a RADIUS client. These clients are network access devices or RADIUS servers (usually belonging to an ISP), that can initiate or forward (proxy) authentication requests to the switch.

Enabled

Click to allow the switch to receive authentication requests from the specified RADIUS client.

Host Name or IP Address

The fully qualified domain name or IP address of the remote RADIUS client from which the switch can receive authentication requests.

Default Client

The first entry in this column is the Default Client. The Default Client is a time-saving feature that enables a switch administrator to allow all public authentication devices that know the specified secret to send or forward authentication requests to the switch. Using this feature, the switch administrator does not have to enter a Host Name or IP Address for each remote device that is a client for the RADIUS Service.

Switch administrators must weigh the convenience that the use of a Default Client provides against possible security implications.

You can disable the use of the default client, but you cannot delete the entry from the list. Initially, the Default Client is disabled (not checked).

Secret

The secret that authorizes the remote RADIUS client to connect to the switch for authentication. You can change the secret on this screen.

Confirm Secret

If you change the secret, you must reenter it here to verify that you typed the new secret correctly.

Action

Delete

Click to remove the selected client. You are prompted to confirm your deletion request.

Add

Click to go to the Add RADIUS Service Client screen.

Add RADIUS Service Client

The Add RADIUS Service Client screen appears when you click the Add button in the RADIUS Service screen.

Figure 37 Add RADIUS Service Client Screen

Host Name or IP Address

Enter either the fully qualified domain name or the IP address of the remote RADIUS Service client from which the switch can receive authentication requests. The name is then listed on the RADIUS Service screen.

Secret

Enter the secret that authorizes the remote RADIUS Service client to connect to the switch for authentication. You can later change the secret on the RADIUS Service screen.

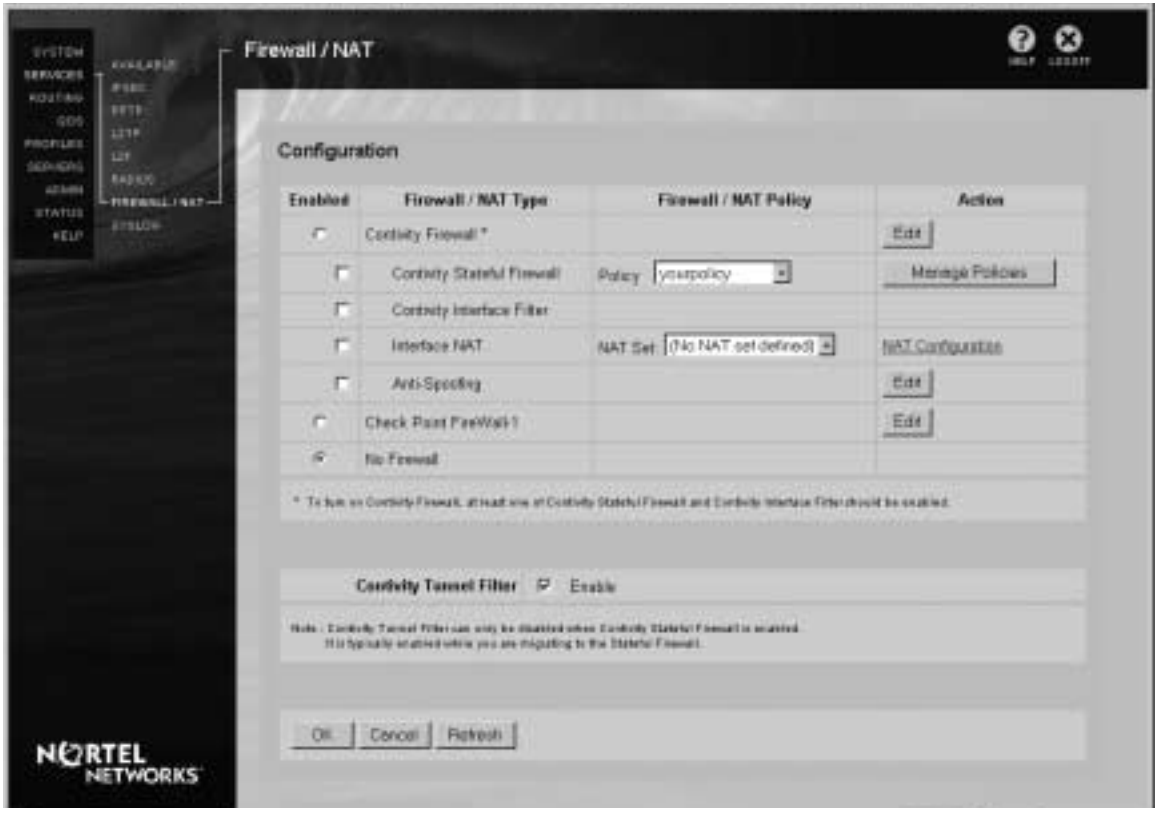
Confirm Secret

Reenter the secret to verify that you typed it correctly.

Firewall/NAT

The Contivity provides a choice of three possible firewall solutions. With the addition of an integrated firewall, the switch can perform a variety of secure routing functions, depending upon how you set up the switch's routing capabilities. For example, you can configure the switch to securely route non-tunneled traffic from its private interface, through the firewall, and out its public interface. This configuration would enable users on the switch's private network to access the Internet without requiring a separate, dedicated router.

Figure 38 Services→Firewall/NAT screen



Configuration

Enabled

Use this column to enable the Firewall/NAT Types you want to use.

By default the No Firewall option is selected.

Firewall/NAT Type

Contivity Firewall

Click to enable the Contivity Firewall. The Contivity Firewall must be enabled in order to run any combination of:

- Contivity Stateful Firewall
- Contivity Interface Filter
- Interface NAT
- Anti-Spoofing

Contivity Stateful Firewall

Check this box to enable the Contivity Stateful Firewall.

The Contivity Stateful Inspection Firewall allows you to statefully inspect traffic on all physical and virtual (tunnel) interfaces. Refer to “Managing the Contivity Stateful Firewall” for more information.

Contivity Interface Filter

Check this box to enable Contivity Interface Filter.

This option can be enabled at the same time as the Contivity Stateful Firewall, enabling you to migrate to the Contivity Stateful Firewall over time. It allows you to continue using existing interface filters with the Stateful Firewall while you build interface filters to regulate non-tunneled traffic and test the firewall policies live. This enables you to continue using the interface filters for traffic that you have not yet added interface rules for in the Stateful Firewall.

Once you are satisfied that the Stateful Firewall policy is correct (that is, it has all of the same rules as the old tunnel interface filters did) you can disable Contivity Interface Filters, and run *only* with the Contivity Stateful Firewall, which is much more efficient.

The policies in the Stateful Firewall take precedence over the interface filters.

Interface NAT

Check this box to enable Interface NAT. This option enables you to apply NAT rules to non-tunneled traffic that you route through the switch. Enabling and configuring Interface NAT here does not affect Branch Office NAT settings.

Anti-Spoofing

Check this box to enable Anti-Spoofing. Anti-spoofing prevents packets from passing into a private network with forged source addresses in the packet header. The source address of each packet entering the switch through a public interface and bound for a private interface is examined to ensure that the source address is not from a subnet reachable through a private interface or a tunnel.

You should disable Anti-Spoofing if you advertise direct routes (see “Policy”) over an interface and you have dynamic Branch Office tunnels defined over that interface, or the tunnel packets will get dropped due to Anti-Spoofing.

Check Point Firewall-1

Check this box to enable Check Point Firewall-1. See “Check Point FireWall-1 Service.”

No Firewall

Check this box to enable a No Firewall state.

Firewall/NAT Policy

Contivity Stateful Firewall Policy

This list-box shows the currently selected Contivity Stateful Firewall Policy being used and lists any additional ones from which you select.

Use the Manage Policies button to launch the CSF Manager applet to create and manage firewall policies. The new policies you create are not automatically applied to the firewall. You cannot apply a policy from the CSF Manager applet.

The system default policy means that the firewall is enabled and no policies are applied except for the implied rules.

NAT Set

This list-box shows the currently selected NAT set being used and lists any additional NAT sets.

You can use the NAT Configuration link to jump to the Profiles→NAT Sets screen to create a new NAT Set if you do not want to use any of the existing ones. You can then use the Return to Firewall/NAT Screen link to jump back to this screen and apply the new NAT Set.

Selection of a NAT set here applies to non-Tunneled traffic only. It does not affect the NAT sets applied to Branch Office tunnels. If any Branch Office tunnel NAT sets are assigned, they remain in effect for those Branch Office tunnels.

Actions

Edit Contivity Firewall

Click the Contivity Firewall Edit button to access the Edit screen for the Contivity Firewall. See “Edit Contivity Firewall.”

Manage Policies

Click the Manage Policies button to configure and manage the Contivity Stateful Firewall. This button launches the CSF Manager applet. Refer to *Managing the Contivity Stateful Firewall* for more information.

NAT Configuration

Click the NAT Configuration link to go to the Profiles→NAT Sets screen to configure NAT Sets. See “Network Address Translation (NAT).”

Edit Anti-Spoofing

Click the Edit Anti-Spoofing button to configure Anti-Spoofing. See "Anti-Spoofing Configuration."

Edit Check Point Firewall-1

Click the Edit button for the Check Point Firewall-1 to configure the Check Point Firewall-1. See "Check Point FireWall-1 Service."

Anti-Spoofing Configuration

All public interfaces in the switch are listed on this page. You can configure Anti-Spoofing for each interface.

Anti-Spoofing Enabled

A check in this box indicates that Anti-Spoofing is enabled for the specific interface.

Public Interface

This field shows the name of the Interface.

IP Address

The IP Address of the Interface.

Edit Contivity Firewall

Click the Edit button for the Contivity Firewall on the Firewall/NAT screen to access the Contivity Firewall Edit screen. Use this screen to configure connection limits and logging activity for the Contivity Firewall.

Connection Number

Maximum Connection Number

Enter the maximum number of connections in this field. The connection number allows you to reserve memory for a maximum number of connections. The number range varies depending on the Contivity model and amount of memory on the switch.

Determining the optimum memory allocation makes it easier to tune your system for firewall traffic. Because the Firewall tracks conversations, it pre-allocates memory.

Logging

Select the types of logging that you want in this section of the screen. These logging options apply only to information going into the EVENTLOG. None of the logged information gets sent to the SYSLOG.

Note: If any of these choices are selected and the switch is under a heavy load, the EVENTLOG could overflow, losing entries.

All

Check this box to enable logging of all activity.

Traffic

Check this box to log flow/conversation creation and deletion type messages to the EVENTLOG.

Policy Manager

Check this box to log policy/rule creation and processing type messages to the EVENTLOG.

Firewall

Check this box to log counts of packets dropped/allowed by Firewall processing to the EVENTLOG.

NAT

Check this box to log all Interface NAT related messages to the EVENTLOG. This does not cause logging of Branch Office NAT message.

Debug

Check this box to log additional debugging information. Because of the amount of logging this generates and the impact it could have on performance, you should enable this option only when advised to do so by a Nortel Networks Customer Support representative.

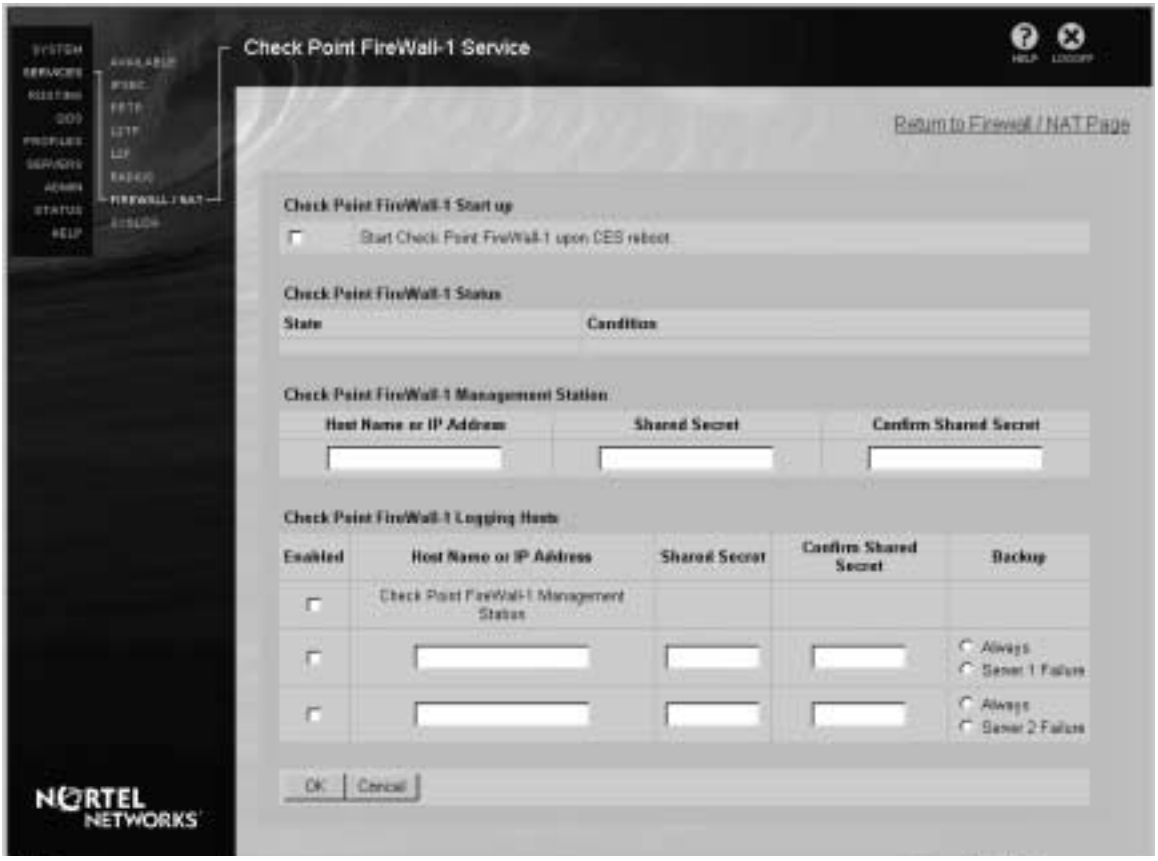
Contivity Tunnel Filter

When the check box is enabled, it allows you to use tunnel filters with the Stateful Firewall and migrate to the Stateful Firewall over time. You can build and test the Stateful Firewall policies while using the tunnel filters for traffic. Once you have the Stateful firewall policy set up (it has all of the same rules as the tunnel filters did), you can disable the tunnel filters and run the Stateful Firewall.

Check Point FireWall-1 Service

Use the Check Point FireWall-1 Service screen (Services→Firewall→Edit button) to start your switch's integrated Check Point firewall and to manage the interaction between the firewall and the FireWall-1 Management Server.

Figure 39 Check Point FireWall-1 Service screen



The following sections describe the fields on the Check Point FireWall-1 Service screen.

Be sure that you click on the OK button to save any changes. After you click on OK, error messages appear at the top of this screen if required information is missing or incorrect.

Check Point FireWall-1 Start Up

Start Check Point FireWall-1 upon reboot

Use this check box to specify that you want the integrated Check Point firewall started when the switch is rebooted. Make sure that you have also enabled the firewall by selecting Check Point on the Services→Firewall screen.

When the firewall is started, the switch provides its enhanced routing capabilities. The enhanced routing is available as long as the switch and the firewall are enabled.

Check Point FireWall-1 Status

State

Indicates the current status of the integrated Check Point firewall.

- Enabled indicates that the Start checkbox has been selected and the firewall has attempted to load. When the firewall is in the Enabled state, a Stop Check Point FireWall-1 button is displayed.
- Disabled indicates that the firewall could not load when you rebooted the switch or that the Stop button was pressed.

Condition

Describes the condition that resulted in the firewall's current state. The possible conditions for each state are as follows:

Table 7 Check Point FireWall-1 states

State	Condition	Meaning
Enabled	Enabled	The firewall has loaded successfully and is up and running.
Enabled	Loading	The firewall has not completed the loading process. This might be caused by an incorrectly configured Management Station. This is an interim condition that eventually changes to either Enabled or Failure.

Table 7 Check Point FireWall-1 states (continued)

State	Condition	Meaning
Disabled	Disabled	The firewall is not loaded or that you have pressed the Stop Check Point FireWall-1 button.
Disabled	Failure	The firewall unsuccessfully attempted to load and run.

Check Point FireWall-1 Management Station

This portion of the screen is used to identify and authenticate the Check Point FireWall-1 Management Station that manages the switch's integrated firewall.

Although the FireWall-1 firewall is a component of the switch, the firewall is set up and configured using a remote Firewall Management Station. The *Installing Check Point Firewall-1* book provides instructions for setting up your switch's firewall to create an efficient, yet secure environment. You should also refer to your Check Point FireWall-1 documentation for detailed firewall configuration instructions.

The integrated Check Point firewall must be running in order for the Management Station to gain access to it. You must also ensure that the switch has been configured to accept management traffic from the firewall's Management Station. Refer to the first two rows in Table 8 for information.

Host Name or IP Address

The fully qualified domain name or IP address of the Management Station that you want to use to manage the firewall on the switch.

Shared Secret

The shared secret between the Management Station and the switch. The secret authorizes the Management Station to access and manage the switch's firewall. The secret must be coordinated between you and the Management Station administrator.

Confirm Shared Secret

Reenter the shared secret to verify that you typed it correctly. You must define the integrated firewall as type switch on all management stations and firewall logging servers that you use.

Check Point FireWall-1 Logging Hosts

Logging hosts are machines to which the firewall writes its log file. As a means of providing backup to the logging information, you can specify multiple logging hosts.

Use the FireWall-1 Management Station GUI to display the log viewer on a selected logging host. The default log file is $FWDIR/log/fw.log.

Enabled

Select the Enabled checkbox to specify that the log file is directed to the listed machine.

Host Name or IP Address

Enter either the fully qualified domain name or the IP address of the logging hosts.

Shared Secret

Enter the shared secret between the logging host and the switch. Secrets must be coordinated between you and the administrator of the logging host.

Confirm Shared Secret

Reenter the shared secret to verify that you typed it correctly.

Backup

You can specify that the log file be sent to multiple logging hosts.

- Use the Always selection to specify that the log file is always sent to the listed logging host.

- Select the Server *n* Failure to specify that the log file is sent to the listed logging host only if Server *n* is not available.

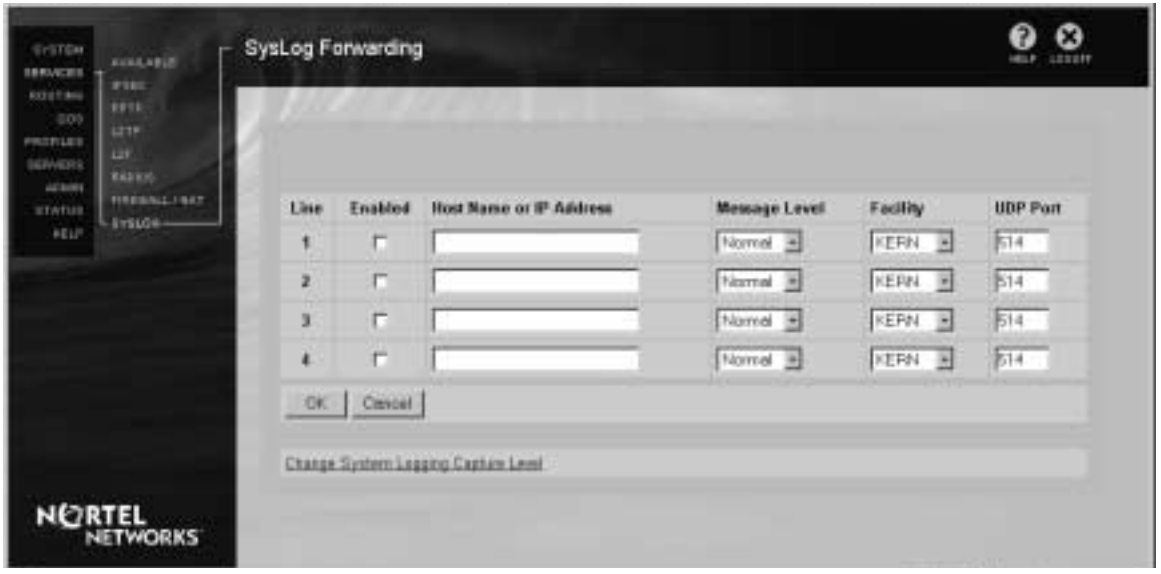
SysLog (System Forwarding)

System forwarding (Syslog) enables you to forward information from the system log to different host machines via the system logging daemon (syslogd). You can send different levels of information to different hosts. For example, you might send only Urgent system information to your primary system while sending "All" messages to a system you use for backup.

Note: The System Log (Status→System Log) setting has precedence over the Message Level you set on the Syslog Forwarding screen. For example, if you set Normal on this Syslog Forwarding screen but Urgent on the System Log screen, only Normal information is captured and available to Syslog Forwarding.

The section "System Log" provides additional information about system logging.

Figure 40 SYSLOG Forwarding



Enabled

Click to allow the switch to send its system messages to the specific machine.

Host Name or IP Address

Enter either the fully qualified domain name or the IP address of the remote machine to which the log information is sent.

Message Level

The Message Level selection enables you to filter the information you send to the specified machines. For example, you might send Urgent system information to your primary system while sending All messages to systems you use for backup.

Urgent

Urgent Events are those that you want to be aware of immediately and that could potentially pose security or access problems; for example:

- Attempts to login with the wrong password.
- Attempts to gain Administrator Access.

Normal

Normal events are the everyday user and system interactions that allow you to review switch activity; for example:

- Logins
- Configuration changes
- Scheduled or actual shutdowns

Detailed

Detailed events are designed specifically for use by Nortel Networks Customer Support personnel to uncover or troubleshoot problems.

All

The All selection is also designed specifically for Nortel Networks Customer Support personnel. This includes every log message that the system generates, including many details that are not of general interest but might allow Nortel Networks to uncover or troubleshoot problems.

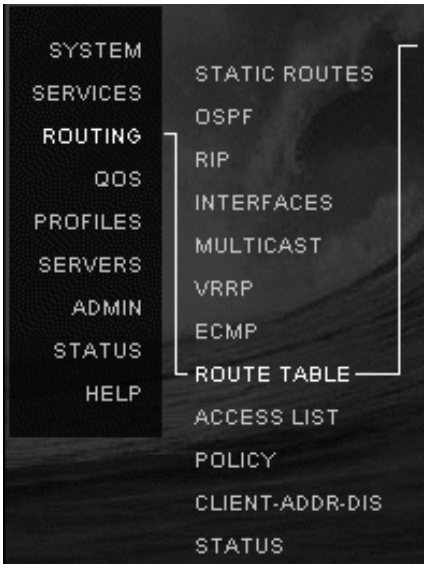
Change System Logging Capture Level

Click this link to go to the Status→System Log screen. At this screen you can specify the level of information you want to capture for the system log. Refer to the section "System log" in Chapter 8 for a description of the System Log.

Chapter 3
Routing

The Routing menu provides access to screens that enable you to configure the various routing capabilities of the switch.

Figure 41 Routing Menu



Static Routes

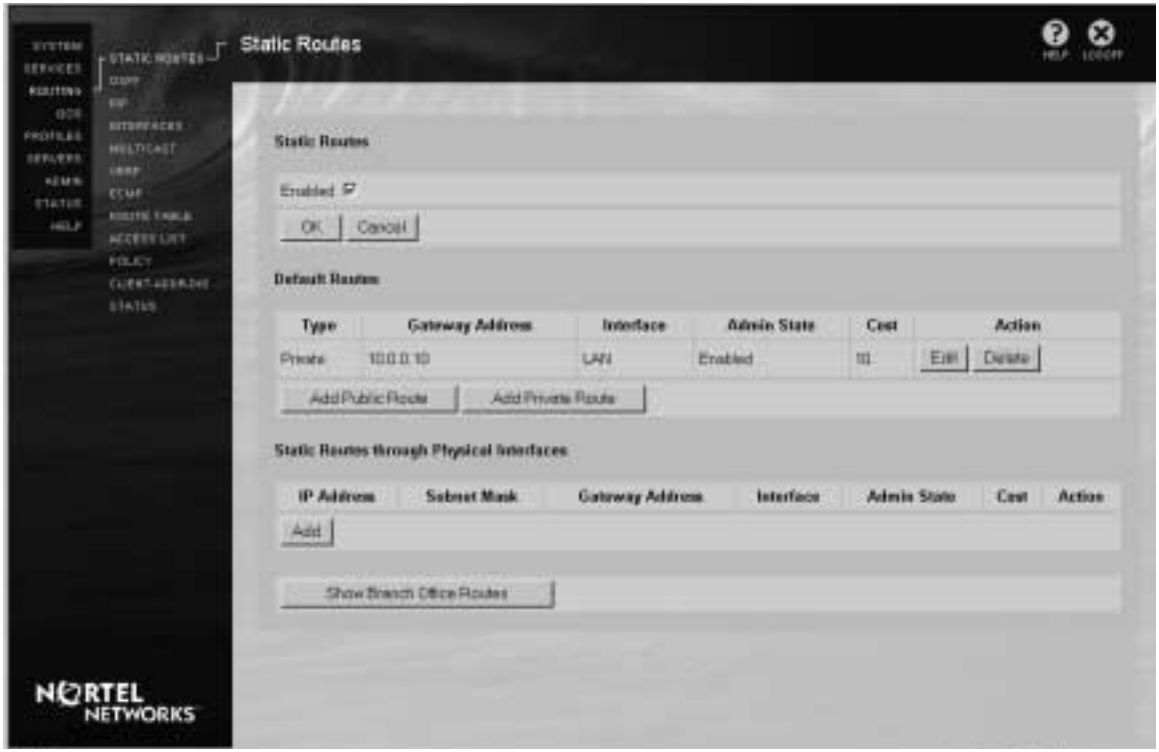
You can use static routes to set up routes between switches when you do not have any dynamic routing protocol, such as OSPF or RIP. Even if you do have dynamic routing protocols, you may want to use static routes because they provide stronger security. The switch supports multiple default and static routes.

You can manually configure static routes on the switch. Based on their states, they are added or removed from the Route Table Manager (RTM). Click Routing→Static Routes to configure static routes.

Static Routes

Check the Enabled box to enable static routes. When this check box is cleared, all of the static routes and default routes are disabled globally. Even if a static route is enabled, the route is not used because the static routes are globally disabled. When static routes are enabled, traffic flow depends on other configuration settings.

Figure 42 Static Routes Configuration



Default Routes

In the absence of any defined route, packets are forwarded to the gateway specified as the default route. These default routes can be either private or public static routes. Private routes are available whether or not a firewall is enabled. Public routes are available only if an integrated firewall is enabled.

A private default static route is the default route used for traffic that comes into the switch from a private interface. Incoming traffic uses the private default route when there is no public default route defined. If you do not define either a public or private default route, the traffic is dropped. When you add a private default route, the route table adds a new static route.

A public default static route is the default route used for traffic that comes into the switch from a public interface or through a tunnel. If you do not define a public default route, the traffic is dropped. When you add a public default route, a new static route is added to the route table. You can configure multiple default routes to the same destination with different gateways.

Type

Shows whether the static route is Public or Private.

Gateway Address

Address where packets are routed onto the network.

Interface

Shows whether the default route is a LAN or WAN interface.

Admin State

Shows whether the route is enabled or disabled.

Cost

Shows the relative cost for the switch. You would use a lower cost number, such as 1, for the least expensive route. When there are multiple default paths, the switch chooses the route with the least cost as the preferred route. The default is 10.

Action

Click on the appropriate buttons to edit or delete default routes.

Edit

To edit an existing default static route, click on the edit button in the Action column. The Static Routes→Edit screen appears with a display of the appropriate information about that route. Select Enable or Disable from the Admin State drop down list. Type in the cost in the Cost edit box and the gateway address in the Gateway Address edit box.

Figure 43 Static Routes→Edit

Delete

Click on the Delete button to delete the default static route.

Add Public Route

To edit a default public static route, click on the edit button in the Action column. The Static Routes→Add Public Default Route screen appears with a display of the appropriate information about that route. Select Enable or Disable from the Admin State drop down list. Type in the cost in the Cost edit box and the gateway address in the Gateway Address edit box.

Figure 44 Static Route→Add Public Default Route screen

Add Private Route

To add a default private route, click on the edit button in the Action column. The Static Routes→Edit screen appears with a display of the appropriate information about that route. Select Enable or Disable from the Admin State drop down list. Type in the cost in the Cost edit box and the gateway address in the Gateway Address edit box.

Figure 45 Static Routes→Add Private Default Route

Static Routes through Physical Interfaces

This section displays a list of all configured static routes (through any physical interface). A static route differs from a default static route in that it specifies a particular destination, such as an IP subnet or an IP host, represented by the IP address and subnet mask. You can configure multiple static routes to the same destination with a different next hop gateway and with the same or different costs.

IP Address

IP address of the static route for the destination network.

Subnet Mask

Subnet mask for the static route for the destination network.

Gateway Address

Address where packets are routed for the destination network.

Interface

Shows whether the default route is a LAN or WAN interface. The default is LAN.

Admin State

Shows whether the route is enabled or disabled. The default is enabled.

Cost

Shows the relative cost for the switch. You would use a lower cost number (for example, 1) for the least expensive route. When there are multiple paths, the switch chooses the route with the least cost as the preferred route. The default is 10.

Action

Click on the appropriate buttons to add, edit, or delete default routes.

Edit

To edit an existing static route, click on the edit button. The Static Routes→Edit Static Route screen appears with a display of the appropriate information about that route. Select Enable or Disable from the Admin State drop down list. Type in the cost in the Cost edit box and the gateway address in the Gateway Address edit box.

Figure 46 Static Routes→Edit Static Route

Delete

Click on the Delete button to delete the static route.

Add Route

Click on the add button to add static routes to the routing table. The Static Routes→Add screen appears. When a static route is added, the switch checks whether the next hop interface address belongs to an attached network. If it does not, the switch does not allow such static routes.

Figure 47 Static Routes→Add Static Route screen

Admin state

Shows whether the route is enabled or disabled. The default is enabled.

Cost

Shows the relative cost for the switch. You would use a lower cost number (for example, 1)for the least expensive route. When there are multiple paths, the switch chooses the route with the least cost as the preferred route. The default is 10.

Network address

IP address of the static route for the destination network.

Subnet mask

Subnet mask for the static route for the destination network.

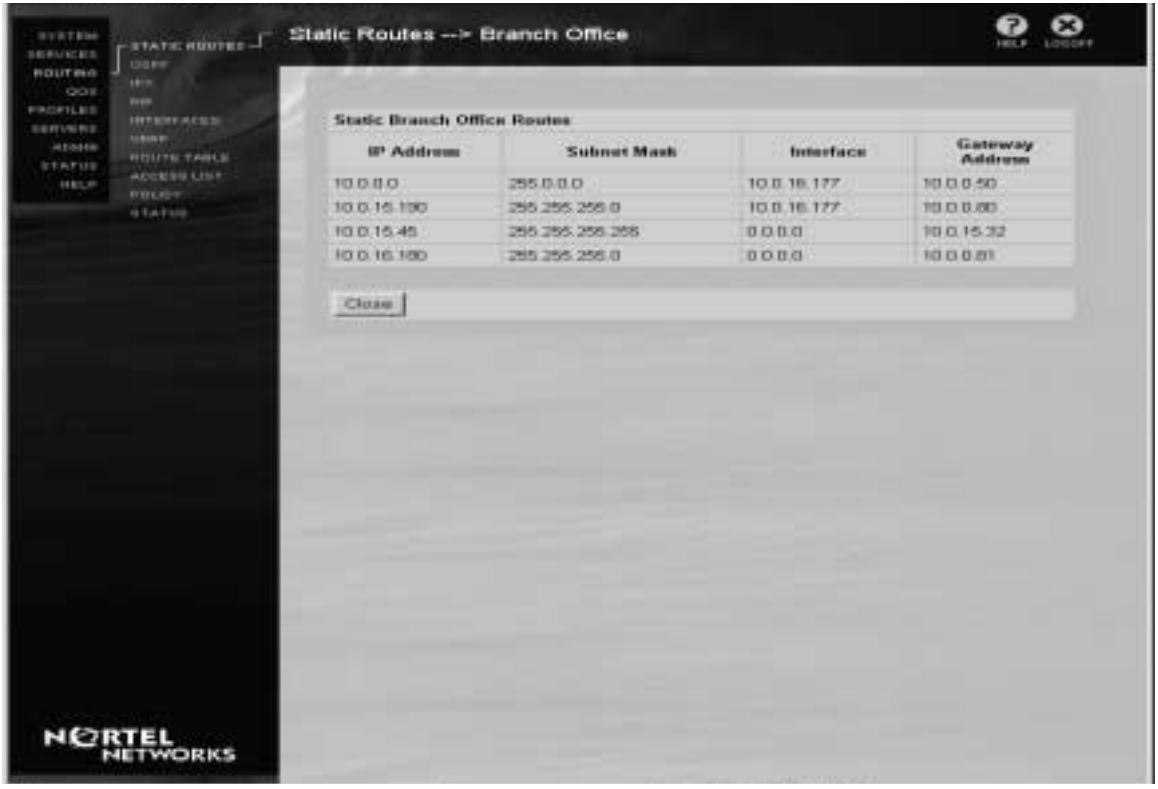
Gateway address

Address where packets are routed for the destination network.

Show Branch Office Routes

This screen shows the configured Branch Office tunnels that are set up as static routes. By default, a tunnel is configured as a static route between the tunnel end points.

Figure 48 Static Routes→Branch Office



IP address

IP address of the branch office route.

Subnet mask

Subnet mask of the branch office route.

Interface

Local IP address of the branch office interface.

Gateway address

Remote peer address where packets are routed onto the network.

Admin State

Enabled or disabled. To edit this field, go to Branch Office→Edit→IP and click on Add Route under the Static Route section.

Cost

Shows the relative cost for the switch. You would use a lower cost number, such as 1, for the least expensive route. If the number is more than 1, the lowest cost is the preferred number. To edit this field, go to Branch Office→Edit→IP and click on Add Route under the Static Route section.

OSPF

OSPF (Open Shortest Path First) is a link-state routing protocol that maintains a database from which a routing table is constructed from the shortest path, using a minimum of routing protocol traffic. It provides a high functionality open protocol that allows multiple vendor networks to communicate using the TCP/IP protocol family. Some of the benefits of OSPF are:

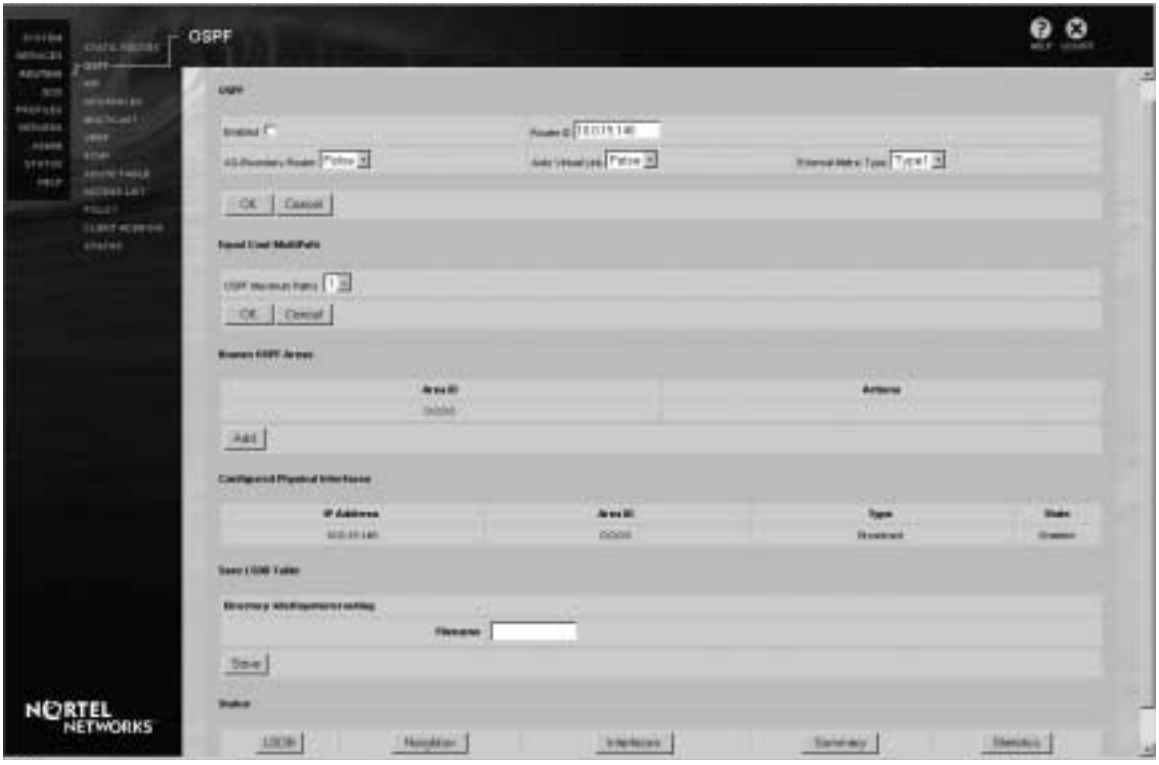
- Fast convergence
- Variable Length Subnet Masks (VLSM)
- Hierarchical segmentation
- Area routing to provide additional routing protection and a reduction in routing protocol traffic

- Authentication

OSPF Configuration

Click Routing→OSPF to configure OSPF global parameters.

Figure 49 Routing→OSPF



Enabled

Indicates that the OSPF protocol is enabled on this screen. The default setting is disabled.

Router ID

Type in the IP address in the Router ID field. This uniquely identifies the router in an area and defaults to the lowest of the IP addresses of management/physical interfaces defined in the switch. You can change this address provided that it is unique within the area. The default is the lowest IP interface in the box.

AS-Boundary-Router

An AS-Boundary-Router is a router that exchanges routing information with routers belonging to other autonomous systems and advertises AS external routing information throughout the AS. To configure the switch as an Autonomous System Boundary Router, select True from the AS-Boundary-Router drop down list. The default is false. This parameter must be set to True if you want to enable redistribution of non-OSPF routes via OSPF.

Auto Virtual Link

To automatically create virtual links to link the segments in a backbone network, select True from the drop down list. The default is False.

External Metric Type

OSPF supports two types of external metrics. Type 1 external metrics are expressed in the same units as OSPF interface cost (in terms of the link state metric). Type 2 external metrics are an order of magnitude larger; any Type 2 metric is considered greater than the cost of any path internal to the AS boundary router. Use of Type 2 external metrics assumes that routing between AS boundary routers is the major cost of routing a packet, and eliminates the need for conversion of external costs to internal link state metrics. Select metric Type 1 or Type 2. Type 1 is the default.

Equal Cost MultiPath

Equal Cost Multipath provides load balancing of packets to a destination that is reachable over more than one physical interface.

OSPF Maximum Paths

OSPF compile time maximum equal cost paths parameter is four paths.

Known OSPF Areas

This section displays all of the OSPF areas defined locally to the switch. The area information is not shared among switches. If you want two switches to have one of their interfaces in a common area, you must configure both switches to define the area information.

Area ID

Area IDs are used as representations of parts of the OSPF network. They help to manage large numbers of networks so that they can exchange information within an area. Each Area ID must be unique for OSPF. By default all switches have an area named 0.0.0.0.

Add

To add an OSPF area, click on the add button. The Routing Protocols→Add Area screen appears.

Area ID

List the ID of the area that you want to edit.

Stub

Select True of False from the drop-down list. The default is False.

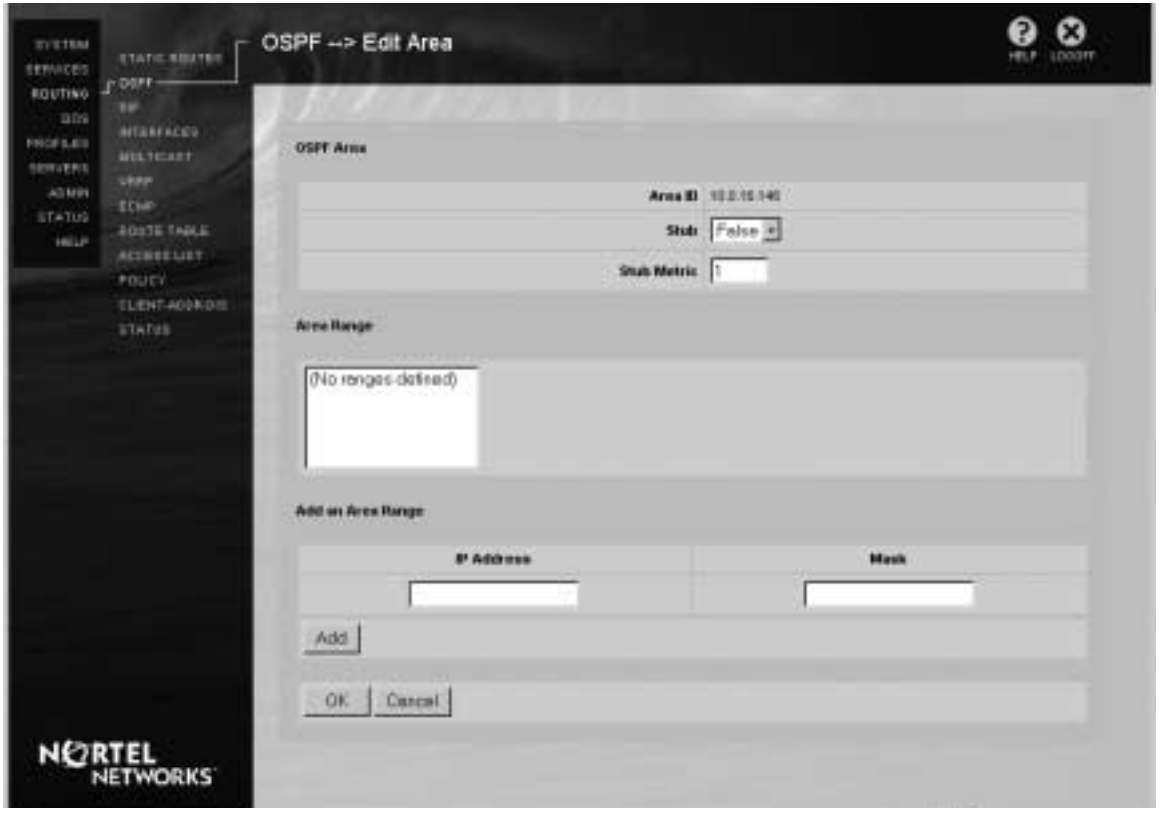
Stub Metric

Type in the number of the stub metric. The default is 1.

Edit

When you add an area, you can edit the information for that area by clicking on the Edit button next to the area. The OSPF→Edit Area screen appears. You can change the information for the Area ID, Stub and Stub Metric as explained above.You can also delete an existing area range or add an area range.

Figure 50 Routing→OSPF→Edit Area



Area Range

The edit box lists all existing area ranges. Select the area range and click the Delete button to delete the range.

Add an Area Range

In the edit boxes, type in the IP address and subnet mask of the area range that you want to specify.

Configured Physical Interfaces

IP address

IP address of the configured OSPF interfaces. The default is 0.0.0.0.

Area ID

Area ID of the configured OSPF interfaces. The default is 0.0.0.0.

Type

Broadcast or Point-to-Point. The default is Broadcast.

State

Enabled or disabled. The default is enabled.

Save LSDB Table

Filename

You can save the LSDB table as a text file in the directory ide0/system/routing.

Status

This section allows you to display. LSDB (Link State Database), Neighbor, Interfaces, or Summary.

LSDB

When you click on the LSDB button, the screen lists the link state databases in all areas that are configured in that switch.

Figure 51 Routing→LSDB

The following table describes the information in the OSPF LSDB screen.

Table 8 LSDB screen

Column	Description
Link State ID	Link state address
Adv Router	Advertising router address
Age	Age in seconds
Seq Nbr	Sequence number

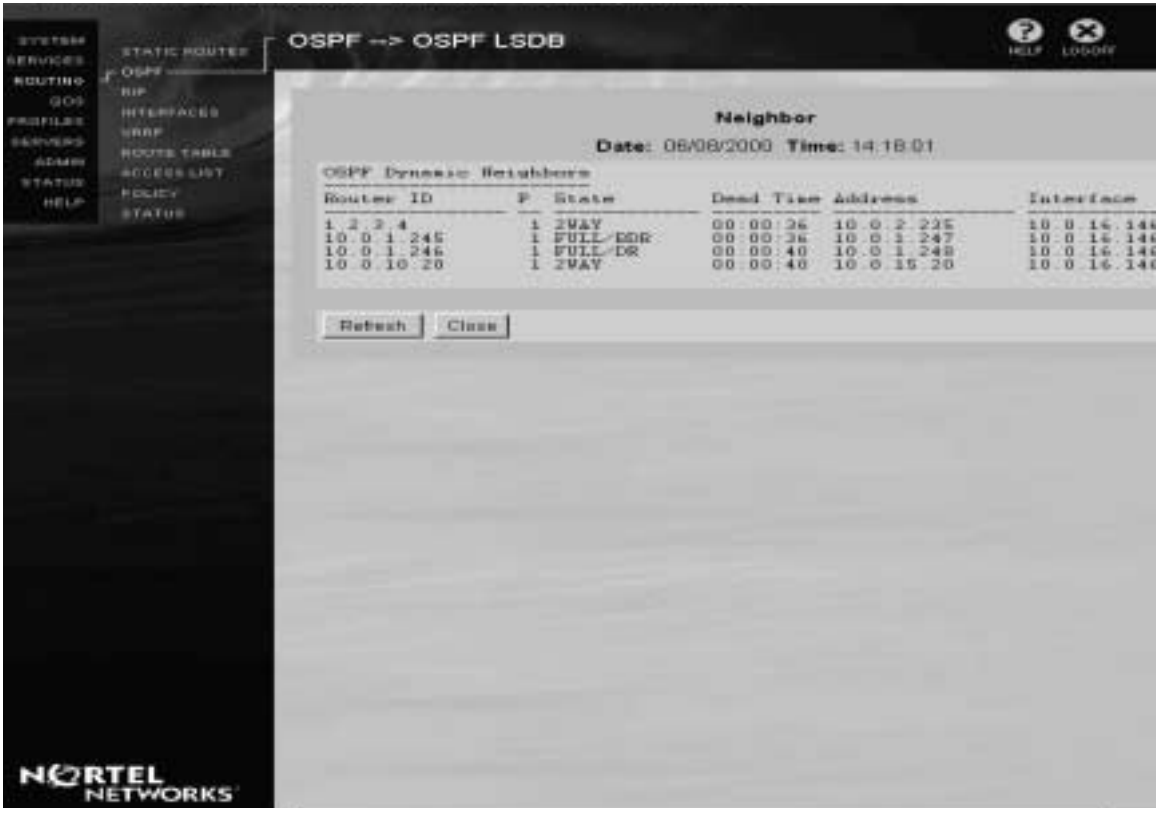
Table 8 LSDB screen (continued)

Column	Description
CheckSum	Checksum
Links	Number of links

Neighbor

When you click on the Neighbor button, the screen shows the list of neighbors on all the interfaces running OSPF.

Figure 52 Routing→OSPF→Neighbor



The following table describes information on the OSPF Neighbors screen.

Table 9 OSPF Dynamic Neighbors screen

Column	Description
Router ID	OSPF ID of neighbor
P	Priority number
State	State of neighbor connection
Dead Time	Time until neighbor is declared dead
Address	Neighbor IP address
Interface	Local IP interface address

Interfaces

When you click on the Interfaces button, the screen shows the list of interfaces that you configured for OSPF.

Figure 53 OSPF→Interfaces screen

The following table describes the fields for the OSPF Interfaces screen.

Table 10 OSPF Interfaces screen

Column	Description
IP Address	Local IP address
Area ID	OSPF area for the interface
Interface Type	Broadcast (BCAST) for Point to Point (PTPT)
Interface State	State of interface: Enabled or Disabled (physical) or Other (tunnel)
Metric Cost	Cost associated with the interface

Table 10 OSPF Interfaces screen (continued)

Column	Description
Priority	Priority used to negotiate DR/BDR state
Designated Router	Designated router (0.0.0.0 for PTPT)

Summary

When you click on the Summary button, the screen shows the overall summary of OSPF running on the switch.

Figure 54 OSPF→Summary

The following table describes fields on the OSPF Summary screen.

Table 11 OSPF Summary screen

Column	Description
Router ID	Unique OSPF ID of router
Router State	OSPF global configured state (up or down)
Supports TOS	Type of Service support
SPF schedule delay	Shows Shortest Path First

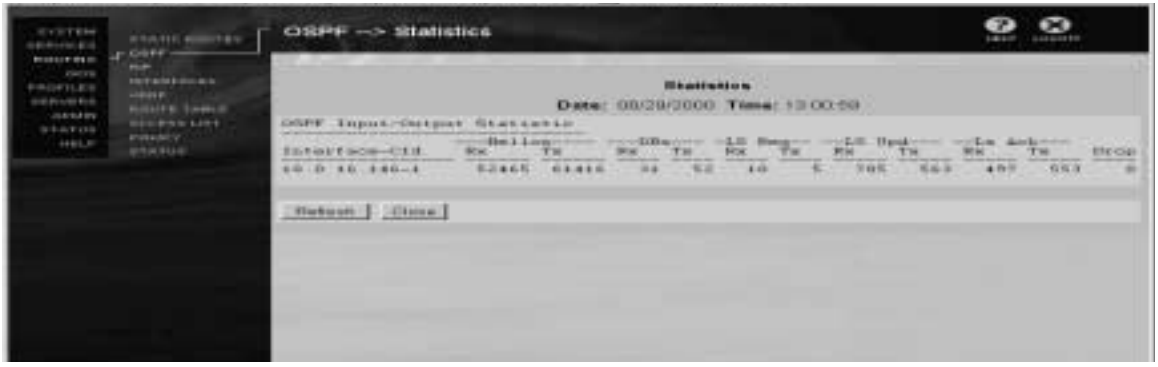
Table 11 OSPF Summary screen (continued)

Column	Description
Hold time between two SPFs	Time between Shortest Path First calls
Minimum LSA interval	Link state advertisement interval
Minimum LSA arrival	Link state advertisement arrival minimum
Number of external LSA	Number of link state advertisements
Link State Update Interval	Time between link state updates
Link State Age Interval	Time between link state age intervals
Number of Areas in this router	Number of areas
Area	Area ID
Number of interfaces in this area	Number of interfaces in this area
SPF algorithm has executed	Number of times shortest path algorithm has been executed

Statistics

When you click on the Statistics button, the system displays statistical information about OSPF.

Figure 55 OSPF→Statistics



The following table describes the fields on the OSPF Statistics screen.

Table 12 OSPF Statistics screen

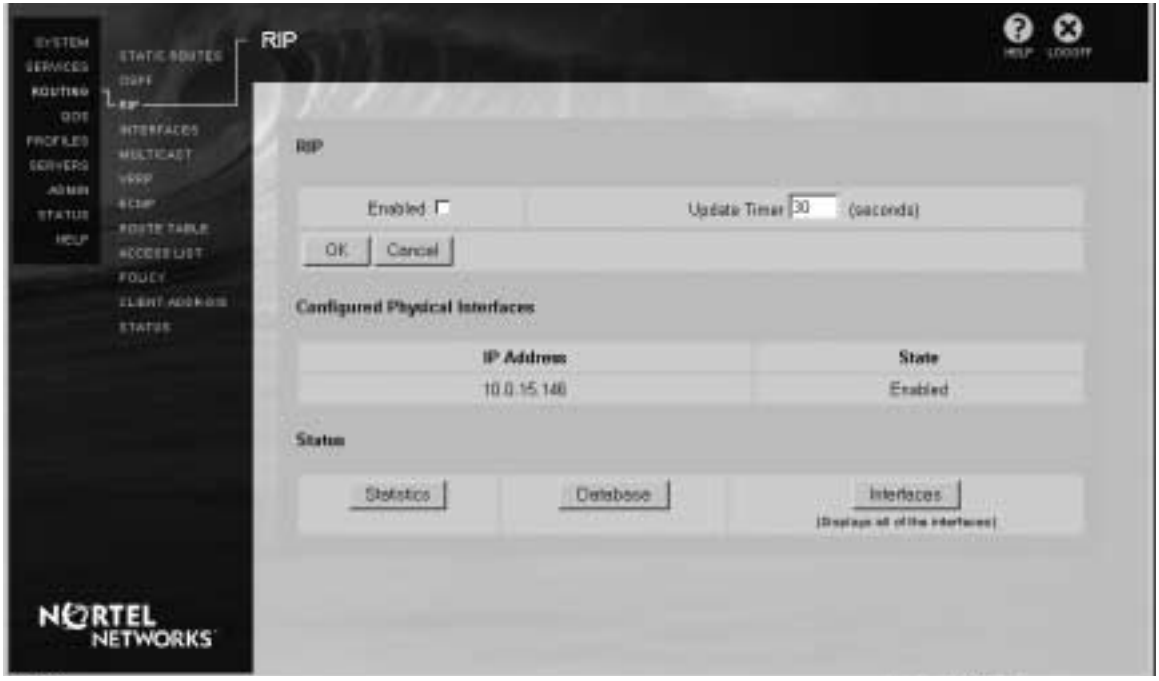
Column	Description
Interface-CID	Local IP interface address and circuit ID
Hellos	Number of “Hello” packets received and transmitted
DBs	Number of “DB” (Database Exchange) packets
LS Req	Link state requests
LS Upd	Link state updates
LS Ack	Link state acknowledgements

RIP

The Routing Information Protocol (RIP) is a distance-vector routing protocol that enables routers to exchange routing information by means of periodic RIP updates. Routers transmit their own RIP updates to neighboring subnets and listen for RIP updates from the routers on those neighboring subnets. Routers use the information in the RIP updates to keep their internal routes current.

For RIP, the “best” path to a destination is the path with the fewest hops. RIP computes distance as a metric, usually the number of hops (or routers) from the origin subnet to the target subnet. RIP can handle a maximum of 15 hops.

Figure 56 RIP



Enabled

Check the Enabled check box to enable RIP on the switch. By default RIP is globally disabled. If RIP is disabled on this screen, the switch does not process any RIP requests. After you enable RIP on this screen, you must also enable it on the Routing→Interfaces screen.

Update Timer

In the Update Timer edit box, enter the amount of time in seconds that you want RIP to update the routes. The default is 30 seconds. The range of values that you can specify is from 5 seconds to 65535 seconds. The hold down timer is six times the update timer. Routes are invalid after the time set on the hold down timer.

Configured Interfaces

IP Address

IP address of the RIP interface.

State

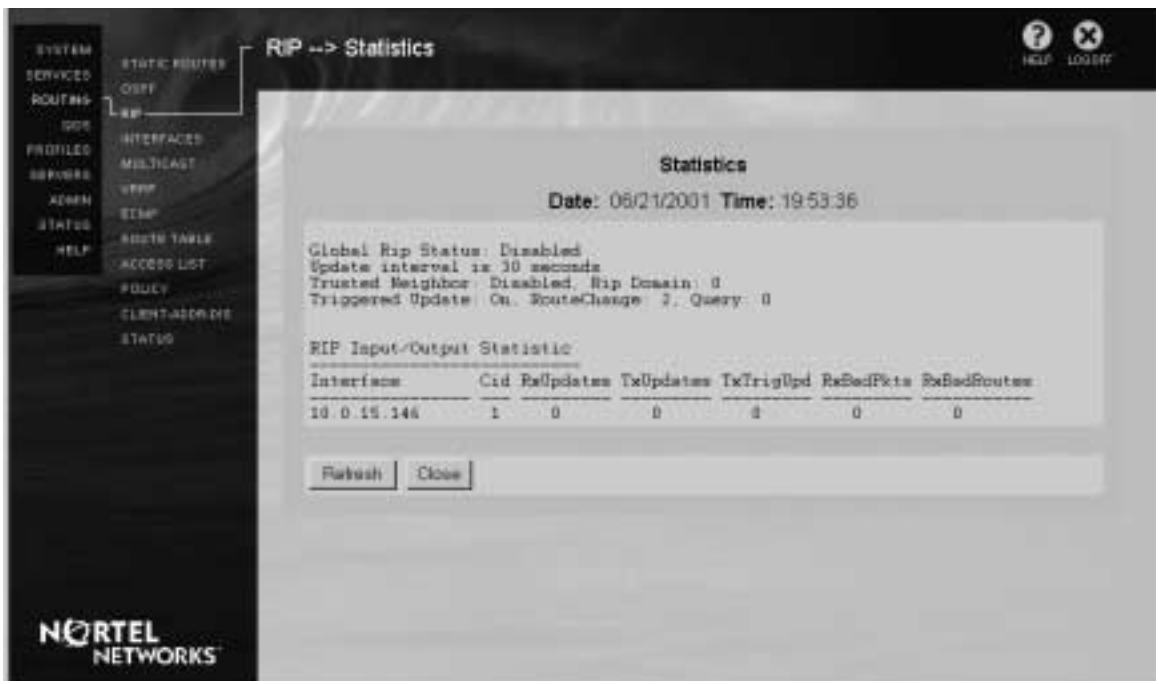
Whether the RIP protocol is enabled or disabled on this interface.

Status

Statistics

Displays statistics about the RIP protocol in the switch.

Figure 57 RIP→Statistics



The following table describes the fields on the RIP Statistics screen.

Table 13 RIP Statistics screen

Column	Description
Global RIP Status	Enabled or disabled
Update interval	Interval in seconds
Trusted Neighbor	Enabled or disabled
Rip Domain	Set or reset
Triggered Update	Set or reset
Route Change	Number of routes changed
Query	Number of queries sent

Database

Displays information for all of the RIP interfaces.

Figure 58 RIP database

The following table describes the fields on the RIP Database screen.

Table 14 RIP Database screen

Column	Description
Circuit	Circuit ID
Address	IP address
Mask	Network mask of IP address
Owner	Protocol
Cost	Import cost of RIP routes
Metric	Export metric of RIP routes
Gw	Gateway IP address

Interfaces

Displays information for all of the RIP interfaces, including tunnels that are running RIP.

Figure 59 RIP→Interfaces

The following table describes the fields on the RIP Interfaces screen.

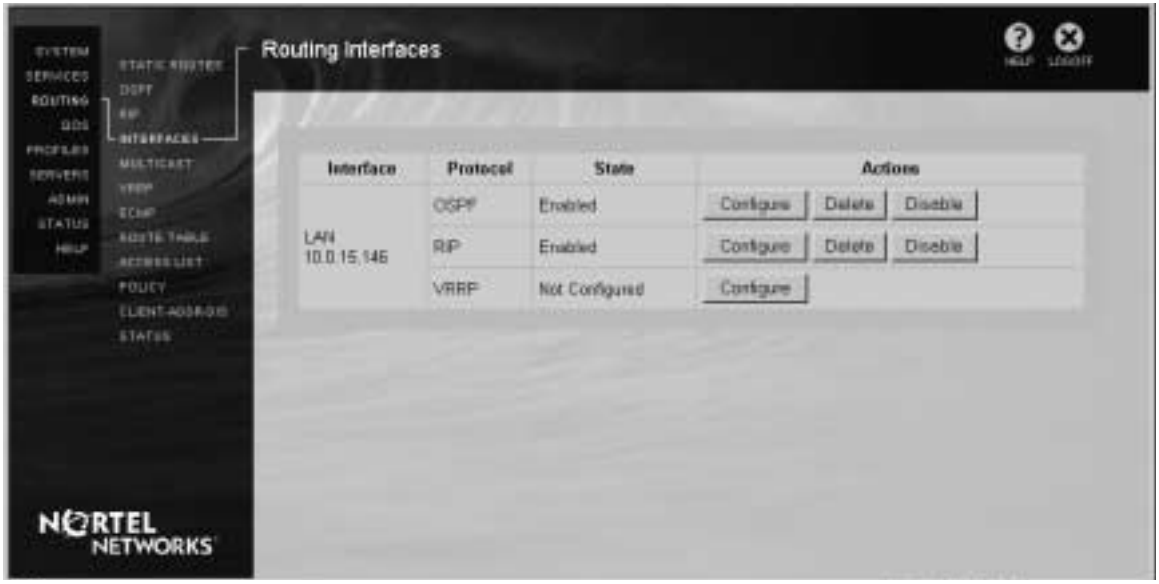
Table 15 RIP Interfaces screen

Column	Description
Ip	RIP IP address
Subnet	Network mask of IP address
RipEnabled	Whether RIP is enabled or disabled
IntfState	Whether up or down
Auth	Authentication type
Type	Interface type
Cid	Circuit ID
RxMode	RIP receive version supported
TxMode	RIP transmit version supported
PoisonRev	Whether enabled or disabled
ImpDRoute	Whether enabled or disabled
ExpTSMetric	Disabled or metric (1-15) export tunnel static route
ExpSMetric	Disabled or metric (1-15) export static route
ExpDMetric	Disabled or metric (1-15) export default route
ExpOspfMetric	Disabled or metric (1-15 export OSPF route

Interfaces

The Interfaces screen allows you to choose the routing interface that you want to configure. The supported routing protocols are OSPF, RIP, and VRRP.

Figure 60 Routing Interfaces



Interface

Slot number, interface number, and corresponding IP address.

Protocol

OSPF, RIP, or VRRP.

State

Enabled, Disabled, or Not configured. The default reflects the configured state.

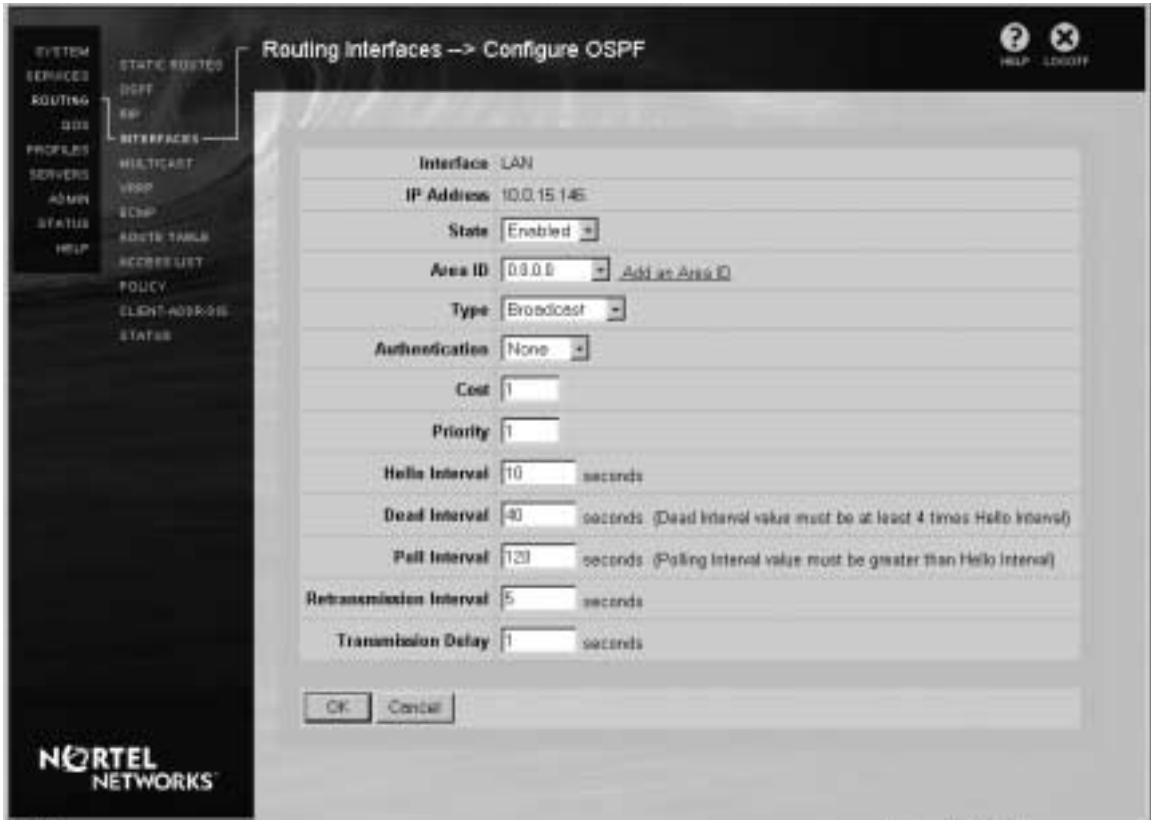
Actions

Configure, Delete, or Disable/Enable.

OSPF

When you click on the Configure button under the Actions Section for OSPF, the Routing Interfaces→Configure OSPF screen appears.

Figure 61 Routing Interfaces→Configure OSPF



Interface

Interface number and slot.

IP Address

IP address of the interface.

State

State of OSPF, either enabled or disabled. The default is enabled.

Area ID

OSPF area to which the attached network belongs. The default is 0.0.0.0.

Type

OSPF network type, such as Broadcast or Point-to-Point. The default is Broadcast.

Authentication

OSPF authentication type, such as Simple, MD5, or none. If you select Simple, you need to supply a password and confirm it. If you select MD5, you must supply the Secret and confirm it. The default is none.

Cost

Cost of sending a packet on the interface expressed in the link state metric. Must always be greater than 0. The default is 10.

Priority

Priority of the routers on this interface. The router with the highest priority takes precedence in determining which is the designated router (DR). If there is a tie, the router with the highest Router ID takes precedence. A priority setting of 0 is ineligible to become a designated router on the attached network. Router priority only applies to broadcast networks. The default is 1.

Hello Interval

Length of time in seconds between the Hello packets that the router sends on the interface. It must be the same for all routers attached to a common network. The default is 10.

Dead Interval

Number of seconds after a router ceases to hear Hello packets before declaring that the router is down. It must be the same for all routers attached to a common network. The default is 40.

Poll Interval

If a neighboring router becomes inactive, the router sends packets at a reduced rate in seconds. The default is 120.

Retransmission Interval

Number of seconds between LSA retransmission for adjacencies belonging to this interface. It is also used for retransmitting Database Description and Link State Request packets. This setting should be considerably over the expected round trip delay between any two routers on the attached network. and should be conservative to prevent needless retransmissions. The default is 5.

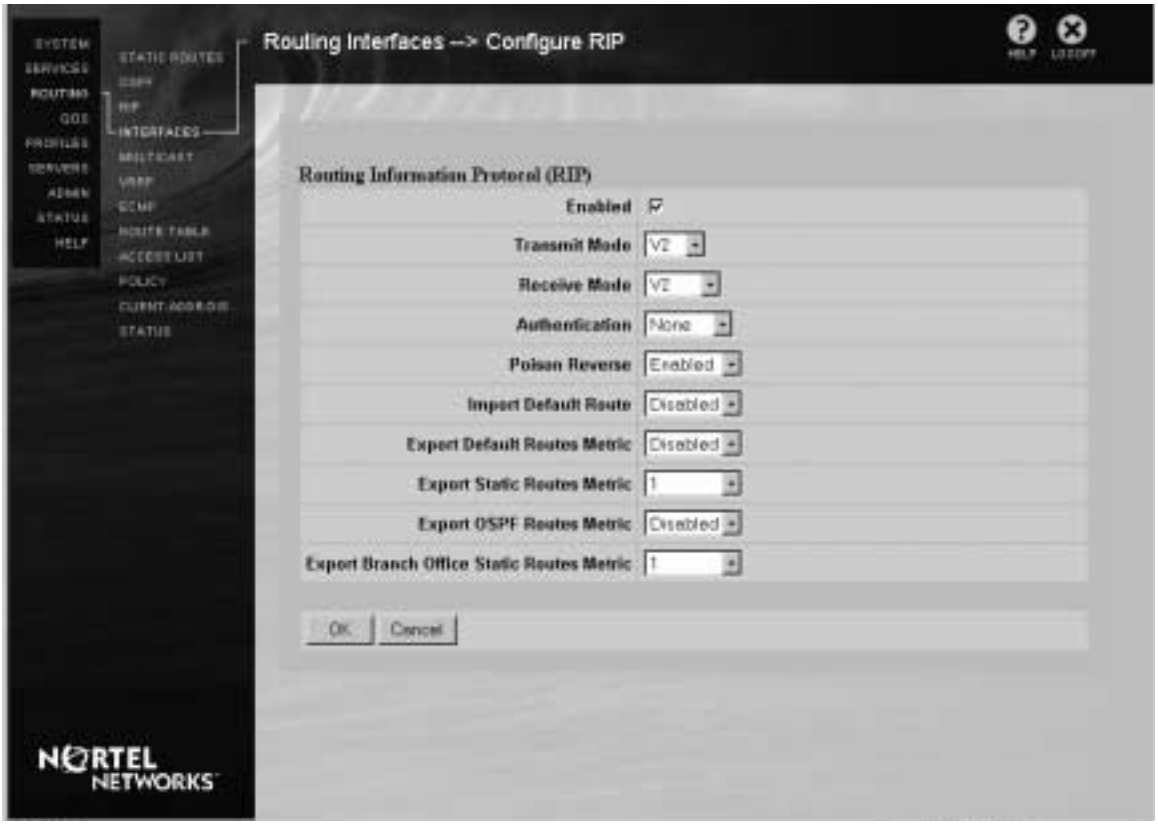
Transmission Delay

Estimated number of seconds it takes to transmit a Link State Update Packet over this interface. The default is 1.

RIP

To change the RIP configuration, go to Routing Interfaces→Configure RIP screen.

Figure 62 Routing Interfaces→Configure RIP



Enabled

Indicates that the RIP specifications on this interface have been enabled. (You have selected the global Enabled specification on the Routing→RIP screen.) The default is Enabled.

Transmit Mode

Transmit Mode enables you to specify which version of the RIP protocol is used when routing traffic from this switch. The default of V2 indicates RIP-2. You can select V1 to specify that RIP-1 traffic is sent. A selection of OFF specifies that RIP is not used.

Receive Mode

Receive Mode enables you to specify which version of the RIP protocol the switch accepts for incoming traffic. The default of V2 indicates that only RIP-2 traffic is accepted. You can select V1 to specify that RIP-1 is accepted. If you select OFF, RIP traffic is not accepted. If you select BOTH, incoming transmissions using either version of RIP are accepted.

Authentication

Indicates the type of authentication that is used as part of the RIP transmission. This authentication is specific to the RIP routing protocol and has no bearing on the authentication done as part of the connection to the switch. The default in None, which specifies that no authentication is required.

SIMPLE indicates that authentication is accomplished by using a simple password. MD5 specifies that authentication is accomplished by using a MD5 secret. If you select either Simple or MD5, password and confirmation fields are displayed below the selection.

Poison Reverse

Click to enable or disable poison reverse. Poison reverse updates remove routing loops in large networks.

Import Default Route

Typically, you specify a default route in the switch's Routing Table using Routing→Static routes. The switch then uses that default route when sending traffic to the private/public network. However, if no default route has been set, you can check the Import Default Route box and the switch uses the default route that it learned during RIP updates. The default is disabled.

Export Default Routes Metric

Use this field to specify that the switch's default route is exported during RIP updates. You can also choose a metric value (1 through 15) to the default route. The default is disabled.

Export Static Routes Metric

Use this field to specify that the switch's static routes are exported during RIP updates. You can also choose a metric value (1 through 15) to the routes. The default is 1.

Export OSPF Routes Metric

Use this field to specify that the switch's OSPF routes are exported during RIP updates. You can also choose a metric value (1 through 15) to the routes or disable the export. The default is disabled.

Export Branch Office Static Routes Metric

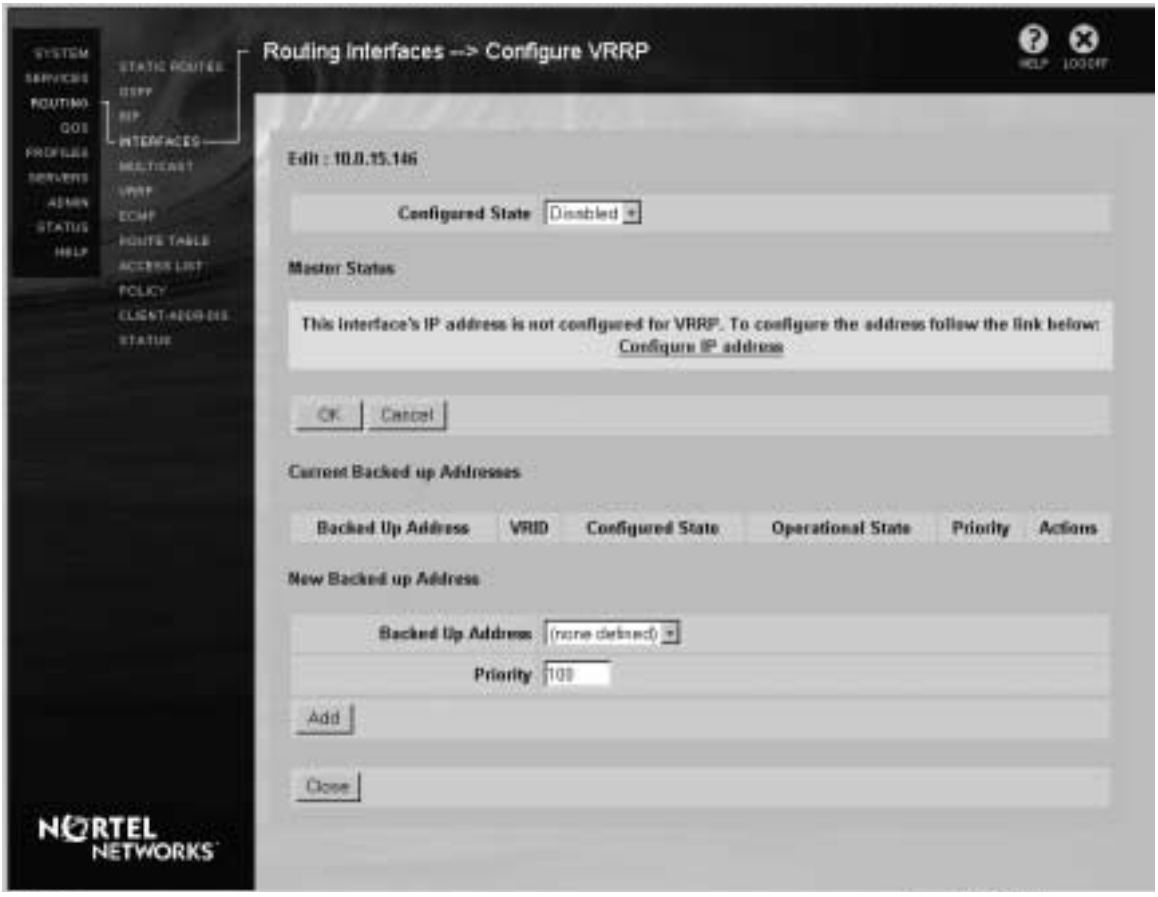
If you have a branch office connection, use this field to export the static routes metric. This informs the remote branch office connection of the routes that are used for the connection and provides the metric value you assign to the routes. The default is 1 and the map value is 15.

VRRP

VRRP is configured on a per-interface basis and is only available on private Ethernet interfaces. VRRP must be configured on each system interface individually. Select Routing→Interfaces to access the Routing Interfaces screen. From this screen, you can configure the switch routing protocols for each system interface.

To configure VRRP on the interface, click the Configure button next to the VRRP Protocol on the Routing Interfaces screen. The Configure VRRP screen appears.

Figure 63 Routing Interfaces→Configure VRRP



Configured State

The Configured State drop-down list box shows the current state, enabled or disabled. Select the desired state from these options.

Master Status

This section of the Configure VRRP screen is where you configure this interface to serve as a master for its own address.

Serve as Master

This drop-down list box lets you enable or disable this interface as a VRRP master of its own address. Enabled means that it serves as master. In order to enable mastership, there needs to be an entry in the Routing→VRRP screen with an IP address that matches this interface's address. The owner of the interface should have the option Serve as Master enabled.

Click OK after making a selection to effect the change.

VRID

The VRID column shows which VRID is used.

Operational State

Operational state shows the current running operational state, either Master or Backup.

Current Backed Up Addresses

The Current Backed Up Addresses section shows information about the currently configured backups. It shows what IP addresses this interface is backing up, the VRID it is using, its configured state (Enabled or Disabled), the current operational state and its priority. Multiple backups for the same address should have different priorities.

Edit

The Edit button allows you to enable or disable the backup address and to change its priority.

New Backed Up Address

New Backed Up Address allows new backups to be added. The pull down list here shows all the IP addresses set in the Routing→VRRP screen minus this interface's address and any other address that is already being backed up.

Backed Up Address

This list shows all the IP addresses set in the Routing→VRRP screen, minus this interface's address and any other address that is already being backed up.

Priority

The priority field specifies the sending VRRP router's priority for the virtual router. Higher values equal higher priority. The default Priority Value is 100 (decimal). If there are multiple backups, the Priorities should be scattered widely. For example, use Priority Values such as 50, 100, and 150, instead of 100, 101, and 102.

VRRP routers that are backing up a virtual router must use Priority Values between 1-253 (decimal). Priority 254 is reserved for use with the master delay mode.

Add

Click Add to add the address selected from the New Backed Up Address list box to the list of Current Backed Up Addresses.

Multicast

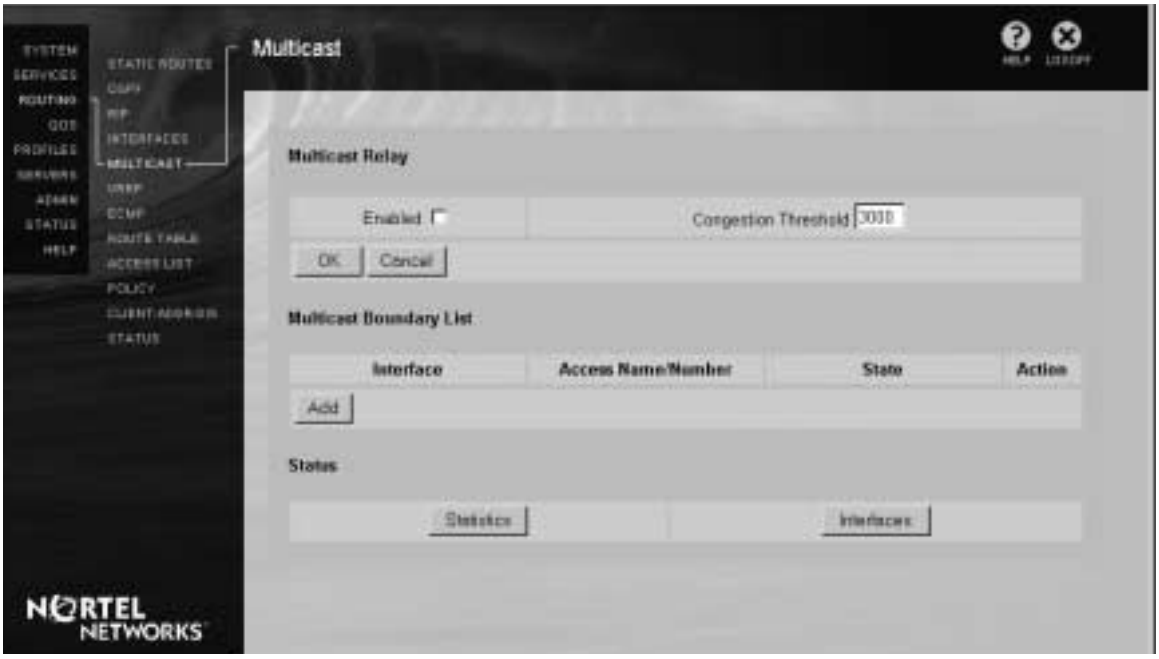
IP Multicast is an extension to the standard IP network-level protocol. It provides efficient delivery of information from a single source to multiple destinations. It is useful for applications such as video conferences, shared white boards, and news feeds. IP multicast uses class D addresses, ranging from 224.0.0.0 through 239.255.255.255. Multicast routing protocols establish the distribution tree for a given multicast group.

A multicast relay listens to an incoming multicast and forwards, or relays, that broadcast to one or more destination addresses in the absence of multicast routing. The destination addresses may be unicast in the case of tunnel or multicast. Multicast relay is not supported on public interfaces.

Multicast Relay

Click Routing→Multicast to configure multicast relay parameters.

Figure 64 Routing→Multicast



Enabled

Check the Enabled check box to enable multicast relay on the switch. By default multicast relay is globally disabled. If multicast relay is disabled on this screen, the switch processes only multicast requests in the range of 224.0.1.0 to 239.255.255.255. When you enable multicast relay, received traffic is filtered according to filter checking and access lists.

Note: Multicast requires use of the Permit All Interface filter (see "Filters").

Congestion Threshold

You can configure the congestion threshold as a percent of system resources. The default value is 3000. If the unicast packet forwarding performance decreases due to multicast traffic, you can reduce this number.

Multicast Boundary List

Interface

The IP address of the interface.

Access Name/Number

The name and number of the access list to apply.

State

Indicates whether the state of the interface is enabled or disabled. You can enable or disable the multicast relay on the switch, which overrides any individually enabled interfaces.

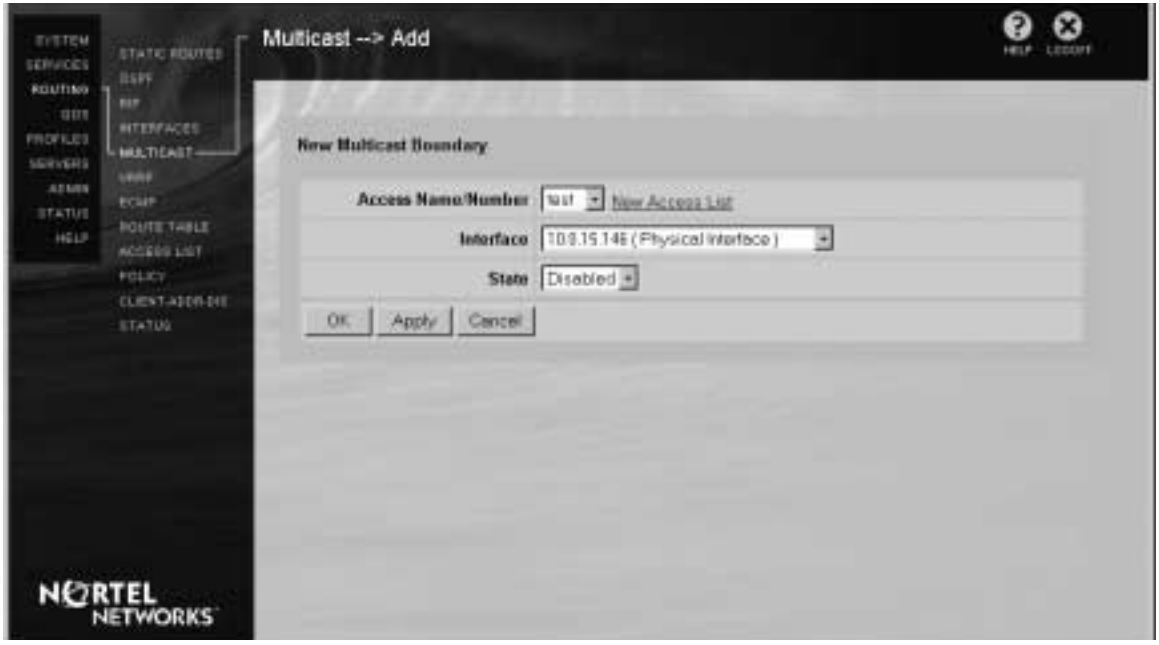
Action

Click on the appropriate buttons to edit, delete or enable/disable the interface.

Add

Click on the Add button to add an interface to the multicast boundary list. The Multicast→Add screen allows you to add an interface.

Figure 65 Multicast→Add screen



Enter the Access Name/Number in the edit box, select the IP address for the interface, and select the either Enabled or Disabled for the State. Click on the New Access List link to view the existing access screen.

Status

Statistics

The statistics screen displays the global multicast relay status and the statistics of the configured multicast interfaces, including branch office interfaces.

Figure 66 Multicast→Statistics screen

The following table describes fields on the Multicast Statistics screen.

Table 16 Multicast Statistics screen

Column	Description
Interface	IP address of interface
CID	Circuit ID
PktsRcvd	Number of packets received
PktsSent	Number of packets sent
PktsDropped	Number of packets dropped

Interfaces

The interfaces screen displays all of the configured information about enabled interfaces, including private physical and branch office tunnel interfaces.

Figure 67 Multicast→Interfaces screen

The following table describes fields on the Multicast Interfaces screen.

Table 17 Multicast Interfaces screen

Column	Description
Interface	IP address of interface
Access-list	Name of the access list

VRRP

Virtual Router Redundancy Protocol (VRRP) is one method you can use to configure the switch to maintain a state of High Availability. VRRP is a standard protocol that handles private interface failures. VRRP targets hosts that are configured with static next-hop routing addresses or default gateways. It provides a means of re-routing traffic in the event of a system/interface failure.

VRRP configuration

VRRP is managed as two separate parts. The first part handles those configuration parameters that must be the same between all switches that make up a VR (Virtual Route).

Use of an external LDAP server makes it easier to configure VRRP because it provides a common location in which information about each switch in the system can be maintained. Use of an external LDAP server enables each switch to see the settings of other switches on the system. Configuration of VRRP requires that VRIDs (Virtual Router IDs) are agreed to by all participating switches.

An external LDAP server is not a requirement. If the internal LDAP server is being used then the various switches must have these parameters configured the same and the responsibility for doing so lies with the administrator.

The second part of VRRP configuration is the information that is specific to a switch. This is information that is related to an interface and the role that the interface plays in VRRP (master or backup). This information is kept in the normal configuration file that is stored on the switch.

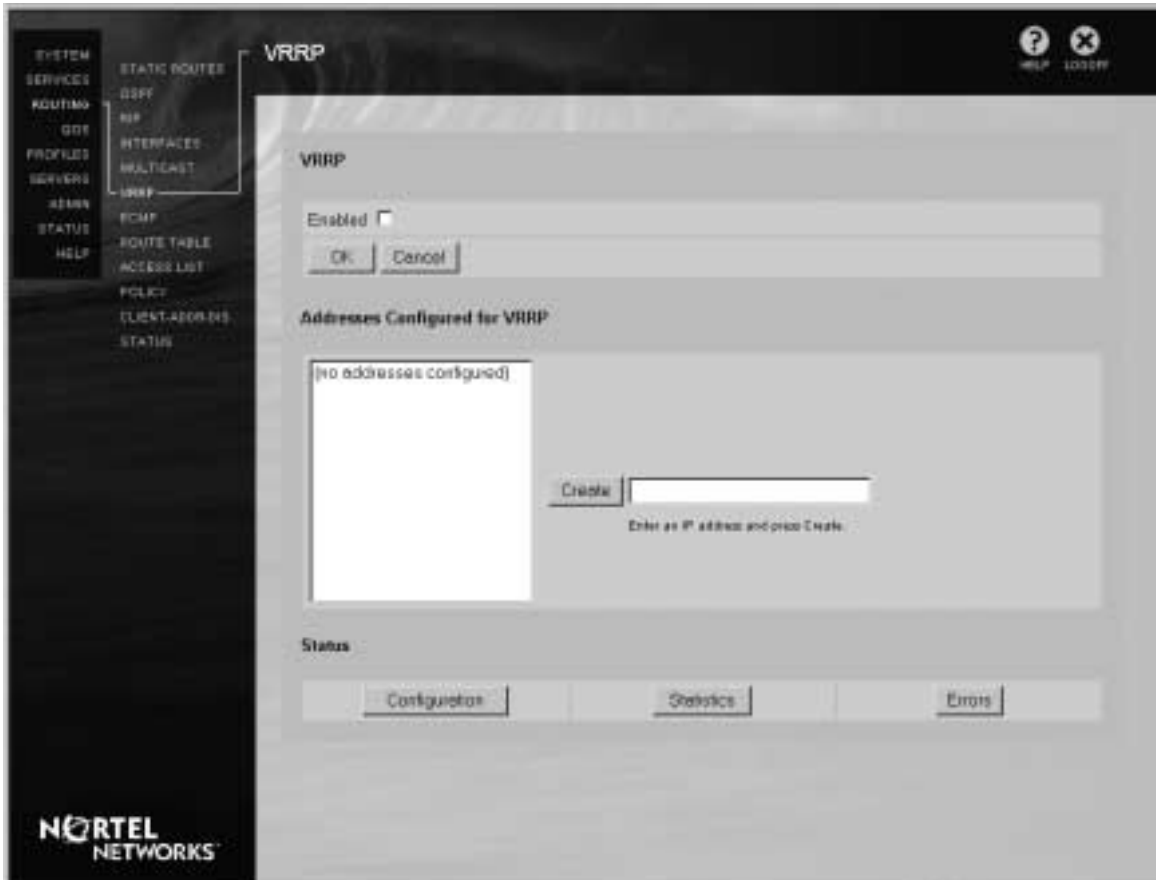
VRRP screen

The Routing→VRRP screen lets you configure addresses for the Virtual Router Redundancy Protocol (VRRP). It also provides access to configuration information, statistics, and error information for VRRP addresses.

The Enabled check box allows you to globally enable or disable VRRP. The default is disabled. If you have an existing VRRP configuration, you must enable VRRP when you upgrade your switch.

Note: You must have the Advanced Routing key to globally enable VRRP. However, you can now enable VRRP on an interface without having the Advanced Routing key installed.

Figure 68 VRRP screen



Addresses Configured for VRRP

This list box shows all IP addresses that have been configured for use with VRRP.

Note: Only one IP address per Virtual Router (VR) is allowed.

IPSec AH (Authentication Handling) is not supported as an authentication option.

Edit

Select the VR that you want to modify from the Addresses Configured for VRRP list and click Edit. The Create/Edit VRRP IP Address screen appears. The Edit VRRP IP Address screen is the same as the Create VRRP IP Address screen.

Delete

Select the VR that you want to delete from the Addresses Configured for VRRP list and click Delete.

Create

To create a new Virtual Router, enter the IP address in the IP Address field and click Create. The IP Address must match an Interface Address, as shown in the Routing→Interfaces screen, when configuring the VR as a Master.

The VRRP→Create/Edit VRRP IP Address screen appears when you click Create. You use this screen to configure the parameters for the VR you are creating.

Create/Edit VRRP IP Address Screen

The VRRP→Create/Edit VRRP IP Address screen appears when you click Create or Edit. You use this screen to configure the parameters for the VR you are creating or editing.

Changes to these parameters take effect only when VRRP is started on an interface, not while it is running. To make any changes take effect, disable VRRP on the Interface and then enable it.

Figure 69 VRRP→Create/Edit VRRP IP Address

VRID

Enter a decimal value in the range 1-255 for the Virtual Router ID (VRID). The VRID must be unique to the LAN segment running VRRP.

Advertise Interval

Enter the interval, in the range 1-255 seconds, at which the VR will advertise its virtual MAC Address. The default is 1 second.

Note: VRRP advertisements are sent to the 224.0.0.18 multicast IP address.

Authentication Type

Select the Authentication Type for this VR, either None or Simple.

Selection of None means that VRRP protocol exchanges are not authenticated. Nortel Networks recommends this type of authentication for environments with minimal security risk and little chance for configuration errors.

Selection of the Simple authentication type means that VRRP protocol exchanges are authenticated by a simple text password. Nortel Networks recommends this type of authentication when there is minimal risk of nodes on a LAN actively disrupting VRRP operation.

Authentication Data

Enter up to 8 characters of text. Any VRRP packet received with an authentication string that does not match the locally configured authentication string is discarded.

Confirm Authentication Data

Enter the same 8-character text password in this field as entered in the Authentication Data field to confirm it.

Master Delay Mode

Master Delay Mode controls when a switch takes mastership of an IP address it owns. Normally, this occurs when the interface becomes enabled. With Master Delay Mode it is possible to delay when this happens. Reasons for using Master Delay Mode include: you might want to wait to ensure that the switch is stable before having it start processing data; or you might want to wait until a slow period of the day to move traffic back.

Master Delay Mode controls when a switch takes back its IP addresses. It has no effect on the underlying VRRP protocol. A switch with Master Delay Mode enabled interoperates with another switch that does not support Master Delay Mode.

Master Delay Mode is optional. The default for a VR is that Master Delay Mode is disabled (None).

Master Delay mode operates in one of two possible ways: Delay or Time of Day.

Note: The Safe Mode feature has the following interaction with Master Delay Mode: When safe mode is enabled, a boot after an unclean failure starts the safe mode image, instead of the normal boot image. If the safe mode image is configured with VRRP then Master Delay Mode works. However, safe mode automatically boots the normal image after some delay. This boot looks as though it was after a clean shutdown and Master Delay Mode is not invoked.

Delay

The Delay mode causes the switch to wait a given amount of time, after a system boot or after the circuit comes up, before the switch asserts its mastership. When you select Delay, the Master Delay Delta field appears on the screen. Enter the Delay time in this field in the form *hh:mm:ss*.

Time of Day

Time of Day mode allows a specified period, or window, of time to be set. Time of Day specifies the start of a window of time (in 24-hour format), and Delay specifies the size of that window of time. If the switch is booted or the circuit comes up within that window, then the switch immediately assumes mastership as though Master Delay mode was not in effect. If the switch is booted or the circuit comes up outside the specified window of time, then the switch waits until the beginning of the window before assuming mastership.

When using an external LDAP database, the following read-only fields appear, providing additional information about external switches.

Master CES

This field displays the serial number of the switch configured to be Master of this address.

Backup CES

This field displays the serial number, name and priority of other switches configured as backups for this address.

Status

The Status section of the VRRP screen provides buttons for accessing information about VRs. This includes configuration, statistics, and error information.

Configuration

You can view configuration information for a VR using the Configuration button. Select from the list of Addresses Configured for VRRP and then click Configuration.

Figure 70 VRRP→Configuration

The following table describes the fields on the VRRP configuration screen.

Table 18 VRRP configuration information

Column	Description
Slot	Slot number associated with the interface on which this VR is configured.
Port	Port number associated with the interface on which this VR is configured.
VRID	Virtual Router ID number.
State	Operational state for this configuration, either M (Master) or B (Backup).
Time	(Hours:minutes) in this particular state
Prio	Shows the Priority level of this VR configuration
IpAddr	IP Address of this VR configuration.
Int	Advertisement interval
Prmt	Preempt Mode setting, either True or False.
Auth	Authentication type for this configuration, either None or Simple

To view statistical information about a VR, select from the list of Addresses Configured for VRRP and then click Statistics.

Figure 71 VRRP→Statistics

The following table describes the fields on the VRRP Statistics screen.

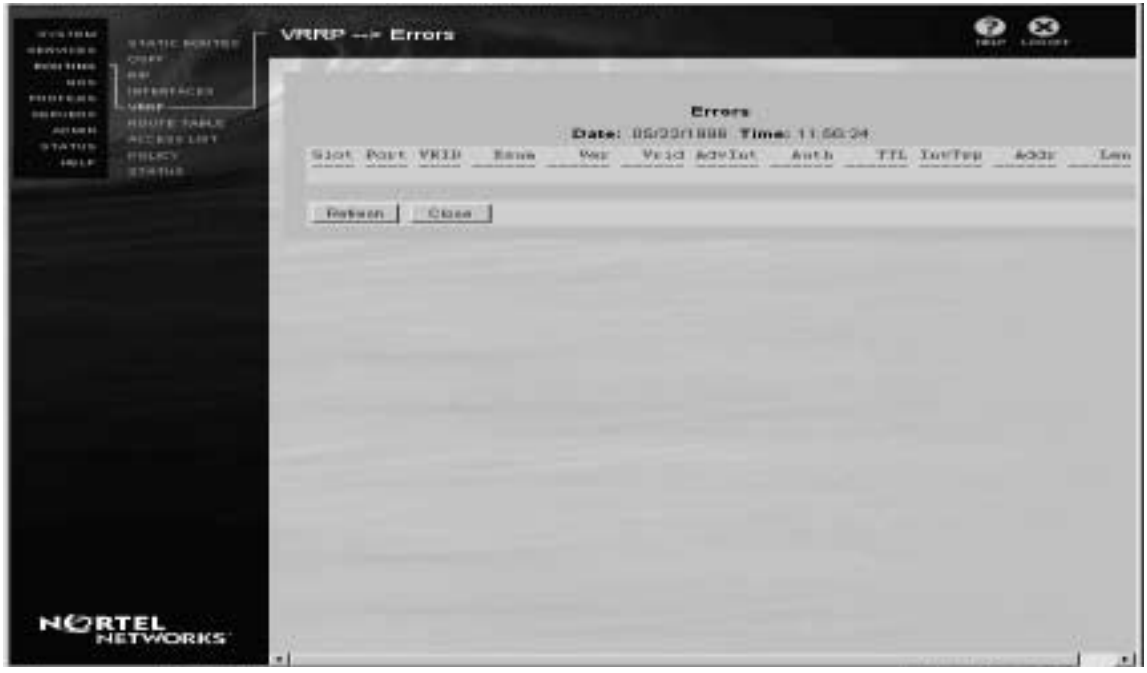
Table 19 VRRP Statistics screen

Column	Description
Slot	Slot number associated with the interface on which this VR is configured
Port	Port number associated with the interface on which this VR is configured.
VRID	Virtual Router ID number
MstCnt	Number of times this switch became master of this address.
AdvSnt	Number of advertisements broadcast by this VR.
AdvRcv	Number of advertisements received by this VR.
0Snt	Number of advertisements with a priority of 0 that were sent. Priority 0 advertisements are sent when VRRP is shutdown on an interface. They allow a backup to take over immediately.
0Rcv	Number of advertisements received with a priority of 0.
Errors	Shows the number of errors that have occurred

Errors

To view error information about a VR, select from the list of Addresses Configured for VRRP and then click Errors.

Figure 72 VRRP→Errors



The following table describes fields on the VRRP Errors screen.

Table 20 VRRP Errors screen

Column	Description
Slot	Slot number associated with the interface on which this VR is configured.
Port	Port number associated with the interface on which this VR is configured.
VRID	Virtual Router ID number.
Xsum	Number of packets received that had bad Checksums
Ver	Number of packets received that specified an unsupported version of VRRP

Table 20 VRRP Errors screen (continued)

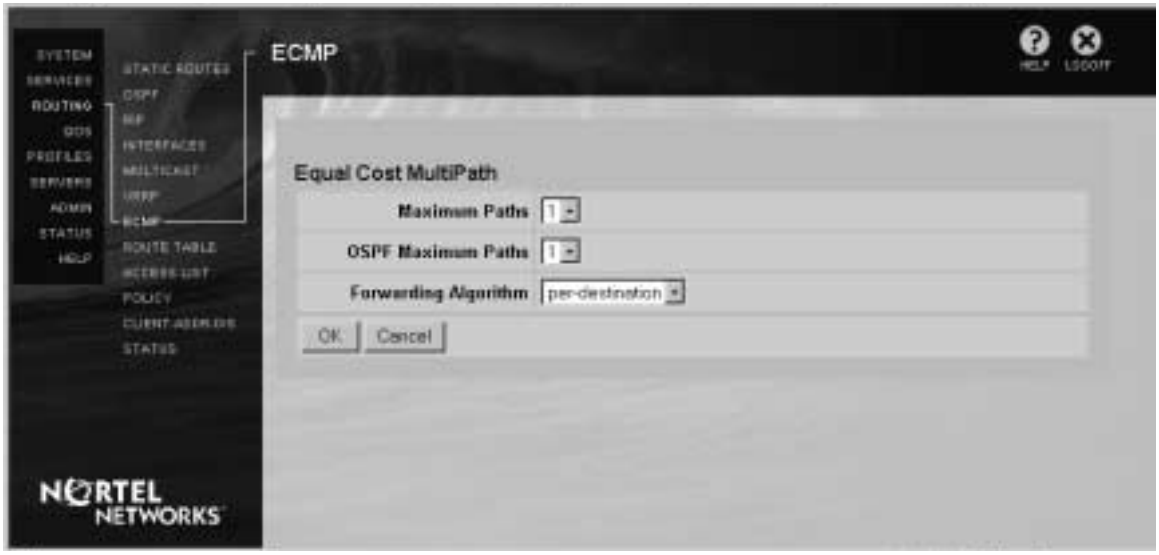
Column	Description
Vrid	Number of packets received that indicate a VRID that is not configured on this interface.
AdvInt	Number of packets received with incorrect Advertisement Intervals
Auth	Number of packets that failed Authentication
TTL	Number of packets received with an invalid TTL value in the IP header.
InvTyp	Number of packets received with invalid VRRP packet types.
Addr	Number of packets received that specified the incorrect IP address for this VR
Len	Number of packets received that had an incorrect length

ECMP

Equal Cost Multipath provides load balancing of packets to a destination that is reachable over more than one physical interface. This can increase the forwarding capacity of a switch that is media bound. Load balancing is provided on a per packet basis or a packet stream basis. You can also use it to balance traffic over tunnels whether or not they are going out a single or multiple physical interfaces.

With Equal Cost Multipath the routing protocol applications can submit an equal cost route for a destination. The routing table manager passes the set of equal cost best paths to the forwarding engine mapper (FEM) and the packet content engine (PACE) load balances the traffic across the equal paths to the destination.

Figure 73 Routing→ECMP



Maximum Paths

The global compile time maximum equal cost paths parameter allows the switch to store the maximum equal cost paths. The compile time equal cost paths is eight paths.

OSPF Maximum Paths

OSPF compile time maximum equal cost paths parameter is four paths.

Forwarding Algorithm

You can change the forwarding algorithm to per-packet, per-destination, or per-source. Changing the forwarding algorithm has no effect on the routing or forwarding databases.

Route Table

The route table contains routes submitted by the routing protocols and the static routes. Dynamic protocols such as OSPF and RIP submit the best rout in their view for a specific destination. The switch stores all of the static routes and default routes in the route table.

The route table manager chooses the best route based on the following order of protocol priority: direct route, static route, OSPF route, RIP route, default route. With this and the protocol cost, the route table manager selects the best route and forwards it to the forwarding table. This screen provides information about the current routing table, and it allows you to view the routes using filter search criteria and save the information in a file.

Figure 74 Route table filter criteria screen

Note: To obtain the total number of routes that are in the routing table, go to the Routing→Status screen and click on Route Table Stats.

Search For

Select the All, Host, or Network option. If you select Host, you can select whether the interface is All or choose the address from the Interface drop-down list. From the Protocol drop-down list, select All or the protocol (OSPF, RIP, Static, or Direct). You must enter the IP address in the edit box.

If the destination is Network, you can select whether the interface is All or choose the address from the Interface drop-down list. From the Protocol drop-down list, select All or the protocol (OSPF, RIP, Static, or Direct). You must enter the IP address and the Network Mask in the edit boxes. You can choose the Exact or Best Match from the Search Type drop-down list.

Interface

Select All or the current switch interface.

Protocol

Select All, OSPF, RIP, Static, or Direct.

Save Route Table

Filename

You can save the route table as a text file in the directory ide0/system/*xxx*/, where *xxx* is the name of the file that you specify.

Route Filter

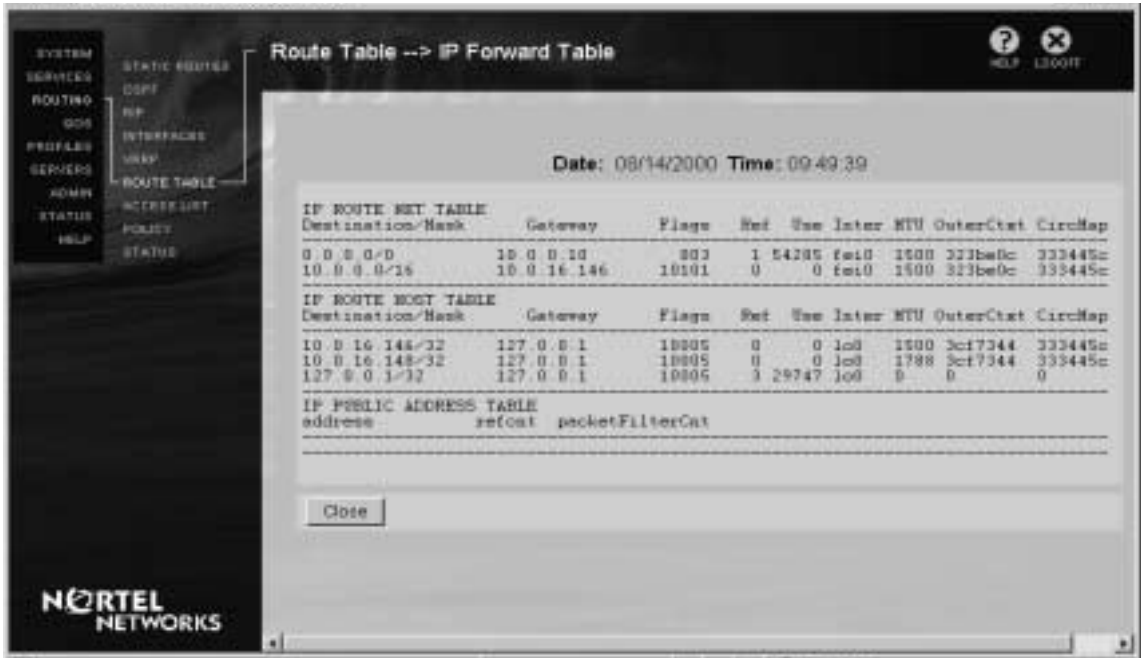
Select Best Routes to view all routes to a single or All Routes to view all destinations. The default is Best Routes.

Status

IP Forward Table

The IP forwarding table displays the following information for the IP Route Network Table, the IP Route Host Table, and the IP Public Address Table.

Figure 75 Route Table→IP Forward Table Screen



The following table describes fields on the IP Forward Table screen.

Table 21 IP Forward Table Screen

Column	Description
Destination/Mast	Network address and mask
Gateway	IP address of next hop gateway
Flags	Internal use flags
Refcnt	Reference count
Use	How many time used
Interface	Interface identifier

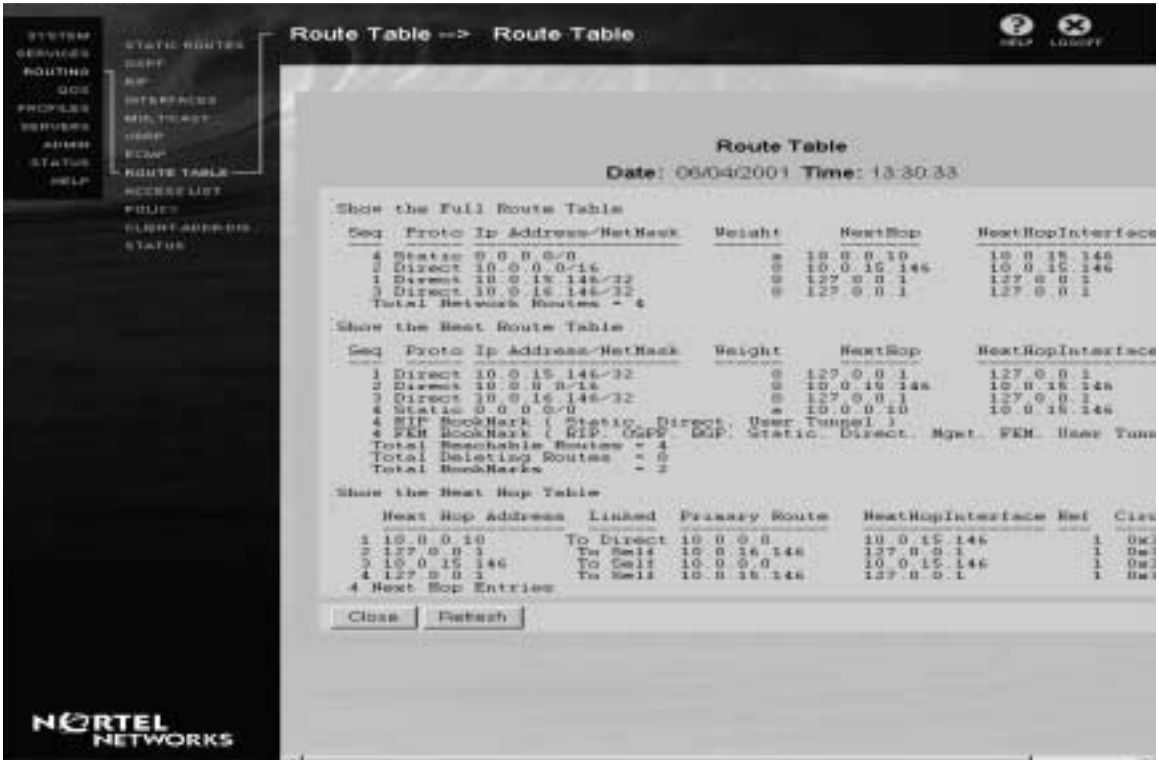
Table 21 IP Forward Table Screen

Column	Description
MTU	Size of packet
OuterCtxt	(For internal use only)
CircMap	(For internal use only)
RtEntryP	(For internal use only)

Route Table

The full internal routing table displays all routing information.

Figure 76 Route Table→Route Table



The following table describes fields on the IP Routing Table screen.

Table 22 IP Routing Table screen

Column	Description
Seq	Sequence number that shows the best route
Proto	Protocol
IP Address/Netmask	IP Address/NetMask
Weight	A combination of cost and priority for the best route
NextHop	IP address of the next hop
NextHopInterface	IP address of the next hop interface
CId	Circuit ID

Access List

Routing policies are based on a set of rules that result in actions. However, you can have access lists that are part of any policy. An access list contains these rules and actions, which allows you to use the same set of rules for different protocols. These rules are tested in order until the first match is found, which then causes the action to occur. Routing policies have an implicit deny all rule, which means that if no rule matches then access is denied; no traffic is transmitted or received unless it is specifically permitted.

The Access Lists screen displays all previously created lists. You can edit or delete a selected list name or create a new one.

Figure 77 Access List

Create

Type in the name of the access list in the edit box and click on the Create button to create a new access list. You can use any name or number that you choose to a maximum length of 64 characters.

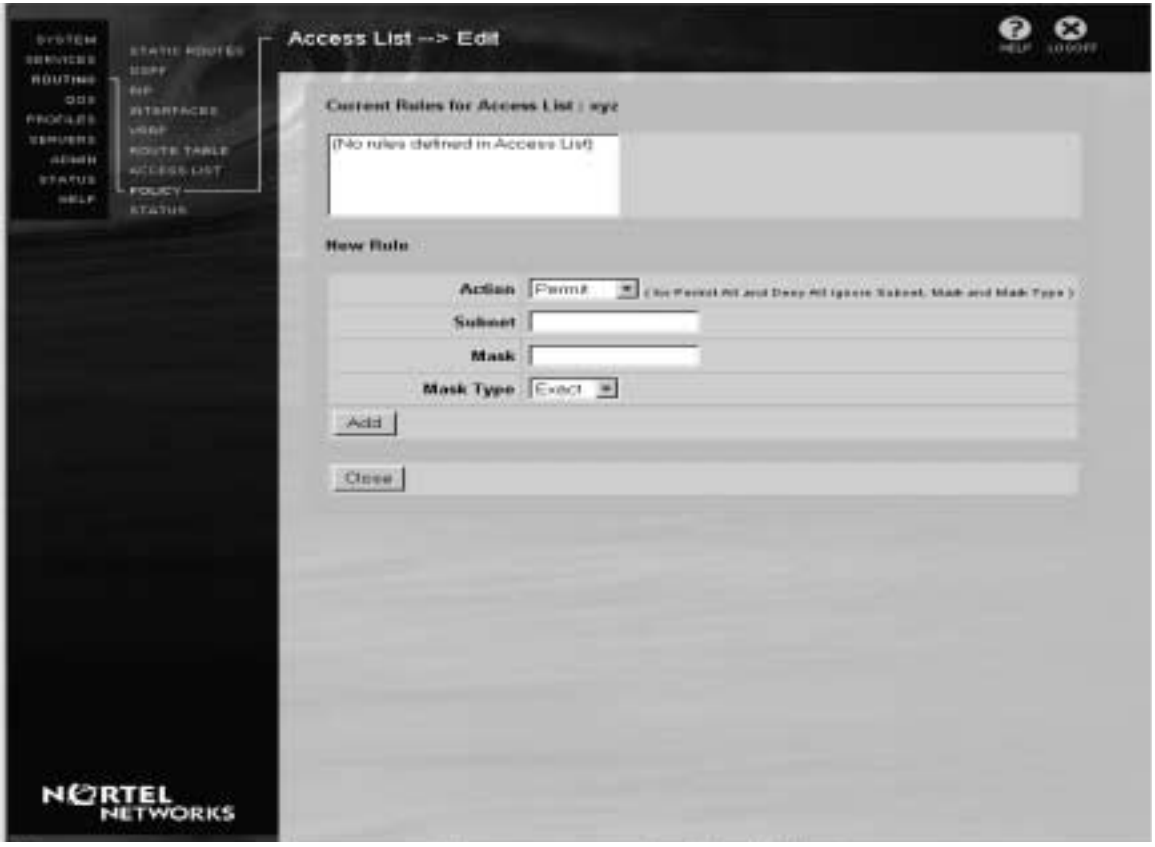
Figure 78 Access List→Create

Current Rules for Access List: *xxx*

Edit

Click on the Edit button to change the existing rule for the selected policy. The current information appears for each policy. You can use either an exact network address or a range of network addresses.

Figure 79 Access List→Edit



Delete

Click on the Delete button to delete the selected rule.

Move selected rule to position

Entering a number in the edit box allows you to specify the position of an existing rule. For example, if you select the third rule and enter 2 in the edit box, this moves the third rule to the second position. Selecting the order of the rules is important because the first match causes the action to occur. If there are no matches, then all traffic is denied. Therefore, you should build your filter rules by first permitting the services that you want to allow. You also might want to add a Deny rule early in the rules sequence so that an unwanted packet is dropped before processing all of the rules.

New Rule

Click on the Create button to add a policy to the policy list. This displays the Access List→Edit screen.

Action

Options are Permit, Deny, Permit All or Deny All. Permit or Deny is the action applied to a route update when the subnet and mask matches the route update. If you choose Permit All or Deny All, you cannot enter anything in the Subnet, Mask or Mask Type fields.

Subnet

IP address of the subnet for which you want to create a rule. Subnet is the number of the network. The subnet should be specified using a 32-bit quantity in four-part, dotted-decimal format.

Mask

Subnet mask of the subnet for which you want to create a rule. Mask is the network mask to be applied to subnet. The network mask is a 32-bit quantity in four-part, dotted-decimal format. Place zeroes in the bit positions you want to ignore.

Mask Type

Specify Exact or Range.

Policy

Policies are used to control reachability by allowing or restricting routing information. RPS controls the flow of routing data to and from the routing table. Routing policies are based on a set of rules that result in actions. Routing policies have an implicit deny all rule, which means that if no rule matches access is denied.

An access list that contains this set of rules and conditions allows you to use the same set of rules for different protocols. Redistribution allows route updates to be redistributed from one routing domain into another routing domain. It helps connect networks of different protocols by allowing specified redistributed routes to know about networks that are not normally advertised.

The Policy screen allows you to set up the routing policies.

Figure 80 Routing Policy Service

Route Policy Service

Check the Enabled box to enable RPS. The default setting is disabled.

Redistribution Table

Protocol

The name of the protocol, either OSPF or RIP.

Route Source

The source of the route for each protocol, either Static, Direct, or RIP.

Policy List

Access Name/Number

This is a way to identify the policy. This can be any name or number that you choose. A numbered access list can use numbers between 1 and 99. A named access list can be any alphanumeric name that begins with a letter of the alphabet. You need to create an Access list before creating policy entries. To create the list, click on the New Access List link. This displays the Access Lists screen with all named items listed. You can edit or delete a selected list name or create a new one by typing the name in the edit box.

Protocol

The name of the protocol, either OSPF or RIP.

Interface

IP address of the physical interface where you want to apply the policy. Use 0.0.0.0 if you want to apply the policy for all interfaces. Use the tunnel endpoint IP address for tunnels.

Policy Type

Accept or announce policy. You can have only one Accept or Announce policy for each protocol per interface.

Action

Edit

Click on the Edit button to edit the selected policy.

Delete

Click on the Delete button to delete the selected policy.

Add

Click on the Add button to display the Policy→Add screen. Enter the Protocol, Access Name/Number, Interface, and Policy Type.

Figure 81 Policy→Add

Client address redistribution

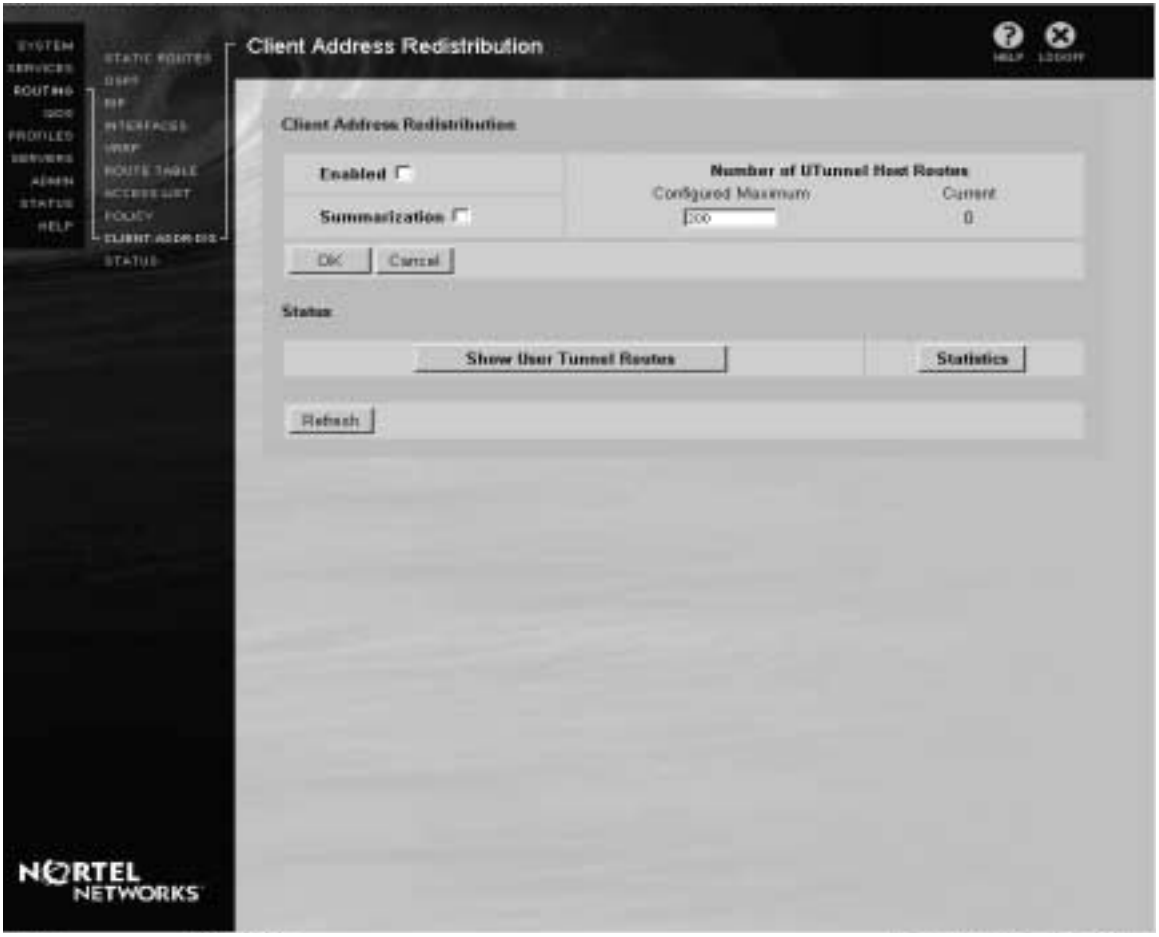
Client address redistribution allows the switch to advertise user tunnel host network routes if the private address does not belong to a locally attached switch network. It dynamically advertises one route for each connected client, which begins when the client logs in and ends when the client logs out. This is the default.

When client address redistribution is active, the switch creates and advertises a user tunnel host route whenever a client tunnel is created using an inner address that does not belong to a locally attached network. When the tunnel is disconnected, the corresponding host route is deleted.

Note: The maximum number of Utunnel routes cannot exceed the maximum number of client tunnels supported by the corresponding hardware platform. The default value is 200.

The Routing Table Manager handles a Utunnel route type that handles advertisement of these routes and they correspond to the Direct, Static, RIP, and OSPF types. Click Routing→Client-Addr-Dis to configure client address redistribution routes.

Figure 82 Client Address Redistribution



Client address redistribution

Enabled

Check the Enabled box to enable client address redistribution. If you enable client address redistribution, operations related to the Utunnel are effective. If you disable client address redistribution, the switch stops redistribution of all Utunnel routes. The routes remain in the route table, but are not advertised. Any existing user tunnels remain logged in, but may not be able to communicate with the private network and any new Utunnel routes are disallowed. The default is disabled.

Number of UTunnel Host Routes

Configured Maximum

This field allows you to limit the maximum number of user tunnel host route entries in the system. The default value is 200.

Current

This field displays the current number of user tunnel hosts logged in to the system.

Summarization

Check the Summarization box to enable summarization. If you disable summarization, the switch inserts a user tunnel host route for the client address into the route table. If you enable summarization, the switch identifies the subnet from the address pools where this address belongs and inserts a user tunnel network route for this subnet in the route table. The default is disabled.

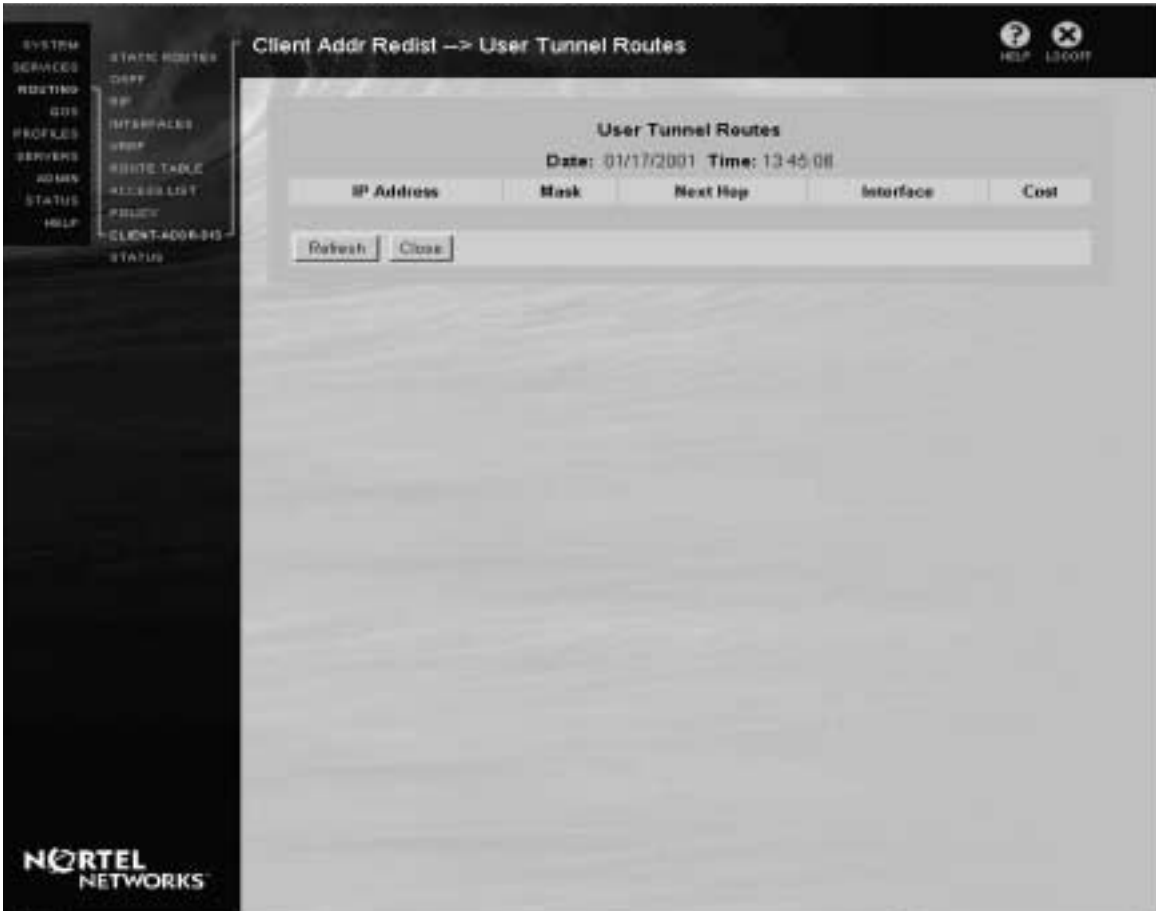
Note: The summarization option works only for address ranges that do not belong to the local subnet and that are allocated by the switch from an address pool.

Status

Show User Tunnel Routes

Click to display user tunnel routes.

Figure 83 Client Addr Redist→User Tunnel Routes



Statistics

Click to display the configuration of client address redistribution, including whether it is globally enabled or disabled, the utunnel limit, current utunnel count, current utunnel redistribution configuration and summarization options. Table 23 describes these statistics.

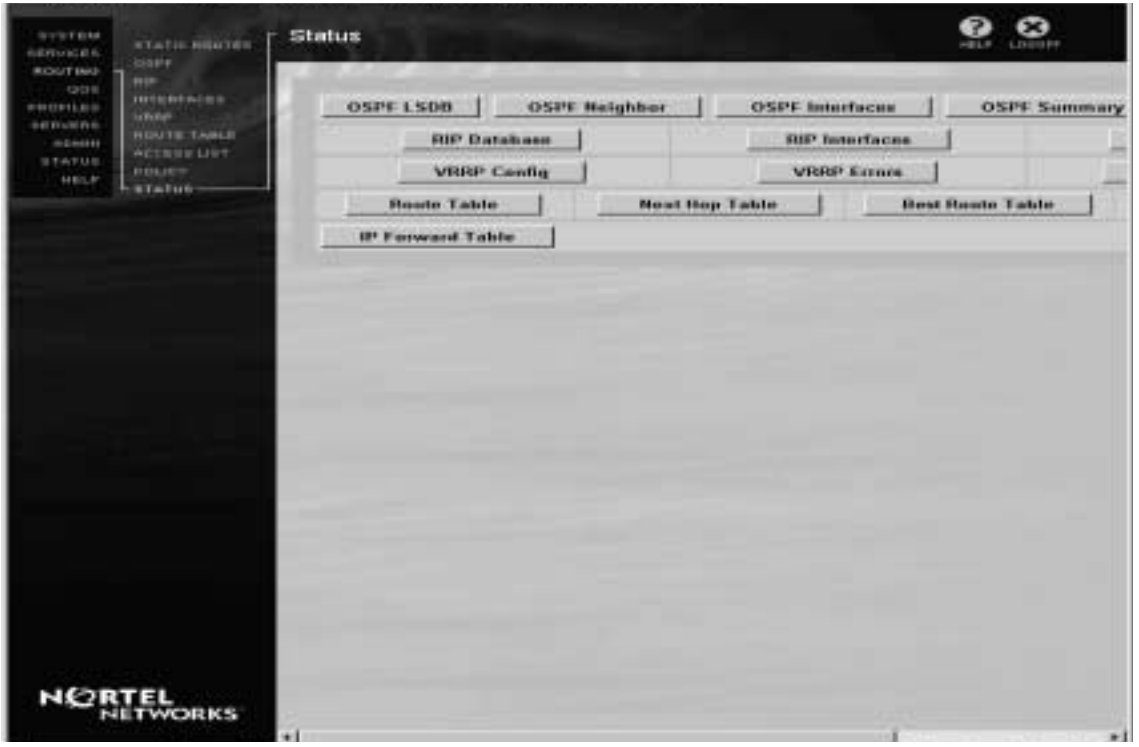
Table 23 Client address redistribution statistics

Column	Description
IP address	IP address
Mask	IP network mask
Next Hop	Next hop address
Interface	IP interface address
Cost	Relative cost for the switch

Status

This screen provides access to information about the status of the OSPF, RIP, and VRRP protocols. It also provides access to the Route Table and RTM Statistics. To view the information for each of these, click on the appropriate button.

Figure 84 Routing Status



OSPF LSDB

Lists the link state databases in all areas that are known to OSPF. For each area, it provides the link state type, ID, advertising router address, metric, ASE, forward address, age, and sequence number.

OSPF Neighbor

Shows the list of neighbors on all the interfaces running OSPF, including the IP interface address, router ID, neighbor IP address, state, and dead time priority.

OSPF Interfaces

Shows the list of interfaces that you configured for OSPF, including the IP address of the interface, the area to which the interface belongs, the type of interface, the state, cost and the designated router in the area to which the interface belongs.

OSPF Summary

Shows the overall summary of OSPF running on the switch. It specifies the router ID, global state (Up or Down), whether it is an area border router and whether it is an autonomous system border router.

OSPF Statistics

Shows system-wide OSPF statistics.

RIP Database

Shows the information contained in the RIP database.

RIP Interfaces

Shows the list of interfaces that you configured for RIP.

RIP Statistics

Shows system-wide RIP statistics.

VRRP Config

Shows VRRP configuration information.

VRRP Errors

Shows system-wide VRRP errors that have occurred.

VRRP Statistics

Shows system-wide VRRP statistics.

Route Table

Shows full routing for all routes, including next hops and best routes.

Next Hop Table

Shows the next hops for routes.

Best Route Table

Used by the forwarding table to determine the best route.

Route Table Stats

Shows statistics about routing table management that provides information about switch traffic.

IP Forward Table

Displays information for the IP route.

Chapter 4
QoS (Quality of Service)

Quality of Service (QoS) is an area of functionality that provides settings for specifying the quality of network connections. QoS is implemented in the IP protocol by the DiffServ Code Point (DSCP) in the IP packet header.

The QoS menu includes screens that provide a convenient way to set and configure DiffServ (Differentiated Services) settings so you can ensure certain treatment, or Quality of Service, of data. QoS capabilities enable you to exert a specified level of control over data transmissions.

Figure 85 QOS menu

Classifiers

An MF Classifier can be defined for an interface (interface MF). The interface MF-Classifier is applied to routing traffic going through that interface.

Interface classifiers are configured from the QoS→Classifiers screen.

Figure 86 QOS→Current Multi-Field (MF) Classifiers

Current Multi-Field (MF) Classifiers

The Current Multi-Field (MF) Classifiers list includes all existing MF Classifiers. You can edit and delete MF Classifiers by selecting from this list. These MF Classifiers can then be associated with user-groups, branch office connections, and physical interfaces.

Create

Enter a name for the new classifier in the field and click Create to create a new MF Classifier.

Delete

Select from the Current MF Classifiers and click Delete to remove the selected Classifier.

Edit

Select from the Current Multi-Field (MF) Classifiers and click Edit to edit the rules for that MF Classifier. The Edit Rule screen appears when you click Edit.

Rules in Classifier

The Rules in Classifier list shows all of the rules that are applied to the MF Classifier.

Available Rules

The Available Rules list shows all of the existing rules. You can select rules from this list to move them into the Rules in Classifier list and apply them to the MF Classifier.

<< (Add Rule)

Click on a rule from the Available Rules list on the right of the screen, then click on the left arrow to add the rule. This adds the selected rule to the current rules list. The new rule is added after the rule currently selected in the Rules in Classifier list.

>> (Remove Rule)

Click on a rule, then click the right arrow to remove or delete it from the Rules in Classifier list.

Manage Rules

You use the Manage Rules button in the Edit Classifier screen to create and edit rules. When you click Manage Rules, the Current Rules screen appears. From this screen you can create, edit, copy and delete MF Classifier Rules.

Figure 87 QOS→Rules

Current Rules

The Current Rules list shows all existing rules. You can edit, copy or delete any of these existing rules.

Create

Click Create to create a new rule. The Edit/Create Rules screen appears when you click Create.

Edit

You can make changes to an existing rule by selecting it from the list of Current Rules and clicking the Edit button. The Edit/Create Rules screen appears when you click Edit.

Copy

You can use the Copy button to create a new rule that starts as a copy of an existing rule, which you can then edit. This is useful if you want to make minor changes to an existing rule. When you copy a rule, the Edit/Create Rules screen appears, populated with the settings of the rule you have copied.

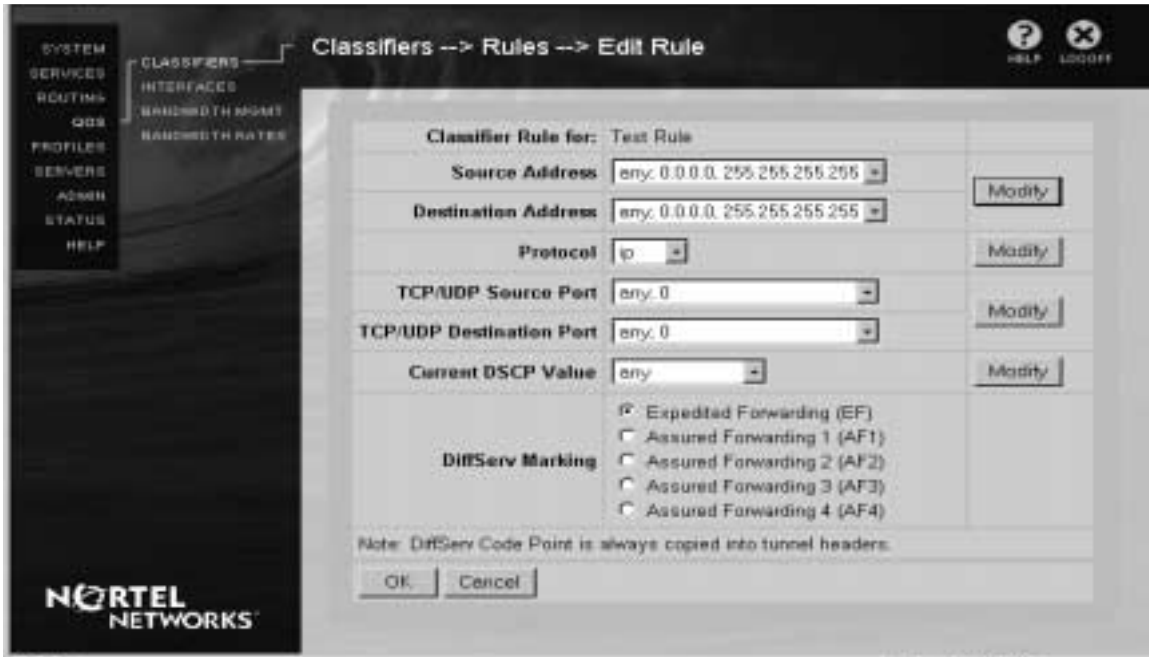
Delete

To remove a rule, select it from the list of Current Rules and click Delete.

Edit/Create Rules screen

The Edit and Create Rules screens let you create and modify MF Classifier rules.

Figure 88 Classifiers→Rules→Edit/Create Rules



Classifier Rule for

When editing an existing rule, this field shows the name of the rule.

Source Address and Destination Address

Enter the Source and Destination addresses to limit the rule to acting on packets from and to these specified addresses.

Source and Destination are relative to the direction of the rule.

Modify Source & Destination Address

Click the Modify button to the right of the Source and Destination Address fields to edit either of these fields. The DiffServ→Rules Definition→Address screen appears.

Protocol

Click the drop-down list box to select the appropriate Protocol. To add, edit, or delete Protocols, click Modify. The default list follows:

- ICMP - Internet Control Message Protocol is a Network protocol layer. The PING utility generates ICMP packets. PING is often used to see if a system's network is available.
- IP - Internet Protocol is a Network layer protocol in the TCP/IP stack that offers a connectionless internetwork service. IP packets that are encapsulated within other packets create “IP over IP.” Multicast IP packets (packets that have multicast destinations), carried between networks that support multicasting over intermediate networks that do not, are the most common implementation. Conferencing and other services that are offered through Multicast Backbone (MBONE) are examples.
- TCP - Transmission Control Protocol is a transport layer protocol in the TCP/IP protocol stack. This is a connection-oriented protocol that provides reliable full-duplex data transmission. Web browsers using HTTP and FTP are examples.
- UDP - User Datagram Protocol is a transport layer protocol in the UDP/IP protocol stack. UDP is a connectionless service that exchanges datagrams without acknowledgment or delivery guarantees, and therefore requires that error handling and retransmissions are handled by other protocols. DNS and WINS are examples.

Modify Protocol

Click the Modify button to the right of the Protocol field to edit the field.

TCP/UDP Source and Destination Ports

You can filter packets to or from the Source and Destination Ports. This would permit or deny any packets from being transferred by the switch based on the Source and Destination Ports.

The Source or Destination is relative to the direction of the rule.

Modify TCP/UDP Source & Destination Ports

Click the Modify button to the right of the TCP/UDP Source and Destination Port fields to edit either of these fields.

Current DSCP Value

The DSCP Value & Mask assignments allow packets that are already marked to retain their settings or to be remarked based on their previous DSCP value.

Modify DSCP Value

Click the Modify button to the right of the Current DSCP Value field to create and edit the DSCP value and mask.

DiffServ Marking

Select the DSCP to be marked on the next meter, either EF (Expedited Forwarding) or an AF (Assured Forwarding) level, that this rule applies to data.

QoS Interfaces

The QoS Interfaces screen provides information about the QoS settings for each physical interface. This screen also enables you to view statistical information for each interface and to edit the QoS settings for each individual interface.

Figure 89 QoS Interfaces screen

Current Interface

For each physical interface, such as a LAN, the QoS Interfaces screen provides information about its current QoS settings. Select the physical interface from the list and click screen to see the QoS settings for a particular interface.

The Interface QoS Statistics button lets you view operational statistics for the Current Interface.

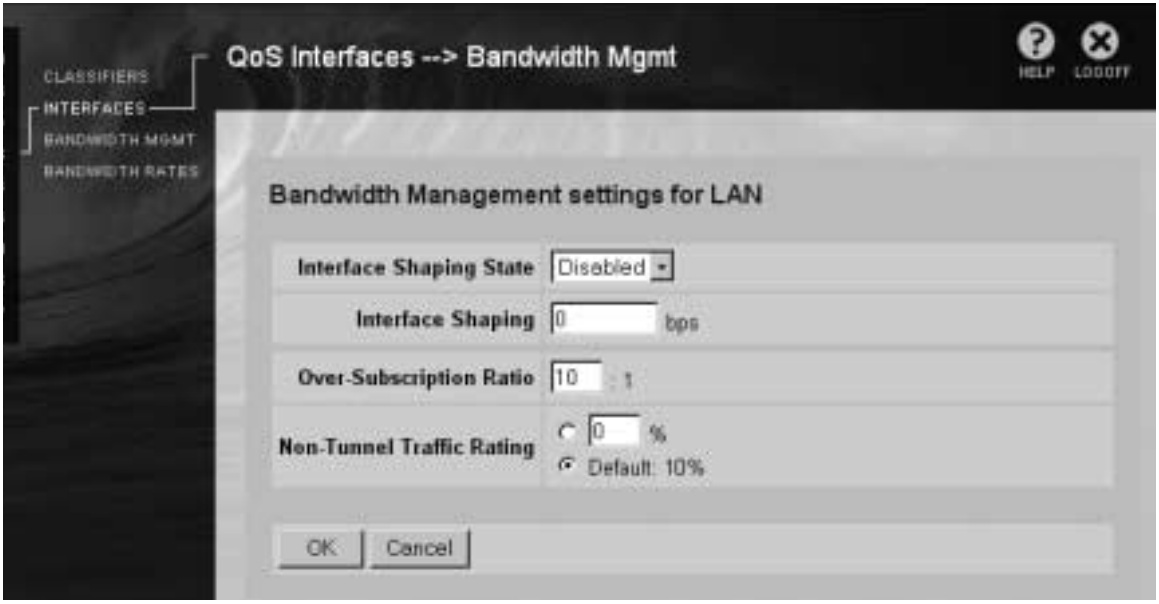
Bandwidth Management

The Bandwidth Management section of the QoS Interfaces screen shows the current Bandwidth Management settings for the selected physical interface. To change any of these settings, click the Configure button.

Configure

The Bandwidth Management screen appears when you click the Configure button. Use this screen to configure Bandwidth Management settings for the selected physical interface.

Figure 90 QoS Interfaces→Bandwidth Management→Configure



Interface Shaping State

Enable or disable Interface Shaping for this physical interface.

Interface Shaping

Enter a value, in bps, for Interface shaping. This value is used to shape (delay) the outgoing packet flow through an interface to better match the throughput of a downstream device. Non conforming traffic is delayed not dropped.

Over-Subscription Ratio

Configure for the interface how much of its bandwidth to over-subscribe. For example, for a value of 5 (5:1 Over-Subscription ratio) for a 1 Mb T1 interface, the switch allows connections up to 5 Mbit of total guaranteed bandwidth on the interface.

Non-Tunnel Traffic Rating

Enter a percentage of the total bandwidth to reserve for non-tunneled traffic on the selected interface. The default is 10 percent.

DiffServ Edge

The DiffServ Edge screen appears when you click the Configure button in the DiffServ section of the QoS Interfaces screen. Use this screen to configure DiffServ Edge settings for the selected physical interface.

Figure 91 QoS Interfaces→DiffServ→Configure

Multi-Field Classifier

Multi-Field Classifier State

Use the drop-down list box to enable or disable the application of MF Classifiers on this interface.

Ingress (Inbound) MF Classifiers

Select from the list of existing MF Classifiers the MF Classifier that you want to apply when packets are coming in from this interface.

Egress (Outbound) Classifiers

Select from the list of existing MF Classifiers the MF Classifier that you want to apply when packets are going out of this interface.

Traffic Conditioning

Use the list box to enable or disable Traffic Conditioning on this interface.

EF Shaping

Enter a value, in bps, for Expedited Forwarding (EF) Shaping. Shaping is a process of delaying the packets in a stream in order to conform to a defined traffic profile, in this case, the EF Shaping value. Nonconforming traffic is delayed, not dropped.

Traffic Conditioning Meter Settings

Traffic conditioning is the process of dropping and remarking a traffic stream in order to shape it into compliance with a traffic metering profile.

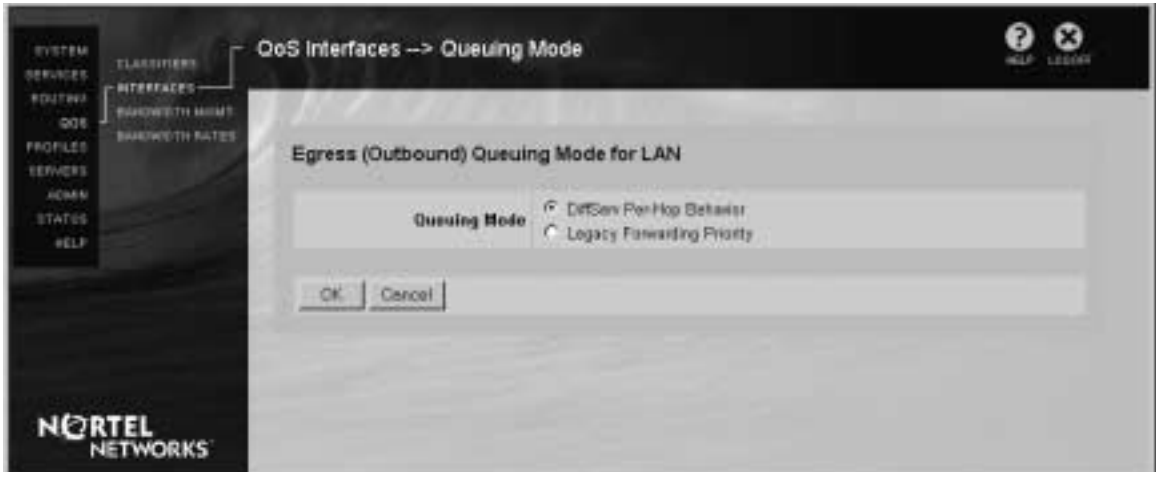
For Expedited Forwarding (EF) and Assured Forwarding 1, Assured Forwarding 4 (AF1-AF4), you can configure a Traffic Conditioning Meter (in bps). For EF, the rate is used as an average rate, though at times traffic can burst as much as twice the configured rate. Traffic below the rate is forwarded; traffic above the rate is dropped.

For AF1-AF4, any packets under the rate are marked as low drop precedence. Any packets under two times the configured rate are marked as medium drop precedence. Any packets above two times the configured rate are marked as high drop precedence.

Egress (Outbound) Queuing Mode

The Egress Queuing Mode screen appears when you click the Configure button in the DiffServ section of the QoS Interfaces screen. Use this screen to configure egress queuing mode settings for the selected physical interface.

Figure 92 QoS Interfaces→Egress Queuing Mode



Queuing Mode

Select the queuing mode for this interface, either DiffServ Per-Hop Behavior or Legacy Forwarding Priority.

Legacy Forwarding Priority provides backward compatibility for earlier versions of the switch.

Interface QoS Statistics

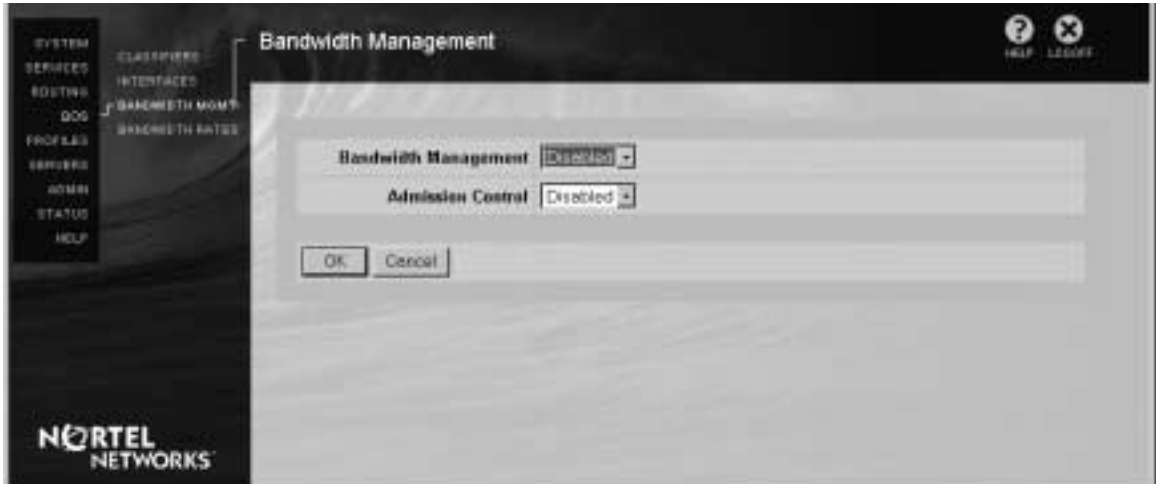
The Interface QoS Statistics button in the QoS Interfaces screen provides access to operational statistics for the interface.

Bandwidth Management

The switch's Bandwidth Management capabilities let you manage CPU and interface bandwidth resources to ensure that tunneled sessions get predictable and adequate levels of service. Bandwidth Management enables you to configure the switch resources for users, branch offices, and interface-routed traffic. Bandwidth components keep track of and control the level of bandwidth being used on the physical interfaces and the tunnels.

Bandwidth management is configured and managed from the QoS→Bandwidth Management screen.

Figure 93 QoS Bandwidth Management screen



Bandwidth Management

Bandwidth Management can be enabled or disabled system-wide by selecting the desired setting from the Bandwidth Management drop-down list box.

When enabled, Bandwidth settings apply.

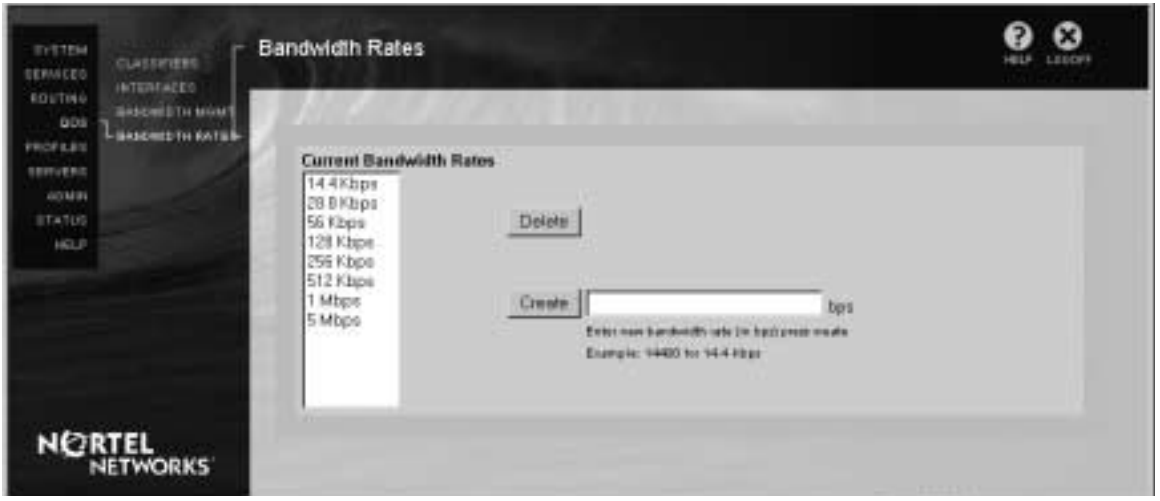
Admission Control

Admission control is a traffic control function that decides whether the switch can supply the requested bandwidth and CPU resources of a new session while continuing to provide the bandwidth and CPU resources requested by previously admitted sessions. Admission Control is used in conjunction with bandwidth policies to limit the number of concurrent user and branch tunnels.

Bandwidth Rates

The Bandwidth Rates screen allows you to manage available bandwidth rates.

Figure 94 Bandwidth Rates screen



Current Bandwidth Rates

The Current Bandwidth Rates list shows all existing bandwidth rates. You can delete an existing bandwidth rate or create a new bandwidth rate.

Delete

Select from the list of Current Bandwidth Rates and click delete to remove a bandwidth rate. A confirmation screen appears, prompting you to confirm that you really want to delete the selected bandwidth rate.

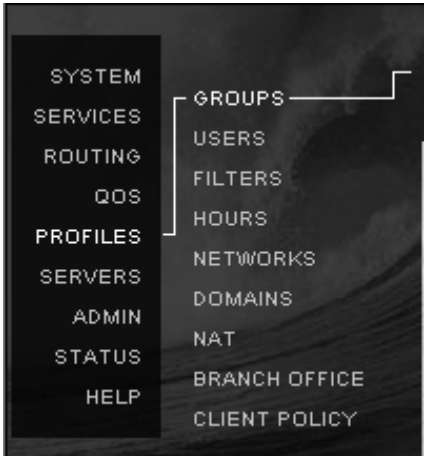
Create

Enter a bandwidth rate (in bits per second) and click Create to create a new bandwidth rate. The new bandwidth rate is added to the list of Current Bandwidth Rates.

Chapter 5
Profiles

The Profiles menu provides access to screens that allow you to configure such things as users, user groups, connections, and so forth.

Figure 95 Profiles menu



Groups

All remote users serviced by the switch are associated with a Group, which dictates the attributes that are assigned to a remote user session.

Groups are organized in a hierarchical manner. At the top of the hierarchy is the Base Group. The Base Group, which might be called “My Company,” contains the default characteristics that each new group inherits. Additional groups are added to the hierarchy as children of the Base Group.

The switch authenticates each user that attempts to connect to the switch by checking the User ID (UID) and Password against a database. The switch supports both LDAP and Remote Access Dial-In User Session (RADIUS) databases for authentication. When using LDAP for authentication, the user is always assigned to a group since LDAP also contains the user, group, and attribute information.

When authenticating a Point-to-Point Tunneling Protocol (PPTP) client against a RADIUS database, the group for a user requesting a session is returned from the RADIUS server as a RADIUS class attribute.

In addition to assigning users to groups and providing authentication access, other group characteristics that you can configure include:

- Access hours
- Call admission priority
- Forwarding priority
- Connectivity settings
- Filters
- RSVP
- Tunneling settings
- User attributes

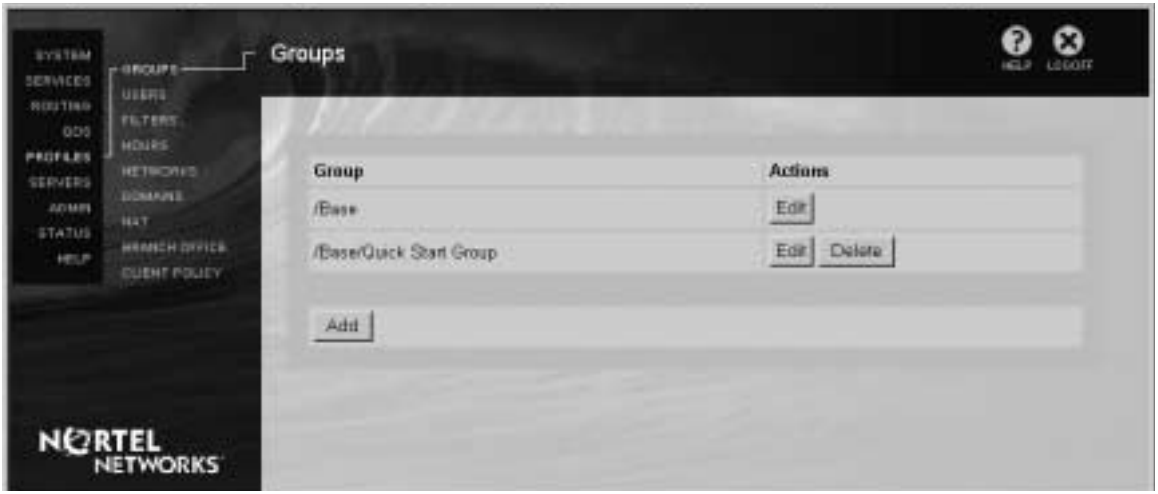
Maximum number of logins

The maximum number of logins is not enforced across tunnel types. If you set the number of simultaneous logins to 1, a client can still get another tunnel type connection if the client is configured to use multiple tunnel types. To limit the number of connections a client can have, configure the user for a single tunnel type.

Groups screen

The Groups screen provides access to all of the groups that you want to manage with the switch. The Groups screen allows you to change attributes that are specific to each group. Each attribute can be configured uniquely; otherwise, the attributes are automatically inherited from the parent group.

Figure 96 Groups screen



Group

This list box displays the current list of groups configured in the switch. You can Add, Edit, or Delete groups using this screen.

Actions

Edit

Click Edit beside the Group name that you want to modify. The Groups Edit screen appears.

Delete

Click Delete beside the Group name that you want to remove from the database. A delete confirmation requests that you verify the deletion.

Note: You cannot delete a group that has subgroups (children) associated with it. Nor can you delete the Base Group.

Add

Click to Add a group. The Groups Add screen appears.

Add Group screen

The Groups Add screen allows you to create a new group and associate it with a parent group.

Inherited Attributes

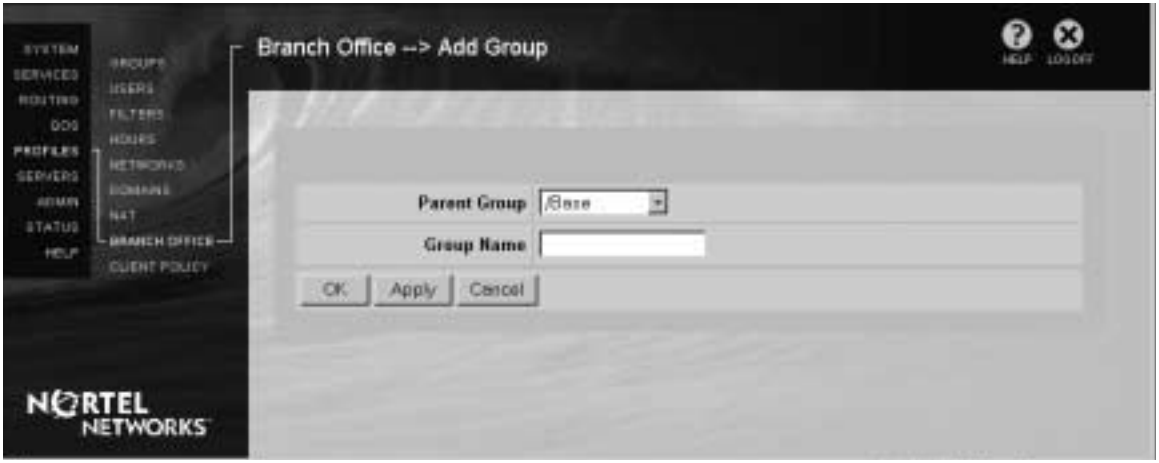
A group inherits attributes from its parent group. For example, if the Research and Development group attributes include All Access Hours and Allow Static Addresses but deny Client-Supplied addresses, PPTP and IPSec tunneling, then the New Products (child) group would inherit these attributes.

New Attributes

You must explicitly configure a group's unique attributes to override this inheritance. You can assign a group unique network access through packet filtering, attribute support for specific tunneling technologies, minimum encryption levels, authentication mechanisms, access hours, and more.

For example, you might want to set up an Administrator group for users who are allowed to manage the switch. This group could be configured to force tunnel connections that use encryption and strong forms of authentication, thereby improving the overall security of the switch.

Figure 97 Groups→Add



Group Name

Enter a group name of up to 64 characters (spaces are permitted); for example, Research and Development.

Parent Group

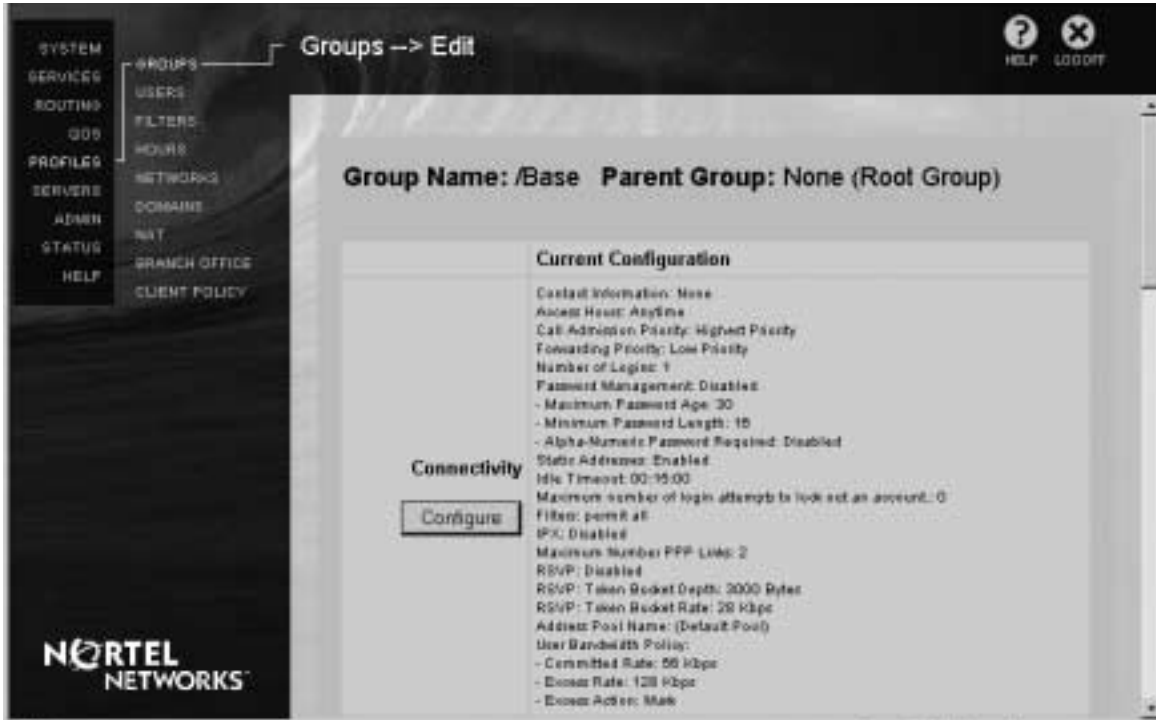
The new group is a child of the selected parent group. Therefore, the new group initially inherits the parent group's network access attributes, including authentication, tunnel types, filtering, and priorities (refer to "Edit Connection" for details). Once created, these inherited options can be overwritten for the new group. Only groups under which the user can create new groups, based on Administrator privileges, are shown.

Edit a group

The Groups Edit screen allows you to change group settings, including the main authentication, access, and connection priorities that define the group's profile.

Note: You can edit the attributes of a Group, but you cannot edit a Group name. To create a Group with the same attributes but a different name, you must add a new group and configure it with the desired attributes.

Figure 98 Profiles→Groups→Edit



Initial configuration

The group at the top of the hierarchy is known as the Base Group. The Base Group, due to its position in the hierarchy, contains the switch's default values and defines the first level of inheritance.

Note: A group inherits its attributes from its Parent Group by default. You can override the default values for any attribute in any group.

Configure

Click to select an option that is different from the Parent Group (the inherited configuration).

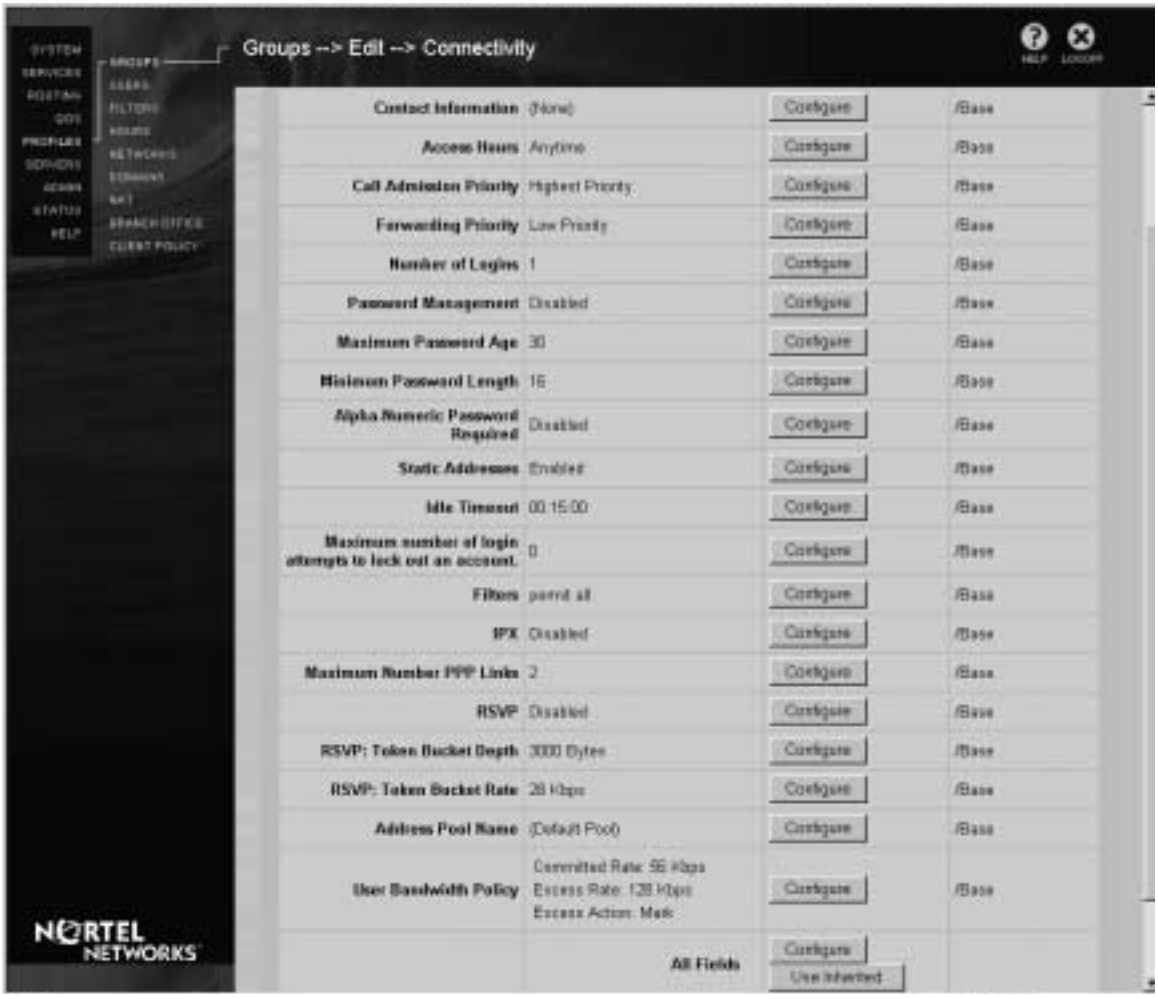
Current Configuration

The Current Configuration shows a summary of the Group's general and tunnel configurations. Details of these listings follow in the sections on Connectivity Settings, IPSec, PPTP, L2TP, and L2F.

Connectivity Settings

This screen allows you to configure Group settings. The Parent group values appear by default. Click the drop-down list boxes to change values.

Figure 99 Groups→Edit→Connectivity



Contact Information

Enter the name of someone who serves as the point of contact, typically the administrator.

Access Hours

Specify the time ranges during which access is allowed for users in this group. These time ranges are configured from the Profiles->Hours screen. The default value is Anytime.

Call Admission Priority

Specify the Call Admission Priority level (from low to highest) you want to permit for this group. Each level is assigned a percentage of the total number of calls allowed access to the switch. If there is a particularly high number of users logged in, new users could be denied call access, based on their Call Admission Priority, until existing callers disconnect.

Possible Call Admission Priority levels are:

- Highest Priority **(**default)
- High Priority
- Medium Priority
- Low Priority

Forwarding Priority

Specify the Forwarding Priority level (from low to highest) that you want to provide to sessions for users in this group. Forwarding Priority assures a certain level of latency and bandwidth allocation. For example, a group with the Highest Forwarding Priority has the highest possible bandwidth service and the lowest level of latency.

Conversely, if there is a particularly high level of traffic on the line, packets for a Low Priority group might be delayed or dropped. Since a Low Priority group has the least amount of bandwidth and the highest level of latency, some of its packets would wait until the higher priority level packets have been forwarded or they would be dropped.

Possible Forwarding Priority levels are:

- Highest Priority
- High Priority
- Medium Priority
- Low Priority (default)

Number of Logins

Click to specify the maximum number of simultaneous logins IPSec clients in the group are allowed.

Password Management

Click to enable the *Password Management facilities*, including Maximum Password Age, Minimum Password Length, and allow Alphabetic Passwords only.

Maximum Password Age

Enter the Maximum Password Age after which the login password expires. The Maximum Password Age range is from 0 (no password expiration) to 180 days (6 months). Default is 30 days. Users receive a warning that the password will expire each time they log in for two days prior to the expiration date. They also receive three warnings before access is denied.

Caution: If your clients are using a Microsoft Dial-Up Networking connection instead of the Nortel Networks Connection Manager, then they are not be notified of a password expiration or be given the opportunity to change the password prior to expiration. You should not use this feature unless you also plan to distribute the Connection Manager.

Minimum Password Length

Enter the Minimum Password Length, which can be from 3 to 16 alphanumeric characters. If you set the minimum length to eight characters, then the remote user must use at least eight characters as the login password. Default is 16 characters.

Alphanumeric Passwords

Click to enable this feature. This forces remote users to log in with a combination of alphabetic (A to Z) and numeric (1 to 9) characters. Nortel Networks does not recommend using all alphabetic characters because this makes it easier for hackers to decode. Default is Disabled.

Static Addresses

Click to Enable Static Addresses. A Static Address allows a user to always use a specific address when logging in to the switch. Since each user needs a unique address, the actual address is configured as part of the user profile. Disabling Static Addresses causes the switch to ignore configured addresses in the user profile for a given group. After the client-specified address, a Static Address is the second choice. If a remote user is using a static IP address as configured on the User's screen, then this user is limited to one login.

Idle Timeout

Enter an appropriate Idle Timeout in days, hours, minutes, and seconds format: dd:hh:mm:ss. The *Idle Timeout* is an amount of time a connection can be idle (no data has been transmitted or received through the connection for the specified amount of time). When the Idle Timeout expires, the session is terminated. This option helps prevent allocation of resources on the switch for sessions that are no longer active.

The default Idle Timeout is 00:15:00 minutes; the range is 00:00:00 to 23:59:59. The maximum number of days is 29. A setting of 00:00:00 specifies no Idle Timeout.

Note: All sessions check their configuration at startup time. Therefore, if you change the time of the idle timeout during a session, the change only affects new sessions and not any existing ones.

Filters

Select the filters you want from the pull-down list or use the default filters. The filters that appear in the drop-down list box are created using the Create Filter screen or have been supplied by Nortel Networks. Packet filtering controls the type of access allowed for users in a group, based on various parameters, including Protocol ID, Direction, IP addresses, Source, Port, and TCP Connection Establishment.

IPX

Click the drop-down list box to enable IPX support for the group.

Maximum Number PPP Links

The switch's Multilink PPP (MP) implementation allows tunneling multilink connections to the switch when the tunneling is being done by the ISP. Enter the Maximum Number of PPP Links that you want the switch to support. The range is 1 to 5; default is 1.

RSVP

Click to enable RSVP (Resource ReSerVation Protocol). The Nortel Networks RSVP implementation allows you to signal the network for required bandwidth. The client must be configured appropriately for RSVP to work. Additionally, only the controlled load-service is supported. This option is Disabled by default.

RSVP: Token Bucket Depth

The Token Bucket Depth influences packet flow delays within the switch and participating routers in the Internet. The largest amount of data the switch holds in its queue determines latency. New packets arriving are delayed by a time that is proportional to the amount of traffic that is ahead of them in the queue, which is no greater than the Token Bucket Depth. When the queue exceeds the Token Bucket Depth, incoming packets are dropped. To guarantee reduced latency, the Bucket Depths should be small. Typically, you should not change this setting. Default is 3000 bytes.

RSVP: Token Bucket Rate

The Token Bucket Rate is the highest long-term average data rate (in Kbps) required over time for the connection. It informs the switch and participating routers in the Internet how much bandwidth to reserve for the RSVP session. Typically, you should not change this setting. Default is 28 Kbps.

Address Pool Name

Click on the drop-down menu to select the Address Pools used by remote users to access this switch. The drop-down list shows all pools that have been defined on the switch. (Address pools are defined on the Servers→User IP Addr screen).

Select the New Address Pool link to define a new pool. Refer to "Remote User IP Address Pool" for details. This option is set to Default Pool by default.

User Bandwidth Policy

Click the Configure button in the User Bandwidth Policy section to modify bandwidth characteristics for this group. Click the Use Inherited button to apply the settings of the parent group to this group.

Committed Rate

Select a Committed Rate from the list of available bandwidth rates. If the desired bandwidth rate is not listed, click on Define new bandwidth rate to create a new one.

Excess Rate

Select an Excess Rate from the list.

Excess Action

Choose an Excess Action for traffic handling, either Drop or Mark.

IPSec Settings

Click the Configure button in the IPSec section to modify IPSec (Internet Protocol Security) characteristics for this group. The IPSec Edit screen appears.

The IPSec standard defines a set of security protocols that authenticate IP connections and add confidentiality and integrity to IP packets. IPSec packets are transparent to applications and the underlying network infrastructure. IPSec supports multiple encryption and authentication protocols so that your security policy can dictate levels of data privacy and authentication.

IPSec allows for multivendor interoperability. It uses a flexible key management scheme called the Internet Security Association Key Management Protocol (ISAKMP), which enables peer connections to quickly and dynamically agree on compatible security and connection parameters (keys, encryption, and authentication).

The following sections describe the fields that are unique to the IPSec screen. fields that are common to other tunneling types appear in the section "Common tunnel settings."

Note: Fields on the IPSec Edit screen that are preceded by an asterisk are proprietary features that apply to the Contivity VPN Client only. These fields are not used for non-Contivity clients.

Figure 100 IPSec Edit

Split Tunneling

All IPSec client traffic is tunneled through the switch by default. Split Tunneling allows you to configure specific network routes that are downloaded to the client. Only these network routes are then tunneled; any other traffic goes to the local PC interface. Split tunneling allows you to print locally, for example, even while you are tunneled into the switch.

Unauthorized Access Prevention and Split Tunnels

The switch takes precautions against unauthorized users potentially hacking tunneled information when the switch is operating in Split Tunnel mode. The primary precaution in this release is to drop packets that do not have the IP address that is assigned to the tunnel connection as its source address. For example, you establish a PPP dial-up connection to the Internet with an IP address of 192.168.21.3. When you start the tunneled connection to a switch, you are assigned a tunnel IP address of 192.192.192.192. Any packets that attempt to pass through the tunnel connection with a source IP address of 192.168.21.3 (or any address other than 192.192.192.192) are dropped. Furthermore, you can enable filters on the switch to limit the protocol types that can pass through a tunneled connection. To completely eliminate security risks, you should not use the Split Tunneling feature.

Split Tunnel Networks

Click to select one of the networks to which you want to send encrypted tunnel traffic only. These networks are designated from the Profiles→Networks screen.

Client Selection

The Client Selection feature enables you to configure your switch to accept tunnel connections from third-party clients, in addition to the Nortel Networks Contivity VPN Client. Refer to the Contivity VPN Release Notes for a list of supported third-party clients.

Configuring for Both Contivity and non-Contivity Clients

If you choose this selection, the switch provides support as described in the two previous sections, depending upon the type of client being used. For example, if you enable RADIUS Authentication, it is only used for Contivity clients, and you must have either preshared keys or RSA digital signature authentication enabled for non-Contivity clients.

Allowed Clients

Use the menu to specify the type of clients that are allowed to create tunnels to your switch.

Allow undefined networks for non-Contivity clients

Enabling this selection allows supported third-party clients to create IPSec tunnels to any internal networks. Nortel Networks recommends that you not allow undefined networks for third-party clients, and use Split Tunneling instead. This selection is ignored for Contivity clients.

Authentication

Authentication is performed with a protected User ID and Password through the ISAKMP key management protocol. When you click configure, the Group Security Credentials (RADIUS) dialog box appears.

Database Authentication (LDAP)

User Name and Password

Click to enable the LDAP User Name and Password to authenticate user identity. Authentication is performed with a protected User ID and Password through the ISAKMP key management protocol.

RSA Digital Signature

Click to enable the Entrust certificate authentication. You must then click the drop-down list box to choose a Default Server Certificate. Servers are configured from the System→Certificates screen.

RADIUS Authentication

The following attributes are associated with RADIUS Authentication when using IPSec tunneling. This is a two step process where (1) the switch authenticates the remote user with the User Name and Password authentication mechanism, AXENT or SecurID hardware or software tokens, and (2) the client uses the Group ID and Group Password to authenticate the switch's identity.

User Name and Password

Click to enable the RADIUS User Name and Password to authenticate user identity. Authentication is performed with a protected User ID and Password through the ISAKMP key management protocol.

AXENT Technologies Defender

Click to enable the AXENT OmniGuard/Defender challenge response token security authentication. The AXENT OmniGuard/Defender uses a personal identification number (PIN) and password, coupled with a challenge response security dialog, to authenticate user identity.

Security Dynamics SecurID

Click to enable the Security Dynamics SecurID token security authentication. The SecurID uses a PIN and the current code generated by a token assigned to the user to authenticate user identity.

Group ID and Password

Enter the Group ID and Password, which are encrypted for transmission.

Group ID

Enter the Group ID, which provides access to the switch. Subsequent LDAP and RADIUS authentication is verified against the User ID.

Note: The Group ID and User ID must not be the same.

Group Password

Enter the Group Password, which provides access to the switch. Subsequent LDAP and RADIUS authentication is verified against the User Password.

Group Confirm Password

Reenter the Group Password.

Encryption

Click Configure, then click the appropriate checkbox to either enable or disable the supported Encryption methods for this group.

Note: Using higher-level encryption, such as Triple DES, decreases performance.

The encryption methods are presented in order of strength, from strongest to weakest. All of the following encryption methods ensure that the packet came from the original source at the secure end of the tunnel. Some of the encryption types do not appear on non-US models that are restricted by US Domestic export laws. Also, MD5 (Message Digest) provides integrity that detects packet modifications.

ESP – Triple DES with MD5 Integrity: Encapsulated Security Payload Triple DES (Data Encryption Standard) uses the same principle as DES (below), but uses a 168-bit key. It uses the DES encryption algorithm three times. The first 56 bits of the key is used to encrypt the data, then the second 56 bits is used to decrypt the data. Finally, the data is encrypted once again with the third 56 bits, which triples the algorithm's complexity.

ESP – 40- or 56-bit DES with MD5 Integrity: Encapsulated Security Payload Data Encryption Standard (DES) is an encryption block cipher algorithm. DES uses a 40- or 56-bit key (with 8 bits of parity) over a 64-bit block. The 40 or 56 bits of the key are transformed and combined with a 64-bit message through a complex process of 16 steps.

Both 40- and 56-bit DES require the same processing demands, so you should use 56-bit DES unless local encryption laws prohibit doing so.

AH – Authentication Only (HMAC-SHA): The Authentication Header Message Authentication Code Secure Hash Algorithm (HMAC-SHA) produces a 160-bit hash. It is regarded by cryptographers as being more resistant to attacks than MD5. It does not encrypt data.

AH – Authentication Only (HMAC-MD5): The Authentication Header Message Authentication Code Message Digest 5 (HMAC-MD5) Algorithm is used to confirm the authenticity of a packet. It produces a 128-bit hash. It does not encrypt data.

If two devices have different encryption settings (due to either US export laws or administrative configuration), the two devices negotiate downward until each has a compatible encryption capability. For example, if a client in the US attempts to negotiate Triple DES encryption with a switch in Australia, then the Australian switch rejects Triple DES encryption in favor of DES.

IKE Encryption and Diffie-Hellman Group

Select the Diffie-Hellman Group level to apply to IKE (Internet Key Exchange) encryptions.

Note: The choice of the IKE encryption algorithm does not affect the choice of the encryption algorithm used to encrypt data in IPSec. For example, one can use DES to encrypt the IKE exchanges, and then negotiate Triple DES for use in IPSec.

The Services→IPSec screen contains a section labeled “IKE Encryption and Diffie-Hellman Group.” This section provides two choices for use with IPSec.

Perfect Forward Secrecy

Click to enable Perfect Forward Secrecy (PFS). With PFS, keys are not derived from previous keys. This ensures that one key being compromised cannot result in the compromise of subsequent keys.

Forced Logoff

For IPSec tunneling, you can specify a time after which all active users are automatically logged off. The default is 0, which means the option is turned off. The possible range is 00:00:01 to 23:59:59.

Client Auto Connect

The Client Auto Connect feature enables remote Contivity VPN Clients to connect their IPSec tunnel sessions in a single step. This is similar to the way Microsoft's Dial-Up Networking automatically connects to an ISP when a Web browser is launched. With Auto Connect, client users simply click on the desired destination, for example, a Web page on the private internal network. This first starts their dialup connection, then makes the tunnel connection to the switch, and finally makes the connection to the requested destination. What has, in the past, taken three distinct user operations is now accomplished by a single action.

Enabled

Click to enable the Client Auto Connect feature on the switch.

Any Network Traffic

Click on this selection to use the autoconnect feature for all client connection requests to authorized destinations. Now, when any network activity is detected on the user's workstation, a tunnel connection is automatically launched to the switch. In this manner, the Client Auto Connect feature works like Microsoft's Dial-Up Network Auto Dial feature.

Specify Networks and/or Domains

Click on this selection to limit autoconnection use to specific domains or networks. Specify the authorized domains or networks in the following two fields.

Domains

Use this selection to designate specific domains or hostnames that trigger the autoconnect feature. The domains that you specify must be configured on the Profiles→Domains page (refer to "Domains"). Select None if you want to limit the autoconnection feature to specific networks, which you specify in the following Networks field.

Networks

Use this selection to designate specific networks that trigger the autoconnect feature (the networks must be configured on the Profiles→Networks page). Select None if you do not want to designate any networks.

Banner

You can customize an enterprise login banner for the Contivity VPN Client by entering text into the space provided. This banner appears at the top of the IPSec client upon login.

Display Banner

Click to enable the banner and have it appear when a remote user logs into the switch.

Client Screen Saver Password Required

Setting this security feature forces the client to use a password in association with a screen saver. When enabled, if the user leaves the system and is connected to a tunnel, the system then gets locked out of the tunnel once the screen saver kicks in.

The end user would enable this feature from the Start→Settings→Control Panel→Display→Screen Saver Password Protected checkbox. Default is Disabled.

Client Screen Saver Activation Time

This setting is used together with the Client Screen Saver Password Required setting. It defines the maximum time (in minutes) before the client's screen saver is activated. The value on the Client PC can be changed from the Start→Settings→Control Panel→Display→Strengthener Wait list box. Default is 5 Minutes.

Client Fail-Over Tuning

Enabled

Check this box to enable client fail-over. Client fail-over uses small packets to check and maintain, or keep alive, the connection between the client and the switch.

Interval

In the Interval section, specify the time interval that the client waits between VPN activity checks.

Nortel Networks recommends a low interval when users are connecting via the client. You should use a higher setting for situations such as when a lease line is used and charges are based on traffic.

Maximum Number of Retransmissions

Specify the maximum number of retransmissions in this field. This is the number of times that the client re-transmits a keepalive packet to the switch to check for connectivity.

Allow Password Storage on Client

You can allow client systems to save the login password in its password list, or you can require that the remote user enters the password each time he requests authentication and access to an IPSec tunnel. Click Enable to allow client systems to save the login password.

Note: When using certificates, saving the password on the client is not allowed.

Compression

Click to enable Compression for IPSec tunneling. Refer to "Compression" for details.

Rekey Timeout

You should limit the lifetime of a single key used to encrypt data or else you compromise the effectiveness of a single session key. Use the Rekey Timeout setting to control how often new session keys are exchanged between a client and a server. You should set the Rekey Timeout setting to no less than 1 hour.

Default is 08:00:00 (8 hours); a setting of 00:00:00 disables the Rekey Timeout setting. The maximum setting is 23:59:59.

Rekey Data Count

You can choose to set a Rekey Data Count depending on how much data you expect to transmit via the tunnel with a single key. Default is 0 Kbytes; a setting of 0 disables the Rekey Data Count.

Domain Name

This setting enables you to specify the name of the domain that is used while an IPSec tunnel is connected. Specifying the domain name in this field ensures that domain lookup operations point to the correct domain. This is particularly important for clients that use Microsoft Outlook or Exchange, to ensure that the mail server is mapped to the correct domain.

When a tunnel is connected, the remote client's registry is updated to use the specified domain. When the client disconnects the tunnel, the remote client's original domain is again used.

Primary DNS

See "Primary DNS" in "Common tunnel settings."

Secondary DNS

See "Secondary DNS" in "Common tunnel settings."

Primary WINS

See "Primary WINS" in "Common tunnel settings."

Secondary WINS

See "Secondary WINS" in "Common tunnel settings."

Nortel Client Requirements

Minimum Version

Select the minimum version of Contivity VPN Client that is required.

Action

Specify the action to take upon detection of a noncompliant client.

Message

Type a message giving users the URL for a Web site or FTP site from which they can download the required version of the Contivity VPN Client software.

Filter

Select a filter to apply from the list of available filters.

New Filter

Click on the New Filter link to go to the screen and create a new filter.

Client Policy

Select a client policy as appropriate. Client Policy helps prevent potential security violations that could occur when you are using the split tunneling feature. Split tunneling allows client data to travel either through a tunnel to the enterprise network or directly to the Internet. Refer to "Client Policy" for additional information.

Allow IPSec Data Protection

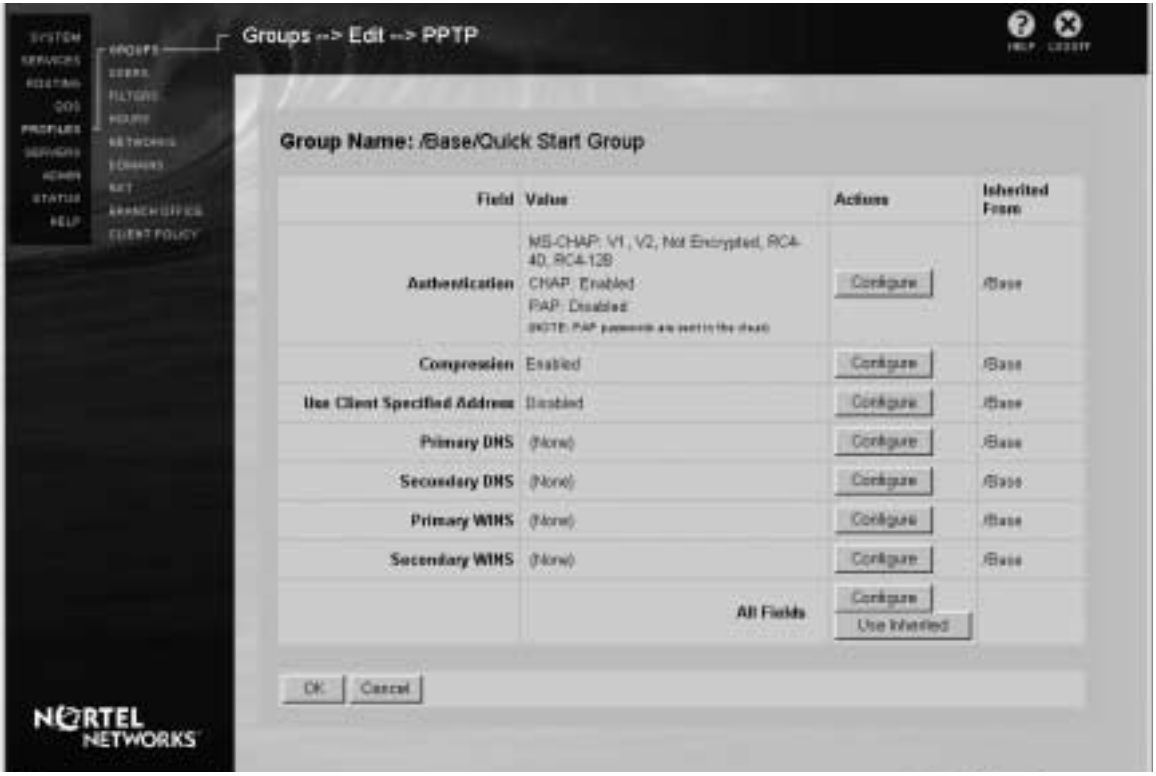
Enable or disable IPSec.

PPTP

Click to modify Point-to-Point Tunneling Protocol (PPTP) characteristics for this group. The PPTP Edit screen appears.

PPTP is a tunneling protocol supported by Nortel Networks, Microsoft, and other vendors. The PPTP client is available for Windows 95 (www.microsoft.com) and is built-in to Windows 98 and Windows NT. PPTP supports multiple authentication schemes: MS-CHAP, CHAP, or PAP. Additionally, you can enable compression, RC4-based encryption, and assign DNS and WINS servers to the tunnel. Refer to "Common tunnel settings" for additional information.

Figure 101 PPTP Edit



L2TP

Click to modify L2TP (Layer 2 Tunneling Protocol) characteristics for this group. The L2TP Edit screen appears.

L2TP is a tunneling protocol supported by Nortel Networks, Cisco Systems, Microsoft, and other vendors. L2TP combines the best features of the L2F and PPTP tunneling types. L2TP tunneling enables secure remote access to enterprise networks across the public Internet. L2TP tunnels are generally established between a network access server (NAS) at the Internet Service Provider (ISP) and the switch.

L2TP allows you to specify MS-CHAP, CHAP, or PAP authentication, enable compression, and assign DNS and WINS servers to the tunnel. The following sections are specific to L2TP over IPSec tunnels. Refer to “Common tunnel settings” for additional information about other settings.

L2TP/IPSec Data Protection

Select the level of protection to apply to the tunnel.

Require IPSec Transport Mode Connections

Specify the group from which this tunnel gets credentials.

Figure 102 L2TP Edit

L2F

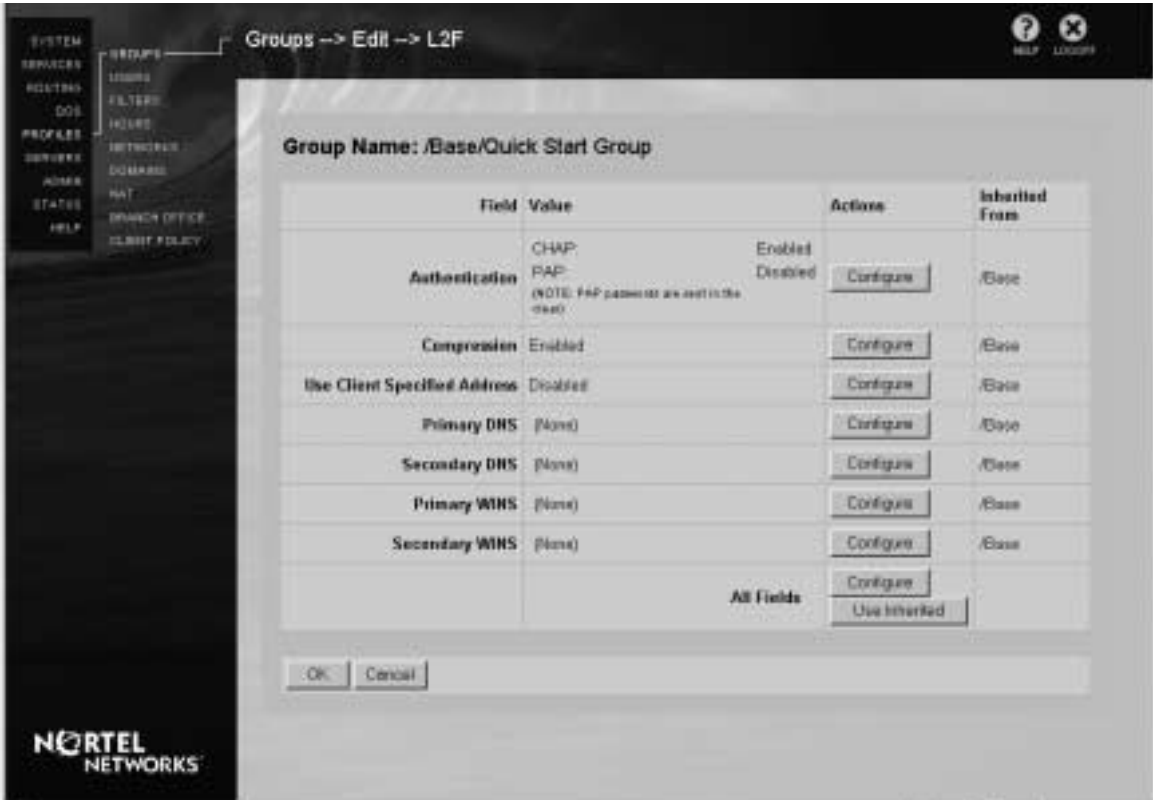
Click to modify L2F (Layer 2 Forwarding) characteristics for this group. The L2F Edit screen appears.

L2F is a tunneling protocol supported by Nortel Networks, Cisco, Shiva, and other vendors. L2F tunneling enables secure remote access to enterprise networks across the public Internet. L2F tunnels are generally established between a network access server (NAS) at the Internet Service Provider (ISP) and the switch.

L2F allows you to specify a CHAP or PAP authentication scheme, enable compression, and assign DNS and WINS servers to the tunnel.

Refer to "Common tunnel settings" for additional information.

Figure 103 L2F Edit



Common tunnel settings

Authentication

Select one or more of the PPTP/L2TP/L2F Authentication methods. These methods are Enabled by default.

- MS-CHAP – Click to enable Microsoft encrypted authentication for PPTP and L2TP only.

Windows NT, Windows 98, and Windows 95 clients can negotiate PPP connections using MS-CHAP as the authentication algorithm. This is the Microsoft version of CHAP; it is a secure form of authentication.

Associated with MS-CHAP authentication are the following optional encryption levels for preserving the privacy of tunneled traffic. These encryption levels are valid for PPTP tunnels only.

Data Encryption

Click to enable acceptable level(s) of data encryption for MS-CHAP.

- Not Encrypted– Tunnels requesting no data encryption are accepted.
- RC4-40 – Tunnels requesting 40-bit RC4 encryption are accepted.
- RC4-128 – Tunnels requesting 128-bit RC4 encryption are accepted. This is the most secure method. The longer the encryption key, the more secure the encryption. US export law controls the export of 128-bit encryption keys.

If two devices have different encryption settings (due to either US export laws or administrative configuration), the two devices negotiate downward until each has a compatible encryption capability. For example, if a client in the US attempts to negotiate RC4-128 encryption with a switch in Ireland, then the destination switch rejects RC4-128 encryption in favor of RC4-40.

Note: You can only use Microsoft Point-to-Point Encryption (MPPE) when using MS-CHAP authentication

- MS-CHAP Version 2 – Microsoft Challenge-Handshake Authentication Protocol Version 2 (MS-CHAP-2) is a Microsoft proprietary Point-to-Point authentication protocol that provides LAN-based users the same functionality as Version 1 and includes bidirectional authentication. Additionally, MS-CHAP-2 integrates the encryption and hashing algorithms used on Windows networks.
- CHAP – Click to enable Challenge Handshake Authentication Protocol (CHAP) encrypted password authentication. CHAP provides protection for passwords, but no data encryption.
- PAP – Click to enable Password Authentication Protocol (PAP) authentication. Neither the password nor the data is protected.

Compression

Click to enable the IPSec HI/fn LZS compression or the PPTP, L2TP, or L2F Microsoft Point-to-Point Compression (MPPC) packet compression. Compression should be used when encryption is selected on analog modems. This is because encryption renders a modem's compression ineffective, and it can severely affect the performance of compressible applications. Also, data that is compressed before being transmitted makes more efficient use of lower speed network links.

You should use data compression in most typical situations. Users with cable modems or *x*DSL connections to the ISP, or locally on the LAN, would find it is probably unnecessary to compress packets. This is because the speed of the link, relative to the rate of compression and the benefit of compressing before encrypting, might be negligible or might not increase performance.

Also, some data cannot be compressed; for example, a previously compressed file does not lend itself well to additional compression.

Use Client-Specified Address

Click to enable use of a Client-Specified Address. This option allows the switch to accept the IP address from a remote user's system during tunnel setup. This option is Disabled by default.

When enabled and the client provides an IP address, this is the IP address that is used by the client for the duration of the tunneled session (it becomes the first or default choice).

Common DNS and WINS server fields

The following DNS and WINS server fields are common to all tunnel types.

Primary DNS

Enter the address of the Primary Domain Name System (DNS) server that is located on your private network. This DNS address is provided by the server to tunnel clients at setup and is used through the tunnel. The DNS server translates textual host names into IP addresses for the switch. For example, DNS can translate the fully qualified host www.mycompany.com to its IP address 192.19.2.33.

The Primary DNS server is the first one addressed for servicing name resolution requests from a remote user; if the Primary DNS server is unavailable, service is requested of the Secondary DNS server. Recent versions of Microsoft Windows operating systems can simultaneously query multiple DNS servers.

Always use the IP address for setting a DNS server host instead of a domain name.

Secondary DNS

Enter an address for the Secondary Domain Name System (DNS) server. If the Primary DNS server is unavailable, service is requested of the Secondary DNS server.

Primary WINS

Enter an address for the primary Windows Internet Naming Service (WINS) server. A WINS server resolves NetBIOS names (for Windows networking file and print services) to IP addresses. Using a WINS server enables normal Windows file and print services to be accessed correctly through a tunnel connection.

Windows NT Server Version 4.0 and later supports a built-in WINS server. The WINS server eliminates the need to manually map NetBIOS names to IP addresses (for example, using the textual LMHOSTS file on Windows) by updating a name-to-address mapping file dynamically on the WINS server.

The Primary WINS server is the first one addressed for servicing name resolution requests from a remote user; if the Primary WINS server is unavailable, service is requested of the Secondary WINS server. Always use the IP address for setting a WINS server host instead of a name.

Note: If no WINS servers are specified, the client is forced to broadcast for NetBIOS names.

Secondary WINS

Enter an address for the Secondary Windows Internet Naming Service (WINS) server; if the Primary WINS server is unavailable, service is requested of the Secondary WINS server.

User Management

The User Management screen allows you to add, edit, delete, or search for a user profile in a group.

Figure 104 User Management Group Profile

Group

Select a Group to which you want to add or modify users from among those in the Group drop-down list box. If you need to add a new group, select Profiles→Groups.

Display

After selecting a Group, you must click Display to view the group members. This allows you to quickly change from viewing one group to another.

Search

The Search option allows you to readily search within a selected group and then configure a specific user's account.

Select a Group from which you want to search for a particular user from the Group drop-down list box (at the top of the screen), and click Display. The search is limited to the available groups. Select one of the following as the preferred search method, then click Search.

- Last Name searches for a Last Name. You must enter the entire last name.
- UID searches for a User ID.
- Admin Rights searches for anyone who has View or Manage Administrator privileges.
- LDAP search allows you to enter any LDAP database attribute that is part of the person, organizational Person, or inetOrgPerson object database (for example, cn=common name or sn=surname) to generate the associated user's profile. Refer to your LDAP vendor's documentation for complete details.

Last/First

The Last names and First names of the selected group's users appear, sorted by Last name.

Actions

Edit – Click to Edit a User Profile in the Group; the Edit User screen appears.

Delete – Click to Delete a User from the Group.

Add User

Click to Add a User to the Group; the Add User screen appears.

User Add or Edit

This screen allows you to Add or Edit a User profile. A *user profile* includes User IDs (UIDs) and passwords for the various tunneling protocols, and the assignment of Administrative rights. This screen also allows for the configuration of an IP address that is always associated with the remote user.

Note: You should not add user profiles for RADIUS authenticated users. Instead, ensure that the proper User IDs and Passwords are in the external RADIUS database.

The switch always queries the LDAP database first, and if a UID and Password combination is found it uses this rather than an external RADIUS authentication server.

Only options that are enabled for the specified group appear on this screen. Furthermore, only options that the administrator who is currently viewing the screen has rights to appear (configuration options only appear if the administrator has Manage Users and Manage Switch Administrator Rights).

Figure 105 User Add/Edit

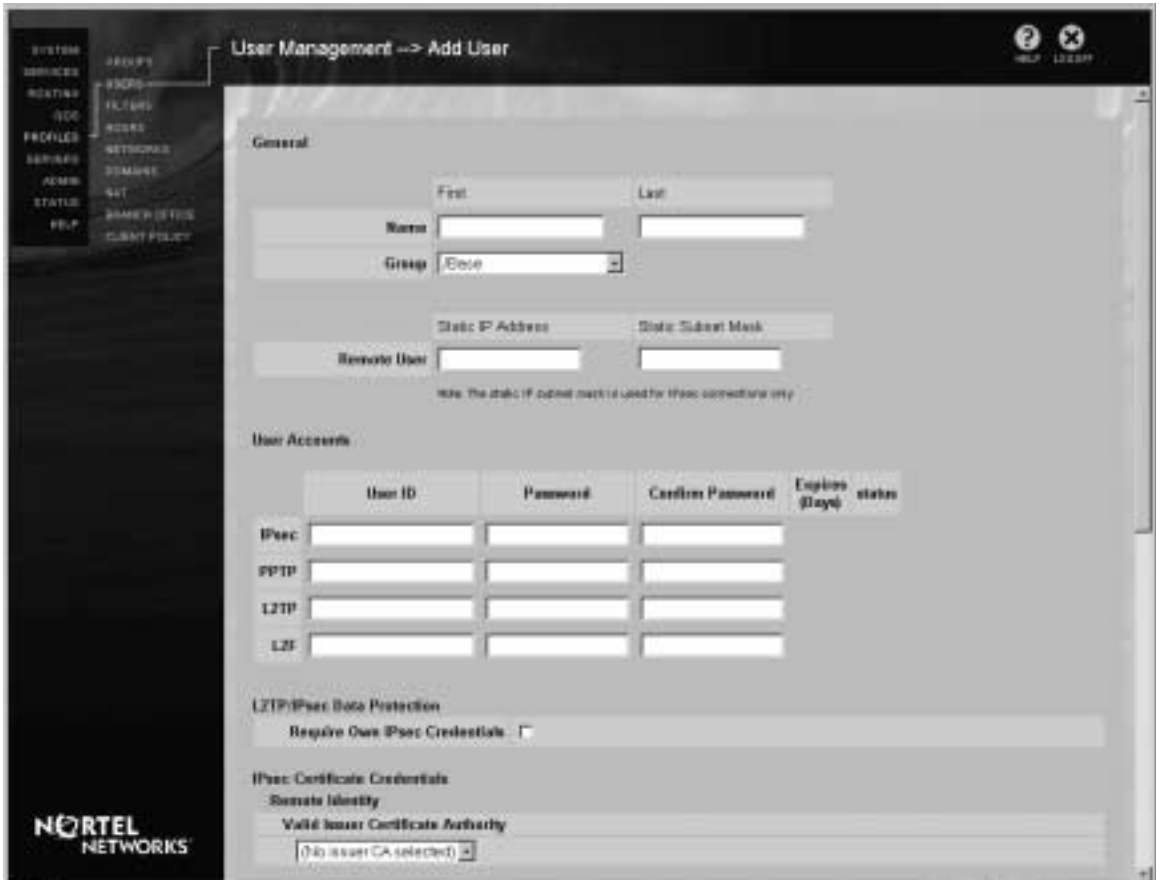
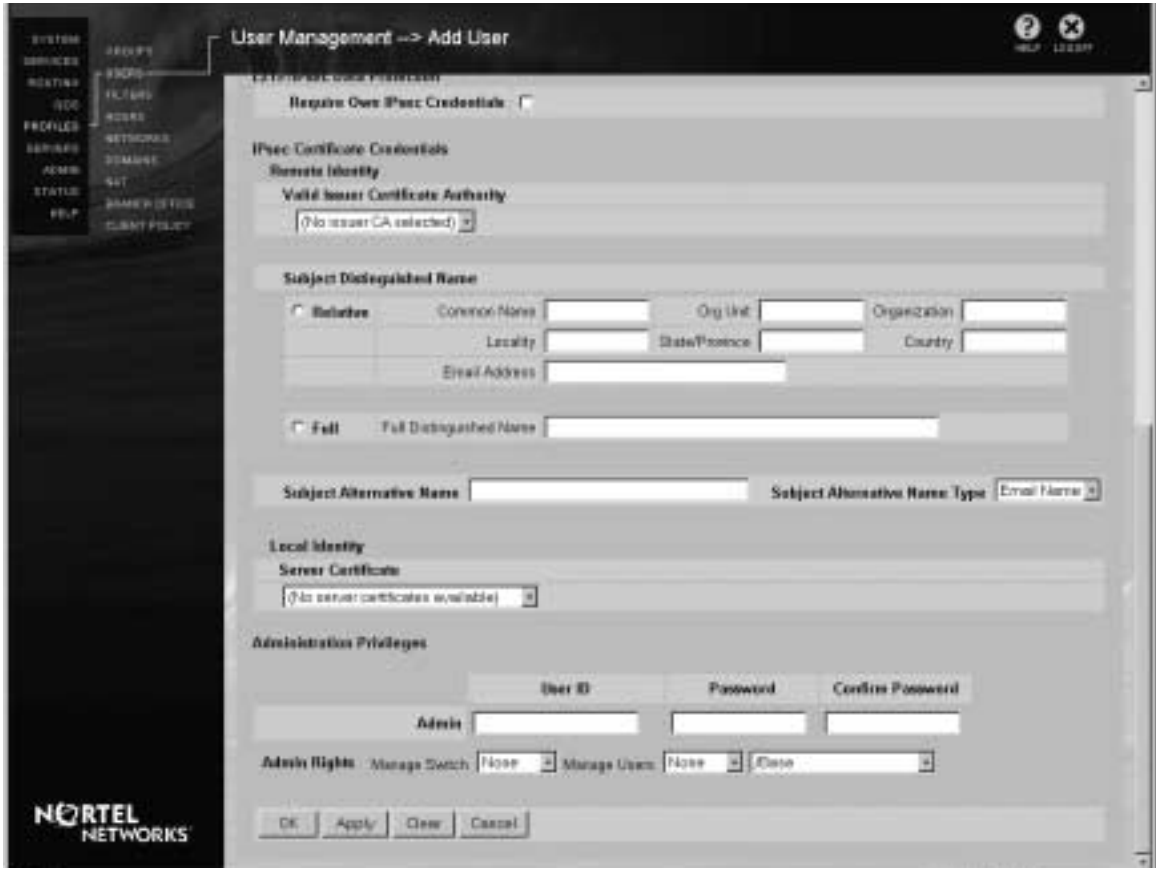


Figure 106 User Add/Edit - continued



You can assign a user to two different groups, but only if the user has two different User IDs (UIDs); for example, mlee and madilee. The system does not allow you to enter the same User ID in two different groups.

Note: When adding a user account, depending on the group configuration, the account can have up to four User IDs. If you are creating an enterprise User ID standard, you should try to avoid schemes that might potentially create conflicts as your company grows. For example, you should not use the person's full first name and last initial.

Name

Enter the First and Last Name of the user whose profile you want to add or change. This is the regular name associated with a person (for example, Mario Lemieux). This user can have different IDs and passwords for each tunnel type.

Group

Shows the Group to which the user belongs and its Parent group. You can move the user to a another Group by selecting a different Group name.

Remote User

Static IP Address

Enter a Remote User Static IP Address to use in place of a pool (client-specified or DHCP) server-assigned IP address. This IP address is associated with the Static IP Address option in the Groups→Connectivity option (it is only used if the group allows it).

Note: If an IP address that is entered here is used instead of a DHCP server-assigned IP address, *then only one login is allowed*.

Static Subnet Mask

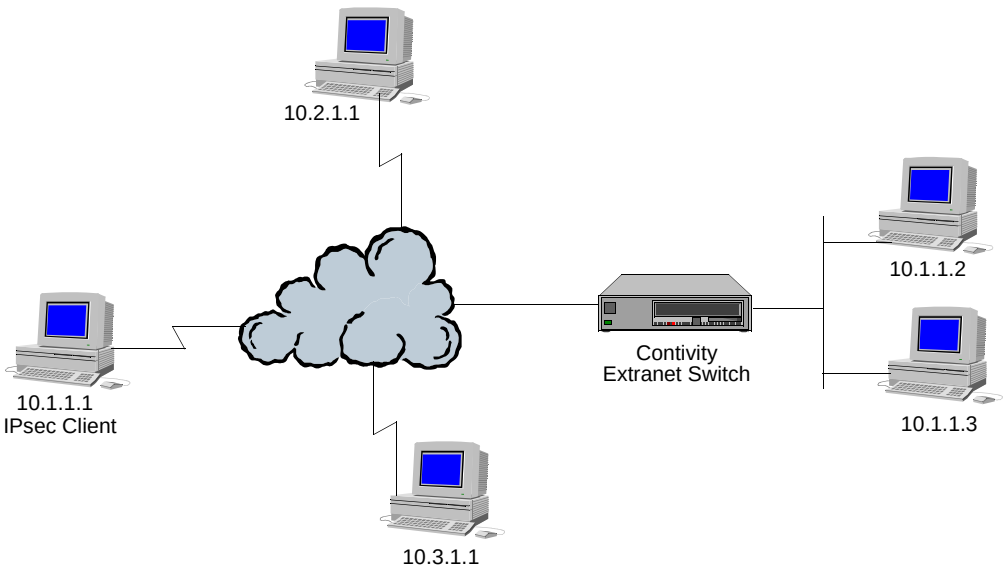
Assigning the correct subnet mask to a remote IPSec client is important when using Split Tunneling. When Split Tunneling is enabled, packets destined to a host listed in the Split Tunnel Network list are directed into the tunnel by the IPSec client. All other traffic goes through a standard LAN or dialup interface. This happens on the client by adding the routes listed on the Split Tunnel Network list to the route table of the Microsoft TCP/IP stack and pointing those routes to the tunnel adapter interface. A route is also added to the route table based on the subnet mask assigned to the tunnel adaptor.

Previously, there was no method to specify the subnet mask to be used on the client, so the client used the natural mask based on the class of the assigned IP address. For example, if the tunnel adaptor is assigned the address 10.1.1.1, the natural mask would be a Class A mask of 255.0.0.0. This would cause a rogue for 10.0.0.0 with a mask of 255.0.0.0 to be added to the route table and all packet destined to any address in the 10 network address space would be directed into the tunnel incorrectly.

The IPSec Subnet Mask field allows you to specifically assign a subnet mask to a remote IPSec client that obtains an IP address either from the IP Address Pool, DHCP, RADIUS, or a static user configuration.

The following illustration helps understand the specified address mask.

Figure 107 IPSec Subnet Mask Assignment



If the IPSec client established a connection and was assigned the IP address 10.1.1.1 using the natural mask, a route would be added from 10.0.0.0 with a mask of 255.0.0.0 to the TCP/IP stack's route table. If the client wanted to send data to 10.1.1.2 on the remote corporate network, the packets would be directed to the tunnel adaptor correctly. But if one client wanted to send data to 10.2.1.1,

which is directly accessible on the Internet, the packet would be directed into the tunnel incorrectly. By configuring a subnet mask of 255.255.0.0, a packet destined for the 10.2.1.1 network would not be directed into the tunnel and would be access directly.

User Accounts

You can establish user accounts for remote users to tunnel into the switch through specific tunneling types, as configured here.

IPSec

Enter the User ID and Password to allow IPSec (IP security) access privileges for this user. Note that the User ID for IPSec accounts is typically, though not required to be, a fully qualified domain name (FQDN); for example, pfassenphepher@penguins.com. LDAP is the only authentication server that currently supports IPSec.

PPTP

Enter the User ID and Password to allow PPTP (Point-to-Point Tunneling Protocol) access privileges for this user if you are not externally authenticating the user; otherwise, use external Authentication.

L2TP

Enter the User ID and Password to allow L2TP (Layer 2 Tunneling Protocol) access privileges for this user if you are not externally authenticating the user; otherwise, use external Authentication.

L2F

Enter the User ID including the domain (for example, npapalapagous@company.com) and Password to allow L2F (Layer 2 Forwarding) access privileges for this user if you are not externally authenticating the user; otherwise, use external Authentication.

Expires (Days)

Shows the number of days remaining before the password expires. When the field says Now, then the password has already expired. You must therefore reset the Maximum Password Age setting for this user. When the field says Never, then the Maximum Password Age setting is 0, which means to never age (expire). Refer to "Maximum Password Age" for additional information on the Maximum Password Age option.

Status

If the account is locked, the enable check box appears, allowing the administrator to check it to unlock the account.

IPSec Certificate Credentials

Remote Identity

Valid Issuer Certificate Authority

Select a Valid Issuer Certificate Authority from the drop-down list. These Certificate Authorities are configured from the System→Certificates: Generate Certificate Request screen.

Subject Distinguished Name

You can use either the relative distinguished name or the full distinguished name.

Relative

The relative distinguished name is a collection of the following components that uniquely identify the remote peer in an IPSec certificate environment.

Organization

Enter the Organization with which the user is associated.

Organizational Unit

Enter the Organizational Unit with which the user is associated.

Common Name

Enter the Common Name with which the user is associated.

Country

Enter the Country in which the user resides.

State/Province

Enter the State/Province in which the user resides.

Locality

Enter the Locality in which the user resides.

Full

You can directly enter the Full Distinguished Name (FDN) in this field rather than entering the individual components in the previously described Relative distinguished name fields. A sample entry follows:

```
CN=MySwitch, O=MyCompany, C=US
```

Subject Alternative Name

You can optionally use a Subject Alternative Name in place of a Subject DN, and specify the format of the name. The following formats are acceptable.

- Email Name (for example, net_admin@company.com)
- DNS Name (for example, gateway.cleveland.company.com)
- IP Address (for example, 192.168.34.21)

Local Identity

Server Certificate

Click the drop-down list box to view all certificates that have been issued to the server. Server Certificates are configured from the System→Certificates: Generate Certificate Request screen.

Administration Privileges

Administrator privileges are assigned to users in charge of configuring, monitoring, and managing the switch. Enter the User ID and Password to allow this person Administrator Rights (and reenter the password to verify that you typed the password you intended).

Admin Rights

There are three types of Administrator access rights: Manage Switch, Manage Users and Add Subgroups. In addition to providing different levels of access rights, the Admin Rights settings also control which status reports you can view (see the section "Status Reports" for the types of reports).

The Manage Switch and Manage Users access right settings can be assigned one of the following privilege levels:

- None - This user does not have Administrator rights to Manage the Switch or Manage Users; the user cannot view or manage switch configuration or user settings.
- View - This user has Administrator rights to view (monitor) Switch Configuration or User Rights settings; however, the User cannot Manage (change) them. This is the lowest level of Administrator Rights.
- Manage - This user has Administrator rights to View (monitor) and Manage (configure) other Switch Configuration or User Rights settings. This is the highest level of Administrative Rights.
- Add Subgroups is a check box that lets you give the user the authority to add and delete subgroups under the given directory when the user only has View authority with Manage Switch access rights.

Manage Switch

This setting allows you to manage the switch completely, including groups, servers, control settings, and encryption levels. However, to manage users, *you must also enable the Manage Users setting for this user.*

Manage Users

This setting allows you to manage users, which allows you to add, delete, or edit User records.

Add Subgroups

This setting allows you to manage subgroups, which allows you to add, delete, or edit subgroups under the pre-configured groups.

Filters

The Filters screen allows you to Create, Modify, Copy, or Delete a Filter. You use this screen to manage your switch's tunnel filters (for user groups) or interface filters (for LAN and WAN interfaces).

Figure 108 Filters

Changing a tunnel filter does not affect any existing tunnels. You must reestablish the existing tunnels for changes to take effect.

Current Filters

The Current Tunnel Filters and Current Interface Filters windows show the currently available filters. A filter usually consists of one or more inbound rules (coming into the enterprise) and one or more outbound rules (leaving the enterprise). Filter names are a convenient way of managing a set of rules.

To perform any of the following operations, click on the filter in the Current Filters window, then click on the appropriate button.

Edit

Click the filter that you want to modify, then click the associated Edit button. The Filter Rules for that filter appear.

Delete

Click the filter that you no longer intend to use, then click the associated Delete button. The name is removed from the list. You cannot delete a filter that is currently in use.

Create

Enter the new filter name and click the associated Create button. The Edit Filter screen appears.

Copy Filter

Use the Copy Filter buttons to copy an existing filter from one filter set to the other. For example, if you have already created a filter for tunnels, you can copy it for use by your switch's interfaces.

Note: If you plan to use a filter for both tunnels and interfaces, it must appear in both windows on the Filters screen.

To copy a filter, click on the existing filter in one Current Filters window, then click the appropriate Up or Down button to move the filter to the other Current Filters window. The Copy Filters screen appears, asking you to confirm that you want to copy the filter.

Figure 109 Copy Filters

You can also rename the filter before you copy it.

Note: Additional set up steps might be required if you copy a tunnel filter for use by a Contivity Firewall. This is because the traffic that uses the Contivity Firewall traverses two of the switch's interfaces (for example it might enter via a public interface and exit through a private interface). On the other hand, tunnel traffic only enters and exits through a single physical interface.

Edit Filter

This screen allows you to add, Edit, Delete, or alter the ordering of Filter Rules by moving them up or down in the rules priority list. If you are editing a tunnel filter, you can also enable or disable HTTP, SNMP, FTP, Telnet, or PING through a tunnel as part of this filter.

Note: The Allow Management Traffic portion of this screen does not appear for Interface Filters.

Filter Set

The name of the filter that you are currently editing.

Rules in Set

Lists the rules that are already contained in the filter that you are editing.

<< (Add Rule)

Click on a rule from the Available Rules list on the right of the screen, then click on the left arrow to add the rule. This adds the selected rule to the current rules list. The new rule is added after the rule currently selected in the Rules in Set list.

>> (Remove Rule)

Click on a rule, then click the right arrow to remove or delete it from the Rules in Set list.

^ (Move Up)

Click on a rule in the Rules in Set list, then click the up arrow to move the rule up one place in the list.

v (Move Down)

Click on a rule in the Rules in Set list, then click the down arrow to move the rule down one place in the list.

Available Rules

This field lists all of the rules that are available on the switch to add to the filter. They appear in the format of:

`Name: Rule String (according to the Cisco format)`

Manage Rules

Click to view the Current Rules screen, from which you can Create, Edit, Copy, or Delete a Rule.

Allow Management Traffic

Note: The Allow Management Traffic section applies only to tunnel filters, and does not appear on the screens for interface filters.

By manipulating these options, you can restrict management access to the switch through tunnels. Each filter set has an explicit list of management services. By specifying the management services allowed through a tunnel, you can control which groups of users are able to perform different management tasks while tunneled into the switch.

The switch's default filter is Permit All, and the settings for this filter are to allow HTTP, SNMP, and PING. But if you create a new filter, all Management Traffic settings are disabled by default.

The management protocols are broken into two groups. The Local Services selections refer to services that reside on the switch. The Remote Servers selections refer to services that reside on other systems that are used by the switch. When enabled, network traffic for these services is allowed through tunnels.

The management services apply to user and branch office connections. These options do not affect HTTP, SNMP, FTP, Telnet, or PING protocol traffic that is passing through the switch outside a tunnel.

For these Local Services

HTTP

Enable or disable access to the Web server on the switch.

SNMP

Enable or disable SNMP “gets” to the switch.

FTP

Enable or disable FTP “puts” or “gets” to the switch.

Telnet

Enable or disable Telnet access to the switch.

PING

Enable or disable PING access to the switch.

RADIUS

Enable or disable access to the switch’s RADIUS authentication service.

FIREWALL

Enable or disable Check Point FireWall-1 management traffic. When enabled, Check Point Management stations can communicate via a tunnel with the switch’s integrated Check Point FireWall-1.

For these Remote Servers

The Remote Servers options restrict traffic to external services that are required by the switch. By specifying these services, you can restrict which tunnels on a switch can send protocol traffic for external services it requires.

FTP

Enable or disable FTP access from the switch to external FTP servers on the other end of a tunnel. The FTP back-up and FTP upgrades facilities are examples of external services that are controlled by this option.

DHCP

Enable or disable access to dynamic host configuration protocol (DHCP) servers from the switch.

RADIUS

Enable or disable the switch's ability to access a remote RADIUS server.

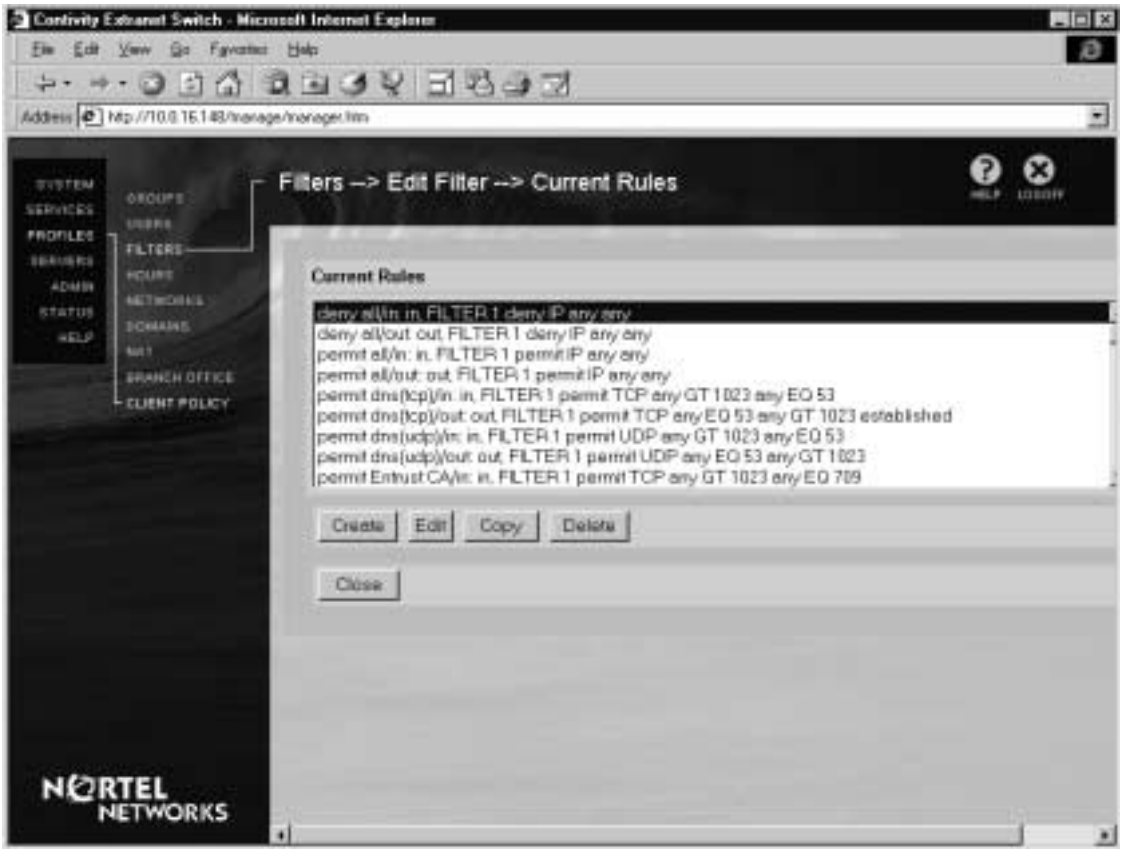
DNS

Enable or disable remote users from using the Domain Name Server (DNS) service for the switch.

Manage Rules

Click Manage Rules to view the current rules that you can manage.

Figure 110 Manage Rules



Create

Click to create a new Rule. The Rule Definition screen appears.

Edit

Click on a rule then click Edit to modify it (refer to "Edit Filter" for details).

Copy

Click on a rule then click copy to create a copy of the rule.

Delete

Click on a rule, then click Delete to remove it from the list of possible filter rules. You are prompted to confirm the rule deletion.

If the rule is contained in any filters, the deletion screen prompt informs you of how many filters are affected by the rule's deletion.

Creating, editing, and copying a filter rule

The Create Filter Rule Definition, the Edit Filter Rule Definition, and Copy Filter Rule Definition screens are similar and therefore the field descriptions are presented together in this section.

Figure 111 Create Filters Rule Definition

Figure 112 Edit Filter Rule Definition

Rule Name or Filter Rule For

Create a Rule Name or show the Rule that you intend to modify. The last rule of a filter by default is always Deny any packet. Therefore, build your filter groups by first permitting the services that you want to allow into or out of the switch. Deny any packet does not appear in the rules list. For efficiency, you might want to add a Deny rule earlier in the rules sequence so that an unwanted packet is dropped before processing all rules in a filter.

Filter Action

The Filter Action determines the switch's action when a packet matches the rule.

Permit

Click Permit to allow such packets.

Deny

Click Deny to drop such packets.

Direction

You can filter packets from either the Inbound or Outbound direction.

For tunnel filters, the direction setting is relative to the switch. For example, if Outbound is selected, packets from the switch headed in the Outbound direction would be filtered (into the tunnel, which is typically out to the Public network).

For interface filters, the direction setting is relative to the interface that the filter is applied to. For example, if Outbound is selected, and the interface filter is applied to a private interface, then packets heading out to the private network from the interface would be filtered.

Inbound

The filter is applied to Inbound packets. For tunnel filters, Inbound is from the Public Data Network (PDN) to the Private network. For interface filters, Inbound is traffic that is received by the interface.

Outbound

The filter is applied to Outbound packets. For tunnel filters, Outbound is from the Private network to the Public Data Network (PDN). For interface filters, Outbound is traffic that is transmitted by the interface.

Address

You can filter packets to or from a given Inbound or Outbound Address. Either select the existing address from the drop-down list box, or click Modify to create a new address and mask, or delete an existing address and mask. Refer to “Current Addresses” for additional information.

The Address is always an enterprise (private) address: for inbound filters, it is a destination address; for outbound filters it is a source address.You might want to create a rule to permit traffic outbound to all addresses.

Protocol

- Click the drop-down list box to select the appropriate Protocol. To add, edit, or delete Protocols that you want to filter, click Modify. Refer to "Current Protocols" for additional information. The default list follows:
- ICMP -- Internet Control Message Protocol is a Network protocol layer. The PING utility generates ICMP packets. PING is often used to see if a system's network is available.
- IP -- Internet Protocol is a Network layer protocol in the TCP/IP stack that offers a connectionless internetwork service. IP packets that are encapsulated within other packets create "IP over IP." Multicast IP packets (packets that have multicast destinations), carried between networks that support multicasting over intermediate networks that do not, are the most common implementation. Conferencing and other services that are offered through Multicast Backbone (MBONE) are examples.
- TCP -- Transmission Control Protocol is a transport layer protocol in the TCP /IP protocol stack. This is a connection-oriented protocol that provides reliable full-duplex data transmission. Web browsers using HTTP and FTP are examples.
- UDP -- User Datagram Protocol is a transport layer protocol in the UDP/IP protocol stack. UDP is a connectionless service that exchanges datagrams without acknowledgment or delivery guarantees, and therefore requires that error handling and retransmissions are handled by other protocols. DNS and WINS are examples.

Source and Destination Ports

You can filter packets to or from the Source and Destination Ports. This would permit or deny any packets from being transferred by the switch based on the Source and Destination Ports. If the port matches any of the following variables, then the configured action is taken.

For example, if a packet's Source Port Equals that in the Filter rule, and the rule is to deny packets from that Source Port from entering the switch, then the packet is dropped. The Source or Destination is relative to the direction of the rule.

- Equal
- Not equal
- Greater than
- Less than
- GT (greater than) or equal
- LT (less than) or equal

The most common source and destination ports in use are available in an alphabetical drop-down list box. Select the appropriate port for your filter rule. To add, edit, or delete ports that you want to filter, click Modify. Refer to "Create or Edit Port" for additional information.

TCP Connection

The TCP Connection setting is used only when the protocol is TCP. This can be useful when setting up rules if you need to identify whether the packet is initiating a TCP connection.

The TCP Connection establishment (ACK bit) allows you to configure a filter rule that does not permit internal systems to establish connections with tunneled hosts. It does, however, permit tunneled hosts to establish connections with internal servers. To configure this, permit TCP packets without the ACK bit (Don't Care) into the tunnels only and not out of the tunnels.

Established

Select Established to identify packets in an already established TCP Connection.

Don't Care

Select Don't Care when you do not care whether a TCP Connection has been established.

Common filter modify fields

Under the Filters→Rules Definition screen, the Modify button for the Addresses, Protocols, and Ports screens all have common fields, which are listed here using the subject Addresses. Each of the other two filter fields responds as stated here, though of course the subject of the action is either Protocols or Ports.

The fields that are not common to other screens are described with the particular screen.

Create

Click to add a new Address.

Edit

Click to Edit a selected Address Mask.

Delete

Click to Delete a selected Address.

Current Addresses

The Current Addresses appear in the screen. To edit or delete an Address, click the Address, then click Edit or Delete. To create an Address, click Create.

Figure 113 Current Addresses

Current Addresses

Displays the current IP addresses that are to be filtered.

Create or Edit Address

Following is a sample Create or Edit Address screen.

Figure 114 Create or Edit Addresses

Address Name

Enter the IP Address Name for the entry to be created or edit an existing Address Name.

Address

Enter the IP Address for the entry to be created or edit an existing Address.

Wildcard

Enter the Wildcard to be applied to the address or edit an existing Wildcard. This follows the Cisco filter rule convention. Place ones in the bit positions that you want to ignore. Following are three Wildcard examples:

Table 24 Wildcard examples

255.255.255.255	The Address does not matter (any address).
0.0.0.0	The system looks for an exact Address match.
0.0.3.255	The first two octets and the six most significant bits of the third octet create the address match.

Current Protocols

The Current Protocols appear in the screen. To edit or delete a protocol, click the protocol number, then click Edit or Delete. To create a protocol, click Create.

Figure 115 Current Protocols

Current Protocols

Lists the Protocols that are currently configured for this filter.

Create or Edit Protocol

Following is a sample Create or Edit Protocol screen.

Figure 116 Create or Edit Protocols

Protocol

Enter a new or edit an existing Protocol Name.

Protocol Number

Enter a new or edit an existing Protocol Number.

Current Ports

The Current Ports appear in the screen. To edit or delete a port, click the port number, then click Edit or Delete. To create a port, click Create.

Figure 117 Current Ports

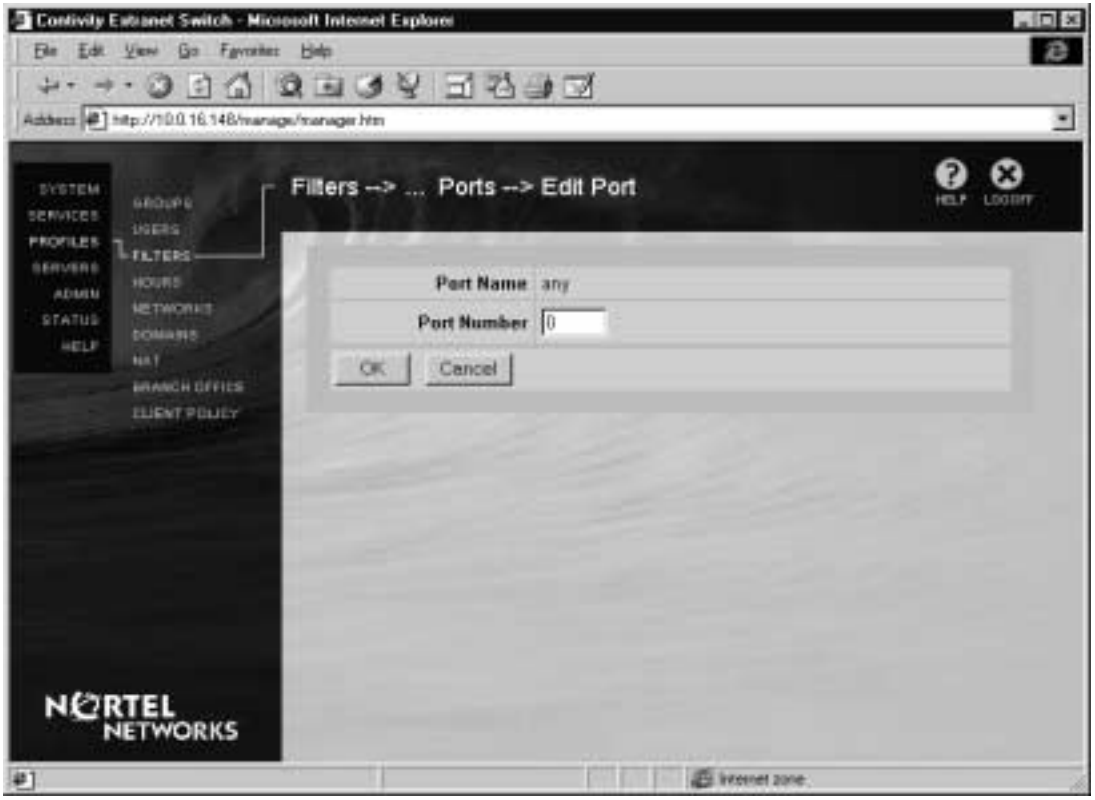
Current Ports

Lists all of the currently configured ports by name and number.

Create or Edit Port

Following is a sample Create or Edit Port screen.

Figure 118 Create or Edit Port



Port Name

Enter a new or edit an existing Port Name.

Port Number

Enter a new or edit an existing Port Number.

Hours

The Hours of Access screen allows you to set predetermined times during which you can permit a group of users access. This time allocation provides for very specific access at certain hours only or complete access anytime; or variations that allow you to shut users out to perform network maintenance.

Figure 119 Hours of Access

Name

The Name of the defined schedules that can be assigned to Groups appear in the list box. Use one of the available buttons to modify the list. Default is **Anytime**.

Edit

Click to modify the profile of the access schedule currently selected.

Delete

Click to Delete the access schedule currently selected. You cannot delete a particular schedule of hours if it is being used by a group.

New Access Hours

Enter the Name for a new profile of access hours.

Add

Click to Add an access profile to the list of defined schedules.

Edit Hours of Access

This screen allows you to configure exact times that a group is permitted access to the switch. The ranges are Monday to Sunday, 00:00:00 to 23:59:59, based on a 24-hour clock.

Figure 120 Edit Hours of Access

Day

Click the Days of the week that you want this group to have access to the switch, from Monday to Sunday.

Hours Allowed

Enter the Hours Allowed that you want this group to have access to the switch: from 00:00:00 to 23:59:59, based on a 24-hour clock.

Networks

The Networks screen allows you to specify network routes that are tunneled when you enable the split tunneling or branch office features.

After you specify networks, you associate them to specific groups for tunneling capabilities through the Profiles→Groups→Connectivity Edit screen. You specify branch office networks through the Profiles→Branch Office Edit screen.

Figure 121 Networks

Current Networks

Shows the currently configured network routes that you can select when specifying split tunneling or branch offices.

Note: A maximum of 16 routes are allowed on the August 1995 version of Windows 95 systems; the switch displays more than 16 routes, but you cannot tunnel through them.

Edit

Click the Network that you want to modify, then click the Edit button. The Filter Rules for that group appear.

Delete

Click to Delete a Network that you no longer intend to use. The name is removed from the list. You cannot delete a Network that is being used.

Create

Enter the new network name and click to Create a new network; the Networks Edit screen appears.

Networks Edit screen

The Networks Edit screen allows you to assign IP addresses and subnet masks to the networks.

Figure 122 Networks Edit

Current Subnets For

Shows the currently configured IP addresses and subnet masks for the network that you are editing.

New Subnets For

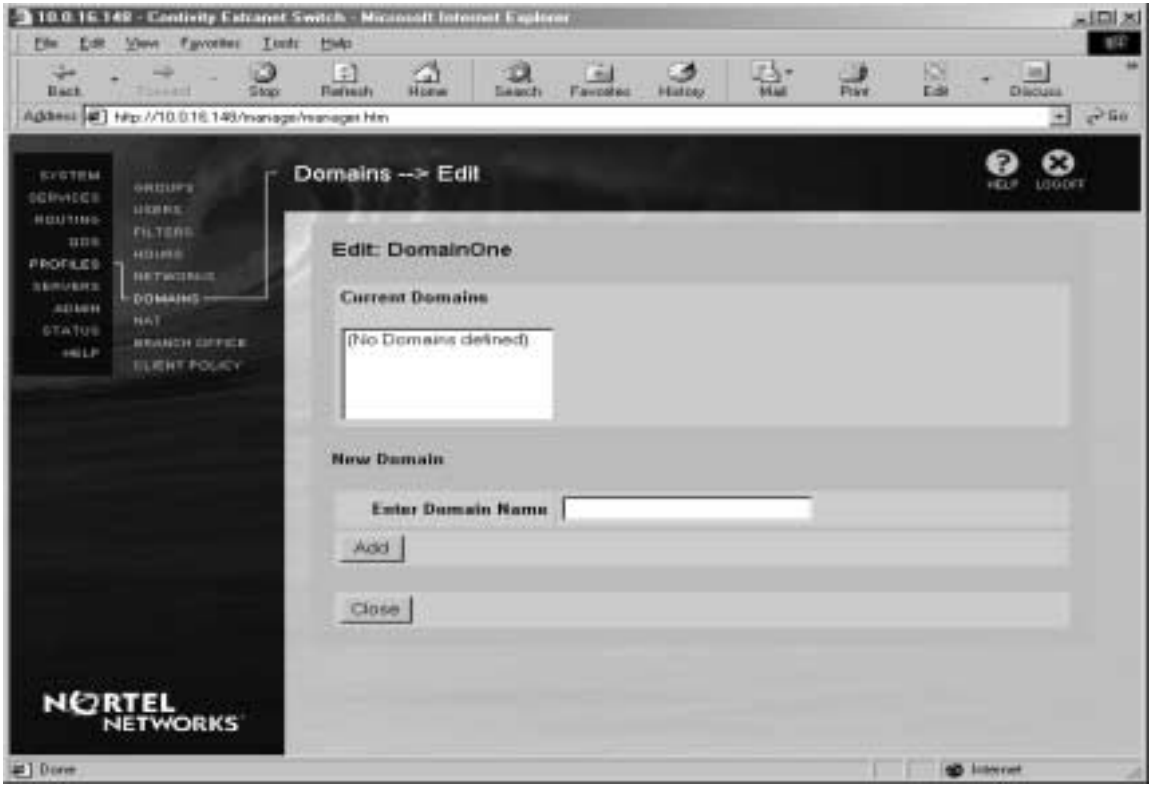
Enter the IP Addresses and Subnet Masks for the networks, then click Add.

Domains

The Domains screen allows you to specify the domains that are used by the Client Auto Connect feature. This screen helps simplify management by grouping domains into sets. You then specify which sets of domains are used for particular IPSec tunnels on the Profiles→Groups→Edit IPSec screen.

When a remote client user attempts to connect to a location, such as a web site, that is in a specified domain or set of domains, the Client Auto Connect feature is started. For more information, refer to "Forced Logoff."

Figure 123 Domain



Current Domain Sets

Shows the currently configured sets of domains that you can use when specifying the Client Auto Connect feature.

Edit

Click the domain set that you want to modify, then click the Edit button. The Edit Domain Set screen appears.

Delete

Click to delete a domain set that you no longer intend to use. The name is removed from the list. You cannot delete a domain set that is currently being used.

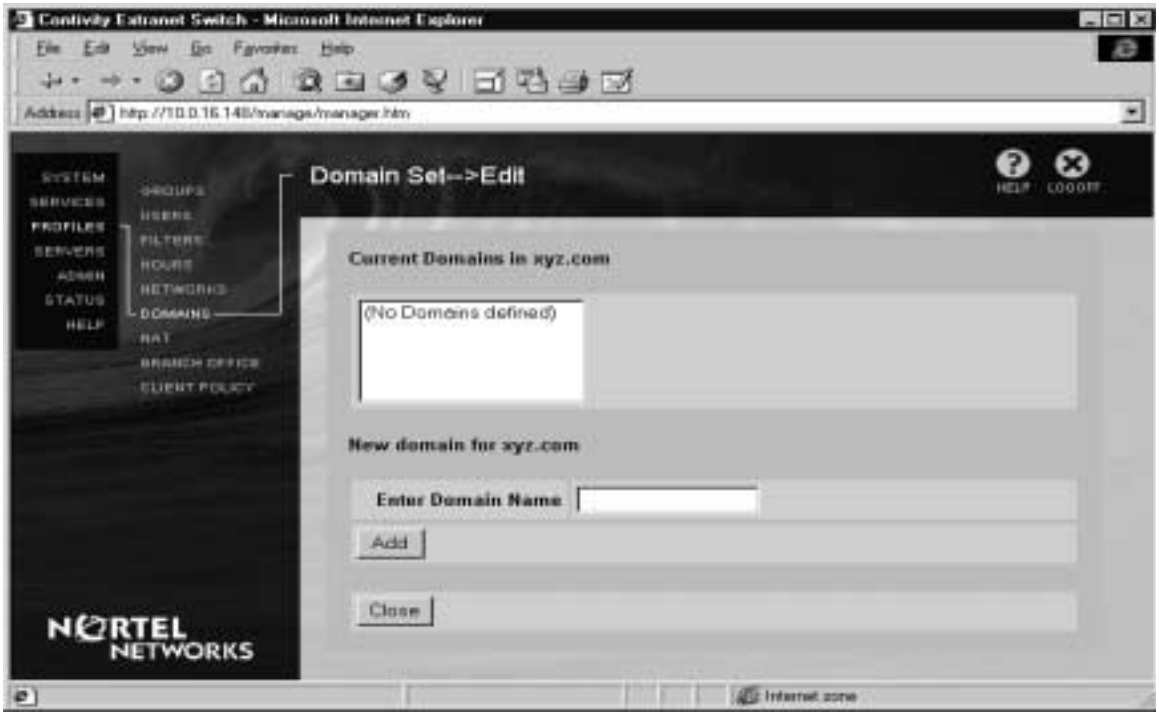
Create Domain

Enter the name of the new domain set, then click the Create Domain button. The new name is added to the Current Domain Sets field. You can then edit the domain set and add the names of the domains that you want included in the set.

Edit Domains screen

The Edit Domains screen allows you to add domains to the selected domain set.

Figure 124 Edit Domains



Current Domains in domain_set

Shows the name of the domain set that you are editing and the names of the domains that are in the domain set.

Delete

Select the domain you want to delete, then click the Delete button. The name is removed from the list. You cannot delete a domain from a domain set that is currently being used.

New Domain for domain_set

Enter the name of the domain you want to add to the domain set, then click Add. The new domain appears in the Current Domains in *domain_set* field.

Network Address Translation (NAT)

Network Address Translation (NAT) is the translation of one network IP address that is used within a LAN to a different IP address that is used outside the LAN. This feature allows a system to be identified by one address on its own network, yet be identified by a totally different address to systems on a different network.

Creating NAT sets

NAT sets are collections of rules that make up a named set. You can create specific NAT sets for certain conditions, and assign the sets as they are appropriate to the conditions. NAT sets are typically applied to branch offices that use either static or dynamic address schemes.

The NAT screen allows you to create NAT sets and edit or delete any currently defined NAT sets. To create new NAT sets, you define a name and click Create.

When you edit an existing NAT set, the NAT Rules screen appears. The NAT Rules screen allows you to add new rules or edit existing rules. This screen lists the currently defined rules for a given set.

Translation Type

Select one of the NAT Translation Types.

Static

A static address is the most specific NAT type or rule and it always overrides dynamic rules. Static addresses are considered to be one-for-one. A host name using this rule is always bound to the same external address. For example, 10.2.3.2 within the intranet is always translated to 192.168.34.65. A static address allows bidirectional access to a destination address, as long as the DNS servers are configured accordingly. Additionally, either client device can use the bidirectional address.

Port

Unlike static rules, dynamic port NAT is not one-for-one. All packet transmissions must be initiated from the internal network. For dynamic port translation, the switch checks to see if the packet matches any translation table entries. If an entry exists, then the destination port and address are modified appropriately. If there are no matching entries, then the switch checks to see if the packet is initiating a connection. If so, then the next available port is allocated, the address and port are added to the translation table, and the packet is modified accordingly. The port assignment is allocated from the range of unassigned port numbers. For an incoming packet, if there are no matching entries in the translation table, then the packet is dropped.

Pooled

Dynamic pooled NAT is similar to dynamic port NAT. The switch checks to see if an address entry has already been allocated for this situation. If so, the packet addressing is updated and the packet is sent. Otherwise, the switch attempts to allocate an address from a pool designated for this session. If an address is available, the switch adds the address pair (the original private address and the newly assigned public address) to the translation table and modifies the packet header. If there are no addresses available, the packet is dropped. For an incoming packet, if there are no matching entries in the translation table, then the packet is dropped.

Internal

Enter the start and end addresses that represent the address pool that is used within the intranet.

Start Address

Enter the first available address that is used within the intranet address pool.

End Address

Enter the last available address that is used within the intranet address pool.

External

The External address is for the endpoint device. Enter the start and end addresses that represent the addresses used for the public network (Internet).

Start Address

Enter the first available address that is used for the public network.

End Address

Enter the last available address that is used for the public network.

Branch Office

You access the Branch Office screen through the Profiles→Branch Office menu selection. You use the subsequent configuration pages to set up a branch office connection. The screens enable you to specify the attributes of the switches that are participating in the connection and to set up network parameters, such as addresses, tunnel type, and connection type, for the connection.

The Contivity VPN supports symmetric, or peer to peer branch office tunnels with fixed endpoints, and asymmetric branch office tunnels. An Asymmetric Branch Office tunnel indicates a branch office tunnel where one of the endpoints does not have a fixed IP address. Such situations exist in the small branch office or SOHO environments where the Contivity VPN Switch's public interface is behind a DSL or Cable modem. The DSL or Cable modem services typically do not guarantee a static IP address. Branch office tunnels in these situations are asymmetric because only one side of the tunnel can initiate a connection.

When you create a branch office connection, you associate it with a group. The branch office connection then inherits the attributes of that group. You can associate multiple branch offices with the same group, thereby saving set up time and increasing management efficiency. For example, you might plan on creating several VPN connections from various remote sales offices into your enterprise headquarters. In this case you would create all of the connections in the same group so they would all have the same attributes, such as hours of access, encryption method, and password management.

You use the main Branch Office screen to create new branch office connections and to edit or delete existing connections. The screen also enables you to add or edit the group that is associated with your branch office connection.

Figure 125 Branch Office

Edit

Accesses the Edit screen for either the selected group or the selected branch office connection. The Groups are shown in bold above the branch office connections.

When you click the Edit button for a Group on the Branch Office screen, you access the Edit Group screen (see "Edit a group" for more information.) This screen is used to set up connectivity, IPSec (for IPSec tunnels), and routing attributes for a particular group. Edit the configuration parameters as appropriate.

When you click the Edit button for a branch office connection, the "Edit Connection screen appears.

Delete

Deletes the selected group or branch office connection.

Test

The Test button provides a mechanism for you to verify that the branch office connection is properly configured and that the remote gateway remains reachable. Detailed messages are sent to the Event Log to help identify failure events.

When you click the Test button, establishment of the Branch Office tunnel is attempted. If the test is successful, this insures that the remote and local gateway configuration is correct. If for any number of reasons the connection establishment fails, a failure message should indicate what the configuration problem might be. The Event Log is used extensively during this test to provide details about the test. Additional logging is done as part of the tunnel protocols (L2TP and IPSec), which should provide enough information to determine the problem.

In some cases, however, the actual reason for the failure is due to some remote configuration issue that is not provided in failure exchange with the remote gateway. In such cases, it may be difficult for you to determine the exact reason. If possible, initiating the test from the remote gateway could provide the necessary details.

Note: The Test button is not supported with Branch Office tunnels that have a connection type of Responder.

Configure IP

The Configure IP button accesses the Branch Office→Edit→IP screen. You use this screen to enable and disable a branch office and to configure routing for the branch office.

Enable/Disable

The Enable/Disable button toggles the Branch Office connection between states.

Define Branch Office Connection

The Define Branch Office Connection button accesses the Define Connection screen, which you use to name a new branch office connection and to associate it with a group.

Add Group button

Accesses the Add Group screen, which is used to create a new group. The new group can then be associated with a branch office connection.

Add Group screen

This screen is used to add a new group that is associated with the branch office connection. The new group inherits the attributes (for example, Access Hours) of its parent group, which are then used by the branch office connection.

Parent Group

The drop-down list box shows all the branch office groups that have been set up on the switch. Select the group whose attributes are inherited by the new group. Refer to the Profiles→Groups→Edit→Connectivity screen for additional details on the hierarchical structure of group attributes.

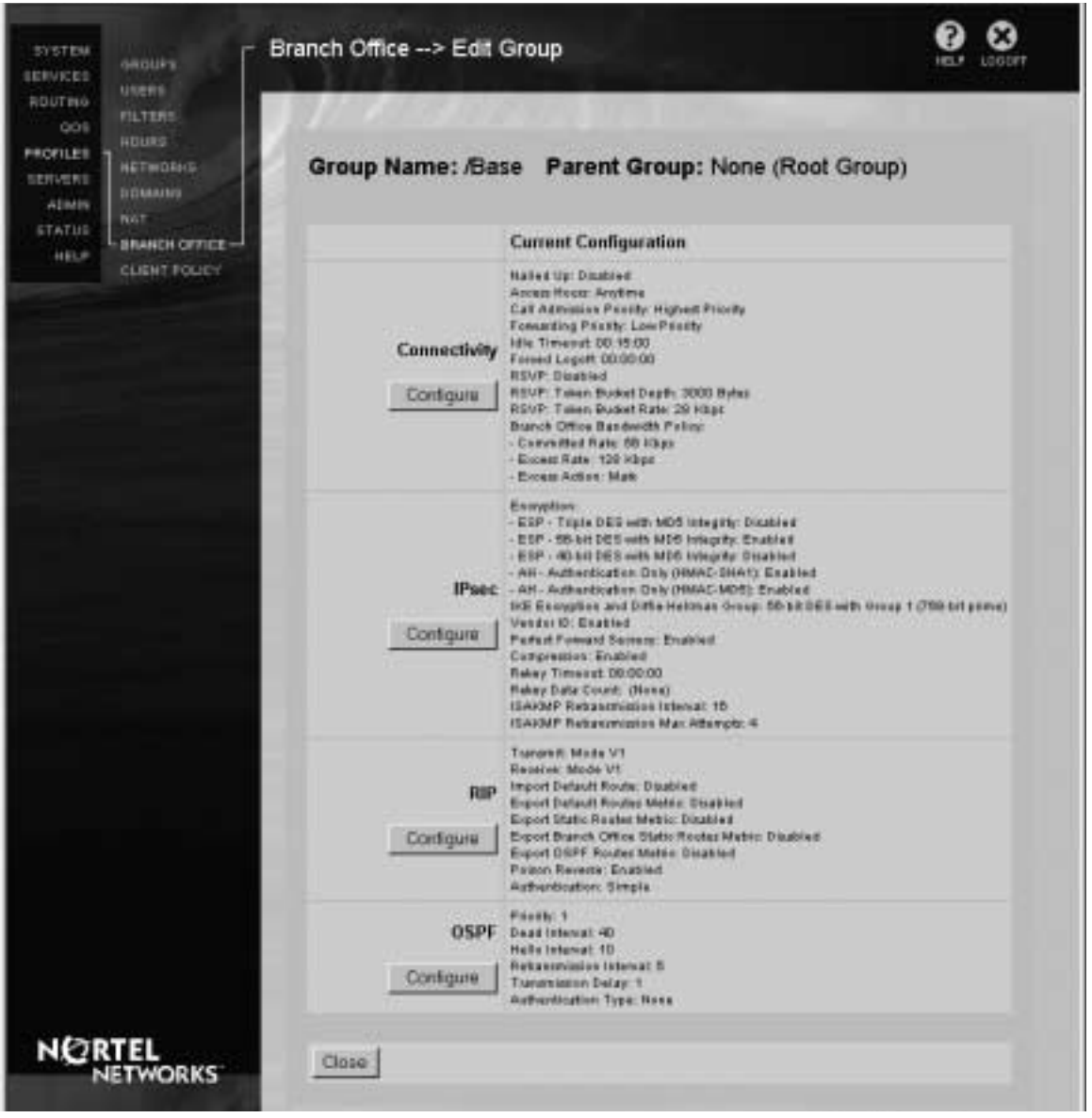
Group Name

The Group Name identifies the new group that are associated with the branch office connection. The Group Name can be a maximum of 64 characters (spaces are permitted).

Edit Group

When you click the Edit button for a Group on the Branch Office screen, you access the Edit Group screen (see “Edit a group” for more information.) This screen is used to set up Connectivity, IPSec (for IPSec tunnels), and routing attributes for a particular group. Edit the configuration parameters as appropriate.

Figure 126 Branch Office→Edit Group



Edit Connectivity

Click Configure in the Connectivity section of the Edit Group screen to configure the connectivity attributes of the group.

Figure 127 Branch Office→Edit→Connectivity

Nailed Up

Specify if the Branch Office connection is nailed up or not.

Branch Office connections can be on-demand or nailed up.

On-demand branch office connections are established as a result of receiving data destined for some remote network or host. This initial data (one or more packets) is discarded until tunnel establishment is complete. Once the connection is established, data is then successfully delivered.

Nailed up branch office connections are established at system start-up or during re-configuration. These connections do not require data to trigger the establishment of the tunnel. Thus, when initial data arrives for a remote network, the tunnel establishment may have already been completed and the data can be delivered. If the tunnel establishment is not complete prior to receiving data for the remote network, (that is, if the connection establishment exchange is in progress or the remote gateway is not reachable), then the data is discarded.

Note: Data for Nailed up connections is not buffered. This is also the case for on-demand connections.

Access Hours

Specify the time ranges during which access is allowed for users in this group. These time ranges are configured from the Profiles->Hours screen. The default value is Anytime.

Call Admission Priority

Specify the Call Admission Priority level (from low to highest) you want to permit for this group. Each level is assigned a percentage of the total number of calls allowed access to the switch. If there is a particularly high number of users logged in, new users could be denied call access, based on their Call Admission Priority, until existing callers disconnect.

Possible Call Admission Priority levels are:

- Highest Priority **(**default)
- High Priority
- Medium Priority
- Low Priority

Forwarding Priority

Specify the Forwarding Priority level (from low to highest) that you want to provide to sessions for users in this group. Forwarding Priority assures a certain level of latency and bandwidth allocation. For example, a group with the Highest Forwarding Priority has the highest possible bandwidth service and the lowest level of latency.

Conversely, if there is a particularly high level of traffic on the line, packets for a Low Priority group might be delayed or dropped. Since a Low Priority group has the least amount of bandwidth and the highest level of latency, some of its packets would wait until the higher priority level packets have been forwarded or they would be dropped.

Possible Forwarding Priority levels are:

- Highest Priority
- High Priority
- Medium Priority
- Low Priority (default)

Idle Timeout

Enter an appropriate Idle Timeout in days, hours, minutes, and seconds format: dd:hh:mm:ss. The *Idle Timeout* is an amount of time a connection can be idle (no data has been transmitted or received through the connection for the specified amount of time). When the Idle Timeout expires, the session is terminated. This option helps prevent allocation of resources on the switch for sessions that are no longer active.

The default Idle Timeout is 00:15:00 minutes; the range is 00:00:00 to 23:59:59. The maximum number of days is 29. A setting of 00:00:00 specifies no Idle Timeout.

Note: All sessions check their configuration at startup time. Therefore, if you change the time of the idle timeout during a session, the change only affects new sessions and not any existing ones.

The Idle Timeout setting is valid for traffic coming into the device only.

Note: Branch Office connections do not support the CA Certificate Allow All feature. Therefore, you must have an explicit entry for each Branch Office connection. Only branch offices with the branch office's certificate subject distinguished names entered into the Profiles→Branch Office: Define Branch Office Connection screen can authenticate using certificates issued by the CA.

Forced Logoff

You can specify a time period to force the logoff of users in this group.

RSVP

Click to enable RSVP (Resource ReSerVation Protocol). The Nortel Networks RSVP implementation allows you to signal the network for required bandwidth. The client must be configured appropriately for RSVP to work. Additionally, only the controlled load-service is supported. This option is Disabled by default.

RSVP: Token Bucket Depth

The Token Bucket Depth influences packet flow delays within the switch and participating routers in the Internet. The largest amount of data the switch holds in its queue determines latency. New packets arriving are delayed by a time that is proportional to the amount of traffic that is ahead of them in the queue, which is no greater than the Token Bucket Depth. When the queue exceeds the Token Bucket Depth, incoming packets are dropped. To guarantee reduced latency, the Bucket Depths should be small. Typically, you should not change this setting. Default is 3000 bytes.

RSVP: Token Bucket Rate

The Token Bucket Rate is the highest long-term average data rate (in Kbps) required over time for the connection. It informs the switch and participating routers in the Internet how much bandwidth to reserve for the RSVP session. Typically, you should not change this setting. Default is 28 Kbps.

Address Pool Name

Click on the drop-down menu to select the Address Pools used by remote users to access this switch. The drop-down list shows all pools that have been defined on the switch. (Address pools are defined on the Servers→User IP Addr screen).

Select the New Address Pool link to define a new pool. Refer to "Remote User IP Address Pool" for details. This option is set to Default Pool by default.

Branch Office Bandwidth Policy

Click the Configure button in the Bandwidth Policy section to modify bandwidth characteristics for this group. Click the Use Inherited button to apply the settings of the parent group to this group.

Committed Rate

Select a Committed Rate from the list of available bandwidth rates. If the desired bandwidth rate is not listed, click on Define new bandwidth rate to create a new one.

Excess Rate

Select an Excess Rate from the list.

Excess Action

Choose an Excess Action for traffic handling, either Drop or Mark.

Edit IPSec

Click Configure in the IPSec section of the Edit Group screen to configure the IPSec attributes of the group.

Edit OSPF

Click Configure in the OSPF section of the Edit Group screen to configure the OSPF routing attributes of the group.

Edit RIP

Click Configure in the RIP section of the Edit Group screen to configure the RIP attributes of the group.

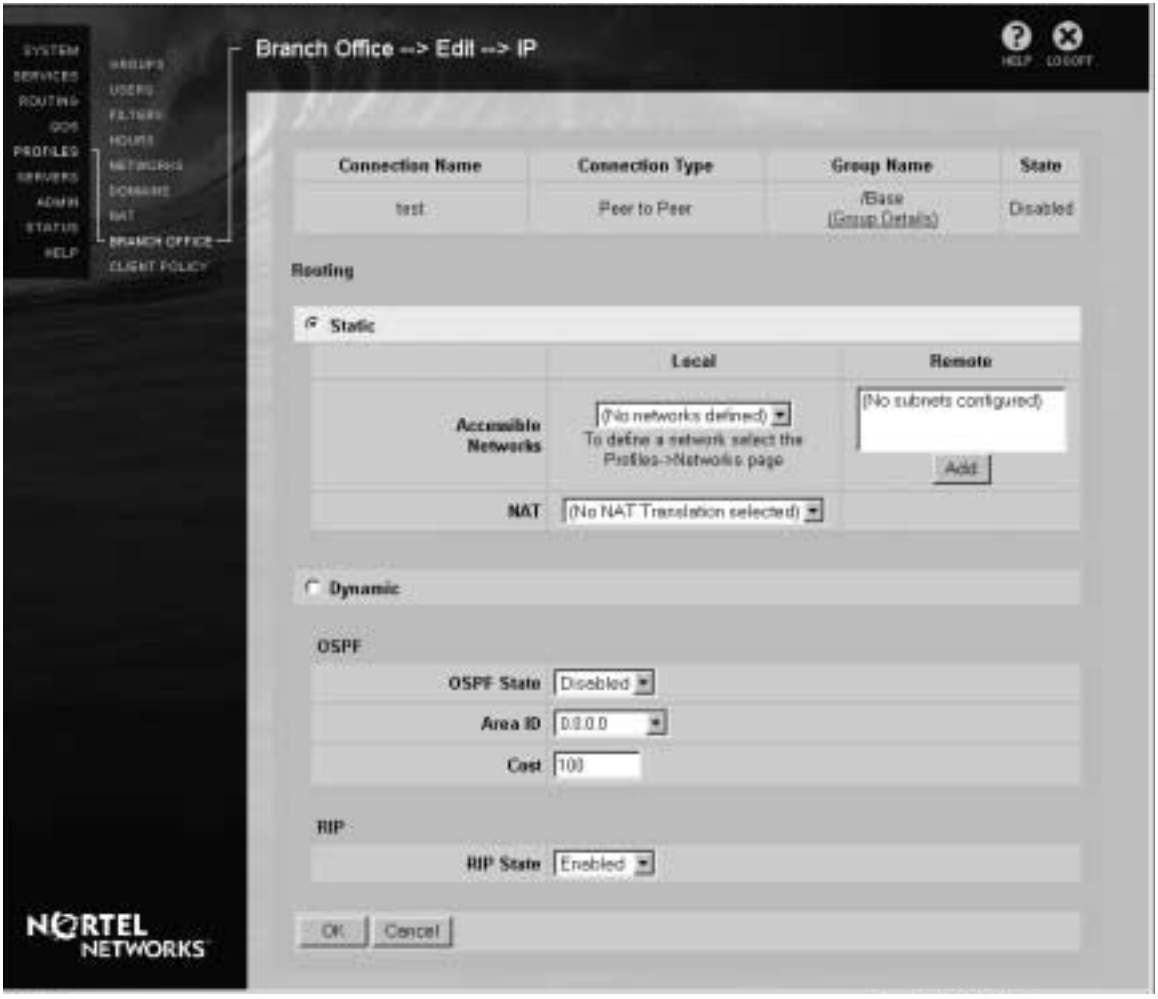
Edit Connection

When you click the Edit button for a branch office connection, the Edit Connection screen appears. See “Edit Connection” for more information.

Configure IP

The Configure IP button accesses the Branch Office→Edit→IP screen. You use this screen to enable and disable a branch office and to configure routing for the branch office.

Figure 128 Branch Office→Edit→IP



Connection Information

Connection Name

Displays the name of this branch office connection.

Group Name

The Group Name list contains the names of all groups that have been set up on this switch. Select the group that you want to use for the branch office connection. The group is a child of its associated Parent Group and inherits the Parent Group's network access attributes (refer to the Profiles→Groups→Edit→Connectivity screen for details). You can later modify the new group's inherited options.

State

Shows the current state of this branch office connection, either enabled or disabled.

Routing

Use the drop-down list box to select either Static or Dynamic routing for this branch office connection.

Static Routes

Accessible Networks

You use the Accessible Networks section of the Static Routes to define local and remote networks to which the branch office has access. Use Profiles→Networks to define local networks and the Add button to define remote networks.

NAT

Use the drop-down list box to select from available NAT sets.

OSPF

OSPF State

Use this to enable and disable OSPF routing for the branch office.

Area ID

Area IDs are used as representations of parts of the OSPF network. They help to manage large numbers of networks so that they can exchange information within an area. If the area represents a subnet, the IP network number can be used for the Area ID. Each Area ID must be unique for OSPF. By default all switches have an area named 0.0.0.0.

Cost

Enter a Cost value for OSPF routing.

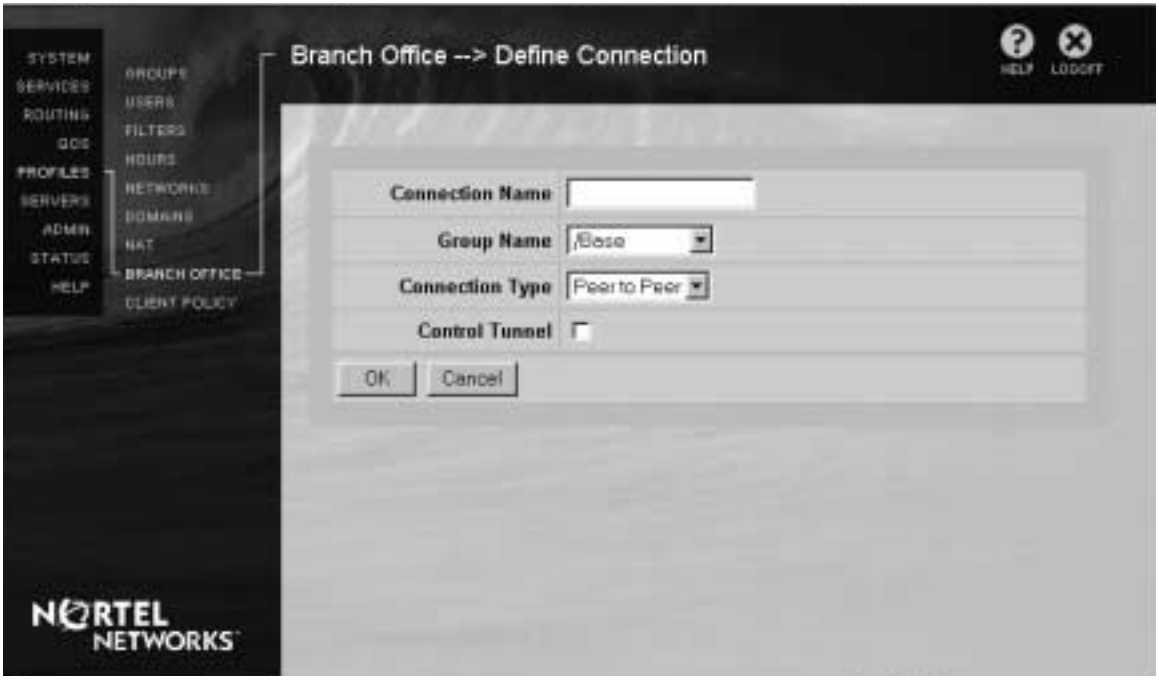
RIP

Use this to enable and disable RIP for the branch office.

Define Branch Office Connection

The Define Connection screen is used to create a new branch office connection. To define a new connection, you first enter its name, then associate the new connection with a group. The connection inherits the attributes of that group. When you click OK, the branch office connection is created and the Define/Edit Connection screen appears.

Figure 129 Define Connection



Connection Name

The name of the new branch office connection. The name can be a maximum of 64 characters (spaces are permitted).

Group Name

The drop-down list box contains the names of all groups that have been set up on this switch. Select the group that you want to use for the branch office connection. The group is a child of its associated Parent Group and inherits the Parent Group's network access attributes (refer to the Profiles→Groups→Edit→Connectivity screen for details). You can later modify the new group's inherited options.

Connection Type

Selection the type of Branch Office connection that you want this branch office to use.

Peer to peer

Peer to peer connection type is the traditional branch office tunnel, where either side can initiate traffic.

Initiator

With Asymmetric Branch Office Tunnels (ABOT), one side has to be configured as the Initiator and the other as the Responder. Only the Initiator can bring up the tunnel.

When the connection type is set to initiator, there is no need to define a local endpoint. It should be configured for a tunnel type of IPSec only, and the IPSec authentication requires an initiator ID.

Responder

When the connection type is set to Responder, neither local or remote endpoints are required. It must be configured to use the IPSec authentication provided by specifying the same initiator ID as in the associated Initiator branch office tunnel.

Control Tunnel

Put a check in the Control Tunnel check box to specify that this branch office connection is for a control tunnel. If you want a branch office connection to be a control tunnel, it must be configured as such at its initial configuration. When you create and save a branch office connection, you cannot later change the control tunnel specification for that connection. You must set up a new connection and create it as a control tunnel.

Note: Administrator User IDs are not tied to control tunnel IDs.

Edit Connection

The Edit Connection screens allows you to enable the Branch Office feature and to specify routing and networking information, local and remote identification, and authentication attributes for the branch office connection.

Figure 130 Branch Office→Edit Connection

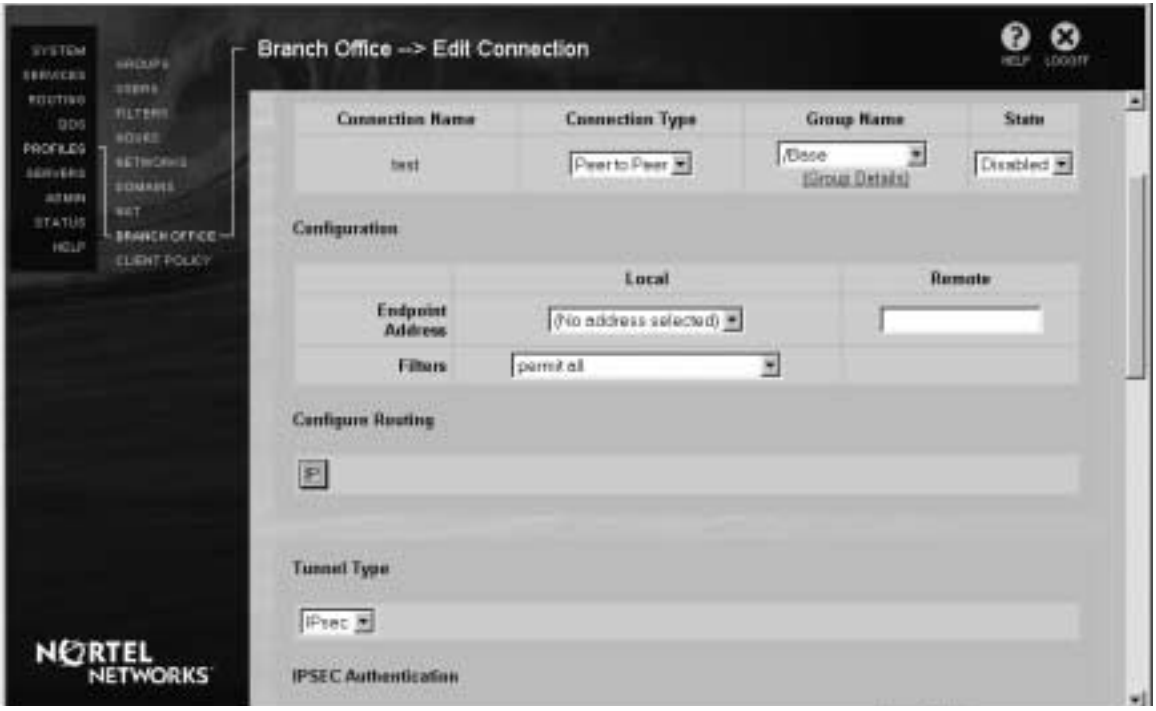
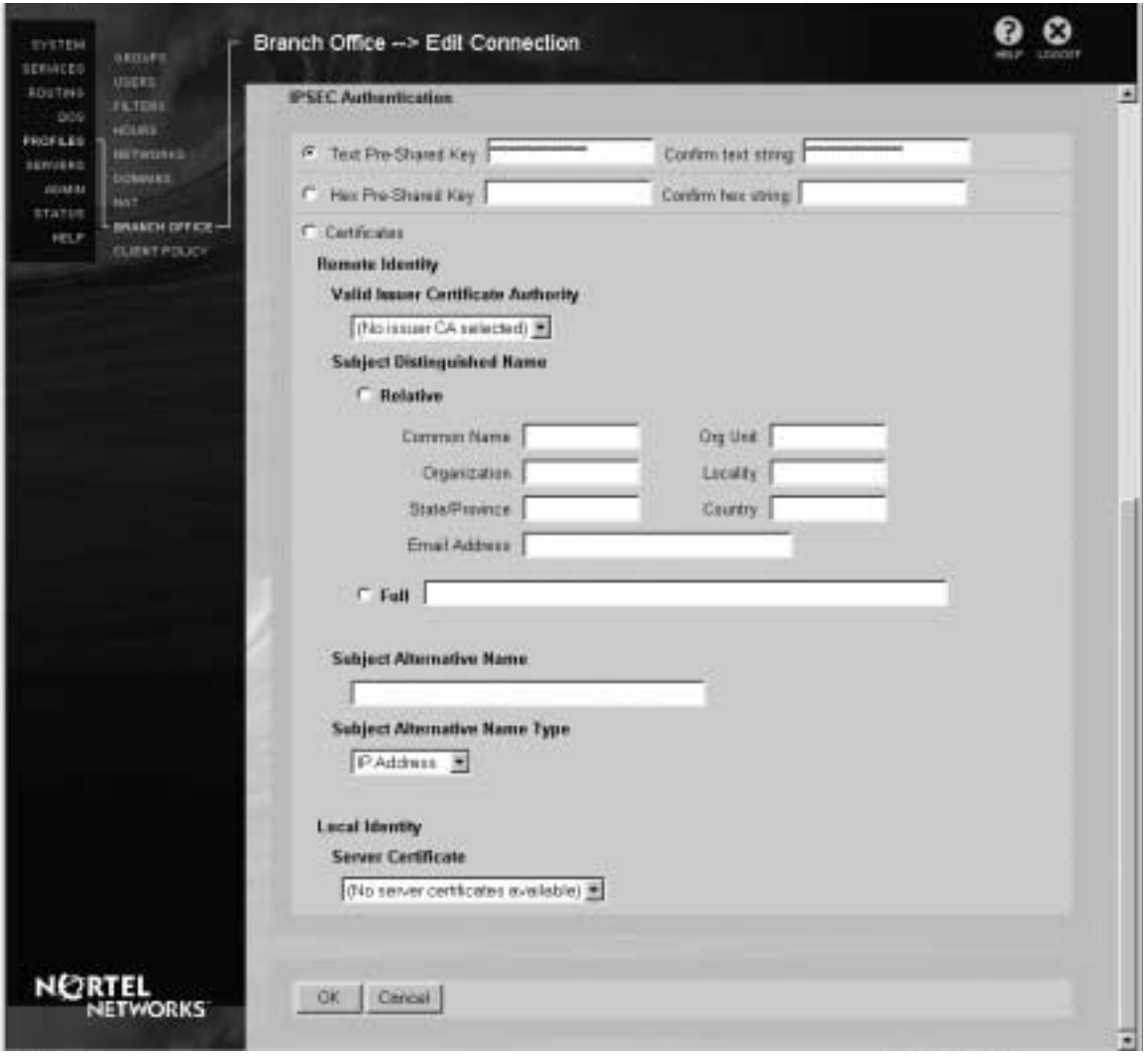


Figure 131 Branch Office→Edit Connection - continued



Connection information

Connection Name

The name you assign to this branch office connection. The name can be a maximum of 64 characters (spaces are permitted).

Connection Type

Selection the type of Branch Office connection that you want this branch office to use.

Peer to peer

Peer to peer connection type is the traditional branch office tunnel, where either side can initiate traffic.

Initiator

With Asymmetric Branch Office Tunnels (ABOT), one side has to be configured as the Initiator and the other as the Responder. Only the Initiator can bring up the tunnel.

When the connection type is set to initiator, there is no need to define a local endpoint. It should be configured for a tunnel type of IPSec only, and the IPSec authentication requires an initiator ID.

Responder

When the connection type is set to Responder, neither local or remote endpoints are required. It must be configured to use the IPSec authentication provided by specifying the same initiator ID as in the associated Initiator branch office tunnel.

Group Name

The group that defines the attributes that are used by the branch office connection. This group is a child (subset) of its associated Parent Group and inherits the settings from the Parent Group. You can click on the Group Details link to view or modify a subset of the group’s settings. Modifications of a child group do not change the settings of the Parent Group.

State

Use the drop-down list box to toggle the state between enabled and disabled.

Configure Routing

Click the IP button to specify the type of routing to use for traffic going through the branch office connection.

- If you choose Static routing, you must manually specify the Accessible Networks (the private internal networks behind a switch that can be accessed via the branch office connection).
- If you choose RIP, the routing protocol automatically determines the accessible networks based on information that is entered on the System→LAN Interfaces→Edit IP Address screen.

Click the drop-down list to choose the routing type that to be used for your branch office connection.

Configuration

Enable Branch Office Connection

Click to Enable the Branch Office feature for this switch.

Note: As a security mechanism, the Enable Branch Office Connection selection is automatically disabled (the check mark is removed) when you attempt to save an incorrect configuration. For example, if you check the box to enable the branch office connection, then fail to specify the remote address, the Enabled check box is cleared (disabled) and an error message appears when you select the OK button to save your configuration.

Address

Used to specify the public interface IP addresses of the switches that form the branch office connection. The Local Endpoint address is the public interface IP address of the switch whose Management Interface you are using. The Remote Endpoint address is the public interface IP address of the switch that forms the opposite end of the branch office connection.

Accessible Networks

If you have chosen the Static routing type, this field appears on the screen. It does not appear if you are using RIP routing. The accessible networks are the private internal networks that can be reached through the tunnel connections of this branch office connection.

- To specify the Local Endpoint networks, click the drop-down list to display a list of available local networks. These networks have been previously set up on the Profiles→Networks screen. The Local networks are the subnetworks on the private internal network of the local switch (the switch whose management interface you are currently using).
- To specify the Remote Endpoint networks, click Add to go to the Add Networks screen and add the remote networks for the branch office configuration. The Remote networks are the subnetworks on the private network of the remote switch.

NAT

If you choose the Static routing type, this field appears on the screen. It does not appear if you are using RIP routing. Network Address Translation (NAT) allows a system to be identified by one address on its own network, and by a totally different address to systems on a different network. NAT enables you to build your VPN without requiring that you reconfigure or rename your existing network. NAT sets are defined on the Profiles→NAT screen. Refer to “Network Address Translation (NAT)” for more information on NAT.

Click the drop-down list and select the NAT set that you want to use.

Filters

Select the desired filter that is associated with this connection, or use the default filters of permit all. Packet filtering controls the types of access allowed for users of this branch connection. Filters are based on various parameters, including Protocol ID, Direction, IP addresses, Source, Port, and TCP Connection Establishment. Filters are defined on the Profiles→Filters screen.

Click the drop-down list and choose the filter that you want this branch office connection to use. The default is permit all. You can specify one filter.

Tunnel Type

Use the drop-down list to change the tunnel type for the connection. The default type is IPSec. Click the drop-down list and select either IPSec, PPTP, or L2TP.

Note: If you change the Tunnel Type, the fields in the Authentication portion of this screen change to reflect the different configuration requirements for the new Tunnel Type.

Authentication

This portion of the screen allows you to configure the authentication that is used between the local and remote branch office switches. The fields that appear in this screen depend on whether you are using an IPSec, PPTP, or L2TP tunnel type.

IPSec Authentication

Pre-Shared Key: Text or Hex String

This is an alphanumeric text or hexadecimal string that is used between the local and remote branches for authentication. In order for authentication to occur, you must use the same pre-shared string on both the local and remote branch offices.

Certificates

Certificates are associated with each endpoint gateway and allow for mutual authentication between two connections. The certificate portion of the screen includes information about the remote branch office system, the authority that issued the certificate, and the certificate identification.

Remote Identity

This is the name of the remote peer initiating the tunnel connection. You can use either a Subject Distinguished Name (Subject DN) or a Subject Alternative Name to uniquely identify the remote branch office system. Specifying both a full subject DN and a subject alternative name on this screen allows the remote peer to use either identity form when making a connection.

Valid Issuer Certificate Authority

Select a Valid Issuer Certificate Authority from the drop-down list box. This CA is the issuer of the remote peer's certificate or a higher level CA in the remote peer's certificate hierarchy. The CA must have the trusted flag set via the certificates screen. If a CA hierarchy is being used, all intermediary CAs below the trusted CA must have been imported to the switch. These Certificate Authorities are configured from the System→Certificates: Generate Certificate Request screen.

Subject Distinguished Name

If you are using a distinguished name to identify the remote branch office site, you can choose to enter the DN as either a relative distinguished name or a full distinguished name. The DN entered here must exactly match the DN in the remote peer's certificate.

Relative

The Relative distinguished name has the following supported components:

Note: Do not include the attribute type as part of your entries in the Relative section. For example, for a name of CN=MySwitch, your entry would be MySwitch (without the CN attribute type).

- Common Name -- Enter the Common Name with which the server is associated.
- Org Unit -- Enter the Organizational Unit with which the server is associated.
- Organization -- Enter the Organization with which the server is associated.
- Locality -- Enter the Locality in which the server resides.
- State/Province -- Enter the State or Province in which the server resides.
- Country -- Enter the Country in which the user resides.

Full

You can directly enter the Full Distinguished Name (FDN) in this field rather than entering the individual components in the previously described Relative distinguished name fields. For example:

```
CN=MySwitch, O=MyCompany, C=US
```

Subject Alternative Name

You can optionally use a Subject Alternative Name in place of a Subject DN, and specify the format of the name. The following formats are acceptable.

- Email Name (for example, net_admin@company.com)
- DNS Name (for example, gateway.cleveland.company.com)
- IP Address (for example, 192.168.34.21)

Local Identity

The Local Identity is the name your switch that you want to use to identify itself when initiating or responding to a connection request. You can use either a Subject Distinguished Name (Subject DN) or a Subject Alternative Name to uniquely identify your system. If you select a subject alternative name from your switch's certificate, then that identity is used in place of your switch's subject DN when communicating with peers.

Note: Your switch's server certificate only has subject alternative names if your CA issued the certificate with the alternative names. For example, with the Entrust PKI the VPN connector can issue certificates with DNS names, IP addresses, or Email alternative names.

Server Certificate

Click the drop-down list box to view all certificates that have been issued to the server. Server Certificates are configured from the System→Certificates: Generate Certificate Request screen.

PPTP Authentication and L2TP Authentication

Authentication Type

Click the drop-down list and select the authentication method that you want to use for the branch office connection. Refer to "Common tunnel settings" for descriptions of the available authentication methods.

Note: When you change the Authentication Type, the screen immediately changes to reflect the requirements of the new authentication method. Any changes that you might have made on the Authentication part of the previous screen are lost.

Local UID

The user ID of the local switch that you are configuring.

Peer UID

The user ID of the remote switch that you are configuring.

Password

Enter the password for the UID, then confirm the password to verify that you entered it correctly. If you selected a variation of MS-CHAP V2 authentication, no password is required for the Local UID.

Details

Compression

Click to Enable or Disable compression. Refer to "Compression" for a detailed description of compression.

Compression/Encryption Stateless Mode

Click to Enable or Disable this selection.This selection is not used if encryption and compression are both disabled.

L2TP Access Concentrator (for L2TP Authentication only)

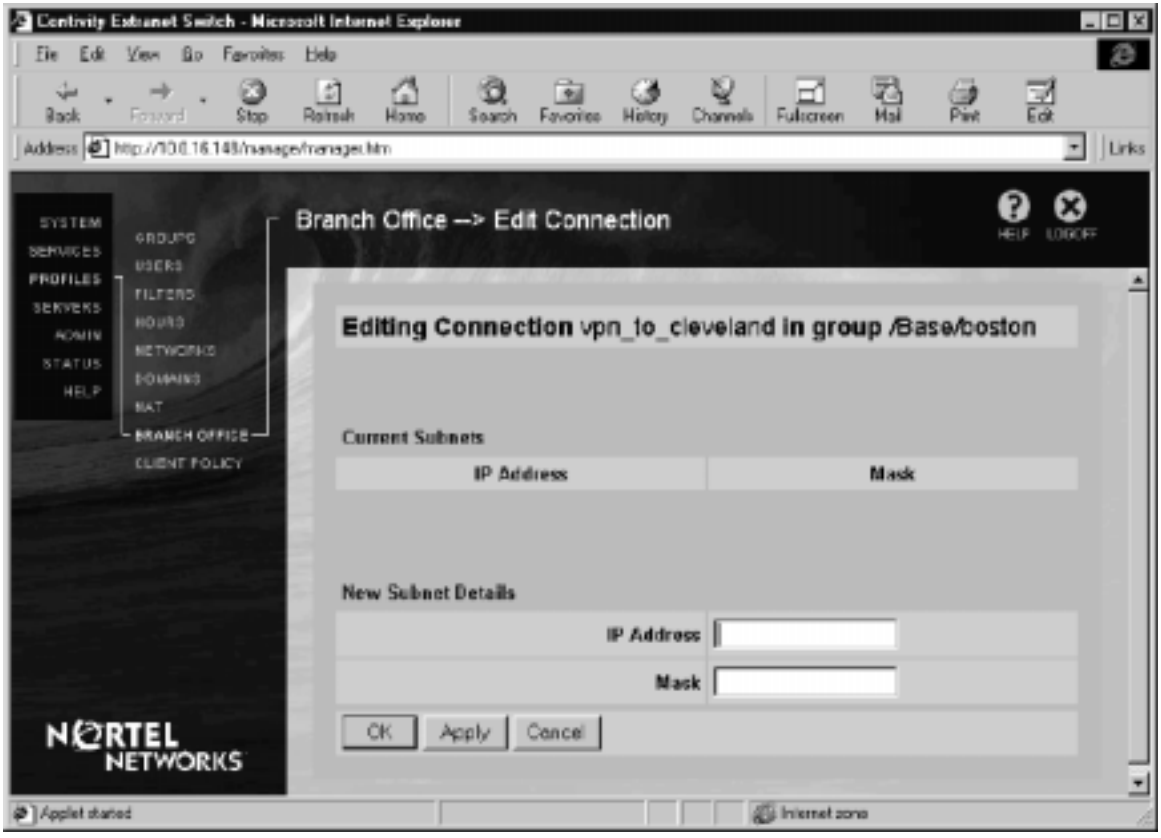
This field appears if you have selected L2TP as the preferred tunnel type for the branch office connection. Use this entry to specify the L2TP Access Concentrator that you want to perform authentication between the switch and the NAS.

Add Remote Networks

When you click Add in the Accessible Networks section of the Edit Connection screen, the Add Remote Network screen appears.

Enter the IP address and subnet mask for the new remote network you want to add for the branch office connection.

Figure 132 Add Remote Networks



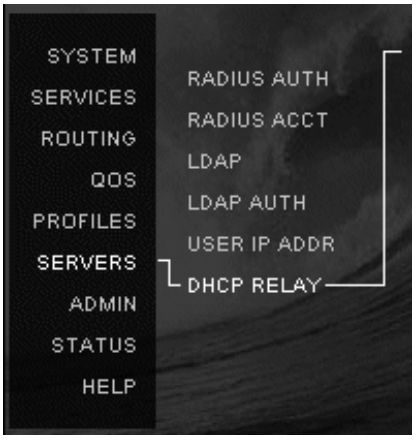
Client Policy

Client Policy helps prevent potential security violations that could occur when you are using the split tunneling feature. Split tunneling allows client data to travel either through a tunnel to the enterprise network or directly to the Internet. Although a powerful feature, this could allow an application on the client to maliciously forward packets from the Internet to the enterprise network.

Chapter 6
Servers

This section provides information about the authentication servers you can configure for authentication of users tunneling into the switch.

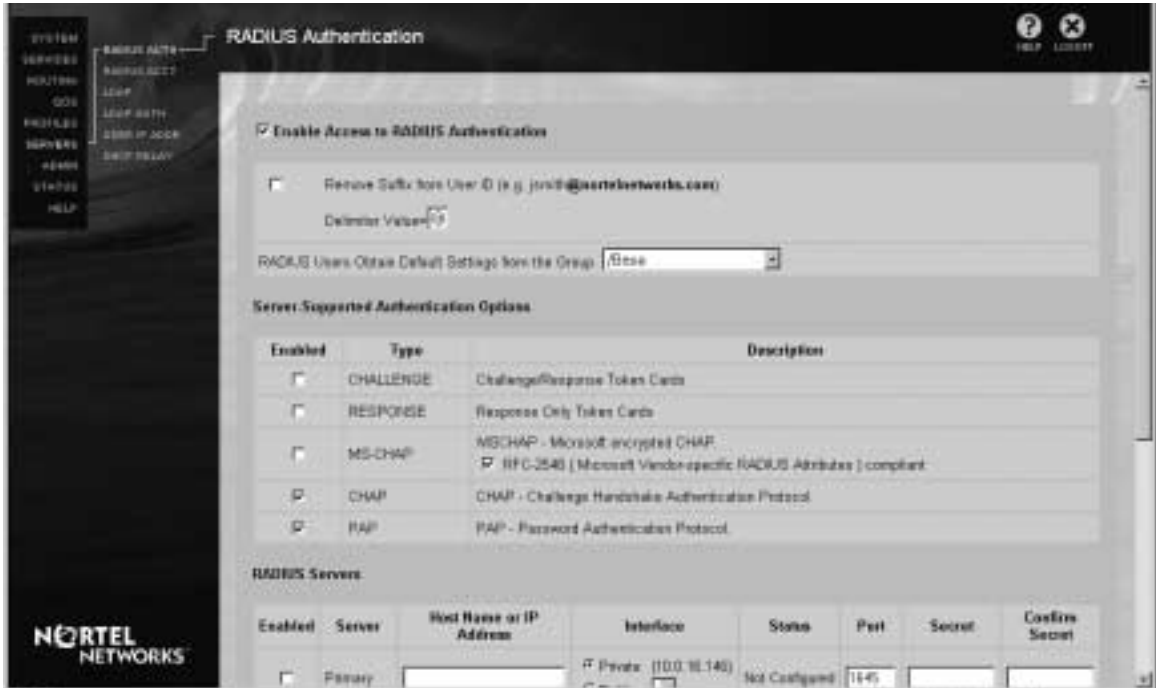
Figure 133 Servers menu



RADIUS Authentication Servers

You use the Servers→RADIUS Authentication screen to configure a RADIUS authentication server.

Figure 134 RADIUS Authentication Servers



Enable Access to RADIUS Authentication

Click to enable access to the RADIUS Authentication servers.

Remove Suffix from User ID

Click to remove the user's fully qualified ID suffix from the UID before sending it to the RADIUS server. You do not need the fully qualified user ID if the DNS server has been properly configured on the switch. A user ID and suffix, where Ncole is the UID and acme.com is the suffix, is *Ncole@acme.com*.

Delimiter Value

Specify the character that separates the suffix from the UID.

RADIUS Users Obtain Default Settings from the Group

Click the drop-down list box to select the default group from which authorization and operational settings are taken. Any user authorized against a RADIUS server acquires the attributes of this group by default.

If the RADIUS server returns a valid group identifier, the switch then uses this group for the user profile. Otherwise, the switch uses the default group.

Server Supported Authentication Options

Enabled

Click to Enable server support each authentication type that your RADIUS Server supports and that you expect to use:

- CHALLENGE – Challenge/Response authentication, for example AXENT OmniGuard/Defender
- RESPONSE – Response Only authentication, for example Security Dynamics SecurID.
- MS-CHAP – Microsoft Challenge Handshake Authentication Protocol encrypted authentication
- RFC-2548 Compliance – Check this box to enable the switch to interoperate with a Microsoft RADIUS Server Version 2.2 or later, or a Version 2.1 with the Microsoft Hotfix applied. Leave this box empty if using a Microsoft RADIUS Server V2.1 (without the Hotfix) or earlier
- CHAP – Challenge Handshake Authentication Protocol authentication
- PAP – Password Authentication Protocol

RADIUS Servers

Enabled

Click to enable the RADIUS servers you want to use for authentication. You can enable up to three servers. The Primary Server receives all RADIUS authentication inquiries unless it is out of service. A RADIUS server that fails to respond five times is temporarily taken off the server list for 30 minutes. After 30 minutes, the server is tried again.

In the event that the Primary Server is unreachable, the switch queries the first and second alternate RADIUS servers.

Select your RADIUS servers by supplying the Host Name or IP Address, Interface type, Port number, and Password. After configuring the servers, the switch reports the current server status.

Host Name or IP Address

Enter either the Host Name or IP Address of the servers. For example, Finance.mycompany.com or 145.22.120.111. You can also use simple names (for example, finance) if you have a DNS server configured on your switch.

Primary

Enter the Primary RADIUS Server host name. This is a required selection if RADIUS is enabled. The Primary server is normally used to process incoming authentication requests.

Alternate 1

Enter the Alternate 1 RADIUS Server host name (this server processes incoming authentication requests if the Primary RADIUS server is unavailable).

Alternate 2

Enter the Alternate 2 RADIUS Server host name (this server processes incoming authentication requests if the Primary RADIUS Server and the Alternate 1 Server are unavailable).

Interface

Specify whether you want the RADIUS server to be accessed via the switch's private or public interface. The address of the specified interface is used to configure the RADIUS Client address information on the remote RADIUS Server.

Note: Be sure you have enabled RADIUS authentication as an allowed service on the Services→Available screen.

Private

Select Private if the RADIUS server is reached through the private interface. The switch's management address is used.

Public

Select Public if the RADIUS server is accessed through the switch's public interface. You must also specify the IP address for the Public interface. The public IP address list is dynamically built from the information on the System→LAN screen. Any change, such as removing an interface card or changing an IP address, is automatically reflected in the drop-down list.

Port

Enter the Server Port Number that you want the RADIUS authentication requests to use. Default is Port 1645.

Secret

All RADIUS Servers share a secret with the switch. To enhance overall security, this secret should be different for each server. The shared secret encrypts the password between the switch and the server when the tunnel connection uses PAP or SecurID. It also verifies the authenticity of each accounting request sent by the switch to the RADIUS server. Furthermore, it verifies the authenticity of each response sent by the RADIUS server to the switch.

Confirm Secret

Reenter the server's Secret (password) to verify that you typed the password correctly.

Response Timeout Interval

Enter the frequency, in seconds, that you want the switch to wait before retrying to connect to the RADIUS servers. By default, the switch tries once every three seconds. The minimum setting is 1.

Maximum Transmit Attempts

Enter the number of times you want the switch to attempt to connect to the RADIUS servers before failing. By default, the switch tries three times.

Diagnostics

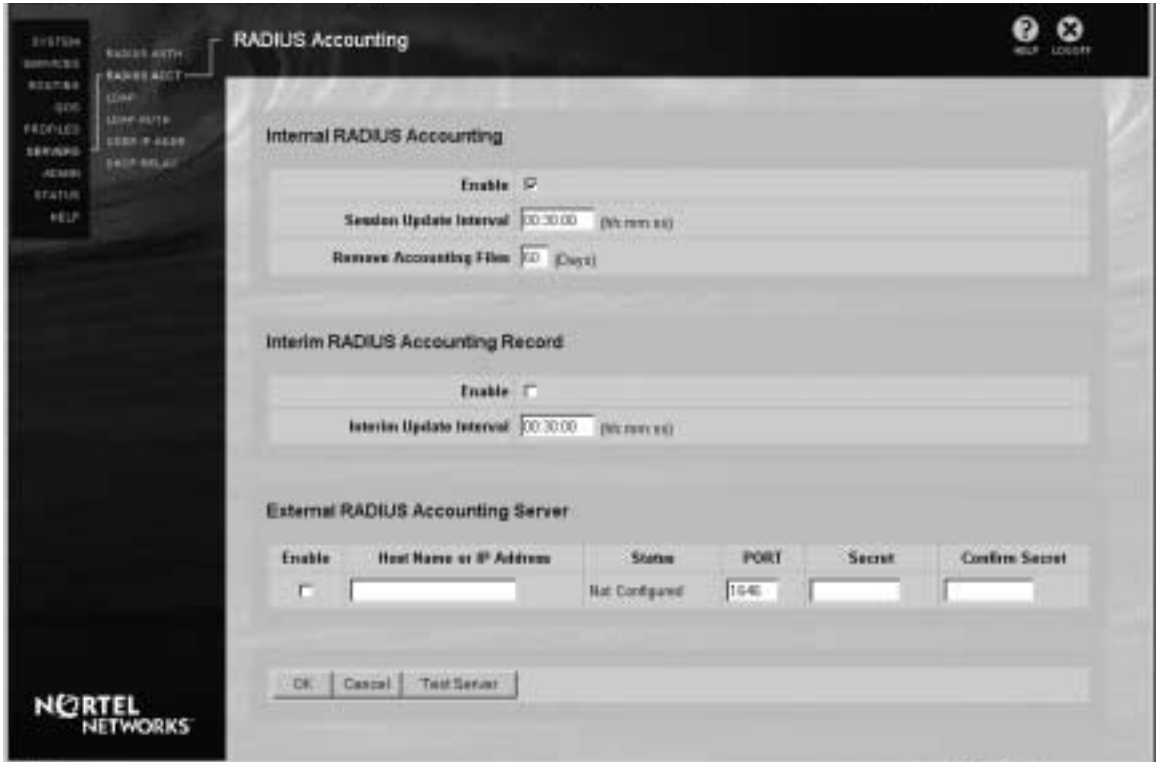
RADIUS Diagnostic Report

Use the RADIUS Diagnostic Report test to check that your RADIUS Authentication configuration is correct. The RADIUS Diagnostic Report compares the settings you have entered on the RADIUS Authentication screen to the corresponding settings that are specified on other switch configuration screens. The title of each section of the diagnostic report lists the name of the related screen. For example, the IPSec RADIUS Configuration section of the report contains information related to the Services→IPSec screen. Refer to Status→Reports for a more detailed description of the RADIUS Diagnostic Report.

RADIUS Accounting Configuration

The RADIUS Accounting configuration screen allows you to specify how your switch saves RADIUS Accounting results. By default, the results are stored locally. You can optionally also save the RADIUS Accounting information to a remote RADIUS Server.

Figure 135 RADIUS Accounting Configuration



Internal RADIUS Accounting

Enable

Click to enable or disable Internal RADIUS Accounting. Internal RADIUS Accounting is Enabled by default.

Session Update Interval

Enter an Interval when a snapshot of the current active tunnel sessions is recorded in a journal file. Use the format, hh:mm:ss, for the Interval. The journal file stores the session information until the user logs out of the tunnel session, after which the session stop record is saved on the local disk. In the event of a system crash, upon reinitialization the switch translates the journal file into a series of stop records on a per session basis. This minimizes accounting data loss. A low interval creates system overhead and requires additional processing.

The default interval is 00:10:00 (10 minutes).

Interim RADIUS Accounting Record

Enable

Click to enable or disable the Interim RADIUS Accounting Record feature. This selection is Enabled by default.

Interim Update Interval

Enter the Interval at which time interim RADIUS records are sent to the specified external RADIUS Server. Use the format, hh:mm:ss, for the Interval. A frequent interval creates system overhead which requires additional processing. The default interval is 00:10:00 (10 minutes).

External RADIUS Accounting Server

The switch can send RADIUS Accounting active session interim start and stop records to an external RADIUS Server. These interim records provide information about the currently active sessions on the switch. An administrator might use this information to evaluate switch usage, such as connection start and stop times.

You provide information identifying the external RADIUS server and specify how often the accounting information is sent to the external server.

RADIUS Server

Enable

Click Enable to specify that the switch send its accounting records to the external RADIUS Accounting Server.

Host Name or IP Address

Enter the external RADIUS Server's Host Name or IP Address. If you enter a Host Name, use a fully qualified domain name; for example Finance.mycompany.com.

Port

Enter the Server Port number that you want the RADIUS Accounting requests to use. Default is Port 1646.

Secret

Enter the external RADIUS Server's required Secret (password).

Confirm Secret

Reenter the remote server's Secret (password) to verify that you typed the password correctly.

Test Server

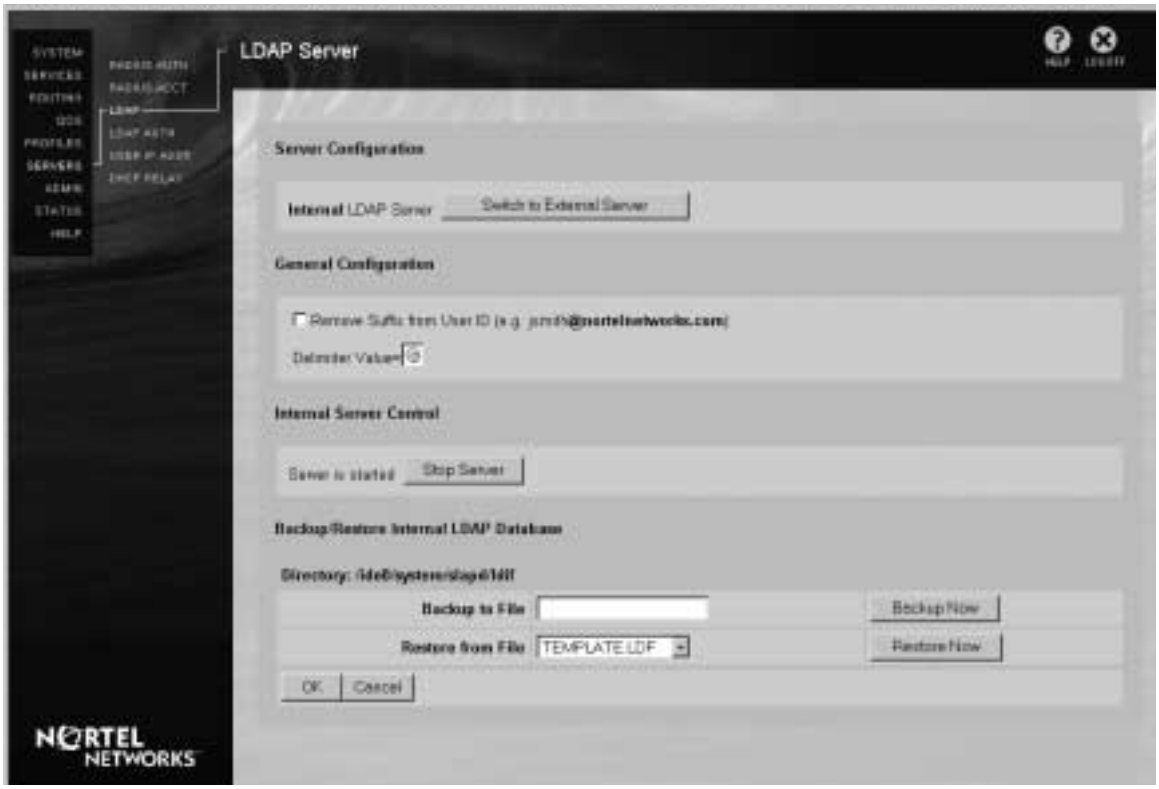
Use the Test Server button to verify the connectivity from your switch to the external RADIUS Server.

Click to test the connection to the external server. A message at the top of the screen shows the results of the test.

Internal LDAP Server

The Group and User Profiles are stored on the internal server of the switch. You can switch to an external LDAP Server.

Figure 136 Internal LDAP Server



Server Configuration

Internal LDAP Server

The Internal LDAP server is internal to the Contivity VPN Switch. If you are using more than one Contivity VPN Switch or if you are using LDAP authentication for other network services, you should consider using an external LDAP server. Refer to “External LDAP” for additional information.

Switch to External Server

Click to enable access to the External LDAP server.

Note: The internal server is disabled if you enable an external LDAP servers.

General Configuration

Remove Suffix from User ID

Click to remove the user's fully qualified ID suffix from the UID before sending it to the LDAP server. A user ID and suffix, where Bhenry is the UID and acme.com is the suffix is Bhenry@acme.com.

Delimiter Value

Specify the character that separates the suffix from the UID.

Internal Server Control

Click Stop Server or Start Server, as appropriate, when you intend to Back up or Restore a configuration, or after you have completed the restoration of a configuration.

Note: The LDAP server must be stopped before you can perform the Backup and Restore procedures.

Backup/Restore Internal LDAP Database

Directory

Shows the current directory path, which begins at the root disk drive (ide0).

Backup to File

Enter a filename (eight characters maximum) to back up the database, and click Backup Now to start the backup procedure. This procedure backs up changes to the internal LDAP LDIF file only (it writes to the LDAP Interchange Format file). The LDIF file is an intermediate database file that you can use to move data between LDAP servers.

Restore from File

Click the drop-down list box and select a file with which to restore the LDAP database, and click Restore Now.

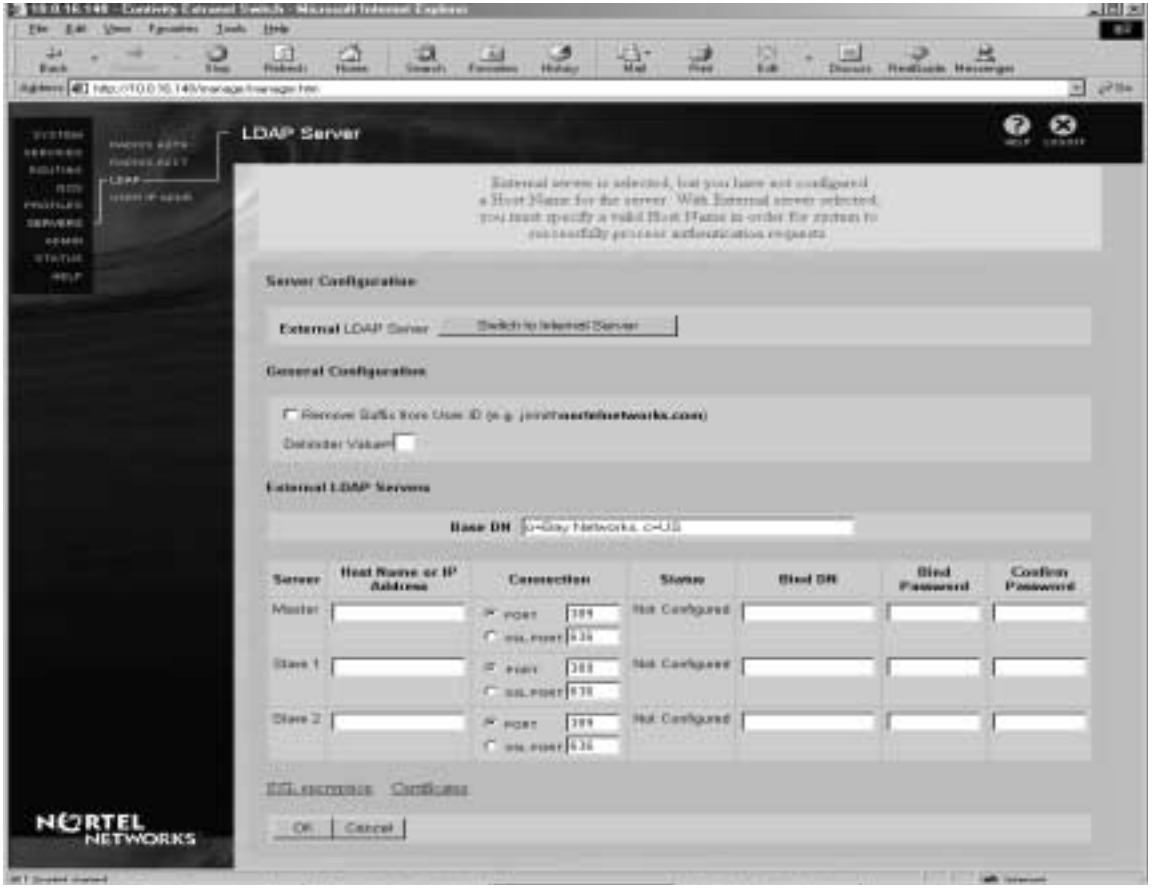
Note: Both the backup and restore processes might take extended periods of time, based on the size of the database.

Make sure the LDAP server has been stopped before performing a Backup or Restore procedure. To resume operation of the switch, you must restart the LDAP server you were running.

External LDAP

The Group and User Profiles are stored on an External LDAP servers.

Figure 137 External LDAP Server



Server Configuration

External LDAP Server

The External LDAP server allows you to configure a Master and two Slave servers. LDAP Slave servers are normally configured to be read-only. In the event that the Master is unavailable, the switch continues to check against the Slaves for authentication. Configuration writes are not possible while the Master is unavailable.

Switch to Internal Server

Click to enable access to the Internal LDAP server. The external server is disabled if you enable an internal LDAP server.

Note: Status messages appear at the top of the screen to prompt you for a required action, such as entering a valid Host Name.

General Configuration

Remove Suffix from User ID

Click to remove the user's fully qualified ID suffix from the UID before sending it to the LDAP server. You would not need the fully qualified user ID if the DNS server has been properly configured on the switch. A user ID and suffix, where Bhenry is the UID and acme.com is the suffix, is Bhenry@acme.com.

Delimiter Value

Specify the character that separates the suffix from the UID.

External LDAP Servers

Base DN

Enter a Base Distinguished Name (DN) for the servers. A distinguished name is usually in the form of:

```
ou=organizational unit, o=organization, c=country
```

For example, ou=Remote Access Users, o=General Motors, c=US

Server

The remote LDAP servers require the following specifics that are necessary for the switch to access the appropriate Master and Slave Remote LDAP servers.

Master

The Master LDAP server is the primary server to process queries. Should the Master server become unavailable, the switch attempts to initiate a connection with the Slave servers. In this case, the switch tries to reestablish authentication services with the Master LDAP server every 15 minutes, or whenever a request is made to perform a configuration write.

Note: Only the Master LDAP server has read and write access.

Slave 1

The Slave 1 LDAP server responds to queries if the Master LDAP server is unavailable. This server is read-only.

Slave 2

The Slave 2 LDAP server responds to queries if the Master LDAP server and Slave 1 are unavailable. This server is read-only.

Host Name or IP Address

Enter either the host name or IP address for the LDAP servers. These host names can be fully qualified domain names or simply names if they are in the same domain as the switch. The entry can alternatively be an IP address.

Connection

Port

Enter the associated Port number that your LDAP server listens to queries on. Port 389 is the default LDAP port number.

SSL Port

Enter the associated Secure Socket Layer (SSL) Port number that your LDAP server listens to queries on. Port 636 is the default SSL LDAP port number.

Note: If you want to use SSL, then you must enable the SSL Port. Additionally, you need to configure the SSL Encryption and Certificates screen options.

Bind DN

The bind distinguished name (DN), which is the LDAP equivalent of a user ID, is required to access the Base DN and its subentries; for example,

```
cn=Directory Manager
```

Leave this field blank if your LDAP server allows anonymous access.

The LDAP server must allow read access for the base DN and all its subentries to authenticated connections that are using this bind DN. It must also allow write access for the master server.

Bind Password

Enter a password of up to 32 characters. The password allows the switch to prove its identity (the bind DN) to the LDAP server.

SSL Encryption

This hyperlink brings you to the LDAP server SSL Encryption screen. This allows you to select the encryption types the switch uses during negotiation with the external LDAP server. If the external LDAP server does not support one of the selected encryption types, then the connection is not established.

Certificates

This hyperlink brings you to the LDAP server Certificate Configuration screen. This allows you to select the Certificate Authorities (CA) that are trusted to sign the external LDAP server certificates. SSL connections established to an external LDAP server whose certificate is not signed by one of the trusted CAs are dropped.

LDAP Authentication

You use the Servers→LDAP Authentication screen to configure the External LDAP Authentication Server.

Figure 138 LDAP AUTH screen

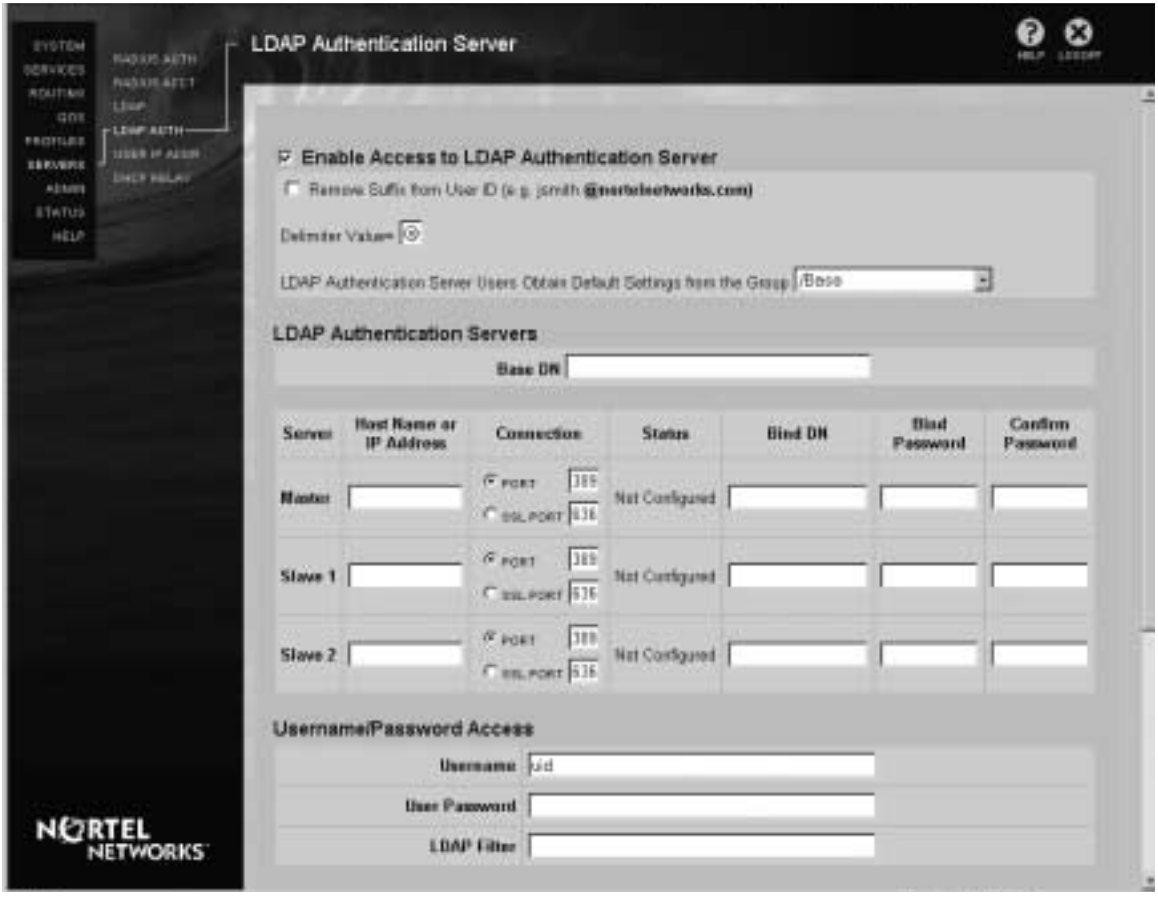


Figure 139 LDAP AUTH screen - continued

Enable Access to LDAP Authentication Server

Check this box to enable access to external LDAP Authentication servers. This is disabled by default.

Remove Suffix from User ID

Click to remove the user's fully qualified ID suffix from the UID before sending it to the LDAP server. You would not need the fully qualified user ID if the DNS server has been properly configured on the switch. A user ID and suffix, where Bhenry is the UID and acme.com is the suffix, is Bhenry@acme.com.

Delimiter Value

Specify the character that separates the suffix from the UID.

Specify default Group to which users are assigned:

This dropdown list contains the names of all Groups. Select the default group to which users are assigned. The /Base group is selected by default.

LDAP Authentication Servers

Base DN

Enter a Base Distinguished Name (DN) for the servers. A distinguished name is usually in the form of:

```
ou=organizational unit, o=organization, c=country
```

For example, ou=Remote Access Users, o=General Motors, c=US

Server

The remote LDAP servers require the following specifics that are necessary for the switch to access the appropriate Master and Slave Remote LDAP servers.

Master

The Master LDAP server is the primary server to process queries. Should the Master server become unavailable, the switch attempts to initiate a connection with the Slave servers. In this case, the switch tries to reestablish authentication services with the Master LDAP server every 15 minutes, or whenever a request is made to perform a configuration write.

Note: Only the Master LDAP server has read and write access.

Slave 1

The Slave 1 LDAP server responds to queries if the Master LDAP server is unavailable. This server is read-only.

Slave 2

The Slave 2 LDAP server responds to queries if the Master LDAP server and Slave 1 are unavailable. This server is read-only.

Host Name or IP Address

Enter either the host name or IP address for the LDAP servers. These host names can be fully qualified domain names or simply names if they are in the same domain as the switch. The entry can alternatively be an IP address.

Connection

Port

Enter the associated Port number that your LDAP server listens to queries on. Port 389 is the default LDAP port number.

SSL Port

Enter the associated Secure Socket Layer (SSL) Port number that your LDAP server listens to queries on. Port 636 is the default SSL LDAP port number.

Note: If you want to use SSL, then you must enable the SSL Port. Additionally, you need to configure the SSL Encryption and Certificates screen options.

Bind DN

The bind distinguished name (DN), which is the LDAP equivalent of a user ID, is required to access the Base DN and its subentries; for example,

```
cn=Directory Manager
```

Leave this field blank if your LDAP server allows anonymous access.

The LDAP server must allow read access for the base DN and all its subentries to authenticated connections that are using this bind DN. It must also allow write access for the master server.

Bind Password

Enter a password of up to 32 characters. The password allows the switch to prove its identity (the bind DN) to the LDAP server.

Username/Password Attributes

These fields can hold case insensitive character strings which are allowable in LDAP search filters. The default value for each field is blank. Without a specified value, external LDAP authentication is unable to access these fields and therefore will not successfully access any user entry, which will result in authentication failure.

Username

Specify the attributes used in the LDAP directory user entries for Username.

Password

Specify the attributes used in the LDAP directory user entries for Password.

LDAP Filter

Enable additional policy checking by specifying an LDAP search filter.

This field can hold a case-insensitive character string which forms an allowable LDAP search filter. The default value for this field is blank. Without a specified value, External LDAP Authentication will not perform any additional policy checking.

User Policy Attributes

Specify the attributes used to store the Contivity Group, static IP address, IP netmask, and customized user filter.

These fields can hold case-insensitive character strings which are allowable in LDAP search filters. The default value for each field is blank. Without a specified attribute name, external LDAP Authentication will not attempt to extract this information.

Contivity Group Assignment

Specify the attributes used in the LDAP directory user entries for the Contivity Group assignment.

Assigned IP Address

Specify the attributes used in the LDAP directory user entries for the assigned IP address.

Netmask

Specify the attributes used in the LDAP directory user entries for the Netmask.

Personal Filter

Specify the attributes used in the LDAP directory user entries for the personal filter.

Response Timeout Interval

Select a Response Timeout Interval, in seconds, from the list box. If the LDAP Authentication server does not respond within the specified timeout interval, the authentication will fail. The default value is 4 seconds.

SSL Encryption

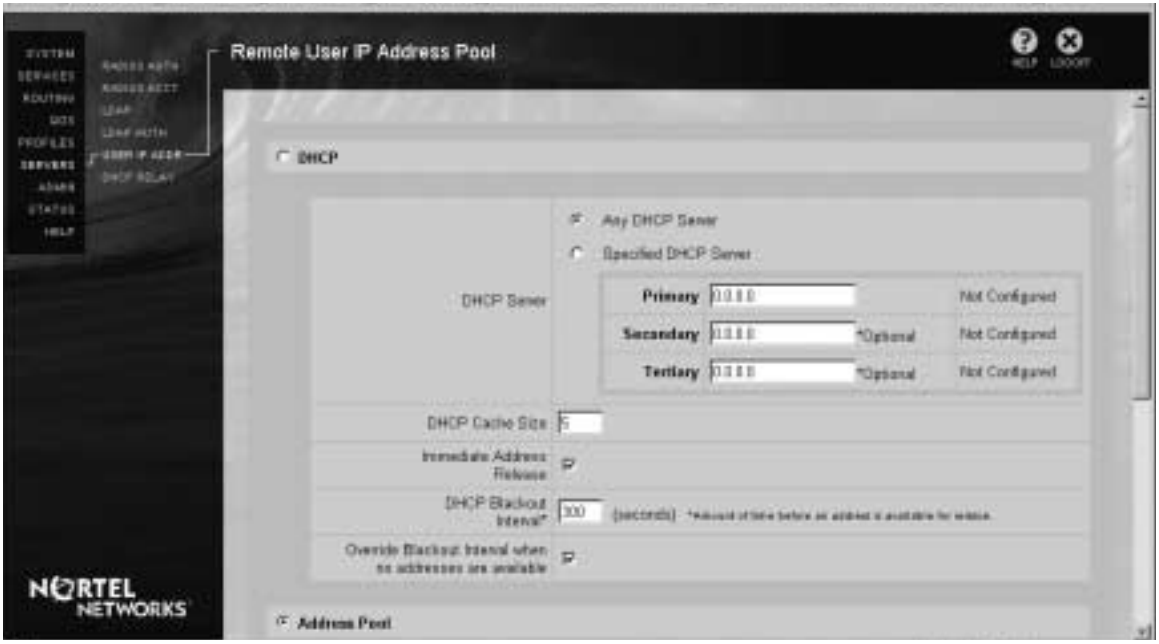
This hyperlink brings you to the LDAP server SSL Encryption screen. This allows you to select the encryption types the switch uses during negotiation with the external LDAP server. If the external LDAP server does not support one of the selected encryption types, then the connection is not established.

Remote User IP Address Pool

The Remote User IP Address Pool (Servers→User IP Addr) screen allows you to select a method for users to obtain IP addresses for access to the private network. These addresses are serviced by the switch and are available to remote users accessing the switch on demand. You can choose to have IP addresses assigned from one of the following:

- External Dynamic Host Configuration Protocol (DHCP) pool
- Internal Address Pool

Figure 140 Remote User IP Address Pool



DHCP

Click to enable an external DHCP server to provide addresses for the address pool. A DHCP server on the private LAN segment dynamically assigns IP addresses on behalf of remote users. You must have an existing DHCP server in your environment to choose this option.

The DHCP server are contacted by a broadcast or unicast (depending on the option selected) DHCP request through the network adapter associated with the Management IP address.

Any DHCP Server

Click to allow any available DHCP server to provide the requested IP addresses. Any DHCP Server is the External DHCP default selection.

Specified DHCP Server

Click to allow IP addresses to be provided from a Specified DHCP Server only. Indicate the IP addresses of the servers that provide DHCP service, including:

- Primary
- Secondary
- Tertiary

A status field provides information on the associated servers. Configuring a Secondary or Tertiary server is optional.

DHCP Cache Size

The switch obtains a number of IP addresses from DHCP servers. These IP addresses are maintained in a local DHCP cache. The DHCP Cache Size is the number of IP addresses that is held in the switch's cache. The minimum number of IP addresses held is five, and the maximum is derived from the maximum number of tunnel sessions that the switch supports.

DHCP Blackout Interval

Enter the amount of time in seconds that a DHCP address is held in a blackout state before it is returned to the DHCP server or the DHCP cache.

Immediate Address Release

When a tunnel session terminates, the switch can either release the inner IP address back to the DHCP server or retain it for use by a new tunnel session. Click Immediate Addresses Release to have the switch release the IP addresses back to the DHCP server immediately. If you have a limited number of IP addresses available, then you should enable this option.

IP addresses from disconnected tunnel sessions remain unavailable for the time you specify (300 to 7200 seconds). This delay prohibits immediate reuse by another user that could represent a security risk.

Address Pool

If you want to share all IP addresses among all users, just use Default pools. If you want to assign some addresses to certain users and groups, you can name your ranges and assign that named range to a groups.

Click on Address Pool to use the internal Address Pool, which appears on this screen. These addresses are held by the switch and are available to clients on demand. Make sure that you populate the local address pool with enough addresses that are not used by other devices on your network. You can create multiple address pools with different ranges of addresses, and you can have multiple address ranges for the same address pool.

Note: If you attempt to delete an address pool that is in use, a message informs you that it is currently being used.

Pools

You can create a default address pool from which users are assigned an IP address dynamically.

Alternatively, you can click Add to name a specific IP address pool. Refer to the Remote User IP Address Pool Add screen for additional information.

Start/End

Shows the first and last IP address for this group of addresses in the local pool.

Subnet Mask

Shows the Subnet Mask for the for the range of pool IP addresses.

Total

Shows the total number of IP addresses in this group of addresses.

In Use

Shows how many of the total number of IP addresses in this pool are currently in use and therefore unavailable.

Action

Click Delete to remove a group of IP addresses.

Click Add to create a new Internal IP address pool.

Address Pool Blackout Interval

Enter the amount of time (0 to 7200 seconds) that an IP address from disconnected tunnel sessions remain unavailable. This delay prohibits immediate reuse by another user that could represent a security risk. Set this number to zero to allow the address to be immediately reissued.

If Named Pool Unavailable

This parameter specifies the action the switch takes if a user requests an address from a named pool and there are no addresses available.

Failover to Default Pool

Click to have the request for an IP address serviced by the Default IP address pool when there are no IP addresses available in a requested pool.

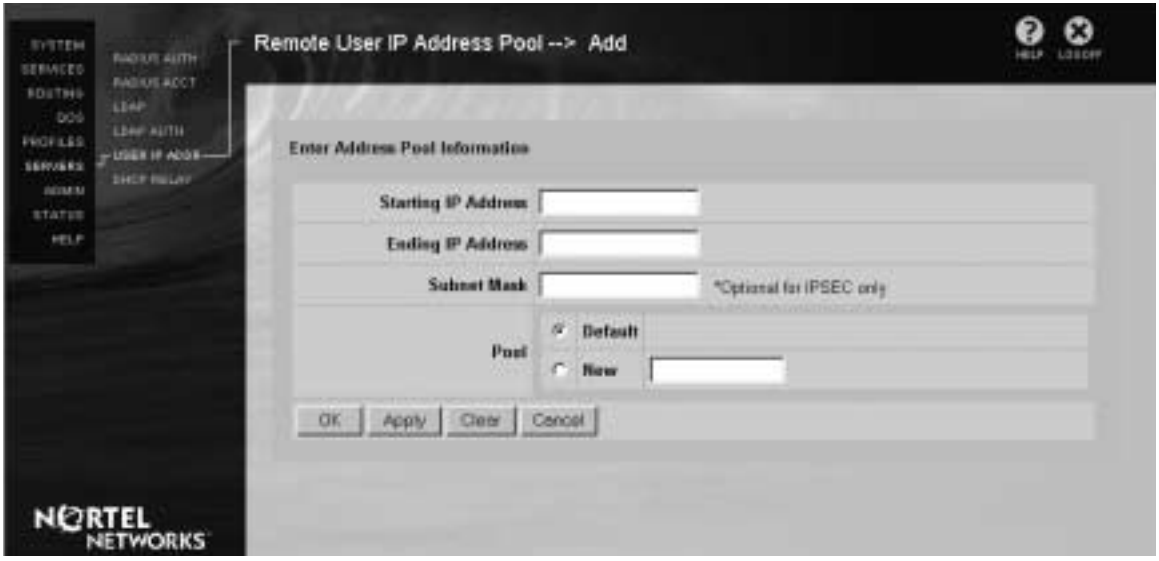
Deny Address Request

Click to deny an IP address when there are no IP addresses available in a requested pool. In this case, the request is denied and the tunnel is not established.

Remote User IP Address Pool Add

Use the Add button in the Address Pool section of the Remote User IP Address Pool screen to access this screen. Enter the necessary Starting and Ending IP Addresses on this screen. Then designate the pool as either default, an additional range of addresses to an existing pool, or a newly named pool.

Figure 141 Internal Address Pool Add



Starting/Ending

Enter the first and last IP addresses for this group of addresses in the pool.

Avoid IP address pool conflicts

When supplying an address pool, make sure that none of the pool addresses are the same as those used for the LAN interfaces or the Management interface IP address. Also, the switch does not check the IP address supplied by a PPTP client to see if it has been assigned to a LAN interface, Management interface, or address pool.

The Use Client-Specified Address option is disabled by default. To avoid potential conflicts, you can verify the current state of the Use Client-Specified Address option from the Profiles→Groups→Edit→Configure PPTP screen.

Subnet Mask (optional)

This field is applicable to IPSec users only. Enter the Subnet Mask for the pool of IP addresses that you are configuring. You can later edit the Subnet Mask as necessary.

Pool

You can designate the Pool as Default, Existing, or New.

Default

Click to designate this pool as the switch's Default IP address pool.

Existing

Click to change the subnet mask or name of an existing pool. If you want to edit the IP addresses of an existing pool, you must either delete the pool (if not in use) or click Add and then associate this new pool with an existing pool.

New

Click to create a new IP address pool and then name the pool.

Action

Click OK to save the entries for the IP address pool and return to the Remote User IP Address Pool screen.

Click Apply to save the entries for the IP address pool and remain at the current screen.

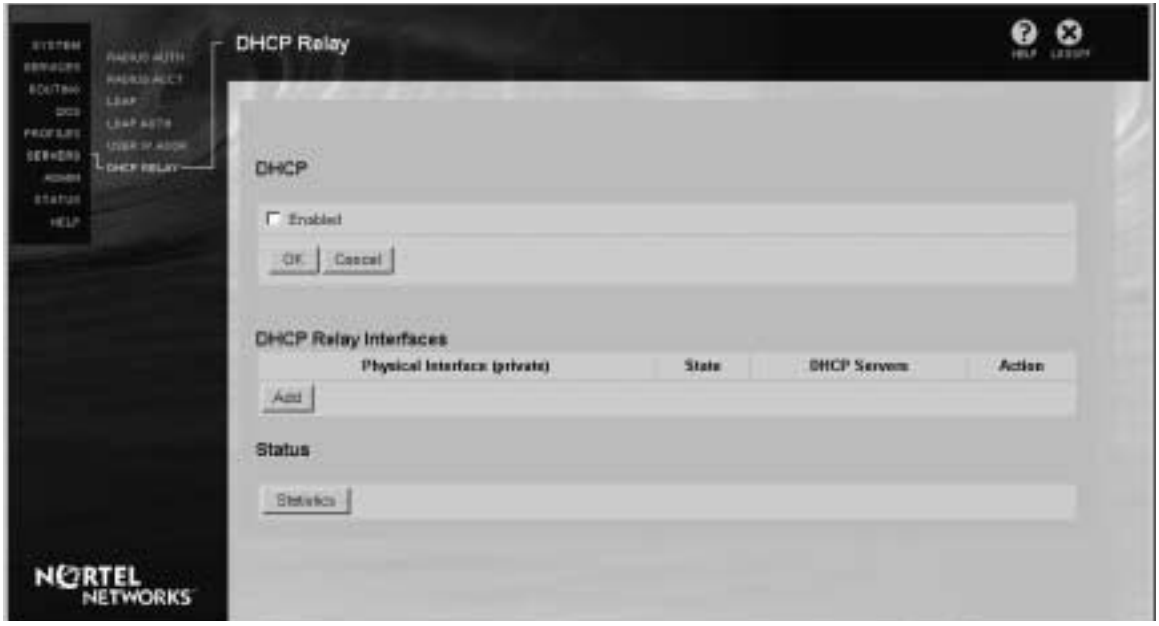
Click Clear to clear the entries on the screen.

Click Cancel to return to the Remote User IP Address Pool screen. Any unsaved entries are lost.

DHCP Relay

The DHCP relay agent on a switch forwards DHCP and BOOTP messages between a server and a client on different subnets. When a locally attached host issues a DHCP or BOOTP request as a broadcast message, the switch will relay the message to a specified DHCP or BOOTP server. DHCP relay agent also forwards DHCP replies from server to client.

Figure 142 Servers→DHCP Relay



DHCP

Enable

Check the Enable checkbox to enable the DHCP Relay agent. When DHCP relay is enabled, the switch forwards DHCP relay messages between client and server.

Note: DHCP relay agent can run only on all the private physical interfaces and tunnels.

DHCP Relay Interfaces

This section of the screen shows the current DHCP Relay configuration. This includes the Physical Interface where it will *receive* DHCP messages. The DHCP Relay agent will ONLY listen on those interfaces with DHCP relay enabled.

Physical Interface (private)

Shows the private IP Address of the private physical interface.

State

Shows the current state of the server, enabled or disabled.

DHCP Servers

DHCP Servers configuration for Physical/Tunnel Interface: Specified DHCP Servers: DHCP relay agent will unicast DHCP packet ONLY to the specified servers (up to 3).

Action

Edit

Click Edit to edit the associated DHCP configuration.

Delete

Click Delete to remove the associated DHCP configuration.

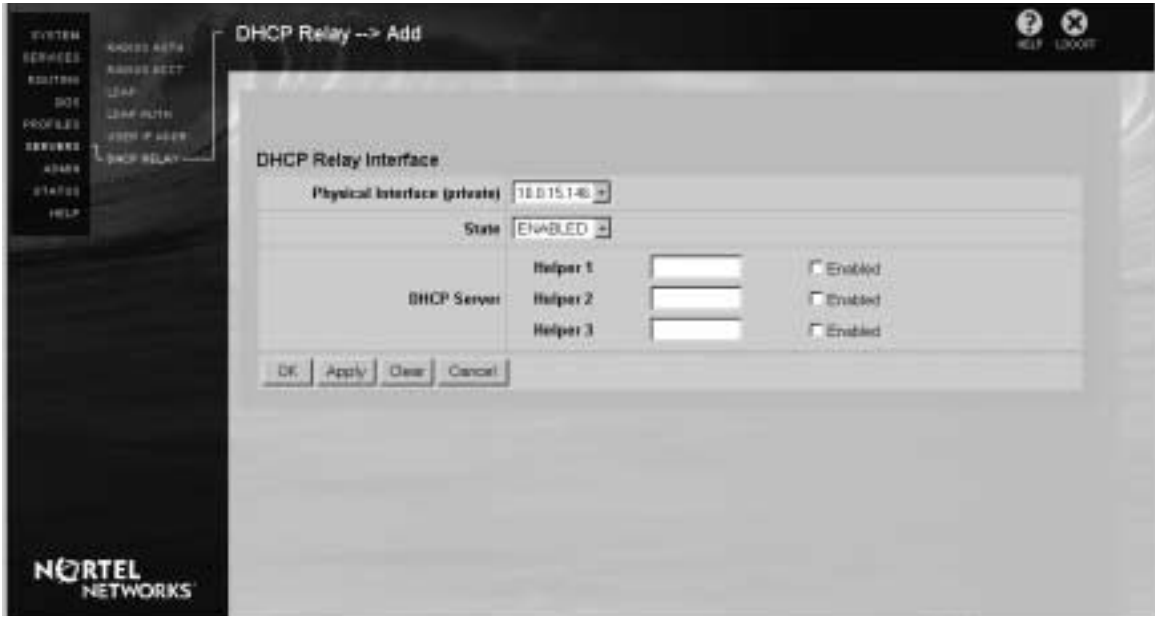
Enable/Disable

Use the Enable and Disable buttons to toggle the state of the associated DHCP configuration.

Add

Click the Add button to configure a new DHCP Relay server. The DHCP Relay→Add screen appears.

Figure 143 Servers→DHCP Relay→Add



Physical Interface (private)

Select the Physical Interface from the list of existing private interfaces.

State

Enable or disable the DHCP Relay agent by choosing from the list.

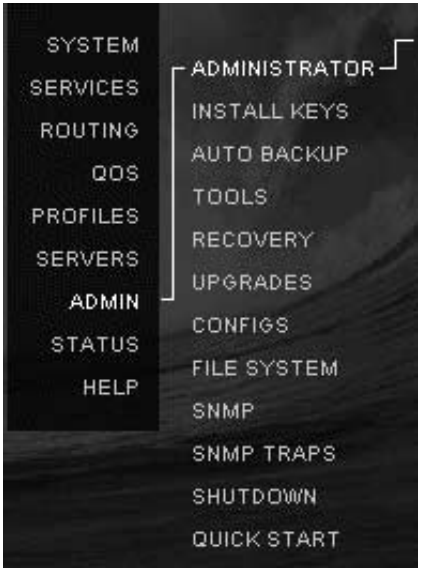
DHCP Servers

The DHCP relay agent will unicast DHCP packets *only* to the specified Helper servers (up to 3). Server 1 address is required. Server 2 and Server 3 addresses are optional. Additionally, you can enable and disable each DHCP server by checking or unchecking the Enable checkbox.

Chapter 7
Administration

This section describes Administration tasks that are central to operating the switch. These tasks provide details on scheduling backups, upgrading the software image, saving configuration files, performing file maintenance, creating recovery diskettes, and shutting down the system.

Figure 144 Administration menu



Also, links allow you to access either the Quick Start Configuration or the Guided Configuration.

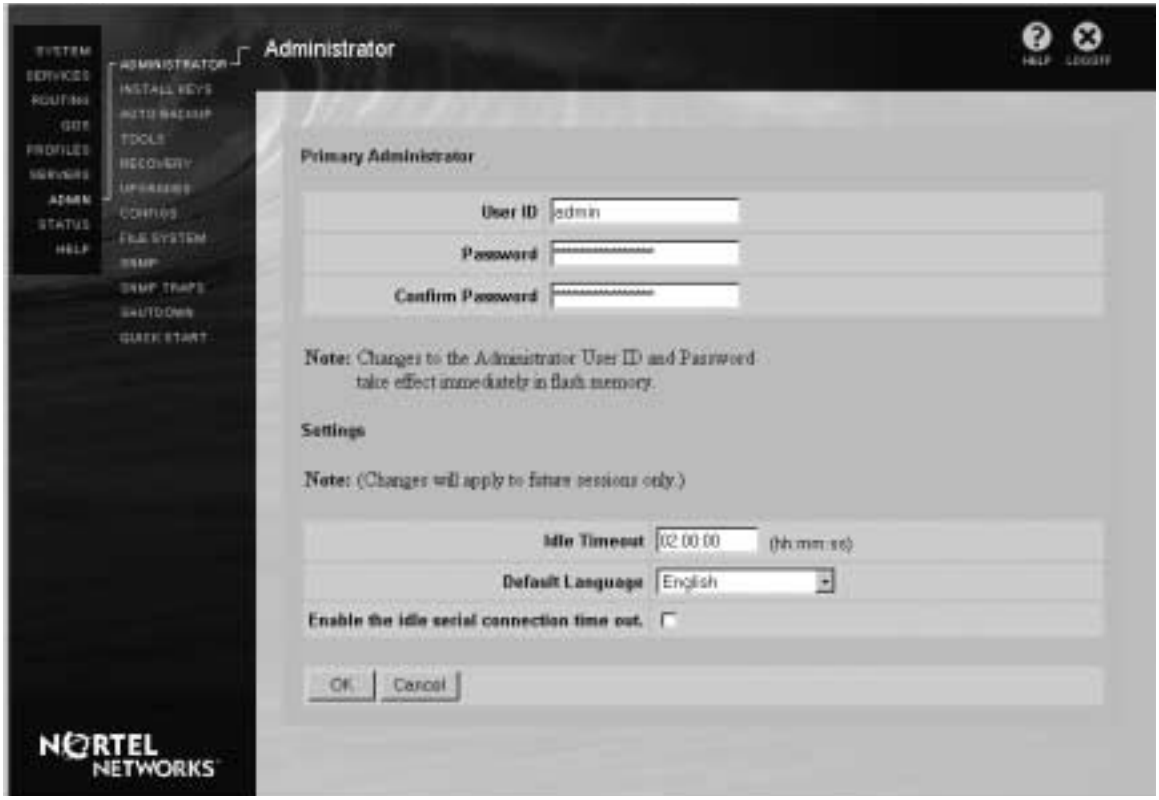
Administrator Settings

The Administrator Settings screen allows you to change the Primary Administrator User ID (UID) and Password. It also controls the Administrator Idle Timeout Setting for all administrators, the default language, and serial port settings.

There can be only one Primary Administrator. The Primary Administrator User ID and Password combination provides the person with this information access to all screens and control settings. The Primary Administrator User ID and Password are also used to access the serial port and the recovery disk.

Note: The Primary Administrator UID and Password are only saved during a system shutdown. Therefore, when you set these parameters you must implement an Admin→Shutdown to save the new settings. Doing a Reset (using the Reset Button on the back of the switch) does not store the parameters.

Figure 145 Administrator Settings



Primary Administrator

User ID

Enter an appropriate user ID for the Primary Administrator. The person using this UID has permission to modify and view all control settings in the switch, including the serial port and the recovery disk.

Password

Enter an appropriate Password for the Primary Administrator.

Caution: Do not lose or forget this Password. Losing or forgetting your Password requires you to return the switch to Nortel Networks for reconfiguration to default settings. All settings and backups are lost. There is no way to access the system without the Primary Administrator Password.

Settings

Idle Timeout

This option allows you to configure a timeout period after which the ID and Password dialog box appears if no interaction with the switch has taken place. This feature helps prevent someone from accessing and modifying the switch from an administrator's Web console that has been left unattended.

The default Idle Timeout is 00:15:00 (15 minutes); the range is 00:15:00 to 23:59:59.

Note: If the Idle Time-out on the switch logs off the Client, and the Client has Client Failover configured on the Services→IPSec screen, that client then fails over to the defined failover server, rather than being disconnected as desired.

Note: An option has been added to the Contivity VPN Client to disable keepalives between the switch and the client. This option enables you to disable keepalives when tunneling over an ISDN link, since the link is not always active. If an Idle Time-out has been set on the switch, and keepalives have been disabled on the client, the client might not receive notice that the connection has been closed (due to the Idle Time-out), when the physical ISDN connection is not active.

Default Language

Select the language that you want to use for your switch's GUI. The switch supports English and Japanese.

Using Japanese

To display the Japanese screens properly, your Web browser must support Kanji characters. Refer to your browser's documentation for additional details.

The following browsers have been tested and found to provide this support.

- Netscape Navigator, Version 4.0 or later
- Japanese version of Microsoft Internet Explorer, Version 4.0 or later

When you select Japanese, your switch's GUI is converted from English to Japanese Kanji characters. However, the following types of information are *not* translated into Japanese:

- Text that is entered by a user
- Information from one of the switch's databases
- Online Help

Note: After you change your switch's language selection, click on your browser's Refresh button (Internet Explorer) or Reload button (Netscape) to update the browser's screen to the new language.

You may notice that some screens appear in English even though you have selected Japanese. These screens were added after the last Kanji translation was done and will always appear in English.

Enable the idle serial connection time out

Check this box to

Install Keys

Use the Admin→Install Keys menu item to install licensing keys that enable optional software functionality.

Key Installation

Feature

The Feature column lists optional features that are currently available.

Key/Status

Enter the key that you obtained from your Nortel Network's sales representative in this text box and click OK. The key must be entered exactly as it is given.

When a valid key is installed the label “Key Installed” appears in this column.

Delete

Click Delete to remove the key. A confirmation page appears. Click Yes to confirm key removal.

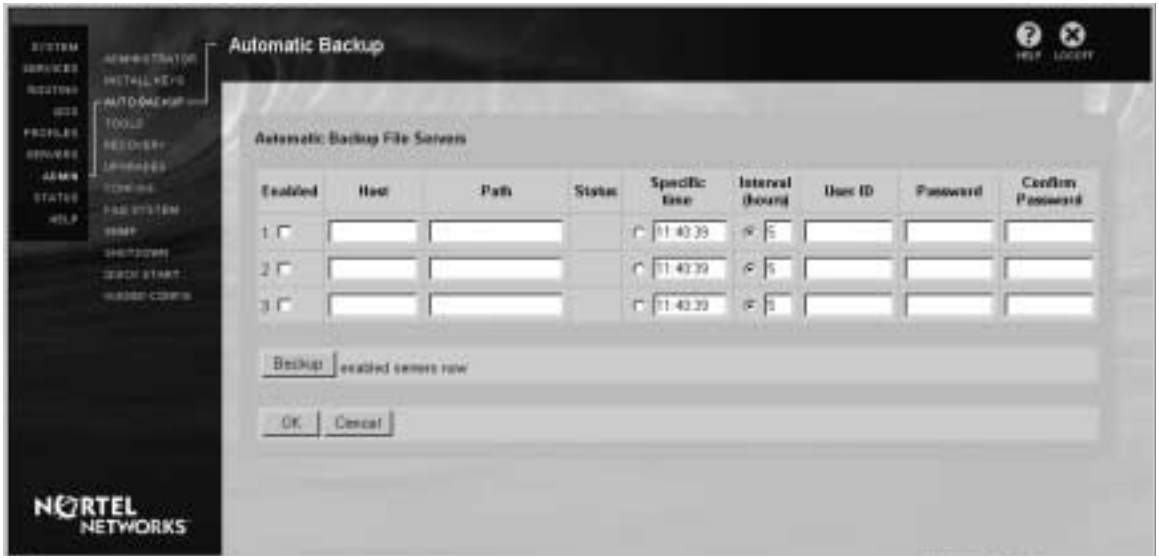
Automatic Backup

The Automatic Backup screen allows you to configure regular intervals or specific times when your system files are saved to designated host backup file servers. You can designate up to three backup file servers.

You should configure Automatic Backups immediately so that you do not lose system or configuration information in case of problems.You configure the Automatic Backup servers from the Admin→Automatic Backup screen.

The switch does not begin a backup for at least 5 minutes after rebooting. This time period is to allow all resources to start operating. This delay occurs even if you go into the Admin→Auto Backup screen and request that a backup be started immediately; it is delayed until after the 5-minute period.

Figure 146 Automatic Backup



Note: After entering the Automatic Backup File Servers information, click on the screen and press the keys Alt and Print Scrn (Screen) to save the screen image to a buffer. Next, paste the image into a file (for example, into Microsoft Word) and keep it as a record of the backup file servers that you are using.

Restoring Configurations

If you want to save a certain configuration for a later date, you must realize that there are two components that define a given configuration: the configuration file and the LDAP database.

Saving a configuration from the Admin→Configs screen Save Current Configurations option saves only the operational parameters in the configuration file, such as interface IP addresses and subnet masks, backup host IP addresses, and DNS names.

To completely save the Contivity VPN Switch configuration on the internal LAN server, you must also save the LDAP database, which contains the group and user profiles, filters, backup file names, and more. Go to the Servers→LDAP screen and click Stop Server. Next, enter a file name in the Backup/Restore LDAP Database field. Note that you should conform to the eight-dot-three MS-DOS* naming convention and append the file name with .ldf; for example, LDAPOne.ldf.

Automatic Backup File Servers

Enabled

Click to Enable the associated Host Backup File Server.

Host

Enter the Backup File Server Host name or IP address.

Path

Enter the Backup File Server Path, for example:

```
Building3/Switch_backups
```

Specific Time

Select this option to execute the backup at a specific time. Enter the time at which you want the backup to occur.

Interval

Select this option to execute the backup at certain intervals of time. Specify in hours the time period after which the system automatically backs up changed files to the backup file server. The minimum interval is 1 hour, and the maximum is 8064 (336 days); the default is 5 hours.

User ID

Enter the user ID that is required for FTP login to the backup file server.

Password

Enter the Password that is required for FTP login to the backup file server.

Confirm Password

Reenter the Password that is required for FTP login to the backup file server.

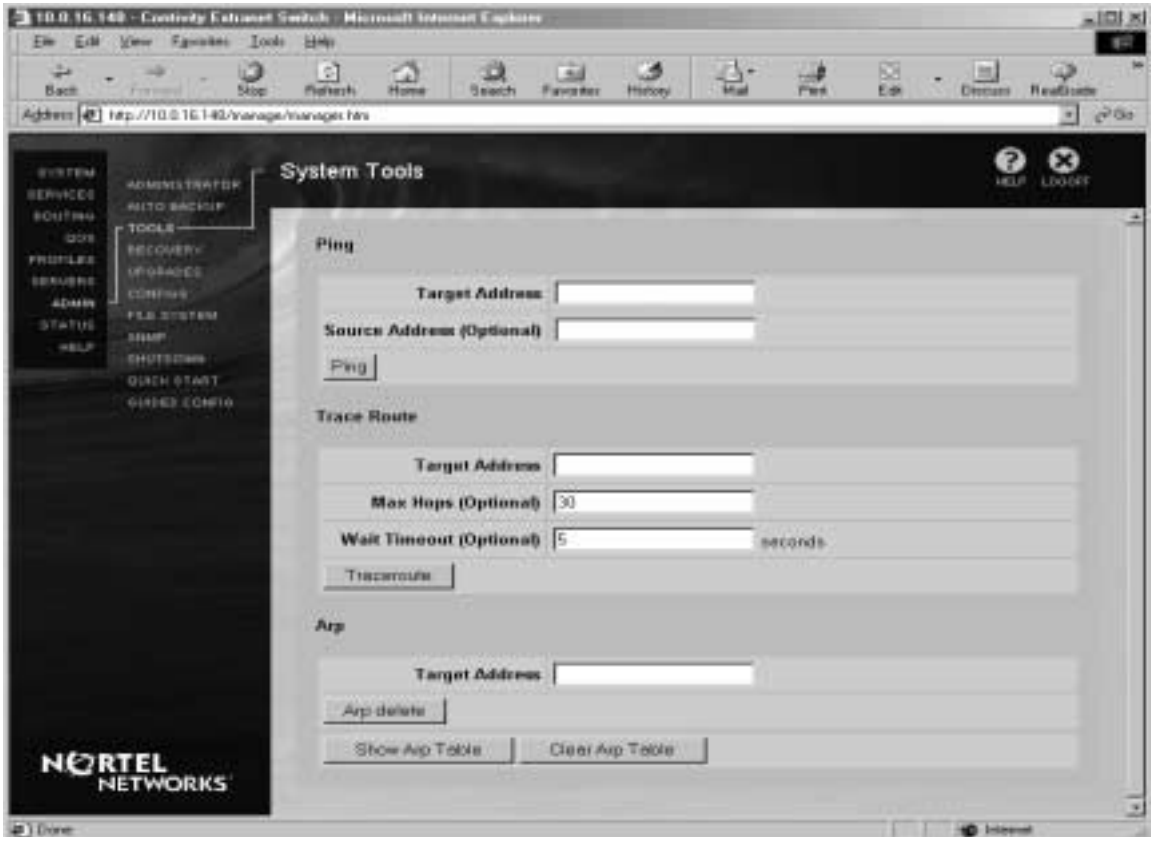
Backup

Click to execute a backup to each enabled server now. This action also synchronizes the hard disk drives when there is more than one in a device. Otherwise, the hard disks synchronize automatically every 60 minutes.

Tools

The Tools screen provides utilities for checking connectivity.

Figure 147 Admin→Tools



Ping

The ping command generates an ICMP echo-request message, which is sent by any host to test node reachability across a network. The ICMP echo-reply message indicates that the node can be successfully reached.

Target Address

Enter the IP address that you want to ping.

Source Address (Optional)

You can optionally enter the address that you are pinging from.

Ping

Click the Ping button to execute the ping.

Traceroute

The traceroute command is a tool used for measuring a network round-trip delay. Messages are sent per hop and the wait occurs between each message. It takes the maximum hops (30) x the wait timeout (5) x 3 seconds for the traceroute to time out if the address is unreachable.

Target Address

Enter the IP address whose route you want to trace.

Max Hops (Optional)

You can optionally enter a maximum number of hops to which to limit the traceroute.

Wait Timeout (Optional)

Enter an optional Wait Timeout value in this field to limit timeouts.

Traceroute

Cling the Traceroute button to execute the traceroute.

ARP

The Address Resolution Protocol (ARP) dynamically discovers the low level physical network hardware address that corresponds to the high level IP address for a host. ARP is limited to physical network systems that support broadcast packets that can be heard by all hosts on the network.

Target Address

IP address of system for which you want to delete ARP table entries.

ARP delete

Clicking on this button deletes the specified entry from the ARP table.

Clear ARP Table

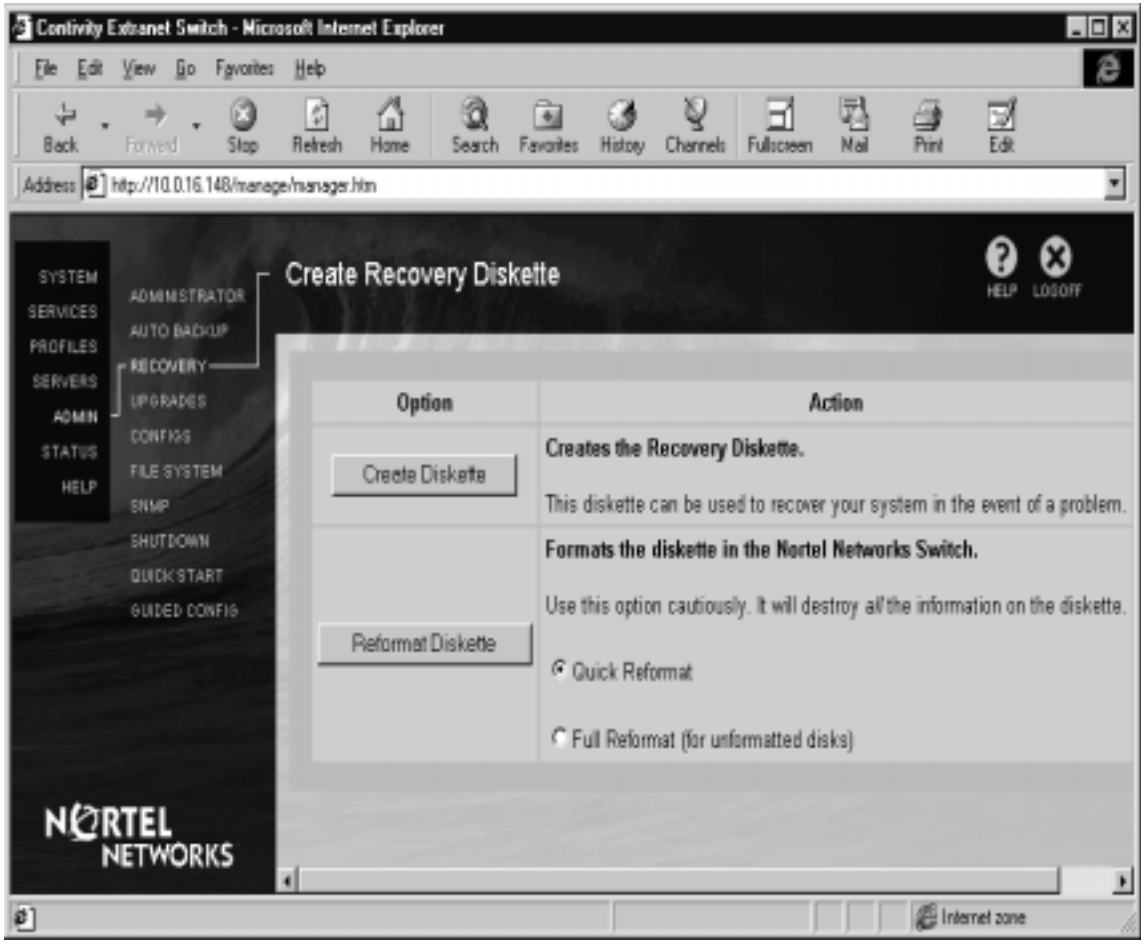
Clicking on this button clears all of the existing ARP table entries.

Recovery

The Recovery screen allows you to create a recovery diskette that can enable you to restore the software image and file system to the hard drive of the switch in the unlikely event there is a hard disk crash. The Recovery diskette is included with your switch. You can also use this screen to create additional copies of the Recovery diskette, as well as to reformat a diskette.

Note: The Recovery diskette cannot be used for the Contivity 1000 due to the lack of a floppy drive in the unit. The Contivity 600 also does not have a floppy drive, but the recovery image is stored in PROM; you can invoke it by pressing a switch on the back of the unit. Refer to *Configuring the Contivity VPN Switch* for more information.

Figure 148 Create Recovery Diskette Display



Creating Recovery Diskette

Create Diskette

Creates the Recovery Diskette that is used to restore the file system on the switch's hard drive in the unlikely event of a hard disk problem. This process creates a boot sector on the diskette, and copies the system software files that are necessary to boot the switch using the diskette.

When the Recovery Diskette creation is complete (approximately 2 minutes), a message appears at the top of the screen indicating success or failure. In case of a failure, follow the instructions in the user messages provided by the switch.

Reformat Diskette

Formats the diskette in the switch. Use this option cautiously; it erases all of the information on the diskette.

The options follow:

- Quick Reformat (default for previously formatted diskettes) - Rewrites header files and existing data.
- Full Reformat (for unformatted diskettes) - Creates the data sectors that comprises the storage space.

The system prompts you to verify that you intend to reformat the diskette.

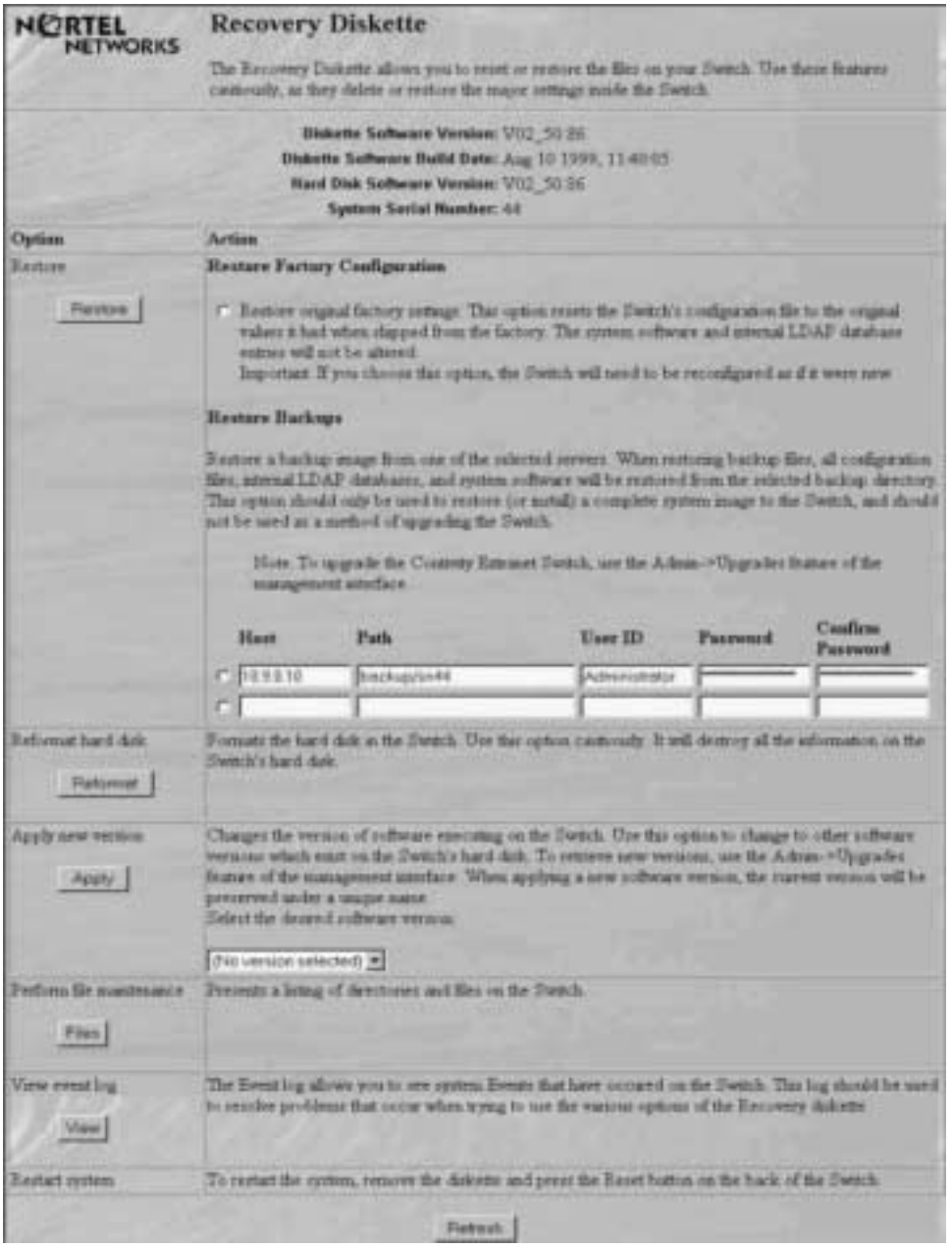
Using the Recovery Diskette

Remove the switch's front cover (refer to your switch's *Getting Started Guide* for instructions). Insert the recovery diskette into the drive and press the Reset button on the back of the switch. This supplies the switch with a minimal configuration utility that allows you to view the switch from a Web browser.

At your Web browser, enter the Management IP address of your switch. The Recovery Diskette screen appears, which allows you to:

- Restore the factory default configuration or the backup configuration.
- Reformat the switch's hard disk.
- Apply a new software version to the switch.
- Perform file maintenance.
- View the Event log.

Figure 149 Recovery Diskette



Restore

Restore to Device

Select the hard disk drive to which you want to restore the system files; either ide0 (drive 0) or ide1 (drive 1).

Restore Factory Configuration

Click Restore Factory Configuration, then click Restore to return the switch to its original factory default configuration. This erases data contained in flash memory and also in the configuration file.

Caution: Selecting this option requires you to rebuild your entire switch configuration again from scratch.

An online message specifies the result of the Factory Configuration reset action.

Restore Backups

Click to restore the switch's previously backed-up configuration. If you previously chose to automatically backup (refer to "Automatic Backup") the file systems, then the Backup Server Host (or IP address) and Path Name, User ID, and Password appear in the table.

Click the radio button of the preferred backup server. The backed-up file system, including software image and configuration files from the latest backup copy residing on the designated server, is restored onto the hard drive of your switch.

You can use the same backup server for multiple switches. Each switch creates a unique directory based on its serial number. The following example shows the Host, Path, and Serial Number (where the serial number [SN] is five digits):

```
C:/software/backup/v101/SN01001
```

Refer to the example in "Automatic Backup File Servers" for additional details on the directory, host, path, and serial number string.

Backup Server and Serial Number

The Serial Number is used to differentiate backup configurations from multiple switches that are saved on the same backup server. The Serial Number uniquely identifies each switch's backup data.

A blank row in the server backup field always appears to allow you to manually enter a backup server in case you did not configure automatic backup server locations.

Alternatively, a new factory default software image and file system can be restored to the switch's hard disk. Specify the name or address and path of the network file server onto which the software from the Nortel Networks CD has been installed.

Note: This restores the disk to an operable but "clean" condition (configuration values are at factory defaults).

To view your switch's Serial Number when the switch is operational, click Status→System from the Navigational Menu. The Serial Number is also listed on the bar code label on the back of the switch.

Reformat Hard Disk

Click to Reformat your switch's Hard Disk. Following are instances when you might need to Reformat the Hard Disk:

- If you have problems restoring your configuration that are not caused by the network or the file/backup server from which the file restoration is being retrieved
- If you want to reconfigure the switch from scratch
- If you install a new disk

Caution: Selecting this option completely wipes out anything that previously resided on the hard disk.

An online message indicates whether the Reformatting of the Hard Disk was successful.

Apply New Version

Click the drop-down list box to view the available software image and file systems that are currently stored on the hard disk. Select the image version that you want to activate.

This selection is applicable if you have more than one version of software available on the switch.

Perform File Maintenance

Click Files to bring up the File Maintenance screen, which allows you to view the entire hard disk file system.

View Event Log

Click View to display the Event Log beneath the Recovery Diskette screen. This is especially useful if a Restore operation fails.

Set Boot Disk

Click the drop-down list box to select the hard disk drive from which you want to boot the switch; either ide0 (drive 0) or ide1 (drive 1). Then click Set.

Synchronize Disks

Click Synchronize to immediately synchronize the primary and secondary disks. Thereafter, the disks automatically synchronize every hour.

Upgrade System Boot Software

Click the drop-down list box to select a drive onto which you want to update the system boot software. Click Upgrade to rewrite the boot software onto the hard disk. You would do this if the system boot sector were to become corrupted.

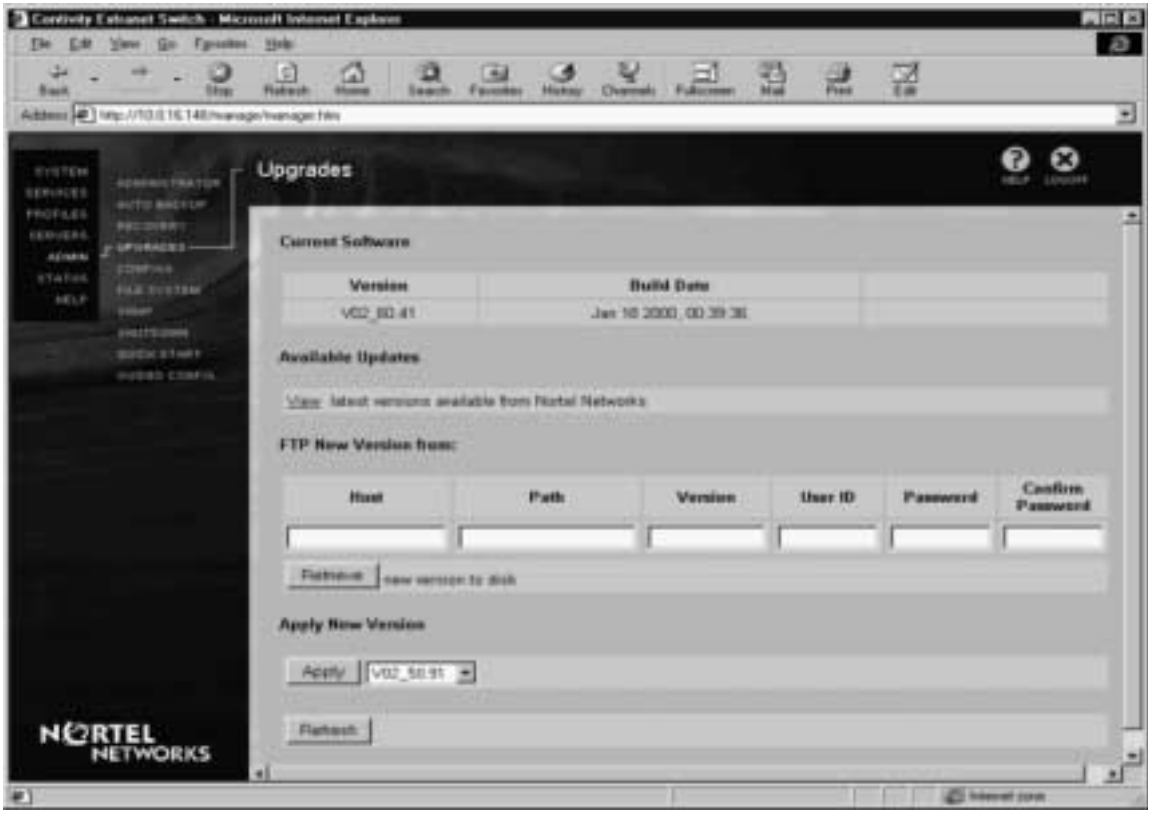
Restart System

Remove the diskette and press the Reset button on the back of the switch. Then reposition your Web browser to the Management IP address, and choose Reload or Refresh from your browser menu to access the management page of the software running on the hard disk.

Upgrades

The Upgrades screen allows you to download the latest Nortel Networks software for the switch via File Transfer Protocol (FTP). In addition to retrieving software you can select which version of software to run.

Figure 150 Upgrades



Current Software

Version

The current Version of software running on the switch.

Build Date

The Build Date of the current Version of software running on the switch.

Available Updates

View

Click to go to the Nortel Networks Web site to determine which software versions are available.

FTP New Version From

If necessary, enter a Host server and its required access information to allow you to retrieve the latest software images for your switch.

Host

If necessary, enter the name or IP address of the Host remote server that contains the switch software version to be retrieved.

Path

If necessary, enter the path to the directories and files where the switch software image is stored.

Version

Enter the software image file Version that you want to download to your switch. Typically, you would enter the latest software Version. However, if you had a problem with a current version and you wanted to revert to an older version, you could do so here.

To determine the latest version of software, check the Version number in the title of the software release notes. Or, you can click View to visit the Nortel Networks Web site to find the latest software version. Contact Nortel Customer Support for additional information.

Note: To operate with the latest version of software, you must first download it, and then select Apply New Version (see below).

User ID

If necessary, enter an appropriate user ID for the FTP server.

Password

If necessary, enter the FTP server Password.

Confirm Password

If you entered an FTP server password, reenter the password to verify it.

Retrieve

Click Retrieve to download the software image file for the switch. The download takes several minutes, and upon completion, the Upgrades screen reappears with a success or failure message.

Apply New Version

Version to Apply

Click the drop-down list box to view the software versions that are available on your system. Select the version that you want to run on the system.

Apply

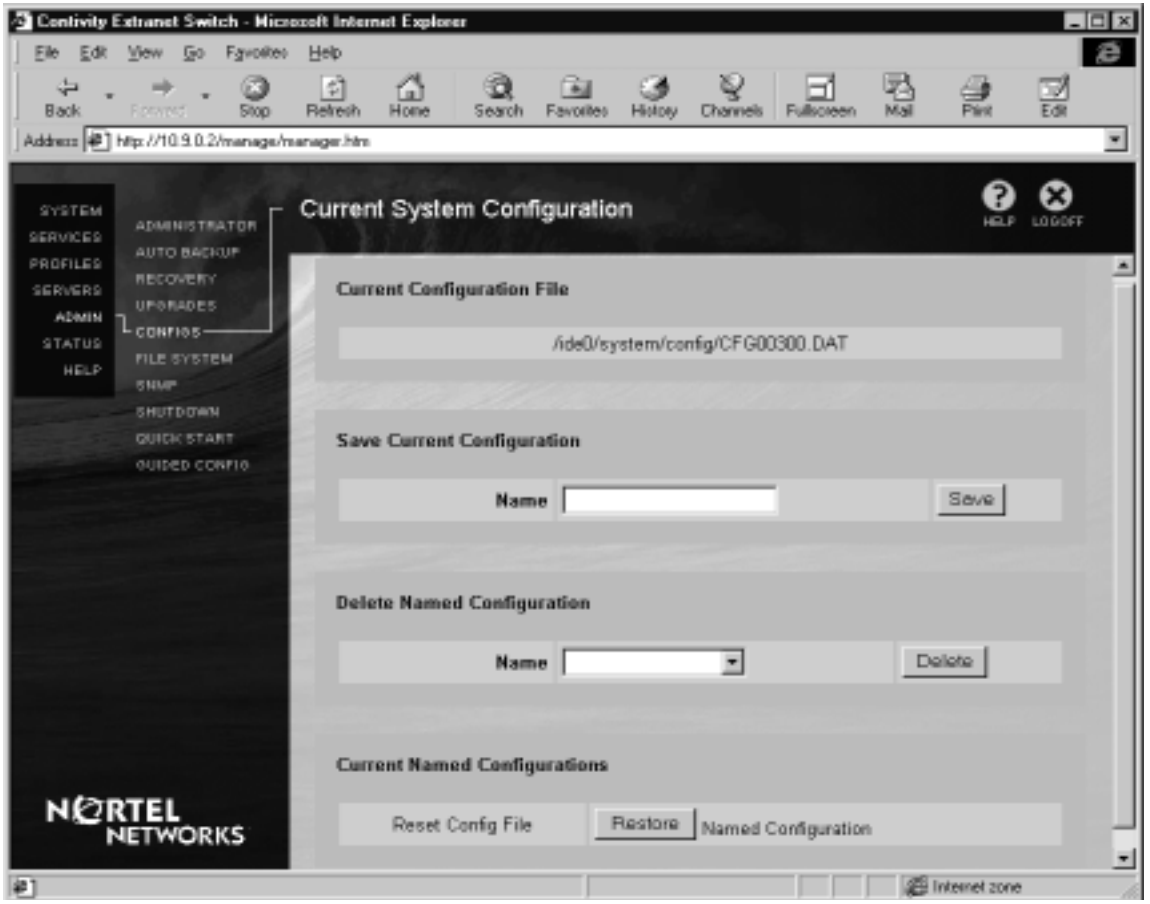
After you select the new version, click Apply. This restarts the system with the version that you now want to run on the switch.

Note: After you apply the upgrade, you should purge your browser's cache. This clears old references to screens that might have changed between versions.

Current System Configuration

The Admin→Config screen allows you to Name and save the Current System Configuration. Additionally, you can select one of the previously named configurations and restore it to be the Current Configuration.

Figure 151 Current System Configuration



Save Current Configuration

Name

Enter a date as the Name for the Current software Configuration; for example, April 15, 1999.

Save

Click to Save the Current software Configuration name.

Delete Named Configuration

Click the drop-down list box to display the name of the Configuration that you want to delete.

Current Named Configurations

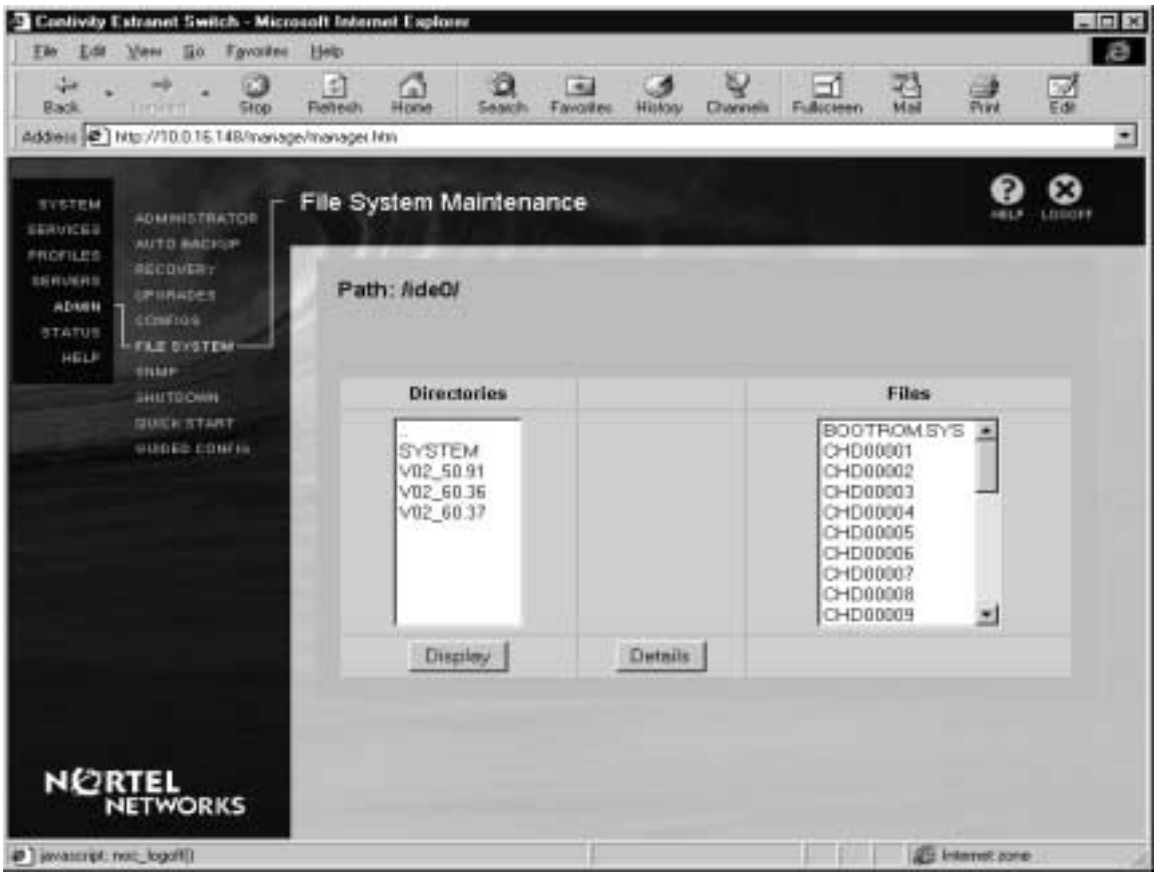
Restore

Click the Restore button to go the System Shutdown screen. From there, click the drop-down list box Under Boot Configuration to select a configuration to be restored as the Current Configuration after a reboot.

File System Maintenance

The File System Maintenance screen allows you to navigate through the switch file system. The top level lists the devices (drives), and beneath a given drive are the directories. This provides flexibility in viewing details of a file or directory, and it allows you to delete unnecessary files. For example, if you had problems performing an FTP transfer with a specific file, you could view the file details to learn its file size and when it was last modified for troubleshooting purposes. Additionally, you can toggle between hard drives when a backup drive is available.

Figure 152 File System Maintenance



Devices

This field applies to the 4000 series switches, which have two hard disk drives. This field appears only when you are at the top level of the file structure; when the hard drives and floppy drive appear in the column. To get to this level, select the two periods (..), then click Display.

Action

Click to Enable or Disable the associated hard disk drive, either ide0 (drive 0) or ide1 (drive 1). Clicking either of these buttons turns the drive online or offline. When the switch boots it makes sure the primary disk is not corrupt; if it is corrupt, then the switch boots from the secondary disk.

If you receive error messages about the secondary drive, disable it so that the synchronization does not even try to read or write to the drive.

Click Enable to activate the listed drive (for example, ide1 – drive 1).

Click Format to reformat the listed drive (for example, ide1 – drive 1). Use this action with discretion, as you would completely wipe out data existing on this drive.

Display

Click on the Directory that you want to view. Next, click Display to change the path to the selected directory.

Details

Click to display the associated Directory or File information. Clicking Details also invokes the Delete option. The Delete option allows you to delete a single file or the contents of an entire directory. Refer to “File System Maintenance Details” for additional information.

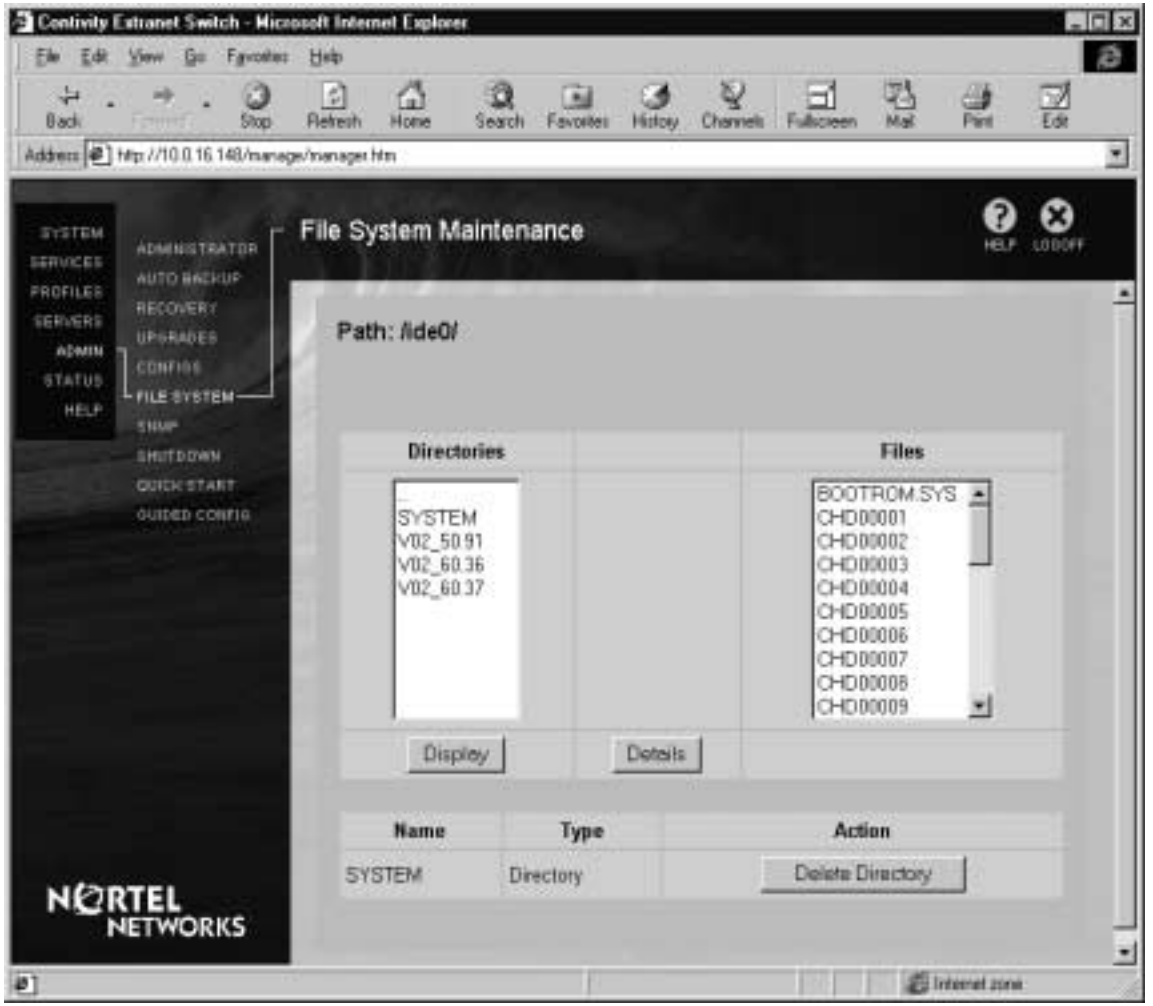
Prepare

Click to Prepare the selected hard disk drive for removal. This clears the system cache of the selected drive's contents. Not preparing the hard disk drive for removal presents the risk that there could be file corruption upon reinsertion of the drive. Additionally, this prevents any possibility of inaccurately accessing data from the drive that was previously in use.

File System Maintenance Details

This screen provides the details associated with a selected directory or file.

Figure 153 File System Maintenance Details



Name

The name of the selected File; for example, bdy_boot.htm.

Type

Shows whether the selected details are from a file or a directory.

Size

The file size, in bytes.

Date

The Date the file was created (mm/dd/yyyy).

Time

The Time the file was created (hh/mm/ss).

Action

Delete Directory/Delete

Click to Delete the contents of a Directory or an associated file. If you choose to Delete a Directory, all of the files in the directory are deleted. Only users with Administrator Rights to Manage the switch can delete files or directories.

The system prompts you to verify that you intend to delete the contents of a Directory (and Directory Name), or selected file.

SNMP

The SNMP screen allows you to generate SNMP Version 1 Traps, based on MIB II. Use this screen to do the following:

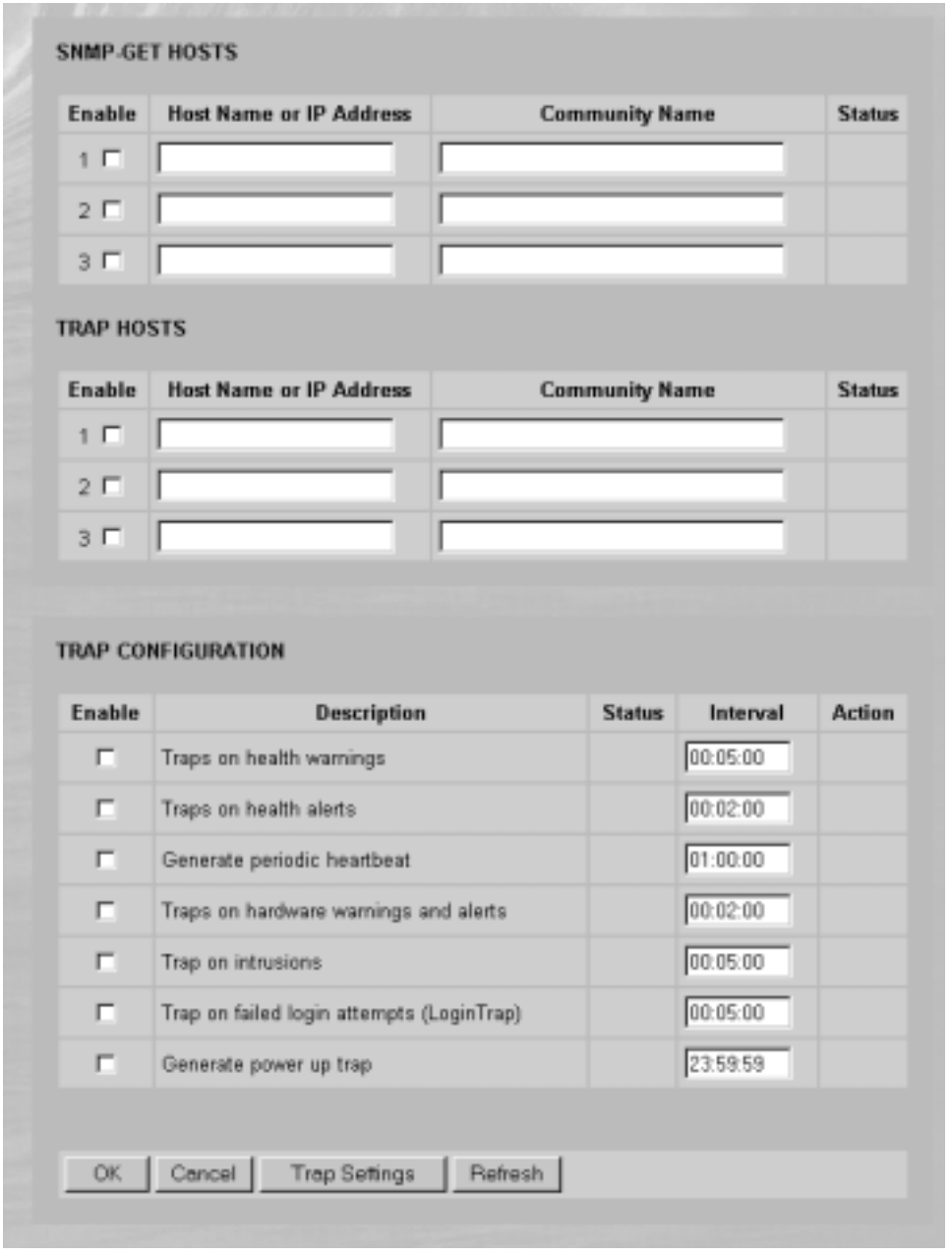
- Designate the remote SNMP management stations that are authorized to send SNMP Gets to the switch.
- Designate the trap hosts to which the traps can be sent.
- Configure the traps.

The SNMP counters measure packet attributes that are based on the outer IP header. In the tunneled environment there is also an inner IP header, but this IP header does not contribute to the SNMP MIB counters. For example, the outer packet header might be a good packet header and be counted, but the inner packet header might be corrupted and would not contribute to the drop counter.

Note: A Nortel Networks proprietary MIB is included on the Nortel Networks CD-ROM. Click on the file named CesTraps.mib to load the MIB. See “Contivity Extranet Switch MIB Support” for a description of CesTraps.mib.

You can view the Health Check screen for the results of SNMP Traps.

Figure 154 SNMP



SNMP GET HOSTS

The SNMP Get Hosts portion of the screen is used to designate SNMP management systems that are authorized to send SNMP Get requests to the switch. The switch ignores Get requests that come from all other systems.

Enable

Click to authorize the specified SNMP management system to send SNMP Gets.

Host Name or IP Address

Enter the Host Name or IP address for the SNMP management station that sends the SNMP Gets.

Community Name

Enter the SNMP Community Name. SNMP Communities serve as an Authentication scheme to enable a network device to validate SNMP Traps from the switch.

Status

Operational indicates that the switch can talk to the SNMP Get Host, while **Error** indicates the switch is unable to make a connection to the host.

TRAP HOSTS

The Trap Hosts portion of the screen is used to designate those systems to which SNMP trap messages can be sent.

Enable

Click to Enable the Trap Host to receive SNMP Traps.

Host Name or IP Address

Enter the Host Name or IP address for the SNMP Trap hosts that receives the SNMP Traps.

Community Name

Enter the SNMP Community Name. SNMP Communities serve as an Authentication scheme to enable a network device to validate SNMP Traps from the switch.

Status

Operational indicates that the switch can talk to the Trap Host, while Error indicates the switch is unable to make a connection to the host.

Note: Certain MIB browsers (for example, SNMPC) only accept traps from a machine that it can also do SNMP Gets from. If your MIB browser has this requirement, you must specify the host name or IP address in both the SNMP Get Hosts and Trap Hosts portions of the SNMP screen. Check your MIB browser documentation for requirements.

TRAP CONFIGURATION

Enable

Click to Enable the specific group of SNMP Traps. When enabled, the switch checks the status at the assigned Interval and send traps to the specified SNMP host servers.

Description

This field lists the conditions that generate SNMP Traps. A check for the trap condition is made at the indicated trap interval. If the trap condition occurs when the check is made, an SNMP Trap is generated. Traps continue to be sent until the condition state clears.

Traps on health

These traps indicate that a hardware or software component has gone into a warning state. The default interval is 00:05:00 (5 minutes).

Trap on health alerts

These traps indicate that a hardware or software component has gone into an alert state. An alert is more severe than a warning. The default interval is 00:0**2**:00 (two minutes).

Generate periodic heartbeat

This trap indicates that the switch is active. This trap is a good test mechanism to verify that the switch is on. The default interval is 01:00:00 (1 hour).

Trap on hardware warnings and alerts

These traps indicate that a warning or alert on any of the following hardware components has occurred. Refer to the discussion on Trap Settings for additional information on specific traps. The default interval for these traps is 00:02:00 (2 minutes).

- Intrusion (the top cover has been opened)
- LAN or WAN interfaces
- One of the dual power supplies has failed
- Either the critical or normal temperature is out of range
- One of the voltage indicators is out of range
- A cooling fan is not working properly
- System memory is low
- Disk space is low

Trap on intrusions

This trap indicates that someone has attempted to send an excessive amount of unauthorized packets through the public interface. The trap contains the user ID and the source and destination IP addresses.

Trap on failed login attempts

This trap indicates that someone has attempted to log on to the switch and failed. The trap contains the user ID and the source and destination IP addresses.

Generate power Up trap

This trap indicates that the switch has gone through a power-up sequence. This trap occurs only once (the default interval, 23:59:59 is ignored).

Status

Shows when a trap was last executed, along with the timestamp. If a trap is generated, a brief description appears.

Interval

Provides a time interval after which the switch checks for new SNMP Trap conditions.

Action

If a trap has occurred, click on the Details button in the Action column to view information about the trap. The Details output includes the System Name, Date and Time, System Uptime, and possibly other information (for example, LAN on Slot *n* Interface *n*).

VRRP

Click to enable VRRP SNMP traps.

OSPF

Click to enable OSPF SNMP traps.

SNMP Authentication

Click to enable SNMP Authentication traps.

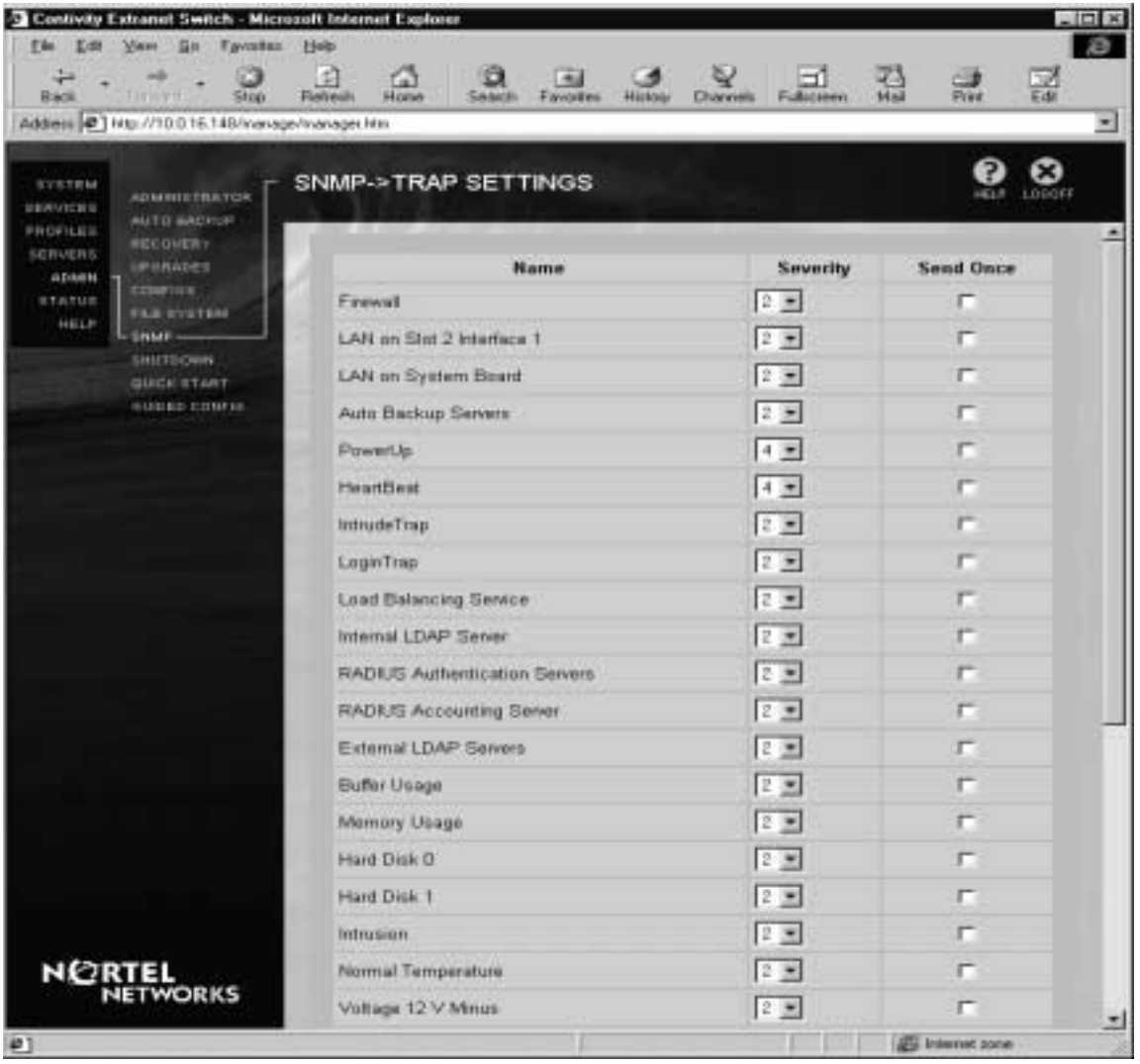
Trap Settings

Click on this button to go to the Trap Settings screen.

SNMP Trap Settings

The SNMP Trap Settings screen (Admin→SNMP→Trap Settings) allows you to specify the level of severity that is reported for the trap. You can also specify that the trap be sent only once.

Figure 155 SNMP Trap Settings



Note: The results of many of the selections you make on the Trap Settings screen are reported on the Health Check screen. Refer to "Alert and Warning Descriptions for Selected Servers" for additional information.

Name

The Name column lists the traps that are available on your switch. The actual list can vary, depending upon the model of your switch and your configuration. For example, if your switch has a single hard disk, the trap that refers to an optional disk (Hard Disk 1) does not appear on your Trap Settings screen.

Firewall

Status of the firewall that is currently enabled on the switch (either the Contivity Firewall or the Check Point firewall).

LAN on System Board

Current status of LAN Interface 1. The trap is sent only if a problem occurs.

LAN on Slot n Interface n

Current status of Slot *n* Interface *n*. The trap is sent only if a problem occurs.

Auto Backup Servers

Current status of the automatic backup servers. The trap is sent only if a problem occurs, for example, if there is no server specified.

PowerUp

Indicates that the switch was powered up.

HeartBeat

Indicates the status of the heartbeat.

IntrudeTrap

Indicates that excessive unauthorized packets were sent to the switch.

LoginTrap

Indicates that an attempted login to the switch failed.

Load Balancing Service

Current status of the load balancing feature. The trap is sent only if a problem occurs. The following table shows possible trap messages and meanings.

Table 25 Load balancing service trap messages

Trap message	Meaning
Warning: Load Balancing Service: Timed out waiting for response from server	Indicates that Load Balancing is enabled (on the Services→IPSec screen) but the configured server is not responding.

Internal LDAP Server

Current status of the internal LDAP server. The trap is sent only if a problem occurs. The following table shows possible trap messages and meanings.

Table 26 Internal LDAP server trap messages

Trap message	Meaning
Alert: Internal LDAP Server: Server not running	Server is configured and selected but is not running. This is displayed after a Restore or Backup operation.
Alert: Internal LDAP Server: Server not enabled	Server is running but is not selected
Warning: Internal LDAP Server: Restore in progress	Restore from an LDIF file in progress. LDAP server is selected but is not running. This changes to an Alert (Server not running) condition when the restore is complete
Warning: Internal LDAP Server: Backup in progress	Backup to an LDIF file in progress. LDAP server is selected but is not running. This changes to an Alert (Server not running) condition when the backup is complete.

RADIUS Accounting Server

Current status of the RADIUS Accounting servers. The trap is sent only if a problem occurs. The following table shows possible trap messages and meanings.

Table 27 RADIUS accounting server trap messages

Trap message	Meaning
Alert: RADIUS Accounting Server: Error	Server has an error condition.

RADIUS Authentication Servers

Current status of the RADIUS authentication servers. The following table shows possible trap messages and meanings.

Table 28 RADIUS authentication server trap messages

Trap message	Meaning
Alert: RADIUS Authentication Servers: Error	All enabled servers have errors
Warning: RADIUS Authentication Servers: Configured	The first server that was enabled is available but has not been contacted for authentication yet. At least one other enabled server has an error.
Warning: RADIUS Authentication Servers: Operational	The first server that was enabled is operational and has been used for authentication. At least one other enabled server has an error
Warning: RADIUS Authentication Servers: Error	The first server that was enabled has an error. At least one other enabled server is available

External LDAP Servers

Current status of the External LDAP servers. The trap is sent only if a problem occurs. The following table shows possible trap messages and meanings.

Table 29 External LDAP servers trap messages

Trap message	Meaning
Alert: External LDAP Servers: Server is down	No servers are running and no servers are selected.
Alert: External LDAP Servers: Server not enabled	All servers are running but none have been selected
Warning: External LDAP Servers: Server is down	At least one server is not running and is not selected.
Warning: External LDAP Servers: Server not enabled	At least one server is running but it is not selected.

Buffer Usage

Indicates the status of the buffer. A warning is sent if more than 75 percent of the buffer is being used. If usage exceeds 87.5 percent, an Alert is sent.

Memory Usage

Indicates the status of the system memory. A Warning is sent if more than 75 percent of memory is being used. An Alert is sent if more then 87.5 percent of the memory is being used.

Hard Disk 0

Indicates the status of the hard disk. A Warning is sent if the disk is more than 75 percent full. An Alert is sent if more then 87.5 percent of the disk is full.

Hard Disk 1

This trap appears only if the switch has a second hard disk, and indicates the status of the second disk. A Warning is sent if the disk is more than 75 percent full. An Alert is sent if more then 87.5 percent of the disk is full.

Dual Power Supply

This trap appears only if the switch has a dual power supply, and indicates the state the dual power supply.

Table 30 Dual power supply trap message

Trap message	Meaning
Alert: Dual Power Supply: Redundant supply faulted	On systems with dual power supplies, one of the power supplies is not working. **Notes:** The switch continues to operate with a single power supply. However you should replace the faulty power supply as soon as possible

Intrusion

Indicates that the switch cover is off. Sensors in the switch make this determination.

Table 31 Intrusion trap message

Trap message	Meaning
Alert: Intrusion: Box has been opened	The cover of the switch has been opened or is being opened, indicating a possible security intrusion. **Notes:** The switch continues to operate while the box is opened. Check to ensure that unauthorized access has not occurred.

Critical Temperature

Indicates the critical temperature state of the switch. If this temperature reaches an Alert condition, you should immediately shut down the switch to prevent any damage.

Table 32 Critical temperature trap message

Trap message	Meaning
Alert: Critical Temperature: Critical temperature out of range	The switch is running at a critically high temperature above its rated normal operating temperature. This indicates a serious problem -- you should shut down the switch immediately. **Notes:** Component failure may have already occurred. Contact your Nortel Networks representative if you cannot determine the cause of the excessive temperature

Normal Temperature

The normal temperature state of the switch. An Alert condition indicates that the switch has exceeded its normal operating range (0°C to 55°C).

Table 33 Normal temperature trap message

Trap message	Meaning
Alert: Normal Temperature: Normal temperature out of range	The switch is running above its rated normal operating temperature. **Notes**: This can occur if the switch fan is not working properly or if there is a high ambient temperature. Continued operation of the switch at excessive temperature can result in performance degradation and component failure. Do not wait for a Critical Temperature Trap, as it is not supported on all switch models

Voltage 12 V Minus

Indicates the state of the -12 voltage. The following table shows voltage-related trap messages.

Table 34 Voltage trap messages

Trap messages	Meaning
Alert: Voltage ***nnn***: Voltage out of range where: ***nnn*** is the voltage, for example, 3.3 V Plus	The supplied voltage to the switch is not within the specified range. This indicates a serious problem and should be checked immediately by a Nortel Networks representative. **Notes:** Improper voltage input can cause erratic switch operation. Not all switch models support traps for all voltages

Voltage 12 V Plus

Indicates the state of the +12 voltage.

Voltage 2.5 VB

Indicates the state of the 2.5 voltage on the auxiliary processor.

Voltage 2.5 VA

Indicates the state of the 2.5 voltage on the main processor

Voltage 3.3 V Plus

Indicates the state of the +3.3 voltage.

Voltage 5 V Minus

Indicates the state of the -5 voltage.

Voltage 5 V Plus

Indicates the state of the +5 voltage.

Chassis Fan 2

Current status of the second chassis fan. If you have an Alert, check to see if the fan is dirty or clogged. This trap is displayed only if the switch has the second chassis fan.

Table 35 Chassis Fan 2 trap message

Trap messages	Meaning
Alert: Chassis Fan 2: Fan not functioning	The second chassis fan is running either below the specified speed or is not running at all. **Notes**: A service technician must check the fan as soon as possible. If the fan is not working correctly, overheating of the switch and possible component failure can result.

Chassis Fan

Current status of the chassis fan. If you have an Alert, check to see if the fan is dirty or clogged.

Table 36 Chassis fan trap message

Trap messages	Meaning
Alert: Chassis Fan: Fan not functioning	The chassis fan is running either below the specified speed or is not running at all. **Notes**: A service technician must check the fan as soon as possible. If the fan is not working correctly, overheating of the switch and possible component failure can result.

CPU Two Fan

Current status of the second CPU fan. If you have an Alert, check to see if the fan is operational. This trap is displayed only if the switch has the second CPU fan.

Table 37 CPU two fan trap messages

Trap messages	Meaning
Alert: CPU Two Fan: Fan not functioning	The fan on the auxiliary processor is running either below the specified speed or is not running at all. **Notes**: This trap can only be sent by systems which contain an actual fan on the auxiliary CPU. If the fan is not working correctly, it must be fixed as soon as possible or damage may result to the processor as well as to the switch.

CPU One Fan

Current status of the primary CPU fan. If you have an Alert, check to see if the fan is operational.

Table 38 CPU one fan trap messages

Trap messages	Meaning
Alert: CPU One Fan: Fan not functioning	The fan on the primary processor is running either below the specified speed or is not running at all. **Notes**: This trap can only be sent by systems which contain an actual fan on the primary CPU. If the fan is not working correctly, it must be fixed as soon as possible or damage may result to the processor as well as to the switch.

CPU 2

Current status of the second CPU. This trap is displayed only if the switch has two CPUs.

Table 39 CPU 2 trap message

Trap message	Meaning
Alert: CPU 2: Program load failed	These traps are only sent from a switch with multiple CPUs and indicate that the application CPU is not functioning correctly. **Notes:** The switch sounds an alarm and the networking performance is degraded. The switch continues to function without the application processor. Reboot the switch to correct the situation. If the problem continues, contact your Nortel Networks support representative
Alert: CPU 2: Bootup did not complete	
Alert: CPU 2: Communication los	
Alert: CPU 2: Failed. Reason unknown	

SNMP Servers

Current status of the SNMP servers. The status is either Operational or Error.

IP Address Pool

The status of the IP Address Pool. An Alert status indicates that there are no addresses available.

FIPS

Current status of FIPS mode.

Table 40 FIPS trap messages

Trap message	Meaning
OK: FIPS disabled	FIPS mode is currently disabled on the switch
OK: FIPS enabled and power-up test in progress	FIPS mode is enabled and the switch has been rebooted and is running the power-up tests
OK: FIPS enabled and all tests have passed	FIPS mode is enabled, the switch has finished rebooting, and has successfully completed the power-up tests.
Warning: FIPS: Random generator test failed	During the FIPS power-up testing, the random generator test failed.
Warning: FIPS: DESMAC check on executables failed	During the FIPS power-up testing, DESMAC check on executables failed.
Warning: FIPS: DES KAT test failed	During the FIPS power-up testing, the DES KAT test failed.
Warning: FIPS: SHA1 self test failed	During the FIPS power-up testing, the SHA1 self test failed
Warning: FIPS disabled due to HW accelerator present	FIPS is disabled because your switch has a hardware accelerator card installed.
Alert: FIPS status not known	The switch is unable to determine the status of FIPS mode.

DNS Servers

Current status of the DNS servers. The following table shows possible trap messages and meanings.

Table 41 DNS servers trap messages

Trap Messages	Meaning
Alert: DNS Servers: Error	None of the configured servers are operational
Warning: DNS Servers: Operational	At least one server is operating properly but another server has errors.

Severity

Click the drop-down list box to select the level of severity that is reported for the trap. The default severity is a value of 2. In most cases, the default is appropriate for the trap. However, you might want to change the severity value to highlight the reporting of a trap. For example, if you want to closely monitor the status of your hard disk, you might assign a severity value of 1 to the Hard Disk 0 trap.

The following table shows the severity choices and their impact on the switch performance.

Table 42 Severity level meanings

Severity	Meaning
1	Fatal, critical condition; severely impacts performance.
2	Major condition; results in poor performance.
3	Minor condition; performance is within specifications but should be monitored.
4	Significant informational event; normal performance.
5	Event of no operational value.
R	Reverses Severity 1, 2, and 3 conditions; returns performance to normal. This code is for future use.

Send Once

This selection takes precedence over the Interval setting on the SNMP screen. Click to specify that if the event occurs, it is trapped only once. Otherwise the trap is repeated using the time interval specified on the SNMP screen. The PowerUp trap is an example of a send once event.

System Shutdown

The Admin→Shutdown screen allows you to gracefully turn off the switch. The Shutdown options allow you to Shutdown immediately, to wait until current users are logged off, or to wait until a designated time. A graceful shutdown safely terminates connections so that no data is lost, compared with a spontaneous loss of power, for example.

Additionally, you can select whether to power off or restart after Shutdown, and also choose the configuration file to use upon restarting. To allow you to conduct an orderly Shutdown, you can disable new logins, and you can disable logins after the Shutdown to perform system maintenance.

You should always use the System Shutdown screen to shut down the system rather than the Power or Reset buttons on the back of the switch. This ensures the integrity of your file system.

Note: After performing a System Shutdown, click the Reload/Refresh button to see the latest switch information.

Figure 156 System Shutdown

Caution: When a System Shutdown has started, do not reset or power down the switch; doing so might cause you to lose data or might render the switch inoperable.

Logins

Disable New Logins

Click to prevent new remote access logins before shutting down. Disabling New Logins prevents the need to log off new users when you power down the system.

Disable Logins After Restart

Click to prevent remote Logins After Restarting the system. For example, you might select this option when performing system maintenance. After the system restarts, the Disable New Logins option is selected. After completing maintenance tasks, you should deselect Disable New Logins to allow normal logins.

Note: Administrators can access the switch via Web management independent of the Login control selection.

System Shutdown

To Shutdown, you must select a System Shutdown option other than None, which is the default.

After All Users Log Off

Click to shut down the system After All remote access Users have Logged Off. Administrators logged into the system via HTTP must also be logged off.

At

Click and assign a specific time to shut down the system as represented by a 24-hour clock (hh:mm:ss); for example, you can shut down the system at 16:50:00.

In *n* Minutes

Enter a specific number of Minutes after which the system shuts down. The possible range is 1 to 1440 (24 hours); default is 1 minute.

Now

Safely shuts down the system immediately by terminating all sessions and closing connections to servers.

None

Do not shut down the system. If there is a previously configured shutdown pending, you must click on the Cancel Pending Shutdown button at the top of the screen. This cancels the pending shutdown and automatically selects the None option.

After System Shutdown

Power Off

Power Off the switch After the System Shutdown occurs.

Restart

Restart the switch After the System Shutdown occurs.

Boot Mode

Select the mode that you want to use when rebooting the switch, either Normal mode or Safe mode.

Boot Configuration

Use

Click the drop-down list box to view the available Configuration Files. To change the configuration files that appear in this list, use the Current System Configuration screen. Select the configuration file that you want the switch to boot from when restarting.

Note that if you choose a new Boot Configuration option, then you must also choose a System Shutdown option to indicate when the System shuts down and subsequently loads the new Boot Configuration file.

Reboot From Drive

/ide0/ (primary)

Click to select the hard disk drive /ide0/ (primary) from which you want to boot the switch.

/ide1/ (secondary)

Click to select the hard disk drive /ide1/ (secondary) from which you want to boot the switch.

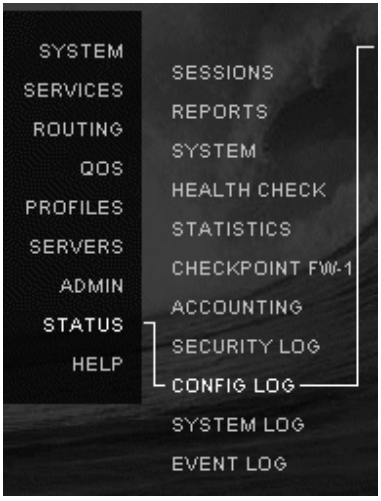
Cancel Pending Shutdown

When a shutdown is pending, the Cancel a Pending Shutdown button is available. Use this button to stop the shutdown or, alternatively, click None under the System Shutdown area of the screen.

Chapter 8
Status

This section describes the System Status screens. The System Status screens allow you to see, from the Web interface, who is logged on, their traffic demands, and a summary of the switch hardware configuration, including available memory and disk space.

Figure 157 Status menu

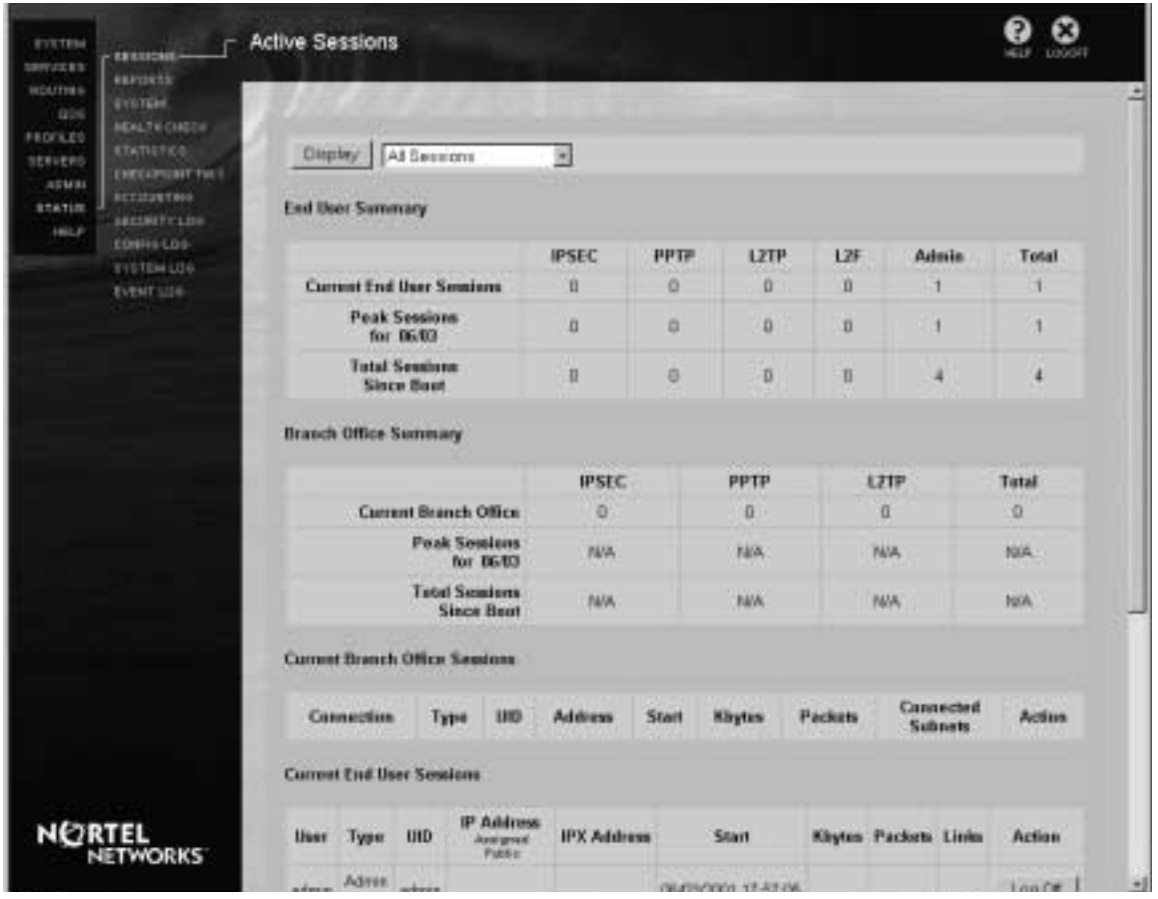


Active Sessions

The Active Sessions screen allows you to see which users are tunneled into the switch, when they logged in, and the number of bytes and packets they have transmitted or received.

Additionally, you can choose to see selected session details and you can even log off users.

Figure 158 Active Sessions



Display

Click the drop-down list box to select one of the following Active Sessions views:

- End User Sessions
- Branch Office Sessions
- All sessions (default)

Summary

The Summary table shows statistics for the number of sessions on the switch, including the current number of sessions, the peak number of sessions, and the total number of sessions since the switch was last booted.

Current Sessions

The current number of sessions.

Peak Sessions for Date

The maximum number of sessions for the cited date.

Total Sessions Since Boot

The total number of sessions since the system was restarted.

Current Branch Office Sessions

Shows the number of Branch Office connections, including the gateway, IP address, start time, number of Kilobytes, and total packets sent through a connection.

Refer to the Current End User Sessions section for most of the Current Branch Office Sessions field descriptions, as they are the same.

Connection

Shows the name of the Connection, either an IP address or a DNS name.

Current End User Sessions

Shows the current end user connections to the switch, including the user name, type, User ID, IP address assigned, the IPX address, start time, number of Kilobytes, total packets sent through a connection, and links.

User

Shows the user’s full name; for example, Madison Lee.

Type

Shows the account type, any of the four tunnel types (IPsec, PPTP, L2TP, L2F) or Admin.

User ID

Shows the User's account ID; for example, mlee.

IP Address Assigned/Public

Shows the IP Address Assigned by the switch (the inner address), and the public IP Address of the client device (possibly assigned by the ISP) that is connected to the switch.

IPX Address

Shows the inner IPX Address of the client device that is connected to the switch.

Start

Shows the session Start date and time using a 24-hour clock (in the format hh:mm:ss). For example, 6/5/1999 21:18:47.

Kbytes

Shows the number of Kilobytes of traffic transmitted In to the corporate network and Out of the corporate network. (Not applicable to Administrator's sessions.)

Packets

Shows the number of Packets going into the corporation and going out of the enterprise’s intranet. (Not applicable to Administrator sessions.)

Links

Shows the number of PPP links associated with this session.

Action

Log Off

Click to log off the associated user immediately, including Administrators. The Log Off button appears only if you have the proper Administrator rights.

Details

Click to view Details such as the group the user belongs to, account type, number of active sessions, and numerous IP session counters. This option is not applicable to Administrator sessions.

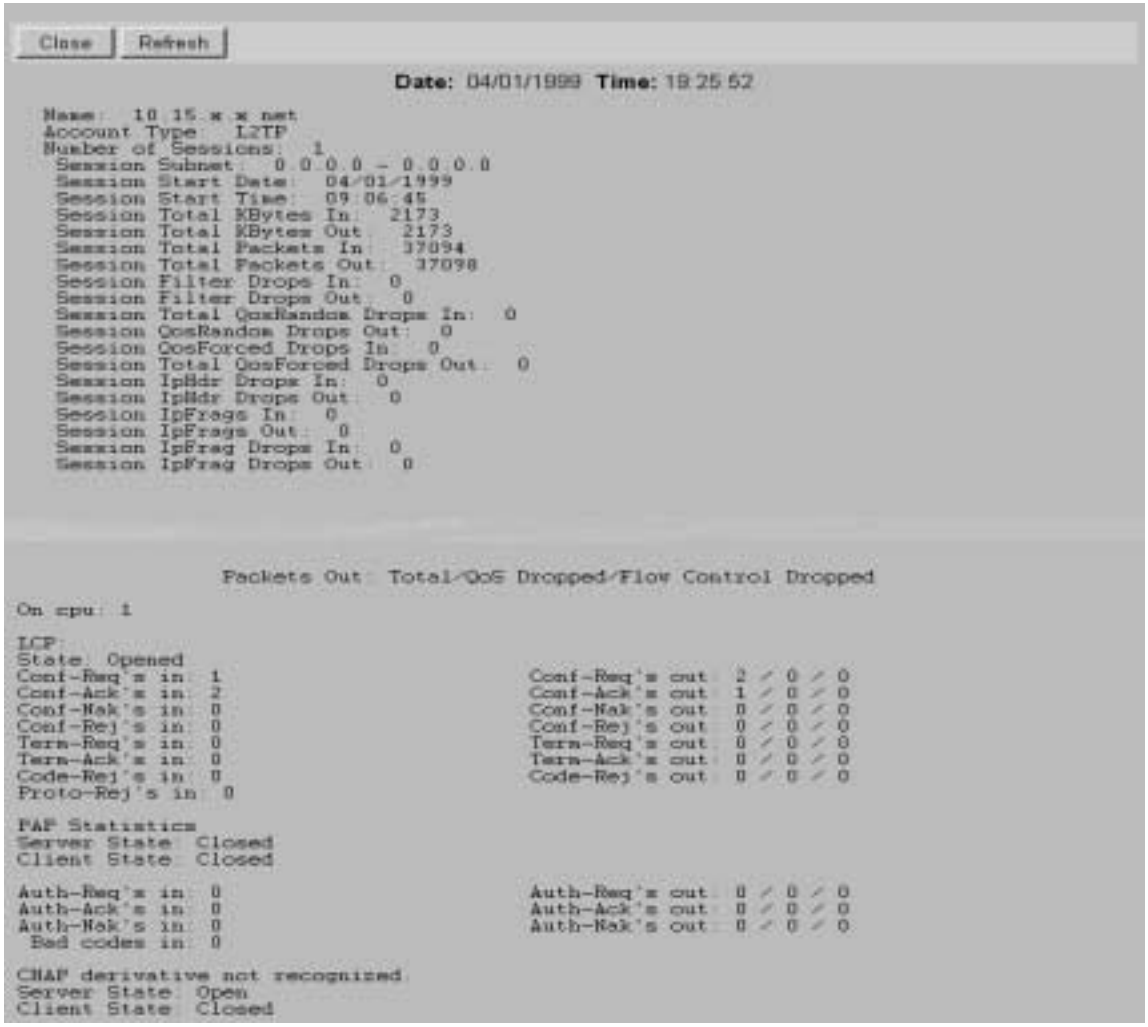
Log Off

Click to log off all non-administrative users immediately. This logs off all tunneled users so that the administrator can perform maintenance.

Active Sessions Details

This screen provides Active Session Details for specific users, including User Name and Group, number and type of accounts, number of active sessions and many IP session-specific details.

Figure 159 Partial Active Sessions Details



The following table provides descriptions of active sessions.

Table 43 Descriptions of active session details

Listing	Description
User Name	Current user's name
Group	Group with which the current user is associated
Number of Accounts	Number of accounts that are currently active
Account Type	Type of the account
Account Userid	User ID for this account
Number o f Active Sessions	Number of sessions that are currently active
Session IP Address	Session inner IP address
Session Start Date	Date the session started
Session Start Time	Time the session started
Session Kbytes In	Kilobytes that are transmitted into the switch
Session Kbytes Out	Kilobytes that are transmitted out of the switch
Session Packets In	Packets that are transmitted into the switch
Session Packets Out	Packets that are transmitted out of the switch
Session IpFrag Drops In	Packets going into the enterprise network that are dropped if the rest of the fragment does not get there in time
Session IpHdr Drops In	Packets going into the enterprise network that are dropped whenever there is an error in the IP header
Session Local Interface Filter Drops In	Packets destined to a physical interface that are dropped due to lack of authorization access
Session Local System Filter Drops In	Packets destined to a LAN management address but are dropped due to lack of authorization access
Session QosRandom Drops Out	Packets dropped as part of Random Early Detection (RED) congestion
Session Routing Filter Drops In	Packets filtered because no access rights are permitted to the resources specified by the designated filters
Session Source Address Drops In	Packets that are dropped due to a source address access conflict
Session Local Interface Filter Drops Out	Packets coming from a physical interface that are dropped due to lack of authorization access
Session Local System Filter Drops Out	Packets coming from a switch management address that are dropped due to lack of authorization access

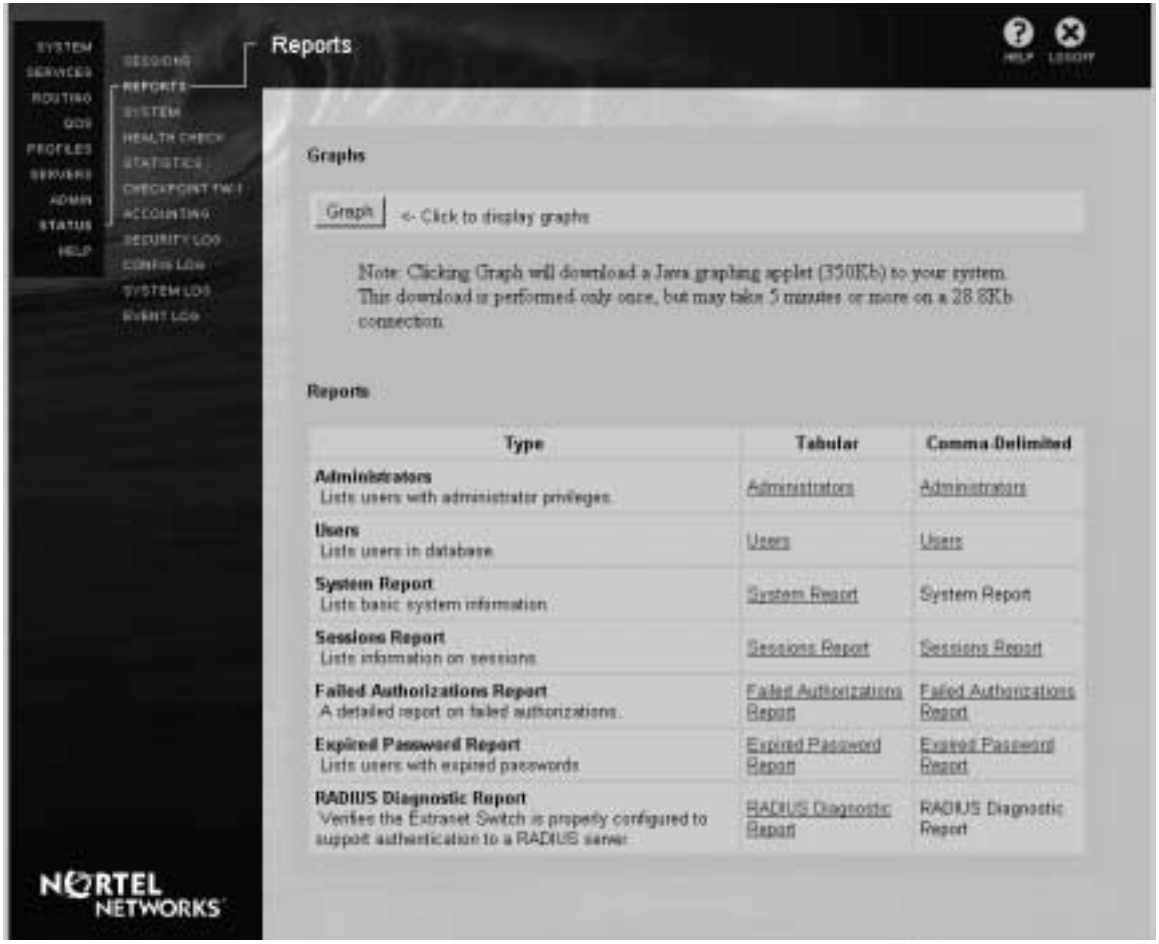
Table 43 Descriptions of active session details (continued)

Session QosForced Drops In	Packets dropped because the peer could not establish a quality of service session
Session Routing Filter Drops Out	Packets filtered because no access rights are permitted to the resources specified by the designated filters
Session IpFrag In	Incoming IP packets that are fragmented
Session IpFrag Out	Outgoing IP packets that are fragmented

Status Reports

The Status Reports screen allows you to view system and performance data in text or graphical format. You can generate current or historical graphs of valuable system data. The Reports feature provides a comprehensive screen or down-loadable reports on user activity.

Figure 160 Status Reports



Graph

Clicking Graph causes a Java graphing applet to be loaded to your browser. When you are there, you can choose between graph types and time features. Click to access the graphical package.

The first time you click Graphs, it can take a few minutes for the graphing package to download over a dial-in line. Thereafter, it is cached and appears quickly.

Reports

You can view reports for Administrators or Users. These reports can be accessed in an on-screen tabular format and they can be put into a comma-delimited format for export into a spreadsheet or database.

Type

You can view reports for the following types. The amount of detail in the reports depends on your access rights, which are set in the Admin Rights area on the Profile→Users: Edit screen.

Administrators

You must have Manage Switch rights to view these reports. The report lists users with administrator privileges, including name, group, and switch or users privileges.

Users

Lists users and the system database groups they are in. You can also generate details of user accounts and user IDs. If you only have Manage User rights, the report is limited to groups that you are allowed to manage.

System Report

You must have Manage Switch rights to view these reports. The report lists basic system information, including configuration, type, services, hardware, and interfaces.

Sessions Report

Lists session information including, model, date, average sessions per minute. If you only have Manage User rights, you must be set up to manage the /Base group.

Failed Authorization Report

Lists failed authorization information including, model, date, total, and average sessions per minute. You can also generate details for individual listings. If you only have Manage User rights, you must be set up to manage the /Base group.

Expired Password Report

Lists users with expired passwords. If you only have Manage User rights, the report is limited to groups that you are allowed to manage.

RADIUS Diagnostic Report

You must have Manage Switch rights to view these reports and the reports are limited to groups that you are allowed to manage. The report lists various RADIUS reports that show whether the switch settings are synchronized with the RADIUS server settings.

On Screen

Click the appropriate listing to generate a tabular On Screen report, which you can then print.

Comma-Delimited

Click the appropriate listing to generate the report in a Comma-Delimited format. You can then import this report into a spreadsheet or database.

Graphs

The graphical utility allows you to generate particular types of graphs for specific time periods. For example, you can generate a system resources graph for the current time period.

Graph Type

You can generate the following Graph Types:

- Bytes In/Out (packets transported by the switch)
- System Resources
- Dropped Packets
- Failed Authentications
- Packets In/Out
- Sessions

Graph Period

Following are the types of Graph Periods you can generate.

- Current - Displays a per minute average for the entire day up to that point. The graphing package then polls the switch every minute for the most recent value and appends it to the graph. You can leave Current up and running and it continues to graph throughout the day.
- Historical - Displays summary data for the last 30 days.
- Date - Displays data for the specified date.

Viewing a Single Value

You can display the values represented by any point on the graph by clicking on the exact data point, then clicking again. A dialog box displays the values of the data point.

Zooming in on a Graph Area

To zoom into an interesting portion of the graph, click at a point to the left of the area that you want to enlarge, drag your mouse past the point that you want to enlarge, then release the mouse button. You can repeat this action to further enlarge the viewed area.

Type a lowercase “r” to stop zooming and reset the graph to its original view

Note: Make a rectangle around the full area that you want to view, including all specific data points.

Graph

After making a change to the Graph Type or Graph Period, click the Graph button to generate a new graph.

Stop

The Stop button, which is available only when graphing current values, stops the browser from updating the graph every minute.

Considerations

Counters

When a graphing counter exceeds the maximum (approximately 4 billion), the counter wraps to zero and the number reported is incorrect until the switch is restarted.

Upgrading and Graphs

After upgrading the switch, it can take up to 20 minutes before the system can generate graphs. This delay accounts for the time necessary to collect enough data to begin graphing.

Bytes In and Bytes Out

The graphing application labels the y-axis using scientific notation.

Historical Graph

The switch must be running at midnight (12:00 a.m.) to generate a historical graph for the day.

Printing

Graphs can be printed directly from your browser.

If you want to use the graph in a document, you can copy it to the clipboard by pressing the Alt-PrintScreen keys, and then paste it into your document.

Reports

The Reports feature allows you to generate comprehensive reports of users and other important information. You generate Reports in an On Screen tabular format and you can import them into a spreadsheet or database through the Comma-Delimited format.

Tabular Report

You can generate an on screen Users Report in tabular format. It indicates the report type, when it was generated, the model number, and the Domain Name Service (DNS) host name. You can also view the user's group, tunnel type, and User IDs.

Comma Delimited Report

You can generate text-based, Comma Delimited reports that can be imported into a spreadsheet or database. The report includes the same information as the tabular report, but in a Comma Delimited format.

System Status

The System Status screen shows the switch's Up Time, software and hardware configurations, along with the current status of key devices. When there is a pending shutdown or an IPX Public Network Address change that requires a reboot, such events are listed at the top of this screen.

Figure 161 System Status

System Up Time

Up Time

Shows the length of time in a 24-hour clock format that the switch has been running: days (if applicable), hours, minutes, and seconds.

System Configuration

Software Version

The Version of Software currently in use.

Software Build Date

The date and time that the software was built by Nortel Networks.

System Serial Number

The system serial number. This number is unique for each switch.

MAC Address

The media access control (MAC) address of the logical system management interface.

BIOS

Basic Input/Output System (BIOS) number, date, and time.

System Hardware

Processors 1 and 2

Processors 1 and 2 are Pentium IIs running at 450 MHz with 512 KB cache. Only the 4000 series of the switch has dual processors.

Memory

The available memory in the switch.

Hard Disk 1 and 2

The amount of the hard disk storage that is available on a particular disk, and also the total storage space. In this case, hard disk 1 has 1399 MB available storage out of a total of 2036 MB; thus, 637 MB is being used. Only the 4000 series of the switch has two hard disks.

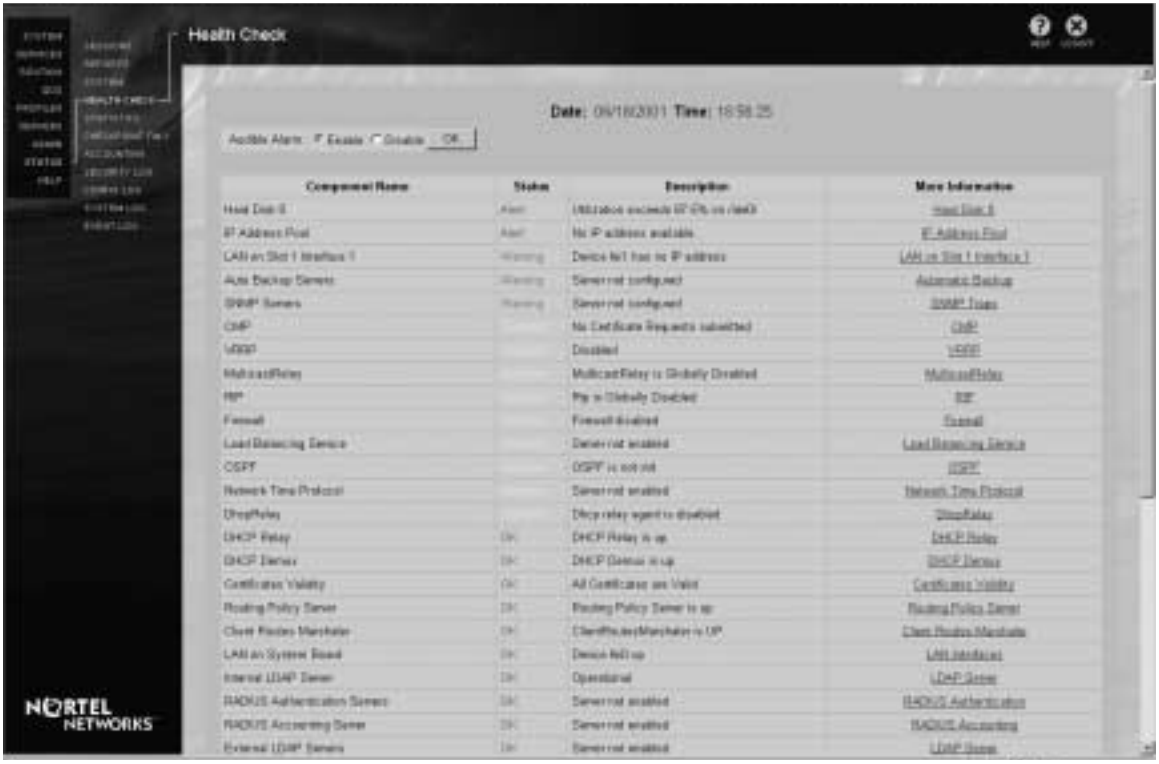
Diskette

The type of diskette drive (3.5-inch) on the switch (located behind the front cover or on the front). The diskette drive is not required for normal operation, but is available to restore the system in the unlikely event of a hard disk failure. For instructions on removing the front cover, refer to the switch's *Getting Started Guide.*

Health Check

The Health Check screen provides an overall summary of the current state of the switch's hardware and software components at a glance.

Figure 162 Health Check



Audible Alarm

Enable

Click to Enable the Audible Alarm, which the switch emits.

Disable

Click to Disable the Audible Alarm, which the switch emits.

Component Name

This is a brief description of the hardware or software components in the switch.

Status

The listings appear from top to bottom in order of severity, based on the following possible listings:

- Alert - A red Alert indicates that something is wrong with the current situation and you should attend to the situation as soon as possible.
- Warning - A yellow Warning indicates that there is an impending failure; you should attend to the situation now in order to avoid an Alert condition. A purple Warning indicates that the server is not yet configured.
- Disabled - A yellow Disabled indicates that the device is not enabled on its related configuration screen. For example, the Load Balancing Service would show a Disabled status if you have not checked the Enabled box for Load Balance on the Service→IPsec screen.
- OK - A green OK indicates that everything is currently operating as expected. There are no problems to be concerned with. Note, however, that servers that are not enabled are also listed as OK.

Description

A brief message describes the component state. The section “Alert and Warning Descriptions” lists descriptions for Alert or Warning conditions.

More Information

This column contains a link to the configuration screen associated with the selected component or for a Status→Statistics screen that has related information. This option is left blank when there are no associated screens.

Additional Information for Health Check screen

This section provides additional information for the descriptions that you might receive from the Health Check screen.

Health Check Components

The following table describes the health check components.

Table 44 Health check components

Component name	Description
LAN on Slot *n* Interface *n*	Current status of Slot *n* Interface *n*
Auto Backup Servers	Current status of the automatic backup servers
SNMP Servers	Current status of the SNMP servers
Load Balancing Service	Current status of the load balancing feature
Firewall	Current status of the switch's firewall
LAN on System Board	Current status of LAN Interface
Internal LDAP Server	Current status of the internal LDAP server
RADIUS Accounting Server	Current status of the RADIUS Accounting servers
External LDAP Servers	Current status of the External LDAP servers
Buffer Usage	Status of the buffer
Memory Usage	Status of the switch's system memory
Hard Disk 0	Status of the switch's hard disk
Dual Power Supply	State the dual power supply
Intrusion	Internal light sensors have determined that the cover is off
Critical Temperature	Critical temperature state of the switch. If this temperature reaches an Alert condition, the switch goes into an impending shutdown state to prevent any damage.

Table 44 Health check components (continued)

Component name	Description
Normal Temperature	Normal temperature state of the switch. If this temperature reaches an Alert condition, then the switch has exceeded the normal operating range (0°C to 55°C).
Voltage 12 V Minus	State of the Voltage 12 V Minus reading
Voltage 12 V Plus	State of the Voltage 12 V Plus reading
Voltage 2.5 VB	State of the Voltage 2.5 VB reading
Voltage 2.5 VA	State of the Voltage 2.5 VA reading
Voltage 3.3 V Plus	State of the Voltage 3.3 V Plus reading
Voltage 5 V Minus	State of the Voltage 5 V Minus reading
Voltage 5 V Plus	State of the Voltage 5 V Plus reading
Chassis Fan 2	Current status of the LAN/WAN card slot fan. If you have an Alert, check to see if the fan is dirty or clogged.
Chassis Fan	Current status of the LAN/WAN card slot fan. If you have an Alert, check to see if the fan is dirty or clogged.
CPU Two Fan	Current status of the CPU Two Fan. If you have an Alert, check to see if the fan is operational.
CPU One Fan	Current status of the CPU One Fan. If you have an Alert, check to see if the fan is operational.
Disk Redundancy	Current status of the two hard disks.
WAN on Slot *n* Interface *n*	Current status of Slot *n* Interface *n*.
RADIUS Authentication Servers	Current status of the RADIUS authentication servers
IP Address Pool	Current status of the DHCP Address pool server.
DNS Servers	Current status of the DNS servers
FIPS	Current status of FIPS Mode

Alert and Warning Descriptions

The use of SNMP traps can provide important status information about your switch's devices. The following table lists possible Health Check messages that can result when Alert and Warning conditions are produced by SNMP traps. This information is for the following types of servers: RADIUS Servers, LDAP Servers, Load Balancing Servers, and DNS Servers. In some cases, the table also shows descriptions for selected OK conditions.

Table 45 Health check messages from SNMP traps

Status	Description	Comments
RADIUS Accounting Server		
Alert	Error	Server has an error condition.
OK	Server not enabled	No server is available. You must enable the server on the Servers→RADIUS Acct screen.
OK	Configured	No errors.
RADIUS Authentication Server		
Alert	Error	All enabled servers have errors.
Warning	Configured	The first server that was enabled is available but has not been contacted for authentication yet. At least one other enabled server has an error.
Warning	Operational	The first server that was enabled is operational and has been used for authentication. At least one other enabled server has an error.
Warning	Error	The first server that was enabled has an error. At least one other enabled server is available.
OK	Configured	No error conditions.
OK	Operational	No error conditions.

Table 45 Health check messages from SNMP traps (continued)

Status	Description	Comments
OK	Server not enabled	No servers available. • Make sure you have enabled RADIUS Authentication on the Servers→RADIUS Auth screen. • Make sure at least one RADIUS server is enabled on the Servers→RADIUS Auth screen.
Internal LDAP Server		
Alert	Server not running	Server is configured and selected but is not running. This is displayed after a Restore or Backup operation.
Alert	Server not enabled	Server is running but is not selected.
Warning	Restore in progress	Restore from an LDIF file in progress. LDAP server is selected but is not running. This changes to an Alert (Server not running) condition when the restore is complete.
Warning	Backup in progress	Backup to an LDIF file in progress. LDAP server is selected but is not running. This changes to an Alert (Server not running) condition when the backup is complete.
OK	Server not enabled	Server is running but is not selected.
OK	Server is down	Server is not running and is not selected.
OK	Operational	Server is running and is selected.
External LDAP Servers		
Alert	Server not enabled	All servers are running but no servers are selected.
Alert	Server is down	No servers are running and no servers are selected.
Warning	Server not enabled	At least one server is running but it is not selected.

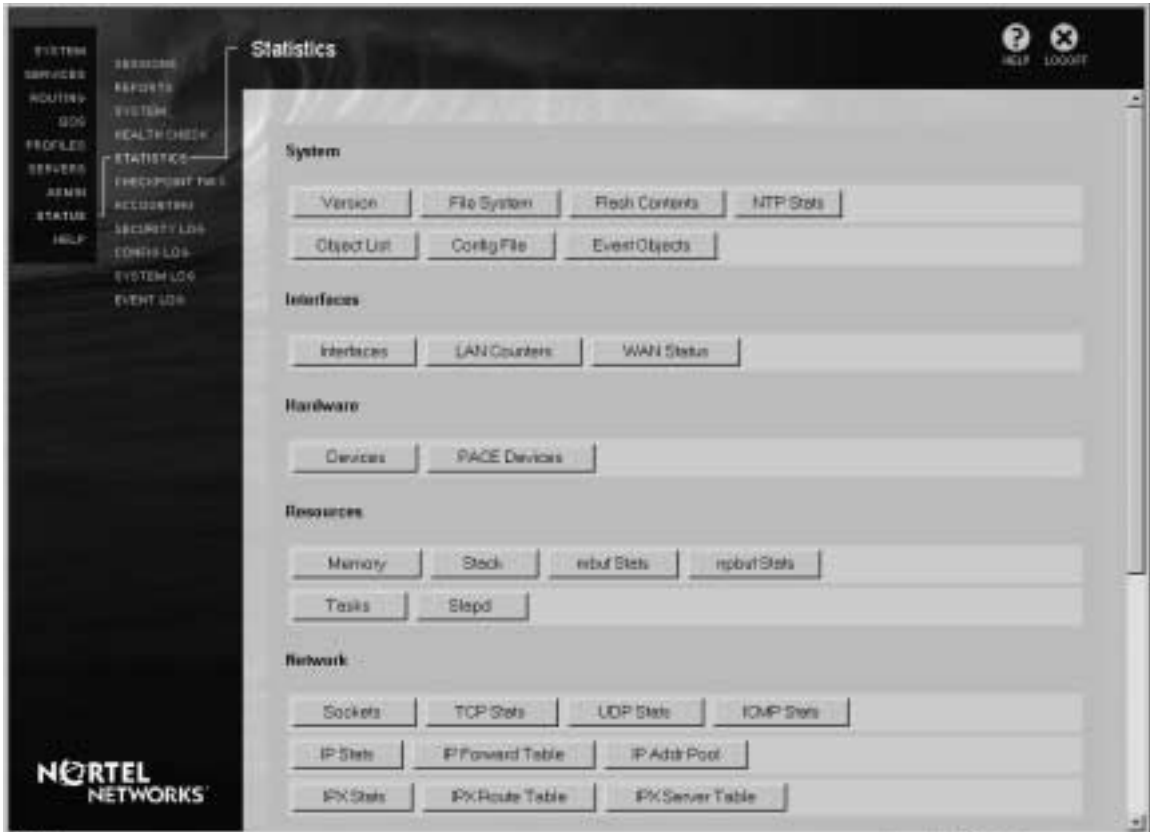
Table 45 Health check messages from SNMP traps (continued)

Status	Description	Comments
Warning	Server is down	At least one server is not running and is not selected.
OK	Operational	Server is running and is selected.
Load Balancing Service		
Warning	Timed out waiting for response from server	Load Balancing is enabled and configured, but the server is not responding.
OK	Server not configured	Load Balancing is enabled but no server is configured.
Disabled	Server not enabled	Load Balancing is not enabled on the Services→IPsec screen.
DNS Servers		
Alert	Error	None of the configured servers are operational.
Warning	Operational	At least one server is operating properly but another server has errors.
CMP Enrollment		
Alert	One or more request errors	Indicates that one or more errors have been encountered.
OK	One or more requests waiting	Indicates a certificate request is pending.
External LDAP Authentication Server		
OK	Operational	Indicates server is reachable and communicating with the switch.
Disabled	Server not enabled	Indicates feature is disabled or all configured servers are disabled.
Warning	Server is down	Indicates at least one server is not reachable and at least one server is reachable.
Alert	Server is down	Indicates all servers are not reachable.

Statistics

The Statistics screen provides numerous subscreens with a wealth of general and diagnostic information about the switch hardware, software, and connections. Much of the information is specifically designed for Nortel Networks Customer Support personnel to assist them in diagnosing problems. Some screens, however, such as the LAN Counters, Interfaces, and the WAN Status might provide you with some interesting traffic insights.

Figure 163 Statistics



Buttons

Version

Shows the software version number (for example, V01_05_01.33), creation date, and build level (for example, BL029).

Tasks

Shows the jobs that are currently running within the switch, including the name, task ID, priority, status, error number, and delay.

Interfaces

Shows the various interface characteristics, including IP and broadcast addresses, subnet masks, the Ethernet address, maximum transfer unit size, packets in and out, multicast packets in and out, and input and output errors.

Stack

Shows the stack characteristics and pointers to the tasks, including name, entry, task ID, and size.

Memory

Shows how memory is being allocated in the switch, including the current free and allocated memory and the cumulative memory. The information includes status, bytes, blocks, average and maximum block sizes.

ARP Table

Shows the link-level Address Resolution Protocol (ARP) information, including the IP address, destination, gateway, and interface.

Route Table

Shows the internal routing table.

Sockets

Shows the port numbers to which the TCP/IP and UDP protocols are bound.

TCP Stats

Shows the system-wide TCP statistics.

UDP Stats

Shows the system-wide UDP statistics.

ICMP Stats

Shows the system-wide ICMP statistics.

IP Stats

Shows the system-wide IP statistics, including total packets, frames too short and too small, bad header lengths, inbound and outbound fragments, fragments dropped and timed out, packets forwarded, redirects, and reassembled.

Mbuf Stats

Shows the memory for forwarding packets.

File System

Shows the key statistics for each of the switch's devices, including sectors, bytes per sector, sectors per cluster, and reserved sectors.

Devices

Shows the device drivers associated with the switch.

LAN Counters

Shows the many LAN transmit and receive counters, all of which are standard for Ethernet devices and are reasonably self-explanatory.

WAN Status

Shows the WAN state variables, configuration values, frame counters, signal values, and the following values.

Table 46 WAN status values

IP fragments received	Description
Routing Filter Drops	Packets filtered because no access rights are permitted to the resources specified by the designated filters.
Local System Filter Drops	Packets destined for the management interface that are dropped due to lack of authorization access.
Local Interface Filter Drops	Packets destined for a physical interface are dropped due to lack of authorization access.
PAT Drops	Public Address Table (PAT) drops are the number of packets dropped before being authenticated and having a tunnel established.
IP Header Error Drops	Packets with an error in the IP header.

Security Stats

Shows security statistics including total and active sessions by tunnel type and quality of service level, authentication failures, dropped sessions, and so forth.

Slapd

Shows internal LDAP statistics.

Flash Contents

Shows the contents of non-volatile memory.

Object List

This information is for Nortel Networks software engineers only.

Config File

Shows the ASCII contents of the configuration file that is currently in use.

IP Addr Pool

Shows the IP addresses listed in the internal address pool, including the total number and the number of addresses allocated.

PACE Statistics

Shows metrics that are used by the Packet Content Engine, a Nortel Networks internal system.

Event Objects

Shows the internal software objects that are active.

IPX Route Table

Shows the IPX routing table.

IPX Server Table

Shows the IPX server table.

IPX Stats

Shows the IPX statistics.

FIPS

Indicates the status of the switch’s FIPS Certification Mode.

Load Balancing

Shows the traffic load allocation.

Check Point FW-1 Stats

Shows statistics for the integrated Check Point FireWall-1, such as the policy, and rejected and accepted data.

Check Point FW-1 Version

Shows the version and build information for the Check Point FireWall-1

Check Point FW-1 Info

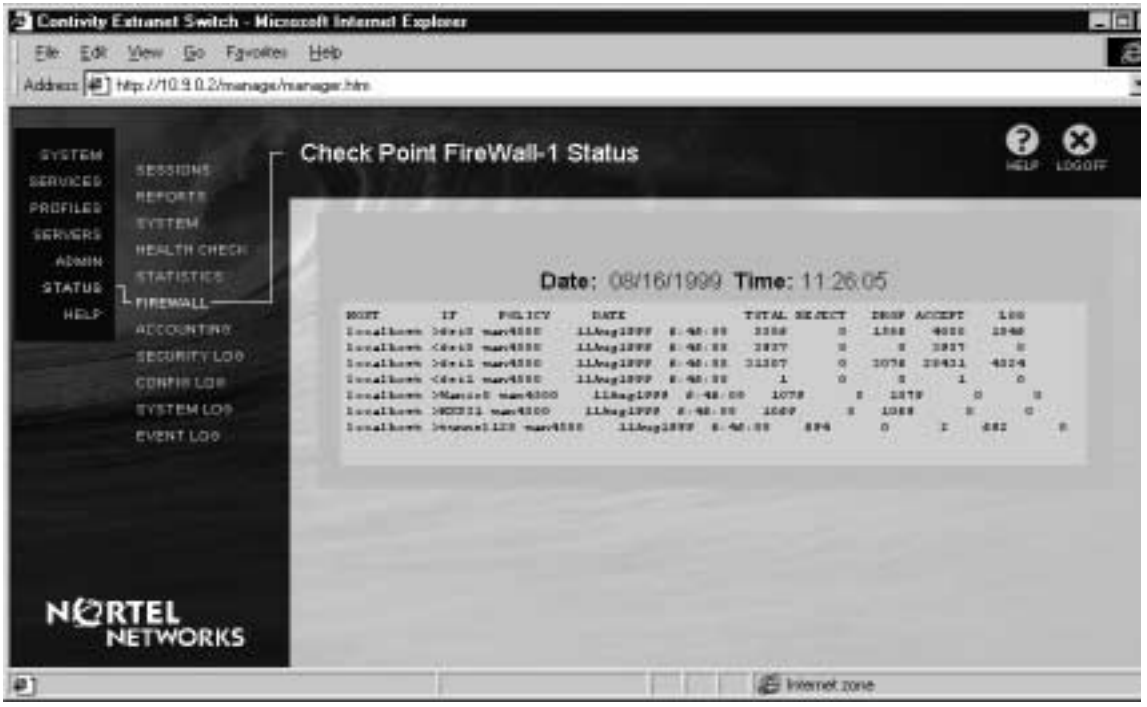
Shows a log file of the Check Point FireWall-1 activity. This information is useful for troubleshooting.

Firewall

The Firewall screen shows the details of the Firewall monitoring session. It is only used for the optional integrated Check Point firewall. This screen provides the same information as the Check Point firewall FW stat -l command.

The message “FW-1 not loaded” is shown if you have specified either the Contivity Firewall or No Firewall on the Services→Firewall screen.

Figure 164 Check Point FireWall-1 Status



Host

The Host is always the “localhost,” which is the switch that you are currently managing.

Interface

Inbound and outbound packets through the Interface are indicated by the left and right arrows, respectively.

Policy

This is the name of the Policy that is currently in use; default is **Standard**.

Date

This is the Date that the Policy was loaded.

Statistics

The Statistics that are returned provide information about the success or failure of the packet transmissions.

Accounting

Accounting logs User sessions. The Log provides Last and First Names, User ID, Tunnel type, session Start and End Dates, and the number of Packets and Bytes transferred. You can search the log according to most of these fields.

Figure 165 Partial Accounting

Accounting Records

Display

Click to choose between:

- All Sessions
- End User Sessions
- Branch Office Sessions

Search

Enter any combination of the search fields by which you want the log to display, and click Search. You can enter a combination of database field requirements (the search fields can be combined to allow more restrictive searches and narrow the options).

For example, instead of searching for the Last Name OToole only, search for:

Last Name: OToole

End Date: 12/5/97

Type: IPsec

All of the listed criteria must be satisfied. This then displays all activity for anyone named OToole who terminated the IPsec Tunnel Type on 12/5/97.

For Local (nontunneled) sessions certain fields are left blank (for example, Last Name, Packets, Kbytes).

Last Name

Shows the user's last Name.

First Name

Shows the user's first Name.

User ID

Shows the Session User ID.

Group

Allows you to search by user groups name when you screen End User Sessions or by branch office name when you display Branch Office Sessions.

Type

Shows the type of tunnel session used. Possible tunnel type sessions include (refer to the "Tunnel Configuration Overview" section for details):

- IPSec
- PPTP
- L2TP
- L2F

Start and End Dates

Shows the start and end session dates (m/d/y) if the session started and stopped on the same day. If the start and end dates are different (the session starts on Monday and ends Tuesday or later) both dates are displayed.

Session Fields

Some of the session fields are the same as those listed above. Refer to the above references for those descriptions.

Name

Shows the user names.

Subnet

Shows the subnet in which the user's system resides.

Time

Shows the session start and end times (hh:mm:ss). If the start and end dates are different (the session starts at 18:00 on Monday and ends Tuesday at 03:15) both dates are displayed in the Date field.

Date

Shows the date of the user session.

Packets

The number of Packets transmitted in and out of the switch during the session.

Kbytes

Shows the number of Kbytes transmitted In to and Out of the switch during the session. The switch does not display bytes transmitted in and out for an Administrator session.

Session ID

Shows a system-allocated user Session ID.

User ID

Shows the User ID for the tunnel session.

IP Address

Shows the inner IP Address (Local) and the outer IP Address (Public) of the client devices that are connected to the switch.

IPX Address

Shows the inner IPX Address (Local) and the outer IP Address (Public) of the client devices that are connected to the switch.

Links

Shows the number of PPP links associated with this session.

Historical event logging

The switch has several logs that provide different levels of information, including:

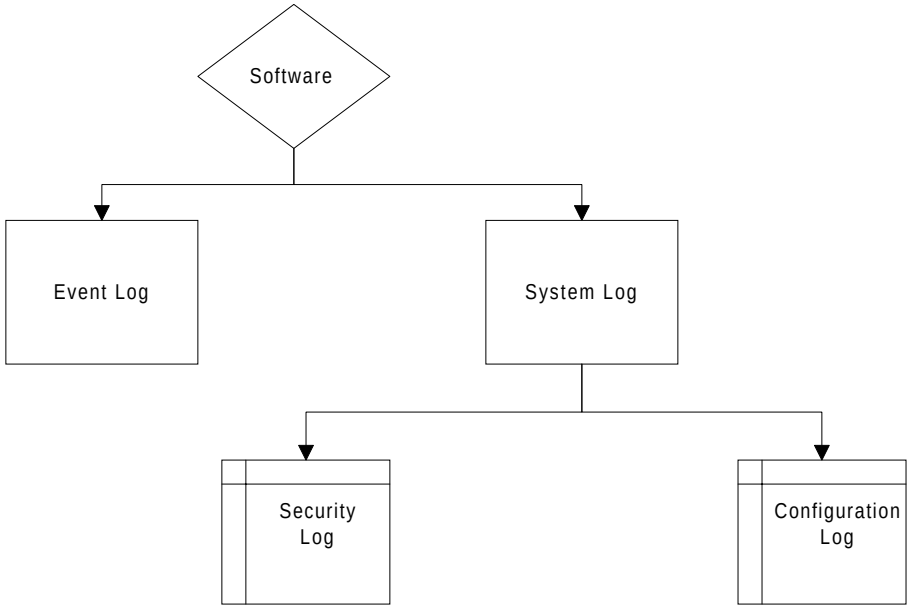
- Event Log
- System Log
- Security Log
- Configuration Log

The logs are stored in text files on disk and they indicate what happened, when, and by whom (IP address and user ID).

The Event Log captures real-time logging over a relatively short period of time (for example, the Event Log could wrap its 2000 possible entries in minutes). The System Log captures data over a longer period of time, up to 61 days.

Most events are sent to the Event Log first. Significant events from the Event Log are sent to the System Log. Not all data that is saved by the System Log comes from the Event Log, but that is generally the case. The switch filters from the System Log security entries for the Security Log and configuration entries for the Configuration Log.

Figure 166 Nortel Networks logging scheme



The different Log options allow you to write specific event levels to the log files and view them, including:

- Normal
- Urgent
- Detailed
- All

Common logging fields

Introductions to the specific logs appear with each sample log screen. Following are the common field descriptions for the log file screens.

Date

Click to select the Date (mm/dd) of the log you want to view. Then click Display.

This field provides log files for up to the last 61 days.

Display Level

Select the appropriate Log Display level from the following options.

Normal

Normal events are the everyday user and system interactions that allow you to review switch activity; for example:

- Logins
- Configuration changes
- Scheduled or actual shutdowns

Urgent

Urgent Events are marked with an asterisk in the left column of the log. Urgent Events are those that you want to be aware of immediately and that could potentially pose security or access problems; for example:

- Attempts to login with the wrong password.
- Attempts to gain Administrator Access.

Detailed

Detailed Events are designed specifically for use by Nortel Networks Customer Support personnel to uncover or troubleshoot problems.

All

All Events are also designed specifically for Nortel Networks Customer Support personnel. They include every log message that the system generates, including many details that are not of general interest but might allow Nortel Networks to uncover or troubleshoot problems.

Display

Click to view the log for the selected Date and Level.

Entries

An asterisk indicates an Urgent entry.

A time stamp indicates when (hours:minutes:seconds) the entry was logged.

A task name indicates the software task logging the message. Generally, these tasks refer to the internal system mechanisms and are for Nortel Networks Customer Support personnel only.

The numbers between brackets [01] indicate whether the event is saved to the System Log and also its priority level. If the first number is a one, then the event is sent to the System Log; when it is a zero it is in-memory information. The priority level for the second number is as follows:

0 - Debug

1 - Low

2 - Medium

3 - High

Therefore, the numbers in brackets [12] represent an event that is sent to the System Log and is considered to be of Medium priority.

The task type indicates the actual type of task that was recorded, for example, Security. Task types are often followed by a corresponding task type number.

A brief message describes the entry.

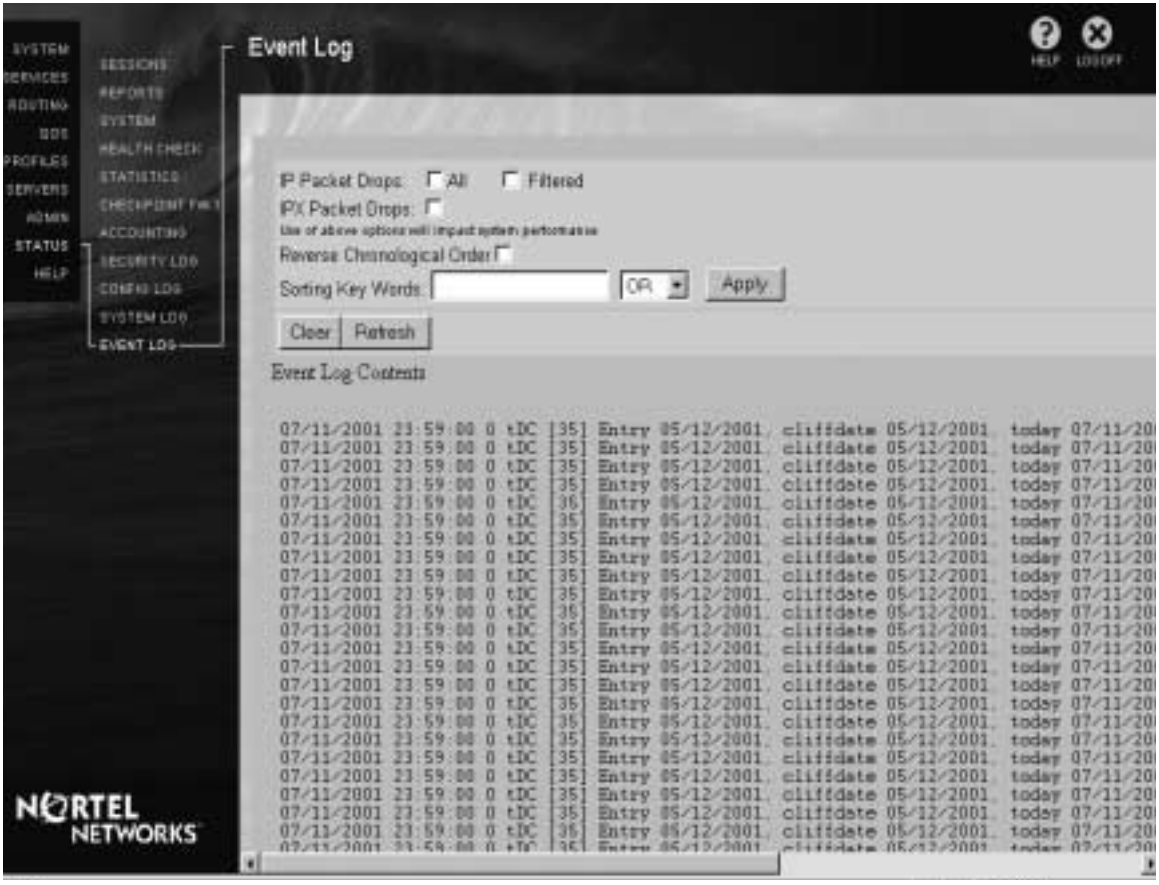
Event log

The Event log is a detailed recording of all events that take place on the system. These entries are not necessarily written to disk, as with the System log. The Event Log retains all system activity in-memory but only the significant entries are saved in the System log (on disk).

The Event log includes information on tunneling, security, backups, debugging, hardware, security, daemon processes, software drivers, interface card driver events, and so forth.

As the Event log adds in-memory information, its oldest entries are overwritten. The Event log retains the latest 2000 entries, and discards old entries when it is refreshed.

Figure 167 Event Log



IP Packet Drops

This option logs an IP dropped packet header (source and destination address). Packets can be dropped due to filtering, corruption, and so forth.

All Packets

This option logs the contents of all packets.

Filtered Packets

This option logs the contents of filtered packets.

IPX Packet Drops

This option logs an IPX dropped packet header (source and destination address). Packets can be dropped due to filtering, corruption, and so forth.

Reverse Chronological Order

Enable this option to log in reverse chronological order.

Sorting Key Words

You can sort the log based on key word matches.

Enter a list of key words, separated by a space or a comma, in the first field.

Select the type of match you want from the list box. Select AND to match all key words. Select OR to match any key words.

Clear

Click to Clear the entire log. Only Administrators can clear the log.

Refresh

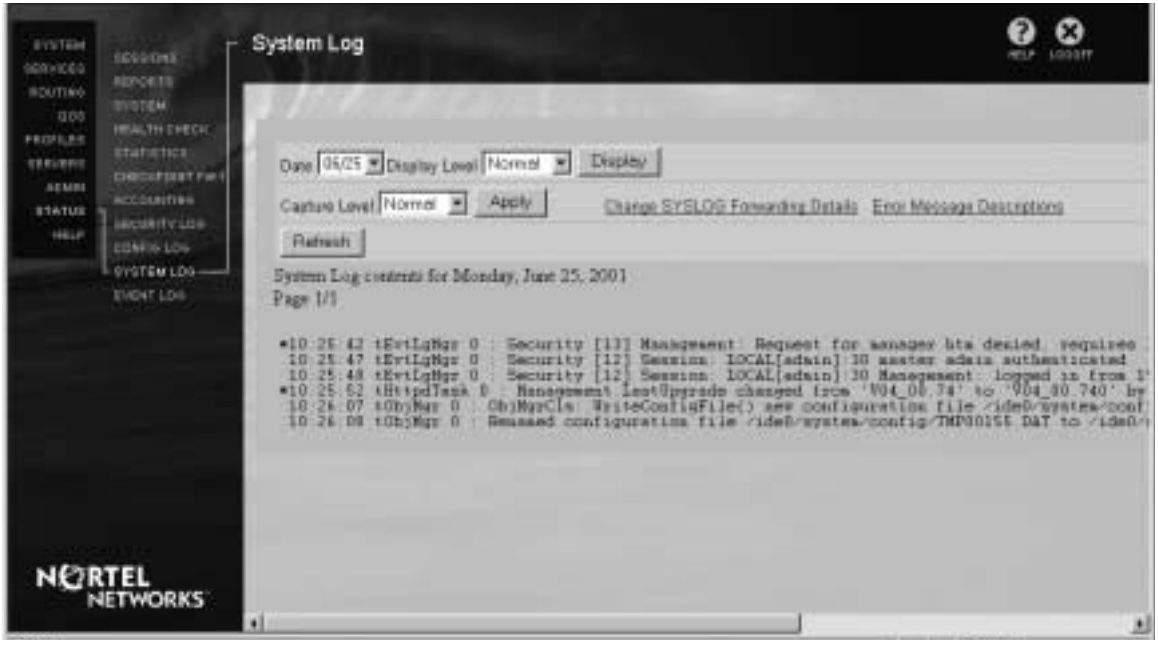
Click to display new log entries.

System log

The System log contains all System events that are considered significant enough to be written to disk, including those displayed in the Configuration and Security logs. Examples of events that would appear in the System log include:

- LDAP activity
- Configuration activity
- Server authentication and authorization requests

Figure 168 System Log



System Log Contents for *Date*

This is the date (day/month/year) of the log file that is currently being displayed. When you change the Date field, then click Display, the new date's log file is displayed and the System Log Contents for *date* field changes to reflect the new request.

Capture Level

The Capture Level option allows you to filter between saving to disk all events including Debug events, and saving Normal and Urgent events only.

Note: Capturing All Events adds a small amount of system overhead and similarly takes a minor toll on performance. Therefore, you should probably capture Debug events at the request of Nortel Networks personnel only.

Normal

These are the events that are normally of typical interest to you.

Urgent

These events would be of critical interest to you. They could represent a severe security or access problem; or even something that might have happened accidentally but if it recurred would be cause for concern.

All

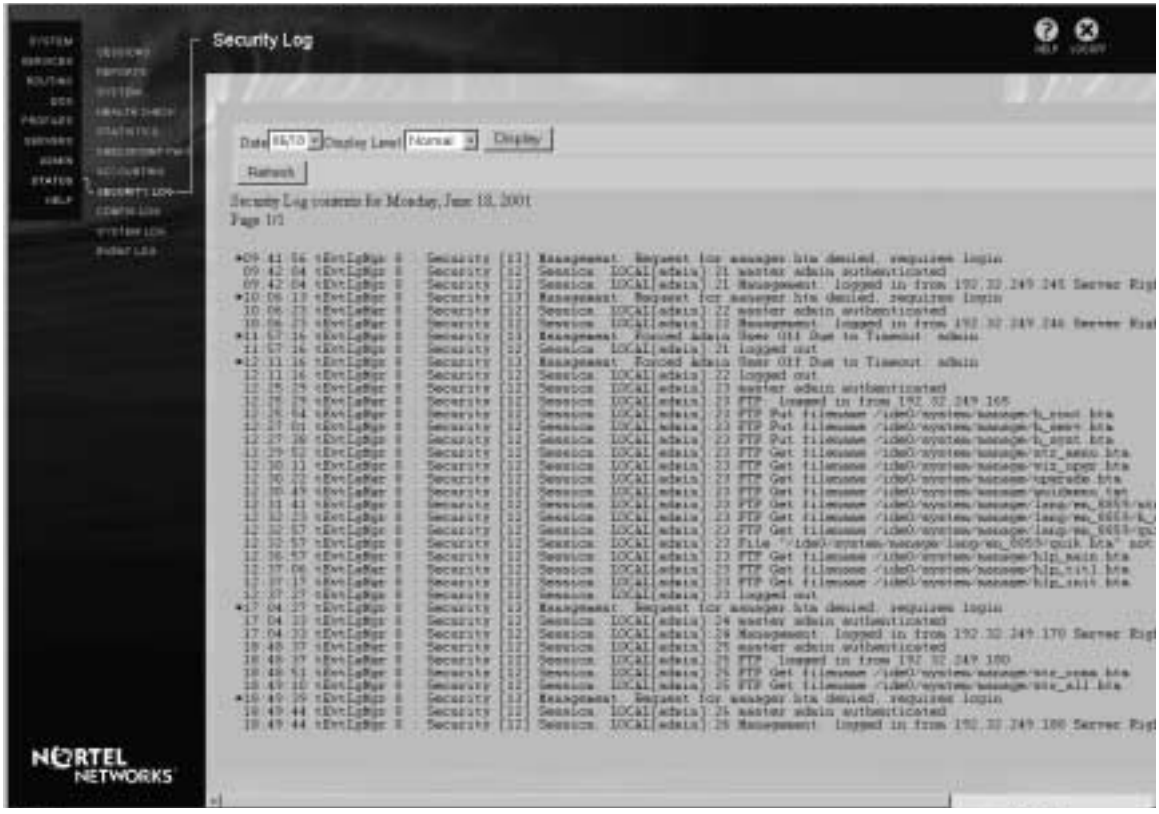
These events allow Nortel Networks Customer Support personnel to learn additional factors that might be contributing to a problem.

Security log

The Security log records *all* activity about system or user security. The Security log lists all security events, both failures and successes. The events can include:

- Authentication and authorization events
- Tunnel or administration requests
- Encryption, authentication, or compression
- Hours of access
- Number of session violations
- Communications with servers
- LDAP
- RADIUS

Figure 169 Security Log

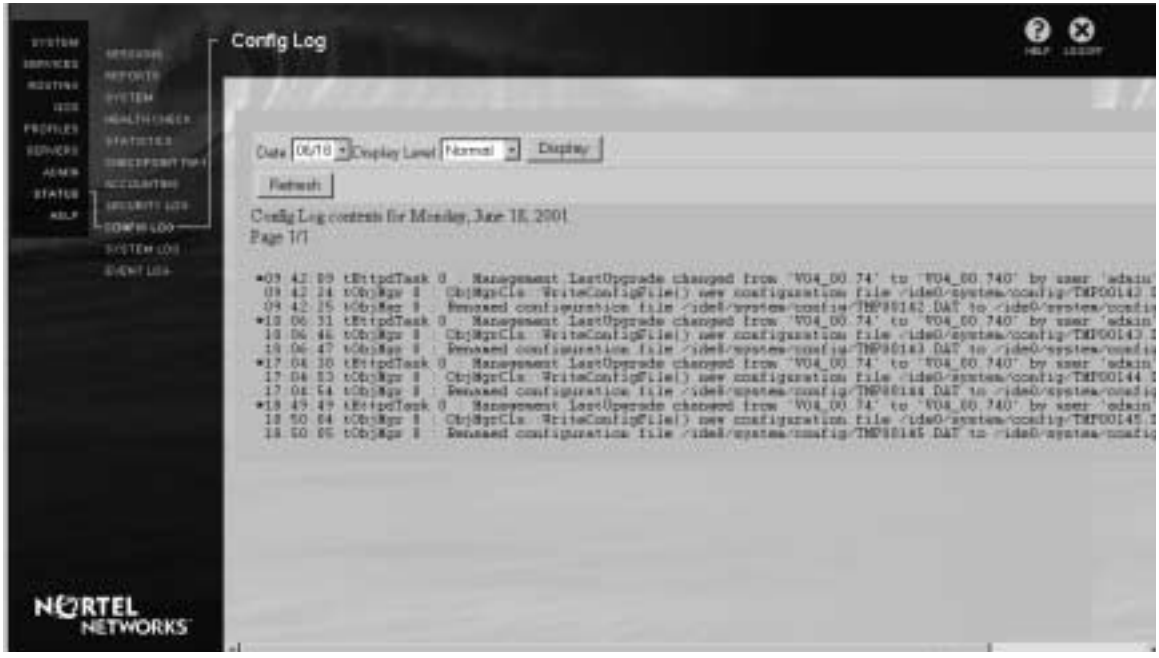


Configuration log

The Configuration log records all configuration changes. For example, it tracks adding, modifying, or deleting configuration parameters:

- Group or user profiles
- LAN or WAN interfaces
- Filters
- System access hours
- Shutdown or startup policies
- File maintenance or backup policies

Figure 170 Configuration Log



Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X