Version 4.3.2
Part No. 310211-4.3.2 Rev 00
June 2003

600 Technology Park Drive
Billerica, MA 01821-4130

Known Anomalies for Optivity NetID 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.

Solaris is a registered trademark 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.

Oracle is a trademark 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.

Known Anomalies in Version 4.3.2

This document provides additional information to the *Release Notes for Optivity NetID Version 4.3.2*. The sections that follow describe the known anomalies in Version 4.3.2 of the Optivity® NetID product family and, when applicable, suggested workarounds.

NetID installation

Anomaly:	**Installing NetID 4.3 over a previous NetID 4.2.x installation does not remove all 4.2.x install information from the system**
Number:	Q00082884
Description:	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 Optivity NetID to 4.3.2, install NetID 4.3.2 to a new directory or remove the previous installation before upgrading.

Application server

Anomaly: **Upon taking the database offline with the Oracle Storage Manager, and either trying to log in to the Management Console or modify the database, the Application server reports an error**

Number: Q00039134

Description: 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.

Anomaly: **A DDNS static host committed by the DNS server is removed by the DHCP server which serves the range**

Number: Q00024884

Description: 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.

Anomaly: **Cannot use ACL and Key ID with the same name in the same BIND match list.**

Number: Q00138539

Description: It is not possible to create a Key ID and an ACL with identical names in the same BIND match list.

Server Manager

Anomaly: **Option 81 requesting non-existent domain results in new root domain creation.**

Number: Q00462164

Description: If you have set Option 81 (allowing client FQDNs) on a dynamic range, non-existant (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.

Anomaly: **Cannot use a domain name on a Solaris system to identify a Sybase server**

Number: Q00103080

Description: 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.

DHCP server

Anomaly: **The DHCP server may not start because the nidraw driver did not start**

Number: Q00156933

Description: After uninstalling and reinstalling the DHCP server, it may fail to start because the *nidraw* driver fails to load. (The error message `Cannot load NIDRAW protocol driver, VxD Error=00000002` will appear in the Event Viewer.)

Workaround: Open a command prompt and type **`net start nidraw`** to load the driver.

Management console

Anomaly: **Vendor or user class options can still be associated with objects after they have been deleted.**

Number: Q00107540

Description: 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.

Anomaly: **If a Server Manager goes offline, the status of the DNS or DHCP servers' connection to that Server Manager is not updated in the Management Console.**

Number: Q00107530

Description: 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.

Anomaly: **Window needs resizing before seeing icons or tree view.**

Number: 3984

Description: Under Openwin on Solaris, you need to resize the window before you can see the icons or tree area.

Anomaly: **DHCP does not allow duplicate hardware or client ID mappings on the same subnet**

Number: 4226

Description: 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

Anomaly: **Inconsistent format of database files exported from DNS export**

Number: 4086, 3533

Description: 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.

Anomaly: **Netscape Communicator may not respond after not being used for a long period of time**

Number: 5869

Description: 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

Anomaly: **Illegal characters in domain names cause problems during import**

Number: 3486

Description: 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.

Anomaly: **Cannot update domain name after importing a resource record with “\”**

Number: 3508

Description: After you import a resource record that contains a backslash 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

Anomaly: **Ping audit results does not display all information**

Number: Q00072400

Description: 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

Anomaly:	**TTL and FLAGS columns missing in NID4_HISTORY table.**
Number:	Q00285595-01
Description:	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.

Anomalies Corrected in NetID 4.3 Series

This section lists all of the customer-reported problems Nortel Networks has corrected since the version 4.3.0 release of the NetID software.

Application server

Fixed Anomaly: **4.3.0.1 Application server cores when user clicks OK on blank New Domain screen.**

Number: Q00216227-01, Q00279413-01

Description: When creating a new domain under the domain tree in the management console, if you click on OK without having entered any data in the fields, the application server cores with a segmentation fault.

Fixed Anomaly: **Application server cannot apply templates properly.**

Number: Q00284121-01

Description: The application was encountering difficulties in applying data to multiple hosts using a host template. After applying the data, if the user selected a number of hosts, then right-clicked the group and chose Properties from the menu, an error message was displayed:

```
The Management Console has encountered an error. You
may experience unexpected results.
```

Fixed in version 4.3.1.

Fixed Anomaly: **Some users encountering "Application server not responding" error message.**

Number: Q00319038-01

Description: Some Netscape 4.7.9 users were encountering the following message when they tried to access the Properties dialog box for a DHCP server:

```
The NetID Application Server is not responding.
```

Fixed in version 4.3.1.

Fixed Anomaly: **Access migration: inaccurate display of admin users on root zone object.**

Number: Q00415532-01

Description: Upgrading from NetID 4.2.2 to NetID 4.3.01 caused problems with the OBJECT_IDENT field in the NID4_OBJECT_ACCESS table. Although users have access on the root zone object, the GUI does not display this. It shows that only a couple of users have admin access to the root zone object. Although it does not appear that users have access to subzones, all regular users are allowed to perform actions (such as Delete) against these subzones.

Fixed in version 4.3.1.

Fixed Anomaly: **Invalid Attribute error caused by un-committable DHCP hosts.**

Number: Q00418630-01

Description: When the DHCP server attempted to commit hosts with invalid FQDNs, an `Invalid Attribute` error message was generated in the log file. In this situation, the commit should fail but the error message is unnecessary.

Fixed in version 4.3.1.

Fixed Anomaly: **Unable to register A records to reserved range through DDNS.**

Number: Q00426055-01

Description: When the DNS attempted to commit an A record (received through DDNS) to a reserved range, the server manager returned the following error:

```
WARNING: DNS server <server_domain_name>. Invalid
Resource Record received from DNS server:
<server_domain_name> <IP_address>
```

The DNS server was then sent a `deleteRR` command for the A record, leaving the system out of DNS.

Fixed in version 4.3.1.

Fixed Anomaly: **(Sybase only) Selecting client pool causes the application server to core.**

Number: Q00427658-01

Description: Previous versions of NetID did not set up primary keys properly in some tables of Sybase databases. In certain cases, this may result in duplicate entries in those tables. These will be reported in the event log as they are detected by the application server or server manager as:

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

The management console will not display doubles of such duplicate entries. However they can be corrected by using the management console to delete and re-create the entries with duplicates.

Possibly affected types include Client Pool Entries (type 6110000), Resource Records (type 1100000) and Name Server Zone associations (type 5110000)."

Fixed in version 4.3.1.

Fixed Anomaly: **Parent_start_ip value is not properly maintained.**

Number: Q00433667-01

Description: When joining two class C subnets (each with a DHCP range), the new subnet (255.255.254.0) contains both ranges and no hosts are present in the GUI. When looking at the records through SQL in the NID4_IP_ADDRESS table, it can be seen that the parent_start_ip value of the dynamic hosts is the subnet number and not the first IP address of its dynamic range.

Fixed in version 4.3.1.

Fixed Anomaly: **(UNIX only) CLI tool doesn't run properly when using the -f flag.**

Number: Q00453791-01

Description: The command line interface (CLI) tool does not work properly when using the `-f` flag on Solaris. If the user calls the CLI tool and the commands file is in a local directory, then the tool it will work properly. If the user is using a directory/filename with the `-f` flag when calling the CLI tool, it only runs the nidcli usage online Help instead of functioning.

Fixed in version 4.3.1.

Fixed Anomaly: **Cannot add CNAME to host that already has more than one CNAME.**

Number: Q00463949-01

Description: When attempting to add a CNAME to an existing host that already has more than one CNAME associated, the following error message is received:

```
The domain name cname.domain.com. has a CNAME type
resource record.
```

No error message is received if you create a new host and add many CNAMES to it.

Fixed in version 4.3.1.

Fixed Anomaly: **Application server crash when deleting domains from a bucket.**

Number: Q00471835-01

Description: When the last domain was deleted from a bucket of domain names, the Application server crashed.

Fixed in version 4.3.1.

Fixed Anomaly: **Attempting to delete a CNAME causes Application Server to core.**

Number: Q00629897-01

Description: The problem was due to a combination of two factors: incorrect values in the `child_count` (formerly a count, now used as a flag to indicate the presence or absence of children), and a domain name who has its own parent as a CNAME alias.

Fixed in version 4.3.2.

Anomaly: **ORA-0900 error while running ExpireLocal.**

Number: Q00550982-01

Description: Running ExpireLocal against a replicated database residing on an Oracle 8.0.6 database causes an ORA-0900 (Invalid SQL) error. ExpireLocal makes a call to a stored procedure to delete deltas that have been moved to history from NID4_DELTA_LOG. However, the syntax to call the procedure ("Call <proc name>") is supported only on Oracle 8i and later.

Fixed in version 4.3.2.

Fixed Anomaly: NetID 4.3.1 Application Server does not run on Solaris 5.6 or 5.8 systems.

Number: Q00498396-01

Description: User installed NetID 4.3.1 on Solaris 5.6 and 5.8. DHCP and DNS Servers and Server Manager worked fine, but unable to start Application Server on either system. OpenSSL was determined to be the problem. The default behavior for the `config` script was to optimize for the machine it is building on. Script was optimized for UltraSparc machines, and would not run on older SPARC stations.

Fixed in version 4.3.2.

Fixed Anomaly: Nidappsrvd requires excessive time to stop with SIGKILL.

Number: Q00537673-01

Description: User found that `nidappsrvd` does not stop with `SIGKILL` command. Only the `kill -9` command would stop the process.

Fixed in version 4.3.2.

Fixed Anomaly: Request to change process by which NetID offers unused addresses.

Number: Q00588012-01

Description: A request was made for a change to the functionality surrounding the NetID mechanism for offering unused IP addresses. The request specified that, wherever possible, only unused addresses that are not part of a dynamic range should be offered.

Addressed in version 4.3.2.

Fixed Anomaly: **BootP Server IP (SIADDR) cannot be reset after being applied once.**

Q00599581-01

Description: The BootP server IP address (SIADDR field) could not be reset to its default value (0.0.0.0) after being applied once. Deselecting the "Bootp Client" option for a host could not effectively prevent the former BootP Client host from receiving the previously-set BootP server IP address.

Fixed in version 4.3.2.

Fixed Anomaly: **Cannot access NetID management console with Application Server running on multi-processor machine.**

Number: Q00607252-01

Description: The user installed NetID 4.3.1 on system with multiple processors. The Application Server functioned properly with only one of the system's processors enabled. With two or more procesors enabled, the user could not access the management console and the Application Server disconnected from the database.

Fixed in version 4.3.2.

Fixed Anomaly: **ACLs on a range are lost after resizing the range.**

Number: Q00656173

Description: If a dynamic, static, or reserved range was resized after an ACL was defined on it, the user could no longer access the ACL after the resizing.

Fixed in version 4.3.2.

Server Manager

Fixed Anomaly: "USR1" signal not accepted on Solaris when using Sybase client.

Number: Q00152466-01

Description: The `kill -USR1 pid` command is not accepted for either the Server Manager or the Application Server running on a Solaris platform running against a Sybase database.

Fixed in version 4.3.1.

Fixed Anomaly: Attempting to schedule captures of the metrics for a Server Manager on HP-UX causes the Server Manager to core

Number: Q00157268

Description: If you attempt to schedule captures of the operating metrics for a Server Manager that is running on an HP-UX system and is connected to a Sybase database, by entering the command **`kill -WINCH`** <*process_number*>, the Server Manager cores.

Fixed in version 4.3.1.

Fixed Anomaly: Excessive time required for get-config function in 4.2 series and 4.3.01.

Number: Q00036149, Q00282029-01

Description: After upgrading from NetID 4.1.6 to NetID 4.2.1, a complete reload of DNS and DHCP servers required twice as much time.

Fixed in version 4.3.1.

Fixed Anomaly: **DDNS add function causes host to be removed from DNS.**

Number: Q00287448-01

Description: In certain cases when DDNS updates containing mixed-case domain names were received, the Server Manager generated the following debug message:

```
WARNING: DNS server reserve02.<server_name>. Invalid
Resource Record received from DNS server:
vwd00002.<server_name>.
e33d9a46-fc00-43c8-ab15-a367f26f2a4e._msdcs.com
```

The cname was removed from the record. The cname would reappear the next time the host attempted to add itself to the DNS through DDNS.

Fixed in version 4.3.1.

Fixed Anomaly: **Server Manager generates large number of Oracle deadlock messages.**

Number: Q00584558-01, Q00566569

Description: The Server Manager was generating a large number of deadlock (ORA-00060) error messages during a Server Manager stress test. The test involved sending thousands of RENEW messages to a DHCP server at random intervals, resulting in floods of DHCP commit messages being sent to the Server Manager.

Description: Fixed in version 4.3.2.

Fixed Anomaly: **Server Manager/Application Server erratic performance during Oracle database backup.**

Number: Q00493213-01

Description: When an Oracle database is backed up, some Server Managers and Application Servers do not disconnect properly. Problem appears to be a failed select not setting the database to a Down state when receiving a database error, and continuing operation as if the query had returned no data.

Fixed in version 4.3.2.

Fixed Anomaly: **Server Manager failed while DNS server recieving zone information.**

Number: Q00537009-01

Description: The Server Manager failed when sending zones to the DNS server. The crash occurred when the Server Manager was applying a delta that signals the deletion of a reverse zone.

Fixed in version 4.3.2.

Fixed Anomaly: **Server Manager failed on issues regarding partitioning and multinets.**

Number: Q00576203-01

Description: Problems were encountered with multinets disappearing from the `dhcpcfg.cur` files on DHCP servers. The problem was related to joining a subnet that has a partitioning table that contains some subnets that are being joined, and some that are not.

Fixed in version 4.3.2.

Fixed Anomaly: **DDNS Delete and DDNS Add processed in reverse order.**

Number: Q00582975-01

Description: Some of the GUID CNAME entries appeared to be deleted from the database. There was a sequential processing problem when taking actions off of the queue with the Server Manager.

Fixed in version 4.3.2.

Fixed Anomaly: **Server Manager crashes at customer site.**

Number: Q00644103-01

Description: Core file analysis showed that the Server Manager was processing a DeltaMove and it was trying to locate the parent of a new domain. However, the pointer to the parent object was null, so the Server Manager crashed when the pointer was used. A check was added to ensure that the parentKey value is not null.

Fixed in version 4.3.2.

Fixed Anomaly: **DNS get-config requires abnormal length of time.**

Number: Q00646835-01

Description: `Get-config` for a version 4.3.1 DNS server was taking more than an hour, whereas using the version 4.3.0.1 DNS server required a maximum of 20 minutes. The problem was caused by the method of retrieving the child count rely on the actual number of subdomains rather than the `child_count` field in the database. Calls to this would require a database call which considerably slowed the DNS `get-config` if a large number of domains with no children was present.

Fixed in version 4.3.2.

Fixed Anomaly: **NetID 4.3.0.1 Server Manager failure on HP-UX.**

Number: Q00526078-01

Description: A customer reported a Server Manager failure under specific circumstances. The problem was determined to be related to memory errors in the Server Manager.

Fixed in version 4.3.2.

Fixed Anomaly: **Server Manager failure.**

Number: Q00542779-01

Description: A customer reported a Server Manager failure. The problem was determined to be a memory error that occured when the cache was flushed under certain circumstances.

Fixed in version 4.3.2.

DNS server

Fixed Anomaly: **DNS server reports "recvfrom: no such device" message.**

Number: Q00208790-01

Description: The DNS server reported a `recvfrom: no such device` message when an external application made a large number of queries that timed out. The problem was caused by a behavior change in the Windows 2000 TCP stack.

Fixed in version 4.3.1.

Fixed Anomaly: **Incorrect WKS resource record format causes DNS to crash.**

Number: Q00432381-01

Description: If a DDNS update to DNS is attempted for a well-known service (WKS) for which the resource record format is incorrect, the DNS server crashes. For example, a resource record that contains the IP address for the WKS but no protocol or service information will cause the server to crash. The application simply continues parsing without verifying that there are enough tokens to be parsed.

Fixed in version 4.3.1.

Fixed Anomaly: **CERT Advisory CA-2002-23: multiple vulnerabilities in OpenSSL.**

Number: Q00495917-01

Description: OpenSSL is an implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. There are four remotely exploitable buffer overflows that affect various OpenSSL client and server implementations. Several of these vulnerabilities could be used by a remote attacker to execute arbitrary code on the target system. All could be used to create denial of service in one form or another.

Addressed in version 4.3.2. NetID was re-compiled using OpenSSL 0.9.6g.

Fixed Anomaly: **Unique constraint error when adding new aliases.**

Number: Q00508612-01

Description: A unique constraint error was genereated when aliases were added to a host with existing aliases.

Fixed in version 4.3.2.

Fixed Anomaly: **DNS export does not handle large number of delegations properly.**

Number: Q00611967-01

Description: When trying to export a zone with many delegated subzones, the DNS export can take many hours to complete the zone.

Fixed in version 4.3.2.

Fixed Anomaly: **Problem with secure recursion.**

Number: Q00041363-01

Description: Secure-recursion was causing problems with name resolution from name servers.

Fixed in version 4.3.2.

Fixed Anomaly: **DNS server fails as a result of invalid command from Server Manager.**

Number: Q00478722-01

Description: The system failed when the DNS server received an invalid command (missing Resource Record value) from the Server Manager.

Fixed in version 4.3.2.

Fixed Anomaly: **SRV records copied to database files with trailing double-dots.**

Number: Q00579536-01

Description: When SRV records are written to the DNS cache, the cache dumping routine that writes the content to the database files adds a trailing dot to all the names it writes.

Fixed in version 4.3.2.

Fixed Anomaly: **When adding new zone, DNS servers disconnect from Server Manager.**

Number: Q00576005-01

Description: A newly-added zone causes the server manager to incorrectly flag all zones for update notifications for all name servers.

Fixed in version 4.3.2.

Fixed Anomaly: **libbind needs to be patched to fix CERT VU#738331.**

Number: Q00511407-01

Description: Versions affected: BIND 4 prior to 4.9.10 and BIND 8 prior to 8.2.5. BIND 9 and BIND 8.3.x are NOT affected.

When looking up address (`gethostbyname(), gethostbyaddr()` etc.) a less than maximum sized buffer is passed to `res_search() / res_query()`. If the answer is too large to fit in the buffer the size of buffer required is returned along with the part of the message that will fit. This value is not checked and is passed to getanswer which then may read past the end of the buffer depending up the contents in the answer section.

An attacker who is able to send DNS responses to a vulnerable system could cause a denial of service, crashing the application that made calls to a vulnerable resolver library. It does not appear that this vulnerability can be exploited to execute arbitrary code.

Addressed in version 4.3.2. Use a 64K buffer when calling `nid_res_query()` which will call `res_send()`. Merged fix from BIND 8.2.6/8.3.3.

Fixed Anomaly: **Request to investigate the impact of CERT VU#738331 on NetID 4.3.1.**

Number: Q00563352-01

Description: Nortel Networks determined that NetID 4.3.1 was vulnerable to the type of denial-of-service attack outlined in CERT advisory VU#738331. A patch was merged into the NetID 4.3.1 code stream to address the vulnerability. The patch has been carried forward into the NetID 4.3.2 code stream.

DHCP server

Fixed Anomaly: **NetID 4.3.0.1: DHCP option 15 does not override inherited domain name.**

Number: Q00281820-01, Q00526572-01

Description: If the user creates a subnet, adds a DNS domain name in the subnet’s DHCP options, and then creates a dynamic range, the domain name is inherited for the range. On the Naming tab, disable the Subnet Default option, enable the Other option, and specify a new domain name.

The new domain name should override the domain name of the subnet in the DHCP options of the range. The DHCP client is not updated with the overridden domain name, but with the domain name of the subnet.

Fixed in version 4.3.2.

Fixed Anomaly: **When renaming a client pool, user access grants are lost to the new pool.**

Number: Q00286612-01

Description: If the user renames a client pool, any users or groups that have access to the pool lose their access.

Fixed in version 4.3.1.

Fixed Anomaly: **DHCP server fails to serve leases when running on Windows 2000 with disabled interfaces.**

Number: Q00448289-01

Description: The DHCP server retrieves in order the list of interfaces from the registry. Once the server encounters a disabled interface, any subsequent interface retrievals are not sent.

Fixed in version 4.3.1.

Fixed Anomaly: **CERT advisory CA-2002-19**

Number: Q00477534

Description: CERT® Advisory CA-2002-19: Buffer overflow in multiple DNS resolver libraries. Original release date: June 28, 2002. Last revised: July 1, 2002.

Operating systems or applications that use multiple DNS resolver libraries are vulnerable to malicious DNS responses and denial of service attacks. The NetID DHCP Server uses the `libbind` resolver library to perform queries when attempting to send DDNS updates. Nortel Networks has updated the DHCP Server to take advantage of the fix for the `libbind` resolver library, fixing the vulnerability concern.

Addressed in NetID 4.3.1.

Fixed Anomaly: **Primary DHCP server crash when sending long lease to backup.**

Number: Q00550012-01

Description: The primary DHCP server crashes with a dhcpcfg.cur file containing long leases (more than 1000 characters in "host ip ..." line) when it tries to send the .cur file to backup.

Fixed in version 4.3.2

Fixed Anomaly: **Auto-generated domain name is blanked-out on lease recommit.**

Number: Q00574946-01

Description: The auto-generated domain name is being overwritten with an empty FQDN when a DISCOVER is performed before the lease expires. Code corrected to replace the auto-generateed name.

Fixed in version 4.3.2.

Fixed Anomaly: **DHCP Server failing with Dr. Watson file.**

Number: Q00591181-01

Description: The crash is caused by an off-by-one error in the calculation of DHCP option 81 length when this option is built for a return packet. This causes later code to de-reference pointers past the boundary of the block of memory holding the option.

Fixed in version 4.3.2.

Fixed Anomaly: **DHCP Server failure after joining or partitioning subnets.**

Number: Q00579488-01

Description: The DHCP configuration was not being properly reloaded after subnet partitioning/joining functions were performed. The resulting corrupted `dhcpcfg.cur` file crashed the DHCP Server.

Fixed in version 4.3.2.

Management console

Fixed Anomaly: **Moving a comment entry Up or Down in the BIND Statement card grays-out the comment**

Number: Q00104479

Description: After you add a name server statement and a comment entry to a name server statement (via the BIND Statements tab of the Management Console) and input data for both entries, the comment entry will appear "grayed-out" if it is moved up or down in the list.

Fixed in version 4.3.1.

Fixed Anomaly: **User cannot Cut and Paste with access level of Admin on a subnet.**

Number: Q00468925-01

Description: A user who has an access level of Admin on a subnet cannot make use of the Cut and Paste clipboard commands within the subnet. If the user has Admin access to the entire network, then the Cut and Paste commands will work within the subnet.

Fixed in version 4.3.1.

Fixed Anomaly: **4.3.0.1: Custom Field headers not shown in search window or when viewing bucket contents.**

Number: Q00305266-01, Q00439596-01

Description: When searching for data within the NetID database, the custom field headers of the found data are not displayed properly. The common field headers are displayed, but not the headings for custom fields. The first column of custom field data is displayed (without a header), but if there is more than one custom field, none of the others are displayed (either header or data).

When buckets are used for any subnet, the following anomalies are present:

When a subnet is highlighted in the tree view, the grid displays the bucket ranges as well as the custom field headings.

When a bucket is highlighted in the tree view, the grid displays the address, domain name, and MAC address headings, but no custom field headings.

Fixed Anomaly: **Creating static host on DHCP server causes status bar to hang at 100%.**

Description: Q00431696-01

Description: An excessive amount of time was required to refresh the DHCP servers after adding a static host to them. Ranges are now requested as they are needed instead of being sent whenever the DHCP server is refreshed.

Fixed in version 4.3.2.

Fixed Anomaly: **Domain suffix from template appears twice in host name.**

Number: Q00494975-01

Description: If the Model option is used on a subnet when a host is added, the domain suffix from the template appears twice in the host's domain name.

Fixed in version 4.3.2

Fixed Anomaly: **FLSM network not restricting subnet mask.**

Number: Q00651431-01

Description: A FLSM network with a fixed-length subnet mask of 255.255.255.0 was allowing more than 254 subnets (the supposed limit) to be created on the subnet.

Fixed in version 4.3.2.

Fixed Anomaly: **Users with read access cannot scroll down through aliases.**

Number: Q00516881-01

Description: A NetID user with read-only access rights could not access the scroll bar in the aliases list in the Properties of Host dialog box.

Fixed in version 4.3.2.

Installation

Fixed Anomaly: **Error in server startup/stop scripts.**

Number: Q00031657

Description: The UNIX version of NetID creates Startup/Stop scripts in the `/etc/rc2.d` directory during install if the autostart option is selected. When these scripts are executed to stop the processes, the scripts use `kill -KILL` to stop processes instead of `kill -TERM`. The processes are not able shut down properly and SNMP traps are not sent.

Fixed in version 4.3.1.

Fixed Anomaly: **dbMaint script does not suspend replication while processing.**

Number: Q00529803-01

Description: When upgrading a replicated database, the `oracle.nidsql` script that runs during the installation process executes a command to suspend replication during the processing of the script. However, the `dbMaint` process runs under a separate SQL session and does not contain this same suspension technique.

In version 4.3.2, code was added suspend recplication before `dbMaint` runs. An error handler was also added to print out database errors and warnings.

Tools and utilities

Fixed Anomaly: **Subnet DHCP options may be corrupt after installing NetID against old database.**

Number: Q00174037

Description: The 4.3.0 dbMaint tool (which normally runs during the NetID installation process) has been extended to add a domain DHCP option on subnets whose default domain name is set. However, a bug exists which may truncate the resulting DHCP options strings if they contain zero values.

Fixed in version 4.3.0.1.

Fixed Anomaly: **Importing a subnet with minimal information removes existing model information.**

Number: Q00448017-01

Description: Fixed in version 4.3.1.

Fixed Anomaly: **Audit report does not display the results.**

Number: Q00480187-01

Description: This problem only occurs if the user key is mixed case.

Fixed in version 4.3.2.

Fixed Anomaly: **Only admin user can produce a DHCP server summary report.**

Number: Q00606427-01

Description: The DHCP Server Summary report (run either from the GUI or command line) produces no output or .html file if the user is not logged into the management console as the admin user.

Fixed in version 4.3.2.

Fixed Anomaly: **Command line export fails to create valid root.cache.db file.**

Number: Q00623387-01

Description: The problem was due to the export user not having access to the root server list. According to the policy on "utility" access to the dictionary, root servers are now retrieved regardless of permissions.

Fixed in version 4.3.2.

Fixed Anomaly: **FixSubnets utility fails (Oracle).**

Number: Q00612050-01

Description: The FixSubnets utility failed when run against a user’s database. The database had a host with a negative secondary names count, resulting in a database-down exception.

Fixed in version 4.3.2.

Fixed Anomaly: **nidcli utility does not set correct Time To Live value.**

Number: Q00667121-01

Description: When the `nidcli` utility was used to add hosts from the command line, it set the TTL value to zero seconds (instead of 24 hours).

Fixed in version 4.3.2.