Novell BorderManager®

3.7

www.novell.com

ADMINISTRATION

Novell®

Legal Notices

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Administration
April 2002
103-000236-001

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

Novell is a registered trademark of Novell, Inc., in the United States and other countries.
BorderManager is a registered trademark of Novell, Inc. in the United States and other countries.
ConsoleOne is a registered trademark of Novell, Inc. in the United States and other countries.
Internetwork Packet Exchange is a trademark of Novell, Inc.
IPX is a trademark of Novell, Inc.
LANalyzer is a registered trademark of Novell, Inc., in the United States and other countries.
NCP is a trademark of Novell, Inc.
NDS is a registered trademark of Novell, Inc., in the United States and other countries.
NetWare is a registered trademark of Novell, Inc., in the United States and other countries.
NetWare Connect is a registered trademark of Novell, Inc., in the United States and other countries.
NetWare Core Protocol is a trademark of Novell, Inc.
NetWare Link Services Protocol is a trademark of Novell, Inc.
NetWare Loadable Module is a trademark of Novell, Inc.
NLM is a trademark of Novell, Inc.
NLSP is a trademark of Novell, Inc.

Third-Party Trademarks

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

Introduction

The purpose of this documentation is to describe how to administer the components of Novell® BorderManager® 3.7. The audience for this documentation is experienced network administrators.

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

Access Control

The following section of the *Novell® BorderManager® 3.7 Administration* guide describes how to manage the access control log file:

- Chapter 1, “Managing Access Control,” on page 15

See the Setting Up Access Control section in the *Novell BorderManager 3.7 Installation Guide* for information on how to set up access control files.

1 Managing Access Control

The following sections explain the tasks you must complete to manage Novell® BorderManager® 3.7 access control by checking the access control log:

Viewing User Statistics

To display the User Statistics window:

1. In NetWare® Administrator, click the Server object representing the Novell BorderManager 3.7 server.
2. Click Tools > Novell Novell BorderManager 3.7.
3. Click Novell Novell BorderManager 3.7 > View Access Control.

   The Access Control Users Statistics window has two list boxes: the Number of Users list box and the Hosts Accessed by User list box. Initially, the list boxes are empty.
4. To display the records for a set of connections from a specific user to a specific host, select Display Records and enter a time range for the records you want displayed.

   For a U.S. English system, the dates are entered in the order of month, day, and year. The order is year, month, and day for a Japanese system; and day, month, and year for European language systems.

   While the records are being read, a dialog box displays the number of records processed, the date and time of the last record that was read, and

a status bar showing the portion of the records read based on the range of dates specified. Cancel the query process at any time by clicking Cancel. Records that have been read are displayed in the Access Control Users Statistics window.

NOTE: You can click the column heading of either list box to sort the entries in that column in ascending or descending order. The sorting order is reversed each time you click the column heading.

The Number of Users list box provides the following information about activity through access control:

- Username—NDS® or eDirectory™ name or IP address of the user. In the case of an IP address, the Domain Name System (DNS) domain name will be displayed if it exists in the local DNS list. The local DNS list is built each time the command WHO IS or DNS Hostname is invoked using the right-click menu.
- Hosts Accessed—Number of hosts accessed for the specified period of time.
- Connections—Total number of connections used to access hosts.

The Hosts Accessed by User list box provides the following information about activity through access control:

- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS name or IP address of the accessed host.
- Allowed—Total number of connections granted access to the host for a user.
- Denied—Total number of connections denied access to the host for a user.

5 To display additional types of user information:

5a To display all the connections made by a user, double-click a username in the Number of Users list box.

The Access Control Log window displays the following information about the user's activity through access control:

- Entry Time—Time connection was established.
- Username—NDS or eDirectory name or IP address of user.
- Access—Action specified in the access rule for this connection.

- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS name or IP address of the accessed host.
- Service—Service used to access the host: Proxy Services or Novell IP Gateway.
- Rule Number—ID number of the rule that grants or denies access to hosts.

5b To see a description of the rule for a connection between a user and a host, double-click the connection entry in the Access Control Log window.

The Rule Description window provides the following information about activity through access control:

- Rule Number—ID number of the rule that grants or denies access to hosts.
- Date of Creation—Day and time the rule was created.
- Action—Whether the connection is allowed or denied.
- Source—IP address, hostname, or interface name of the connection source to which the rule is applied.
- Destination—IP address, hostname, or interface name of the connection destination to which the rule is applied.
- Access Specification—Any protocol, URL, or SurfControl* rule that determines connection access or denial.

5c To view usage trend graphs, click Usage Trends in the User Statistics window > select any of the following graphs to view usage trend data by time of day in one-hour increments:

- Users—Bar graph showing the number of unique users allowed to connect to a host.
- Hosts Accessed—Bar graph showing the number of hosts accessed.
- Access Volume—Line graph showing the number of allowed and denied connections.
- Access Allowed—Bar graph showing the number of allowed connections.

- Access Denied—Bar graph showing the number of denied connections.
- Users, Hosts, and Access Volume—Combination line and bar graph showing the number of users, hosts accessed, and total connections.

All graphs can be saved to disk, copied to the clipboard, or printed.

Viewing Host Statistics

To display specific host information:

1. In NetWare Administrator, click the Server object representing the Novell BorderManager 3.7 server.
2. Click Tools > Novell Novell BorderManager 3.7.
3. Select Novell BorderManager 3.7 > View Access Control.
4. To display the records for a set of connections from a specific user to a specific host, click Display Records and enter a time range for the records you want displayed.
5. To see which users have accessed a host, double-click the entry for that host in the Hosts Accessed by User list box in the User Statistics window.

   The Access Control Hosts window displays two list boxes: the Number of Hosts list box and the User Access list box. As in the User Statistics window, the entries can be sorted by selecting the column headings.

   The Number of Hosts list box provides the following information:

   - Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
   - Hostname—DNS name or IP address of a host.
   - Users Accessed—Number of users who have accessed the selected host.
   - Connections—Number of connections that have been allowed access.

   The User Access list box provides the following information:

   - Username—IP address or DNS name of the user who accessed the host.

- Allowed—Number of connections granted access to the host.
- Denied—Number of connections denied access to the host.

6 To see a list of connections for users who have accessed a host, double-click the entry for the host in the Host Statistics window.

The Access Control Log window for the selected host is displayed. The Rules Description window can be viewed by double-clicking an entry.

The Access Control Log list box provides the following information about activity for the selected host through access control:

- Entry Time—Time connection was established.
- Username—NDS or eDirectory name or IP address of the user.
- Access—Action specified in the access rule for this connection: either Allowed or Denied.
- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS domain name or IP address of the accessed host.
- Service—Service used to access the host: Proxy Services or Novell IP Gateway.
- Rule Number—ID number of the rule that grants or denies access to the hosts.

Exporting Data

The access control log is stored in a Btrieve* file on the Novell BorderManager 3.7 server and is maintained by CSAUDIT.NLM. The access log cannot be edited or manipulated from the server; however, the data can be exported for analysis. The format of the exported data is compatible with trend analysis software packages, such as WebTrends*.

There are two ways to export the access control log from NetWare Administrator:

- “Exporting Data from the Access Control Users Statistics Window” on page 20
- “Exporting Data Using the Export Logs Option” on page 21

If you use the second method, you can also combine the audit log files from other Novell BorderManager 3.7 services with the access control log into a single ASCII file.

Exporting Data from the Access Control Users Statistics Window

To export records from the Access Control Users Statistics window:

1. In NetWare Administrator, click the server object representing the Novell BorderManager 3.7 server.
2. Click Tools > Novell Novell BorderManager 3.7.
3. Click Novell BorderManager 3.7 > View Access Control.
4. Click Display Records > enter the dates for the records you want to display > click OK.
5. In the Access Control Users Statistics window, click Export Data > enter the path and filename.

   Or

   Click Browse to select the destination of the export file.
6. Select one of the following sort formats under Information Output Selection and click OK.
   - Entry Time (connection by connection)—(Default selection) Sorts records from the earliest entry time to latest entry time.
   - Access by users—Sorts records in alphabetic order based on the user's NDS or eDirectory username.
   - Access by hosts—Sorts records in ascending order (for IP addresses) or alphabetic order (for DNS hostnames).
7. If the export filename already exists under the directory path selected, you are prompted to replace the file. Click Yes to overwrite the file or No to specify the destination as described in Step 5 on page 16.

The record fields are written to disk with a tab as the delimiter. Each record ends with a carriage return and line feed. The exported data has the following format:

- Entry Time—Time connection was established.
- Username—NDS or eDirectory name or IP address of the user.

- Access—Action specified in the access rule for this connection: either Allowed or Denied.
- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS name or IP address of the accessed host.
- Service—Service used to access the host: Proxy Services or Novell IP Gateway.
- Rule Number—ID number of the rule that grants or denies access to the hosts.

Exporting Data Using the Export Logs Option

The procedure to export access control data using the Export Logs option from the Novell BorderManager 3.7 menu extracts the same data from the Btrieve database, but offers additional export options that cannot be activated from the Access Control Users Statistics window.

To export the access control log:

1. In NetWare Administrator, click the server object representing the Novell BorderManager 3.7 server.
2. Click Tools > Novell Novell BorderManager 3.7.
3. Click Novell BorderManager 3.7 > Export Logs.
4. Click Set Range to enter the date range.

   This is the range of dates comparable to the dates used to display records in the Access Control Users Statistics window. The default range is the current server date.
5. Click Browse to select the drive mapped to the destination for the export file.

   This is the path and filename for the export file. The default destination is A:\YYYYMMDD.LOG, where YYYY is the current year, MM is the current month, and DD is the current day. If you change the filename from the default format, the filename will not reflect the current server date. For example, if you change the filename format to MMDDYYYY.LOG, the next time you try to export logs on another day, the log filename will not have incremented to the current date.

6. (Optional) If the default filename is unacceptable, enter the filename in the File field.

7. (Optional) If you want to combine the access control log with audit logs from other Novell BorderManager 3.7 services, check the Combine Log Files check box.

   This feature allows log files from different services to be combined into a single output file. When log files are combined, they are appended to one file, service by service.

8. Under Log Selection, check the box for ACL.

   If the Combine Log Files feature has been selected, check all the services whose data will be combined into the export log file.

9. (Optional) If you checked Combine Log Files in Step 7, under Log Selection, check all other Novell BorderManager 3.7 services audit log files to be combined with the access control log file.

10. Click OK.

The access control log is exported to an ASCII file. The record fields are written with a tab as the delimiter. Each record ends with a carriage return and line feed. The exported access control data has the following fields:

- Keyword—ACL. If the Combine Log Files option was selected, the keyword is at the beginning of each line from the access control list (ACL) audit log.
- Date.
- Time.
- Source—Typeless eDirectory name and context, such as mlira.pubs.novell, or an IP address.
- Destination—Domain name or IP address.
- Bytes received.
- Status—Allow or Deny.
- Protocol—Protocol used, such as HTTP or FTP.
- Service—Service used to access the host: Proxy Services or Novell IP Gateway.
- Rule ID—An 8-digit hexadecimal number that identifies the rule associated with the allowed or denied access.

If the Combine Log Files feature is *not* selected and you select one or more services under the Log Selection field, a separate export file is created for each service under a subdirectory of the export destination path.

The export subdirectories used are shown in the following table.

Log Type	Export Subdirectory
HTTP Proxy	HTTP
FTP Proxy	FTP
NNTP Proxy	NNTP
Mail Proxy	SMTP
RealAudio* and Real Time Streaming Protocol (RTSP) Proxies	RAUDIO
DNS Proxy	DNS
Generic Proxy	GENERIC
SOCKS Client	SOCKS
IPX Gateway (Novell IP Gateway)	IPXGW
VPN	VPN
ACL (access control)	ACL

For example, if you specified an export destination of VOL1:LOGS\19981019.LOG, did not select the Combine Log Files feature, and checked the boxes for HTTP Proxy, SOCKS client, and ACL, the following log files would result:

- VOL1:LOGS\HTTP\19981019.LOG
- VOL1:LOGS\SOCKS\19981019.LOG
- VOL1:LOGS\ACL\19981019.LOG

Alerts

The following section of the *Novell® BorderManager® 3.7 Administration* guide provides the basic information you need to set up Novell BorderManager 3.7 Alert. To view alert messages and to know how to respond to them see:

- Chapter 2, “Managing Alert Messages,” on page 27

See the Setting Up Alert Notification section in the Novell BorderManager 3.7 Installation Guide for information on how to set up alerts.

2 Managing Alert Messages

The following sections describe how to view alert messages generated by Novell® BorderManager® 3.7 Alert and how to respond to them:

Viewing Alerts Sent as E-Mail Messages

All e-mail notifications triggered by Novell BorderManager 3.7 Alert contain a time stamp, the name of the server where the event occurred, the service affected, and an error message.

NOTE: When the message is sent to a pager, the time stamp, server name, and error message appear first, followed by the sender, recipient, and subject. This is done to accommodate paging services that limit the amount of alphanumeric text that is displayed.

In the sample e-mail message that follows, substitute your own Domain Name System (DNS) domain name for novell.com:

From: *nbmalert@novell.com*

To: *admin_1@novell.com admin_2@novell.com*

Subject: The system is short on disk space and operations may fail

Time: 7-17-98 9:45:07am

Server: SJ-NW5

Service: NetWare Operating System

The system is short on disk space and operations may fail

NOTE: If a loaded NetWare® Loadable Module™ (NLM™) causes the alert, the e-mail message might not always identify the offending NLM because the NLM that detected the error might be reported instead. Therefore, load MONITOR.NLM to check any unusual statistics if the cause of the alert is not clearly evident.

If Novell BorderManager 3.7 Alert has been configured and e-mail notification fails to occur when alerts are displayed on the server console, verify the following:

- The alert condition has been enabled for notification in NetWare Administrator.
- All e-mail addresses configured for the Novell BorderManager 3.7 server are for valid accounts.
- The primary and backup e-mail servers have e-mail forwarding enabled.
- The primary e-mail server or at least one backup e-mail server is up and running.
- All NDS® or Novell eDirectory™ partitions have been synchronized if the alert configuration was recently changed. A delay in synchronization can mean that your server has not been updated with the latest configuration, especially if the alert configuration applies to an entire organization.
- A route to the mail server has been established. Ping the mail server from the Novell BorderManager 3.7 server and inspect the trace on the route.
- There are no filters on routers between the Novell BorderManager 3.7 server and the mail server that deny Simple Mail Transfer Protocol (SMTP) traffic.

Viewing Alerts in Audit Trail Log File

Novell BorderManager 3.7 Alert logs server events in the audit trail log file. The alert record contains information such as the type of alert, a description of the event, the name of the server that generated the alert, and a time stamp. Use the audit trail log file to check for anomalies or suspicious activities that affect routing and security on your network.

The audit trail log file, CSAUDIT.LOG, is maintained by CSAUDIT.NLM. The audit trail log file is managed with the CSLIB audit trail utility. Use this

utility to view records in the audit trail log and configure a schedule for archiving the log. The active audit trail log file is located in SYS:SYSTEM\CSLIB. Archived audit log files are located in SYS:SYSTEM\CSLIB\LOGS.

This section contains the following procedures:

Displaying Audit Trail Log Records with Audit Trail Utility

To view the audit trail log file:

1. To run the CSLIB audit trail utility from the server console, enter

   CSAUDIT

2. Click Display Audit Trail Records.

   The currently active log file is displayed. If the current log file has the record you need, you are done. Otherwise, to view an archived log file, continue with Step 3.

3. Press *Insert* to view the other display options.
4. Click Display Options menu > Select from Archived File List.
5. Use the *Up-arrow* and *Down-arrow* to locate the archived log file to view.
6. Press *Enter* to view the records in the log file.
7. Press *Esc* until you are prompted to exit the audit trail utility.

Archiving the Audit Trail Log File

As with most log files, the audit trail log file can grow rapidly. Because the audit trail log file is stored on the SYS: volume, it is important to archive it and rotate the archived log files on a regular basis.

To configure the frequency of archiving and the number of archived log files, complete the following steps:

1. From the server console, enter

   CSAUDIT

2. Click Audit Trail Configuration.

3 Press *Enter* in the Archive Hour field and select the hour at which the audit trail log file should be archived.

4 In the Archive Interval field, enter the number of days for which the active audit log file records data.

5 In the Archive Files Retained field, enter the number of audit log files that will be archived before the first archived file is overwritten.

6 Press *Esc* > select Yes to save the changes.

7 Press *Esc* until you are prompted to exit the audit trail utility.

Viewing Alerts in Control Log

Because Novell BorderManager 3.7 Alert sends alert messages to the server console, if CONLOG is running on the server, the alert message is also saved in SYS:ETC\CONSOLE.LOG.

To view the console log at the server console, enter

LOAD EDIT SYS:ETC\CONSOLE.LOG

Responding to Alerts

Novell BorderManager 3.7 Alert monitors server performance, license acquisition for licensed Novell BorderManager 3.7 services, security, and Proxy Services availability.

For information on specific alerts:

- “Server Performance Alerts” on page 32
- “License Acquisation Alerts” on page 32
- “Security Alerts” on page 33
- “Proxy Alerts” on page 36

The following table describes some recommended responses to the Novell BorderManager 3.7 alerts.

Alert	Recommended Actions
Disk space shortage	Reduce the size and number of log files. Add more disk space, if necessary.

Alert	Recommended Actions
Memory shortage	Check server resources using MONITOR.NLM to determine whether a module is using excessive memory. Add more memory, if necessary. Depending on the bus type, some NetWare servers do not register all the memory present unless a REGISTER MEMORY statement exists in the STARTUP.NCF file. More information about REGISTER MEMORY is located in the NetWare 5 online documentation at the following path: Reference > Utilities Reference (under the General Reference heading) > Utilities > REGISTER MEMORY
ECB shortage	Check server resources using MONITOR.NLM to determine which NLM uses the most event control blocks (ECBs). Increase the maximum packet receive buffers on the server if server memory allows.
License error	Verify the current licenses installed for the server and check for license conflicts or expired trial licenses. Install additional licenses, if necessary.
Loading or unloading a security-sensitive NLM	This alert is primarily informational. Verify that the server console is secure and all remote sessions are authorized. Reload or unload the NLM, if necessary.
Oversized ping packet	Use a packet sniffer to capture packets and determine the source IP address. Configure a TCP/IP packet forwarding filter to block pings originating from that source.
SYN packet flooding	Use a packet sniffer to capture packets and determine the source IP address. Configure a TCP/IP packet forwarding filter to block TCP packets originating from that source.
Oversized UDP packet	Use a packet sniffer to capture packets and determine the source IP address. Configure a TCP/IP packet forwarding filter to block UDP packets originating from that source.
Cache hierarchy parent (ICP parent) down	Ping the parent server to check if there is a routing problem. Verify that the parent server for the cache hierarchy is down and bring the server back up. Note that if the cache hierarchy has multiple parents configured, proxy servers lower in the hierarchy will use the other parent servers while this server is down.

Alert	Recommended Actions
SOCKS server down	Ping the SOCKS server to check if there is a routing problem. Verify that the SOCKS server is down and bring the server back up.
POP3 or SMTP server down	Ping the Post Office Protocol 3 (POP3) or SMTP server to check if there is a routing problem. Verify that the POP3 server or internal mail server is down. You might not be able to resolve this problem if the POP3 server is administered by someone who is outside your organization.

Server Performance Alerts

Server performance alerts notify you of potential problems with server parameters or operations that can cause Novell BorderManager 3.7 services to underperform or fail.

The server performance alerts are as follows:

- Disk space shortage

  A disk space shortage warning indicates that the shortage of disk space is severe enough to potentially cause server operations to fail.

- Memory shortage

  A memory shortage warning indicates that the shortage of memory is severe enough to potentially cause server operations to fail.

- Event control block (ECB) shortage (out of receive buffers or no ECBs available)

  An ECB shortage warning indicates that the packet receive buffer or ECB shortage is severe enough to potentially cause network input or output to degrade or fail.

License Acquisation Alerts

A license alert indicates that a Novell BorderManager 3.7 service was unable to acquire the license it needs to operate.

Novell BorderManager 3.7 Alert monitors license acquisition for the following:

- Proxy Services
- Novell IP Gateway
- Virtual Private Network (VPN) servers and clients
- Access control

Security Alerts

Security alerts notify you of possible security breaches. The causes of these alerts should be investigated further because your server might be the target of a denial-of-service attack.

Denial-of-service attacks commonly plague servers connected to the Internet and are initiated by someone without authorized access to servers. A denial-of-service condition can be caused by a bombardment of packets sent to a server that consumes significant memory or CPU processing time. After these server resources have been allocated to handle the packets, connection requests made by legitimate users cannot be processed effectively.

As with computer viruses, new denial-of-service attacks are launched on the Internet community without warning. Many of the known denial-of-service attacks are documented on various Web sites.

The Novell BorderManager 3.7 security alerts include:

- Loading or unloading a security-sensitive NLM

  Security-sensitive modules are those that can potentially compromise network or server security when they are loaded or unloaded.

  The modules that are considered security-sensitive are

  - DS.NLM
  - FTPSERV.NLM
  - IPXIPGW.NLM
  - PROXY.NLM
  - REMOTE.NLM
  - TFTPSERV.NLM
  - VPNINF.NLM
  - VPMASTER.NLM
  - VPSLAVE.NLM

- Oversized ping packet

  An oversized ping packet warning can indicate that malicious activity is occurring on the server. This alert is generated when the server receives and discards ping packets that have more than 10,240 bytes of data. The server is enabled to discard these packets by default.

  For certain situations which require your server to receive larger ping packets, such as router stress tests, enter the following SET commands at the server console to change the largest ping packet size or disable packet discarding:

  SET LARGEST PING PACKET SIZE=*n*

  SET DISCARD OVERSIZED PING PACKETS=OFF

  The variable *n* is a decimal number representing the number of bytes allowed. Never specify a number with commas.

  To reenable packet discarding, enter the following command at the server console:

  SET DISCARD OVERSIZED PING PACKETS=ON

  NOTE: Because packet sizes are limited by the type of media used, you should know your network topology before changing the largest ping packet size. For Ethernet only, the oversized ping packet alert is not generated if the largest ping packet size is set between 35,541 and 65,535 bytes. However, alerts are generated for packets smaller than 35,541 bytes. The acceptable packet size ranges for other media differ and depend on each medium's maximum transmission unit (MTU)—the largest packet size a medium can transport without fragmentation.

- SYN packet flooding

  A TCP SYN packet flood warning can indicate that malicious activity is occurring on the server which can cause a denial-of-service condition. TCP connections require a three-way handshake between the server and client: 1) the client sends a packet in which the SYN flag is set in the TCP header, 2) the server sends a SYN/ACK (acknowledgment) packet, and 3) the client sends an ACK packet so data transmission can begin. A denial-of-service condition occurs when the client fails to send the last ACK packet and intentionally sends successive TCP connection requests to the server to fill up the server's buffer. After the server's buffer is full, other clients cannot establish a connection, resulting in a denial-of-service condition.

  IMPORTANT: Novell BorderManager 3.7 Alert detects only SYN packet floods for socket applications, such as FTP.

Due to the importance of defending your server against SYN packet floods, the detection of SYN packet floods should always be enabled. However, for extreme troubleshooting measures, use the following SET command to disable detection if necessary:

SET TCP DEFEND SYN ATTACKS=OFF

Reenable detection with the following command:

SET TCP DEFEND SYN ATTACKS=ON

- Oversized UDP packet

  An oversized UDP packet warning can indicate that malicious activity is occurring on the server. This alert is generated when the server receives and discards UDP packets larger than 16,384 bytes. The server is enabled to discard these packets by default.

  If necessary, enter the following SET commands at the server console to change the largest UDP packet size or disable packet discarding:

  SET LARGEST UDP PACKET SIZE=*n*

  SET DISCARD OVERSIZED UDP PACKETS=OFF

  The variable *n* is a decimal number representing the number of bytes allowed. Never specify a number with commas.

  To reenable packet discarding, enter the following command at the server console:

  SET DISCARD OVERSIZED UDP PACKETS=ON

  NOTE: Because packet sizes are limited by the type of media used, you should know your network topology before changing the largest UDP packet size. For Ethernet only, the oversized UDP packet alert is not generated if the largest UDP packet size is set between 35,541 and 65,535 bytes. However, alerts are generated for packets smaller than 35,541 bytes. The acceptable packet size ranges for other media differ and depend on each medium's MTU—the largest packet size a medium can transport without fragmentation.

Many other documented denial-of-service attacks can be detected by Novell BorderManager 3.7 Alert, although attacks are not identified by name.

Proxy Alerts

Proxy alerts generally indicate that a proxy server has not been configured correctly or is down.

The proxy alerts are as follows:

- Cache hierarchy parent (ICP parent) down

  A cache hierarchy parent down warning indicates a problem with the parent proxy cache server in a configured cache hierarchy. If the cache hierarchy client is enabled on the proxy server and the proxy fails to connect to the parent, the alert will be triggered. If the option to forward all requests through the hierarchy has been selected and the parent is down, requests that cannot be fulfilled through the cache can result in an error because the parent is not available to access the source information.

- SOCKS server down

  A SOCKS server down warning indicates that the SOCKS server to which the proxy cache server connects as a client is down. If the SOCKS client is enabled on the proxy server and the proxy fails to make a connection, the alert will be triggered. Because a SOCKS server is often used as a firewall, requests that cannot be fulfilled through the cache can result in an error because the proxy cannot forward requests through the firewall.

- POP3 or SMTP server down

  A POP3 server down warning indicates that there is a problem with a POP3 server or an internal SMTP mail server. The mail proxy enabled on the Novell BorderManager 3.7 server cannot forward outgoing mail to the POP3 server or deliver incoming mail to the SMTP server.

III Authentication

The following section of *Novell® BorderManager® 3.7 Administration* guide describes the configuration procedures for setting up additional features available with Novell BorderManager 3.7 Authentication Services. To find information about the features, see:

- Chapter 3, “Advanced Configuration of Authentication Services,” on page 39

See the Setting Up Authentication Services section in the *Novell BorderManager 3.7 Installation Guide* to find out about how to install the Novell BorderManager 3.7 Authentication Service.

3 Advanced Configuration of Authentication Services

The following sections describe advanced configuration procedures for Novell® BorderManager® 3.7 Authentication Services:

Changing RADIUS Server Options

You can change Remote Dial-In User Services (RADIUS) server options from the NetWare® server command line, including the distinguished name of the Dial Acess System object and the Dial Access System password for the specified Dial Access System object.

```
LOAD RADIUS
[name = Dial Access System distinguished name] [password =
  Dial Access System password] [threads = number of threads]
  [port = UDP port number for RADIUS] [acctPath = RADIUS
  accounting directory] [fileFormat = [standard|comma] ]
  [rollOver = [daily|weekly|monthly] ]  [serverType =
  [accounting|authentication] [decrementGraceLogins =
  [YES|NO]
```

All parameters are optional. The values you specify override the default values.

If you do not specify the name or password on the command line, you will be prompted to provide a name and password at startup. Names can be specified as relative distinguished names, distinguished names, or partial distinguished names. Both typed and typeless names are supported. Refer to the NDS® or Novell eDirectory™ documentation at for details on specifying names.

The default context is set to the current bindery context. After Novell Novell BorderManager 3.7 Authentication Services has been loaded, the default context is set to the Dial Access System name context.

Strings with embedded spaces must be contained in quotation marks. In addition, a quoted parameter must be preceded with a space.

The valid values for the number of threads range between 1 and 127. The default number of threads is 5, which should be satisfactory in most cases.

The default UDP port number is 1645 (the most commonly used). However, a new UDP port number (1812) has been assigned by the Internet Engineering Task Force (IETF) for RADIUS services.

The default path for the RADIUS accounting files is SYS:\ETC\RADIUS\ACCT.

The RADIUS accounting server is typically implemented as a separate process of the RADIUS authentication server. The RADIUS accounting server listens on UDP port number 1813. When an accounting packet is received from a RADIUS client (such as a network access server), the RADIUS accounting server logs the information in an ASCII text file and returns an acknowledgment to the RADIUS client.

The default RADIUS accounting file format is comma-delimited text (standard ASCII file format is optional).

The default period before a RADIUS accounting file is rolled over is daily (weekly and monthly are optional).

By default, the Novell BorderManager 3.7 Authentication Services software runs both the authentication server and the accounting server when you do not specify the ServerType option on the command line. (Running just the authentication server or the accounting server is optional.)

By default, the Novell BorderManager 3.7 Authentication Services software does not decrement grace logins.

Setting Up Dial Access Server

You must perform the following tasks to create and set up the necessary eDirectory objects in your NDS or eDirectory tree to support dial access services with Novell Novell BorderManager 3.7 Authentication Services:

- “Creating and Setting Up Dial Access System Object” on page 41
- “Creating A Dial Access System Object” on page 42
- “Configuring a Dial Access System Object” on page 42

Creating and Setting Up Dial Access System Object

You must create a Dial Access System object in your eDirectory tree to manage common configuration tasks for a collection of RADIUS servers working together. The information stored in this object consists of the following:

- Client configuration—Enables you to define IP addresses for network access servers and shared secrets among the RADIUS servers and the various network access servers.
- Domains—Enables you to configure other RADIUS servers to which you want to forward RADIUS requests.
- Authentication policy—Enables you to define the authentication policy for the Dial Access System object.
- Dial Access System object password—Enables you to restrict access to authorized users.
- Lookup contexts—Enables contexts to be searched when the common name portion of the username is received in an authentication request.

- Remote connection restrictions—Enables you to limit the number of connections that a remote user can have concurrently per network.

Typically, you need only one Dial Access System object in your eDirectory tree.

You can easily assign rights to an NDS or eDirectory object using NetWare Administrator. For example, you can assign Browse and Read rights from NetWare Administrator by dragging the Dial Access System object over an Organizational Unit object near the root of an eDirectory tree.

This section contains the following tasks:

- "Creating A Dial Access System Object" on page 42
- "Configuring a Dial Access System Object" on page 42
- "Specifying A Dial Access System Password" on page 43

Creating A Dial Access System Object

To create a Dial Access System object, complete the following steps:

1. In NetWare Administrator, select the Organizational Unit container object.
2. Click Object > Create > Dial Access System.
3. Enter the name of the Dial Access System object and click Create.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Configuring a Dial Access System Object

To configure a Dial Access System object, complete the following steps:

1. In NetWare Administrator, select the Dial Access System object.
2. Click Clients > Add to add a RADIUS client. Enter the following information:
   - IP address of the network access server
   - Client type
   - RADIUS secret
3. Click Authentication Policy > Add to configure an authentication policy. Specify the following information:

- Policy type
- Policy rules

4. Click Lookup Context > Add if you want to use common name login. Browse and select the name context, then click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Specifying A Dial Access System Password

To specify a Dial Access System password, complete the following steps:

1. In NetWare Administrator, select the Dial Access System object.
2. Click Miscellaneous > Change Dial Access System Password.
3. Enter and reenter the new password > click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Creating Dial Access Profile Objects

You must create at least one Dial Access Profile object in your eDirectory tree to define common services used by many dial-in users. The Dial Access Profile object contains a list of RADIUS dial access attributes that specify the configuration for creating a specific service.

You can set up as many profiles as you need to define different services. For example, you can create a Point-to-Point Protocol (PPP) profile that enables users to dial in and access the Internet. You can also create a Telnet profile that enables users to connect to a local host using a terminal or terminal emulator. You can specify dial access profiles in the User object that can override settings in the Dial Access Profile object.

Creating a Dial Access Profile Object

To create a Dial Access Profile object:

1. In NetWare Administrator, select the Organizational Unit container object.
2. Click Object > Create > Dial Access Profile.
3. Enter the name of the Dial Access Profile object > click Create.

4. Select the Dial Access Profile object you created > Attributes > Add and specify RADIUS attributes.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Creating and Setting Up User Objects

The User Dial Access Services page allows you to

- Enable a user for dial access services
- Select the appropriate Dial Access System object for a user
- Set a Dial Access System Password for a user (if you use separate passwords for dial-in users)
- Configure (or define) dial-in services for a user (such as enabling a user to select one or more Dial Access Profile objects and associate user-specific settings for each)
- Select a default dial access service if a user is configured for more than one
- Configure remote connection restrictions as well as view active connections and connection history
- Assign an authentication device

This section contains the following tasks:

- "Enabling a User Object for Dial Access Service" on page 44
- "Disabling Dial Accesss Services for User Object" on page 45
- "Adding a User's Token Assignment" on page 45
- "Deleting a User's Token Assignment" on page 45

Enabling a User Object for Dial Access Service

To enable a User object for dial access services:

1. In NetWare Administrator, select the User object.
2. Click Dial Access Services, specify a dial access control setting > click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Disabling Dial Accesss Services for User Object

To disable a User object for dial access services:

1. In NetWare Administrator, select the User object.
2. Click Dial Access Services > Select Disable > click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Adding a User's Token Assignment

To add an Authentication Device assignment:

1. In NetWare Administrator, select the User object.
2. Select Authentication Devices > Add.
3. Browse to the context containing the object to assign, select the object > click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Deleting a User's Token Assignment

To delete an Authentication Device assignment:

1. In NetWare Administrator, select the User object.
2. Click Authentication Devices.
3. Select the device to delete, then click Delete > OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Setting Up Group and Container Administration

Perform the following tasks to modify the eDirectory objects in your eDirectory tree to manage dial access services with Novell BorderManager 3.7 Authentication Services:

- "Setting Up Organization and Organizational Unit Container Objects" on page 46
- "Setting Up Group Objects" on page 47

Setting Up Organization and Organizational Unit Container Objects

You can specify common dial access properties for all users in Organization or Organizational Unit container objects. The Dial Access Service page of an Organization or Organizational Unit allows you to

- Enable dial access services for all users
- Select the Dial Access System object for all users
- Configure the dial access services that can be used by all users in a container

For example, if your organization has several departments that want to allow remote users to access your corporate network, you could use Novell BorderManager 3.7 Authentication Services to manage users who authenticate with the RADIUS protocol. Each department could specify rights to applications, file and print services, and dial-in configuration information. However, multiple departments could be managed by the same network administrator without the requirement to maintain multiple databases.

Specifying dial access properties in the Dial Access Service page for an Organization or Organizational Unit container object has the following benefits:

- Configuring all users in an Organization or Organizational Unit to have the same dial-in rights simplifies administration over per-user administration.
- Configuring users in different containers with different access rights enhances security.

The dial access properties that you define for an Organization or Organizational Unit container object apply to every user in the selected container object (but not to users in Organizational Units that are at a lower level in the eDirectory tree). Refer to the NetWare Administrator online help for information about specific configuration procedures.

You can override the dial access properties of an Organization container object or Organizational Unit container object by modifying the Dial Access Services page of a User object. This allows you to specify unique dial access properties for any User object in your NDS or eDirectory tree.

Enabling Dial Access Services for Users in a Container Object

To enable users in an Organization or Organizational Unit container object for dial access services:

1. In NetWare Administrator, select the Organization or Organizational Unit container object.
2. Click Dial Access Services > Enable Dial Access and click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Setting Up Group Objects

You can grant rights to use one or more specified Dial Access System objects to members of a Group object. Group-based administration leverages the powerful access control list (ACL) capability of eDirectory to enforce user dial-in access restrictions. For example, separate Dial Access System objects could be created for firewall and dial-in access servers. Then a Firewall Group object and a Dial-In Users Group object could be created with access privileges to the firewall Dial Access System object and the dial-in Dial Access System object. By making a user a member of one or both groups, access to these resources is granted selectively based on group membership. Group-based administration can also be used to allow access to high-speed connections by selected users only, while allowing low-speed connections by all users by creating multiple Dial Access System objects.

Restricting access based on assignment to a geographical region is another use for group-based administration. Dial Access System objects could be created for each geographical region that a set of users are allowed to access. Groups such as West Coast, Midwest, and East Coast could be created with users in those regions added as members. Certain users, such as sales staff, could be included in more than one geographical group to allow access to different locations.

Each Dial Access System object must have sufficient rights to any User object that can be authenticated. This can be done for multiple users in a Group object by assigning a parent container object to which the users belong as a trustee of a Dial Access System object.

Likewise, the Group object must have sufficient rights to the Dial Access System object used for authentication. This can be done by assigning the Group object as a trustee of the Dial Access System object.

This section contains the following tasks:

- "Assigning a Container Object as a Trustee of a Dial Access System Object" on page 48
- "Assigning a Group Object as a Trustee of a Dial Access System Object" on page 48

Assigning a Container Object as a Trustee of a Dial Access System Object

To assign a container object as a trustee of a Dial Access System object:

1. In NetWare Administrator, select the Dial Access System object.
2. Select Object > Trustees Of This Object > Add Trustees.
3. Select the Organization or Organizational Unit container object and check the following properties:
   - Object Rights > Browse
   - Property Rights > All Properties > Read
   - Property Rights > All Properties > Write
4. Click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Assigning a Group Object as a Trustee of a Dial Access System Object

To assign a group object as a trustee of a Dial Access System object, complete the following steps:

1. In NetWare Administrator, select the Dial Access System object.
2. Select Object > Trustees Of This Object > Add Trustees.
3. Select the Group object and check the following properties:
   - Object Rights > Browse
   - Property Rights > All Properties>Read
   - Property Rights > All Properties>Write
4. Click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Setting Up Remote Connections Restrictions

You can limit the number of connections that a remote user can have concurrently per network. You can restrict the number of concurrent dial-in connections for each User object, or you can set a default value for concurrent dial-in connections for each Dial Access System object.

This section contains the following tasks:

- "Specifying Dial Access System Login Restrictions" on page 49
- "Specifying Per-User Login Restrictions" on page 51

Specifying Dial Access System Login Restrictions

By default, the RADIUS server allows unlimited dial-in connections. You can also specify the number of concurrent dial-in connections that the RADIUS server will allow for each User object that authenticates through a given Dial Access System object.

For a given Dial Access System object, you can specify the following types of information tracked for each dial-in user:

- Timeout interval for an interim accounting packet (determines if a dial-in connection is active)
- Time interval (in days) before an entry in a user's current login connection is removed
- Maximum number of records kept in a user's login connection history

This section contains the following tasks:

- "Setting Dial Access System Remote Connection Restrictions" on page 49
- "Setting the Current Connection Interval" on page 50
- "Setting the Interim Accounting Timeout Interval" on page 50
- "Setting the Maximum Records in the Remote Connection History" on page 50

Setting Dial Access System Remote Connection Restrictions

To add remote connection restrictions, complete the following steps:

1. In NetWare Administrator, select the Dial Access System object.

2. Select Object > Details > Remote Connections.
3. Select Limit Connections, specify the number of concurrent dial-in restrictions, then click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Setting the Current Connection Interval

To set the current connection interval, complete the following steps:

1. In NetWare Administrator, select the Dial Access System object.
2. Select Object > Details > Remote Connection Restrictions.
3. Enter a value (in days) > click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Setting the Interim Accounting Timeout Interval

To set the interim accounting timeout interval, complete the following steps:

1. In NetWare Administrator, select the Dial Access System object.
2. Select Object > Details > Remote Connection Restrictions.
3. Enter a value (in minutes) and click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Setting the Maximum Records in the Remote Connection History

To add concurrent login restrictions, complete the following steps:

1. In NetWare Administrator, select the Dial Access System object.
2. Select Object > Details > Remote Connection Restrictions.
3. Enter a value > click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Specifying Per-User Login Restrictions

You can accept the default number of concurrent dial-in connections that the RADIUS server will allow for each User object (as specified for a given Dial Access System object), or you can override the default value for a given User object to either specify a different number of concurrent dial-in connections or allow unlimited dial-in connections.

For a given User object, the following types of information are tracked automatically:

- Active connections
- Login connection history

Setting User Remote Connections Restrictions

To add remote connections restrictions, complete the following steps:

1. In NetWare Administrator, select the User object.
2. Select Object > Details > Remote Connections.
3. Specify the login restrictions > click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Planning Token Authentication

To configure tokens for a particular vendor, you must perform a series of procedures. Use the following list to ensure you perform all the required procedures:

- ❑ Create an Authentication Container object.

  You must create at least one Authentication Container object for each vendor you support.

- ❑ Initialize the tokens.

  You must initialize or program each token with the profile parameters.

  The initialization information must also be stored in NDS or eDirectory in an Authentication Device object. There are three methods to initialize tokens, create an Authentication object, and store the data in eDirectory:

- Import factory initialization data (device images) on preinitialized tokens from a disk into NDS or eDirectory.
- Locally initialize the token by selecting the parameters in NetWare Administrator and downloading the data to the token using special initialization hardware.
- Manually initiailize the token by selecting the parameters in NetWare Administrator and manually keying in the initialization codes from the keypad.

❑ Assign the tokens.

You can assign tokens to users from the Authentication Device object page or from the User object page.

❑ Configure token authentication in the Dial Access System object.

You must configure the Dial Access System object policy to allow token authentication as a method.

❑ Grant rights to access token objects.

You must grant the appropriate rights to the Dial Access System object to access the token objects.

Authentication Container Object

The Authentication Container object contains the Authentication Device objects (tokens or smart cards) from a single vendor and manages the common configuration tasks for these objects. All Authentication Device objects must be contained within an Authentication Container object. Therefore, you must create at least one Authentication Container object for each vendor you support. You may create multiple Authentication Container objects if you would like to store the Authentication Device objects from a vendor in more than one location in eDirectory. This object consists of the following pages:

- Identification—Identifies the name of the Authentication Container object and the type of tokens (from what vendor) that are contained in the object.
- Import Device Images—Lets you to import the device images containing the initialization information of a series of factory-preinitialized tokens. For each device image you import, a device object in eDirectory is automatically created.

- Manual Initialization—Lets you to initialize a token by generating and displaying the necessary initialization codes for you to enter manually into the token keypad. When you manually initialize a token, if the device object does not already exist in eDirectory, one is automatically created.
- Local Initialization—Lets you to initialize a token which you have placed in the token initializer hardware attached locally to your administration workstation. When you locally initialize a token, if the device object does not already exist in eDirectory, one is automatically created.
- Token Assignment—Lets you to assign devices to users. You can use this page to assign a single token to a user, or quickly assign a series of serialized tokens to a series of users.

Authentication Device Object

The Authentication Device object contains information about a single token or other device. When you import or initialize a token, an Authentication Device object is created. This object contains the following pages:

- Identification—Identifies the token name, assigned user, type, and status.
- Assignment—Lets you assign the token to a user and enable or disable the token.
- Synchronize—Lets you synchronize the token. You have the option of synchronizing the token manually or automatically the next time the token is used. For manual synchronization, you must specify the event, clock value, or both.
- Password Tests—Lets you test the token to verify that it can correctly generate a password. You can test both the synchronous and asynchronous methods of password generation.

Protecting Device Data in NDS or eDirectory

The authentication device data stored in NDS or eDirectory is critical to system security. This data should be carefully protected and access to it should be restricted to authentication servers and administrators who require access.

Sensitive information stored on authentication device objects is encrypted automatically; however, additional measures should be taken to protect this data. We recommend the following:

- Create a partition at the authentication device container

- Restrict replication of authentication device partitions to a few servers that are well controlled
- Ensure that backup copies of authentication device objects are protected
- Create access controls to allow administrators and Dial Access System objects to read and write these objects
- Block inherited rights and ensure access control lists (ACLs) are only for objects that should have access

Managing Token Authentication

Novell BorderManager 3.7 Authentication Services enables you to use NDS or eDirectory as the database to manage token authentication. Using the NetWare Administrator utility on the administration workstation, you can perform the following management tasks:

- "Creating an Authentication Container Object" on page 54
- "Creating an Authentication Device Object" on page 55
- "Importing a Token" on page 55
- "Manually Initializing a Token" on page 55
- "Locally Initializing a Token" on page 56
- "Assigning a Single Token" on page 56
- "Assigning a Series of Tokens" on page 56
- "Synchronizing a Token" on page 57
- "Unlocking a Token" on page 57
- "Testing Passwords" on page 57

Creating an Authentication Container Object

To create an authentication container:

1. In NetWare Administrator, select Object > Create > Authentication Container.
2. Specify the name of the authentication container and click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Creating an Authentication Device Object

To create an authentication device object:

1. In NetWare Administrator, select Object > Create > Authentication Device.
2. Specify the name of the authentication device and click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Importing a Token

To import a token:

1. In NetWare Administrator, select the authentication container object.
2. Select Object > Details > Import Device Images and browse to the file that contains the token device image to import.
3. Click Import Images > Create Objects Now > OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Manually Initializing a Token

To manually initialize a token:

1. In NetWare Administrator, select the authentication container object.
2. Select Object > Details > Manual Initialization > specify the following information:
   - Profile
   - Language
   - Token serial number
   - Token initial PIN
3. Click Initialize Device > Create Object Now.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Locally Initializing a Token

To locally initialize a token:

1. In NetWare Administrator, select the authentication container object.
2. Select Object > Details > Local Initialization > specify the following information:
   - Profile
   - Language
   - Token type
   - Serial port
   - Welcome message
   - Token initial PIN
3. Click Initialize Device > Create Object Now.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Assigning a Single Token

To assign a single token:

1. In NetWare Administrator, select the authentication device object.
2. Select Object > Details > Assignment > browse to the User object to assign the token.
3. Click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Assigning a Series of Tokens

To assign a series of tokens:

1. In NetWare Administrator, select the authentication container object.
2. Select Object > Details > Token Assignment > specify the following information for each token:
   - Token serial number
   - User name

3. Click Assign Now.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Synchronizing a Token

To synchronize a token:

1. In NetWare Administrator, select the authentication device object.
2. Select Object > Details > Synchronization > click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Unlocking a Token

To unlock a token:

1. In NetWare Administrator, select the authentication device object.
2. Select Object > Details > Unlock Code.
3. Enter the challenge code displayed by the token > click Unlock Now.
4. Enter the response code into the token.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Testing Passwords

To test an asynchronous password:

1. In NetWare Administrator, select the authentication device object.
2. Select Object > Details > Password Tests > Asynchronous > Test Now and enter your PIN.
3. Enter the challenge code into the token.
4. Enter the password and click OK.

To test a synchronous password:

1. In NetWare Administrator, select the authentication device object.

2. Select Object > Details > Password Tests > Synchronous > Test Now > enter your PIN.
3. Enter the password and click OK.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Planning Authentication Policies

All users accessing services through Novell BorderManager 3.7 must be authenticated. All authentication, regardless of which Novell BorderManager 3.7 service is being accessed, is processed by a special module, the Authentication Device Manager (ADM), that authenticates users for the following services:

- Virtual Private Networks (VPN)
- Proxy Services
- SOCKS
- Dial-In Authentication Services

The authentication policies enforced by the ADM are defined and stored in an eDirectory object called the Authentication Policy object (APO). The APO contains authentication rules that define the relationships among the services, users, and authentication methods so that the ADM can determine and enforce the appropriate authentication requirements.

Authentication Device Manager

All Novell BorderManager 3.7 servers must load the ADM. On each Novell BorderManager 3.7 server object, an attribute specifies the Authentication Policy object that contains the authentication rules to be enforced on that server. If ADM is loaded and no Authentication Policy object is specified, then the ADM loads but does not process authentication requests. Therefore, until a Authentication Policy is set, access to Novell BorderManager 3.7 from any service is not available.

IMPORTANT: You must set up a generic authentication policy to allow all users to access network services through each of the various Novell BorderManager 3.7 services.

When a particular service needs to authenticate a user, that service calls the ADM and passes the necessary information about itself (such as its service

ID) and the user, container, or group object (the distinguished name and credentials) for the ADM to process the request. The ADM uses this information to determine the applicable authentication rule from the rule set stored in the Authentication Policy object, and then enforces that rule set.

Authentication Policy Object

Authentication rules or policies are defined and stored in eDirectory in the Authentication Policy object. This allows you to define policies that can be used locally (on a single server), or globally (across multiple servers and services throughout the NDS or eDirectory tree).

NOTE: You will usually need only one Authentication Policy object for each eDirectory replica.

The Authentication Policy object is administered through NetWare Administrator. This object enables you to set up authentication rules that allow you to manage authentication for the following Novell BorderManager 3.7 service types:

- VPN
- Proxy Services
- SOCKS
- Dial-In Authentication Services
- All services (includes VPN, proxy services, SOCKS, and dial-in authentication services)

To define a rule for a service type, you must select the service type from NetWare Administrator. The VPN, Proxy Services, and SOCKS service types are predefined. The Authentication Services service type is represented by an eDirectory Dial Access System (DAS) object. To define a rule for Authentication Services, you must select the distinguished name of the DAS object associated with the service.

Supported Authentication Methods

Novell BorderManager 3.7 supports a variety of authentication methods. The exact methods supported depend on the service type. The following table lists the authentication methods supported for each service type.

Table 1 Authentication Methods Supported

Service Type	Authentication Methods Supported
Proxy Services	Any user-assigned device
	eDirectory passwords
	Token-based authentication methods
SOCKS	Any user-assigned device
	eDirectory passwords
	Token-based authentication methods
VPN	Any user-assigned device
	eDirectory passwords (mandatory)
	Token-based authentication methods
	NOTE: When token-based authentication is selected, the VPN client will be required to supply both a token password and an eDirectory password
Authentication Services	Any user-assigned device
	eDirectory passwords
	Token-based authentication methods
	Dial access passwords (PAP)
	Dial access passwords (CHAP)

Authentication Rules

Authentication rules define the authentication method required for a specific user, container, or group object to access a particular Novell BorderManager 3.7 service. When a user requests access, the applicable rule will be enforced. You can define a single authentication rule for all Novell BorderManager 3.7 services, or different authentication rules for the different Novell BorderManager 3.7 service types. If you define multiple authentication rules, the rules are applied in the order in which they appear in the list. Once a rule has been matched, no other rules are evaluated. To change the priority of a rule, simply change its position in the list.

You can also define the level of enforcement for a rule. The following enforcement levels are defined:

- Mandatory—The user must authenticate using this method.
- Required if assigned—The user is required to authenticate using this method if one is assigned for them.
- Optional—The user may authenticate using this method.

The following table illustrates some possible authentication rules.

Table 2 Authentication Rule Examples

Service	Users	Authentication Method	Enforcement
<VPN>	.hr.acme	<eDirectory password> .token.acme	Mandatory Mandatory
<Proxy>	.sales.acme	.token.acme <eDirectory password>	Required if assigned Mandatory
<SOCKS>	<Any>	.token.acme	Required if assigned
.das.acme	<Any>	.token.acme <eDirectory password>	Required if assigned Mandatory
<Any>	<Any>	<eDirectory password>	Mandatory

Setting Up Authentication Policies

To set an authentication policy for Novell BorderManager 3.7 Authentication Services, complete the following tasks:

- “Creating an Authentication Policy Object” on page 62
- “Defining the Server to Host the Authentication Policy Object” on page 62
- “Configuring Authentication Policy Rules” on page 62

Creating an Authentication Policy Object

To create an Authentication Policy object, complete the following steps:

1. In NetWare Administrator, select the Organization or Organizational Unit object where you want to place the Authentication Policy object.
2. Select Create from the Object menu.
3. Select Authentication Policy > click OK.
4. Enter the name of the Authentication Policy object > click OK.

Defining the Server to Host the Authentication Policy Object

To define the servers using the Authentication Policy object, complete the following steps:

1. In NetWare Administrator, select the Authentication Policy object > right-click Details.
2. Select Hosts > Add.
3. Browse to select the server object that will host the Authentication Policy object > click OK.

Configuring Authentication Policy Rules

To configure authentication policy rules, complete the following steps:

1. In NetWare Administrator, select the Authentication Policy object > right-click Details.
2. Select Rules > Add.
3. Select a predefined Service Type, or browse to select the distinguished name of a Service object.
4. Click Users > add the User objects or Group objects that will use the policy > click OK.
5. Click Methods > Add.
6. Select the Authentication Method Type.
7. (Optional) If you selected the Distinguished Name authentication method, browse and select the authentication method container.
8. Select the appropriate Method Enforcement.

9. Check Decrement Grace Logins if desired > click OK.
10. Use the Up and Down arrows to specify the priority that the methods will be used (first to last).

Planning RADIUS Proxy Services

You can use RADIUS proxy to outsource the management of dial-in hardware to an Internet Service Provider (ISP) while you manage the users in your eDirectory tree. This benefit provides you with the flexibility to manage dial-in users without the investment in dial-in hardware or the burden of managing the hardware.

Using RADIUS proxy, a remote user (such as jane@acme.com) dials in to an ISP network. The user's access request (user ID and password) is forwarded to a RADIUS proxy server on the ISP network. The ISP RADIUS proxy server forwards the access request to your company's RADIUS server (such as acme.com). The RADIUS server then checks the information in the access request and either accepts or rejects the request. If the RADIUS server accepts the request, it returns configuration information specifying the type of connection service (such as PPP or Telnet) to deliver to the user.

Authentication Services can act as both a conventional RADIUS server and a RADIUS proxy server at the same time. To set up a RADIUS proxy, you must add a domain to the Dial Access System object's domain list. The domain name you assign is the target domain the user must use to be directed to that proxy for authentication. The RADIUS server supports usernames specified as either an eDirectory distinguished name or a common name. For access requests that have a username without a domain, you can configure search domains that can be checked to determine if valid authentication information is available. The search domains consist of configured domains that do not authenticate by eDirectory context. Domains are defined as one of the following types:

- NDS or eDirectory Context—Any Novell BorderManager 3.7 Authentication Services server

  This domain type configures an authentication domain for the Dial Access System object that will look up users by NDS or eDirectory context. The authentication request can be processed by any Novell BorderManager 3.7 Authentication Services server in the eDirectory tree. For this domain type, you specify the eDirectory context and define whether to look for the user in that context and any context under it, or look for the user only in the specified context. If the user is not found, you can set the option to look up the user in any defined search domains.

- NDS or eDirectory Context—Specific Novell BorderManager 3.7 Authentication Services server

  This domain type also configures an authentication domain for the Dial Access System object that will look up users by NDS or eDirectory context. However, this domain type will forward the authentication request to a specific Novell BorderManager 3.7 Authentication Services server in the eDirectory tree where the user belongs to reduce network latency. For this domain type, you specify the eDirectory context and define whether to look for the user in that context and any context under it, or look for the user only in the specified context. The search domain option is not available. To define the target server, specify the IP address, port, and RADIUS secret of the server. To define how accounting packets are handled, specify whether to log accounting locally on the server or forward accounting packets to an accounting server on a remote domain.

- Generic proxy server

  This domain type configures a simple domain proxy. Authentication requests will be forwarded to the designated RADIUS server. If the server expects to see only the common username, set the option to remove the target domain name the user logged in with. To target the server, specify the IP address, port, and RADIUS secret for the server. To define how accounting packets are handled, specify whether to log accounting locally on the server or forward accounting packets to an accounting server on a remote domain.

- Search Domain Server

  This domain type configures a search domain. Search domains are searched when a user logs in with a common username (no target), or when a user with a target domain is not found in a specified eDirectory context and usage of a search domain is allowed for that domain. If the server expects to see only the common username, set the option to remove the target domain name the user logged in with. To target the server, specify the IP address, port, and RADIUS secret for the server. To define how accounting packets are handled, specify whether to log accounting locally on the server or forward accounting packets to an accounting server on a remote domain.

- External Authentication Service Object

  This domain type configures a domain that targets an external authentication server (such as a Security Dynamics ACE/Server). If the server expects to see only the common username, set the option to remove the target domain name the user logged in with. To target the server,

specify the IP address, port, and RADIUS secret for the server. You can create External Identity objects for third-party tokens administered by an External Authentication Service object and assign NDS or eDirectory users to an External Identity object.

Refer to the NetWare Administrator online help for information about specific configuration procedures.

This section contains the following tasks:

- "Setting Up a RADIUS Authentication Proxy to Authenticate Remote Users by NDS or eDirectory Context to Any RADIUS Server" on page 65
- "Setting Up a RADIUS Authentication Proxy to Authenticate Remote Users by NDS or eDirectory Context to a Specific RADIUS Server" on page 66
- "Setting Up a RADIUS Authentication Proxy as an ISP to Forward Requests to a Corporate RADIUS Server" on page 66
- "Setting Up a RADIUS Authentication Proxy to Forward Requests to a Third-Party Authentication Server Supporting Token Authentication" on page 67
- "Setting Up a RADIUS Authentication Proxy to Forward Requests to Third-Party Authentication Server Supporting Token Authentication with Token Serial Numbers as Usernames" on page 67
- "Setting Up a RADIUS Authentication Proxy to Authenticate Usernames to a Search Domain" on page 68

Setting Up a RADIUS Authentication Proxy to Authenticate Remote Users by NDS or eDirectory Context to Any RADIUS Server

A user logs in as jane@acme.com. You want this user to authenticate using the local NDs or eDirectory tree and search for the user from the [Root] context of the NDS or eDirectory tree and any context below [Root]. You don't care which RADIUS server handles the authentication. If the user cannot be authenticated in the NDS or eDirectory tree, you want the server to send the authentication request to all the search domains for the Dial Access System object. Configure the Dial Access System object as follows:

Domain Name: acme.com

Domain Type: NDS or eDirectory Context—Any BMAS Server

eDirectory Context Name: [Root]

Look for user in any lookup context under this context: checked

Use search domains if user not found: checked

Setting Up a RADIUS Authentication Proxy to Authenticate Remote Users by NDS or eDirectory Context to a Specific RADIUS Server

A user logs in as jane@sales.acme.com. You want this user to authenticate using the local NDS or eDirectory tree, but you want to search for the user only in the sales.acme context. You also want a specific RADIUS server that is within the same partition of the NDS or eDirectory tree as the sales context to handle the authentication to reduce network latency for the login. The IP address for the RADIUS server is 1.2.3.4 and the secret is 12345678998765432100. You need the accounting to be logged locally on the RADIUS server. Configure the Dial Access System object as follows:

Domain Name: sales.acme.com

Domain Type: eDirectory Context—Specific BMAS Server

eDirectory Context Name: sales.acme

Look for user in this context only: checked

Primary Address: 1.2.3.4 Port: 1645

Secret: 12345678998765432100

Log at proxy server: checked

Setting Up a RADIUS Authentication Proxy as an ISP to Forward Requests to a Corporate RADIUS Server

You manage an ISP. Acme Corporation user joe dials in with the username joe@acme.com, and you need to forward the authentication request to the corporation's RADIUS server at IP address 1.2.3.4, port 1645, with a RADIUS secret of 12345678998765432100. You also need to forward accounting to the Acme corporation RADIUS accounting server at IP address 1.2.4.5, port 1646, with a RADIUS secret of 98765432112345678900 and a retry limit of 24 hours. Configure the Dial Access System object as follows:

Domain Name: acme.com

Domain Type: Generic Proxy

Primary Address: 1.2.4.5 Port: 1645

Secret: 12345678998765432100

Forward to domain: checked

Use alternate addresses/secret: checked

Primary Address: 1.2.4.5 Port: 1646

Secret: 98765432112345678900

Setting Up a RADIUS Authentication Proxy to Forward Requests to a Third-Party Authentication Server Supporting Token Authentication

Your corporation has a Security Dynamics ACE/Server external server that supports token authentication. Your sales force uses this token implementation extensively and you need to preserve your investment in this hardware. You want to use the token authentication capabilities of this server, but would like to manage the users in eDirectory with Novell BorderManager 3.7 Authentication Services. Salesperson Olivia Olsen logs in as Olivia.Sales.Acme. You want to remove the domain name on this login and create a domain, ace, to forward the request to the external authentication server at IP address 1.2.3.4, port 1645, with a RADIUS secret of 09876543211234567890. To implement this example, you must create an External Authentication Service object and an External Identity object.

Configure the External Authentication Service object as follows:

Domain Name: ace

Domain Type: External Authentication Server

Remove domain name: checked

Primary Address: 1.2.3.4

Port: 1645

Secret: 09876543211234567890

Accounting Log at proxy server: checked

Assign the User object to the External Identity Object as follows:

Login Name: Olivia.Sales.Acme

Given Name: Olivia

Last Name: Olsen

Setting Up a RADIUS Authentication Proxy to Forward Requests to Third-Party Authentication Server Supporting Token Authentication with Token Serial Numbers as Usernames

Your implementation is exactly the same as in the previous configuration; however, you want to eliminate the need to manage user accounts on the token server. Instead of using usernames on your external authentication server, you have assigned the serial number of the token as the login name. The serial number and login name for the token used by salesperson Olivia Olsen is 12345. You still want Olivia to log in as Olivia.Sales.Acme. However, you

want eDirectory to substitute 12345 as Olivia's other name. To implement this configuration, you must configure the User object Olivia as follows:

Login Name: Olivia.Sales.Acme
Given Name: Olivia
Last Name: Olsen
Other name: 12345@ace

Configure the External Authentication Service object as follows:

Domain Name: ace
Primary Address: 1.2.3.4
Port: 1645
Secret: 09876543211234567890

Setting Up a RADIUS Authentication Proxy to Authenticate Usernames to a Search Domain

Acme Corporation has a legacy RADIUS server. You want to migrate your remote access to Novell BorderManager 3.7 Authentication Services; however, you want to do it gradually, moving one department a month from the legacy system to Novell BorderManager 3.7. You want your users to authenticate to the Novell BorderManager 3.7 RADIUS server and you want this server to search the legacy RADIUS server if the user does not exist in eDirectory.

To allow users to authenticate, you can set up a search domain on the Novell BorderManager 3.7 Authentication Services RADIUS server. The legacy RADIUS server, RAD1, is at IP address 1.2.3.4, port 1645, with a secret of 09876543211234567890. You also want accounting to be logged at the legacy proxy server. Configure the Dial Access System object on the Novell BorderManager 3.7 Authentication Services RADIUS server as follows:

Domain Name: RAD1
Domain Type: Search Domain Server
Primary Address: 1.2.3.4
Port: 1645
Secret: 09876543211234567890
Accounting Log at proxy server: checked

Managing RADIUS Proxy Services

Using the NetWare Administrator utility on the administration workstation, you can perform the following management tasks for RADIUS proxy services:

Adding an NDS or eDirectory Context Domain Processed by Any RADIUS Server

To add an NDS or eDirectory context domain to be processed by any RADIUS server:

1. In NetWare Administrator, select the Dial Access System object.
2. Select Object > Details > Add > enter the name of the authentication domain.
3. Select Domain Type > Any BMAS Server > browse to the name of the eDirectory context to search.
4. Click OK twice.

Refer to the NetWare Administrator online help for more detailed configuration instructions.

Adding an NDS or eDirectory Context Domain Processed by a Specific RADIUS Server

To add an eDirectory context domain to be processed by a specific RADIUS server, complete the following steps:

1. In NetWare Administrator, select the Dial Access System object.
2. Select Object > Details > Add > enter the name of the authentication domain.
3. Select Domain Type > Specific BMAS Server and browse to the name of the eDirectory context to search.
4. Specify the IP address and TCP port number of the specific RADIUS server.
5. Enter and re-enter the RADIUS secret.
6. Click OK twice.

Adding a Generic Proxy Server Domain

To add a a generic proxy server domain, complete the following steps:

1. In NetWare Administrator, select the Dial Access System object.
2. Select Object > Details > Add > enter the name of the authentication domain.
3. Select Domain Type > Generic Proxy Server.
4. Specify the IP address and TCP port number of the RADIUS server.
5. Enter and re-enter the RADIUS secret.
6. Click OK twice.

Adding a Search Domain Server Domain

To add a search domain server domain, complete the following steps:

1. In NetWare Administrator, select the Dial Access System object.
2. Select Object > Details > Add > enter the name of the authentication domain.
3. Select Domain Type > Search Domain Server.
4. Specify the IP address and TCP port number of the RADIUS server.

5. Enter and re-enter the RADIUS secret.
6. Click OK twice.

Adding a RADIUS Accounting Proxy Domain

To add a RADIUS accounting proxy domain, complete the following steps:

1. In NetWare Administrator, select the Dial Access System object.
2. Select Object > Details > Domains > specify the following information:
   - Accounting > Forwarding
   - Retry Limit
3. Click OK twice.

Adding an External Authentication Service Object

To add an External Authentication Service object:

1. In NetWare Administrator, select the NDS or eDirectory tree.
2. Select Create > External Authentication Service.
3. Enter the name of the External Authentication Service object.
4. Check Define Additional Properties to assign additional properties to the External Authentication Service object during creation.
5. Specify the IP address and TCP port number of the external RADIUS server.
6. Enter and re-enter the RADIUS secret.
7. Click OK twice.

Adding an External Identity Object

To add an External Identity object, complete the following steps:

1. In NetWare Administrator, select the External Authentication Service object.
2. Select Create > External Identity.
3. Enter the name of the External Identity object.

4. Check Define Additional Properties to assign additional properties to the External Authentication Service object during creation.
5. Click OK twice.

Modifying a Domain

To modify a domain, complete the following steps:

1. In NetWare Administrator, select the Dial Access System object.
2. Select Object > Details > Domains > select the domain name to modify.
3. Click OK.

Deleting a Domain

To delete a domain, complete the following steps:

1. In NetWare Administrator, select the Dial Access System object.
2. Select Object > Details > Domains > select the domain name to delete.
3. Click OK.

Displaying RADIUS Status Messages

The Novell BorderManager 3.7 Authentication Services status display provides status messages that are helpful in troubleshooting user access problems. You can view the status display in the following ways:

- From the the NetWare server console, enter the following commands to control the status display:

```
RADIUS display {on|off}
RADIUS display {+|-} {failure|success}
RADIUS SystemLog {on|off}
RADIUS SystemLog file_location
RADIUS SystemLogSize new_size
RADIUS SystemLogPolicy [daily|weekly|days]
RADIUS LogStatus
```

- When a Novell BorderManager 3.7 Authentication Services server is started, the status window displays only messages for authentication

failures. Descriptions of failure messages are listed in the following categories:

- Access Rejected Messages
- Messages Dropped Messages
- Other Messages

Each message is listed with the possible causes.

Access Rejected Messages

Device not enabled

The authentication device has not been enabled for use.

Device not present

The authentication device was not detected.

Exceeded concurrent login limit

The number of remote connections has exceeded the limit specified in the Dial Access System object or User object.

Invalid password

Possible causes:

- User entered the wrong password.
- Shared secret does not match between the network access server and the RADIUS server. The shared secret is case sensitive.
- Client workstation attempted to authenticate using the Challenge Handshake Authentication Protocol (CHAP), but the password policy was set to use an eDirectory password. (CHAP authentication requires a separate dial access password.)

Login disabled

The user eDirectory account has been disabled on the login restriction page.

Method not allowed

The specified authentication method is not permitted by the Authentication Device Manager.

Method not supported

The Authentication Device Manager does not support the authentication method.

No authentication policy configured

No authentication policy has been configured for the Dial Access System object.

No devices assigned

No authentication device has been assigned to the User object.

No more search domains

All search domains defined for a Dial Access System object have been searched without success.

No service data

No service data is available for the authentication device.

No such context

The specified NDS or eDirectory context does not exist.

No such domain

The domain name is not defined on the Dial Access System object.

No such profile

The Dial Access System object does not have Browse and Read rights to the Dial Access Profile object.

No such proxy target

No entry exists in the proxy target page for the domain that the user entered.

No such service tag

No service is defined for the User or container object that matches the service tag entered by the user.

No such user

Possible causes:

- User object does not exist.

- Lookup context does not exist.
- User entered the username incorrectly (distinguished name syntax error).
- Dial Access System does not have Browse and Read rights to the User object.

Password expired

The eDirectory password has expired.

Proxy rejected

The target RADIUS server rejected the authentication request. Consult the output of the final RADIUS server in the proxy chain to determine the problem.

Unknown method tag

The authentication method tag is not defined for the Dial Access System object.

User not a member of dial access system

Possible causes:

- Dial Access System object does not have Browse and Read rights to the User object or container object.
- Dial Access System object has not been specified for the User or container object.
- User or container object has been configured to use a different Dial Access System object.

User not enabled for RADIUS login

Possible causes:

- Dial access is disabled on the User object.
- Dial access is disabled on the container object for a User object using the container setting.
- Dial Access System object does not have Browse and Read rights to the User object or container object.

Message Dropped Messages

Proxy loop detected

The chain of proxy RADIUS servers has been configured in a loop. A loop is an invalid configuration. Check your proxy target configuration to ensure that no loops occur.

Unknown RADIUS client

No entry exists in the Dial Access System client table for the RADIUS client that issued the access request.

Other Messages

RADIUS Error -150

Insufficient Memory

A system error has occurred (sufficient memory was not available to satisfy the current memory allocation request).

RADIUS Error -307

Missing NDS or eDirectory Replica

The NDS or eDirectory replica that the RADIUS server is using failed.

RADIUS Error -601

The Dial Access System object is not valid.

RADIUS Error -672

The user does not have sufficient rights to perform this operation.

RADIUS Error -801

Insufficient Buffer

An internal failure occurred (the system allocated a buffer of insufficient size).

RADIUS Error -802

Invalid Request

An invalid request was received.

RADIUS Error -803

No Such Attribute

Possible causes:

- A requested RADIUS attribute was not found.
- An invalid attribute was detected in an incoming RADIUS message.

RADIUS Error -804

Invalid Data

Malformed data was detected in the eDirectory directory.

RADIUS Error -805

Invalid Transport

The host system is not configured properly for TCP/IP.

RADIUS Error -806

Invalid Signature

The signature on a proxy reply message is invalid.

RADIUS Error -807

Invalid Data Version

Unknown data was found in the eDirectory directory.

RADIUS Error -808

Proxy Loop Detected

The chain of proxy RADIUS servers has been configured in a loop. A loop is an invalid configuration. Check your proxy target configuration to ensure that no loops occur.

RADIUS Error -809

Invalid Parameter

An invalid parameter value was specified.

ADM Error 900

Device Already Supported

The authentication device is already defined.

ADM Error 901

Invalid Structure Version

An invalid version was specified.

ADM Error 902

Invalid Request Entry Point

An invalid request was specified.

ADM Error 903

Device Not Present

The authentication device is not present.

ADM Error 904

Method Tag Already Supported

The authentication method tag has already been defined.

ADM Error 905

Invalid Snap-In Handle

The snap-in handle is not supported.

ADM Error 906

Invalid Subject

The subject is not supported.

ADM Error 907

Unknown Method Tag

The authentication method is not supported.

ADM Error 908

Method Not Allowed

This authentication method is not permitted.

ADM Error 909

Invalid Policy Count

An invalid policy count was specified.

ADM Error 910

Invalid Service Count

An invalid service count was specified.

ADM Error 911

Invalid Policy Type

This authentication policy is not supported.

ADM Error 912

Method Not Supported

This authentication method is not supported.

ADM Error 913

No Devices Assigned

No authentication devices have been assigned to a User object.

ADM Error 914

No Default Device

No default authentication device has been specified.

ADM Error 915

No Service Data

No service data is available.

ADM Error 916

Invalid State

The authentication device is in an invalid state.

ADM Error 917

Snap-In Registration Table Empty

An error occurred to the snap-in registration table.

ADM Error 918

Memory Allocation

A memory allocation error has occurred.

ADM Error 919

Unable to Locate Snap-in

The snap-in module cannot be found.

ADM Error 920

Invalid NDS or eDirectory Response

An invalid NDS or eDirectory response was received.

ADM Error 921

Unsupported Version

An unsupported version is being used.

ADM Error 922

No Such Attribute

This attribute is not supported.

ADM Error 923

Invalid Encryption Type

This encryption type is not supported.

ADM Error 924

Invalid Service Tag

This service tag is not supported.

ADM Error 925

Invalid Object DN

The distinguished name for the object is not valid.

ADM Error 926

Unable to Locate Pending Request

A pending authentication request cannot be located.

ADM Error 927

Unable to Load Snap-In

The snap-in module cannot be loaded.

ADM Error 928

Unable to Retrieve Required Data

The required data cannot be retrieved.

ADM Error 929

Shutdown in Progress

The program is being shut down.

ADM Error 930

Device Not Enabled

The authentication device is not enabled.

ADM Error 931

Invalid Buffer Size

An invalid buffer size was specified.

ADM Error 932

Invalid Authentication Materials

An invalid configuration was supplied.

ADM Error 933

Unsupported Cryptography Algorithm

This cryptography algorithm is not supported.

ADM Error 934

Invalid Password

An invalid password was specified.

ADM Error 935

Login Disabled

Login for the user is disabled.

ADM Error 936

Account Expired

The user account has expired.

ADM Error 937

Password Expired

The supplied password has expired.

ADM Error 938

Intruder Detection

An intruder has been detected.

IV Filters

The following sections of the *Novell® BorderManager® 3.7 Administration* guide provides the basic information you need to set up packet filters.

For NetWare® 6, Novell BorderManager 3.7 delivers filter configuration based on Novell iManager. NetWare 5.1 customers will still need to use FILTCFG.

However, NetWare 5.1 customers can also use filter configuration based on Novell iManager if they have one Netware 6 in a tree. Novell BorderManager 3.7 extends the directory schema to add attributes to server objects for IP packet filtering. The filter configuration is stored in Novell eDirectory™. This allows the use of either FILTCFG or Novell iManager on an Novell BorderManager 3.7 server, and also provides a natural backup of the firewall configuration. Changes in Novell iManager are automatically moved out to the server and put into effect.

During the installation of Novell BorderManager 3.7, if packet filtering is already configured on the server, the existing configuration should be imported into eDirectory. By storing the firewall configuration in eDirectory Novell BorderManager 3.7, extends the functionality. See the following sections for more information:

- Chapter 4, “Advanced Configuration of IP Packet Filters Using FILTCFG,” on page 85 to set up HTTP, FTP, Telnet, SMTP, POP3, and DNS filters.
- Chapter 5, “Managing IP Packet Filters,” on page 97 to find the configuration parameters for the IP packet filter log and the standard IP packet filter log format.
- Chapter 6, “Packet Filtering based on Novell iManager,” on page 101 to set up RIP, EGP, OSPF and Packet Forwarding Filters.

- Chapter 7, “Back Up and Restore Filters,” on page 119 on NDS® or Novell eDirectory™.

See the Setting Up Packet Filters section in the *Novell BorderManager 3.7 Installation Guide* for information on how to set up filters.

4 Advanced Configuration of IP Packet Filters Using FILTCFG

The following sections describe how to configure exceptions using FILTCFG to allow specific IP services through the Novell® BorderManager® 3.7 firewall when the action of the filters is to deny packets in the filter list. A server SET command to filter packets that have IP header options is also described.

A server SET command to filter packets that have IP header options is also described.

Choosing between Stateful or Static Packet Filters

Stateful packet filters are more secure because they allow only the packets in response to requests to pass through the firewall. For this reason, the procedures in this chapter describe how to configure stateful packet filters. However, because static packet filters offer faster performance, a list of equivalent static filters is provided should you choose to configure them.

If you choose to configure static filters for the TCP protocol, you should enable ACK bit filtering so that all inbound packets that do not have the TCP ACK bit set are dropped by the server.

Setting Up an HTTP Filter

You can set up an HTTP filter on your server's public interface to filter HTTP packets in the inbound or outbound direction. An inbound HTTP filter might be required to allow public access to specific Web servers in your private network. An outbound HTTP filter might be required to allow certain users to bypass proxy services and connect directly to origin Web servers.

This section contains the following tasks:

- "Setting Up a Stateful HTTP Filter" on page 86
- "Setting Up Static Filters for HTTP" on page 87

Setting Up a Stateful HTTP Filter

To set up a stateful HTTP filter exception,

1. Select Configure TCP/IP Filters > Packet Forwarding Filters > Exceptions.
2. Press *Ins* to define a new exception.
3. If you are creating an inbound exception, do the following:
   - **3a** Specify *All Interfaces* for the Source Interface parameter.
   - **3b** Specify the server's public interface for the Destination Interface parameter.
   - **3c** Press *Enter* for Packet Type > select www-http-st.

     NOTE: The www-http-st packet type is for HTTP over TCP. This packet type will not work for HTTP over UDP.
   - **3d** If you want the server to forward HTTP packets from certain public hosts only, specify Host or Network for the Src Addr Type parameter > enter the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.
   - **3e** If you want the server to forward HTTP packets addressed to certain private hosts only, specify Host or Network for the Dest Addr Type parameter > enter the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.

3f Press *Esc* > select Yes to save the filter.

4 If you are creating an outbound exception, do the following:

4a Specify the server's private interface for the Source Interface parameter.

4b Specify the server's public interface for the Destination Interface parameter.

4c Press *Enter* for Packet Type > select www-http-st.

4d If you want the server to forward HTTP packets from certain private hosts only, specify Host or Network for the Src Addr Type parameter > enter the IP address for Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.

4e If you want the server to forward HTTP packets addressed to certain public hosts only, specify Host or Network for the Dest Addr Type parameter > enter the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.

4f Press *Esc* > select Yes to save the filter.

IMPORTANT: The outbound stateful HTTP filter does not allow packets for Domain Name System (DNS) name resolution to be forwarded to a DNS server on the public network. DNS names in URLs cannot be resolved unless you set up a DNS filter.

Setting Up Static Filters for HTTP

If you do not want to configure a stateful HTTP exception, you can create static filters instead.

In the direction that HTTP requests will be sent, create one or both of the following static packet filter exceptions:

- www-http (for HTTP over TCP)
- www-http/udp (for HTTP over UDP)

Most browsers are configured to use HTTP over TCP, but they can also use HTTP over UDP. If you support browsers using HTTP over UDP, you should create both filters.

In the direction that HTTP responses will be sent, create one or both of the following static packet filter exceptions:

- dynamic/tcp (for HTTP over TCP)
- dynamic/udp (for HTTP over UDP)

The exceptions you create depend on which exceptions you created for the opposite direction of packet flow. If you created exceptions for both www-http and www-http/udp, you should create filter exceptions for both dynamic/tcp and dynamic/udp. The dynamic port range is 1024 to 65,535.

IMPORTANT: These filters do not allow packets for DNS name resolution to be forwarded.

Setting Up an FTP Filter

You can set up an FTP filter on your server's public interface to filter FTP packets in the inbound or outbound direction. An inbound FTP filter might be required if public users connect to an FTP server in your private network. An outbound FTP filter might be required to allow certain users to bypass proxy services and connect directly to FTP servers on the public network.

When you set up an FTP filter, you can configure it to inspect for active FTP connections, passive FTP connections, or both. For tighter security, some administrators only allow active FTP connections in the inbound direction so the data connection is always on port 20. In contrast, passive FTP connections use any dynamic ports that are available.

This section contains the following tasks:

- "Setting Up a Stateful FTP Filter" on page 88
- "Setting Up Static Filters for FTP" on page 90

Setting Up a Stateful FTP Filter

To set up a stateful FTP filter exception,

1. Select Configure TCP/IP Filters > Packet Forwarding Filters > Exceptions.
2. Press *Ins* to define a new exception.
3. If you are creating an inbound exception, do the following:
   - **3a** Specify *All Interfaces* for the Source Interface parameter.
   - **3b** Specify the server's public interface for the Destination Interface parameter.
   - **3c** Press *Enter* for Packet Type > select ftp-port-pasv-st.

NOTE: The packet type ftp-port-pasv-st allows both active and passive FTP connections. To allow active FTP connections only, select ftp-port-st. To allow passive FTP connections only, select ftp-pasv-st.

3d If you want the server to forward FTP packets from certain public hosts only, specify Host or Network for the Src Addr Type parameter > enter the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.

3e If you want the server to forward FTP packets addressed to certain private hosts only, specify Host or Network for the Dest Addr Type parameter > enter the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.

3f Press *Esc* > select Yes to save the filter.

4 If you are creating an outbound exception, do the following:

4a Specify the server's private interface for the Source Interface parameter.

4b Specify the server's public interface for the Destination Interface parameter.

4c Press *Enter* for Packet Type > select ftp-port-pasv-st.

NOTE: The packet type ftp-port-pasv-st allows both active and passive FTP connections. To allow active FTP connections only, select ftp-port-st. To allow passive FTP connections only, select ftp-pasv-st.

4d If you want the server to forward FTP packets from certain private hosts only, specify Host or Network for the Src Addr Type parameter and enter the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.

4e If you want the server to forward FTP packets addressed to certain public hosts only, specify Host or Network for the Dest Addr Type parameter > enter the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.

4f Press *Esc* and select Yes to save the filter.

IMPORTANT: The outbound stateful FTP filter does not allow packets for DNS name resolution to be forwarded to a DNS server on the public network. Users establishing an FTP connection to an FTP server must use the FTP server's IP address unless you set up a DNS filter.

Setting Up Static Filters for FTP

If you do not want to configure a stateful FTP exception, you can create static filters instead.

To allow public hosts to establish active FTP connections to a server in the private network, configure the following inbound and outbound filter exceptions:

- ftp (the control channel)
- ftp-data (the data channel)

If you want to allow users in your private network to establish passive FTP connections to public servers, configure additional filter exceptions for dynamic/tcp in both directions so dynamic ports can be used as the data channel instead of port 20. Enable ACK bit filtering for the dynamic/tcp exceptions.

IMPORTANT: These filters do not allow users to establish FTP connections using the FTP server's DNS name. A DNS filter is required.

Setting Up a Telnet Filter

You can set up a Telnet filter on your server's public interface to filter Telnet packets in the inbound or outbound direction. An inbound Telnet filter might be required if public users establish Telnet sessions to a server in your private network. An outbound Telnet filter might be required to allow users to establish a Telnet session on the public network.

This section contains the following tasks:

- "Setting Up a Stateful Telnet Filter" on page 90
- "Setting Up Static Filters for Telnet" on page 91

Setting Up a Stateful Telnet Filter

To set up a stateful Telnet filter exception,

1. Select Configure TCP/IP Filters > Packet Forwarding Filters > Exceptions.
2. Press *Ins* to define a new exception.
3. If you are creating an inbound exception:

3a Specify *All Interfaces* for the Source Interface parameter.

3b Specify the server's public interface for the Destination Interface parameter.

3c Press *Enter* for Packet Type and select telnet-st.

3d If you want the server to forward Telnet packets from certain public hosts only, specify Host or Network for the Src Addr Type parameter > enter the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.

3e If you want the server to forward Telnet packets addressed to certain private hosts only, specify Host or Network for the Dest Addr Type parameter > enter the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.

3f Press *Esc* > select Yes to save the filter.

4 If you are creating an outbound exception, do the following:

4a Specify the server's private interface for the Source Interface parameter.

4b Specify the server's public interface for the Destination Interface parameter.

4c Press *Enter* for Packet Type and select telnet-st.

4d If you want the server to forward Telnet packets from certain private hosts only, specify Host or Network for the Src Addr Type parameter > enter the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.

4e If you want the server to forward Telnet packets addressed to certain public hosts only, specify Host or Network for the Dest Addr Type parameter > enter the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.

4f Press *Esc* > select Yes to save the filter.

IMPORTANT: The outbound stateful Telnet filter does not allow packets for DNS name resolution to be forwarded to a DNS server on the public network. Users establishing a Telnet session must use IP addresses unless you set up a DNS filter.

Setting Up Static Filters for Telnet

If you do not want to configure a stateful Telnet exception, you can create static filters instead. Simply create a static Telnet filter exception in both the

inbound and outbound directions. Make sure you enable ACK bit filtering for the exception in the inbound direction.

IMPORTANT: These filters do not allow users to establish Telnet sessions using a server's DNS name. A DNS filter is required.

Setting Up an SMTP Filter

You can set up a Simple Mail Transfer Protocol (SMTP) exception on the server's public interface to allow SMTP mail servers or SMTP gateways in your private network to send and receive mail through the Novell BorderManager 3.7 firewall.

This section contains:

- "Setting Up a Stateful SMTP Filter" on page 92
- "Setting Up Static Filters for SMTP" on page 93

Setting Up a Stateful SMTP Filter

To set up a stateful SMTP filter exception,

1. Select Configure TCP/IP Filters > Packet Forwarding Filters > Exceptions.
2. Press *Ins* to define a new exception.
3. Specify the Source Interface by doing one of the following:
   - **3a** If you want private SMTP servers or gateways to be able to send mail through the firewall, specify the server's private interface.
   - **3b** If you want public SMTP servers to be able to send mail to the SMTP server in your private network, and you have not enabled the Mail proxy, specify the server's public interface.
4. Specify the Destination Interface by doing one of the following:
   - **4a** If you want private SMTP servers or gateways to be able to send mail through the firewall, specify the server's public interface.
   - **4b** If you want public SMTP servers to be able to send mail to the SMTP server in your private network, and you have not enabled the Mail proxy, specify the server's private interface.
5. Press *Enter* for Packet Type > select smtp-st.

6 Press *Esc* > select Yes to save the filter.

IMPORTANT: The outbound stateful SMTP filter does not allow domain names to be resolved by a DNS server on the public network.

Setting Up Static Filters for SMTP

If you do not want to configure a stateful SMTP exception, you can create static filters instead. Simply create a static SMTP filter exception in both the inbound and outbound directions. Make sure you enable ACK bit filtering for the exception in the inbound direction.

IMPORTANT: These filters do not forward requests for domain name resolution. A DNS filter is required.

Setting Up a POP3 Filter

You can set up a Post Office Protocol 3 (POP3) exception on the server's public interface to allow public clients to access a private POP3 server behind the Novell BorderManager firewall.

This section contains:

- "Setting Up a Stateful POP3 Filter" on page 93
- "Setting Up a Static POP3 Filter" on page 94

IMPORTANT: These filters do not forward requests for domain name resolution by a DNS server in your private network. A DNS filter is required.

Setting Up a Stateful POP3 Filter

To set up a stateful POP3 filter exception,

1 Select Configure TCP/IP Filters > Packet Forwarding Filters > Exceptions.

2 Press *Ins* to define a new exception.

3 Specify *All Interfaces* for the Source Interface parameter.

4 Specify the server's public interface for the Destination Interface parameter.

5 If you want the server to forward mail from certain public hosts only, specify Host or Network for the Src Addr Type parameter > enter the IP

address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.

6. If you want the server to forward mail addressed to certain private hosts only, specify Host or Network for the Dest Addr Type parameter > enter the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.
7. Press *Enter* for Packet Type > select pop3-st.
8. Press *Esc* > select Yes to save the filter.

Setting Up a Static POP3 Filter

If you do not want to configure a stateful POP3 exception, you can create a static filter instead. Make sure you enable ACK bit filtering for the exception in the inbound direction.

Setting Up a DNS Filter

TCP/IP connections to a server can be made by specifying the server's IP address, but most servers, particularly those connected to the Internet, are accessed by their DNS names.

This section contains:

Setting Up a Stateful DNS Filter

To set up a stateful DNS exception to allow users to use DNS names to connect to servers accessed through the Novell BorderManager 3.7 server's public interface, complete the following steps from the main FILTCFG menu:

1. Select Configure TCP/IP Filters > Packet Forwarding Filters > Exceptions.
2. Press *Ins* to define a new exception.
3. Specify the server's private interface for the Source Interface parameter.
4. Specify the server's public interface for the Destination Interface parameter.

5 Press *Enter* for Packet Type > select dns/udp-st.

6 Press *Esc* > select Yes to save the filter.

IMPORTANT: If applications are configured to use DNS over TCP, you can also configure a stateful DNS exception for DNS over TCP. In Step 5, select the dns/tcp-st packet type instead of the dns/udp-st packet type.

Setting Up Static Filters for DNS

If you do not want to configure a stateful DNS exception, you can create static filters instead.

In the direction that DNS queries will be sent, create the following static packet filter exception:

- dns/udp

In the direction that DNS responses will be sent, create the following static packet filter exception:

- dynamic/udp

Filtering IP Packets that Use the IP Header Options Field

In addition to containing 32-bit source IP address and destination IP address fields, IP packets also contain an options field. This field can be used for the following purposes:

- Security restrictions—United States Department of Defense (DoD) basic and extended security options to identify classification levels and secuirty information.
- Record route—List of IP addresses to identify each router that forwarded the packet.
- Time stamp—List of IP addresses and time stamps to identify each router that forwarded the packet.
- Source routing—List of IP addresses to which the packet must be routed.

Although the NetWare® TCP/IP stack does not process these options, it can be a security risk to forward packets with these options specified. In particular, the source routing option can force all packets that are routed from your network to be forwarded to an untrustworthy host in the public network.

When you install Novell BorderManager 3.7 firewall/caching services, a server SET command is automatically enabled to drop packets with IP header options enabled.

To view the current setting for your server:

1. At the server console, enter

   SET

2. Select option 1 (Communications).

3. Verify that the SET command displays as

   SET FILTER PACKETS WITH IP HEADER OPTIONS = ON

It is best not to change the default setting, but under certain circumstances you might need to turn this setting off. For example, you could use the source routing option to specify the routers that must handle the traffic from your network.

IMPORTANT: Because routers often do not support IP header options, be sure to verify the capability of your routers before disabling the filtering to perform such tests.

To disable the filtering of packets that use IP header options from the server console, enter

SET FILTER PACKETS WITH IP HEADER OPTIONS = OFF

To reenable the filtering from the server console, enter

SET FILTER PACKETS WITH IP HEADER OPTIONS = ON

5 Managing IP Packet Filters

The following sections describe how to manage Novell® BorderManager® 3.7 IP packet filters used as part of your firewall: refer to Table 3, "IPPKTLOG.CFG Configuration Parameters," on page 97 for the logging configuration parameters in IPPKTLOG.CFG.

Modifying Default IP Logging Parameters

If global logging for IP has been enabled, IP packets are automatically logged to a text file located in the SYS:ETC\LOGS\IPPKTLOG directory on the server. The configuration file, SYS:ETC\IPPKTLOG.CFG, specifies the logging parameters.

IMPORTANT: IP packets that match a specific packet filtering rule are not logged unless logging has been explicitly enabled for the filter.

Refer to the following table for the logging configuration parameters in IPPKTLOG.CFG.

Table 3 IPPKTLOG.CFG Configuration Parameters

Parameter	Default Value	Available Settings
LOG_FILE_TYPE	1	1 = Sequential log file.
LOG_FILE_LOCATION	SYS:ETC\LOGS\IPPKTLOG	Any directory.

Parameter	Default Value	Available Settings
LOG_FILE_ROLL_METHOD	3	1 = Roll log file every *n* hours, where *n* is the value assigned to LOG_FILE_ROLL_ METHOD_VALUE. 2 = Roll log file every *n* days, where *n* is the value assigned to LOG_FILE_ROLL_ METHOD_VALUE. 3 = Roll log file when the log file size exceeds *n* KB, where *n* is the value assigned to LOG_FILE_ROLL_METHOD_ VALUE.
LOG_FILE_ROLL_METHOD_ VALUE	100	Any value representing hours when LOG_FILE_ROLL_METHOD is 1. Any value representing days when LOG_FILE_ROLL_METHOD is 2. Any value representing KB when LOG_FILE_ROLL_METHOD is 3.
LOG_FILE_DELETE_METHO D	2	1 = Do not delete log files. 2 = Begin deleting log files when the number of log files reaches the limit specified by LOG_FILE_DELETE_ METHOD_VALUE. 3 = Begin deleting log files when the age of the log files reaches *n* hours, where *n* is the value assigned to LOG_FILE_DELETE_ METHOD_VALUE.

Parameter	Default Value	Available Settings
LOG_FILE_DELETE_METHOD_VALUE	512	Any value representing the number of files when LOG_FILE_DELETE_METHOD is 2. Any value representing the number of hours when LOG_FILE_DELETE_METHOD is assigned a value of 3. The value assigned should be greater than LOG_FILE_ROLL_ METHOD_VALUE if LOG_FILE_ROLL_ METHOD is assigned a value of 1.
LOG_CACHE_BUFFER_SIZE	80	Any value representing the size in KB. The value assigned should not exceed the available memory on the server.
DATE_TIME_FORMAT	2	1 = Do not insert a date and time stamp for each entry to the log file. 2 = Insert a date and time stamp for each entry to the log file. The date and time have the format of MM/DD/YYYY, HH:MM:SS +/- TimeZoneOffset, where MM is the month, DD is the day, and YYYY is the year.

If global logging for IP has been enabled, the Novell BorderManager 3.7 server is also configured by default to shut down the public interface when logging fails to occur. A logging failure can occur when the server experiences a shortage of disk space. If you want to disable the automatic shutdown of the public interface when logging fails, at the server console enter

SET SHUTDOWN PUBLIC INTERFACE ON LOG FAILURE = OFF

To reenable the automatic shutdown of the public interface, enter

SET SHUTDOWN PUBLIC INTERFACE ON LOG FAILURE = ON

Viewing IP Packet Log Information

The IP packet filter logs stored in the SYS:ETC\LOGS\IPPKTLOG directory can be viewed with any text editor. Because the log file conforms to the Microsoft* standard format, the data in the log file can be imported by most third-party applications for analysis.

Each entry in the log file contains the following fields:

- Date
- Time
- Source IP Address
- Destination IP Address
- Protocol
- Source Port
- Destination Port
- TCP Flags
- Access—1 indicates accept; 0 indicates deny
- IP Header
- IP Payload

NOTE: A dash (-) appearing in any of the fields indicates that the information was unavailable or did not apply to the type of packet that was logged.

6 Packet Filtering based on Novell iManager

Novell® BorderManager® 3.7 comes with a Packet Filtering Configuration Task based on Novell iManager for configuring TCP/IP filters. The Novell BorderManager Access Management Role and Packet Filtering Configuration Task is automatically plugged into into Novell iManager during Novell BorderManager 3.7 installation.

For an upgrade, ensure that all filters have been migrated to Novell eDirectory™. This can be done by loading FILTSRV MIGRATE on the server console.

Make sure that Novell iManager is up and working on the NetWare® 6 server.

To log in to Novell iManager:

1. In Internet Explorer > go to https://*ipaddress:2200* or use https://*DNS:2200*.
2. Log in to Novell iManager to use the Packet Filtering Configuration Task.
3. When you log in to Novell iManager, you can see the role of NBM Access Management on the left panel. Click NBM Access Management to see the Filter Configuration task.
4. Click the Filter Configuration task to see the NBM Server Selection option.
5. Select the Novell BorderManager 3.7 server.

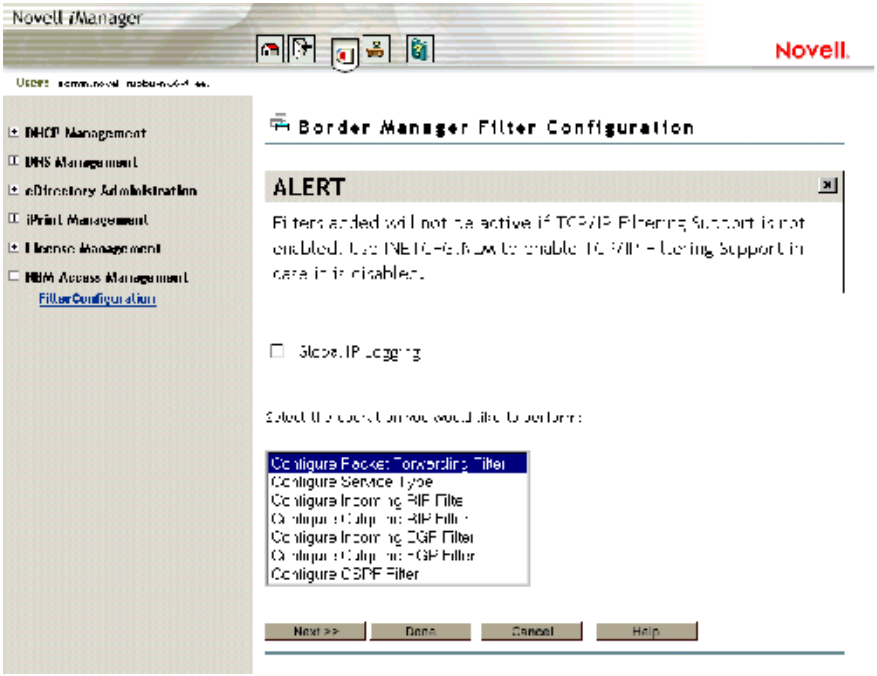
To set up the Packet Filtering Configuration Task, refer to Using Novell iManager for Filter Configuration in the *Novell BorderManager 3.7 Installation Guide*

To ensure that the configured filters are active, check to see that you have enabled filter support using INETCFG.

After you have reached the filter configuration task, the following seven types of configuration can be seen:

- Configure Packet Forwarding Filter
- Configure Service Type
- Configure Incoming RIP Filter
- Configure Outgoing RIP Filter
- Configure Incoming EGP Filter
- Configure Outgoing EGP Filter
- Configure OSPF Filter

Figure 1 Configuration Menu



The global logging status for all filter types can be enabled or disabled from the configuration menu.

Select any one of these for configuration:

- **Configuring Packet Forwarding Filter—**TCP/IP Packet Forwarding Filters allow the router to selectively filter packets based on their packet type, source, and destination.
- **Configuring Service Type—**Service Type includes the System and User defined packet types used for configuring Packet Forwarding filters.
- **RIP Filter—**Routing Information Protocol filters are used to control the propagation of routing information by this router. They provide a low level of security by hiding the existence of specific IP networks from other routers. There are two types of routing filters: Incoming and Outgoing.

  Incoming RIP filters restrict the acceptance of routing information from the adjacent routers. Outgoing RIP filters restrict the routing information advertised by the router to its adjacent routers.
- **EGP Filter—**The routes that the router may share with the EGP peers are defined with EGP filters. There are two types of EGP filters: Incoming and Outgoing.

  Incoming EGP filters restrict what routes can be accepted from an EGP peer. Outgoing EGP filters restrict what routes learned from RIP, OSPF, or static routes can be propagated to EGP peers.
- **Configuring OSPF Filter—**The router can use OSPF to exchange routing information within its Autonomous System. OSPF External Route Filters define the route and the source of the source of the route that will be propagated into the OSPF domain.

Select an operation from the list and click Next to continue.

Click Done if you want to save changes to IP logging and exit Filter Configuration.

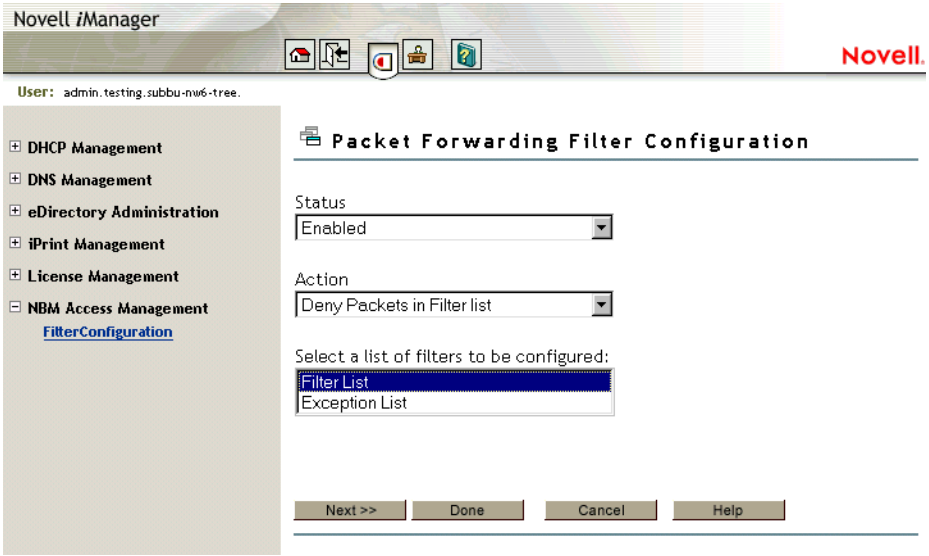
Click Cancel to exit Filter Configuration.

The next three sections contain information about configuring filter types:

- “Configuring the Packet Forwarding Filter” on page 104
- “Configuring the Service Type” on page 111
- “Configuring an Incoming RIP Filter” on page 113

Configuring the Packet Forwarding Filter

Figure 2 Packet Forwarding Filter Configuration



This page helps you to set the properties of the selected filter type:

Status—Choose between Disabling or Enabling the selected filters. If Filtering Support has been enabled in INETCFG.NLM for this protocol, altering the status will cause configured filters to immediately become active (Enabled) or inactive (Disabled).

Action—Choose between Denying and Permitting packets on the filter list. Specify the action taken when a packet matches a filter in the Filter List. If the filters in the Exception List overlap with the filters in the Filters List, the Exception List is used.

Select the list of Filters to be Configured—Select the list of filters to be configured: choose between the Filter List or the Exception List.

Filter List—Displays all configured filters. You can add new filters, or delete or modify existing filters. The data packets that match any filter are either permitted or denied depending on the setting of the Action parameter. Data packets that match any filter in the Exceptions List are not filtered, even if they match a filter in the Filters List.

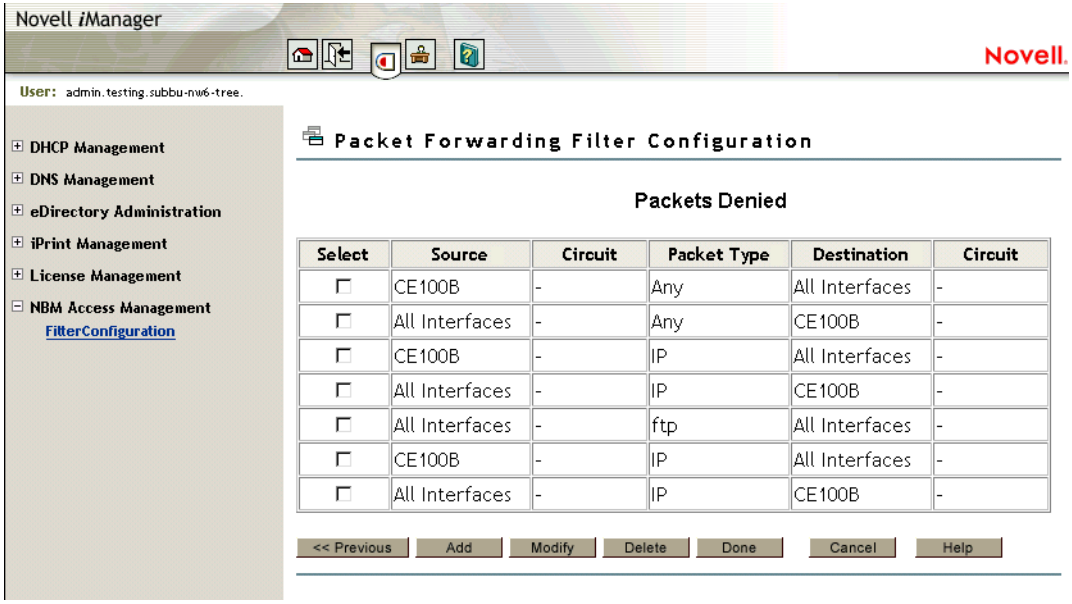
Exception List—Displays the exceptions to the filters defined in the Filters List, and allows you to specify additional exceptions. Exception filters take priority over filters in the Filter List. If a packet does not match an exception filter, it is checked against the Filters List. The packet is filtered if it matches any filter.

Select Filter List or Exception List and click Next to configure filters in that list.

Click Done to save changes to Status and/or Action of this filter type and return to the filter configuration menu.

Click Cancel to discard changes to Status and/or Action and return to the filter configuration menu.

Figure 3 Packet Forwarding Filter Configuration - Packets Denied



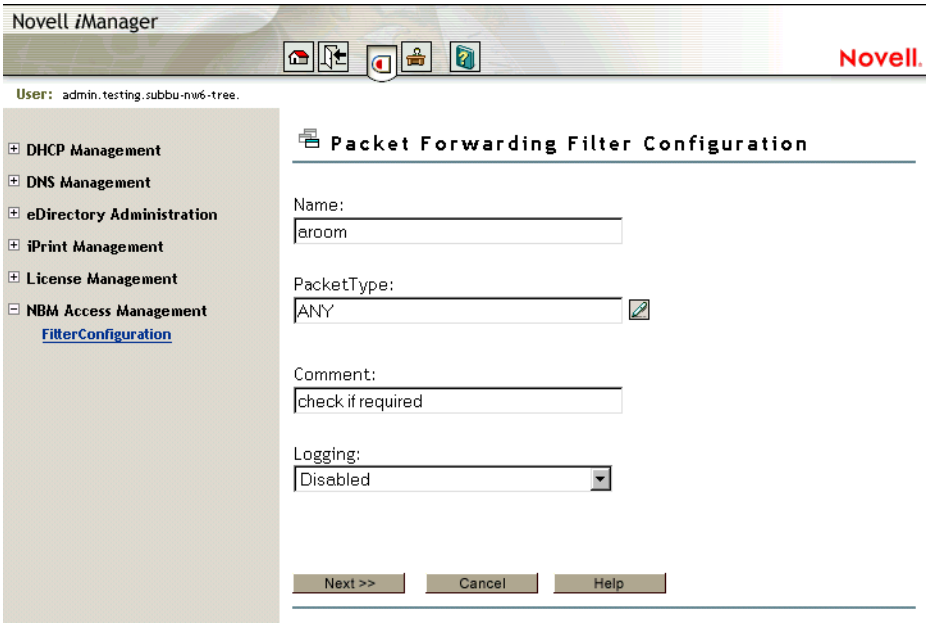
This page gives you a summary of Packet Forwarding Filters.

You can add new filters, or delete or modify existing filters. The data packets that match any filter are either permitted or denied depending on the setting of the Action parameter. Data packets that match any filter in the Exceptions List are not filtered, even if they match a filter in the Filters List.

Click Done to return to the beginning of Packet Forwarding Filter configuration.

Click Cancel to return to the filter configuration menu.

Figure 4 Packet Forwarding Filter Configuration - Add or Modify



This page helps you to add or modify your filter properties.

Name—Gives you the name of the packet filter. This is the name of the filter object that would be created in Novell eDirectory.

Service Type—Defines the service type to be filtered. Click the button to view a list of defined TCP/IP service types. You can select an entry for the filter being edited. If you want to add or modify or delete user-defined service types, go to the Configre Service Type option on the configuration menu. See Figure 1, “Configuration Menu,” on page 102.

Comment—Enter a short comment in this field, to save in the database along with the other entries in the form.

Logging—Choose to Enable or Disable this option.

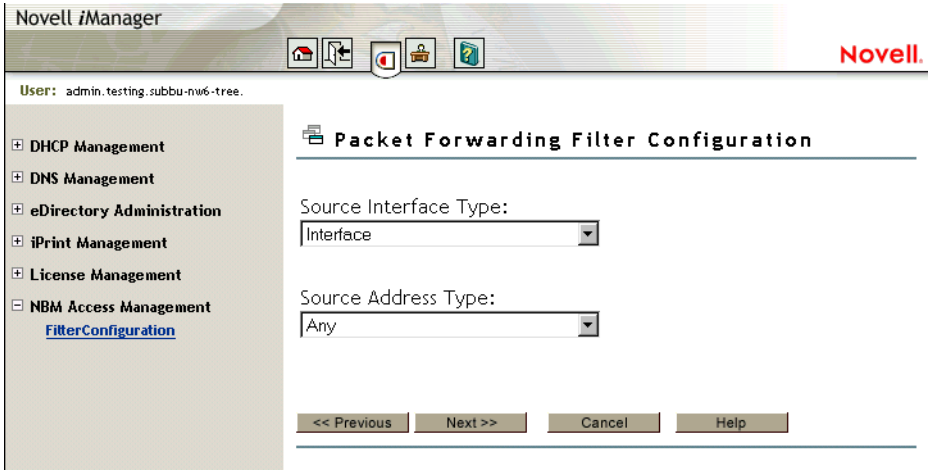
- Enable: The header of the packet that matches the options in the filters or exceptions will be logged as long as the global logging status and the filters/exception logging status are enabled. The LOG file is a BTRIEVE database file (CSAUDIT.LOG) located at SYS:\ETC\LOGS\IPPKTLOG directory.
- Disable: Packet that matches the options in filters or exceptions is not logged. Data logging slows down the server's performance and you should turn it on for a short time only. The local logging status can be enabled or disabled from the filter/exception definition menu.

Enter a name in the Name dialog box and click Next.

Click Done (in case of Modify only) to save changes to the filter and return to the Packet Forwarding Filter Summary.

Click Cancel to discard any changes to the filter and return to the Packet Forwarding Filter Summary.

Figure 5 Packet Forwarding Filter Configuration - type of information



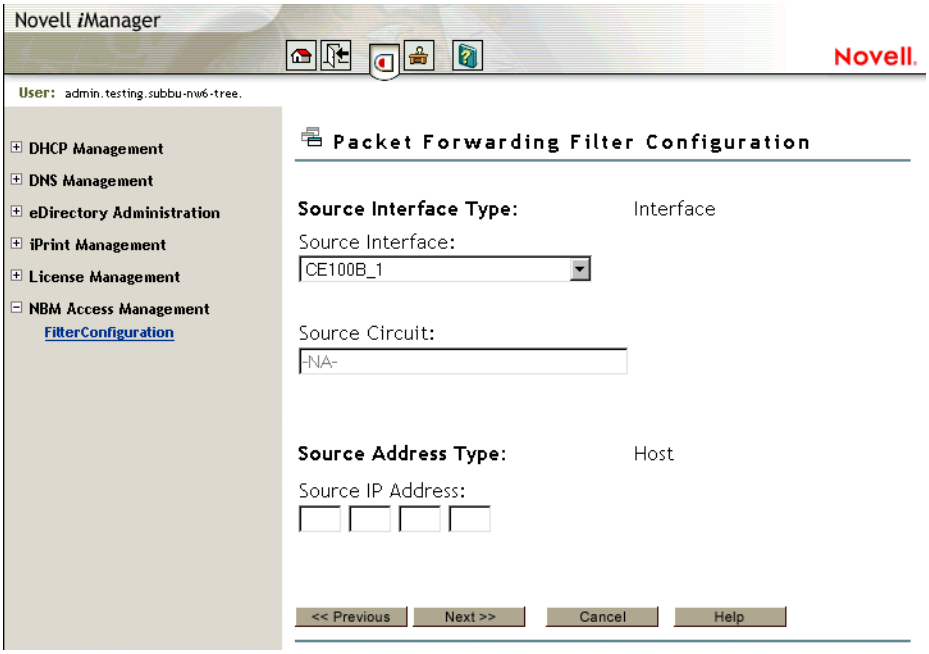
This page helps you to alter the type of information regarding the filter.

Source Interface Type—Select the source interface type of the TCP/IP packet forwarding filter. The available source types are Interface and Interface Group.

Source Address Type—Select the Source Address Type of the TCP/IP packet forwarding filter. The available source types are Network, Host, or Any Address.

Click Next.

Figure 6 Packet Forwarding Filter Configuration - information



This page helps you to alter the type of information regarding the filter.

Source Interface—Select a source interface.

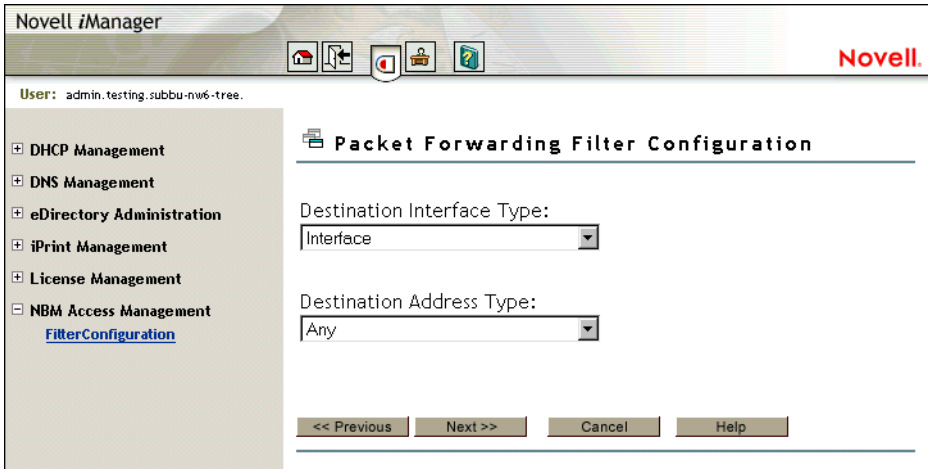
Source Circuit—Enter the information about the circuit to be configured. The source circuit is valid only if the source interface is of WAN media type. The default source circuit value is All Circuits.

Source IP Address—Gives the IP Address of your network or host.

Source Subnet Mask—Gives the Subnetwork mask of your network.

Click Next.

Figure 7 Packet Forwarding Filter Configuration - information



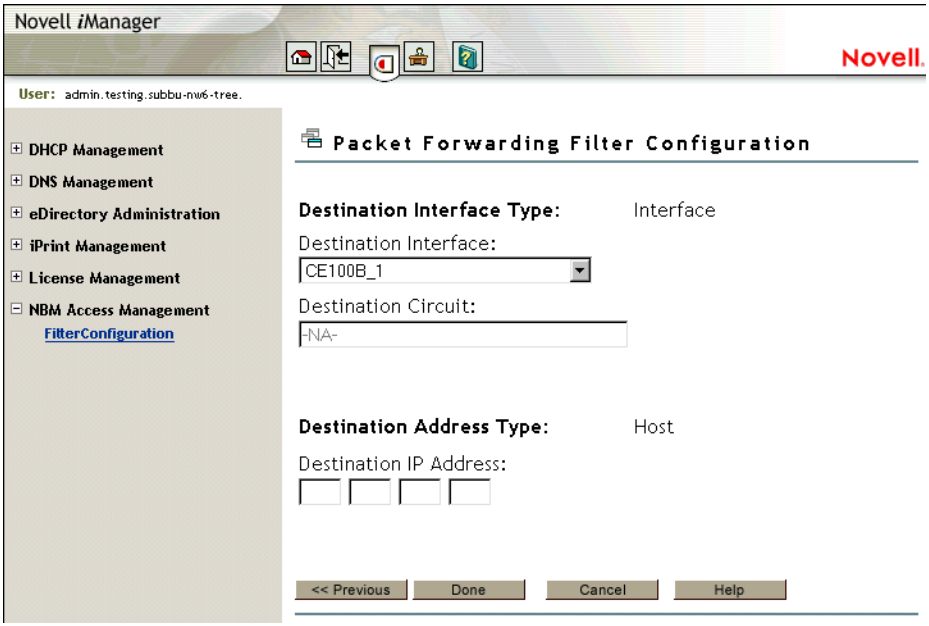
This page helps you to alter the type of information regarding the filter.

Destination Interface Type—Select the destination interface type of the TCP/IP packet forwarding filter. The available source types are Interface and Interface Group.

Destination Address Type—Select the Destination Address Type of the TCP/IP packet forwarding filter. The available types are Network, Host, Multicast, or Any Address.

Click Next.

Figure 8 Packet Forwarding Filter Configuration - information



This page helps you to alter the type of information regarding the filter.

Destination Interface—Select the destination interface.

Destination Circuit—Enter the information about the circuit to be configured. The destination circuit is valid only if the destination interface is of WAN media type. The default destination circuit value is All Circuits.

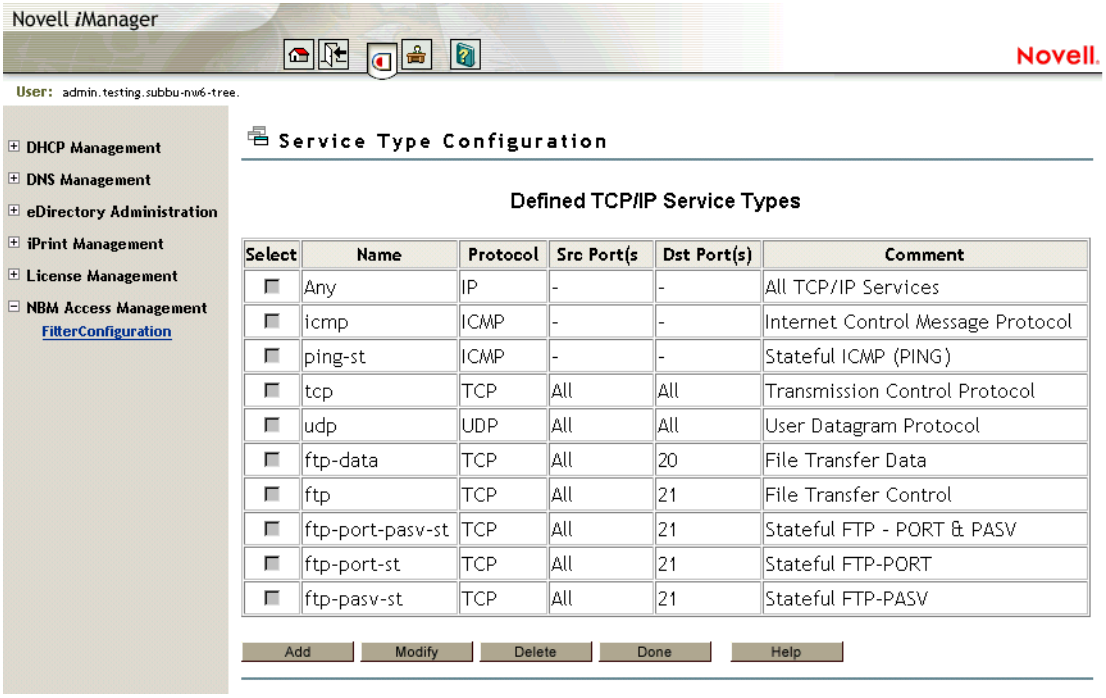
Destination IP Address—Gives the Network, Host or Multicast address.

Destination Subnetwork Mask—Gives the subnetwork mask of your Network.

Click Done.

Configuring the Service Type

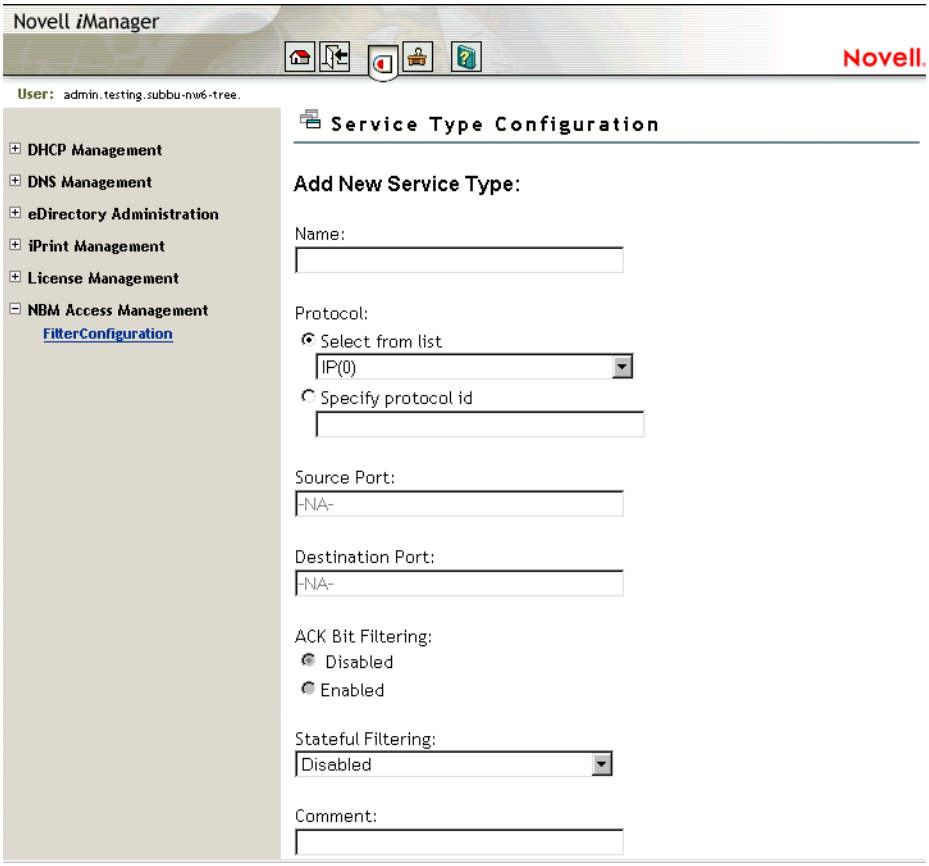
Figure 9 Service Type Configuration



This page gives you a summary of defined TCP/IP service types.

You can add new service types, or delete or modify only User service types.

Figure 10 Service Type Configuration - TCP/IP



This page helps you to configure the TCP/IP service types.

Name—Name of the TCP/IP service type.

Protocol—Either select from a list of commonly used internet protocols or specify a valid protocol ID between 0 - 255.

Source and Destination Port—Define a single TCP/IP port or range of ports separated by a hyphen for the TCP or UDP protocols. Valid port number range from 1 to 65535. If not defined, the default value for this field is All.

ACK Bit Filtering—this field is enabled only if the protocol selected is TCP. If the TCP ACK Bit filtering is enabled in a filter route, only the packets with the ACK Bit set are allowed through. This will effectively block all the

connections being initiated, in the direction defined by the filter rule. TCP ACK Bit filtering is often applied to all inbound TCP packets in a network.

Stateful Filtering—If stateful filtering is enabled in a filter rule, a dynamic filter will also be created in the reverse of the direction that is defined by the filter rule. The reverse filter is created with the information such as source IP address, source interface, source port, destination IP address, destination interface, and destination port. This information is stored in a table which will later be used to compare against the reply. If it is not a reply to the original request packet, stateful filtering will not allow the packet through. Stateful filtering supports both connection and connectionless protocols. For ICMP packets, only the reply ICMP messages are allowed. ICMP redirect messages will not be allowed. Stateful filtering is slower than the current static filtering but it is more secure. It does not open up all the ports as static filters do; instead, dynamic filters are created with more specific information on the IP address, source, and destination ports.

Comment—Enter a short comment in this field to save in the database along with the other entries in the form.

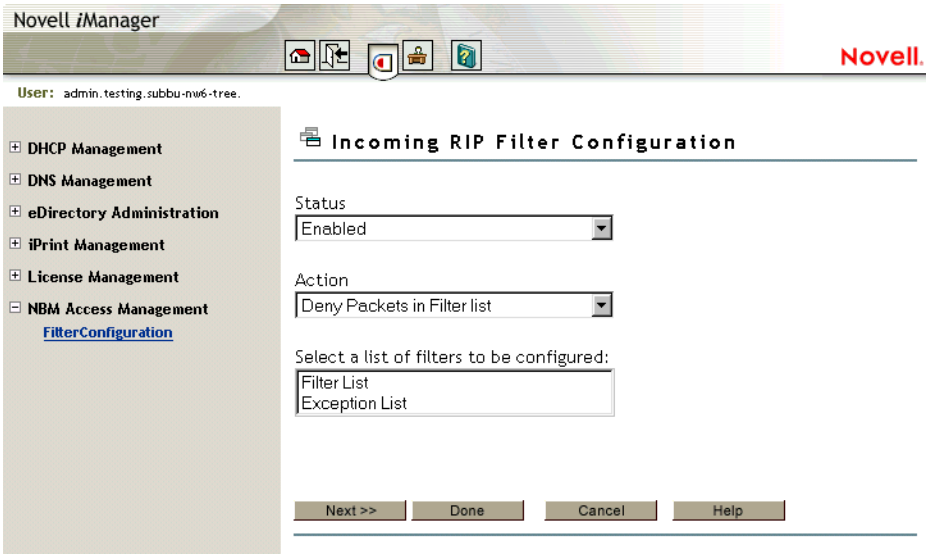
Click OK.

Configuring an Incoming RIP Filter

The following sections contain an overview of the Incoming RIP Filter Configuration screens. The same order of screens holds good for other configurations such as:

- Configure Outgoing RIP Filter
- Configure Incoming EGP Filter
- Configure Outgoing EGP Filter
- Configure OSPF Filter

Figure 11 Incoming RIP Configuration



This page helps you to set the properties of the selected filter type.

Status—Choose between Disabling or Enabling the selected filters. If Filtering Support has been enabled in INETCFG.NLM for this protocol, altering the status will cause configured filters to immediately become active (Enabled) or inactive (Disabled).

Action—Choose between Denying and Permitting packets on the filter list. Specify the action taken when a packet matches a filter in the Filter List. If the filters in the Exception List overlap with the filters in the Filters List, the Exception List is used.

Select the list of Filters to be Configured—Select the list of filters to be configured. Choose between the Filter List or the Exception List.

Filter List—Displays all configured filters. You can add new filters, or delete or modify existing filters. The data packets that match any filter are either permitted or denied depending on the setting of the Action parameter. Data packets that match any filter in the Exceptions List are not filtered, even if they match a filter in the Filters List.

Exception List—Displays the exceptions to the filters defined in the Filters List, and allows you to specify additional exceptions. Exception filters take priority over filters in the Filter List. If a packet does not match an exception

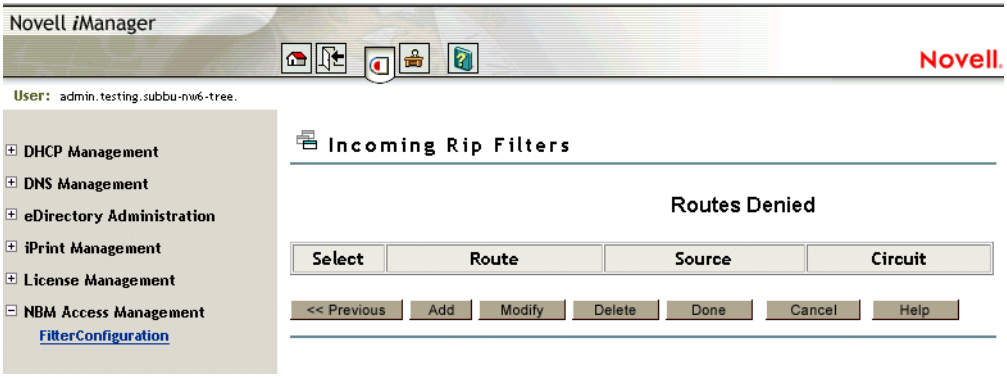
filter, it is checked against the Filters List. The packet is filtered if it matches any filter.

Select Filter List or Exception List and click Next to configure filters in that list.

Click Done to save changes to Status and/or Action of this filter type and return to the filter configuration menu.

Click Cancel to discard changes to Status and/or Action and return to the filter configuration menu.

Figure 12 Incoming RIP Configuration - TCP/IP



This page displays the configured TCP/IP incoming (route acceptance) RIP filters.

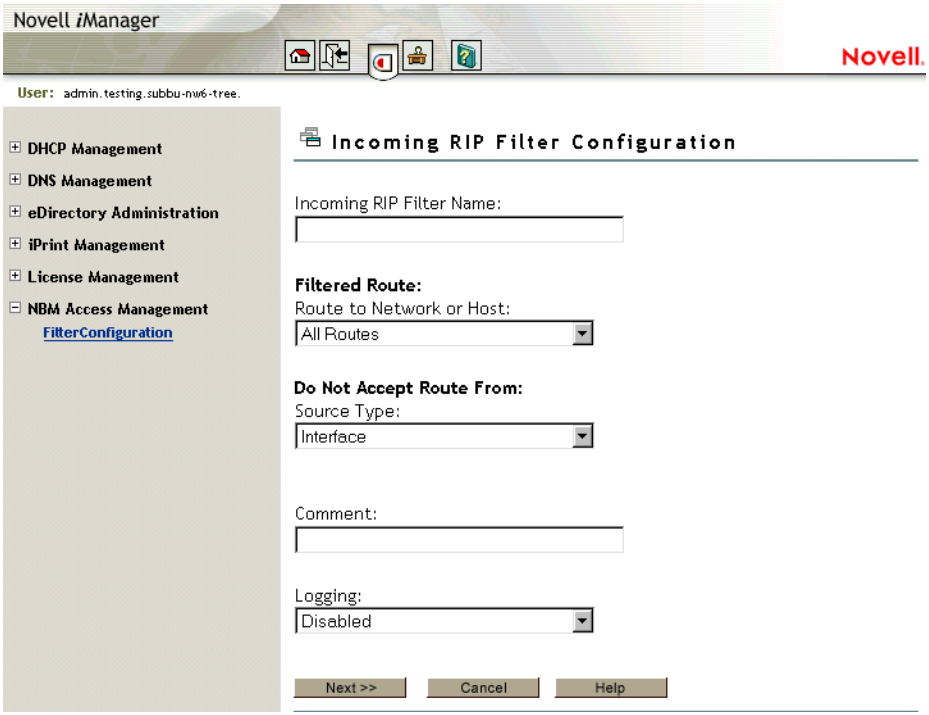
The filters are in Deny or Permit mode depending on what you have selected in the Action field. If the Action is deny then the RIP routes that match the criteria of a filter in the Filter List will not be accepted by the router. All other RIP routes will be accepted. If the Action is permit then the RIP routes that match the criteria of a filter in the Exception List will always be accepted by the router, even if another filter in the Filter List is configured to do the opposite.

You can add new filters, or delete or modify the filters in the list. After you save the changes, TCP/IP dynamically updates to the new configuration. The action taken on routes matching filters in this list is described in the Action field. You can select the Route and Source parameters from the list of defined values.

Click Done to return to the beginning of Incoming RIP Filter configuration.

Click Cancel to return to the filter configuration menu.

Figure 13 Incoming RIP Configuration



This page helps you to configure an Incoming RIP Filter.

Incoming RIP Filter Name—Enter the name of the RIP filter. This name becomes the distinguished name of the filter in the eDirectory.

Route to Network or Host—Specify the Host, Route, or Network to be filtered.

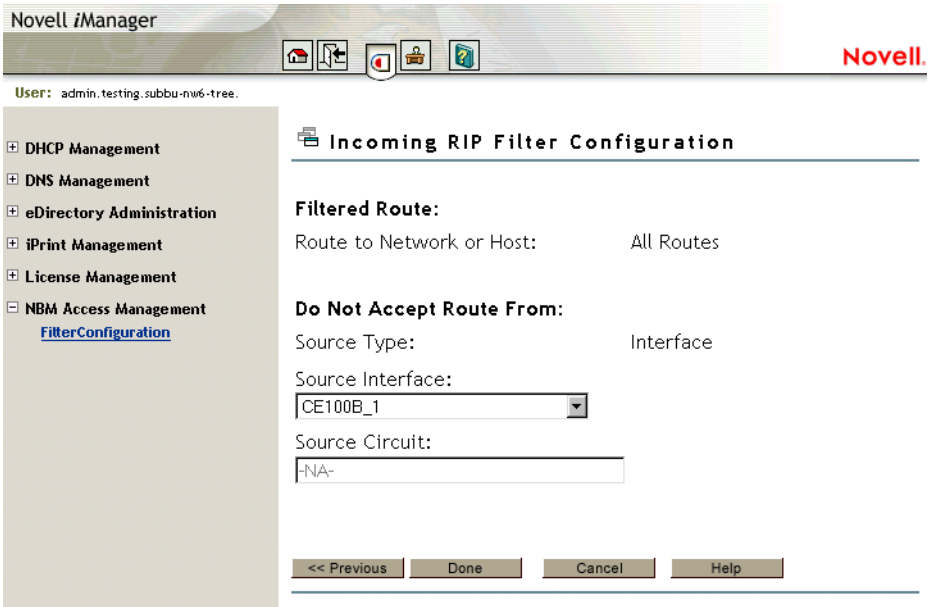
Source Type—Specify the source type that the router will accept or block the route to. Select from the list. The available types are Host, Interface, Interface Group and Network.

Comment—Enter a short comment in this field to save in the database along with the other entries in the form.

Logging—Choose to enable or disable this option.

- Enable: the header of the packet that matches the options in the filters or exceptions will be logged as long as the global logging status and the filters/exception logging status are enabled. The LOG file is a BTRIEVE database file (CSAUDIT.LOG) located at SYS:\ETC\LOGS\IPPKTLOG directory.
- Disable: Packet that matches the options in filters or exceptions is not logged. Data logging slows down the server's performance and you should turn it on for a short time only. The local logging status can be enabled or disabled from the filter/exception definition menu.

Figure 14 Incoming RIP Configuration - information



This page helps you to alter the type of information regarding the filter.

Filtered Route

IP Address of Network/Host—Enter a four-byte IP address in dotted decimal notation. For example: 130.57.172.0.

NOTE: When configuring RIP filters for IP networks you should be aware of the fact that depending on the network topology, RIP broadcasts on a particular interface may only advertise the networks even if the network has been divided into several subnetworks. Configuring a filter for a subnetwork of a network, in this

case, will not stop information about the network itself from being included in the RIP broadcast. This means that you may have to configure a filter for the network and not the subnetwork to prevent the subnetwork information from being advertised on an interface. You can configure filters for subnetworks to prevent those subnetworks being advertised on other subnetworks of the same network, but be aware that their effectiveness will be influenced by the routing topology.

Subnetwork Mask—Enter a four-byte mask in dotted decimal format. 255.255.255.255 is invalid. The mask must also cover the nature mask.

Address Type of Routing Peer

Source Type—Specifies whether the source is a Host, Interface, Interface Group, or Network.

Source Interface—If your Source Type is Interface or Interface or Interface Group select a source location from the list of network interfaces.

Source Circuit—If the current source is of type Interface or Interface Group and is of WAN Media Type, enter the destination circuit parameters.

Source IP Address—if your Source Type is Network or Host, enter the IP address.

Subnetwork Mask—if your Source Type is Network, enter the Subnetwork Mask.

7 Back Up and Restore Filters

Novell® BorderManager® 3.7 features filtering based on NDS® or Novell eDirectory™. All the stored filters will be created under the container NBMRuleContainer. The container NBMRuleContainer is created at the same level as the NCP™ server object of the server where Novell BorderManager 3.7 is installed.To back up or restore IP filters in NDS or eDirectory you can use any one of the tools that supports the LDAP Import/Export utility.

The following sections discuss how to back up or restore filters using the ConsoleOne® NDS Import/Export utility.

- “Back Up NDS or eDirectory Filters to LDIF” on page 119
- “Restoring Filters to NDS or eDirectory from LDIF” on page 120

NOTE: Before using this utility, make sure that you have enabled the Allow Clear Text Passwords option of the LDAP Group object. To do so, on ConsoleOne, select the LDAP Group > right click the LDAP Group > Properties > enable Allow Clear Text Passwords.

Back Up NDS or eDirectory Filters to LDIF

To back up NDS or eDirectory filters to LDIF: .

1. Create a dummy file. This is required because the utility will not allow you to create the file online.
2. Start ConsoleOne > authenticate yourself.
3. Select Wizards > NDS or eDirectory Import/Export.
4. Select the Export LDIF File (the file you created in Step 1) Radio button > click Next.
5. Enter the Server DNS Name/IP Address.

6. Enter the Port:389.
7. Select Authenticated Login.
8. Enter the User Distinguished Name and password in LDIF format > click Next. An example of the entries could be cn=admin, o=novell.
9. Enter the Distinguished Name of the NBMRuleContainer as the Base Distinguished Name. For example, cn=NBMRuleContainer, O=novell
10. Select One Level as the scope > Click Next.
11. Select the Destination LDIF File > click Next > Finish.

Restoring Filters to NDS or eDirectory from LDIF

To restore filters to NDS or eDirectory from LDIF:

1. Start ConsoleOne and authenticate yourself.
2. Select Wizards > NDS or eDirectory Import/Export.
3. Select Import LDIF File Radio button > Click Next.
4. Select Source LDIF File > Click Next.
5. Enter the Server DNS Name/IP Address.
6. Enter the Port:389.
7. Select Authenticated Login.
8. Enter the User Distinguished Name and password in LDIF format > click Next > Finish. For example, of the enties could be cn=admin, o=novell.

V Gateway

The following section of *Novell® BorderManager® 3.7 Administration* guide describes the monitoring tools and log files that help you verify Novell IP Gateway performance.

- Chapter 8, “Managing the Novell IP Gateway,” on page 123

See the Setting Up the Novell IP Gateway section in the Novell BorderManager 3.7 Installation Guide for information on how to set up the Novell IP Gateway.

8 Managing the Novell IP Gateway

The following sections describe the tools and log files that help you manage the Novell IP Gateway:

Setting Up Logging for All Gateway Services

Logging can be enabled for all Novell® BorderManager® 3.7 gateway services from the configuration window for any gateway service. All gateways, however, must share the same log configuration. For example, if you enable and configure logging for the Internetwork Packet Exchange™ (IPX™)/IP gateway, logging for the IP/IP gateway and SOCKS 4 and SOCKS 5 services is enabled with the same parameters.

Logging is not required for gateway operation, but if it is enabled, the services that have been accessed and the source and destination IP addresses of each access are recorded. This information is useful for monitoring gateway performance and network security.

To enable universal logging for all gateway services:

1. In NetWare® Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. From the server's Gateway tab and under Enable Service, double-click an enabled gateway service.
3. In the Logging Format field, select Indexed to enable event logging.
4. In the Log Level field, specify a number between 0 and 3 that indicates the type of information to be logged by the server.

   The options are as follows:

   - 0—No information.
   - 1—Internet access information. The server records the user's fully distinguished NDS® or Novell eDirectory™ name, the access protocol (HTTP, for example), and the destination (www.novell.com, for example).
   - 2—Error codes (for example, NDS or eDirectory errors). Level 2 information can help you determine why a user cannot access a particular service.
   - 3—Debugging information (internal server communications, such as socket calls). Level 3 information is typically of interest only to software developers.

   Each log level is additive; for example, level 1 information is also logged at level 2.
5. Click OK to close the gateway service configuration window.

   Because the log configuration is universal, if you double-click another gateway service, the logging format and log level have already been configured. Note that logging is activated only after the Novell BorderManager 3.7 Setup page is closed.

Decoding Gateway Packet Traces

If you use the LANalyzer® for Windows* software on your intranet, you can decode IPX/IP gateway packet traces by adding TCP/IPX and UDP/IPX packet decodes to the LZFW.INI file. These packet decodes are not needed for the IP/IP gateway.

To add gateway packet decodes to LZFW.INI,

1. Open the LZFW.INI file.

2 Add the following lines under the NetWare IP section:

```
tcp(IPX)=TCP/IP,ipx,NetWare,0,0x9091,0x9091,0,0,0,0

udp(IPX)=TCP/IP,ipx,NetWare,0,0x9092,0x9092,0,0,0,0
```

3 Restart LANalyzer.

Checking Gateway Realtime Activity

To check Novell IP Gateway realtime activity, complete the following steps:

1 In NetWare Administrator, click the Server object representing the Novell BorderManager 3.7 server.

2 Select Novell BorderManager 3.7 from the Tools menu.

3 Click IP Gateway and select Monitor Realtime Activity from the Object menu.

The IP Gateway Monitor window displays, providing the following summary information about the Novell IP Gateway:

- Licenses Installed—Number of Novell IP Gateway licenses installed.
- Licenses in Use—Number of Novell IP Gateway licenses in use.
- Bytes Received—Total number of bytes received by the gateway for all users.
- Bytes Sent—Total number of bytes sent through the gateway by all users.

The window also provides the following information about each user currently using the Novell IP Gateway:

- Username.
- Duration—Duration of the current gateway session.
- Bytes Received—Number of bytes received by the user.
- Bytes Sent—Number of bytes sent by the user.
- Last Access—Last location to which the user was connected.
- Network Address—Network address of the user.

Checking the Access Control Log

The access control log contains access information for all Novell BorderManager 3.7 services that enforce access rules, not just the Novell IP Gateway.

To check the access control log:

1. In NetWare Administrator, click the Server object representing the Novell BorderManager 3.7 server.
2. Select Novell BorderManager 3.7 from the Tools menu.
3. From the NetWare Administrator menu, select Novell BorderManager 3.7 > View Access Control Log.

Viewing User Statistics

To display user statistics in the Novell IP Gateway audit log,

1. In NetWare Administrator, click the Server object representing the Novell BorderManager 3.7 server.
2. Select Novell BorderManager 3.7 from the Tools menu.
3. Click IP Gateway and select View Audit Log from the Object menu.

   The IP Gateway Users Statistics window displays, with two list boxes: the Number of Users list box and the Hosts Accessed by User list box.

   NOTE: You can click the column heading of either list box to sort the entries in that column in ascending or descending order. The sorting order is reversed each time you click the column heading.

   The Number of Users list box provides the following information about activity through the gateway:

   - Username—NDS or eDirectory name or IP address of the user. In the case of an IP address, the Domain Name System (DNS) hostname will be displayed if it exists in the local DNS list. The local DNS list is built automatically each time the WHO IS or DNS Hostname command is invoked using the right-click menu.
   - Duration—Total amount of time connections have been used by user to access listed hosts.
   - Hosts Accessed—Number of hosts accessed by user during the queried period of time.

- Bytes Received—Total amount of data received by user from all hosts.
- Bytes Sent—Total amount of data sent from user to all hosts.

The Hosts Accessed by User list box provides the following information about activity through the gateway:

- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS hostname or IP address of the accessed host.
- Connections—Total number of connections made to host by user during specified period.
- Bytes Received—Total amount of data received by user from host.
- Bytes Sent—Total amount of data sent from user to host.

4 To display additional types of user information, do one of the following:

4a To display the records for a set of connections from a specific user to a specific host, click Display Records and enter a time range for the record you want displayed.

For a U.S. English system, the dates are entered in the order of month, day, and year. The order is year, month, and day for a Japanese system; and day, month, and year for European language systems.

4b To see all the connections made by a particular user, double-click the username in the Number of Users list box.

The IP Gateway Log displays, providing the following information about activity through the gateway:

- Entry Time—Time connection was established.
- Username—NDS or eDirectory name or IP address of user.
- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS hostname or IP address of the accessed host.
- Bytes Received—Total amount of data received by user from host.

- Bytes Sent—Total amount of data sent from user to host.

4c To see all the connections made by a particular user, double-click the username in the Number of Users list box.

The IP Gateway Log displays, providing the following information about activity through the gateway:

- Entry Time—Time connection was established.
- Username—NDS or eDirectory name or IP address of user.
- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS hostname or IP address of the accessed host.
- Bytes Received—Total amount of data received by user from host.
- Bytes Sent—Total amount of data sent from user to host.

NOTE: Right-clicking a record in the list displays a menu of options with three selections. Click Connect to launch your browser and connect to that host. Click Who Is to determine the IP address of a host listed with a DNS hostname. Click DNS Hostname to determine the DNS hostname of a host listed with an IP address.

4d To view usage trends graphs, click Usage Trends. In the IP Gateway Usage Trends window > select the date and the category of usage trend data.

You can view the following categories of usage trend data by time of day in one-hour increments:

- Users—Bar graph showing the number of unique users allowed to connect to a host through the Novell IP Gateway.
- Hosts Accessed—Bar graph showing the number of hosts accessed through the Novell IP Gateway.
- Bytes Received/Sent—Line graph showing the number of bytes received and sent through the Novell IP Gateway.
- Bytes Received, Sent and Users—Combination line and bar graph showing the number of bytes received and bytes sent, and the number of users.

All graphs can be saved to disk, copied to the clipboard, or printed.

Viewing Host Statistics

To display the hosts statistics in the Novell IP Gateway audit log:

1. In NetWare Administrator, click the Server object representing the Novell BorderManager 3.7 server.
2. Select Novell BorderManager 3.7 from the Tools menu.
3. Click IP Gateway and select View Audit Log from the Object menu.

   The IP Gateway Users Statistics window displays, with two list boxes: the Number of Users list box and The Hosts Accessed by User list box.
4. To display additional types of host information, do one of the following:

   4a. To see which users have accessed a particular host, double-click the entry for that host in the Hosts Accessed by User list box.

   The IP Gateway Hosts Statistics window displays, with two list boxes: the Number of Hosts list box and the Users Accessed list box.

   NOTE: You can click the column heading of either list box to sort the entries in that column in ascending or descending order. The sorting order is reversed each time you click the column heading.

   The Number of Hosts list box provides the following information about activity through the gateway:

   - Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
   - Hostname—DNS hostname or IP address of host.
   - Users Accessed—Number of users who accessed the host during specified period.
   - Bytes Received—Total amount of data received by all users from host.
   - Bytes Sent—Total amount of data sent from all users to host.

   NOTE: Right-clicking a record in the list displays a menu of options with three selections. Click Connect to launch your browser and connect to that host. Click Who Is to determine the IP address of a host listed with a DNS hostname. Click DNS Hostname to determine the DNS hostname of a host listed with an IP address.

   The Users Accessed list box provides the following information about activity through the gateway:

- Username—IP address or DNS hostname of the user who accessed the host.
- Duration—Total amount of time connections have been used by user to access host.
- Connections—Number of requests by user.
- Bytes Received—Amount of data received by user from host.
- Bytes Sent—Amount of data sent from user to host.

4b To see a list of the records for users who have accessed a particular host, double-click a host entry in the Number of Users list box.

The IP Gateway Log window displays, providing the following information about activity through the gateway:

- Entry Time—Time connection was established.
- Username—NDS or eDirectory name or IP address of user.
- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS hostname or IP address of the accessed host.
- Bytes Received—Total amount of data received by user from host.
- Bytes Sent—Total amount of data sent from user to host.

NOTE: Right-clicking a record in the list displays a menu of options with three selections. Click Connect to launch your browser and connect to that host. Click Who Is to determine the IP address of a host listed with a DNS hostname. Click DNS Hostname to determine the DNS hostname of a host listed with an IP address.

Exporting Data

The Novell IP Gateway audit log is stored in a Btrieve* file on the Novell BorderManager 3.7 server and is maintained by CSAUDIT.NLM. The audit log cannot be edited or manipulated from the server; however, the data can be exported for analysis. The format of the exported data is compatible with popular trend analysis software packages, such as WebTrends*.

There are two ways to export the Novell IP Gateway audit log information from NetWare Administrator:

- "Exporting Data from the IP Gateway Users Statistics Window" on page 131
- "Exporting Data Using the BorderManager Pull-Down Menu" on page 132

If you use the second method, you can combine the audit log files from other Novell BorderManager 3.7 services with the Novell IP Gateway audit log file into a single ASCII file.

Exporting Data from the IP Gateway Users Statistics Window

To export records from the IP Gateway Users Statistics window, complete the following steps:

1. In NetWare Administrator, click the Server object representing the Novell BorderManager 3.7 server.
2. Select Novell BorderManager 3.7 from the Tools menu.
3. Click IP Gateway > select View Audit Log from the Object menu.
4. If the records you want to export do not appear, click Display Records, enter the dates for the records you want to display > click OK.
5. In the IP Gateway Users Statistics window, click Export Data and enter the path and filename or click Browse to select a destination for the export file.
6. Select one of the following sort formats under Information Output Selection > click OK:
   - Time entry (connection by connection)—(Default selection) Sorts records from earliest entry time to latest entry time.
   - Access by users—Sorts records in alphabetic order based on the user's eDirectory username.
   - Access by hosts—Sorts records in ascending order (for IP addresses) or alphabetic order (for DNS hostnames).
7. (Conditional) If the export filename already exists under the directory path selected, you are prompted to replace the file. Click Yes to overwrite the file or No to specify the destination as described in Step 5.

The record fields are written to disk with a tab as the delimiter. Each record ends with a carriage return and line feed. The exported data has the following format:

- Entry Time—Time connection was established.
- Username—NDS or eDirectory name or IP address of user.
- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS hostname or IP address of the accessed host.
- Bytes Received—Total amount of data received by user from host.
- Bytes Sent—Total amount of data sent from user to host.

Exporting Data Using the BorderManager Pull-Down Menu

Use the Export Logs selection from the Novell BorderManager 3.7 pull-down menu to export the Novell IP Gateway audit log. This procedure extracts the same data from the Btrieve database, but offers additional export options that cannot be activated from the IP Gateway Users Statistics window.

To export the Novell IP Gateway audit log using the Export Logs menu selection:

1. In NetWare Administrator, click the Server object representing the Novell BorderManager 3.7 server.
2. Select Novell BorderManager 3.7 from the Tools menu.
3. From the Novell BorderManager 3.7 menu, select Export Logs.
4. Click Set Range > enter the date range.

   This is the range of dates comparable to the dates used to display records in the IP Gateway Users Statistics window. The default range is the current server date.
5. Click Browse to select the drive mapped to the destination for the export file.

   This is the path and filename for the export file. The default destination is A:\YYYYMMDD.LOG, where YYYY is the current year, MM is the current month, and DD is the current day. If you change the filename from the default format, the filename will not reflect the current server date. For example, if you change the filename format to MMDDYYYY.LOG, the next time you try to export logs on another day, the log filename will not have incremented to the current date.

6. (Optional) If the default filename is unacceptable, enter a new filename in the File field.

7. (Optional) If you want to combine the Novell IP Gateway audit log with audit logs from other Novell BorderManager 3.7 services, check the Combine Log Files check box.

   This feature allows log files from different Novell BorderManager 3.7 services to be combined into a single output file. When log files are combined, they are appended to one file, service by service.

8. Under Log Selection, check the IPX gateway check box.

   NOTE: Checking the box for IPX gateway exports the entire audit log file for the Novell IP Gateway, not just the records for the IPX/IP gateway service.

9. (Optional) If you checked Combine Log Files in Step 7, under Log Selection, check all other Novell BorderManager 3.7 audit log files to be combined with the Novell IP Gateway audit log file.

10. Click OK.

The audit log is exported to an ASCII file. The record fields are written with a tab as the delimiter. Each record ends with a carriage return and line feed. The exported data has the following fields:

- Keyword—IPXGW. If the Combine Log Files option was selected, the keyword is at the beginning of each Novell IP Gateway audit log line.
- Date.
- Time.
- Source—Typeless eDirectory name and context, such as mlira.pubs.novell, IP address, or IPX address.
- Destination—DNS domain name or IP address.
- Bytes received.
- Bytes sent.
- Protocol—Protocol used, such as HTTP or FTP.

If the Combine Log Files feature is *not* selected and you select one or more services under the Log Selection field, a separate export file is created for each service under a subdirectory of the export destination path.

The export subdirectories used are shown in the following table.

Log Type	Export Subdirectory
HTTP Proxy	HTTP
FTP Proxy	FTP
NNTP Proxy	NNTP
Mail Proxy	SMTP
RealAudio* and Real Time Streaming Protocol (RTSP) Proxies	RAUDIO
DNS Proxy	DNS
Generic Proxy	GENERIC
SOCKS Client	SOCKS
IPX Gateway (Novell IP Gateway)	IPXGW
VPN	VPN
ACL (access control)	ACL

For example, if you specified an export destination of VOL1:LOGS\19981019.LOG, did not select the Combine Log Files feature, and checked the boxes for HTTP proxy, FTP proxy, and IPX gateway, the following logs would result:

- VOL1:LOGS\HTTP\19981019.LOG
- VOL1:LOGS\FTP\19981019.LOG
- VOL1:LOGS\IPXGW\19981019.LOG

Checking the Information Log

The information log contains information about the Novell IP Gateway only. This log does not record information about other Novell BorderManager 3.7 services.

To display the Information Log window, complete the following steps:

1. In NetWare Administrator, click the Server object representing the Novell BorderManager 3.7 server.
2. Select Novell BorderManager 3.7 from the Tools menu.
3. From the Novell BorderManager 3.7 menu, select View Information Log.

   The Information and System Logs window displays, with two tabs: the Information Log tab and the SYS$LOG.ERR tab.

   From the Information Log tab, you can view configuration information such as the following:

   - When the Novell IP Gateway module was loaded or unloaded on the server
   - Logging level
   - Whether audit logging is turned on or off
   - Which gateway service is enabled—IPX/IP gateway, IP/IP gateway, or SOCKS gateway
   - The Novell IP Gateway control port and data port addresses
   - The Novell IP Gateway's public or private address
   - Which clients have been authenticated by the Novell IP Gateway

   NOTE: Each message in the information log is also stamped with the date and time it was recorded in the log file.

   From the SYS$LOG.ERR tab, you can view the system error messages recorded from the server console.

   NOTE: If you click the SYS$LOG.ERR tab, you might be warned that the log file is too large. In this case, only the last 32 KB of data in the log file is displayed.

VI Network Address Translation

The following sections of the *Novell® BorderManager® 3.7 Administration* guide provides the basic information you need to set up Network Address Translation (NAT). See

- Chapter 9, “Advanced Configuration of NAT,” on page 139 for the procedures you need to set up and configure various NAT features and parameters.
- Chapter 10, “Managing NAT,” on page 145 for tips and guidelines for monitoring NAT functionality.

See the Setting Up NAT section in the *Novell BorderManager 3.7 Installation Guide* for instuctions on how to set up Network Address Translation.

9 Advanced Configuration of NAT

This section provides an example of using Novell® BorderManager® 3.7 Network Address Translation (NAT) in a private network when the network uses both registered and unregistered addresses.

In this example, NAT is used to separate a segment of a private network, which uses registered addresses, from the rest of the network, which uses unregistered addresses. As shown in the illustraion below, the segments of the private network that use unregistered addresses (network 10.0.0.0 and network 11.0.0.0) have an FTP server and database server that need to be accessible from the Internet.

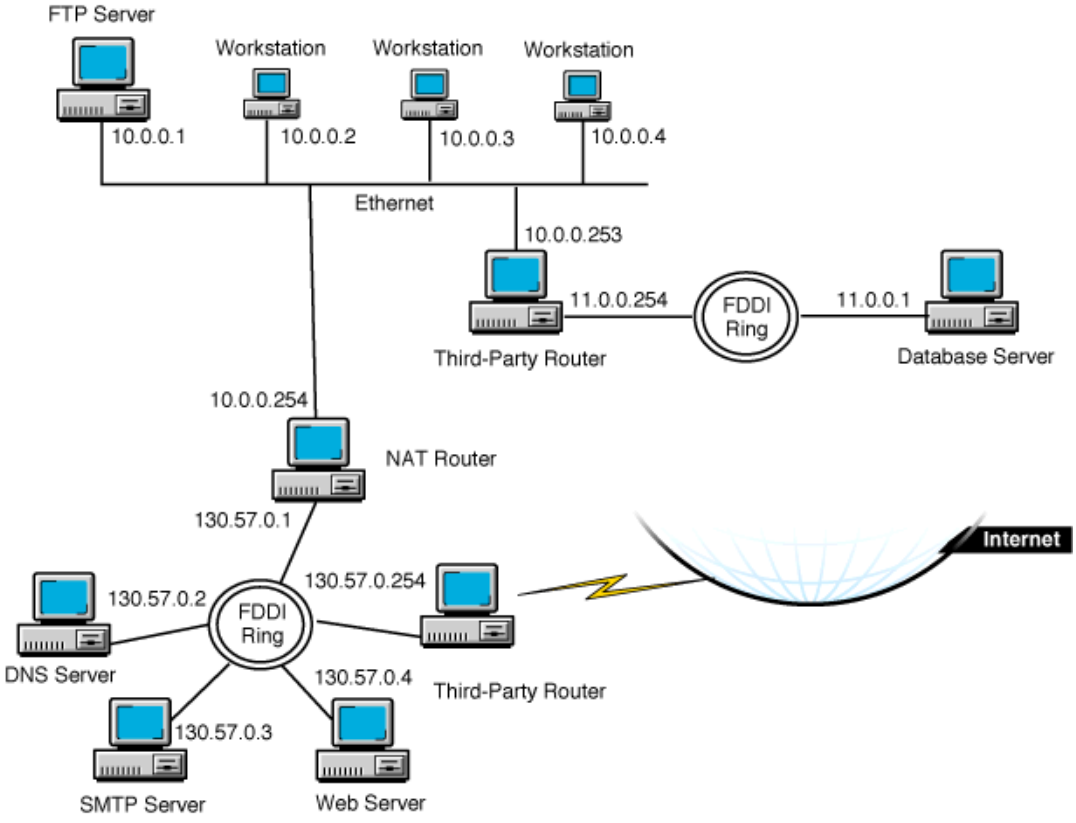
Workstations on network 10.0.0.0 should be able to access the rest of the private network and the Internet.

The segment of the private network that uses registered addresses (network 130.57.0.0) has a Web server, a Domain Name Server (DNS) server, and a Simple Mail Transfer Protocol (SMTP) gateway server that should be accessible from the workstations on the rest of the private network.

In this example, the following registered IP addresses have been obtained from an Internet Service Provider (ISP) for NAT use: 130.57.100.1, 130.57.100.2, 130.57.100.3, 130.57.100.4, and 130.57.110.1.

These addresses are to be mapped to the FTP server, database server, and workstations on the 10.0.0.0 and 11.0.0.0 networks.

Figure 15 Using NAT within a Private Network



For this example, an administrator must complete the following tasks:

- Add the secondary IP addresses on the NAT router interface that has been assigned IP address 130.57.0.1.
- Enable network address translation on the NAT router interface.
- Create a network address translation table mapping the secondary IP addresses to the private hosts on networks 10.0.0.0 and 11.0.0.0.
- Create static (default) routes on the routers to enable routing between the private network segments if the routers have been configured to filter Routing Information Protocol (RIP) packets.

To perform these tasks:

1. At the server console, enter

LOAD INETCFG

2. Select Protocols.
3. If TCP/IP was not configured on the NAT router interfaces, enable TCP/IP for each interface under Protocols, and bind IP addresses to the public and private interfaces under Bindings.

   In this example, bind 130.57.0.1 to the public interface, and bind 10.0.0.254 to the private interface.
4. Press *Esc* until you are prompted to save your changes, then select Yes.
5. Select Manage Configuration > Edit AUTOEXEC.NCF.
6. Enter the commands to bind secondary IP addresses after the line that executes INITSYS.NCF.

   In this example, enter the following lines:

   ADD SECONDARY IPADDRESS 130.57.100.1

   ADD SECONDARY IPADDRESS 130.57.100.2

   ADD SECONDARY IPADDRESS 130.57.100.3

   ADD SECONDARY IPADDRESS 130.57.100.4

   ADD SECONDARY IPADDRESS 130.57.110.1
7. Press *Esc* until you are prompted to save your changes, then select Yes.
8. Press *Esc* until you return to the Internetworking Configuration menu.
9. Select Bindings.
10. Select the public interface which has a registered address bound to it.

    In this example, select the interface bound to the address 130.57.0.1.
11. Select Expert TCP/IP Bind Options.
12. Select Network Address Translation.
13. For Status, select Static Only.
14. Select Network Address Translation Table, then press *Ins*.

    Enter the following public address and private address pairs:

Public Address	Private Address
130.57.100.1	10.0.0.1
130.57.100.2	10.0.0.2
130.57.100.3	10.0.0.3

130.57.100.4	10.0.0.4
130.57.110.1	11.0.0.1

15 Press *Esc* until you are prompted to save your changes, then select Yes.

16 Press *Esc* to return to the Internetworking Configuration menu.

17 If the third-party router that connects the 10.0.0.0 network to the 11.0.0.0 network is filtering outgoing RIP packets, add a static route on the NAT router for the 11.0.0.0 network with a next hop of 10.0.0.253.

Also verify that each host on the 10.0.0.0 network that will be allowed to access the 11.0.0.0 network has a static route to the router with the IP address 10.0.0.253.

To configure a static route on the NAT router, complete the following substeps:

17a From the Internetworking Configuration menu, select Protocols > TCP/IP.

17b If necessary, change the status of LAN Static Routing from Disabled to Enabled.

17c Select the LAN Static Routing Table field.

17d Press *Ins* to add a TCP/IP static route.

17e For Route Type, select Network.

17f For IP Address of Network/Host, enter 11.0.0.0.

17g For Subnetwork Mask, accept the default, FF.0.0.0, or enter the subnet mask for your network.

17h For Next Hop Router on Route, enter 10.0.0.253.

17i Press *Esc* and select Yes to update the database.

17j Press *Esc* and select Yes to update the TCP/IP configuration.

17k Press *Esc* to return to the Internetworking Configuration menu.

18 If the NAT router is filtering incoming RIP packets, add a default static route for the 130.57.0.0 network on the third-party router that connects the 11.0.0.0 network to the rest of the network.

Also verify that each host on the 10.0.0.0 network that is allowed to access the Internet uses 10.0.0.254 bound to the NAT interface as the default route to the 130.57.0.0 network.

NOTE: Because the 10.0.0.0 network is not using registered addresses, both incoming and outgoing RIP packets should always be filtered. This enables NAT to hide the 10.0.0.0 network while allowing its hosts to access the Internet.

19 If the third-party router that connects the 130.57.0.0 network to the Internet is filtering incoming RIP packets, add a default route to the Internet on the NAT router with a next hop of 130.57.0.254.

Also verify that each host on the 130.57.0.0 network that is allowed to access the Internet has a default route to the router with the IP address 130.57.0.254.

To configure a default static route on the NAT router:

19a From the Internetworking Configuration menu, select Protocols > TCP/IP.

19b If necessary, change the status of LAN Static Routing from Disabled to Enabled.

19c Select the LAN Static Routing Table field.

19d Press *Ins* to add a TCP/IP static route.

19e For Route Type, select Default Route.

19f For Next Hop Router on Route, enter 130.57.0.254.

19g Press *Esc* twice and select Yes to update the database.

19h Press *Esc* and, if prompted, select Yes to update the TCP/IP configuration.

You are prompted to update the TCP/IP configuration if you enabled LAN Static Routing in Step 19b.

19i Press *Esc* to return to the Internetworking Configuration menu.

20 If you want the static routes to take effect immediately, select Reinitialize System and select Yes to activate your changes.

10 Managing NAT

This section provides tips and guidelines for managing Novell® BorderManager® 3.7 Network Address Translation (NAT) on your server. The primary means of managing NAT is to monitor NAT functionality. To monitor NAT functionality, verify the following:

- TCP/IP routing and connectivity is established. You can test IP connectivity using the LOAD PING command at the server console.
- NAT is enabled on the public interface. You can check whether NAT is enabled in NIASCFG.
- TCP/IP is bound to more than one interface. You can check the bindings in NIASCFG.
- Filters are not blocking outgoing packets. You can verify the configured filters using FILTCFG.
- Entries in the Static NAT Table are correct.
- Load TCPIP.NLM and then issue the **SET TCPIP DEBUG=1** command:
  - The NAT server is receiving incoming packets.
  - The correct address translation is performed.
  - Discarded packets are not displayed on the console screen.
  - The connection is not being reset by the NAT router.
- TCP reset packets (RSTs) are not displayed on LAN traces.

VII Proxy

The following sections of the *Novell® BorderManager® 3.7 Administration* guide provide information on how to use the Proxy Services.

- Chapter 11, “Advanced Configuration of Proxy Services,” on page 149 describes the procedures you need to set up a proxy cache server beyond the basic configuration and configure various advanced Proxy Services features and parameters.
- Chapter 12, “Managing Proxy Services,” on page 161 explains how to set up proxy logging and describes the information found in the Proxy Services logs.

See the Setting Up Proxy Services section in the *Novell BorderManager 3.7 Installation Guide* for information on how to set up Proxy Services.

11 Advanced Configuration of Proxy Services

This section contains the following procedures to enhance the Novell® BorderManager® 3.7 Proxy Services performance:

Configuring Cache Parameters

The following sections describe how to configure advanced cache parameters for Novell BorderManager 3.7:

Configuring Cache Aging Parameters

To configure cache aging parameters:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. Select an HTTP or FTP proxy or acceleration service, then click Caching.
3. From the Cache Aging tab, specify the following HTTP cache aging values:
   - HTTP Maximum Revalidation Time—The maximum number of hours or days HTTP data is cached before it is revalidated with the origin Web server. This overrides the Time to Expire specified by the origin Web server if it is greater than this value.
   - HTTP Default Revalidation Time—The number of hours or minutes HTTP data is cached before it is revalidated with the origin Web server. The data is revalidated if the origin Web server does not specify the Time to Expire.
   - HTTP Minimum Revalidation Time—The minimum number of hours or minutes HTTP data is cached by the server. This overrides the Time to Expire specified by the origin Web server if the time specified is less than this value. This parameter does not override the No Cache or Must Revalidate directives from the origin Web server.
   - FTP Revalidation Time—The number of hours or days FTP data is cached before it is revalidated with the origin Web server.
   - Gopher Revalidation Time—The number of hours or days Gopher data is cached before it is revalidated with the origin Web server.
   - HTTP Failed Request Cache Time—The number of seconds or minutes after which HTTP will return a failure for the requested pages that the proxy server could not retrieve from the origin Web server.
   - Maximum Hot Unreferenced Time—How long a node (or page) stays hot, or in a state where it can be more quickly accessed by the browser again after it has accessed the node once. The default is 20 minutes, after which the node is closed and the information is removed from memory. It takes longer for the proxy to access a node in cold state.

NOTE: This parameter works in conjunction with the Maximum Number of Hot Nodes parameter on the Cache Control tab. Refer to "Configuring Cache Parameters" on page 149 for more information.

4. Click OK, then click OK again from the Novell BorderManager 3.7 Setup page.

Configuring Cache Control Parameters

These parameters let you specify the maximum cached file size for each protocol, as well as the cache hash table size, number of hot nodes, and age ratio of the cache size to deleted files.

To configure cache control parameters:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. Select an HTTP or FTP proxy or acceleration service, then click Caching.
3. From the Cache Control tab, specify the following:
   - Maximum size of the file that is cached for each URL protocol request type—Enter this value in megabytes. Any file larger than the specified size is not cached. The default is 30 MB.
   - Size of the cache hash table—The table is used by the proxy to locate a URL in its cache. Its size determines the speed of the information lookup. The default is 128,000 entries, or 51 KB of memory.

     NOTE: Increasing the maximum number of hot nodes may enhance performance more than increasing the size of the cache hash table.
   - Maximum number of hot nodes or objects that can be cached—This is the number of nodes or pages that are hot, or in a state to be more quickly accessed by the browser again after it has accessed the node once. This parameter works in conjunction with the Maximum Hot Unreferenced Time parameter on the Cache Aging tab.

     NOTE: The maximum number of hot nodes must always be less than the maximum number of open files in NetWare. If you increase the maximum number of hot nodes from the default, make sure you also increase the maximum number of open files, up to a maximum of 100,000.
   - Maximum age ratio of the cache size to deleted files—This value determines how much space on the volume is used for caching and how many deleted files remain on the volume.

- Whether Read-ahead is enabled and whether the proxy should read ahead for embedded images or page links—Read-ahead signals the proxy to cache the data and examine the HTML page to locate all embedded objects, including images and links to other pages. When Read-ahead is enabled, the browser recognizes requests ahead of time.

4. Click OK > OK from the Novell BorderManager 3.7 Setup page.

Configuring Cache Location Parameters

You can specify a different location for the cache.

To configure cache location parameters:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. Select an HTTP or FTP proxy or acceleration service > click Caching.
3. From the Cache Location tab, specify the following:
   - A server pathname as a cache storage directory—The default is \ETC\PROXY\CACHE. The volume name is optional. If you do not specify a volume name, the default SYS: is used.

     NOTE: For improved stability and performance, we recommend that you set up a separate volume other than SYS: for the proxy cache directory, with compression and suballocation disabled, no long namespace support, and block size set to 16K.

   - (After clicking Add) A volume name to the Volume list—This specifies a different cache location. Be sure to include a colon at the end of the volume name.
   - The number of directories available per volume.
4. Click OK, then click OK again from the Novell BorderManager 3.7 Setup page.
5. Stop and restart the proxy server for the changes to take effect.

   The cache on the SYS: volume will not be moved to the new volume name.

Configuring Cachable Object Control Parameters

These parameters let you control which URL patterns are not cached, as well as what happens with objects that have a question mark (?) in the URL, /cgi in the pathname, or a no-cache reply header.

You can specify whether to cache URLs and objects with certain predefined patterns or access them directly without caching by the proxy server (be noncachable). When no caching is specified, the proxy server simply forwards the request from the server to the requesting client. Objects with a question mark (?) in the URL, /cgi in the pathname, or a no-cache reply header are not cached by default unless you specify otherwise.

To configure cachable object control parameters, complete the following steps:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. Select an HTTP or FTP proxy or acceleration service, then click Caching.
3. Click the Cachable Object Control tab.
4. Click Add to specify a list of URL patterns that will not be cached.

   4a Specify the following information:

   - Scheme—Specify a scheme type of HTTP, FTP, Gopher, or HTTPS.
   - Hostname—Specify any hostname or enter a specific hostname that must be matched. You can also check the check box to match any hostname that ends with the specified domain.
   - Port—Specify any port number or enter a specific port number.
   - Path—Specify any path or enter a specific pathname. You can also check the check box to match any path that begins with the specified name.
   - Extension—Specify any extension or enter a specific extension.

   4b Click OK.

   NOTE: If you specify a long list of patterns, the proxy server performance will be affected.

5 Specify the actions taken for the following objects:

- Objects with a question mark (?) in their URL
- Objects with /cgi in their paths
- Objects with a no-cache reply header

These objects are not cached by default. Specify to cache these objects if you are setting up an accelerator. Or you can specify to not cache and send replies to all browsers that request the information at the same time. This reduces how often the proxy must retrieve information from the origin Web server. Specify to not cache or split requests that have a cookie to avoid sending different replies to different users for the same request.

6 Click OK, then click OK again from the Novell BorderManager 3.7 Setup page.

Specifying Batch Downloading of Sites or URLs

Use batch downloading to keep the Novell BorderManager 3.7 cache of objects up to date for your users. You can schedule downloads of HTTP files from a Web site to the local cache. You can download a URL, multiple URLs up to a specified number of links, or an entire Web site. You can specify batch downloading for both forward and reverse HTTP proxies. Reverse proxy, however, will not download links that are external to a site.

Schedule downloads for low network usage times to conserve your network resources.

To specify batch downloading:

1 In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.

2 Select an HTTP proxy or acceleration service > click Caching.

3 Click the Scheduled Download tab > click Enable Scheduled Downloads and specify whether to perform the downloads sequentially.

4 Click Add from the Download List > specify the following download parameters:

- Enable this particular download.
- HTTP URL—A URL, the number of levels to download in that URL, and whether to follow links from that URL to other hosts.

- Maximum number of concurrent requests—The number of concurrent downloads to perform.
- Maximum number of objects to download—The number of objects that can be downloaded during a session.
- Maximum amount of data to download—The maximum size of data (in MB) that can be downloaded during a session.

5. Click the Frequency tab and specify the following parameters:
   - One time only—The date and time for a single download event.
   - Once a day at—The start time for a daily download.
   - Daily from—The interval and frequency for multiple daily downloads. Also, whether to perform the downloads only on certain days of the week.
6. Click OK > OK from the Novell BorderManager 3.7 Setup page.

Configuring Caching Hierarchies

If several proxy servers are serving the network, you can set up a hierarchy of proxy caches. If a proxy server does not find the requested page in its cache, it queries its peers and parents for the information. The queried peers and parents can then, in turn, query additional peers and parents for the requested information. The origin server is queried as the last resort. Note that the Novell Novell BorderManager 3.7 proxy server is compatible with other Internet Cache Protocol (ICP)-based proxy servers that exist on the Internet. You can set up these proxy servers as peers (neighbors), parents, or both.

You can configure a CERN hierarchy, a cache hierarchy (ICP), or both. If both are configured, the cache hierarchy takes precedence and the CERN hierarchy is used as a backup. CERN hierarchies have only parents, whereas cache hierarchies have both parents and peers.

To configure a hierarchical cache, complete the following steps:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. From the Application Proxy tab, select the HTTP Proxy service and click Details.
3. Click the Cache Hierarchy Server tab > check the Enable Cache Hierarchy Server check box.

4 Specify the following > click OK:

- Whether to enable source round-trip time—This parameter is used by the proxy to determine whether to send a request to the parent or to the origin server. The proxy uses the route that returns the shortest round-trip time.
- Whether to enable ICP ACL—This enables the cache hierarchy or ICP access control on the server.
- ICP listening port number—The UDP port on which the cache listens for queries from other caches.
- (After clicking Add) One or more multicast IP addresses for the multicast group list—Multicast addresses on which the cache hierarchy server receives multicast cache hierarchy queries.
- (After clicking Add) One or more hostnames or IP addresses for the access control list—The hostnames or IP addresses on this list are used to verify whether proxies can send a request. The clients on this list are allowed to send a cache hierarchy request.

5 Click the Cache Hierarchy Client tab > check the Enable Cache Hierarchy Client check box.

6 Specify the following:

- Must Only Forward Through Hierarchy—Deselect this option if you want the proxy server to retrieve the requested objects directly from the origin server.
- Cache Neighbor Timeout value—The number of seconds or minutes the proxy server waits for a response to a cache hierarchy request from another proxy server. Do not enter a value if you are configuring a CERN client.
- (After clicking Add) One or more neighbors for the Neighbors List, with the following information specified:

  Name of the nearest host server neighbor.

  Port number of the neighbor HTTP proxy.

  Port number of the neighbor cache hierarchy client—Do not enter a value if you are configuring a CERN client.

  Type of neighbor: peer, parent, or CERN—Select peer or parent if you are configuring a cache hierarchy client; select CERN if you are configuring a CERN client.

Priority for each neighbor, from 1 (lowest) to 10 (highest)—You can prioritize a set of parents or neighbors. A cache hierarchy client chooses the fastest responding hierarchy cache with the highest priority to service a request. CERN uses pure priority routing without querying.

Domains that the cache hierarchy client will serve—The default is null, or all neighbors receive all queries. CERN also supports domain routing.

- (After clicking Add) One or more unicast addresses or names and port numbers for the multicast responder list—This is a list of all acceptable neighbors (unicast) that can respond to a multicast query. This list lets the cache hierarchy client verify that the responses are from a valid neighbor. Do not enter a value if you are configuring a CERN client.

7 Click OK.

8 Click the Cache Hierarchy Routing tab > specify the following:

NOTE: Use cache hierarchy (ICP) routing when the parent cannot contact the origin server.

- Whether a URL's home site is used as a peer cache (not recommended).
- (After clicking Add) The local domain name for origin Web servers that are in close proximity—The proxy server prefers to query for a URL that it cannot resolve from these servers instead of from the cache hierarchy.
- (After clicking Add) One or more stop patterns for which the cache must query the origin Web server directly—Specify patterns for which the delays caused by hierarchical caching are unacceptable, for example, static pages that change frequently.

9 Click OK > OK from the Novell BorderManager 3.7 Setup page.

Specifying Transport Timeout Parameters

You can fine-tune various transport-related timeout parameters that are used by the Novell BorderManager 3.7 proxy server for connections. Do not change the defaults unless you are certain of the outcomes. You might need to change the parameters based on your network load.

To specify transport timeout parameters:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. Click Transport > enter values for any of the following TCP timeout parameters you want to set:
   - Establish Connection Timeout—The number of seconds or minutes the proxy server attempts to establish a connection before timing out because the other side has not responded. You might want to increase this value if you notice that the remote server is reachable (the ping succeeds) but the load is heavy.
   - Connection Keepalive Interval—The number of minutes or hours a connection is idle before the proxy server queries to check if the other server is still responding.
   - Data Read Timeout—The number of seconds or minutes the proxy server waits for expected data to begin arriving before it times out. You might want to increase this value if you notice that the browser receives incomplete data or the connection is disconnected in the middle of data transfer.
   - Idle Server Persistent Connection Timeout—The number of minutes or hours the proxy server keeps the TCP connection between the browser and the proxy server active, even if there is no data flow.
   - Idle Client Persistent Connection Timeout—The number of seconds or minutes the proxy server keeps the connection to the origin Web (or FTP or Gopher) server or another proxy server active, even if there is no data flow.
3. Click OK > OK from the Novell BorderManager 3.7 Setup page.

Specifying DNS Parameters

You can fine-tune some of the parameters used by the Domain Name System (DNS) Resolver of the Novell BorderManager 3.7 proxy server.

To change DNS parameters:

1. In NetWare Administrator, select the Novell BorderManager 3.7 Setup page for the server.
2. Click DNS > specify TCP or UDP (the default) as the transport protocol used by the DNS Resolver to query the DNS name server.

NOTE: If you select UDP and notice an increase in Bad Gateway error messages while the origin Web server is running, you might want to increase the DNS Resolver Timeout value.

3 For UDP, specify the DNS Resolver Timeout value.

This value indicates how long the proxy server waits before timing out after it sends a request to a DNS name server to resolve a domain name.

4 Enter values for the following parameters:

- Negative DNS Lookup—How long a failed DNS lookup domain name remains in the proxy server cache. If the proxy server cannot resolve a domain name, it stores that information in its cache for the specified amount of time. If the proxy server receives requests for that domain name within this period, it will send a Bad Gateway error message to the browser and will not resolve the domain name again.
- Maximum DNS Entry TTL—The maximum amount of time that DNS entries are cached before they expire. This is the maximum value, regardless of the value returned by the DNS name server.
- Minimum DNS Entry TTL—The minimum amount of time that DNS entries are cached before they expire. This is the minimum value, regardless of the value returned by the DNS name server.
- Maximum DNS Entry Threshold—The maximum number of DNS cache entries. When this number is reached, the proxy server deletes old entries to make room for newer ones. The default is 2,500.

5 Click OK > OK from the Novell BorderManager 3.7 Setup page.

12 Managing Proxy Services

The following sections explain the tasks you complete to manage Novell® BorderManager® 3.7 Proxy Services:

Setting Up HTTP Proxy Services Logging

You can set up proxy logging for the HTTP server or HTTP acceleration at any time.

Logging does not appreciably slow access to Internet services and locally cached information. You can, therefore, leave logging enabled for an extended period of time.

The following types of logging are available:

- Common format—Logs the following information: remote hostname, user's remote login name, authenticated username, date, request line from client, status, and length of data in bytes.
- Extended format—Logs the common format information plus the following: cached status, date, time, client IP address, URL method, and URL.

- Indexed format—Also referred to as the audit log. Logs the common and extended format information plus the following: when access was allowed or denied, the IP address that initiated an access attempt, the destination, the HTTP command used, and the result of the attempt (hit or miss).

In addition to setting up common format, extended format, or indexed format logging for an HTTP server or HTTP acceleration using this procedure, you can also set up indexed format logging for FTP, Mail, News, Generic, Domain Name System (DNS), and RealAudio* and Real Time Streaming Protocol (RTSP) proxy services from the individual proxy configuration dialogs. Refer to the individual proxy service configuration procedures in <<*name of book*>> for more information.

To set up HTTP proxy logging, complete the following steps:

1. In NetWare Administrator, double-click the Server object representing the Novell BorderManager 3.7 server and select Novell BorderManager 3.7 Setup.
2. Do one of the following:
   - For HTTP, from the Application Proxy tab select HTTP Proxy, then click Details.
   - For HTTP acceleration, from the Acceleration tab select HTTP Acceleration, then click Details. From the HTTP Acceleration list, double-click an accelerator or click Add.
3. Click the Logging tab, then select one or more of the logging formats (common, extended, or indexed).
4. If you selected common or extended logging, click the format name and specify the following parameters for each format:
   - Log File Directory—Directory to which the common or extended format log file is written.
   - Log Rollover—How often the file is overwritten (rolls over) by time (days or hours) or by size (KB or MB).
   - Old Log Files—Whether old log files are deleted because of their age or because of the number of old log files that are retained in the database.
   - Stop Services If Logging Fails—When enabled, stops all proxy services when the log file is full and log rollover is not specified.
5. Click OK, then click OK again from the Novell BorderManager 3.7 Setup page.

Monitoring Proxy Cache Realtime Activity

To display the Proxy Cache Monitor window and view proxy cache activity information, complete the following steps:

1. In NetWare Administrator, click the Server object representing the Novell BorderManager 3.7 server.
2. Select Novell BorderManager 3.7 from the Tools menu.
3. Click Proxy Cache > select Monitor Realtime Activity from the Object menu.

   The Proxy Cache Monitor window displays, providing the following information about proxy activity:

   - Sites Cached—Number of proxy sites currently in the cache.
   - Bytes Cached—Number of bytes cached on the proxy server.
   - Bytes Transferred—Number of bytes transferred to the proxy server.
   - Cache Misses—Number of times the cache was unable to serve a client request.
   - Cache Hits—Number of times the cache was able to serve a client request.
   - Hostname—Name of the Web server, including the name of the service (HTTP, for example) and the DNS domain name of the server.
   - Connections—Number of TCP connections required for a direct connection to the host server. Because Proxy Services has cached the site, this number represents the number of connections the proxy cache has saved its clients.
   - Bytes from Cache—Number of bytes transferred from the cache.
   - Bytes from Host—Number of bytes transferred from the host to the cache.
   - Bytes from Neighbors—Number of bytes transferred from the nearest neighbors to the cache.

Viewing User Statistics

To display user statistics in the proxy services audit log:

1. In NetWare Administrator, click the Server object representing the Novell BorderManager 3.7 server.
2. Select Novell BorderManager 3.7 from the Tools menu.
3. Click Proxy Cache > select View Audit Log from the Object menu.
4. Double-click the entry for that host in the first list box in the User Statistics window.

   A window with two list boxes displays: the Number of Users list box and the Hosts Accessed list box.

   NOTE: You can click the column heading of either list box to sort the entries in that column in ascending or descending order. The sorting order is reversed each time you click the column heading.

   The Number of Users list box provides the following information about Proxy Services activity:

   - Username—NDS® or Novell eDirectory™ name or IP address of the user. In the case of an IP address, the DNS domain name will be displayed if it exists in the local DNS list. The local DNS list is built automatically each time the WHO IS or DNS Hostname command is invoked using the right-click menu.
   - Hosts Accessed—Number of hosts accessed for the specified period of time.
   - Hit Volume—Total number of times data was found in the cache for all hosts accessed.
   - Miss Volume—Total number of times data was not found in the cache for all hosts accessed.
   - Hit Size—Total amount of data that was found in the cache for all hosts accessed.
   - Miss Size—Total amount of data that was not found in the cache for all hosts accessed.

   The Hosts Accessed list box provides the following information about Proxy Services activity:

- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS domain name or IP address of the accessed host.
- Hit Volume—Number of times data was found in the cache for this host.
- Miss Volume—Number of times data was not found in the cache for this host.
- Hit Size—Amount of data that was found in the cache for the accessed host.
- Miss Size—Amount of data that was not found in the cache (misses) for the accessed host.

5 To display additional types of user information, do one of the following:

5a To display all the connections made by a user, double-click a username in the Number of Users list box.

The User Log Entries window displays, providing the following information about Proxy Services activity:

- Entry Time—Time connection was established.
- Username—NDS or eDirectory name or IP address of user.
- Status—Whether the proxy server found the requested data in the cache (hit or miss).
- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS domain name or IP address of the accessed host.
- Data Length—Amount of data transferred from the cache or the original host.
- Command—Commands used: Get, Post, Passthrough, and so on.

5b To view usage trends graphs, click Usage Trends > select the category of usage trend data.

You can view the following categories of usage trend data by time of day in one-hour increments:

- Number of users—Bar graph showing the number of unique users allowed to connect to a host.
- Number of hosts accessed—Bar graph showing the number of hosts accessed.
- Amount of hit and miss data (volume)—Bar graph showing the number of cache hits and misses.
- Number of hosts accessed and amount of hit and miss data (volume)—Combination line and bar graph showing the number of hosts accessed, cache hits, and cache misses.

All graphs can be saved to disk, copied to the clipboard, or printed.

Viewing Host Statistics

To display the Host Statistics window and view host statistics:

1. In NetWare Administrator, click the Server object representing the Novell BorderManager 3.7 server.
2. Select Novell BorderManager 3.7 from the Tools menu.
3. Click Proxy Cache > select View Audit Log from the Object menu.

   The HTTP Proxy Host Statistic window displays, with two list boxes: the Number of Hosts list box and the User Accessed list box.

   NOTE: You can click the column heading of either list box to sort the entries in that column in ascending or descending order. The sorting order is reversed each time you click the column heading.

   The Number of Hosts list box provides the following information about Proxy Services activity:

   - Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
   - Hostname—DNS domain name or IP address of a host.
   - Users Accessed—Number of users who have requested information from the selected host.
   - Hit Volume—Number of times the requested information has been successfully delivered from the proxy server cache.

- Miss Volume—Number of times the requested information was not found in the cache.
- Hit Size—Total amount of data the proxy server has retrieved from its cache to satisfy user requests.
- Miss Size—Total amount of data the proxy server did not find in its cache.

The User Accessed list box provides the username—either the NDS or NDS or eDirectory name or IP address of the user, or the DNS domain name or the IP address.

4 To display additional types of host information, do one of the following:

4a To display the records for a set of connections from a specific user to a specific host, click Display Records and enter a time range for the records you want displayed.

For a U.S. English system, the dates are entered in the order of month, day, and year. The order is year, month, and day for a Japanese system; and day, month, and year for European language systems.

4b To see a list of connections for users who have accessed a particular host, double-click an entry in the Hosts Statistics window.

The Hosts Records Entries window displays, providing the following information about Proxy Services activity:

- Entry Time—Time connection was established.
- Username—NDS or NDS or eDirectory name or IP address of user.
- Status—Whether the proxy server found the requested data in the cache (hit or miss).
- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS domain name or IP address of the accessed host.
- Data Length—Amount of data transferred from the cache or the origin Web server.
- Command—Commands used: Get, Post, Passthrough, and so on.

Exporting Data

The proxy audit logs are generated by enabling indexed format logging for the HTTP, FTP, Mail, News, Generic, DNS, and RealAudio and RTSP proxy services. The proxy audit logs are stored in a Btrieve* file on the Novell BorderManager 3.7 server and are maintained by CSAUDIT.NLM. The proxy audit logs cannot be edited or manipulated from the server; however, the data can be exported for analysis. The format of the exported data is compatible with trend analysis software packages, such as WebTrends*. This section describes how to export proxy audit logs and lists the data exported for the HTTP, FTP, Mail, News, Generic, DNS, and RealAudio and RTSP proxy services.

NOTE: Logging information for Telnet Transparent proxy is provided in the Generic TCP audit log.

There are two ways to export the proxy audit logs from NetWare® Administrator:

- Export the data from the HTTP Proxy Hosts Statistics window.
- Select Export Logs from the Novell BorderManager 3.7 pull-down menu.

To export audit logs for all proxies other than HTTP, you must use the second method. If you use the second method, you can also combine the audit log files from other Novell BorderManager 3.7 services with the proxy audit log into a single ASCII file.

For additional information, refer to:

- "Exporting HTTP Audit Log Proxy Records" on page 168
- "Exporting Audit Logs for All Other Proxies" on page 169
- "Export File Subdirectories" on page 171

Exporting HTTP Audit Log Proxy Records

To export HTTP audit log proxy records from the HTTP Proxy Hosts Statistics window, complete the following steps:

1. In NetWare Administrator, click the Server object representing the Novell BorderManager 3.7 server.
2. Select Novell BorderManager 3.7 from the Tools menu.
3. Click Proxy Cache and select View Audit Log from the Object menu.

4. Click Display Records, enter the dates for the records you want to display, and click OK.
5. In the HTTP Proxy Hosts Statistics window, click Export Data and enter the path and filename or click Browse to select the destination of the export file.
6. Select one of the following sort formats under Information Output Selection > click OK:
   - Time entry (connection by connection)—(Default selection) Sorts records from earliest entry time to latest entry time.
   - Access by users—Sorts records in alphabetic order based on the user's NDS or eDirectory name.
   - Access by hosts—Sorts records in ascending order (for IP addresses) or alphabetic order (for DNS hostnames).
7. (Conditional) If the export filename already exists under the directory path selected, you are prompted to replace the file. Click Yes to overwrite the file or No to specify the destination as described in Step 5.

The record fields are written to disk with a tab as the delimiter. Each record ends with a carriage return and line feed. The exported HTTP proxy data has the following format:

- Entry Time—Time connection was established.
- Username—Typeless NDS or eDirectory name or IP address of user.
- Status—Whether the proxy server found the requested data in the cache (hit or miss).
- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS domain name or IP address of host accessed.
- Data Length—Amount of data transferred from the cache or the original host.

Exporting Audit Logs for All Other Proxies

Use the Export Logs selection from the Novell BorderManager 3.7 pull-down menu to export all the proxy audit logs. This procedure extracts the same data from the Btrieve database, but offers additional export options that cannot be

activated from the HTTP Proxy Hosts Statistics window. More important, the audit logs for all other proxies (FTP, Mail, News, Generic, DNS, and RealAudio and RTSP) can be accessed only this way.

To export an audit log for any proxy, complete the following steps:

1. In NetWare Administrator, click the Server object representing the Novell BorderManager 3.7 server.
2. Select Novell BorderManager 3.7 from the Tools menu.
3. From the Novell BorderManager 3.7 menu, select Export Logs.
4. Click Set Range > enter the date range.

   This is the range of dates comparable to the dates used to display records in the Access Control Users Statistics window. The default range is the current server date.
5. Click Browse to select the drive mapped to the destination for the export file.

   This is the path and filename for the export file. The default destination is A:\YYYYMMDD.LOG, where YYYY is the current year, MM is the current month, and DD is the current day. If you change the filename from the default format, the filename will not reflect the current server date. For example, if you change the filename format to MMDDYYYY.LOG, the next time you try to export logs on another day, the log filename will not have incremented to the current date.
6. (Optional) If the default filename is unacceptable, enter a new filename in the File field.
7. (Optional) If you want to combine the proxy audit log with audit logs from other Novell BorderManager 3.7 services, check the Combine Log Files check box.

   This feature allows log files from different Novell BorderManager 3.7 services to be combined into a single output file. When log files are combined, they are appended to one file, service by service.
8. Under Log Selection, check one or more boxes for the proxy type.

   If the Combine Log Files feature has been selected, check all the services you want combined into the export log file.
9. (Optional) If you checked Combine Log Files in Step 7 on page 170, under Log Selection, check all other Novell BorderManager 3.7 services audit log files to be combined with the access control log file.

10 Click OK.

The proxy audit logs are exported to an ASCII file. The record fields are written with a tab as the delimiter. Each record ends with a carriage return and line feed. The ASCII file format depends on which proxy audit log is exported.

Export File Subdirectories

If the Combine Log Files feature is *not* selected and you select one or more services under the Log Selection field, a separate export file is created for each service under a subdirectory of the export destination path.

The export subdirectories used are shown in the following table.

Log Type	Export Subdirectory
HTTP Proxy	HTTP
FTP Proxy	FTP
NNTP Proxy	NNTP
Mail Proxy	SMTP
RealAudio and RTSP Proxies	RAUDIO
DNS Proxy	DNS
Generic Proxy	GENERIC
Telnet Transparent Proxy	GENERIC
SOCKS Client	SOCKS
IPX Gateway (Novell IP Gateway)	IPXGW
VPN	VPN
ACL (access control)	ACL

For example, if you specified an export destination of VOL1:LOGS\19981019.LOG, did not select the Combine Log Files feature, and checked the boxes for HTTP proxy, the Novell IP Gateway, and access control, the following logs would result:

- VOL1:LOGS\HTTP\19981019.LOG

- VOL1:LOGS\IPXGW\19981019.LOG
- VOL1:LOGS\ACL\19981019.LOG

For more information, refer to:

- "Exported HTTP Proxy Data" on page 172
- "Exported FTP Proxy Data" on page 173
- "Exported NNTP Proxy Data" on page 173
- "Exported Mail Proxy Data" on page 174
- "Exported RealAudio and RTSP Proxy Data" on page 174
- "Exported DNS Proxy Data" on page 175
- "Exported Generic Proxy Data" on page 175
- "Exported SOCKS Client Data" on page 176

Exported HTTP Proxy Data

The exported HTTP proxy data has the following fields:

- Keyword—HTTP. If the Combine Log Files option was selected, the keyword is at the beginning of each HTTP proxy audit log line.
- Date.
- Time.
- Source—Typeless NDS or eDirectory name and context, such as mlira.pubs.novell, or IP address.
- Destination—DNS domain name or IP address.
- Bytes received.
- Command—Command used, such as Get, Head, Put, Post, Connect, or Delete.
- Status of command—Status of command used, such as Cache Hit, Cache Miss, IC Hit, ICP Miss, or Passthrough.
- Protocol—Protocol used, such as HTTP.

Exported FTP Proxy Data

The exported FTP proxy data has the following fields:

- Keyword—FTP. If the Combine Log Files option was selected, the keyword is at the beginning of each FTP proxy audit log line.
- Date.
- Time.
- Source—IP address.
- Destination—IP address.
- File length.
- Proxy username—Name used to log in to the FTP proxy.
- FTP username—Name used to log in to the FTP session.
- File—Full path of the file transferred using FTP.
- Cache status—Hit or Miss.
- Status of the FTP request, such as Success, ACL rejection, DNS domain name resolution failure, FTP protocol error, and Connect failure.

Exported NNTP Proxy Data

The exported Network News Transfer Protocol (NNTP) or News proxy data has the following fields:

- Keyword—NNTP. If the Combine Log Files option was selected, the keyword is at the beginning of each NNTP proxy audit log line.
- Date.
- Time.
- Source—IP address of client.
- Destination—IP address of news server.
- Status of the NNTP request, such as Success; Connect failure; ACL: news group denied; ACL: user/group posting not allowed; and NNTP protocol error # *number*, where error numbers are per RFC 977.

Exported Mail Proxy Data

The exported Mail proxy data has the following fields:

- Keyword—MAIL. If the Combine Log Files option was selected, the keyword is at the beginning of each Mail proxy audit log line.
- Date.
- Time.
- Source IP address.
- Destination IP address.
- User—Typeless NDS or eDirectory name or IP address of user.
- Protocol—Simple Mail Transfer Protocol (SMTP) or Post Office Protocol 3 (POP3).
- Status of the SMTP or POP3 request, such as Success, ACL check failure, Spool creation error, Failed connection, Spool size limitation, Protocol and transport failure, and Resource allocation failure.
- Command—SMTP or POP3 command used.
- Source domain—DNS domain name (for SMTP use only).
- Recipients—First 256 bytes of comma-separated list in user@domain format (for SMTP use only).
- Process step—Examples of process steps, include Incoming, Spool processing, and Forwarding (for SMTP use only).

Exported RealAudio and RTSP Proxy Data

The exported RealAudio and RTSP proxy data has the following fields:

- Keyword—RAUDIO. If the Combine Log Files option was selected, the keyword is at the beginning of each RealAudio proxy audit log line.
- Date.
- Time.
- Source—IP address.
- Destination—IP address.
- Destination port—Port number of the host.
- RealAudio mode—TCP or UDP.
- Status of the RealAudio request, such as Success, ACL failure, Connection error, and DNS domain name resolution error.

Exported DNS Proxy Data

The exported DNS proxy data has the following fields:

- Keyword—DNS. If the Combine Log Files option was selected, the keyword is at the beginning of each DNS proxy audit log line.
- Date.
- Time.
- Source—IP address.
- Destination—IP address of DNS name server.
- Resource record type—Decimal number indicating the record type that was transferred. Valid record types are 1 through 16, 252, and 253.
- Resource record class—Decimal number from 1 through 3. A 1 indicates Internet, a 2 indicates CHAOS, and a 3 indicates Hesiod.
- Resource record name—Text string of up to 64 characters.
- Transport—UDP or TCP.
- Cache status—Hit, Miss, or Tunnel.
- Status of the DNS request, such as Success, DNS packet data format error, Connect error, Name error, and Unable to resolve request.

Exported Generic Proxy Data

NOTE: Logging information for Telnet Transparent proxy is provided in the Generic TCP audit log.

The exported Generic proxy data has the following fields:

- Keyword—GENERIC. If the Combine Log Files option was selected, the keyword is at the beginning of each Generic proxy audit log line.
- Date.
- Time.
- Source—IP address.
- Destination—IP address.
- Destination port—Port number of the host.
- Transport—UDP or TCP.
- Cache status—Hit, Miss, or Tunnel.
- Status of the Generic request, such as Success, ACL failure, and Connection error.

Exported SOCKS Client Data

The exported SOCKS client data has the following fields:

- Keyword—SOCKS. If the Combine Log Files option was selected, the keyword is at the beginning of each Generic proxy audit log line.
- Date.
- Time.
- Source—IP address of client.
- Destination—IP address of destination host.
- Destination port—Port number of the host.
- Transport—TCP or UDP.
- Cache status—Hit, Miss, or Tunnel.
- Status of the SOCKS request, such as Success, DNS resolution failed, Server connect failed, Server authentication failed, Server ACL failed, and General server failure.

Blocking Virus Requests in HTTP Accelerator

For Web servers that are being accelerated by the Novell BorderManager 3.7 reverse proxy capability, Novell has added a new Virus Pattern Recognition feature that can help protect against such attacks.

The Virus Pattern Configuration Screen

The Virus Pattern Configuration screen is a console-based screen dedicated to virus pattern configuration and monitoring. This screen is reached by entering 23 on the Proxy Console screen. The information displayed is periodically refreshed for monitoring.

The following information describes each section of this screen, the parameters, their meaning, and, where applicable, their default values and configuration methods.

Configuration

The items in the Configuration section of the screen are as follows:

Number of Patterns—The current number of patterns in the database. This value is not configurable. It starts at 0 and is incremented each time a new pattern is successfully added to the database.

Pattern Size—The size of the pattern, in bytes. The default setting is 16. This is a global setting that is used for all patterns, so modify it with care.

Pattern Start Offset—Indicates where the virus pattern starts, as a byte offset from the actual beginning of the request. The default setting is 1. This is a global setting that is used for all patterns, so modify it with care.

Refresh Interval—Specifies the time interval when the incoming request distribution is studied for Auto Update heuristic purposes. The default value is 10 seconds. The value can be modified using the virus -r *interval* command.

Hit Threshold—The threshold upon which the automatic detection of new virus patterns is based. The default value is 250. The value can be modified using the virus -t *threshold* command.

Virus Auto Update—Indicates whether or not the Auto Update feature is enabled. The default value is 0 (disabled). The Auto Update feature can be enabled using the virus -e 1 command.

Monitoring

The items in the Monitoring section of the screen are as follows:

Virus Requests—The number of incoming requests that have matched a virus pattern. This value is not configurable. It starts at 0 and is incremented each time a pattern match is detected.

Non Virus Requests—The number of incoming requests that did not match a virus pattern. This value is not configurable. It starts at 0 and is incremented each time a pattern match fails.

Recommend Threshold—A recommended value for the Auto Update threshold parameter. After the server has been up for a while, this gives a good lower limit for the hit threshold.

Maximum Non Virus Hit Rates—The maximum or peak number of incoming humble (non-virus) requests received in one time interval.

Average Virus Hit Rates—The average number of incoming virus requests received over all the time intervals crossed so far.

Average Non Virus Hit Rates—The average number of incoming humble (non-virus) requests. The threshold setting must be greater than this value.

Virus Source IP Address

This section displays the last ten IP addresses of sources that sent virus requests.

Last Predicted Request.

This section displays the last request that was made a suspect.

Choosing a Proper Threshold

The configuration section of the Virus Pattern Configuration screen contains a Hit Threshold parameter that gives the current threshold value.

The following rules of thumb can be used for arriving at an appropriate new threshold value:

- The Threshold value must be always greater than the Ave Non Virus Hit Rate.
- The Recommend Threshold gives a possible threshold value. However, you can use this value as a new threshold only if it is considerably higher than the Ave Non Virus Hit Rate value.

You can change the threshold value by executing the following command at the system console:

```
virus -t threshold
```

The threshold and refresh time interval settings are tightly coupled. If you raise the threshold, you need to increase the time interval accordingly, and vice versa. You can change the refresh time interval value by executing the following command at the system console:

```
virus -r time interval
```

Miscellaneous Tasks

This section outlines how to perform various tasks involved in the day-to-day operation of the Virus Pattern Recognition feature.

Specifying a Maximum Number of Patterns

Each pattern added to the database takes up 64 bytes of RAM. For memory and performance reasons, you may want to set a limit on the number of patterns allowed in the virus pattern database. To do this, enter the following command at the system console:

virus -m *max virus patterns*

where *maximum virus patterns* is an integer specifying the maximum number of patterns allowed in the database. This value should be set below 256.

Clearing Existing Virus Patterns

To clear all existing patterns from the database, type the following command at the system console:

virus -c

Viewing Online Help

To display online help and usage information, type the following command at the system console:

virus -? or virus -h

Verifying the Blocking of Virus Requests

To verify whether the Virus Pattern Recognition feature is working, check the PROXY.LOG file (located in SYS:\ETC\PROXY) for drop.

The following is an example of a dropped request:

```
63.146.66.41 - - [09/Aug/2001:04:47:27 -0600] "(bad request
  line)

GET%00/default.ida?XXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX (truncated)" 400 2248
```

Disabling the Virus Pattern Recognition Feature

To disable the Virus Pattern Recognition feature, change the value of the ScanVirusPatterns parameter in PROXY.CFG to 0 and restart the Proxy Server.

```
[Extra Configuration]

ScanVirusPatterns=0
```

VIII Virtual Private Networks

The following sections of the *Novell® BorderManager® 3.7 Administration* guide provides the information you need to use a Virtual Private Network (VPN).

- Chapter 13, "Advanced Configuration of Virtual Private Networks," on page 183 describes the procedures you need to set up and configure various VPN features and parameters.
- Chapter 14, "Managing Virtual Private Networks," on page 243 describes how to set up VPN logging and describes the information found in the VPN logs.

See the Setting Up Virtual Private Networks section in the *Novell BorderManager 3.7 Installation Guide* for information on how to set up a Virtual Private Network.

13 Advanced Configuration of Virtual Private Networks

This section explains the advanced configuration tasks for the Virtual Private Network (VPN) component of the Novell® BorderManager® 3.7 software.

The section contains the following information:

Merging NDS or eDirectory across a VPN

The procedure for merging NDS® or Novell eDirectory™ across a VPN is the same as for any other network. Refer to the NetWare® online documentation for detailed instructions for merging NDS or eDirectory across a LAN or WAN.

Performance Tuning across VPNs

Because VPN performance is mostly determined by the routers on the Internet, you are limited to tuning each VPN server's Internet Service Provider (ISP) connection to increase your VPN's performance. Depending on which path is used through the Internet, increasing the bandwidth of your ISP connections might or might not improve the performance of your VPN. However, if a slow link exists, try the following adjustments:

- Tune the Internetwork Packet Exchange™ (IPX™) timeouts for the client and for the server using NIASCFG.
- Increase the IPX application timeouts.
- Increase the TCP/IP application timeouts.
- Turn off UDP checksumming.
- Use the NetWare Link Services Protocol™ (NLSP™) software instead of the Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) for IPX.
- Increase the number of packet receive buffers as allowed by the amount of available memory.

Setting up Site-to-Site VPNs

This section explains the tasks you complete to configure a site-to-site VPN. This section contains procedures for the following:

- "General Configuration Using VPNCFG" on page 184
- "General Configuration Tasks Using NetWare Administrator" on page 187
- "Setting Up Implementation-Specific Site-to-Site Configurations" on page 196

General Configuration Using VPNCFG

This section explains the advanced configuration task for a site-to-site VPN using the VPNCFG utility. Use VPNCFG to regenerate the encryption information.

Regenerating the Encryption Information

To maintain security, we recommend that you regenerate the encryption information every six months after the initial configuration of the VPN. To regenerate the encryption information:

1. At the master server console prompt, enter

   `LOAD VPNCFG`

2. Select Master Server Configuration.

3 Generate the master server encryption information.

3a Select Generate Encryption Information.

3b Enter up to 255 characters for the random seed.

There is no need to record this value. The software uses this value to help randomize the master server RSA public and private keys and the master server Diffie-Hellman public and private values that it generates.

4 Copy the master encryption information file (MINFO.VPN) to diskette or save it to a local hard disk.

4a Select Copy Encryption Information.

4b Enter the path in which you want to save the master encryption information file.

5 Give the MINFO.VPN file to the network administrator of each slave server you want to add to the VPN.

You can either send the diskette containing the file by surface mail or send the file as an e-mail attachment. There is no danger of compromising security if the file is intercepted because it cannot be interpreted without the slave server's RSA public and private keys and Diffie-Hellman public and private values.

6 Exit VPNCFG.

7 Load VPNCFG on the slave server.

8 Select Slave Server Configuration.

9 Generate the slave server encryption information.

9a Select Generate Encryption Information.

9b Enter the location of the master encryption information file (MINFO.VPN).

9c Contact the master server administrator and verify that you have the same digest values.

Having the same digest values ensures the authenticity of the MINFO.VPN file.

IMPORTANT: If the message digest values do not match, the encrypted tunnel between the slave and master servers cannot be created. In this case, the master server administrator must provide a new MINFO.VPN file.

9d Ask the master server administrator to select Authenticate Encryption Information to authenticate the MINFO.VPN file.

To authenticate this file, the administrator must load VPNCFG and select the following menu path:

Master Server Configuration > Authenticate Encryption Information

9e If the MINFO.VPN file is valid, enter up to 255 characters for the random seed.

There is no need to record this value. The software uses this value to help randomize the Diffie-Hellman public and private values that it generates for the slave server.

10 Copy the slave encryption information file (SINFO.VPN) to diskette or save it to a local hard disk.

10a Select Copy Encryption Information.

10b Enter the path or name of the file in which you want to save the slave encryption information file. The default is A:\SINFO.VPN.

HINT: Rename your SINFO.VPN file to a name such as SINFO_S1.VPN. This enables the master server administrator to collect all slave encryption information files in a single directory without overwriting them. You can also use a server or location name when renaming the SINFO.VPN file.

11 Give your slave encryption information file to the master server administrator.

You can either send the diskette containing the file by surface mail, or send the file as an e-mail attachment. There is no danger of compromising security if the file is intercepted because it contains only public information. Any alteration of the file can be detected by verifying the message digest when the master server adds the slave server to the VPN.

12 Press *Esc* until you exit VPNCFG.

13 Use NetWare® Administrator to remove all slave servers and add them back again.

For more information, refer to the *Novell BorderManager 3.7 Installation Guide* .

General Configuration Tasks Using NetWare Administrator

This section explains the advanced configuration tasks for a site-to-site VPN using the NetWare Administrator utility. Use NetWare Administrator to complete the following tasks:

Selecting Network Protocols on Your VPN

With Novell BorderManager 3.7, you can select the network protocols—IP and IPX—that are encrypted and sent over the VPN tunnel.

This capability offers the following advantages:

- You can temporarily suspend IPX or IP traffic without bringing down the VPN.
- You can choose to run only one protocol over the VPN, even if your intranet uses both. This capability also conserves server resources and network bandwidth on intranets that use only one network protocol.

Both protocols are tunneled by default.

IMPORTANT: Disabling both IPX and IP effectively disables the VPN without bringing it down.

To enable or disable protocol tunneling on your VPN, complete the following steps:

1. In NetWare Administrator, double-click the VPN master server and select the Novell BorderManager 3.7 Setup page.

2. Click the VPN tab.
3. Double-click Master Site-to-Site under Enable Service.
4. Click Control Options.
5. Check the check box for the network protocol you want to enable.

   A checked box indicates that the protocol will be encrypted and sent over the VPN tunnel.
6. Click OK until you exit the NetWare Administrator utility.

   Exiting the NetWare Administrator utility triggers a VPN synchronization. If you plan to perform additional VPN configuration tasks, you can trigger a synchronization immediately by clicking Status, then clicking Synchronize All.

Specifying Networks Protected by a Site-to-Site VPN

For each VPN server, you can specify the addresses of one or more local IP networks or hosts that can exchange encrypted data across the VPN. This is equivalent to setting up static routes for encrypted data. When you synchronize the VPN, the static routes are automatically added to the routing tables of the other VPN servers, which use the routes to forward encrypted data to the server.

The alternative to using static routes to determine which networks can exchange encrypted data is using dynamic routing across the VPN. For a description of the advantages and disadvantages of using static routes, refer to the *Novell BorderManager 3.7 Overview and Planning Guide*.

IMPORTANT: You must set up all static routes for protected networks on VPN servers using the NetWare Administrator utility, not the NIASCFG utility. Any static routes you set up from NIASCFG with a tunnel address as the next-hop router are removed from the VPN server routing tables when a VPN resynchronization occurs.

To specify an address of a local private network or host that you want to be protected by a particular server, complete the following steps:

1. In NetWare Administrator, double-click the VPN master server and select the Novell BorderManager 3.7 Setup page.
2. Click the VPN tab.
3. Double-click Master Site-to-Site under Enable Service.

4. In the VPN Members list box, double-click the VPN server you want to set up.
5. To use RIP to dynamically determine which networks are protected by this server, select Enable IP RIP.
6. To statically configure the list of networks protected by this VPN server, complete the following substeps:
   - **6a** Click Add.
   - **6b** Select Network or Host.
   - **6c** Enter the IP network address and subnet mask of the network or host that you want to be protected by this server.
   - **6d** Click OK.
   - **6e** Specify any additional protected networks, then click OK to return to the main VPN page.

   NOTE: At this point, your master server recognizes the slave server, but the slave server has not been updated yet with the VPN configuration information. The slave server must be updated in order for the VPN to come up. Make sure that the master and slave servers can communicate using IP before synchronizing the servers.
7. To update all VPN members with the entire VPN configuration, complete the following substeps:
   - **7a** From the main VPN page, click Status.
   - **7b** Click Synchronize All to update all VPN members with the current configuration.

     This might take some time, depending on the number of members that must be updated. When the process is complete, all members should have a status of Up-to-Date.
   - **7c** If any VPN server remains with a status of Being configured, select that VPN server, then check the audit log for configuration errors.
   - **7d** Click OK.

Selecting Data Encryption and Data Authentication Methods

The preferred data encryption and authentication methods are used during negotiation between the two sides of a VPN connection to determine the actual methods that are used for the connection. The preferred data encryption and authentication methods for the server apply to both site-to-site and client-to-site connections.

To change the preferred values used to negotiate the methods of data encryption and data authentication, complete the following steps:

1. In NetWare Administrator, double-click the VPN master server and select the Novell BorderManager 3.7 Setup page.
2. Click the VPN tab.
3. Double-click Master Site-to-Site under Enable Service.
4. In the VPN Members list box, double-click the VPN server you want to set up.
5. Select an option for the Preferred Encryption Method parameter.
6. Select an option for the Preferred Authentication Method parameter.
7. Specify a value for the Data Encryption Key Change Interval parameter.
8. Click OK until you exit the NetWare Administrator utility.

   Exiting the NetWare Administrator utility triggers a VPN synchronization. If you plan to perform additional VPN configuration tasks, you can trigger a synchronization immediately by clicking Status, then clicking Synchronize All.

Selecting Your VPN Topology

With Novell BorderManager 3.7, you can select from one of the following topologies to use with your VPN:

- Mesh (default)

  In this topology, all VPN members have connections to each other.

- Star

  In this topology, all VPN members have connections only to the master server.

- Ring

  In this topology, each VPN member has connections to two of its neighbors.

To select the topology for your VPN, complete the following steps:

1. In NetWare Administrator, double-click the VPN master server and select the Novell BorderManager 3.7 Setup page.
2. Click the VPN tab.

3. Double-click Master Site-to-Site under Enable Service.
4. Click Control Options.
5. Check the check box for the type of topology you want to use.
6. Click OK until you exit the NetWare Administrator utility.

   Exiting the NetWare Administrator utility triggers a VPN synchronization. If you plan to perform additional VPN configuration tasks, you can trigger a synchronization immediately by clicking Status, then clicking Synchronize All.

Selecting Whether the Connection Is Initiated from One Side or Both Sides

With Novell BorderManager 3.7, you can specify whether a connection between two VPN servers is always initiated by only one server or is initiated by either server.

Selecting One Side indicates that a connection made between two servers is always initiated by one server. This setting typically results in faster calls. Selecting Both Sides allows either server to initiate the connection. However, if two servers initiate a connection to each other simultaneously, the connection takes longer to be established. In this case, the longer connection time is caused by the servers negotiating which one initiated the connection first.

To specify whether a connection between two VPN servers can be initiated by only one server or either server, complete the following steps:

1. In NetWare Administrator, double-click the VPN master server and select the Novell BorderManager 3.7 Setup page.
2. Click the VPN tab.
3. Double-click Master Site-to-Site under Enable Service.
4. Click Control Options.
5. Check the check box for One Side or for Both Sides.
6. Click OK until you exit the NetWare Administrator utility.

   Exiting the NetWare Administrator utility triggers a VPN synchronization. If you plan to perform additional VPN configuration tasks, you can trigger a synchronization immediately by clicking Status, then clicking Synchronize All.

Adjusting the VPN Server Response Timeout

The response timeout determines how long an individual VPN server waits for a response from another server before terminating the connection. Increasing the response timeout can help to maintain connectivity between servers if the link between them is slow.

To adjust the response timeout for a VPN server, complete the following steps:

1. In NetWare Administrator, double-click the VPN master server and select the Novell BorderManager 3.7 Setup page.
2. Click the VPN tab.
3. Double-click Master Site-to-Site under Enable Service.
4. In the VPN Members list box, double-click the VPN server you want to configure.
5. Enter the response timeout.
6. Click OK until you exit the NetWare Administrator utility.

   Exiting the NetWare Administrator utility triggers a VPN synchronization. If you plan to perform additional VPN configuration tasks, you can trigger a synchronization immediately by clicking Status, then clicking Synchronize All.

Tuning Master-Slave Server Synchronization

On a VPN, the master server communicates with the slave servers to ensure that they maintain the same information about the VPN topology and use the current public encryption keys. For this purpose, you can customize the Update Interval, Connect Timeout, and Response Timeout parameters. Tuning these parameters represents a balance between quick convergence of the VPN and the traffic and CPU overhead.

If your servers and ISP connections are working properly, the default timeout values are adequate to enable your VPN to synchronize in the shortest possible amount of time.

To tune master-slave server synchronization, complete the following steps:

1. In NetWare Administrator, double-click the VPN master server and select the Novell BorderManager 3.7 Setup page.
2. Click the VPN tab.
3. Double-click Master Site-to-Site under Enable Service.

4 Click Control Options.

5 Enter values for the Update Interval, Response Timeout, and Connect Timeout parameters.

Values for the Update Interval and Response Timeout parameters range from 0 to 5 hours and 59 minutes. The Connect Timeout parameter value ranges from 0 to 20 hours and 59 minutes.

6 Click OK until you exit the NetWare Administrator utility.

Exiting the NetWare Administrator utility triggers a VPN synchronization. If you plan to perform additional VPN configuration tasks, you can trigger a synchronization immediately by clicking Status, then clicking Synchronize All.

Removing a Slave Server from a VPN

When you remove a slave server from a VPN, the master server distributes an updated VPN members list to the remaining slave servers. The master server also sends a request to the removed server to detach itself from the VPN.

NOTE: You cannot remove the master server from a VPN.

To remove a slave server from a VPN, complete the following steps:

1 Verify that the slave server you want to remove does not have INETCFG loaded.

If INETCFG is loaded when the VPN slave server is removed, the remaining slave servers will not synchronize properly.

2 In NetWare Administrator, double-click the VPN master server and select the Novell BorderManager 3.7 Setup page.

3 Click the VPN tab.

4 Double-click Master Site-to-Site under Enable Service.

5 In the VPN Members list box, click the slave server you want to remove.

6 Click Delete in the VPN Members list box.

7 Click Status.

8 Click Synchronize All, then click OK.

9 After the VPN has synchronized, go to the slave server and remove the VPN configuration from the slave, as follows:

9a Load VPNCFG.

9b Select Remove VPN Server Configuration.

Adding a Server that Is a Member of Another VPN

A VPN server that is a member of another VPN can also be included in your VPN using the multiple tunnel support provided by Novell BorderManager 3.7.

IMPORTANT: The tunnel connection to the third-party VPN server is an IP-only connection. Only the local VPN server that is associated with the third-party VPN server can exchange encrypted information with the third-party VPN server.

For third-party servers to function, your local VPN must use a mesh topology. If the third-party VPN is running Novell BorderManager 3.7 VPN software, it must also use a mesh topology.

When adding a third-party server to your VPN, the administrators of both VPN servers must configure the same authentication or encryption algorithms or the encrypted tunnel will not be established. Your local VPN server will not negotiate authentication or encryption algorithms with a third-party slave server, even if the third-party server is also running Novell BorderManager 3.7 VPN software.

Servers that are members of two VPNs are managed differently than servers that are members of just one VPN. Refer to the Virtual Private Network online documentation for more information.

Adding a Third-Party VPN Server that Is Not Running Novell BorderManager Software

If the third-party VPN is running another vendor's VPN software, you must create a new SINFO.VPN file and complete the procedure for adding a server to a VPN, as described in Novell BorderManager 3.7 Installation Guide a new SINFO.VPN file with the following fields:

- Major version number—Should always be set to 1.
- Minor version number—Should always be set to 5.
- Server name—Arbitrary name assigned to the third-party server. You can pick any name for convenience.
- Master or slave ID—Should always be set to 1.
- Public IP address—Public IP address of the third-party server.
- Public IP address mask—Public IP address mask of the third-party server.
- Private IP address—Not used. Should always be set to 0.0.0.0.
- Private IP address mask—Not used. Should always be set to 0.0.0.0.

- Tunnel IP address—IP address of the VPN tunnel that you want to assign to the third-party server. The address must belong to the same IP network as the local VPN's tunnel address.
- Tunnel mask—Should be set to match the mask of your local VPN tunnel.
- Public value length—Length of the third-party server's Diffie-Hellman public value, in bytes.
- Public value in BER—Third-party server's Diffie-Hellman public value, in BER format. 1024-bit values are supported.
- Security capabilities—Decimal equivalent of a 32-bit binary integer you must compute using the following bit values:
  - Bit 0—If you are using the export version of the VPN software, set this bit to 1. Otherwise set it to 0.
  - Bit 1—If Keyed_MD5 is supported, set this bit to 1. Otherwise, set it to 0.
  - Bit 2—If Keyed_SHA1 is supported, set this bit to 1. Otherwise, set it to 0.
  - Bit 3—If HMAC_MD5 is supported, set this bit to 1. Otherwise, set it to 0.
  - Bit 4—If HAC_SHA1 is supported, set this bit to 1. Otherwise, set it to 0.
  - Bit 5 to bit 15—Set these bits to 0.
  - Bit 16—If DES-CBC is supported, set this bit to 1. Otherwise, set it to 0.
  - Bit 17—If 3DES-CBC is supported, set this bit to 1. Otherwise, set it to 0.
  - Bit 18—If RC5-CBC is supported, set this bit to 1. Otherwise, set it to 0.
  - Bit 19—If RC2-CBC is supported, set this bit to 1. Otherwise, set it to 0.
  - Bit 20 to bit 29—Set these bits to 0.
  - Bit 30—Set this bit to 1.
- Flag to indicate third-party—Should always be set to 1 to indicate that the server is a member of a third-party VPN.

- Local VPN member—Name of your local VPN server that is directly connected to the third-party VPNs server. This is the only local server to which the third-party VPN server can be connected.

Adding a Third-Party VPN Server that Is Running Novell BorderManager Software

If the third-party VPN is running Novell BorderManager, you must generate the third-party's encryption information, as described in the Install and Setupguide. Edit the third-party's SINFO.VPN file, and complete the procedure for adding a server to a VPN, as described in the guide. To edit the third-party's SINFO.VPN file, obtain the file from the other VPN's administrator and change the values of only the following fields:

- Server name—Arbitrary name assigned to the third-party server. You can pick any name for convenience.
- Tunnel IP address—IP address of the VPN tunnel that you want to assign to the third-party server. The address must belong to the same IP network as the local VPN's tunnel address.

  This field must be changed from the third-party server's VPN tunnel address to the VPN tunnel address of your local server.
- Tunnel mask—Should be set to match the mask of your local VPN tunnel.

  This field must be changed from the third-party server's VPN tunnel mask to the VPN tunnel mask of your local server.
- Flag to indicate third-party—Should always be set to 1 to indicate that the server is a member of a third-party VPN.
- Local VPN member—Name of your local VPN server that is directly connected to the third-party VPNs server. This is the only local server to which the third-party VPN server can be connected.

  This field is not present in the SINFO.VPN file that you receive from the third-party VPN. Therefore, you must add the field after the Flag to indicate third-party field.

IMPORTANT: Do not change the Security Capabilities field in the server's SINFO.VPN file.

Setting Up Implementation-Specific Site-to-Site Configurations

This section describes implementation-specific examples for site-to-site VPNs. Some of these examples require that you complete the preparatory

steps provided in Novell BorderManager 3.7 Installation and Setup guide. For in-depth information to help you plan your VPN configuration, refer to Novell BorderManager 3.7 Overview and Planning Guide.

Site-to-site VPNs can be implemented in the following ways:

- To exchange secure information over the Internet

  In this case, VPN servers at two or more remote sites use the Internet to exchange encrypted confidential information. The VPN servers can connect directly to the Internet, or connect through an existing firewall or high-speed router. Examples of both are provided in this section. In these examples, it is assumed that you selected the Setup Novell BorderManager 3.7 for Secure Access to Public Interface option during Novell BorderManager 3.7 installation.

- To exchange secure information within a private network

  In this case, a VPN is set up on a corporate intranet or private network to exchange encrypted information. An example of this case is provided in this section.

This section contains the following topics:

Using the VPN Server as a Border Server

This section discusses the following two possible scenarios for using the VPN server as a border server:

- VPN servers using the same network for both public and private addresses
- VPN servers using different networks for both public and private addresses

VPN Servers Using the Same Network for Both Public and Private Addresses

In this example, assume the company has offices at two remote sites: San Jose and Athens. The Finance and corporate offices are in San Jose, and the Accounting office is in Athens. At each office, the public and private addresses are on a different subnet of the same Class B IP network address.

Both offices must share data without allowing other users on networks that are not protected by the VPN servers to access the data from within the company or through the Internet.

At both sites, the VPN server is connected directly to the Internet and is being used as the border server. The following procedure shows you how to connect the two remote sites in this example by setting up the two border servers as VPN servers and using an encrypted tunnel to send data between the sites.

To connect two remote Internet sites using a VPN:

1. Choose a master server for your VPN.

   In this example, the San Jose site is selected because the corporate office has the Corporate Information Services staff, who are better equipped to manage the VPN.

2. Contact an ISP and arrange for Internet connectivity. Write down the public IP address and subnet mask that the ISP provides you.

   Repeat this step for each site that will be a part of the VPN.

   In this example, the public IP address and subnet mask for the VPN master server in San Jose are 135.27.180.1 and FF.FF.FC.0, respectively. The public IP address and subnet mask for the VPN slave server in Athens are 135.145.188.25 and FF.FF.FC.0, respectively.

3. Choose an IP address and subnet to use for your VPN tunnel interface.

   Because this address will never be sent over the Internet, it can be any unregistered address, for example, 10.0.0.1 and FF.0.0.0 for the master server, and 10.0.0.2 and FF.0.0.0 for the slave server.

   The master server and all slave servers must use IP addresses on the same network or subnet for the VPN tunnel interfaces.

4. Install the NetWare and Novell BorderManager 3.7 software on your master server.

5. Use NIASCFG to configure the protocols and routing on your master server as follows:

   - Configure a WAN interface to connect to your ISP.
   - Create a WAN call configuration to connect to your ISP.
   - Enable TCP/IP.

- Bind TCP/IP to the WAN interface that connects your VPN server to your ISP (135.27.180.1). This interface must have a registered IP address.
- Reinitialize the system to make these changes take effect.

6 Establish a connection to your ISP and verify that the master server can communicate with the ISP router.

Do this before you add the VPN. Before testing the connection, you must verify that the Novell BorderManager 3.7 filters are configured to allow Internet Control Message Protocol (ICMP) packets through. After testing, the filters should be returned to their previous configuration. If you configured your call as Permanent-Automatic, the server should connect to your ISP immediately after you reinitialize the system. If you configured your call as any other type, you might need to initiate the call yourself by loading CALLMGR at the console and initiating an IP WAN call to your ISP. After the call is connected, ping the ISP router by entering **LOAD PING** at the console prompt and entering the IP address of the router (provided by the ISP). If you can ping the ISP router, you are connected to the ISP and should be able to reach any location on the Internet, including your other sites after they are connected.

7 Use VPNCFG to configure your VPN master server. Make sure you do the following:

- Specify the public IP address and subnet mask. In this example, specify 135.27.180.1 for the public IP address, and FF.FF.FC.0 for the subnet mask.
- Specify the VPN tunnel IP address and subnet mask. In this example, specify 10.0.0.1 for the VPN tunnel IP address, and FF.0.0.0 for the subnet mask.

  NOTE: VPNCFG automatically adds some filters to prevent the IP address of the VPN tunnel from being sent through the public interface, and to prevent the public IP address from being sent through the tunnel interface.
- Generate encryption information for the VPN master server.
- Copy the encryption information to a diskette.

Refer to Novell BorderManager 3.7 Install and Setup guide or the online help for the procedure to set up the master server.

8 If you did not select the Setup Novell BorderManager 3.7 for Secure Access to the Public Interface option during installation, load BRDCFG and select this option.

9. Send the MINFO.VPN file with the master encryption information to the administrator configuring the VPN slave server.

10. Repeat Step 4 on page 198, Step 5 on page 198, Step 6 on page 199, and Step 8 on page 199 for the slave server.

11. At the VPN slave server, use VPNCFG to configure the VPN slave server. Make sure you do the following:

    - Specify the public IP address and subnet mask. In this example, specify 135.145.188.25 for the public IP address, and FF.FF.FC.0 for the subnet mask.
    - Specify the VPN tunnel IP address and subnet mask. In this example, specify 10.0.0.2 for the VPN tunnel IP address, and FF.0.0.0 for the subnet mask.
    - Generate encryption information for the VPN slave server using the master encryption information file (MINFO.VPN). Call the master server administrator and verify that the digest values match.
    - Copy the slave encryption information to a file.

    Refer to Novell BorderManager 3.7 Install and Setup or the online help for the procedure to set up the slave server.

12. Send the SINFO.VPN file with the slave encryption information back to the administrator configuring the VPN master server.

13. At the administrative workstation, install the Novell BorderManager 3.7 guide snap-in for the NetWare Administrator utility if it has not already been installed.

    The installation program for this utility (SETUP.EXE) is in the \PUBLIC\BRDMGR\SNAPINS directory on the SYS: volume of your server after Novell BorderManager 3.7 has been installed.

    NOTE: Perform this step from a client that is authenticated to the NDS or eDirectory tree in which the VPN master server resides. The machine must be logged in with Supervisor rights to the VPN master server. If this is the first VPN server or border server on this tree, then Supervisor rights to the root directory are required in order to extend the NDS or eDirectory schema.

14. In NetWare Administrator, double-click the VPN master server and select the Novell BorderManager 3.7 Setup page.

15. Click the VPN tab.

16. Double-click Master Site-to-Site under Enable Service.

Your master server should be listed in the VPN Members list. For example, if you named the master server Corporate, you should see Corporate displayed as a VPN member with an IP address of 135.27.180.1, as configured in Step 7 on page 199.

17 Manually configure a list of networks protected by this VPN master server.

In this example, a list of protected networks must be configured for all VPN servers even if Enable IP RIP is selected. Because the public and private networks are subnets of the same network, the RIP packets that pass through the VPN tunnel interface are blocked by the default VPN filters. Because the routes to the protected networks cannot be learned using RIP, a list of protected networks must be configured manually.

In this example, you can specify the 135.27.188.0 network as a protected network by completing the following substeps:

17a Double-click the slave server to view details for that server.

17b Click Add.

17c Select Network.

17d Enter 135.127.188.0 for the IP network address.

17e Enter FF.FF.FC.0 for the subnet mask.

17f Click OK.

17g Specify any additional protected networks, then click OK to return to the main VPN page.

18 Click Add to add the slave server to the VPN Members list.

19 Specify the name and pathname for the slave encryption information file (SINFO.VPN).

20 Ask the administrator of the VPN slave server to use VPNCFG to authenticate the encryption information and verify that the message digest values match. Click Yes if the values match.

To authenticate the encryption information using VPNCFG, select Authenticate Encryption Information.

21 Click Yes to manually configure a list of networks protected by this VPN slave server.

In this example, a list of protected networks must be configured for all VPN servers even if Enable IP RIP is selected. Because the public and

private networks are subnets of the same network, the RIP packets that pass through the VPN tunnel interface are blocked by the default VPN filters. Because the routes to the protected networks cannot be learned using RIP, a list of protected networks must be configured manually.

In this example, you can specify the 135.145.180.0 network as a protected network by completing the following substeps:

21a Double-click the slave server to view details for that server.

21b Click Add.

21c Select Network.

21d Enter 135.145.180.0 for the IP network address.

21e Enter FF.FF.FC.0 for the subnet mask.

21f Click OK.

21g Specify additional protected networks and modify other VPN parameters as needed, then click OK to return to the main VPN page.

NOTE: At this point, your master server recognizes the slave server, but the slave server has not been updated yet with the VPN configuration information. The slave server must be updated in order for the VPN to be brought up. Make sure that the master and slave servers are attached to the Internet through their respective ISPs so that they can communicate with each other and the master server can update the slave server.

22 Update all VPN members with the entire VPN configuration as follows:

22a From the main VPN page, click Status.

22b Click Synchronize All to update all VPN members with the current configuration.

This might take some time, depending on the types of Internet connections and the number of members that must be updated. When the process is completed, all members should have a status of Up-to-Date.

22c If any VPN members remain with a status of Being Configured, select the member or master, then check the audit log for configuration errors.

22d Click OK.

The VPN is now set up between two sites. You can add more sites and update all members at the same time. To add another site, repeat Step 9 on page 200 through Step 22 on page 202.

Note that the firewall's public IP address must be prevented from being advertised through the VPN tunnel interface. If it is learned through this interface, packets destined for the public IP address will pass through the VPN tunnel interface and never arrive.

From a routing standpoint, the VPN tunnel interface is just another interface. One attribute of this interface is that all routes that are advertised through it add a cost of only one. Because the VPN tunnel interface provides the lowest cost to any network or host that advertises through it, all future access to that network or host will be through the VPN tunnel interface, in which case the data is encrypted. However, because the networks learned through the VPN tunnel interface can be advertised by the public interface, you might want to configure filters to prevent the networks from being advertised.

In this example, the VPN server is directly connected to the Internet. You must configure this machine as a firewall to secure the server and machines behind it. You should implement basic filtering using TCP/IP RIP filters and TCP/IP packet forwarding filters. If you do not want any clients to access the Internet, set all parameters to Deny, and allow only traffic that must pass through. If you selected the Setup Novell BorderManager 3.7 for Secure Access to Public Interface option during installation, these filters are already set for you and you are not required to perform any further configuration.

VPN Servers Using Different Networks for Public and Private Addresses

As shown in the earlier example, this scenario is the same as the previous scenario, except that the public and private addresses use different Class B IP addresses at each office.

The procedure for this scenario is almost the same as for the previous scenario, with the following differences:

- Use FF.FF.F0.0 for the network masks of the public interfaces.
- Instead of configuring a list of protected networks in Step 17 on page 201 and Step 21 on page 201, select Enable IP RIP to configure the use of a dynamic routing protocol.

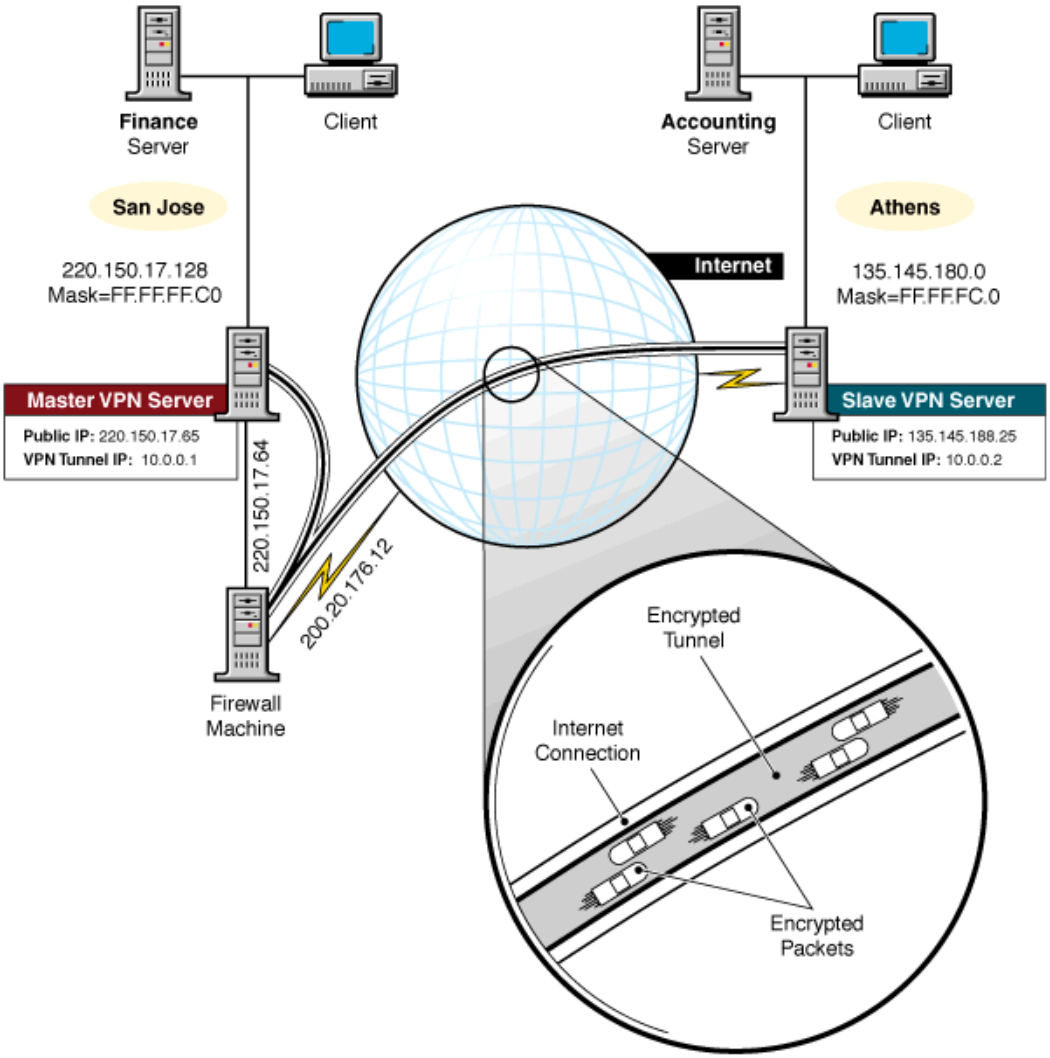
Using the VPN Server behind a Firewall

In this example, the VPN master server for the Finance office in San Jose is behind a firewall server that is connected to the Internet, as shown in the following figure Figure 16, “Remote Sites Linked by VPN Nodes behind a Firewall,” on page 205. The public IP address and subnet mask for the VPN

server are part of a local network. The firewall has an IP address of 200.20.176.12 on the Internet connection. The VPN master server has a public IP address of 220.150.17.65. The local network is using a subnet mask of FF.FF.FF.C0.

The slave server in Athens is connected through an ISP. The public IP address and subnet mask are 135.145.188.25 and FF.FF.FC.0, respectively. Both offices are sharing data that must be encrypted and sent through a VPN tunnel. The procedure shows you how to connect the two remote sites using an encrypted tunnel to send the data.

Figure 16 Remote Sites Linked by VPN Nodes behind a Firewall



To connect remote Internet sites using a VPN through a firewall, complete the following steps:

1 Choose a master server for your VPN.

In this example, the San Jose site is selected because the corporate office has the Corporate Information Services staff, who are better equipped to manage the VPN.

2. Contact an ISP and arrange for Internet connectivity for the slave server. Write down the public IP address and subnet mask that the ISP provides you.

   NOTE: Repeat this step for each site that will be a part of the VPN.

   In this example, the public IP address and subnet mask for the VPN master in San Jose are 220.150.17.65 and FF.FF.FF.C0, respectively. The public IP address and subnet mask for the VPN slave in Athens are 135.145.188.25 and FF.FF.FC.0, respectively.

3. Choose an IP address and mask to use for your VPN tunnel interface.

   Because this address will never be sent over the Internet, it can be any unregistered address, for example, 10.0.0.1 and FF.0.0.0 for the master server, and 10.0.0.2 for the slave server.

   NOTE: The master server and all slave servers must use IP addresses on the same network or subnet for the VPN tunnel interfaces.

4. Install NetWare and Novell BorderManager 3.7 software on your master server.

5. Use NIASCFG to configure the protocols and routing on your master server:

   - Configure a LAN interface to connect to your local network behind the firewall.
   - Enable TCP/IP.
   - Bind TCP/IP to the LAN interface that connects your VPN server to your firewall (220.150.17.65). This interface must have a registered IP address.
   - Reinitialize the system to make these changes take effect.

6. Establish a connection to your firewall router and verify that the master server can communicate with the ISP router.

   Do this before you add the VPN. Before testing the connection, you must verify that the firewall is configured to allow ICMP packets through. After testing, the filters should be returned to their previous configuration. Because the Internet connectivity is provided by the firewall or another router, you are not required to make a WAN call. Enter **`LOAD PING`** at the console prompt and enter the IP address of the ISP

router. If you can ping the router, you are connected to the ISP and should be able to reach any location on the Internet, including your other sites after they are connected.

7. Use VPNCFG to configure your VPN master server. Make sure you do the following:

   - Specify the public IP address and subnet mask. In this example, specify 220.150.17.65 for the public IP address, and FF.FF.FF.C0 for the subnet mask.
   - Specify the VPN tunnel IP address and subnet mask. In this example, specify 10.0.0.1 for the VPN tunnel IP address, and FF.0.0.0 for the subnet mask.

     NOTE: VPNCFG automatically adds some filters to prevent the IP address of the VPN tunnel from being sent through the public interface, and to prevent the public IP address from being sent through the tunnel interface.
   - Generate encryption information for the VPN master server.
   - Copy the encryption information to a diskette.

   Refer to Novell BorderManager 3.7 Install and Setup guide or the online help for the procedure to set up the master server.

8. Configure your firewall to allows VPN packets to pass through.

   For a list of filters that must be configured, refer to the prerequisites section in Novell BorderManager 3.7 Install and Setup guide.

9. Send the MINFO.VPN file with the master encryption information to the administrator configuring the VPN slave server.

10. Repeat Step 4 on page 198, Step 5 on page 198, Step 6 on page 206, and Step 11 on page 207 for the slave server.

11. If you did not select the Setup Novell BorderManager 3.7 for Secure Access to the Public Interface option for the slave server during installation, load BRDCFG and select this option.

12. At the VPN slave server, use VPNCFG to configure the VPN slave server. Make sure you do the following:

    - Specify the public IP address and subnet mask. In this example, specify 135.145.188.25 for the public IP address, and FF.FF.FC.0 for the subnet mask.

- Specify the VPN tunnel IP address and subnet mask. In this example, specify 10.0.0.2 for the VPN tunnel IP address, and FF.0.0.0 for the subnet mask.
- Generate encryption information for the VPN slave server using the master encryption information file (MINFO.VPN). Call the master server administrator and verify that the digest values match.
- Copy the slave encryption information to a file.

Refer to Novell BorderManager 3.7 Install and Setup guide or the online help for the procedure to set up the slave server.

13 Send the SINFO.VPN file with the slave encryption information back to the administrator configuring the VPN master server.

14 At the administrative workstation, install the Novell BorderManager 3.7 snap-in for the NetWare Administrator utility if it has not already been installed.

The installation program for this utility (SETUP.EXE) is in the \PUBLIC\BRDMGR\SNAPINS directory on the SYS: volume of your server after Novell BorderManager 3.7 has been installed.

NOTE: Perform this step from a client that is authenticated to the NDS or eDirectory tree in which the VPN master server resides. The machine must be logged in with Supervisor rights to the VPN master server. If this is the first VPN server or border server on this tree, then Supervisor rights to the root directory are required in order to extend the NDS or eDirectory schema.

15 In NetWare Administrator, double-click the VPN master server and select the Novell BorderManager 3.7 Setup page.

16 Click the VPN tab.

17 Double-click Master Site-to-Site under Enable Service.

Your master server should be listed in the VPN Members list. For example, if you named the master server Corporate, you should see Corporate displayed as a VPN member with an IP address of 220.150.17.65, as configured in Step 7 on page 207.

18 Manually configure a list of networks protected by the VPN master server.

In this example, a list of protected networks must be configured for all VPN servers even if Enable IP RIP is selected. Because the public and private networks are subnets of the same network, the RIP packets that pass through the VPN tunnel interface are blocked by the default VPN

filters. Because the routes to the protected networks cannot be learned using RIP, a list of protected networks must be configured manually.

In this example, you can specify the 220.150.17.128 network as a protected network by completing the following substeps:

18a Double-click the slave server to view details for that server.

18b Click Add.

18c Select Network.

18d Enter 220.150.17.128 for the IP network address.

18e Enter FF.FF.FF.C0 for the subnet mask.

18f Click OK.

18g Specify any additional protected networks, then click OK to return to the main VPN page.

19 Click Add to add the slave server to the VPN Members list.

20 Specify the name and pathname for the slave encryption information file (SINFO.VPN).

21 Ask the administrator of the VPN slave server to use VPNCFG to authenticate the encryption information and verify that the message digest values match. Click Yes if the values match.

To authenticate the encryption information using VPNCFG, select Authenticate Encryption Information.

22 Click Yes to manually configure a list of networks protected by this VPN slave server.

In this example, a list of protected networks must be configured for all VPN servers even if Enable IP RIP is selected. Because the public and private networks are subnets of the same network, the RIP packets that pass through the VPN tunnel interface are blocked by the default VPN filters. Because the routes to the protected networks cannot be learned using RIP, a list of protected networks must be configured manually.

In this example, you can specify the 135.145.180.0 network as a protected network by completing the following substeps:

22a Double-click the slave server to view details for that server.

22b Click Add.

22c Select Network.

22d Enter 135.145.180.0 for the IP network address.

22e Enter FF.FF.FC.0 for the subnet mask.

22f Click OK.

22g Specify any additional protected networks and modify other VPN parameters as needed, then click OK to return to the main VPN page.

NOTE: At this point, your master server recognizes the slave server, but the slave server has not been updated yet with the VPN configuration information. The slave server must be updated in order for the VPN to be brought up. Make sure that the master and slave servers are attached to the Internet through their respective ISPs so that they can communicate with each other and the master server can update the slave server.

23 Update all VPN members with the entire VPN configuration as follows:

23a From the main VPN page, click Status.

23b Click Synchronize All to update all VPN members with the current configuration.

This might take some time, depending on the types of Internet connections and the number of members that must be updated. When the process is completed, all members should have a status of Up-to-Date.

23c If any VPN members remain with a status of Being Configured, select the member or master, then check the audit log for configuration errors.

23d Click OK.

The VPN is now set up between two sites. You can add more sites and update all members at the same time. To add more sites, repeat Step 9 on page 200 through Step 23 on page 210.

Note that the firewall's public IP address must be prevented from being advertised through the VPN tunnel interface. If it is learned through this interface, packets destined for the public IP address will pass through the VPN tunnel interface and never arrive.

From a routing standpoint, the VPN tunnel interface is just another interface. One attribute of this interface is that all routes that are advertised through it add a cost of only one. Because the VPN tunnel interface provides the lowest cost to any network or host that advertises through it, all future access to that network or host will be through the VPN tunnel interface, in which case the data is encrypted. However, because the networks learned through the VPN

tunnel interface can be advertised by the public interface, you might want to configure filters to prevent the networks from being advertised.

In this example, access to the Internet by private clients is probably controlled by the firewall. However, depending on the firewall's configuration, you might want to implement filtering using TCP/IP RIP filters and TCP/IP packet forwarding filters to prevent access to the Internet. When configuring your firewall, do not remove any of the filters that are listed in the prerequisites section in Novell BorderManager 3.7 Install and Setup guide.

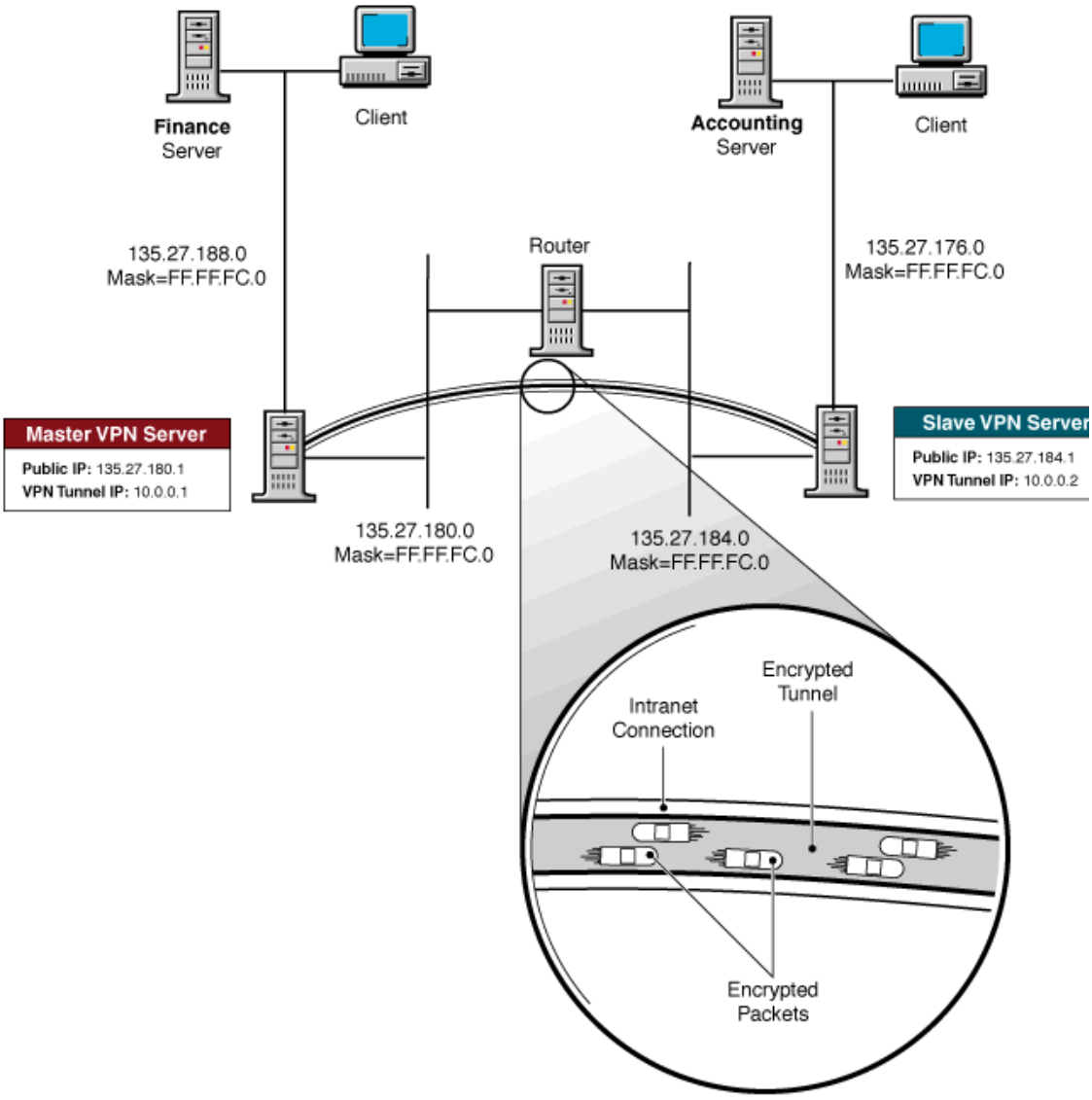
Setting Up a VPN within a Private Network

In this example, the Finance and Accounting servers in San Jose are on the corporate intranet or private network, as shown in following figure Figure 17, “LAN Segments on an Intranet Linked by a VPN,” on page 212. In this scenario, access to the Internet and an ISP are not required, just IP connectivity between the master server and slave server. The master server has a public IP address of 135.27.180.1, and the local network is using a subnet mask of FF.FF.FC.0. In this example, the master server and slaver server must use different subnet addresses because they are on different LAN segments. The slave server has an IP address of 135.27.184.1 and a subnet mask of FF.FF.FC.0.

Although not shown in this example, the VPN nodes could also be joined using a point-to-point connection, which requires that the nodes have the same network address.

Both departments are sharing data that must be encrypted and sent through a VPN tunnel. The procedure shows you how to connect the two LAN segments using an encrypted tunnel to send the data.

Figure 17 LAN Segments on an Intranet Linked by a VPN



To set up a VPN to operate within an intranet, complete the following steps:

1. Choose a master server for your VPN.

   In this example, a machine is selected that is easy to physically secure and easy for the Corporate Information Services staff to access.

2 Choose an IP address and mask to use for your VPN tunnel interface.

Because this address will never be sent over the Internet, it can be any unregistered address, for example, 10.0.0.1 and FF.0.0.0 for the master server, and 10.0.0.2 for the slave server.

NOTE: The master server and all slave servers must use IP addresses on the same network or subnet for the VPN tunnel interfaces.

3 Install NetWare and Novell BorderManager 3.7 software on your master server and slave server.

4 Use NIASCFG to configure the protocols and routing on your master server and slave server:

- Configure a LAN interface to connect to your local network.
- Enable TCP/IP.
- Bind TCP/IP to the LAN interface (135.27.180.1 for the master server). Because VPN servers are not connected to the Internet, this interface is not required to use a registered IP address.
- Reinitialize the system to make these changes take effect.

IMPORTANT: Make sure that the IPX protocol is not bound to the public interface of any of the VPN servers.

5 Verify that IP connectivity exists between the VPN members.

Before testing the connection, you must verify that the Novell BorderManager 3.7 filters or other firewalls are configured to allow ICMP packets through. After testing, the filters should be returned to their previous configuration. Enter **`LOAD PING`** at the console prompt of the VPN master server and enter the IP address of the VPN slave.

6 Use VPNCFG to configure your VPN master server. Make sure you do the following:

- Specify the public IP address and subnet mask. In this example, specify 135.27.180.1 for the public IP address, and FF.FF.FC.0 for the subnet mask.
- Specify the VPN tunnel IP address and subnet mask. In this example, specify 10.0.0.1 for the VPN tunnel IP address, and FF.0.0.0 for the subnet mask.

  NOTE: VPNCFG automatically adds some filters to prevent the IP address of the VPN tunnel from being sent through the public interface, and to prevent the public IP address from being sent through the VPN tunnel interface.

- Generate encryption information for the VPN master server.
- Copy the encryption information to a diskette.

Refer to Novell BorderManager 3.7 Installation Guide or the online help for the procedure to set up the master server.

7. If you did not select the Setup Novell BorderManager 3.7 for Secure Access to the Public Interface option during installation on your master server and slave server, load BRDCFG and select this option.
8. Send the MINFO.VPN file with the master encryption information to the administrator configuring the VPN slave server.
9. At the VPN slave server, use VPNCFG to configure the VPN slave server. Make sure you do the following:
   - Specify the public IP address and subnet mask. In this example, specify 135.27.184.1 for the public IP address, and FF.FF.FC.0 for the subnet mask.
   - Specify the VPN tunnel IP address and subnet mask. In this example, specify 10.0.0.2 for the VPN tunnel IP address, and FF.0.0.0 for the subnet mask.
   - Generate encryption information for the VPN slave server using the master encryption information file (MINFO.VPN). Call the master server administrator and verify that the digest values match.
   - Copy the slave encryption information to a diskette.

   Refer to Novell BorderManager 3.7 Install and Setup guide or the online help for the procedure to set up the slave server.
10. Send the SINFO.VPN file with the slave encryption information back to the administrator configuring the VPN master server.
11. At the administrative workstation, install the Novell BorderManager 3.7 snap-in for the NetWare Administrator utility if it has not already been installed.

    The installation program for this utility (SETUP.EXE) is in the \PUBLIC\BRDMGR\SNAPINS directory on the SYS: volume of your server after Novell BorderManager 3.7 has been installed.

    NOTE: Perform this step from a client that is authenticated to the NDS or eDirectory tree in which the VPN master server resides. The machine must be logged in with Supervisor rights to the VPN master server. If this is the first VPN server or border server on this tree, then Supervisor rights to the root directory are required in order to extend the NDS or eDirectory schema.

12 In NetWare Administrator, double-click the VPN master server and select the Novell BorderManager 3.7 Setup page.

13 Click the VPN tab.

14 Double-click Master Site-to-Site under Enable Service.

Your master server should be listed in the VPN Members list. For example, if you named the master server Corporate, you should see Corporate displayed as a VPN member with an IP address of 135.27.180.1, as configured in Step 6 on page 213.

15 Manually configure a list of networks protected by this VPN master server.

In this example, a list of protected networks must be configured for all VPN servers even if Enable IP RIP is selected. Because the public and private networks are subnets of the same network, the RIP packets that pass through the VPN tunnel interface are blocked by the default VPN filters. Because the routes to the protected networks cannot be learned using RIP, a list of protected networks must be configured manually.

In this example, you can specify the 135.27.188.0 network as a protected network by completing the following substeps:

15a Double-click the slave server to view details for that server.

15b Click Add.

15c Select Network.

15d Enter 135.27.188.0 for the IP network address.

15e Enter FF.FF.FC.0 for the subnet mask.

15f Click OK.

15g Specify any additional protected networks, then click OK to return to the main VPN page.

16 Click Add to add the slave server to the VPN Members list.

17 Specify the name and pathname for the slave encryption information file (SINFO.VPN).

18 Ask the administrator of the VPN slave server to use VPNCFG to authenticate the encryption information and verify that the message digest values match. Click Yes if the values match.

To authenticate the encryption information using VPNCFG, select Authenticate Encryption Information.

19 Click Yes to manually configure a list of networks protected by this VPN slave server.

In this example, a list of protected networks must be configured for all VPN servers even if Enable IP RIP is selected. Because the public and private networks are subnets of the same network, the RIP packets that pass through the VPN tunnel interface are blocked by the default VPN filters. Because the routes to the protected networks cannot be learned using RIP, a list of protected networks must be configured manually.

In this example, you can specify the 135.27.176.0 network as a protected network by completing the following substeps:

19a Double-click the slave server to view details for that server.

19b Click Add.

19c Select Network.

19d Enter 135.27.176.0 for the IP network address.

19e Enter FF.FF.FC.0 for the subnet mask.

19f Click OK.

19g Specify any additional protected networks and modify other VPN parameters as needed, then click OK to return to the main VPN page.

NOTE: At this point, your master server recognizes the slave server, but the slave server has not been updated yet with the VPN configuration information. The slave server must be updated in order for the VPN to be brought up. Make sure that the master and slave servers can communicate with each other so that the master server can update the slave server.

20 Update all VPN members with the entire VPN configuration as follows:

20a From the main VPN page, click Status.

20b Click Synchronize All to update all VPN members with the current configuration.

This might take some time, depending on the number of members that must be updated. When the process is completed, all members should have a status of Up-to-Date.

20c If any VPN members remain with a status of Being Configured, select the member or master, then check the audit log for configuration errors.

20d Click OK.

The VPN is now set up between two LAN segments. You can add more segments and update all members at the same time. You can repeat Step 3 on page 213 through Step 20 on page 216 to add another slave server.

Note that if you are using a firewall, the firewall's public IP address must be prevented from being advertised through the VPN tunnel interface. If it is learned through this interface, packets destined for the public IP address will pass through the VPN tunnel interface and never arrive.

From a routing standpoint, the VPN tunnel interface is just another interface. One attribute of this interface is that all routes that are advertised through it add a cost of only one. Because the VPN tunnel interface provides the lowest cost to any network or host that advertises through it, all future access to that network or host will be through the VPN tunnel interface, in which case the data is encrypted. However, because the networks learned through the VPN tunnel interface can be advertised by the public interface, you might want to configure filters to prevent the networks from being advertised.

Setting up Client-to-Site VPNs

This section explains the advanced tasks you complete to configure a client-to-site VPN and to make a client-to-site connection. This section contains the following procedures:

- “Setting Up the Phone Book Capability” on page 217
- “Distributing VPN Server Addresses to Users” on page 221
- “Setting Up Dial Properties” on page 222
- “Setting Up Remote Access on a VPN Server to Support Dial-In VPN Clients” on page 222

Setting Up the Phone Book Capability

The phone book capability enables you to easily dial an ISP by selecting a phone number from a preconfigured phone book or from a phone book that you created. Because the VPN client can use any phone book created in the Microsoft* Connection Manager, the VPN client can find any phone book distributed by an ISP that was created in that format and enables you to select entries from it. Furthermore, ISP phone books that were not created by the Microsoft Connection Manager can be converted to a usable format using the VPN client phone book capability.

When the phone book capability is selected, any phone books found on the workstation are listed in the Phone Book drop-down menu. The list can contain the following phone book names:

- Microsoft Network.
- iPass* Corporate Connection.
- Any other phone books located on the workstation that were created using the Microsoft Connection Manager. These phone books will be named after the directories in which they are located.
- Any phone book that was created using the VPN client phone book capability.
- Any phone book that was converted with the VPN client phone book capability.

Selecting a Phone Number from a Phone Book

To select a phone number from a phone book, complete the following steps:

1. From the VPN Login dialog box, click the Dial-Up tab, then click Settings.
2. Click Phone Book.
3. Select a phone book from the Phone Book drop-down menu.
4. Select a country from the Country drop-down menu.

   Only countries that contain phone book entries are displayed.
5. Select a state or region from the State or Region drop-down menu.

   When a state or region is selected, only phone book entries for that state or region are displayed. If no states or regions were assigned to the phone book entries, the drop-down menu is grayed out and all phone book entries for the selected country are displayed.
6. To sort the phone book entries, click the Sort by Name or Sort by Number radio buttons.
7. To select a phone book entry, double-click the desired entry and click OK.

Converting an ISP Phone Book

To convert an ISP phone book to the Microsoft Connection Manager format, complete the following steps:

1. From the VPN Login dialog box, click the Dial-Up tab, then click Settings.
2. Click Phone Book, then click Manage.
3. Select Convert an ISP Phone Book.
4. Select the type of ISP phone book that will be converted and click Convert.

   A default directory is indicated for each phone book. If you choose to not load a phone book in the default directory, you must set the path to the correct directory, as described in "Defining the Phone Book Path" on page 221.

   When the phone book is converted, it is displayed in the Phone Book drop-down menu, allowing you to select phone book entries.

Creating a New Phone Book

To create a new phone book, complete the following steps:

1. From the VPN Login dialog box, click the Dial-Up tab, then click Settings.
2. Click Phone Book, then click Manage.
3. Select Create a New Phone Book.
4. Enter a name for the phone book.
5. For each phone book entry, complete the following substeps:

   5a. Select a country.

   5b. Select a state or region.

   If a state or region does not exist for the selected country, select All or add a new state or region by editing the file \NOVELL\VPNC\PHONE BOOKS\DEFAULT.PBR. Use a text editor to add new regions to the end of the file and increment the number on the first line of the file to match the new number of regions in the file.

   5c. Enter a location name.

5d Enter an area code.

5e Enter a phone number.

5f Click Add.

6 Click Save to save the phone book entries.

Changing the States and Regions

When a phone book is created, states and regions are retrieved for display from the DEFAULT.PBR file in the PHONE BOOKS directory. When a newly created phone book is saved, the states and regions are saved in a newly created phone book directory under the PHONE BOOKS directory. The system administrator can change the DEAULT.PBR file to add, replace, or delete states or regions and then distribute the file to the users. When editing the file, you must make sure that the first entry indicates the number of states or regions listed in the file.

Editing a Phone Book

You can edit the entries in any phone book that you created or converted. You cannot edit phone books that were created by an ISP in Microsoft Connection Manager format.

To edit a phone book,

1 From the VPN Login dialog box, click the Dial-Up tab, then click Settings.

2 Click Phone Book, then click Manage.

3 Select Edit an Existing Phone Book.

4 Select the name of the phone book that you want to edit from the drop-down menu.

5 Double-click the phone book entry that you want to edit and make the desired changes.

6 Click Save to save your changes.

Protecting a Phone Book

To disable the user's capability to edit a phone book that you created,

1. Remove the line UpdateFlags=1 from the .ini file in the phone book directory.

   Without this line, the phone book will not appear as a phone book selection when you attempt to edit it.

2. Change the attributes of all files in the phone book directory to Read-only.

3. Make a copy of the phone book directory and distribute it to the users.

Defining the Phone Book Path

Normally, the VPN phone book utility can locate phone books that use the Microsoft Connection Manager format. However, if the VPN phone book utility cannot find a phone book that uses the Microsoft Connection Manager format, you should move the phone book files to the directory listed in the Define Phone Book Path dialog box or change the path configured in the dialog box.

To change the phone book path, complete the following steps:

1. From the VPN Login dialog box, click the Dial-Up tab, then click Settings.

2. Click Phone Book, then click Manage.

3. Select Define Phone Book Path.

4. Set Alternate Phone Book Path to the location of the phone book files and click OK.

Distributing VPN Server Addresses to Users

If you have a file named VPNHOSTS.TXT in the DISK1 directory of your VPN client installation directory, the installation program will take IP addresses from this file and enter them into the workstation's Registry. Each line of the VPNHOSTS.TXT file might contain one address, optionally followed by a description of the entry. For example:

130.1.1.1 My Corporate VPN in San Jose

These entries can be edited using any text editor. You can create the VPNHOSTS.TXT file in the DISK1 directory of your VPN client installation directory, and distribute the DISK1 and DISK2 directories to the users.

Setting Up Dial Properties

You can configure the dial properties for Microsoft Dial-Up Networking connections using the VPN client login interface. For more information about the dial properties, refer to the Microsoft documentation for Dial-Up Networking.

To configure the dial properties using the VPN client interface, complete following steps:

1. From the VPN Login dialog box, click the Dial-Up tab, then click Settings.
2. Click Dial Properties.
3. Configure the properties for each Microsoft Dial-Up Networking connection, as required, and click OK.

Setting Up Remote Access on a VPN Server to Support Dial-In VPN Clients

This section describes how to configure the remote access software to support Novell BorderManager 3.7 VPN clients. Remote access is required only for VPN clients that dial in to a VPN server directly. It is not required for VPN clients that access a VPN server through an ISP connection.

The configuration of remote access consists of the following procedures:

- "Adding a Board Using a Serial Port Driver" on page 222
- "Setting Up PPPRNS to Support Remote IP Nodes" on page 226
- "Setting Up PPPRNS Security" on page 233
- "Setting Up a Remote Client Password" on page 234

Adding a Board Using a Serial Port Driver

This section describes how to configure a board to support dial-in clients. Two separate procedures are required to configure a board using a serial port driver. This section contains the following procedures:

- "Loading the AIO Drivers" on page 223
- "Setting Up Ports for Remote Access" on page 224

Loading the AIO Drivers

To load the appropriate driver, complete the following steps:

1. Insert a physical AIO board into your system or enable one of your COM ports.
2. Load NIASCFG.
3. Select Configure NIAS > Remote Access > Set Up > Add a Serial Adapter Board.

   If you are loading NIASCFG for the first time, the program prompts you with instructions to configure remote access. These instructions roughly correspond to the procedures contained in this section.
4. For each communications adapter you have installed, load its AIO driver once by selecting the appropriate serial adapter entry from the list.
5. If no AIO ports are defined or the board cannot be loaded, you see a warning message. Press *Enter* and step through configuring the board. Otherwise, skip to Step 8 on page 223.

   To configure a board, you must enter its name and other specific information. Follow the prompts on the screen.
6. If you are using an ISDN connection, press *Ins* and select the WHSMCAPI driver.

   NOTE: Some ISDN boards, such as the USRobotics* Allegra series for the NetWare® software, use WAN ODI drivers instead of WHSMCAPI. Select the appropriate driver, or press *Ins* and use your manufacturer-supplied driver diskette. Specify your board parameters, then continue with Step 8 on page 223.
7. If you are using a Point-to-Point Tunneling Protocol (PPTP) connection, do the following:

   7a Press *Ins* and select the AIOPPTP driver.

   7b Select Number of AIOPPTP Ports and select a value.

   This number is used in conjunction with First AIO Port Number to determine the total number of ports, starting with the first port, that are available for use by PPTP.

   Valid values range from 4 to 249.
8. Select Continue with Automated Setup after the remote access software has determined which ports have modems attached. Select Try Modem Discovery Again if modems were not discovered (not turned on).

Setting Up Ports for Remote Access

You use the NIASCFG utility to configure the remote access ports. When the utility starts, function keys are enabled. The keys that are enabled for a particular remote access window are displayed at the bottom of the utility window. Table 4, "Remote Access Function Key Definitions," on page 224 summarizes the key functions:

Table 4 Remote Access Function Key Definitions

Function Key	Operation
F1	Open context-sensitive help
F2	Customize a configuration report; save port statistics to file; write an audit report to file
F3	Rename; modify the field
F4	Copy from
F5	Mark/unmark (select multiple items from a list)
F6	Copy to
F7	Clear all marks
F8	Display instructions; identify the port
F10	Activate the AIOPAD configuration; run a service-specific NetWare Loadable Module™ (NLM™) file
Alt+F1	Display additional key help
Alt+F5	Mark all
Alt+F7	Abort the configuration report

To configure ports for remote access, complete the following steps:

1. Load NIASCFG.
2. Select Configure NIAS > Remote Access.

   The Remote Access Options window is displayed.

3. Select Configure Ports.

   A window listing port information by port name is displayed. The window lists the ports that the AIO NLM recognizes. Default port names are assigned, depending on the existing configuration.

   The Status column displays the status of the port: Available, Unavailable (the driver is not loaded), or Port_Acquired.

4. Select the port that you want to configure and press *Enter*.

5. Specify the following port parameters:

   - Port Name—Enter a unique port name of up to 15 characters, or up to 14 characters if you will use the port for the NASI (NetWare Asynchronous Services Interface) Connection Service (NCS). Only alphanumeric characters, underscores (_), hyphens (-), and periods (.) are allowed. Port names must be unique on a server and begin with a letter in the first character position. The port name can indicate the type of connection, the telephone number of the port, or other information for troubleshooting purposes. Default port names are supplied based on the driver type. In NASI applications, port names are called *specific names*. More information is located in the NetWare 5 online documentation at the following path:

     Contents > Connectivity Services (under Network Services heading) > Remote Access Configuration

   - Port Description—(Optional) Enter a description for the port. For example, if you plan to use the port to manage remote access, you can describe it as System administrator's private line.

   - Modem Type—Select Modem Type and press *Enter*. A list of modem types is displayed. Select the type of modem that is attached to the port.

     If your modem is not listed, select a similar modem. If no similar modems are listed, select Hayes* Compatible. Select Automatic Detection to have the remote access software determine the modem type for you. The default is None, which means that the line is a direct connection and does not use a modem.

     For direct connections, select None. For X.25 ports, select AIOPAD. For ISDN adapters (not ISDN terminal adapters that connect to a serial port like a modem), select ISDN (AT Controlled). For PPTP ports, select AIOPPTP.

NOTE: For a list of supported modems and the current support file, download NWCMOD.EXE from developer.novell.com/devres/wan/modemscr/mdmscr.htm. Note that the modem script files in Novell BorderManager 3.7 are not backward-compatible with the NetWare Connect® 2.0 software. More information about creating and editing modem scripts is located in the NetWare 5 online documentation at the following path:

Contents > Connectivity Services (under Network Services heading) > Routing Configuration

6. (Optional) Select Additional Parameters and press *Enter*.

   The Port Configuration window displays additional port configuration parameters. Usually, you can keep the defaults for most of these parameters. More information about configuring these parameters is located in the NetWare 5 online documentation at the following path:

   Contents > Connectivity Services (under Network Services heading) > Remote Access Configuration

7. When you have configured the port, press *Esc* and select Yes to save the changes.

8. Press *Esc* to return to the Remote Access Options window.

Setting Up PPPRNS to Support Remote IP Nodes

This section describes how to configure your server to support remote IP users. Several separate procedures are required to configure Point-to-Point Protocol Remote Node Service (PPPRNS) for remote IP nodes. This section contains the following procedures:

- "Setting Up the Server as a TCP/IP Router" on page 226
- "Loading PPPRNS with IP Support" on page 228
- "Setting Up PPPRNS for IP Support" on page 231
- "Setting Up Client Software" on page 233

Setting Up the Server as a TCP/IP Router

To provide remote access to other TCP/IP hosts on the network, you must configure the remote access server as an IP router. TCP/IP routing enables forwarding IP traffic from one network to another.

You use the Protocols and Routing option in NIASCFG to configure your server as an IP router. More information about using this option and

configuring a TCP/IP router is located in the NetWare 5 online documentation at the following path:

Contents > Connectivity Services (under Network Services heading) > Routing Configuration

When you configure the server as an IP router, the appropriate LOAD and BIND commands are added to the INITSYS.NCF and NETINFO.CFG files in the SYS:\ETC subdirectory.

IMPORTANT: Modifications to existing IP addresses take effect the next time you load TCPIP.NLM, start the remote access server, or reinitialize the system.

You can also use the Protocols and Routing option in NIASCFG to configure PPTP on a remote access server. PPTP allows the remote access software to accept PPP calls from remote users through any ISP that supports PPTP by tunneling PPP packets through an IP tunnel.

NOTE: Your ISP must have a PPTP access concentrator, and your network must have access to a port on that concentrator. Contact your ISP for details.

You can configure the remote access server as a Dynamic Host Configuration Protocol (DHCP) server. Use this option to assign IP addresses to remote access clients from the remote access server address range through DHCP (refer to "Loading PPPRNS with IP Support" on page 228). You can also use this option when the clients want to obtain client information such as the domain name server from the remote access server (refer to "Setting Up PPPRNS for IP Support" on page 231).

To install the DHCP server, complete the following steps:

1. Enter the following command at the console prompt on the remote access server:

   For NetWare 4.11 systems, **`LOAD DHCPD`**

   For NetWare 5 systems, **`LOAD DHCP`**

2. Set the following parameters.

   For more information about these parameters, refer to "Loading PPPRNS with IP Support" on page 228.

   2a Set the Client Address Range parameter to Yes.

   2b Enter the IP addresses for the Client Address Range Start and Client Address Range End parameters.

2c If necessary, enter IP addresses for the Secondary Local IP Address, Secondary Address Range Start, and Secondary Address Range End parameters.

2d If your clients want to receive domain information from the DHCP server, specify the Domain Name Server Address and Domain Name parameters.

NOTE: The DHCPD and DHCP NLM files can be used only for remote node clients. They cannot be used for LAN clients. You must set up a separate DHCP server for LAN clients.

Loading PPPRNS with IP Support

Loading PPPRNS with IP support allows IP clients to dial in and become remote nodes on the network. This procedure adds the appropriate LOAD and BIND commands to the NETINFO.CFG file.

Table 5, "PPPRNS IP Parameters," on page 228 describes the IP parameters that you configure for PPPRNS with IP support:

Table 5 PPPRNS IP Parameters

Parameter	Description
Local IP Address	Specifies the local IP address for the WAN interface on the remote access server. This is a 4-byte (32-bit) numeric value that identifies both a network and a local host or node on that network. The address is represented in dotted decimal notation. Each byte is represented by a decimal number, with periods separating the bytes, for example, 130.57.45.240. Each byte can range from 0 through 255. Do not use hexadecimal numbers. The local IP address must be on the same subnet as the client address range. The remote access software creates a virtual LAN segment (network) for all IP clients accessing this server. The IP address on the remote node can be configured statically or dynamically: Statically—The user explicitly specifies the IP address in the client software. Dynamically—The remote access software assigns IP addresses through the Internet Protocol Control Protocol (IPCP). Specify a client range. Dynamically—The remote access server is a DHCP server and assigns IP addresses. Configure the remote access server as a DHCP server.

Parameter	Description
Subnet Mask	Specifies a 4-byte subnet mask in dotted decimal notation. Each byte ranges from 0 through 255, with periods separating the bytes.
Use Header Compression	Specifies whether to use header compression over the WAN link with the remote client. The default is No. If you specify Yes, the remote access IP service will use TCP header compression with all remote access clients connecting to this address. Make sure that the settings for header compression on the server and the client agree: both are enabled or both are disabled. If the client is not configured to use header compression but the server is, TCP will not run between the remote access server and the client.
Specify Client Address Range	Specifies whether the remote access software assigns IP addresses to the remote nodes. After you have specified the range and a client requests an address, the remote access software chooses an address that is not in use by another client from the address range and assigns it to the requesting client. Address assignments can be made through either IPCP or DHCP if the remote access server is configured as a DHCP server. If the remote access server is not configured as a DHCP server and a client address range is specified, IPCP address assignment is used.
Client Address Range Start	Specifies the starting address for the remote IP client address range. The client address range must be on the same network or subnet as the server address specified in the Local IP Address parameter.
Client Address Range End	Specifies the ending address for the remote IP client address range.
Specify Secondary Client Address Range	**Note:** You configure a user to use the primary or secondary client address range with the NetWare Administrator utility. The secondary client address range feature might or might not be available on your system; it is an optional part of the standard Novell remote access software.
Secondary Local IP Address	Specifies an additional (secondary) local IP address on the remote access server.
Secondary Subnet Mask	Specifies an additional (secondary) subnet mask on the remote access server.
Secondary Address Range Start	Specifies the starting address for the secondary remote IP client address range. This is a separate group of addresses that you can specify to limit or restrict access to network locations.

Parameter	Description
Secondary Address Range End	Specifies the ending address for the secondary remote IP client address range. This is a separate group of addresses that you can specify to limit or restrict access to network locations.

To load PPPRNS with IP support,

1. Load NIASCFG.
2. Select Configure NIAS > Remote Access > Set Up > Select Remote Access Services > PPPRNS > IP.
3. Select Local IP Address and enter a valid, unique local IP address.

   The local IP address must be on the same subnet as the client address range.
4. Select Subnet Mask > enter a 4-byte value in dotted decimal notation.
5. Select Use Header Compression > specify Yes to use TCP header compression. Otherwise, specify No.

   Make sure the settings for header compression on the server and the client agree, that is, both are enabled or disabled.
6. Select Specify Client Address Range and do the following:

   The Client Address Range parameters must be set when the remote access server is configured as a DHCP server.

   6a Specify Yes if you want the remote access server to assign IP addresses to the remote nodes. Otherwise, specify No and continue with Step 7 on page 230.

   6b Specify the Client Address Range Start and Client Address Range End parameters.

   The address range is for address assignment only, and is not for authenticating the remote IP address. If the client already has an address configured locally and does not need address assignment from the remote access server, the remote access software will not check the client address against the address range to make sure it is within the range.
7. (Optional) Select Specify Secondary Client Address Range and do the following:

7a Specify Yes if you want the remote access server to assign secondary IP addresses to the remote nodes. Otherwise, specify No and continue with Step 8 on page 231.

7b Specify the Secondary Subnet Mask, Secondary Address Range Start, and Secondary Address Range End parameters.

The secondary address parameters might not be available on your system. If these parameters are available, you can use them to limit access to certain network locations.

8 Press *Esc* and specify Yes to save your changes.

The service is selected but is not necessarily running. When a service is selected, it is added to the NWCSTART.NCF file. To verify that the service is running, you can view service statistics.

The changes take effect the next time you start the PPPRNS service.

Setting Up PPPRNS for IP Support

This section is optional. You can set up your remote access server to function as a DHCP server for remote clients. When your remote access server is configured as a DHCP server, specify the following parameters per user or container:

- Domain Name Server Address
- Domain Name
- Boot Filename (used for diskless clients)

For these parameters to apply, you must load DHCPD (for NetWare 4.11 systems) or DHCP (for NetWare 5 systems).

To configure IP addresses for PPPRNS, complete the following steps:

1 Load NIASCFG.

2 Select Configure NIAS > Remote Access > Configure Services.

The Remote Access Services window is displayed.

3 Select PPPRNS.

The PPPRNS Configuration Options window is displayed.

4 Select Set IP Parameters.

A list of users and containers in the default NDS or eDirectory context is displayed.

Select the single period (.) to set IP information for the current container. If users are distributed over multiple contexts, select the double period (..) to move up the NDS or eDirectory tree to a common branch. Select names with a plus (+) prefix to move down the tree.

If the CONNECT object does not have Browse rights to move up the NDS or eDirectory tree, press *Ins* and enter the new NDS or eDirectory context. This enables you to jump to another branch of the tree where the CONNECT object does have rights.

5 Select a user or container.

The User IP Parameters window is displayed. You can set the remote access parameters if the CONNECT object has Write attribute rights, in addition to having Browse and Read attribute rights, to that container.

6 Select Set Domain Information and specify Yes.

The domain information can be specified when the remote access server is set up as the DHCP server for remote clients and the clients want to receive this information.

7 Specify the following domain parameters:

NOTE: The following parameters are available to clients only if the remote access server is a DHCP server and the clients request the information using DHCP. If the remote access server is not set up as a DHCP server (refer to "Setting Up PPPRNS to Support Remote IP Nodes" on page 226) or if the clients do not use DHCP to request information, these parameters are not used.

- Domain Name Server Address—Enter the address of the domain name server to resolve hostnames for client requests.
- Domain Name—Enter the suffix to append to local hostnames. For example, if the domain name is novell.com, the client appends this name to ca (the local hostname) to provide the complete name of ca.novell.com.

  You can specify the Domain Name Server Address parameter without specifying the Domain Name parameter if the client uses complete hostnames. Specifying the Domain Name parameter without the server address is not useful.

8 Press *Esc* twice to save your changes.

The changes take effect when you have saved them.

Setting Up Client Software

After you have completed the procedure to support remote IP nodes, you can configure the PPPRNS client software. The Windows* client software for PPPRNS is available on a separate client CD-ROM. Install and configure the client software on the remote PC and try to establish an IP connection. For more information, refer to the remote access online help.

Setting Up PPPRNS Security

To configure PPPRNS security,

1. Load NIASCFG.
2. Select Configure NIAS > Remote Access > Configure Security.

   The Remote Access Security window is displayed.
3. Select PPPRNS.

   The PPPRNS Configuration Options window is displayed.
4. Select Configure Security.

   The PPPRNS Configuration window is displayed.
5. Select Enable Security and specify Yes or No to enable or disable PPPRNS security.

   When security is disabled, callers can establish a connection successfully by entering a valid username without a password. However, callers must still log in to the network.
6. Specify Yes or No to enable or disable the NetWare Connect Authentication Protocol (NWCAP).

   This method is supported by the remote access dialer. NWCAP allows the NetWare password to be used as the Remote Client password (the default).
7. Specify Yes or No to enable or disable the Password Authentication Protocol (PAP).

   The default is No. If you enable this protocol, callers configured for PAP must specify the Remote Client password to successfully establish a connection. This method is supported by the remote access dialer. Enable this option if you have UNIX* clients that support PAP.

   NOTE: For dial-in VPN clients, either PAP or CHAP must be enabled. If you want PAP or CHAP users to authenticate and they do not have a Remote Client

password, enter **`Set PPPRNS AdmitNoConfig=ON`** at the server console. The default is OFF. Setting this option to ON is not recommended.

8 Specify Yes or No to enable or disable the Challenge Handshake Authentication Protocol (CHAP).

This method is not supported by the remote access dialer shipped with NetWare. This method requires callers to specify a Remote Client password to establish a connection. To set Remote Client passwords, refer to "Setting Up a Remote Client Password" on page 234.

Setting Up a Remote Client Password

You must complete the following procedures to configure a remote client password:

- "Setting Remote Client Passwords" on page 235
- "Setting Password Restrictions" on page 236
- "Allowing Users to Change Passwords" on page 237

The Remote Client password is required to establish a connection, and the NetWare password is required for logging in to the NetWare network. Both passwords are specified for the same username.

You can set Remote Client passwords for the following types of callers:

- Remote user on a Macintosh* computer
- Remote user on a PC using the PAP or CHAP method of authentication
- Remote user accessing a remote control host session on the network

You assign Remote Client passwords at first, then later allow callers to choose and change their own passwords. The remote access software has Windows and Macintosh tools to enable users to change their passwords. Refer to the remote access online help for more information about these tools. More information about using the NetWare Administrator utility to assign and change Remote Client passwords is located in the NetWare 5 online documentation at the following path:

Contents > Connectivity Services (under Network Services heading) > Remote Access Configuration

Enhance security for Remote Client passwords by requiring the following:

- Minimum password length

- Limited number of connection attempts
- Periodic password change

  The user has a grace login limit of three logins after a password has expired. During this grace period, the password must be changed by either the user or the administrator. NCS dial-in users can see the number of grace logins remaining as they authenticate with the Service Selector (if their password has expired) before they select a host session. A separate utility on the remote access client allows the user to check for the number of remaining grace logins. Refer to the remote access online help for more information.

Setting Remote Client Passwords

To set Remote Client passwords, complete the following steps:

1. Load NIASCFG.
2. Select Configure NIAS > Remote Access > Configure Security.

   The Remote Access Security window is displayed.
3. Select Set User Remote Client Password.

   A list of authorized users is displayed.

   If users are distributed over multiple contexts, select the double period (..) to move up the NDS or eDirectory tree to a common branch. Select any other container object to move down the tree.

   If the CONNECT object does not have Browse rights to move up the NDS or eDirectory tree, press *Ins* and enter the new NDS or eDirectory context. This allows you to jump to another branch of the tree where the CONNECT object does have rights.
4. Select a username.

   The current status of the user's password is displayed, for example, never set or expired.
5. Enter a password.

   The password must be alphanumeric and can contain up to 16 characters. The password is case sensitive.

   IMPORTANT: You must enable the long password option in order to specify passwords longer than eight characters. Refer to "Setting Password Restrictions" on page 236 for more information.

You can configure user passwords if the CONNECT object has Write attribute rights, in addition to having Browse and Read attribute rights, to the container.

IMPORTANT: The Remote Client password is less secure than the NetWare password. Make sure it is not the same as the NetWare password.

6. Reenter the password.
7. Press *Esc* to save your changes.
8. Distribute the passwords to the corresponding users.

A user must enter this password to establish an initial connection with remote access.

An NCS dial-in user is prompted for a Remote Client password when dialing into the remote access server. If no Remote Client password is defined for this user, access will be denied.

NOTE: An undefined password is not the same as a NULL password. If the password is set to NULL, the user must press *Enter* when prompted for a password.

The Service Selector indicates when a Remote Client password has expired and enables the NCS dial-in user to change the password at login time.

Setting Password Restrictions

To set password restrictions for Remote Client passwords, complete the following steps:

1. Load NIASCFG.
2. Select Configure NIAS > Remote Access > Configure Security.

   The Remote Access Security window is displayed.
3. Select Set Remote Client Password Restrictions.
4. Select Enable Long Passwords > specify Yes or No to enable or disable this option.

   IMPORTANT: You cannot disable the long passwords feature after you have enabled it. If you enable long passwords, you must upgrade all your NetWare Connect 2.0 servers to the latest version of the remote access software. Users will no longer be able to use NetWare Connect 2.0. You must also set the Enable Long Passwords parameter on each server.
5. Enter a value between -1 and 20 for the Maximum Invalid Login Attempts parameter.

This sets the number of times the user can enter the wrong password. The Remote Client password is disabled and cannot be used after the specified number of failed tries. The default of -1 allows the user to reenter an incorrect password indefinitely.

6. Enter a value between -1 and 16 for the Set Minimum Password Length parameter.

   This sets the minimum number of characters for a password. The change takes effect the next time the password is set. To increase security, have users specify passwords of five or more characters. The default of -1 means no limit is set.

7. Press *Esc* to save your changes.

Allowing Users to Change Passwords

You can allow or disallow users to change their passwords. If you allow users to change passwords, you can increase password security by requiring them to change passwords periodically. More information about allowing users to change their passwords is located in the NetWare 5 online documentation at the following path:

Contents > Connectivity Services (under Network Services heading) > Remote Access Configuration

NOTE: The user has a grace login limit of three logins after a password has expired. During this grace period, the password must be reset or changed by either the user or the administrator. NCS dial-in users can see the number of grace logins remaining if their passwords have expired during authentication with the Service Selector.

The remote access software has Windows tools that enable users to change their Remote Client passwords, and it has Windows and Macintosh tools that enable users to check for the remaining number of grace logins. Refer to the remote access online help for more information.

The Service Selector also has a menu option for changing the Remote Client password. This option is available to NCS dial-in users or PPP dialers using the Terminal Window After Dial-in option.

Setting Up Implementation-Specific Client-to-Site Configurations

The Novell VPN client software enables remote clients to connect to a VPN server and exchange confidential information without risk. As with site-to-site configurations, the information is encrypted and its confidentiality is preserved until it reaches the VPN server. This section describes the various options for establishing a client-to-site VPN.

This section contains the following examples:

- "Using the Client to Dial In to an ISP and Connect to the VPN Server over the Internet" on page 238
- "Using the Client to Dial Directly In to the VPN Server" on page 239
- "Using the Client to Connect to the VPN Server over a Broadband Connection" on page 240

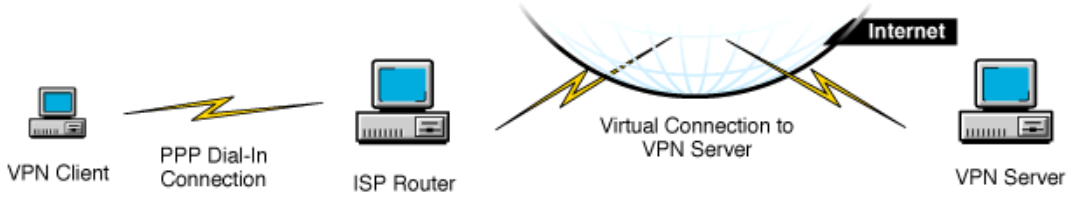
Using the Client to Dial In to an ISP and Connect to the VPN Server over the Internet

With this option, the client connects to the VPN server using the Point-to-Point Protocol (PPP) through an ISP, as shown in Figure 18, "VPN Client Using an ISP Connection," on page 239. Although using an ISP connection does not offer guaranteed bandwidth and could be slower than a direct dial-in connection, this option has the advantage of being less expensive than a direct dial-in connection. In addition to the cost of the phone line, a direct dial-in connection requires that you maintain a dial-up server, modems, and other related equipment.

If your ISP supports PPTP, the VPN client can use the PPTP to access the VPN server through an ISP connection.

Although Figure 18, "VPN Client Using an ISP Connection," on page 239 does not show that the VPN server is a member of a site-to-site VPN, VPN servers can support both client-to-site and site-to-site connections. If the VPN server is part of a site-to-site VPN, the client can also access all the other members of the site-to-site VPN and the networks that they protect. In addition, the site-to-site connections can be either Internet connections or intranet connections.

Figure 18 VPN Client Using an ISP Connection



To set up a VPN client to connect to the VPN server using PPP through an ISP,

1. Install and configure the VPN client.

   For detailed instructions, refer to Novell BorderManager 3.7 Install and Setup guide.

2. Configure the VPN server to support the VPN client.

   For detailed instructions, refer to Novell BorderManager 3.7 Install and Setup guide.

3. Configure IP routing on your network so that packets can return to the VPN client through the VPN server.

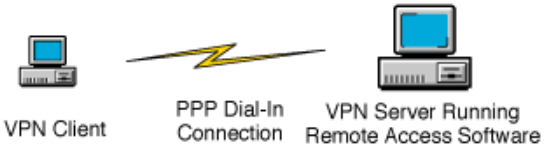
Using the Client to Dial Directly In to the VPN Server

With this option, the client uses PPP to dial directly in to the VPN server, as shown in Figure 19, “VPN Client Using a Direct Dial-In Connection,” on page 240. Although a direct PPP connection has guaranteed bandwidth, it is more expensive and might not be any faster than an ISP connection.

For some remote clients, a direct dial-in connection might be the only option available.

Although Figure 19, “VPN Client Using a Direct Dial-In Connection,” on page 240 does not show that the VPN server is a member of a site-to-site VPN, VPN servers can support both client-to-site and site-to-site connections. If the VPN server is part of a site-to-site VPN, the client can also access all the other members of the site-to-site VPN and the networks that they protect. In addition, the site-to-site connections can be either Internet connections or intranet connections.

Figure 19 VPN Client Using a Direct Dial-In Connection



To set up a VPN client to dial directly in to the VPN server, complete the following steps:

1. Install and configure the VPN client.

   For detailed instructions, refer to Novell BorderManager 3.7 Install and Setup guide.

2. Configure the remote access software.

   For detailed instructions, refer to the "Setting Up Remote Access on a VPN Server to Support Dial-In VPN Clients" on page 222.

3. Configure the VPN server to support the VPN client.

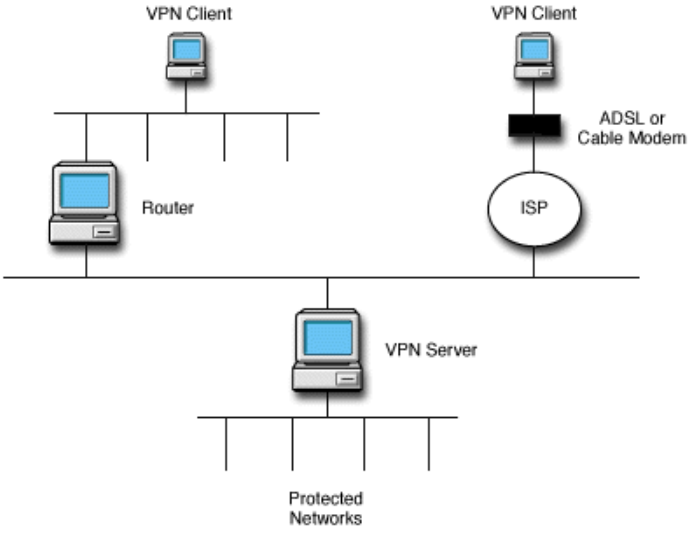
   For detailed instructions, refer to Novell BorderManager 3.7 Install and Setup guide.

Using the Client to Connect to the VPN Server over a Broadband Connection

With this option, the client accesses the VPN server through an ISP using a cable modem, an ADSL device, a LAN connection, or an established dial-up connection, as shown in Figure 20, "VPN Client Using a LAN Connection," on page 241. If it is available, a broadband connection is faster and less expensive than a dial-in connection.

Although Figure 20, "VPN Client Using a LAN Connection," on page 241 does not show that the VPN server is a member of a site-to-site VPN, VPN servers can support both client-to-site and site-to-site connections. If the VPN server is part of a site-to-site VPN, the client can also access all the other members of the site-to-site VPN and the networks that they protect. In addition, the site-to-site connections can be either Internet connections or intranet connections.

Figure 20 VPN Client Using a LAN Connection



1. Install and set up the VPN client.

   For detailed instructions, refer to Novell BorderManager 3.7 Install and Setup guide.

2. Set up the VPN server to support the VPN client.

   For detailed instructions, refer to Novell BorderManager 3.7 Install and Setup guide.

3. Configure IP routing on your network so that packets can return to the VPN client through the VPN server.

14 Managing Virtual Private Networks

The following sections describe the statistics used to monitor the operation of your Novell® BorderManager® 3.7 Virtual Private Network (VPN). It contains the following procedures:

Checking the Activity of a VPN Server

The VPN Member Activity window displays the real-time activity of a selected VPN member and its associated VPN tunnel connections for IP or the Internetwork Packet Exchange™ (IPX™) software.

There are two ways to display the VPN activity. If you select a slave server, both methods have the same capabilities: 1) From the VPN tab, and 2) From the Tools menu. If you select a slave server, both methods have the same capabilities. If you select the VPN master server, the first enables you to view connection information from the perspective of any VPN member, while the second enables you to view connection information only from the perspective of the master server.

IMPORTANT: To view the activity of any VPN server that is also a member of another VPN, you must go to the VPN server in your local VPN that is directly connected to that server.

Displaying the VPN Activity from the VPN Tab

To display the VPN activity using the first method, complete the following steps:

1. In NetWare Administrator, double-click a VPN server and select the Novell BorderManager 3.7 Setup page.
2. Click the VPN tab.
3. Double-click Master Site-to-Site or Slave Site-to-Site under Enable Service.
4. Click Status.

   For the master server, the screen displays the VPN's synchronization status, the progress of the master server updating all slave servers with the current VPN topology and encryption information. A server's synchronization status can assume one of the following states:

   - Up-to-Date—The server has been configured with the latest topology and encryption information. This state does not indicate that the server's VPN tunnel connections are up. Use the Activity display to determine the status of the VPN tunnel connections.
   - Being Configured—The server has not received the newest topology and encryption information from the master server.
   - Being Removed—The server is being removed from the VPN.

   NOTE: Any server state that remains at Being Configured or Being Removed for an extended period of time indicates a problem with the master server's ability to communicate with that VPN member. If a VPN member has been removed from the VPN, its state will remain at Being Removed as long as the master server cannot communicate with it. You can remove the VPN member from the Synchronization Status list by clicking Free VPN Member. For all other cases, view the audit log to troubleshoot the problem.
5. If you are viewing the status from the master server, click a VPN server.
6. Click Activity.
   - To check the activity between the selected VPN member and an associated connection, click the name of the associated connection in the Associated Connections window.

     This updates the IPX Associated Connection Details and the IP Associated Connection Details windows, and reflects the VPN tunnel activity information for this VPN member.

- To see the latest activity information, click Update.

  This updates the VPN Associated Connections window with the latest activity information. The monitor is automatically updated every 10 seconds.

Displaying VPN Activity from the Tools Menu

To display VPN activity only from the perspective of the server that you select, complete the following steps:

1. In NetWare Administrator, click the VPN server from whose perspective you want to view the activity information.
2. Select Novell BorderManager 3.7 from the Tools menu to open the Novell BorderManager 3.7 window.
3. Right-click Virtual Private Network and select View Member Activity/Log from the menu of options to view the VPN Activity window.

The VPN Activity Window

The following information is contained in the VPN Activity window:

- VPN Associated Connections—Displays the real-time activity of the currently selected VPN member and all associated VPN tunnel connections for either protocol (IPX or IP). The activity arrows are defined as follows:
  - Green Up-arrow—The encryption tunnel is currently active between the selected VPN member and the associated connection. This arrow indicates that packets have been received within the last 35 seconds.
  - Light Blue Up-arrow—The encryption tunnel is currently active and packets have been received from 35 to 70 seconds earlier.
  - Yellow Up-arrow—The encryption tunnel is currently active and packets have been received at one time, but not in the last 70 seconds.
  - Magenta Up-arrow—The tunnel connection was previously established and packets were received, but the connection is currently unattached.
  - Red Up-arrow—The encryption tunnel is in the process of being established.

- Red Down-arrow—The encryption tunnel is currently down between the selected VPN member and the associated connection. This arrow indicates that no packets were ever received. Check the audit log for both VPN members to determine why this encryption tunnel is down.

To view the activity between the selected VPN member and a particular associated connection, click the associated VPN member name in the VPN Associated Connections list. The IPX Associated Connection Details and the IP Associated Connection Details windows are updated to reflect the VPN tunnel activity information for this VPN member.

- VPN Tunnel Global Details—Displays the following global VPN connection information for the selected VPN member:
  - Tunnel Status—Whether the VPN tunnel is currently loaded or unloaded.
  - Tunnel Time Active—How long the VPN tunnel has been active.
  - Successful Client Connects—Total number of times a successful connection was made with a VPN client.
  - Failed Client Connects—Total number of times an attempt to make a connection with a VPN client failed.
  - IPX Packets Sent—Total number of encrypted IPX packets sent to all VPN members.
  - IPX Packets Received—Total number of encrypted IPX packets received from all VPN members.
  - IP Packets Sent—Total number of encrypted IP packets sent to all VPN members.
  - IP Packets Received—Total number of encrypted IP packets received from all VPN members.
  - Total Packets Sent—Total number of IPX and IP packets sent to all VPN members.
  - Total Packets Received—Total number of IPX and IP packets received from all VPN members.
  - Total Bytes Sent—Total number of bytes sent to all VPN members.
  - Total Bytes Received—Total number of bytes received from all VPN members.
  - Total Sent Packets Discarded—Total number of outgoing IPX and IP packets discarded.

- Total Receive Packets Discarded—Total number of incoming IPX and IP packets discarded.

- Associated Connection Details—Displays the following information about the tunnel connection between the selected VPN member and the associated VPN member:
  - Associated Connection—Associated VPN member's server name.
  - Associated Address—Associated VPN member's IP address. This is the configured public IP address.
  - Time to Disconnect—Amount of time left before the Disconnect Timeout expires and the VPN tunnel is disconnected if the connection remains inactive.
  - Send Key Changes—Number of times the outgoing data encryption key was changed.
  - Receive Key Changes—Number of times the incoming data encryption key was changed.
  - Total Bytes Sent—Number of bytes of encrypted IPX data sent to the associated VPN member.
  - Total Bytes Received—Number of bytes of encrypted IPX data received from the associated VPN member.
  - Sent Packets Discarded—Number of IPX and IP packets sent to the associated VPN member that were discarded.
  - Receive Packets Discarded—Number of IPX and IP packets received from the associated VPN member that were discarded.
- IPX Associated Connection Details—Displays the following information about the IPX tunnel connection between the selected VPN member and the associated VPN member:
  - Connection State—Current connection state with the associated VPN member. The connection states are defined as follows:

    Established—The connection has been established and packets have been sent and received.

    Pending—A call has been made, but no packets have been received from that member.

    Unattached—The connection has not been made or the WAN call terminated after the connection was established.

- Call Direction—Call direction for the associated VPN member. The call directions are defined as follows:

  Outgoing—For this connection, the selected VPN member initiated the call.

  Incoming—For this connection, the associated VPN member initiated the call.

- Time Active—Total amount of time this VPN tunnel connection has been active.
- Packets Sent—Number of encrypted IPX packets sent to the associated VPN member.
- Packets Received—Number of encrypted IPX packets received from the associated VPN member.

- IP Associated Connection Details—Displays the following information about the IP tunnel connection between the selected VPN member and the associated VPN member:
  - Connection State—Current connection state for the associated VPN member. The connection states are defined as follows:

    Established—The connection has been established and packets have been sent and received.

    Pending—A call has been made, but no packets have been received from that member.

    Unattached—The connection has not been made or the WAN call terminated after the connection was established.

  - Call Direction—Call direction for the associated VPN member. The call directions are defined as follows:

    Outgoing—For this connection, the selected VPN member initiated the call.

    Incoming—For this connection, the associated VPN member initiated the call.

  - Time Active—Total amount of time this VPN tunnel connection has been active.
  - Packets Sent—Number of encrypted IP packets sent to the associated VPN member.
  - Packets Received—Number of encrypted IP packets received from the associated VPN member.

To view the latest activity information, click Update. The VPN Associated Connections window is refreshed with the latest activity information. The monitor automatically refreshes every 10 seconds.

The Security Window

To view the encryption and authentication key parameters, click Security. The following information is contained in the Security window:

- Global Packets Per Key Change—Number of packets sent or received that will cause the data encryption key to change.
- Key Management—Protocol used for key management. Currently, only SKIP is supported.
- Send Encryption Type—Outgoing data encryption algorithm used.
- Receive Encryption Type—Incoming data encryption algorithm used.
- Encryption Send Key Size—Outgoing data encryption key length in bits.
- Encryption Receive Key Size—Incoming data encryption key length in bits.
- Send Authentication Type—Outgoing data authentication algorithm used.
- Receive Authentication Type—Incoming data authentication algorithm used.
- Authentication Send Key Size—Outgoing data authentication key length in bits.
- Authentication Receive Key Size—Incoming data authentication key length in bits.

Checking the Audit Log on a VPN Server

The VPN audit log enables you to view audit log messages generated by a VPN server. You can also view a detailed explanation of any message.

There are two ways to display the VPN audit log. Both methods have the same capabilities. Using either method from the master server, you can view the audit log of any slave server.

IMPORTANT: You cannot view the audit log of any VPN server that is also a member of another VPN. You can view the audit log of only those VPN servers that are exclusively members of your local VPN.

To display a VPN audit log using the first method, complete the following steps:

1. In NetWare Administrator, double-click a VPN server and select the Novell BorderManager 3.7 Setup page.
2. Click the VPN tab.
3. Double-click Master Site-to-Site or Slave Site-to-Site under Enable Service.
4. If you selected Master Site-to-Site, select a VPN member.
5. Click Status.
6. Click a VPN server > click Audit Log.

To display a VPN audit log using the second method, complete the following steps:

1. In NetWare Administrator, click a VPN server whose audit log information you want to view.
2. Select Novell BorderManager 3.7 from the Tools menu to open the Novell BorderManager 3.7 window.
3. Right-click Virtual Private Network and select View Member Activity/ Log from the menu of options to view the VPN Audit Log window.

   The Audit Log window is under the VPN Activity window.
4. Do one of the following:
   - To view the audit log for the selected VPN member, click Acquire.

     The latest audit log messages in the database are displayed. Only ten messages are visible at a time, with the most current (latest time stamp) message displayed first. Use the scroll bar or PageDown key to see earlier messages. By default, the latest 100 messages in the audit log database are acquired at a time.
   - To acquire the next set of audit log messages for the selected VPN member, click More.

     The next 100 messages in the database are displayed. Because only ten messages are visible at a time, use the scroll bar or PageDown key to see the rest. The More button is not available if no more audit log

messages are in the database. The More button does not emulate the screen settings. Changes made to the audit log controls take effect after you click Acquire. Only then does the More button use the current settings.

- To change the number of message entries to acquire at any one time, click the Up-arrow or Down-arrow in the Phase Entries control box.

  The new Phase Entries value is the number of audit log messages acquired the next time you click Acquire.

- To view additional information about a particular message, double-click the message or click Details.

  An explanation of the message is displayed. If the message is an error message, it also explains how to solve the problem.

The VPN Audit Log Window

The following information is contained in the VPN Audit Log window:

- Audit Log Provider—Allows you to choose which VPN software components will have their messages displayed.
- Selection Type—Allows you to choose which audit log message types to display.
- Audit Log Enable—Allows you to enable or disable the VPN audit log feature of the selected VPN member.

  If the check box is not selected, the VPN member stops saving VPN error and informational messages to the audit log database. This control feature takes effect only after you click Acquire.

- Audit Log Start and Audit Log End— Specifies a range of audit log messages to view based on date and time. The Audit Log End field specifies the most recent VPN messages saved in the audit log database. The Audit Log Start field specifies the earliest VPN messages saved in the audit log database. Use the Valid Audit Log Range group box to set the current range of the VPN audit log messages for the selected VPN member. Use the Up-arrow and Down-arrow to change the date and time for both controls.
- Audit Log Progress—Indicates the current progress of the audit log retrieval according to the defined settings.

- Audit Log Messages—Displays the audit log messages for each VPN member.

  Each message includes a time stamp indicating when the message was generated and the message type. There are four types of audit log messages: VPN Control, VPN Tunnel, SKIP, and IPSEC. VPN Control messages correspond to the VPN autoconfiguration process. VPN Tunnel messages correspond to the encryption tunnels established between VPN members. SKIP and IPSEC messages correspond to those two security protocols. Each audit log type is also categorized as either an error message or an informational message. The following types of messages are displayed:

  - Green T—Informational messages for VPN Tunnel.
  - Green C—Informational messages for VPN Control.
  - Green S—Informational messages for SKIP.
  - Green IP—Informational messages for IPSEC.
  - Red T—Error messages for VPN Tunnel.
  - Red C—Error messages for VPN Control.
  - Red S—Error messages for SKIP.
  - Red IP—Error messages for IPSEC.

Checking the VPN Real-Time Monitor

The VPN Monitor window displays the real-time activity of a selected VPN member and its associated VPN tunnel connections for IPX or IP.

To display the VPN Monitor window, complete the following steps:

1. In NetWare Administrator, click the VPN server from whose perspective you want to view the monitor information.
2. Select Novell BorderManager 3.7 from the Tools menu to open the Novell BorderManager 3.7 window.
3. Right-click Virtual Private Network and select Monitor Real-Time Activity from the menu of options to view the VPN Monitor window.

The VPN Monitor Window

The following information is contained in the VPN Monitor window:

- Active Connections—Number of currently active VPN connections.
- Remote Site—Location and ID of the remote VPN site.
- Connection ID—Connection ID for the VPN member.
- Connection Type—Whether the connection is for a dial-in client, LAN client, server, or third party.
- Bytes Sent—Number of bytes of encrypted data sent to the associated VPN member.
- Bytes Received—Number of bytes of encrypted data received from the associated VPN member.
- Duration—Total amount of time that the VPN tunnel connection has been active.
- Encryption Type—Type of data encryption algorithm being used.
- Key Size—Data encryption key length in bits.
- Key Lifetime—Duration of the current data encryption key.
- Key Changes—Number of times the data encryption key was changed.
- IP Packets Sent—Number of encrypted IP packets sent to all VPN members.
- IP Packets Received—Number of encrypted IP packets received from all VPN members.
- IPX Packets Sent—Number of encrypted IPX packets sent to all VPN members.
- IPX Packets Received—Number of encrypted IPX packets received from all VPN members.
- Authentication Type—Type of data authentication algorithm being used.
- Authentication Key Size—Data authentication key length in bits.
- Key Management Type—Protocol used for key management. Currently, only SKIP is supported.

Checking the Status of a VPN Client Connection

The VPN Status and VPN Statistics windows for VPN clients enable you to determine whether the client has established a connection with a VPN server and to monitor the activity over an established connection.

To check the status of a VPN client connection, complete the following steps:

1. After a VPN client connection has been initiated, click the VPN Status tab in the VPN Login dialog box.

   This window displays the progress of the VPN client connection.

   After the connection is established, the VPN Statistics icon is displayed in the task bar. Click on the icon to view the VPN statistics. The icon is available until the connection is closed.

2. To minimize the VPN Statistics window, click OK

3. To terminate the VPN connection, click Disconnect.

   On Windows NT* systems, you must terminate your dial-up VPN connection from this window. If you terminate your dial-up connection using Windows NT's Dial-Up Monitor, your VPN connection is maintained by the VPN server until the connection times out. This open connection cannot be used by other VPN clients and is not a security risk. However, an open connection reduces the amount of resources available to the server for VPN clients.

The VPN Client Status Window

The following information is contained in the VPN client Status window:

- Server Address—IP address of the VPN server to which the client is connected.
- Local Address—IP address of the VPN client.
- Server icon—Name of the VPN server to which the client is connected.
- Tree icon—Name of the NDS® or Novell eDirectory™ tree that contains the VPN server to which the client is connected.
- Status
  - Key Management—Protocol used for key management. Currently, only SKIP is supported.

- Encryption Type—Data encryption algorithm used by the VPN connection.
- Authentication Type—Data authentication algorithm used by the VPN connection.
- Encryption Key Size—Data encryption key length in bits.
- Authentication Key Size—Data authentication key length in bits.

- Progress
  - Dial-Up Complete—When checked, the dial-up connection to the VPN server has been established.
  - Authenticated NetWare User—When checked, the VPN Authentication has been completed.
  - Enabled IP Encryption—When checked, the encrypted tunnel has been established for IP packets.
  - Enabled IPX Encryption—When checked, the encrypted tunnel has been established for IPX packets.
  - Performing NetWare Login—When checked, you have been successfully logged in to NetWare.

The VPN Client Statistics Window

The following information is contained in the VPN client Statistics window:

- VPN State
  - Server IP Address—IP address of the VPN server to which the client is connected.
  - Local IP Address—IP address of the VPN client.
  - Time Active—Amount of time the connection between the VPN client and server has been active.
  - Key Management—Protocol used for key management. Currently, only SKIP is supported.
  - Encryption Type—Data encryption algorithm used by the VPN connection.
  - Authentication Type—Data authentication algorithm used by the VPN connection.
  - Encryption Key Size—Data encryption key length in bits.

- Authentication Key Size—Data authentication key length in bits.
- IP Encryption Enabled—Whether the VPN tunnel has been configured to encrypt IP packets.
- IPX Encryption Enabled—Whether the VPN tunnel has been configured to encrypt IPX packets.
- Disconnect Timeout—Amount of time the VPN tunnel can remain inactive before it is disconnected.
- Time to Disconnect—Amount of time remaining before the VPN tunnel is disconnected if no activity occurs.

- VPN Transfer
  - IPX Encrypted Packets Sent—Number of encrypted IPX packets sent from the VPN client on this connection.
  - IPX Encrypted Packets Received—Number of encrypted IPX packets received by the VPN client on this connection.
  - IP Encrypted Packets Sent—Number of encrypted IP packets sent from the VPN client on this connection.
  - IP Encrypted Packets Received—Number of encrypted IP packets received by the VPN client on this connection.
  - Unencrypted Packets Sent—Number of unencrypted packets sent from the VPN client on this connection.

    Even if the VPN client has been configured to encrypt all networks, the number of unencrypted packets sent or received might be a nonzero value. Unencrypted packets are used to bring up the encrypted tunnel itself. Although the packets are not encrypted using IPSEC, their contents are protected using Novell's proprietary protocol and encryption methods. The number of unencrypted packets should be less than 10 and should not increase after the tunnel has been established. If the value continues to increase, make sure that no other path from the protected network to the VPN client is shorter than the path through the tunnel. A shorter path can exist if another server on the protected network has a connection to the Internet. The number of unencrypted packets received is also increased by the receipt of broadcast packets from the Internet, such as BOOTP broadcast packets sent to clients.
  - Unencrypted Packets Received—Number of unencrypted packets received by the VPN client on this connection.

- Sent Packets Discarded—Number of IPX and IP packets sent from the VPN client on this connection that were discarded. The packets are sent by applications after the connection is established, but before the encrypted tunnel is brought up.
- Receive Packets Discarded—Number of IPX and IP packets received by the VPN client on this connection that were discarded. A nonzero value probably indicates decryption errors. Check the integrity of the line if a high value is displayed.
- Total Packets Sent—Total number of IPX and IP packets sent from the VPN client on this connection.
- Total Packets Received—Total number of IPX and IP packets received by the VPN client on this connection.
- Total Bytes Sent—Total number of bytes sent from the VPN client on this connection.
- Total Bytes Received—Total number of bytes received by the VPN client on this connection.

The More Window

The following information is contained in the VPN client More window:

- Server icon—Name of the VPN server to which the client is connected.
- Tree icon—Name of the NDS or eDirectory tree that contains the VPN server to which the client is connected.
- User Name—Client's NDS or eDirectory username.
- Context—Client's NDS or eDirectory context.
- Baud Rate—Speed at which the dial-up connection between the VPN client and Internet Service Provider (ISP) or VPN server is running.
- Protected IP Networks—Local IP networks or host addresses that can exchange encrypted data across the VPN.

Exporting Data

The VPN audit log is stored in a Btrieve* file on the Novell BorderManager 3.7 server and is maintained by CSAUDIT.NLM. The audit log cannot be edited or manipulated from the server; however, the data can be exported for analysis. The format of the exported data is compatible with popular trend analysis software packages, such as WebTrends*.

To export the VPN audit log, complete the following steps:

1. In NetWare Administrator, click the Server object representing the Novell BorderManager 3.7 server.
2. Select Novell BorderManager 3.7 from the Tools menu.
3. From the Novell BorderManager 3.7 menu, select Export Logs.
4. Click Set Range and enter the date range.

   This is the range of dates comparable to the dates used to display records in the VPN Users Statistics window. The default range is the current server date.
5. Click Browse to select the drive mapped to the destination for the export file.

   This is the path and filename for the export file. The default destination is A:\YYYYMMDD.LOG, where YYYY is the current year, MM is the current month, and DD is the current day. If you change the filename from the default format, the filename will not reflect the current server date. For example, if you change the filename format to MMDDYYYY.LOG, the next time you try to export logs on another day, the log filename will not have incremented to the current date.
6. (Optional) If the default filename is unacceptable, enter a new filename in the File field.
7. (Optional) If you want to combine the VPN audit log with audit logs from other Novell BorderManager 3.7 services, check the Combine Log Files check box.

   This feature allows log files from different Novell BorderManager 3.7 services to be combined into a single output file. When log files are combined, they are appended to one file, service by service.
8. Under Log Selection, check the VPN check box.

9. (Optional) If you checked Combine Log Files in Step 8, under Log Selection, check all other Novell BorderManager 3.7 audit log files to be combined with the VPN audit log file.

10. Click OK.

The audit log is exported to an ASCII file. VPN audit log entries are messages created by various processes and do not follow a fixed format. The messages will be copied to the export file without change.

If the Combine Log Files feature is *not* selected and you select one or more services under the Log Selection field, a separate export file is created for each service under a subdirectory of the export destination path.

The export subdirectories used are shown in the following table.

Log Type	Export Subdirectory
HTTP Proxy	HTTP
FTP Proxy	FTP
NNTP Proxy	NNTP
Mail Proxy	SMTP
RealAudio* and Real Time Streaming Protocol (RTSP) Proxies	RAUDIO
DNS Proxy	DNS
Generic Proxy	GENERIC
SOCKS Client	SOCKS
IPX Gateway (Novell IP Gateway)	IPXGW
VPN	VPN
ACL (access control)	ACL

For example, if you specified an export destination of VOL1:LOGS\19981019.LOG, did not select the Combine Log Files feature, and checked the boxes for HTTP proxy, FTP proxy, and VPN, the following logs would result:

- VOL1:LOGS\HTTP\19981019.LOG
- VOL1:LOGS\FTP\19981019.LOG
- VOL1:LOGS\VPN\19981019.LOG