Release notes for Nortel Networks NetID Version 4.4

NORTEL
NETWORKS™

Copyright © December 2004 Nortel Networks

Trademarks

Restricted Rights Legend

Statement of Conditions

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. network management software license agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying network management software or installing the hardware unit with pre-enabled 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 Nortel Networks NetID Version 4.4

These release notes apply to version 4.4 of the Nortel Networks 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

The NetID 4.4-series product family includes the following new features:

- BIND 9.2.3 support: The NetID Name Server supports all BIND 9 directives, including Incremental Zone Transfer (IXFR). The BIND 9.2 code stream includes new functionality and enhanced security features. The NetID DNS server has been split into a NetID BIND Controller and a BIND 9.x-based Name Server. (Note: the IXFR directive is enabled by default on all Name Servers.)

- Secure DNS (DNSSEC) support.

- Enhanced CLI tool functionality: NetID 4.4 adds common user and administrator functions, including Add/Update/Delete of networks, subnets, and zones, as well as the addition of zones to Name Servers.

- Conformance with RFC 3011.

- Nortel DHCP options. A new Nortel vendor class with two pre-defined DHCP options (for Nortel IP phones and WLAN devices) are installed with the product.

- Support for global BIND statements.

- Support for global bookmarks.

Related publications

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

- *Installing Nortel Networks NetID* (part number 310209-4.4 Rev 00)

  Provides NetID administrators information about installing and configuring NetID software.

- *Managing IP Addressing in Nortel Networks NetID* (part number 310210-4.4 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 Nortel Networks NetID Server Products* (part number 310207-4.4 (Rev 00)

  Provides NetID administrators information about starting, running, and stopping the Application Server, BIND Controller, 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∗.

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 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

Product	Platform/operating system	Software dependencies	RAM	Disk space
NetID Application Server	Pentium®4, 1.4 GHz (or better) PC Windows 2000 Server or Windows 2003 Server	Oracle 9.2 client kit Sybase® 12.5 client kit	512 MB	15 MB
NetID DHCP Server	Pentium®4, 1.4 GHz (or better) PC Windows 2000 Server or Windows 2003 Server	not applicable	256 MB	10 MB
NetID DNS Server	Pentium®4, 1.4 GHz (or better) PC Windows 2000 Server or Windows 2003 Server	not applicable	512 MB	10 MB
NetID Management Console	not applicable	Netscape 7 series (on Windows or UNIX systems) or Internet Explorer 6 series (on Windows systems only) Sun JRE 1.4.2	n/a	n/a
NetID Server Manager	Pentium®4, 1.4 GHz (or better) PC Windows 2000 Server or Windows 2003 Server	Oracle 9.2 client kit Sybase® 12.5 client kit	512 MB	15 MB
Oracle Runtime Database	Pentium®4, 1.4 GHz (or better) PC Windows 2000 Server or Windows 2003 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® (or better) Solaris 2.8/2.9 or HP 9000/700 (or better) HP-UX® 11i	Oracle 9.2 client kit Sybase 12.5	512 MB	65 MB
NetID DHCP Server	Sun UltraSPARC (or better) Solaris 2.8/2.9 or HP 9000/700 (or better) HP-UX 11i	not applicable	256 MB	10 MB
NetID BIND Controller and Name Server	Sun UltraSPARC (or better) Solaris 2.8/2.9 or HP 9000/700 (or better) HP-UX 11i	not applicable	512 MB	10 MB
NetID Management Console	not applicable	Netscape 7 series (on Windows or UNIX systems) or Internet Explorer 6 series (on Windows systems only) Sun JRE 1.4.2	n/a	n/a
NetID Server Manager	Sun UltraSPARC (or better) Solaris 2.8/2.9 or HP 9000/700 (or better) HP-UX 11i	Oracle 9.2 client kit Sybase 12.5	512 MB	15 MB
Oracle Runtime Database	Sun UltraSPARC (or better) Solaris 2.8/2.9 or HP 9000/700 (or better) HP-UX 11i	not applicable	512 MB	500 MB plus 2 KB per IP address

Obtaining a license for Nortel Networks NetID

A 90-day license is supplied with NetID for installation, setup, and evaluation purposes. After this license expires, you will not be able to access NetID until you renew the license. To avoid this inconvenience, you should obtain a full license immediately after installation.

> ➡ **Note:** After completing the licensing procedure (for a new license or an upgrade license) you must log out of NetID and log back in to make the new license take effect. You must also stop and re-start the Application Server and Server Manager.

To obtain license keys for NetID, follow these steps:

1 Open your Web browser and go to the following URL:

http://www.nortelnetworks.com/ops_netidlicense

The NetID Licensing Web page appears.

2 Type your organization name, contact information, and address information in the appropriate fields.

3 Type the server key value in the Server Key field.

4 Type the serial number in the Serial Number field.

The serial number appears in the License Agreement supplied with the NetID CD package.

5 Click the Send button.

A license key and an expiry date are returned.

6 Type the new license key in the License Key field in the Update License dialog box.

7 Type the expiry date of the license in the Update License dialog box.

If an expiry date of `00/00/0000` is returned, enable the Unlimited option button. Otherwise, enable the Expires On option button, and type the date in the field in the format *YYYY/MM/DD*.

8 Click OK.

NetID operating system and database compatibility matrices

Table 3 and Table 4 list the operating systems and databases on which NetID 4.4 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-to-NetID version compatibility

Product	Operating system			
	Windows 2000	Windows 2003	Solaris	HP-UX
NetID 4.3	Yes(SP2)		2.6, 2.8	11.0
NetID 4.3.2	Yes(SP3)		2.6, 2.8	11.0
NetID 4.3.3	Yes(SP3)	Yes	2.8	11.0
NetID 4.4	Yes(SP3)	Yes	2.8/2.9	11i

Table 4 Database-to-NetID version compatibility

Product	Database								
	Oracle client kit		Oracle database					Sybase database and client kit	
	8.1	9.2	8.0.5	8.0.6	8i, 8.1.7	9i (rel. 2)	9.2	11.9.2	12.5
NetID 4.3	2000, UNIX				2000, UNIX			2000, UNIX	
NetID 4.3.2	2000, UNIX				2000, UNIX	2000, UNIX		2000, UNIX	2000, UNIX
NetID 4.3.3		2000, 2003, UNIX					2000, 2003, UNIX		2000, 2003, UNIX
NetID 4.4		2000, 2003, UNIX					2000, 2003, UNIX		2000, 2003, UNIX

Guidelines for using NetID

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

DNS zone serial numbers

With the introduction of the NetID 4.4 series, it is no longer possible for the user to edit the value in the Serial field for a DNS zone. Because NetID now uses DDNS updates to send changes to the BIND Name Server from the NetID BIND Controller, these DDNS updates also affects a zone's serial number. Allowing the user to modify zone serial numbers would cause problems with the synchronization of zone serial numbers.

Users will be able to migrate into a NetID 4.4 system with a data store that uses date-formatted serial numbers (yyyymmddxx) for their zones. The version 4.4 Name Server will treat date-formatted serial numbers as simple numbers and continue to increment these numbers with each DDNS update. The serial numbers will, for this reason, eventually lose their date-formatted appearance. As the number of updates moves into the 100's and 1000's, the day, month, and year columns will be overwritten as simple numbers.

Upgrading from NetID 4.3 series to NetID 4.4

It is advisable to back up your NetID tablespace before upgrading from a NetID 4.3 series product to NetID 4.4. There have been modifications to the version 4.4 database that would result in incompatibilities if you needed to revert to a NetID 4.3 series Server Manager or Application Server.

It is important that all NetID Application Servers and Server Managers are upgraded at the same time. The NetID 4.4 Server Manager will work with both version 4.4 and 4.3.x DNS and DHCP servers so that network server upgrades can take place incrementally.

Migrating from BIND 8 to BIND 9

The NetID 4.4 Name Server supports BIND 9.x directives, but will not support all BIND 8 directives, or any NetID 4.3.x proprietary directives. If you are not prepared to migrate your network immediately to BIND 9, you can run NetID 4.3.x servers in a NetID 4.4 environment.

The NetID 4.4 system continues to support NetID Name Servers based on BIND 8 in order to allow existing customers to upgrade their DNS deployments in a controlled manner.

For information on new functionality in BIND 9 and issues around integrating BIND 9 servers into your network, refer to:

- http://www.nominum.com/content/documents/bind9arm.pdf for BIND information
- http://sysadmin.oreilly.com/news/dnsandbind_0401.html for a discussion of important configuration considerations in upgrading from BIND 8 to BIND 9.

Unsupported BIND directives

The following BIND 8 directives and Nortel proprietary directives are not supported in BIND 9. If you are running a NetID 4.3 (or earlier) environment with any of the following directives, they must be removed or reset before you upgrade to the BIND 9 Name Server that is installed with NetID 4.4:

BIND 8 (not supported in BIND 9)	Nortel proprietary (not supported in BIND 9)
cachesize	cachedump-interval
check-names (supported in BIND 9.3)	persistent-cache
deallocate-on-exit	rr-allow
fake-iquery	secure-mail-addr
fetch-glue	secure-nameservers
has-old-clients	secure-recursive
host-statistics	secure-source
memstatistics-file	secure-ttl
min-roots	secure-zones

BIND 8 (not supported in BIND 9)	Nortel proprietary (not supported in BIND 9)
multiple-cnames	ddns-allow
named-xfer	
frc2308-type1	
rrset-order	
serial-queries	
statistics-interval	
topology	
treat-cr-as-space	
use-id-pool	

New syslog messages from BIND 9 Name Server

The NetID 4.4 Name Server logs a variety of new syslog messages which may be
unfamiliar to the user. Users can find explanations for (and discussions around)
many of these messages by searching for the message text at the
http://marc.theaimsgroup.com/ Web site.

DNS Export limitations

In exported DNS configurations, only the data in the database is exported, without
the modifications that the NetID BIND Controller needs to make locally in order
to function properly. Because the NetID BIND Controller needs to change the
BIND configuration in order to be able to control it, the configuration that is given
to Name Servers will be somewhat different from what users see in the
management console.

For example, the NetID BIND Controller depends on BIND allowing rndc
commands and DDNS updates (authenticated with HMAC-MD5 keys). This can
only be achieved by altering the configuration. Since these changes depend on the
local settings for each machine (the Server Manager doesn't handle the generation
or storage of HMAC-MD5 keys), they are not applied to the database but to the
machine were the DNS is running.

Users must address the following issues when exporting BIND 9 configuration
data from NetID 4.4:

- A `directory` statement must be added to the exported `named.conf` file to avoid a BIND 9 error. BIND 9 is significantly less tolerant of errors in the configuration file and will generally fail to start when they occur.

- NetID exports the Name Server configuration files with include statements like `include "pre.conf"`. For BIND 9, the full path to the included file must be specified (for example, `include "c:\Program Files\Nortel Networks\netid\dns\etc\pre.conf"`). They are not searched for in the directory specified by the `directory` statement.

- Signed zones and DNSSEC private keys are not stored in the database (only public keys are stored). An exported DNS configuration includes a `named-dnssec.dump` file, which includes the DNSSEC configuration used by NetID. The file can be imported back into NetID and the DNSSEC keys are re-created, but it cannot be used in a clean ISC BIND configuration. Signed zones cannot be exported together with the signature records, since those records are not stored in the database. The user can only export the zone in unsigned form (without NXT and SIG records). KEY records are not exported for the same reason (private keys are not kept in the database, and exporting private keys would not be secure). Public keys can be seen in the exported `named-dnssec.dump` file. When importing, if the `named-dnssec.dump` file exists, all DNSSEC configurations are imported, but the public keys and the tags of the key pairs are not imported. This leads to a full import of the exported DNSSEC configurations, but key pairs will be regenerated by the NetID BIND Controller when it configures the zones after import.

- A BIND 9 Name Server running with an exported configuration (slightly altered in order to make BIND start) will behave somewhat differently than a NetID-controlled BIND 9 server with regards to DDNS updates and rndc commands. In order to use rndc with the exported configuration, the user must manually add the `"controls"` section to `named.conf`.

> **Note:** Importing DNS configurations back into NetID 4.4 will work as expected.

Suggested changes to DNS architecture

In versions of NetID prior to the version 4.4 series, users were encouraged to use a multi-master zone structure (i.e. several master servers with few or no slave servers). This arrangement was suggested because of limitations in the master-slave update mechanism in earlier versions of BIND. With the improvements to Incremental Zone Transfer (IXFR) functionality in BIND 9, it is now feasible to configure additional Name Servers within a zone as slaves instead of as masters, in order to facilitate DNS updates.

Each zone should have two master Name Servers for redundancy purposes, but the rest of the servers in the zone can be slaves.

NetID 4.4 DNS directory structure and key management

This section outlines the new DNS directory structure and key management scheme implemented in version 4.4.

NetID DNS directories and files

The `<NetID_home>/bin` directory contains `nidnbc` (the NetID BIND Controller). This is a NetID process which starts and stops the BIND name server and manages the update process between the NetID database/NetID Server Manager and the BIND Name Server.

The `<NetID_home>/dns/bin` directory contains symbolic links to `opt/csw/sbin` for the following processes:

- `named` is the BIND Name Server daemon, the operation of which is controlled by the NetID BIND Controller.
- `rndc` is the administration utility for `named`, through which the user can issue command signals directly to the Name Server to reload zones, dump statistics, etc.
- `dnssec-signzone` is the DNSSEC zone signing tool.

`<NetID_home>/dns/etc` contains the following:

- The zone data files (`*.db`).
- The journal files (`*.jnl`) store changes to zone data that have occurred. This file is used mainly by the Name Server to implement the IXFR mechanism and by `nidnbc` to update NetID database.
- The `named.conf` file contains Name Server configuration statements. The `named.conf` file includes:
  - The `pre.conf` and `post.conf` files, through which the user can configure the Name Server with non-NetID managed BIND statements.
  - The `intern_pre.conf` and `intern_post.conf` files, which are used by NetID to define Global BIND Statements. Currently the NetID Server Manager is using only `intern_pre.conf` to define global ACLs.
  - The `intern_keys.conf` file (included in `intern_pre.conf`) is used by NetID to define keys used to secure internal server communications.
  - The `K*+xxx+xxxxx.key` and `K*+xxx+xxxxx.private` files store DNSSEC asymmetric keys, using BIND encoding.
  - The `rndc.conf` is the configuration file for the rndc utility. At install, a link to this file is created in `/etc/rndc.conf`.
  - A variety of other files: `*.old`, `named.pid`, `named.run`, and possibly some `*.tmp` files.

Control keys

The keys used to secure channels for communication with the BIND Name Server are HMAC-MD5 keys (symmetric keys, 128 bits in length). The command channel key is called `_nbc_command_channel_key_only_` and is used to establish a secure channel for the nidnbc CommandChannel module, which controls the functionality of the BIND Name Server, and is used to issue stop, halt, reconfig, and the Windows NetID Control Panel commands. This key is also used in the `rndc.conf` file for establishing the channel. In the `named.conf` file, this key is set as a control key through the following statement:

```
controls {
    inet 127.0.0.1 allow {any;} keys
{_nbc_command_channel_key_only_;};
};
```

The update channel key is called _nbc_update_channel_key_only_ and serves to establish a secure channel for the nidnbc UpdateChannel module, which sends updates to the BIND Name Server via DDNS. In named.conf, this key is set on all Master-type zones by one of the following methods:

1 Through an update-policy directive:

```
update-policy {
grant _nbc_update_channel_key_only_ wildcard * ANY;
grant * name omihnea.itcnetworks. ANY;
};
```

2 Through an allow-update directive:

```
allow-update { key _nbc_update_channel_key_only_; 127.0.0.1;Any; };
```

The update-policy directive is more secure but is only useful when TSIG is supported by all entities that can update the zone. Microsoft Active Directory Domain Controllers do not support TSIG, so the allow-update directive is used to set access control on zones when ACLs are configured through the NetID Global BIND Statements feature.

Key generation

During the NetID installation process, a default set of keys is created in the intern_key.conf file. Any time that configuration is sent to the BIND Name Server (for example, when the BIND Controller contacts the Server Manager and requests the Name Server's configuration files), these keys are recreated and stored with Base 64 encoding. The keys are generated using the operating system's random number generator device, which produces the raw material for the keys. NetID simply encodes and stores them.

Obtaining Oracle database software

The Oracle 9i database and client kit software supported by NetID can be obtained from the following locations:

- http://www.oracle.com/technology/software/products/oracle9i/htdocs/winsoft.html
- http://www.oracle.com/technology/software/products/oracle9i/htdocs/solsoft.html

• http://www.oracle.com/technology/software/products/oracle9i/htdocs/
hpsoft.html

Memory settings on HP-UX

If you are encountering "unknown exception" messages on HP-UX and there is no apparent reason for these exceptions, it may be worthwhile to check the maxdsiz parameter and set it to a larger value. The maxdsiz parameter is the kernel parameter on HP-UX that specifies the maximum size for a process data segment, and is set by default to 64MB. While this value is sufficient in most cases, the loading of large DNS zones has on occasion been shown to exceed this limit. When the limit is reached, the Server Manager receives an "unknown exception" message and disconnects the BIND Controller.

To fix this problem, you must run the System Administrator Manager (SAM) utility on HP-UX (as root, with the DISPLAY environment variable set to a valid X server). Select Kernel Configuration, and then select Configurable Parameters. Scroll down the list to find maxdsiz. Double-click on this entry and enter a new value in bytes (for example, 256 MB or 256 x 1024 x 1024 = 268435456 bytes). Then close the window and SAM will prompt you to either compile the new kernel and replace the old one immediately, or wait. Choose the option to recompile right away. After the kernel has recompiled, the system will restart with the new kernel.

Running NetID BIND Controllers on HP-UX

If you are running NetID Name Servers on HP-UX 11i, you may encounter repeated instances of a "no source of entropy found" error message in the syslog file. In order to stop this error message from appearing, the NetID 4.4 BIND Controller requires the installation of a secure random number generator on HP-UX 11i. The secure random number generator is used in the DNSSEC encryption mechanism. This application can be installed from:

http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/
displayProductInfo.pl?productNumber=KRNG11I.

Popup disabling software blocks Import/Export/Report status applets

If you are running popup blocking software on your Web browser, you will not be able to view the status messages generated by the Import, Export, and Report utilities. In order to view the messages, you can configure your popup disabling software to accept popup messages originating from the NetID Application server address.

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. NetID 4.4 supports the Sun Java Runtime Environment (JRE) with Internet Explorer.

Enabling the SUN JRE

NetID has been designed to support the SUN Java Runtime Environment (JRE). If you are running the NetID management console through Microsoft Internet Explorer, you must ensure that the SUN JRE (version 1.4.2 or later) is installed and enabled on the same system. The JRE can be installed from the NetID install CD (\auxiliary folder).

For information on upgrading the Sun JRE, refer to:

http://java.com/en/download/help/switchvm.jsp

To enable 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 enable the Use Java *<version_number>* For Applets check box.

4 Shut down and then restart Internet Explorer.

Internet Explorer security warning

Opening the management console in Microsoft Internet Explorer using default security settings could result in the following warning message:

```
Your current security settings prohibit running Active X
controls on this page. As a result, the page may not display
correctly.
```

If you see this warning, you will have to change your Internet Explorer security setting to Medium. For more information, refer to the Internet Explorer documentation.

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 4.4. Therefore, if you are migrating from a prior version of NetID to NetID 4.4 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 Nortel Networks NetID)*, then add the name saver to that zone (refer to "Adding a Name Server to a zone" in *Managing IP Addressing in Nortel Networks 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 NID4_DOMAIN and NID4_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 4.4.

Preparing NetID for Windows DDNS support

By default, the NetID Name Server is not configured to accept dynamic DNS (DDNS) updates from Windows 2000 or Windows 2003 servers. To enable DDNS updates from Windows servers, refer to the "Supporting Windows DDNS updates" section in *Managing IP Addressing in Nortel Networks 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 *named.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 Name 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 4.4 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
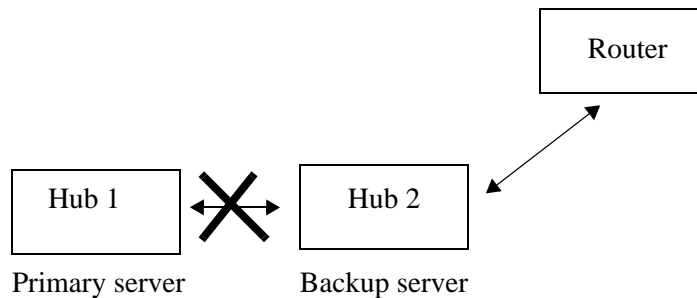
In Figure 2, a network failure between hub 1 and hub 2 would result in both servers serving the same addresses. To resolve this problem, it is recommended that you place the primary server on hub 2 or on a dedicated subnet.

Figure 2 Scenario 2: Network error
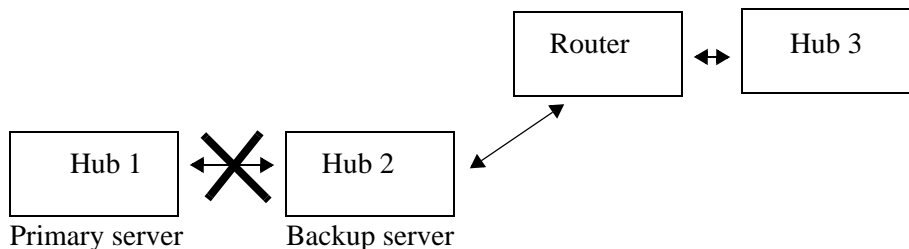
Oracle HTTP server

An Oracle 9.2 database installed on a Windows 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 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 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 5 lists the NetID manuals available in PDF files.

Table 5   PDF files for NetID

File name	Manual title	Product and topics
relnotes.pdf	*Release Notes for Nortel Networks NetID Version 4.4*	Release notes for NetID 4.4 (this document)
installguide.pdf	*Installing Nortel Networks NetID*	How to install the entire NetID product family (requires administrator access)
serverguide.pdf	*Managing Nortel Networks 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 Nortel Networks NetID*	Management Console Application Server Server Manager DHCP Server DNS Server Import, export, report, and ping audit utilities

Known Limitations and Considerations

Open issues

This section covers known issues and limitations with the Version 4.4 release of Nortel Networks NetID. When applicable, workarounds are suggested for each issue. This section is organized under the following categories:

- "Installation" on page 37
- "Application server" on page 38
- "Server Manager" on page 38
- "BIND Controller" on page 38
- "Management console" on page 39
- "Export utility" on page 39
- "Import utility" on page 40
- "Ping audit utility" on page 40
- "Migration" on page 40

Installation

- (Q00082884) If you install NetID 4.3 over an existing installation of NetID 4.2.x, some NetID 4.2.x information is not removed. (For example, if you click the Start menu on Windows 2000, then choose Programs > NetID, there may be duplicate entries.)

  Workaround: If you are upgrading from an earlier version of Nortel Networks NetID to 4.4, install NetID 4.4 to a new directory or remove the previous installation before upgrading.

Application server

- (Q00039134) If the database is taken offline using the Oracle Storage Manager while the Application server is running, and then you attempt to log in to the Management Console, you receive a message stating that there is a problem with the user ID or password.

  However, if you are already logged in to the Management Console when you take the database offline using the Storage Manager, and then you attempt to modify the database, you receive an error stating that the current action has created a conflict or that the changes cannot be saved.

- (Q00024884) When a DDNS static host is committed to a dynamic range, a subsequent DHCP request coming into the DHCP Server serving the range may result in the replacement of the DDNS host with the DHCP client.

  Workaround: Avoid the creation of static hosts on dynamic ranges through DDNS.

- (Q00138539) It is not possible to create a Key ID and an ACL with identical names in the same BIND match list.

Server Manager

- (Q00462164) If you have set Option 81 (allowing client FQDNs) on a dynamic range, non-existent (in NetID) domain names could be admitted to the domain tree. This could result in the accumulation of superfluous information in the domain tree.

  Workaround: If you are using Option 81 on a dynamic range, you must take care to set DHCP client domain names accurately.

- (Q00103080) When you are configuring a Sybase client kit on a Solaris® system to connect to the Sybase server, you cannot use a domain name to identify the Sybase database server.

  Workaround: Use the IP address instead of a domain name.

BIND Controller

- (Q00972702) If the BIND process is down, the ASM icon for DNS still appears as connected because the NetID BIND Controller is connected.

• (Q00985991-01) Intermittent service loss on DHCP Servers, relating to the manner in which the DHCP Server is interfacing with the DNS resolver routines. This problem only occurs if the DHCP Servers are sending DDNS updates to Name Servers.

Management console

• (Q00107540) If you make a change to an object in the NetID hierarchy (for example, a dynamic range) that had a user or vendor class associated with it, but that user or vendor class has since been deleted, an error message that the deleted option is still associated with that object appears.

  Workaround: In the Properties dialog box for the object, click the DHCP options tab. Select the vendor or user class option, and click the Remove button.

• (Q00107530) If a Server Manager that is connected to an active DNS or DHCP Server goes offline, the status of the DNS or DHCP Server's connection to that Server Manager is not changed from "Connected" to "Disconnected" in the list area of the Management Console.

• (3984) Under Openwin on Solaris, you need to resize the window before you can see the icons or tree area.

• (4226) The DHCP Server does not allow multiple hosts with the same hardware or client IDs on the same subnet. All client IDs on a subnet (including hosts on ranges in the subnet) and all entries with only hardware IDs must have unique hardware IDs.

Export utility

• (4086, 3533) There are a number of inconsistencies in the format of information in database files exported using a DNS export. These inconsistencies include the following:

  In the database files for *reverse* lookup zones, $origin appears at the beginning of the file, but all of the records are still in fully qualified domain name format.

  In the database files for *forward* lookup zones, there is no $origin, and all of the records are in fully qualified domain name format.

- (5869) If the Management Console is idle for a greater part of the expire time, and then you perform a task, the new information is added to the database. But if you try to perform another task after the expire time has passed, Netscape may not respond to the request.

  Workaround: Close Netscape Communicator® and launch it again.

Import utility

- (3486) Some of the illegal characters in domain names cause problems (such as line breaks in odd places) with viewing or importing data in the GUI.
- (3508) After you import a resource record that contains a back-slash character ("\"), it is not possible to update the domain name in the Management Console.

  Workaround: Log out of the Management Console and log in again.

Ping audit utility

- (Q00072400) When a ping audit is run from the Management Console, there is a slight delay before the Web browser window that displays the ping audit results launches. Therefore, some of the results of the ping audit are not displayed in that Web browser window, even though all of the host addresses were pinged. In addition, if you run a ping sync to resolve the results of the ping audit, there is a slight delay before the Web browser window that displays the ping sync results launches. Therefore, some of the results of the ping sync will not appear in the Web browser results window, even though all of the appropriate host addresses will be added or deleted.

Migration

- (Q00285595-01) The NID4_HISTORY table is not built with TTL and FLAGS columns when migrating from the NetID 4.2-series product to the NetID 4.3-series product. This is not really a problem because the TTL and FLAGS columns are utility columns intended to make delta processing faster. They are not actually used for the history table.