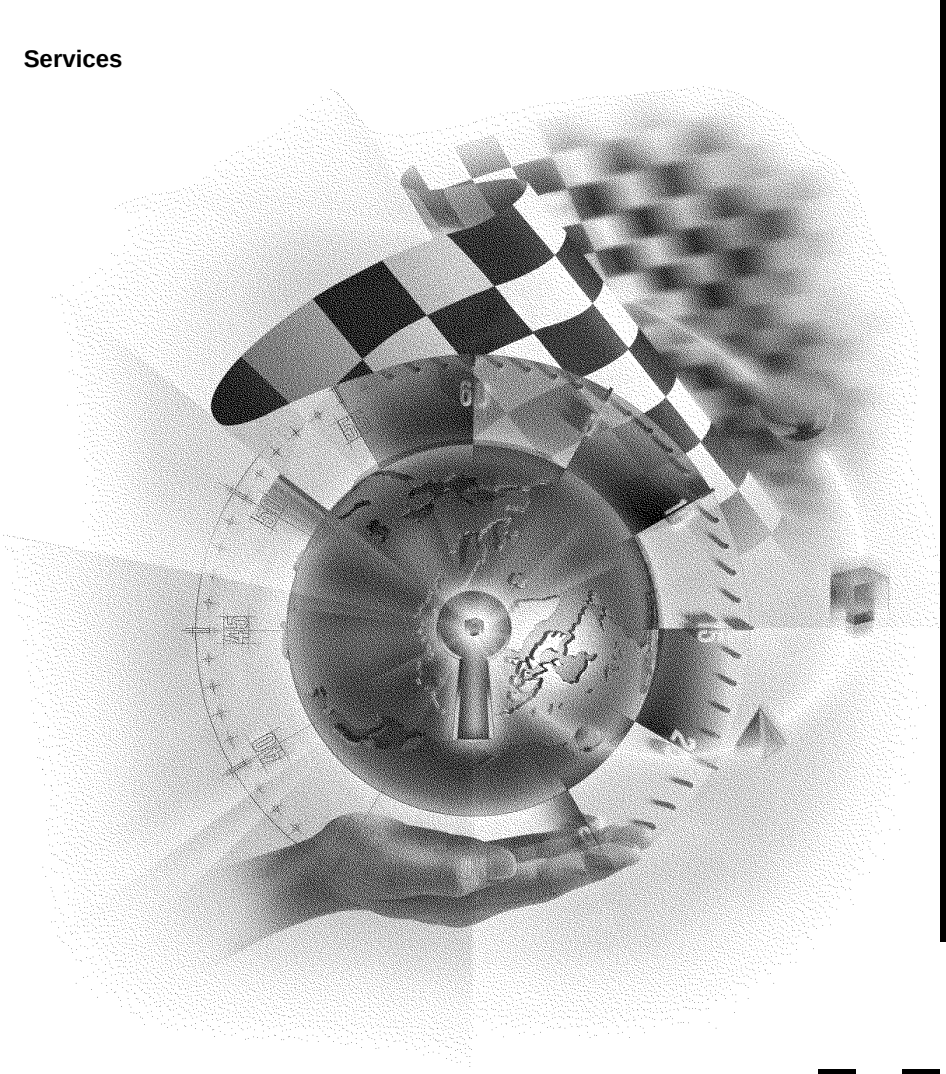
VERSION 3.5

Proxy

Services



BorderManager™

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.

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.

Proxy 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 reimplementation 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.

Contents

About This Guide

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

This documentation provides the following additional information:

- Chapter 1, “Advanced Configuration of Proxy Services,” on page 1

  This chapter 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 2, “Managing Proxy Services,” on page 13

  This chapter explains how to set up proxy logging and describes the information found in the Proxy Services logs.

chapter

1 Advanced Configuration of Proxy Services

This chapter contains the following procedures to enhance the Novell® BorderManager™ Proxy Services performance:

Configuring Cache Parameters

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

- “Configuring Cache Aging Parameters”

  This section includes configuration of HTTP, FTP, and Gopher revalidation times.

- “Configuring Cache Control Parameters”

  This section includes configuration of maximum cached file size and whether Java* applets are stripped from HTML files.

- “Configuring Cache Location Parameters”

  This section includes configuration of the cache directory and volume.

- “Configuring Cachable Object Control Parameters”

  This section includes configuration of noncachable URL patterns.

Configuring Cache Aging Parameters

To configure cache aging parameters, complete the following steps:

1. **In NetWare® Administrator, select the BorderManager 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 Control Parameters” on page 3 for more information.

4. **Click OK, then click OK again from the BorderManager 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, complete the following steps:

1. **In NetWare Administrator, select the BorderManager 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, then click OK again from the BorderManager Setup page.**

Configuring Cache Location Parameters

You can specify a different location for the cache.

To configure cache location parameters, complete the following steps:

1. **In NetWare Administrator, select the BorderManager Setup page for the server.**
2. **Select an HTTP or FTP proxy or acceleration service, then 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 BorderManager 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 BorderManager 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 BorderManager Setup page.**

Specifying Batch Downloading of Sites or URLs

Use batch downloading to keep the Novell® BorderManager™ 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, complete the following steps:

1. **In NetWare® Administrator, select the BorderManager Setup page for the server.**

2. **Select an HTTP proxy or acceleration service, then click Caching.**

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

4. **Click Add from the Download List and 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, then click OK again from the BorderManager 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® BorderManager™ 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 BorderManager 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 and check the Enable Cache Hierarchy Server check box.**

4. **Specify the following and 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 and check the Enable Cache Hierarchy Client check box.**

6. **Specify the following and click OK:**

   - 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 the Cache Hierarchy Routing tab and 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.

8. **Click OK, then click OK again from the BorderManager Setup page.**

Specifying Transport Timeout Parameters

You can fine-tune various transport-related timeout parameters that are used by the Novell® BorderManager™ 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, complete the following steps:

1. **In NetWare® Administrator, select the BorderManager Setup page for the server.**

2. **Click Transport, then 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, then click OK again from the BorderManager 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™ proxy server.

To change DNS parameters, complete the following steps:

1. **In NetWare® Administrator, select the BorderManager Setup page for the server.**

2. **Click DNS, then 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, then click OK again from the BorderManager Setup page.**

chapter

2 Managing Proxy Services

This chapter explains the tasks you complete to manage Novell® BorderManager™ Proxy Services. It contains the following sections:

Setting Up HTTP Proxy Services Logging

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

Important 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 *Novell® BorderManager™ Enterprise Edition 3.5 Installation and Setup* for more information.

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

1. **In NetWare® Administrator, double-click the Server object representing the BorderManager server and select BorderManager 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 BorderManager 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 BorderManager™ server.**

2. **Select Novell BorderManager from the Tools menu.**

3. **Click Proxy Cache and 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, 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 Proxy Cache and 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™ 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 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, then 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, 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 Proxy Cache and 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™ 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 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™ 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 BorderManager 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 BorderManager services with the proxy audit log into a single ASCII file.

For additional information, refer to:

- “Exporting HTTP Audit Log Proxy Records” on page 21
- “Exporting Audit Logs for All Other Proxies” on page 22
- “Export File Subdirectories” on page 23

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 BorderManager server.**
2. **Select Novell BorderManager 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 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™ 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 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 BorderManager 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 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 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 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 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, under Log Selection, check all other BorderManager 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 25
- “Exported FTP Proxy Data” on page 25
- “Exported NNTP Proxy Data” on page 26

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 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 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.