

VERSION 3.5

Novell IP

Gateway Services



BorderManagerTM

ENTERPRISE EDITION 3

Novell[®]

disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

The Harvest software was developed by the Internet Research Task Force Research Group on Resource Discovery (IRTF-RD):

Mic Bowman of Transarc Corporation.
Peter Danzig of the University of Southern California.
Darren R. Hardy of the University of Colorado at Boulder.
Udi Manber of the University of Arizona.
Michael F. Schwartz of the University of Colorado at Boulder.
Duane Wessels of the University of Colorado at Boulder.

Copyright © 1994, 1995, Internet Research Task Force Research Group on Resource Discovery. All rights reserved. This copyright notice applies to software in the Harvest "src/" directory only. Users should consult the individual copyright notices in the "components/" subdirectories for copyright information about other software bundled with the Harvest source code distribution.

Copyright © 1999 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

U.S. Patent Nos. 5,553,139; 5,553,143; 5,572,528; 5,719,786; 5,758,069; 5,818,936; 5,903,650; 5,905,860. U.S. and Foreign Patents Pending.

**Novell, Inc.
122 East 1700 South
Provo, UT 84606
U.S.A.**

www.novell.com

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

**Novell IP Gateway Services
June 1999**

TERMS OF USE

The Harvest software may be used and redistributed without charge, provided that the software origin and research team are cited in any use of the system. Most commonly, this is accomplished by including a link to the Harvest Home Page (<http://harvest.cs.colorado.edu/>) from the query page of any Broker you deploy, as well as in the query result pages. These links are generated automatically by the standard Broker software distribution.

The Harvest software is provided “as is,” without express or implied warranty, and with no support nor obligation to assist in its use, correction, modification or enhancement. We assume no liability with respect to the infringement of copyrights, trade secrets, or any patents, and are not responsible for consequential damages. Proper use of the Harvest software is entirely the responsibility of the user.

DERIVATIVE WORKS

Users may make derivative works from the Harvest software, subject to the following constraints:

- You must include the above copyright notice and these accompanying paragraphs in all forms of derivative works, and any documentation and other materials related to such distribution and use must acknowledge that the software was developed at the above institutions.
- You must notify IRTF-RD regarding your distribution of the derivative work.
- You must clearly notify users that you are distributing a modified version and not the original Harvest software.
- Any derivative product is also subject to these copyright and use restrictions.

Note that the Harvest software is NOT in the public domain. We retain copyright, as specified above.

HISTORY OF FREE SOFTWARE STATUS

Originally we required sites to license the software in cases in which they were going to build commercial products/services around Harvest. In June 1995, we changed this policy. We now allow people to use the core Harvest software (the code found in the Harvest “src/” directory) for free. We made this change in the interest of encouraging the widest possible deployment of the technology. The Harvest software is really a reference implementation of a set of protocols and formats, some of which we intend to standardize. We encourage commercial reimplementations of code complying to this set of standards.

*export
notice*

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

trademarks

Novell, Inc. has attempted to supply trademark information about company names, products, and services mentioned in this manual. The following list of trademarks was derived from various sources.

LANalyzer, LAN WorkPlace, Novell, and NetWare are registered trademarks of Novell, Inc. in the United States and other countries. BorderManager, Client 32, ConsoleOne, Internetwork Packet Exchange, IPX, NASI, NCP, NDPS, NDS, NetWare 5, NetWare Asynchronous Services Interface, NetWare Connect, NetWare Core Protocol, NetWare/IP, NetWare Link Services Protocol, NetWare Loadable Module, NetWare MultiProtocol Router, NLM, NLSP, Novell BorderManager, Novell BorderManager FastCache, Novell Client, Novell Distributed Print Services, Virtual Loadable Module, VLM, and Z.E.N.works are trademarks of Novell, Inc.

AppleTalk is a registered trademark of Apple Computer, Inc.
Btrieve is a registered trademark of Pervasive Software, Inc.
Cyber Patrol is a registered trademark of Learning Company Properties, Inc.
CyberNOT is a trademark of Learning Company Properties, Inc.
CyberNOT List is a trademark of Learning Company Properties, Inc.
CyberNOT is a trademark of Learning Company Properties, Inc.
CyberYES List is a trademark of Learning Company Properties, Inc.
Hayes is a registered trademark of Hayes Microcomputer Products, Inc.
Java is a trademark of Sun Microsystems, Inc. in the United States and other countries.
JavaScript is a trademark of Sun Microsystems, Inc.
Macintosh is a registered trademark of Apple Computer, Inc.
Microsoft is a registered trademark of Microsoft Corporation.
NCSA is a registered trademark of Bales, Gates & Associates, Inc.
Netscape is a registered trademark of Netscape Communications Corporation.
Netscape Communicator is a registered trademark of Netscape Communications Corporation.
Netscape Navigator is a registered trademark of Netscape Communications Corporation.
OS/2 is a registered trademark of International Business Machines Corporation.
PS/2 is a registered trademark of International Business Machines Corporation.
Pentium is a registered trademark of Intel Corporation.
RealAudio is a registered trademark of RealNetworks, Inc.
RealPlayer is a registered trademark of RealNetworks, Inc.
RealVideo is a registered trademark of RealNetworks, Inc.
The Learning Company is a registered trademark of Learning Company Properties, Inc.
UNIX is a registered trademark of X/Open Company, Ltd.

USRobotics is a registered trademark of U.S. Robotics, Inc.
WebTrends is a trademark of WebTrends Corporation.
Windows is a registered trademark of Microsoft Corporation.
Windows 95 is a trademark of Microsoft Corporation.
Windows 98 is a trademark of Microsoft Corporation.
Windows NT is a registered trademark of Microsoft Corporation.
X Window System is a trademark of Massachusetts Institute of Technology.

The RSA logo is a trademark of RSA Data Security, Inc.



Contents

About This Guide

1 Managing the Novell IP Gateway

Setting Up Logging for All Gateway Services	1
Decoding Gateway Packet Traces	3
Checking Gateway Realtime Activity	3
Checking the Access Control Log.	4
Viewing User Statistics	4
Viewing Host Statistics	7
Exporting Data	9
Exporting Data from the IP Gateway Users Statistics Window	10
Exporting Data Using the BorderManager Pull-Down Menu	11
Checking the Information Log.	14

About This Guide

Novell® BorderManager™ Enterprise Edition 3.5 Installation and Setup provides the basic information you need to set up the Novell IP Gateway.

This documentation provides the following additional information: “Managing the Novell IP Gateway” on page 1—Describes the monitoring tools and log files that help you verify Novell IP Gateway performance.

X Novell IP Gateway Services

1 **Managing the Novell IP Gateway**

This chapter describes the tools and log files that help you manage the Novell® IP Gateway. It contains the following sections:

- “Setting Up Logging for All Gateway Services” on page 1
- “Decoding Gateway Packet Traces” on page 3
- “Checking Gateway Realtime Activity” on page 3
- “Checking the Access Control Log” on page 4
- “Viewing User Statistics” on page 4
- “Viewing Host Statistics” on page 7
- “Exporting Data” on page 9
- “Checking the Information Log” on page 14

Setting Up Logging for All Gateway Services

Logging can be enabled for all Novell® BorderManager™ 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, complete the following steps:

- 1. In NetWare® Administrator, select the BorderManager 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™ name, the access protocol (HTTP, for example), and the destination (www.novell.com, for example).
- 2—Error codes (NDS errors, for example). 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 BorderManager 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, complete the following steps:

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 BorderManager™ server.**
2. **Select Novell BorderManager 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™ services that enforce access rules, not just the Novell IP Gateway.

To check the access control log, complete the following steps:

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

Refer to the Access Control Services online documentation for information about the contents of the access control log.

Viewing User Statistics

To display user statistics in the Novell® IP Gateway audit log, complete the following steps:

1. **In NetWare® Administrator, click the Server object representing the BorderManager™ server.**
2. **Select Novell BorderManager 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™ 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 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 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, complete the following steps:

- 1. In NetWare® Administrator, click the Server object representing the BorderManager™ server.**
- 2. Select Novell BorderManager 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™ 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™ 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 10
- “Exporting Data Using the BorderManager Pull-Down Menu” on page 11

If you use the second method, you can combine the audit log files from other BorderManager 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 BorderManager server.**
2. **Select Novell BorderManager from the Tools menu.**
3. **Click IP Gateway and 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, and 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 and 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™ 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 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 BorderManager 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, complete the following steps:

- 1. In NetWare Administrator, click the Server object representing the BorderManager server.**
- 2. Select Novell BorderManager from the Tools menu.**
- 3. From the BorderManager 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 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 BorderManager services, check the Combine Log Files check box.**

This feature allows log files from different BorderManager 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 BorderManager 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 NDS 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™ services.

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

- 1. In NetWare® Administrator, click the Server object representing the BorderManager server.**
- 2. Select Novell BorderManager from the Tools menu.**
- 3. From the BorderManager 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 `SYSS$LOG.ERR` tab, you can view the system error messages recorded from the server console.

Note If you click the `SYSS$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.

