Version 4.3.2
Part No. 310212-4.3.2 Rev 00
June 2003

600 Technology Park Drive
Billerica, MA 01821-4130

Release notes for Optivity NetID Version 4.3.2

NORTEL NETWORKS™

Copyright © 2003 Nortel Networks

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

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

Trademarks

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Java and Solaris are registered trademarks of Sun Microsystems, Inc.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

Netscape, Netscape Communicator, and Netscape Navigator are trademarks of Netscape Communications Corporation.

Norton AntiVirus is a trademark of Symantec Corporation.

Oracle and SQL*Plus are trademarks of Oracle Corporation.

Sybase is a trademark of Sybase, Inc.

UNIX is a trademark of X/Open Company Limited.

Restricted Rights Legend

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

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

Statement of Conditions

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

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

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. Optivity* network management software license agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying Optivity network management software or installing the hardware unit with pre-enabled Optivity network management software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License grant. Nortel Networks Inc. (“Nortel Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks’ and its licensors’ confidential and proprietary intellectual property. Licensee shall not disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee’s facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date the Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks Inc., 2375 N. Glenville Dr., Richardson, TX 75082.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Release Notes for Optivity NetID Version 4.3.2

These release notes apply to Version 4.3.2 of the Optivity® NetID product family, which includes the following server products:

- NetID Application Server
- NetID DHCP Server
- NetID DNS Server
- NetID Server Manager

The NetID product family also includes the NetID Management Console that you can run using a Java® compliant Netscape Communicator® or Microsoft® Internet Explorer Web browser.

These release notes contain the following information:

- "New features in the NetID product family" on page 9
- "Related publications" on page 13
- "How to get help" on page 14
- "System requirements" on page 15
- "NetID operating system and database compatibility matrix" on page 17
- "Guidelines for using NetID" on page 18
- "Electronic documentation" on page 28
- "Documentation changes" on page 30

New features in the NetID product family

The NetID 4.3-series product family includes the following new features:

- "Oracle 9i and Sybase 12.5 database component support" on page 10
- "Secure Socket Layer functionality" on page 10

- "Globally unique domain label creation" on page 10
- "DNS server is based on BIND 8.2.4" on page 11
- "Windows 2000 platform support" on page 11
- "Option 81 support" on page 11
- "DHCP client history reports" on page 11
- "ACL object access" on page 11
- "BIND statement validation" on page 12
- "Rotation of DHCP options" on page 12
- "Server metrics" on page 12
- "Enhanced trim log" on page 12
- "Command-line interface" on page 13
- "Memory optimization" on page 13
- "PXE client support" on page 13

Oracle 9i and Sybase 12.5 database component support

NetID 4.3.2 introduces support for the Oracle® 9i (release 2) and Sybase 12.5 database server components. The Oracle 8i (8.1.7) client kit or Sybase Open Client 11 remain as the only supported client kits.

Secure Socket Layer functionality

Secure Socket Layer (SSL) technology protects information passing between the management console and the Application server. SSL technology is supported by both Netscape Navigator and Microsoft Internet Explorer as a protocol for transmitting private information over the internet. For more information, refer to Appendix A in this manual.

Globally unique domain label creation

You can enforce globally unique domain labels created by DHCP autonaming or host templates. For more information, refer to "Globally unique domain label creation" on page 30.

DNS server is based on BIND 8.2.4

The NetID 4.3 DNS Server now supports BIND 8.2.4 under both Microsoft Windows® 2000 and UNIX (Solaris® and HP-UX®) operating systems.

Windows 2000 platform support

In addition to supporting dynamic DNS updates from a Windows 2000 environment, NetID 4.3 operates on Microsoft Windows 2000 Server.

Option 81 support

The NetID DHCP server supports the Client FQDN option (Option 81). This option allows a DHCP client that supports option 81 (Windows 2000 and XP clients) to suggest a domain label or a fully qualified domain name (FQDN) for itself when obtaining a lease, and to retain that label or FQDN if the client later acquires a different address. The DHCP server may also be configured to update the DNS server with some or all of the client's DNS information if it is requested by the client.

DHCP client history reports

You can track the movement of DHCP clients across subnets and networks with DHCP client history reports. A DHCP client history report can display what MAC address, client ID, IP address, FQDN, DHCP server, and IP address are used by each DHCP client. It also displays the time and date when this client information is assigned or changes.

ACL object access

Access privileges for NetID are set for NetID users (non-administrators) on a per-object basis. This allows NetID administrators to more precisely define what portions of the network users can access and what administrative tasks they can perform. The access privileges granted to NetID users are registered in an access control list stored in the NetID database.

BIND statement validation

BIND and NetID name server statements can be validated as they are entered through the Management Console. The BIND statement validation feature provides a predefined list of BIND and NetID name server statements that can be applied to name servers. When a name server statement from this list is selected, you enter the variable information required by a name server statement (such as channel types, IP addresses, or time) in the fields provided. The BIND statement validation feature ensures that the proper syntax, formatting, and parameters are used. This eliminates input errors that commonly occur when name server statements are manually applied to name servers. (For more information on enabling BIND statement validation, refer to "BIND statement validation is disabled by default" on page 31).)

Rotation of DHCP options

NetID DHCP servers can rotate IP address list type DHCP options to improve load balancing.

Server metrics

Optivity NetID can log a detailed account of server usage and performance. These server metrics allow you to analyze the performance of the Server Manager and the Application Server and to diagnose and resolve any problems you may encounter with them.

Enhanced trim log

Object history and server alarm logs can be trimmed according to a date or the number of records maintained, and the trims can be scheduled to automatically run at non-peak periods. In addition, object histories can be enabled for only specific objects. These changes improve NetID's memory usage.

Command-line interface

A command-line interface (CLI) utility is provided to allow the addition, deletion, modification of hosts, domain names, and resource records through a non-graphical client. The CLI utility is especially effective for performing batch operations when the network is not being extensively used.

Memory optimization

The architecture of the CORE layer has been reworked to enable faster caching of objects and a more efficient use of memory. A Memory Management feature has also been provided to assist enterprises with very large data sets. The Memory Management feature allows you to maintain an acceptable level of memory used for caching information by defining low, optimal, and excessive levels of memory usage. This feature also allows you to schedule when the level of memory usage should be examined, and when memory should be reclaimed from aged data structures.

PXE client support

A DHCP option (**`Boot File`**) is included to allow the support of PXE clients. The PXE protocol can be used to pass additional information between the client and server.

Related publications

For more information about using NetID, refer to the following publications:

- *Installing Optivity NetID* (part number 310209-4.3 Rev 00)

  Provides NetID administrators information about installing and configuring NetID software.

- *Managing IP Addressing in Optivity NetID* (part number 310210-4.3 Rev 00)

  Provides overview and procedural information for NetID administrators and NetID users about setting up and managing a system of IP addressing for a network, using DNS and DHCP.

- *Managing Optivity NetID Server Products* (part number 310207-4.3 (Rev 00)

  Provides NetID administrators information about starting, running, and stopping the Application Server, DNS server, DHCP server, and Server Manager.

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

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

How to get help

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

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

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

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

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

System requirements

Table 1 lists the system requirements for NetID products running on Windows 2000 systems. The latest patches for the operating systems supported by NetID must be installed to ensure that NetID products operate as designed.

Table 1 System requirements for Windows 2000

Product	**Platform/operating system**	**Software dependencies**	**RAM**	**Disk space**
NetID Application Server	Pentium® class PC Windows 2000 Server	Oracle 8.1.7 client kit Sybase® 11.9.2	256 MB	10 MB (executable size plus 5 MB for *core.dll*)
NetID DHCP Server	Pentium class PC Windows 2000 Server	not applicable	256 MB	10 MB
NetID DNS Server	Pentium class PC Windows 2000 Server	not applicable	256 MB	10 MB
NetID Management Console	not applicable	Netscape 4.7, JVM 1.1.5 Internet Explorer 5.5, Microsoft VM for Java 5.0.0	n/a	n/a
NetID Server Manager	Pentium class PC Windows 2000 Server	Oracle 8.1.6 or 8.1.7 client kit Sybase 11.9.2	256 MB	10 MB
Oracle Runtime Database	Pentium class PC Windows 2000 Server	not applicable	512 MB	500 MB plus 2 KB per IP address

Table 2 lists the system requirements for NetID products running on UNIX®. The latest patches for the operating systems supported by NetID must be installed to ensure that NetID products operate as designed.

Table 2 System requirements for UNIX

Product	Platform/operating system	Software dependencies	RAM	Disk space
NetID Application Server	Sun® UltraSPARC® Solaris 2.6, 2.8 or HP 9000/700 HP-UX® 11.0	Oracle 8.1 client kit Sybase 11.9.2	256 MB	65 MB plus room for any support files
NetID DHCP server	Sun UltraSPARC Solaris 2.6, 2.8 or HP 9000/700 HP-UX 11.0	not applicable	256 MB	10 MB
NetID DNS server	Sun UltraSPARC Solaris 2.6, 2.8 or HP 9000/700 HP-UX 11.0	not applicable	256 MB	10 MB
NetID Management Console	not applicable	Netscape 4.7, JVM 1.1.5 on Windows, HP-UX, and Solaris systems Internet Explorer 5.5, Microsoft VM for Java 5.0.0, on Windows 2000 systems	n/a	n/a
NetID Server Manager	Sun UltraSPARC Solaris 2.6, 2.8 or HP 9000/700 HP-UX 11.0	Oracle 8.1.7 client kit Sybase 11.9.2	256 MB	10 MB
Oracle Runtime Database	Sun UltraSPARC Solaris 2.6, 2.8 or HP 9000/700 HP-UX 11.0	not applicable	512 MB	500 MB plus 2 KB per IP address

NetID operating system and database compatibility matrix

Table 3 lists the operating systems and databases on which NetID 4.3.2 products will run. The latest patches for the operating systems supported by NetID must be installed to ensure that NetID products operate as designed.

Table 3 Operating system and database compatibility

Product	**Operating system**				**Database**						
	Windows NT 4.0	Windows 2000	Solaris	HP-UX	Oracle Client Kit 8.1	Oracle Database				Sybase Database	
						8.0.5	8.0.6	8i 8.1.7	9i (rel. 2)	11.9.2	12.5
NetID 4.2.1	SP6	SP1	2.6	11.0	NT, UNIX	NT	UNIX			NT, UNIX	
NetID 4.2.2	SP6	SP1	2.6	11.0	NT, UNIX	NT, 2000	UNIX	NT, 2000, UNIX		NT, 2000, UNIX	
NetID 4.3	SP6	SP2	2.6, 2.8	11.0	2000, UNIX			2000, UNIX		2000, UNIX	
NetID 4.3.2	SP6	SP3	2.6, 2.8	11.0	2000, UNIX			2000, UNIX	2000, UNIX	2000, UNIX	2000, UNIX

*Oracle 9i and Sybase 12.5 are supported as database components only and not as client kit components for the Application Server and Server Manager. The Oracle 8i (8.1.7) client kit or Sybase Open Client 11 remain as the only supported client kits.

Guidelines for using NetID

This section describes issues you may need to consider when using NetID.

Microsoft Virtual Machine

As of January 2004, Microsoft will no longer distribute or support the Microsoft Virtual Machine (VM) as part of the Microsoft Internet Explorer package. Instead, it will distribute the Sun Java Runtime Environment (JRE) with Internet Explorer. Because NetID 4.3.2 requires the Microsoft VM in order to run the management console through Internet Explorer, the Microsoft VM will be included with the NetID 4.3.2 install package for any customers who require it.

Because future versions of Internet Explorer will be distributed with the Sun JRE, it is important that the JRE be disabled on any system on which you plan to run the NetID management console (refer to "Disabling the SUN JRE" on page 18).

Disabling the SUN JRE

NetID has not been designed to support the SUN Java Runtime Environment (JRE). If you are running the NetID management console through Microsoft Internet Explorer on a system that has the SUN JRE installed, you should disable the JRE. To disable the JRE, follow these steps:

1. In Internet Explorer, click Tools > Internet Options.
2. In the Internet Options dialog box, click on the Advanced tab.
3. In the Settings list, scroll down to the Java (SUN) entry and disable the Use Java <*version_number*> For Applets check box.
4. Shut down and then restart Internet Explorer.

BIND statement validation cannot be enabled if forward or stub zones were set

`Zone type stub` or `zone type forward` statements that were manually set for name server objects (those displayed under the Name Servers root object, not under the Zones root object) in previous versions of NetID will not be considered valid by the BIND statement validation feature in NetID 4.3.2. Therefore, if you are migrating from a prior version of NetID to NetID 4.3.2 and you want to enable BIND statement validation, you must remove the `zone` statements from name server objects and set the zone type for that name server under the zone(s) for which it is associated.

To remove the `zone` BIND statements from a name server object, follow these steps:

1. Under the Name Servers root object, navigate to a name server for which `zone type stub` or `zone type forward` statements were previously set.
2. Right-click the name server object, and choose Properties from the menu.

   The Name Server Properties dialog box appears.
3. Click the BIND Statements tab.
4. From the list, delete the entire `zone` group.
5. Click OK.
6. Repeat these steps for each name server for which `zone type stub` or `zone type forward` statements were previously set.

   Once you remove the `zone` statements from all name server objects, you can enable BIND statement validation. (To enable BIND statement validation, right-click the System Options object, and choose Properties from the menu. In the System Options Properties dialog box, click the Admin tab, and enable the Validate BIND Statements check box).
7. To reset the zone type for those name servers, you must recreate the zone (follow the steps in “Creating a zone” in *Managing IP Addressing in Optivity NetID),* then add the name saver to that zone (refer to “Adding a name server to a zone” in *Managing IP Addressing in Optivity NetID.)*

   You can define the zone as a type forward or type stub when you add the name server to the zone.

Comment text in name server statements

Comment text must be placed before or after the group or statement portions of name server statements (BIND and those proprietary to NetID) to be properly validated by NetID.

The following example shows acceptable locations for comment text to be placed in relation to a name server statement group:

```
/* Acceptable comment location*/
options {
   also-notify {
      199.250.176.1;199.250.176.2;199.250.176.3;199.250.176.4;
   };
};
/* Acceptable comment location*/
```

The following example shows acceptable locations for comment text to be placed in relation to a name server statement:

```
options {
   /* Acceptable comment location*/
   also-notify {
      199.250.176.1;199.250.176.2;199.250.176.3;199.250.176.4;
   };
   /* Acceptable comment location*/
};
```

Reference counts in database tables serve as flags

The reference count fields in the NID_4DOMAIN and NID_4_IP_ADDRESS tables no longer count how many dependent objects there are. Rather, the reference counts now serve as flags: A value of 1 indicates that there are dependent objects, whereas a value of 0 indicates that there are no dependent objects. As a result of these changes, the *countcheck.sql* and *countfix.sql* scripts, which could be obtained from the Nortel Networks Technical Solutions Support Center, cannot be used for NetID 4.3.2.

Preparing NetID for Windows 2000 DDNS support

By default, the NetID DNS server is not configured to accept dynamic DNS (DDNS) updates from Windows 2000 servers. To enable DDNS updates from Windows 2000 servers, refer to the “Supporting Windows 2000 DDNS updates” section in *Managing IP Addressing in Optivity NetID.*

Importing Microsoft Active Directory DDNS-enabled zones

When you import a zone that contains Microsoft Domain Controller DDNS updates, the host name associated with the domain controller is randomly assigned because the primary domain name for the IP address is determined by the first A record encountered during the import. (This depends upon the order of zones in the *niddnsd.conf* file and the order of records in the zone file.) To resolve this problem, you can manually update the host name in the import file, or use the Management Console to set the IP address with the desired host name as primary before importing.

DDNS updates in a multiple master environment

If you are running multiple master DNS servers in the same zone, and both servers are configured to receive DDNS updates for the same zone, temporary discrepancies between serial numbers can occur between master servers as a result of DDNS updates on individual servers. These discrepancies can result in an `Unexpected SOA` message in the slave server's event log. The Server Manager should resolve these discrepancies over time.

If a master server receives a DDNS update while it is in the process of performing a zone transfer to a slave server, the zone transfer is halted. This results in a `premature EOF of <zone>` message in the slave server's event log. This should not affect server functionality.

Clearing the Sybase transaction log

If you are using a Sybase database, it is recommended that you modify and clear the transaction log before you perform a large data import or export. Failure to perform this maintenance task could result in the process running out of memory.

To clear the transaction log, follow these steps:

1. Run `isql`, and log in as **sa**.
2. Enter the following commands at the prompt:

```
sp_dboption <database_name>, “trunc log on chkpt”, true
go
```

3 Manually create a checkpoint for the database by entering the following commands at the prompt:

```
use <database_name>
go
checkpoint
go
```

4 Examine the size of the transaction log by entering the following commands at the prompt:

```
use <database_name>
go
dbcc checktable (syslogs)
go
```

The output will look similar to the following:

```
Checking syslogs
The total number of data pages in this table is 1.
*** NOTICE: Space used on the log segment is 0.00 Mbytes, 0.02%.
*** NOTICE: Space free on the log segment is 10.00 Mbytes, 99.98%.
Table has 23 data rows.
```

5 Manually truncate the transaction log by entering the following commands at the prompt:

```
use master
go
dump transaction <database_name> with truncate_only
```

If the dump transaction command is suspended (which can happen if the log is very full), you may need to enter the following command at the prompt:

```
dump tran <database_name> with no_log
```

6 Exit from `isql`.

7 Restart the database.

Disabling Oracle urgent data messages

To ensure that NetID runs properly when using a Solaris 2.6 Oracle Client Kit connecting to an Oracle database running on HP-UX, you must disable Oracle urgent data messages by editing the client’s *sqlnet.ora* file found in the *$ORACLE_HOME/network/admin* directory.

To disable urgent data messages, follow these steps:

1. Open the *$ORACLE_HOME/network/admin/sqlnet.ora* file.
2. Locate the following commented line within the file:

   ```
   #DISABLE_OOB=ON
   ```

3. Remove the initial # symbol to un-comment the line.
4. Save the file.

Note: If the *sqlnet.ora* file does not appear in the *$ORACLE_HOME/network/admin* directory, you can copy the file to this location from the *$ORACLE_HOME/network/admin/samples* directory.

Import utility

When you start an import process from the Management Console, you cannot use the Windows Task Manager to stop it.

During a DNS import, the Import utility ignores slave zones and sub-zones.

During any import, users other than those running the import may experience a slowdown in the performance of their Management Consoles.

Resource records and fully qualified domain names

NetID automatically changes domain name entries in resource records to fully qualified domain names (FQDNs).

DHCP server may not recognize multiple VLANs

If you install a VLAN card (NIC card) and its associated drivers on a system on which a NetID DHCP server already resides, the DHCP server may not recognize multiple VLANs. To run multiple VLANs and a DHCP server on the same system, install the VLAN card and its associated drivers before you install the DHCP server.

Duplicate entries in Sybase client pool table

If you are installing NetID 4.3.2 against an existing Sybase database, the Application server may occasionally generate an error message if it detects duplicate entries in the client pool, resource record, or name server zone tables. The messages are reported in the event log as they are detected by the Application server or Server Manager:

```
Attempt to add a duplicate object to the cache, type T, delta
identifier X.
```

The management console cannot display such duplicate entries. They can be corrected by using the management console to delete and re-create the entries.

Pipe character causes problems

The pipe character (|) causes data to be displayed incorrectly in the Java-based Management Console, because it is pre-defined as an illegal character for Java.

In addition, if you import a DNS database file that has comments within its name server statements, the import utility will process the name server statements until a | character in a comment is encountered; it will then skip the remaining name server statements and resume processing the DNS information in the zones section of the DNS database file. It is recommended that you remove any | characters from your name server statement comments before importing a DNS database file.

Spaces in file names cause problems for HP-UX systems

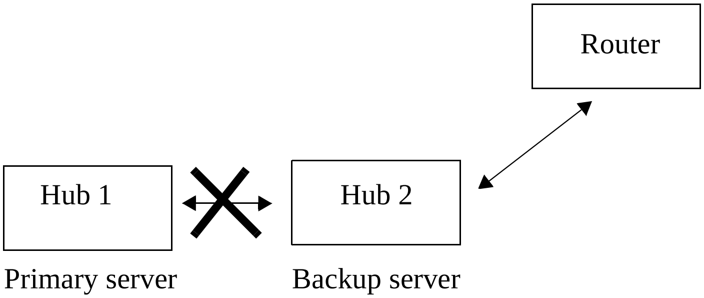
If you are using an Application Server that is running on an HP-UX system, you cannot import, export, or save a file with names that contains spaces. You also cannot save or use import, export, or report templates with names that contains spaces.

DHCP redundancy

If you are implementing DHCP redundancy, you should position your primary and backup servers to ensure that a network failure does not result in DHCP DISCOVER messages from the same subnet reaching both servers. Otherwise, both servers could begin to serve the same addresses at the same time.

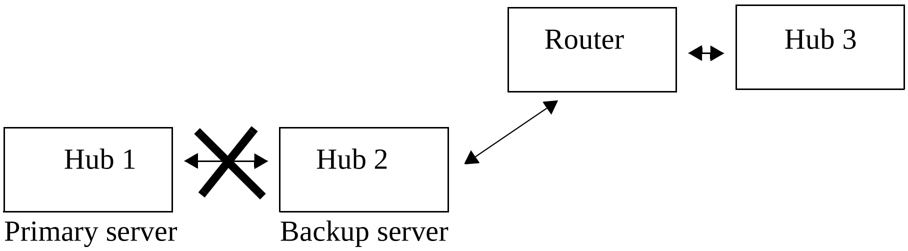
In Figure 1, a network failure between hub 1 and hub 2 would result in both servers serving the same addresses. To resolve this problem, it is recommended that you place the primary and backup servers on the same hub (in other words, place the backup server on hub 1).

Figure 1 Scenario 1: Network error



In Figure 2, a network failure between hub 1 and hub 2 would result in both servers serving the same addresses. To resolve this problem, it is recommended that you place the primary server on hub 2 or on a dedicated subnet.

Figure 2 Scenario 2: Network error



DNS server

If the BIND DNS server is running in the foreground, and you press [Ctrl]+C (send a `SIGINT` command), the process dumps the zones. Pressing [Ctrl]+C on any of the other servers (DHCP server, Server Manager, or Application Server) shuts down the process.

Oracle HTTP server

An Oracle 8.1.7 database installed on a Windows 2000 system will automatically run the Oracle HTTP server on port 80 when the system starts up. If you have also installed an Application Server on that system and it is configured to use port number 80, when you enter that system's URL in the Location or Address field of your Web browser you will connect to the Oracle HTTP server instead of the Application Server. Therefore, it is recommended that you use another port for the Application Server or use Windows Services to stop the Oracle HTTP server, and change its startup type from automatic to manual.

Management Console performance

The NetID Management Console is tested to run from both the Netscape Communicator and Microsoft Internet Explorer Web browser applications. Although the Management Console has been verified to run properly from both applications, its performance is better when run from Microsoft Internet Explorer.

The use of Norton AntiVirus® on the system from which you are running the Management Console may also reduce its performance when running from Netscape Communicator.

Running the Management Console from a Netscape 4.7.x Web browser on the same system as the Application Server to which it is connecting may reduce the Management Console's performance on a Windows 2000 system.

NetID administrators or NetID users will experience very slow response times from their Management Consoles if they are connecting to an Application Server that is processing a large commands file. It is recommended that commands files be processed during times when other NetID administrators or NetID users are not connected to the Application Server, or that an Application Server be dedicated for tasks performed by the CLI utility.

Changing a client's user class prior to IP address release

If you change the user class of a client without first releasing the client's IP address, when that client tries to renew its lease, its request will be ignored because it is for the renewal of an address in a range associated with its former user class. To ensure successful renewal of the client IP address, you must release the address before changing the client's user class.

Microsoft Windows 95 and Windows 98 (FE) DHCP clients

A Microsoft Windows 98 (First Edition) DHCP client will send a DHCP DECLINE packet to the DHCP server if it discovers that the IP address it is offered is already in use on the network. While the intent is to improve the handling of duplicate IP addresses in a pure Microsoft DHCP environment, the DHCP DECLINE packet lacks the Client ID in the DHCP Options field (as specified in RFC 2131), preventing proper processing by the NetID DHCP Server.

When multiple Windows 95 or Windows 98 FE DHCP clients disconnect from and reconnect to the network, a reconnecting client may receive a 'duplicate IP address' warning during the DHCP lease renewal process. Furthermore, because the Windows 98 client's DHCP DECLINE packet cannot be processed properly, the NetID DHCP Server will not have removed the client's previous lease from the database. In the case of the Windows 95 client, a DHCP DECLINE packet will not even be sent to alert the DHCP Server that it has discovered a duplicate IP address. In each case, the client is refused a new IP address.

Setting the Server Manager blocking threshold

If a database connection or a connection between NetID servers is blocked for some reason, the Server Manager will keep retrying the connection. However, a warning message is displayed when the data is being resent too many times. A sample message follows:

```
ConnectionWrite :: 20000 retries on connection to 47.130.101.202 on
port 34771. Continue retrying.
```

This message is displayed every 20,000 connection retries.

A retry threshold for the Server Manager can be set in the Windows registry, or in UNIX by modifying the *registry.cfg*, to close a problem connection when the threshold is reached. The syntax for this setting is:

```
SOFTWARE\Nortel Networks\NetID\CurrentVersion\Server
Manager\SMBlockedThreshold
```

For example, assigning a DWORD value of 10000 to this registry setting sets the threshold to 10,000, forcing a reset of the blocked connection after 10,000 retries. At each reset interval, a message is appended to the syslog as follows:

```
ConnectionWrite :: Blocking threshold (10000) surpassed
```

Electronic documentation

Documentation for NetID is available both online (through the Management Console) and in Portable Document Format (PDF). PDF documentation is available either on the system with installed documentation in the *<NetID_home>/docs* directory or from the www.nortelnetworks.com/documentation URL.

Viewing online Help

Viewing Web sites from an online Help window in Internet Explorer can cause an error in the online Help system. To go to a Web site during an online Help session, you must open a second Internet Explorer window.

If you open an online Help topic and minimize the Web browser window, then press another Help button, a new topic appears in the Help browser window, but the Web browser window remains minimized.

If you are using Netscape Communicator on a Solaris system, you may have difficulty viewing the NetID online Help. To resolve this problem, change the font configuration in Netscape Communicator by following these steps:

1. Start Netscape Communicator.
2. Choose Edit > Preferences.

   The Preferences dialog box opens.
3. In the Category list area, expand the Appearance object, and choose Fonts.

   The Fonts screen appears in the right pane.
4. From the For the Encoding list, choose Western (ISO-8859-1).
5. From the Variable Width Font list, choose Times (Linotype).
6. From the Variable Width Font Size list, choose 12.
7. From the Fixed Width Font list, choose Courier.
8. From the Fixed Width Font Size list, choose 12.
9. Click OK.

PDF documentation

Table 4 lists the NetID manuals available in PDF files.

Table 4 PDF files for NetID

File name	**Manual title**	**Product and topics**
anml.pdf	*Known Anomalies for Optivity NetID 4.3.2*	Known anomalies in NetID 4.3.2
relnotes.pdf	*Release Notes for Optivity NetID Version 4.3.2*	Release notes for NetID 4.3.2 (this document)
installguide.pdf	*Installing Optivity NetID*	How to install the entire NetID product family (requires administrator access)
ip_tutorial.pdf	*Learning IP Addressing in Optivity NetID*	A tutorial for using Optivity NetID from the Management Console

Table 4 PDF files for NetID (continued)

File name	Manual title	Product and topics
serverguide.pdf	*Managing Optivity NetID Server Products*	How to use the NetID server product family, including NetID Application Server, Server Manager, DHCP Server, and DNS Server (requires administrator access)
ipguide.pdf	*Managing IP Addressing in Optivity NetID*	Management Console Application Server Server Manager DHCP Server DNS Server Import, export, report, and ping audit utilities

Documentation changes

This section describes corrections and additions to the existing documentation for NetID.

Globally unique domain label creation

NetID includes a system setting that enforces globally unique domain labels created by DHCP autonaming or host templates. The setting also allows non-unique labels to be created manually or through DDNS. This allows Windows 2000 domain controllers to register themselves. To enable globally unique domain labels, follow these steps:

1. Under the Setup root object, right-click the System Options object, and choose Properties from the menu.
2. In the System Options Properties dialog box, click the Domains tab.
3. Enable the Domain Names Created with Autonaming Must Be Globally Unique check box.
4. Click OK.

BIND statement validation is disabled by default

Procedures in the “Configuring name servers” and “Managing DNS zones” chapters of *Managing IP Addressing in Optivity NetID* that describe how to set BIND or name server statements assume that BIND statement validation is enabled. However, by default, BIND statement validation is disabled to facilitate the migration of existing NetID 4.x data (refer to “BIND statement validation cannot be enabled if forward or stub zones were set” on page 18).

To perform these procedures, you must enable BIND statement validation or enter the BIND or name server statements manually (see below).

BIND statement validation is disabled by default to prevent users of prior versions of NetID from encountering errors when they upgrade to NetID 4.3.2. In prior versions of NetID, `zone type forward` and `zone type stub` were manually applied to name server objects (those displayed under the Name Servers root object). However, the BIND statement validation feature for NetID 4.3.2 does not consider a `zone` statement associated with a name server object as valid. In NetID 4.3.2, the role of master, slave, forward, or stub are predefined options that can be set for name servers that are associated with zones (those name server objects displayed under the Zones root object). Manually setting BIND statements for these name servers is unnecessary.

To enable BIND statement validation

1. Right-click the System Options object and choose Properties from the menu.
2. In the System Options Properties dialog box, click the Admin tab.
3. Enable the Validate BIND Statements check box.
4. Click OK.

Refreshing the display

You can choose View > Refresh to refresh the display in the Management Console. When you select this menu item, the information displayed below the selected root object is refreshed. To refresh the display for all the objects displayed in the Management Console window, you must select the company name, or top root object, in the tree area.

Setting the maximum number of database connections

If you manually set the server manager registry key `MaxDBConns` value (as outlined on page 48 of *Managing Server Products in Optivity NetID),* you must also update the server manager registry key `MaxWorkItems` to the same value.

Appendix A
Enabling Secure Socket Layer functionality

Optivity NetID uses Secure Socket Layer (SSL) technology to protect information passing between the management console and the Application server. SSL technology is supported by both Netscape Navigator and Microsoft Internet Explorer as a protocol for transmitting private information over the Internet. Security is maintained through the use of a key that encrypts data transmitted through the SSL connection.

In order for NetID to use SSL encryption, SSL certificates must be available in the `<NetID_HOME>\etc` directory. NetID installs the following files in the directory:

- `cacert.pem -` contains the public key information.
- `cakey.pem -` contains the private key information.
- `random.pem -` contains random information used by SSL.

These files are installed in a default state and do not offer unique authentication. You must create your own unique SSL certificates.

The Ping Audit, Import, Export, and Report tools will run in SSL mode without special configuration if the NetID management console connects to the Application server in SSL mode. To confirm this, look for the Lock icon at the bottom of your browser. Information about the certificate can be viewed by double-clicking the lock icon.

Creating SSL certificates

You can create an SSL certificate for Windows, Solaris, or HPUX. When creating a certificate, you must specify information that is specific to your company in the certificate. The SSL certificate certifies to a client connecting to the NetID Application server that it is, indeed connecting to the NetID Application server of your company.

This section covers the following subjects:

- “Creating a certificate for Windows” on page 35
- “Creating a certificate for HPUX or Solaris” on page 36

After you have created a certificate, the permissions on the SSL files `cacert.pem`, `cakey.pem` and `random.pem` are set to be read-only for the owner of the files on UNIX platforms. For NetID, the owner is the root user. These permissions are set as a security precaution. World readable permissions are not recommended for the key file (`cakey.pem`) because this file must be kept private.

The CLI tool is the only tool you can start in SSL mode, which means that the CLI requires access to the root-readable SSL files. You can run the CLI as root to have access to these files, but this is not very convenient. In order to allow a user with no root privileges to run the CLI, it is necessary to give this user read rights to these files. One way to achieve this is to create a UNIX group, assign group read permissions on the SSL files, and assign CLI tool users to this group. Write or Execute permissions are not required for these files.

One or more of the following error messages may be displayed if the rights of the user are not sufficient to access the SSL files when running the Application server or CLI tool.

- SSL: Certificate file `cacert.pem` is inaccessible or invalid
- SSL: Private key file `cakey.pem` is inaccessible or invalid
- SSL: Private key does not match the public certificate
- SSL: SSL_CTX_load_verify_locations error

If the Application server fails to start in SSL mode, it will shut down. However, if the CLI server fails to run in SSL mode, it will simply not accept any incoming connections.

Creating a certificate for Windows

In the *<NetID_HOME>*`\ssl` directory of your NetID install directory, you will find the files needed to create a self-signed certificate for your company:

- `certificate.bat` - a batch file that calls the `openssl.exe` tool to create or sign certificates.
- `libeay32.dll` - a dynamic link library required by `openssl.exe`.
- `ssleay32.dll` - a dynamic link library required by `openssl.exe`.
- `openssl.exe` - a configuration script used by `openssl.exe`.
- `openssl.exe` - the OpenSSL console tool.

The `openssl.exe` tool generates the files `cacert.pem` and `cakey.pem`. The contents of these files must not be edited directly. Nor should their names be changed. NetID specifically looks for these files when SSL is enabled.

To create a certificate and private key for Windows, follow these steps:

1 Open a DOS window on the computer on which you installed NetID.

2 From the `/ssl` sub-directory of your NetID install directory, type the following command:

```
certificate.bat
```

3 Enter the information requested by the tool.

4 You now have a private and a public key. The following files are generated and must be placed in the *<NetID_HOME>*`/etc` directory of any system on which the Application server or CLI client is installed:

- `cakey.pem`
- `cacert.pem`

Creating a certificate for HPUX or Solaris

In the *<NetID_HOME>*/ssl directory of your NetID install directory, you will find the files needed to create a self-signed certificate for your company:

- `ReadMe.txt` - instructions for creating a certificate and key using the command line.
- `openssl.cnf` - a configuration script used by `openssl*`.
- `openssl*` - the OpenSSL console tool.
- `.rnd` - a random file data file used by `openssl` to generate certificates

  The `openssl*` tool generates the files `cacert.pem` and `cakey.pem`. The contents of these files must not be edited directly. Nor should their names be changed. NetID searches for these files when SSL is enabled.

To create a certificate and private key for HPUX or Solaris, follow these steps:

1 Open a console, and navigate to the <*NetID_HOME>*/ssl directory.

2 To create the certificate/key pair, type the following command.

```
openssl req -config openssl.cnf -new -x509 -keyout
cakey.pem -out cacert.pem -days 365
```

The private key must be named `cakey.pem` and the certificate must be named `cacert.pem`.

a At the `CA certificate filename` prompt (or `enter to create` prompt), press [ENTER] to create a new certificate.

b Follow the on-screen instructions.

A private and a public key are generated.

3 Place the following lines in your *<NetID_HOME>*/etc directory.

- `cakey.pem`
- `cacert.pem`

Removing previous certificates

Before removing existing SSL certificates from your system, ensure that you do not require them for other applications. To remove certificates from your system, do the following:

➨ Open the *<NetID_HOME>*/ect directory and delete the following files:

- `cakey.pem`
- `cacert.pem`

Starting the Application server in SSL mode

On Windows, you can start the Application server in SSL mode by typing the following at the command prompt:

```
<NetID_HOME>/bin> nidappsv.exe -p 443
```

On UNIX, the root user can start the Application server by typing the following at the command prompt:

```
#./nidappsrv -p 443
```

The Application server must be started with the **`-p 443`** command parameter (which specifies port 443) to activate SSL. This parameter can also be set in the registry (or `registry.cfg` file on UNIX), either by specifying port 443 during the NetID installation, or by editing the Application server port number value in the existing key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Nortel Networks\NetID\CurrentVersion\
Application Server
```

NetID can only be configured to use SSL with this port number. If the Application server finds the necessary files for SSL (`cacert.pem`, `cakey.pem`, and `random.pem`) the server is started successfully in SSL mode. Otherwise it will not start.

Secure management console connection

To open a secure connection between the management console and the Application server, you must point the browser on which the management console is running to the following URL:

`https://`*`<application_server_address>`*

or

`https://`*`<application_server_address>`***`:443`**

Note: If the Application server is running in SSL mode, you MUST use the **`https://`** prefix in the browser when establishing a connection. You will need to edit the URL (to show the **`https://`** prefix) in the properties of the NetID management console shortcut to use it to establish a secure connection.

Microsoft Internet Explorer and Netscape Communicator interpret and process certificates differently, although the basic concepts are similar. To accept the certificate, follow the instructions provided by the Security Alert dialog box (in Internet Explorer) or the New Site Certificate dialog box (in Netscape). Both applications provide a simple wizard-type acceptance process.

The Command Line Interface

The CLI application must be started with the `-s` parameter to set the CLI in SSL mode. The CLI client displays certificate information when you connect to the Application server running in SSL mode. An Application server running at a debug level of 9 displays the CLI client connecting through an exportable cipher combination. You cannot connect to an Application server running in SSL mode without using the `-s` parameter.

The CLI client must have the same version of the files `cakey.pem` and `cacert.pem` as the Application server. The CLI user must have Read access to `cacert.pem`, `cakey.pem` and `random.pem`.