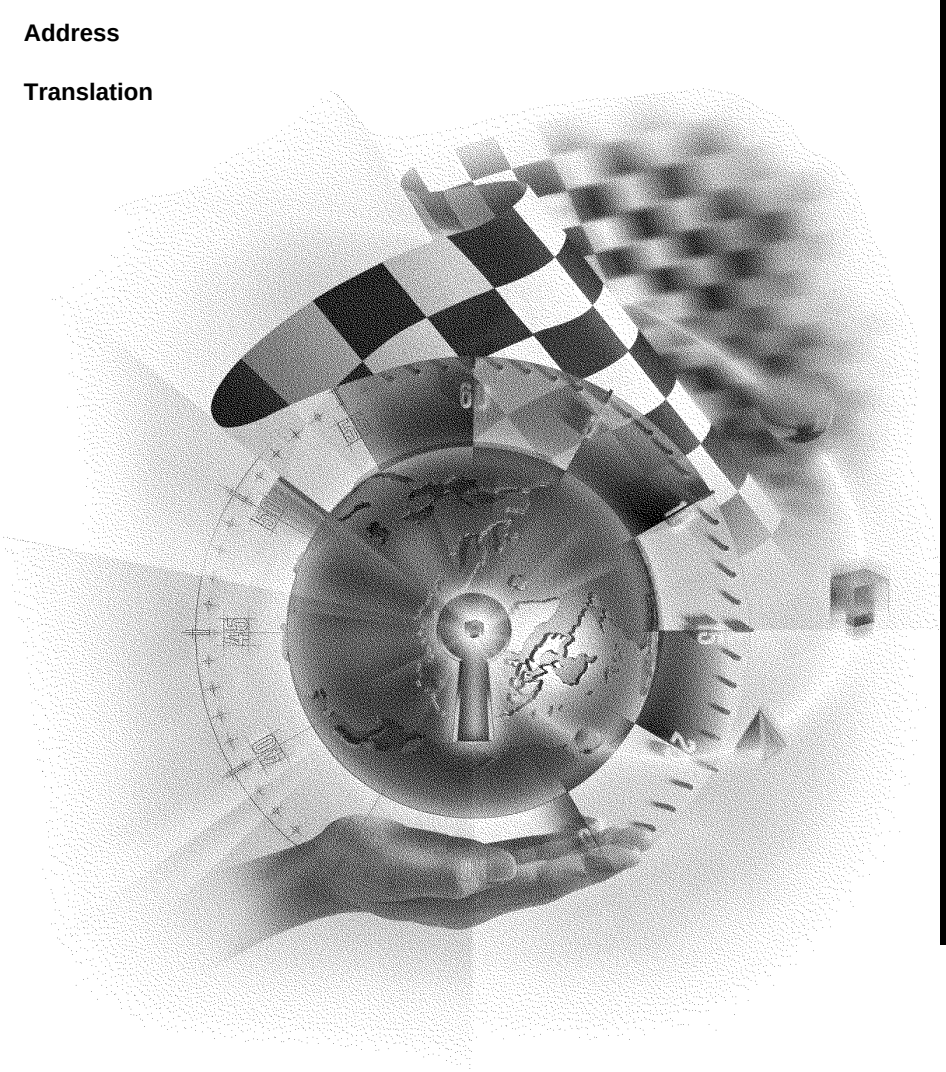
VERSION 3.5

Network Address Translation



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.

Network Address Translation
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 Network Address Translation (NAT).

This documentation provides the following additional information:

- Chapter 1, “Advanced Configuration of NAT,” on page 1

  This chapter describes the procedures you need to set up and configure various NAT features and parameters.

- Chapter 2, “Managing NAT,” on page 7

  This chapter describes tips and guidelines for monitoring NAT functionality.

chapter

1 Advanced Configuration of NAT

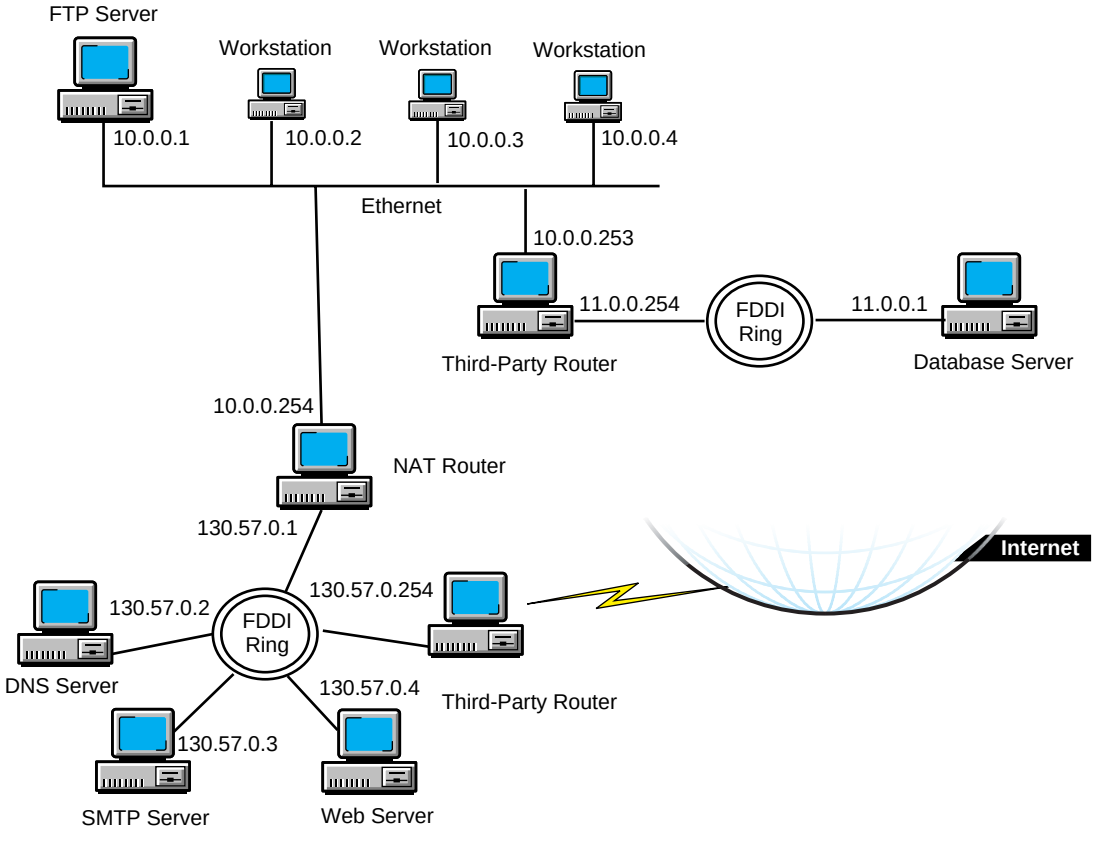
This chapter provides an example of using Novell® BorderManager™ Network Address Translation (NAT) in a private network when the network uses both registered and unregistered addresses.

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 Figure 1-1, 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 1-1

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, complete the following steps:

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, complete the following substeps:

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.

chapter

2 Managing NAT

This chapter provides tips and guidelines for managing Novell® BorderManager™ 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.
- After first loading TCPIP.NLM and then issuing 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.