Alcatel-Lucent VitalQIP

DNS/DHCP & IP MANAGEMENT SOFTWARE | LUCENT DHCP RELEASE 5.4

BUILD 45
RELEASE NOTES

190-409-113R5.4
NOVEMBER 2008
ISSUE 12

Contents

List of tables

About this document

Purpose

This document provides important information about the contents of Lucent DHCP 5.4 B45. It covers new features, system requirements, installation, upgrades, resolved problems, and known issues.

Reason for reissue

The Lucent DHCP 5.4 Release Notes have been reissued for the following reasons:

- Removal of incorrect note in UNIX upgrade instructions on page 8-2. (LDHCP00002008)
- Fix for documentation problems. Refer to Table 5.1 on page 5-2.

The following table shows the revision history of this document.

Issue number	Date of issue	Description of changes
11, Build 45	July 2008	Fix for customer-reported problem and addition of Known vendor issues section. Refer to "Known vendor issues", on page 6-2.
10, Build 43	May 2008	Support added for Windows 2008 Server
9, Build 42	March 2008	• RFC 4833 time zone options support • Client Class support at the subnet level • Vendor and User Class exclusions at the scope level
8, Build 39	August 2007	• DHCP last known good configuration support • DHCP failover configuration verification

Issue number	Date of issue	Description of changes
7, Build 34	February 2007	• DHCPRELEASE API callout • AckRenewForUnusedAddress DHCP Server policy • OfferOnlyAPIRequestedAddress DHCP Server policy • LogDhcpMsgTraffic DHCP Server policy functionality extended
5, Build 28	June 2006	• Enhanced DHCP API Callout libraries for VA Extension Service failover • DHCP server differentiates between Vendor Classes in a many-to-one failover environment • Reduction in the number of duplicate messages sent to the database • Support for RFC 3361 SIP Server option • Support for RFC 4280 Broadcast and Multicast Service (BCMCS) options
4, Build 22	August 2005	Fixes for customer-reported problems
3, Build 21	June 2005	Support for LDRM policies
2, Build 10	September 2004	• Conditional processing of DHCPINFORM packets • PingResponseReceived trap • Dynamic DNS override option • New DHCP server policies to support VitalAccess 2.1

Issue number	Date of issue	Description of changes
1, Build 5	June 2004	• Option 82 support in Active Lease File • Option 82 support for device class suboption • Option 82 support for Subnet (Link) Selection suboption • Enhanced debug level control • SNMP trap enhancements • Wildcard support for User and Vendor Class • RFC 3396 support • RFC 3442 support • RFC 3397 support • RFC 3495 support • New server policies • New configuration policies • Multiple NIC card support with DHCPServer and DHCPSocketAddr policies

Conventions used

The following table lists the typographical conventions used throughout this document.

Typographical conventions

Convention	Meaning	Example
Trebuchet bold	Names of items on screens.	Select the **Client** check box.
	Names of buttons you should click.	Click **OK**.
Courier	Output from commands, code listings, and log files	`# Name: Share shared-network _200_200_200_0`
Courier bold	Input that you should enter from your keyboard.	Run the following command: **`c:\setup.exe`**
	Names of commands and routines	The **`qip_getappllst`** routine returns the entire list of existing applications.

Convention	Meaning	Example
Courier bold italic	Input variable for which you must substitute another value. The angle brackets also indicate the value is a variable.	**`isql -U sa -P <sa_password>`**
Times bold	Names of keys on the keyboard to be pressed.	Press **Enter** to continue.
	Uniform Resource Locators (URLs)	The VitalQIP product site can be found at **http://www.alcatel-lucent.com/wps/portal/products/**.
Times italics	Manual and book titles.	Refer to the *VitalQIP User's Guide*.
	Directories, paths, file names, and e-mail addresses.	A symbolic link must be created from */etc/named.conf* that points to *named.conf*.
Times bold italic	Emphasis	***Read-only***. The name of the service element.

Technical Support

For assistance, contact Technical Support:

- For North America customers: **1-866-LUCENT8** (**582-3688**), Option 1, Option 2
- For Europe, Middle East, Africa, and China technical support: **00 800 00 LUCENT** or **+353 1692 4579**
- For Central and South America customers:
  - Mexico: 01 800 123 8705 or (52) 55 5278 7005
  - Brazil: 0800 89 19325 or (55) 193707 7900
  - Argentina: 0800 666 1687
  - Venezuela: 0 800 1004136
  - Costa Rica: 0800-012-2222 or 1800 58 58877

  Important! For other local CALA numbers consult the web site http://www.alcatel-lucent.com/support or contact your local sales rep.
- For Asia Pacific technical support:
  - **1800-458-236** (toll free from within Australia)

- (IDD) **800-5823-6888** (toll free from Asia Pacific –Hong Kong, Indonesia, South Korea, Malaysia, New Zealand, Philippines, Singapore, Taiwan, and Thailand)
- **(613) 9614-8530** (toll call from any country)

How to comment

To comment on this document, go to the Online Comment Form (http://www.lucent-info.com/comments/) or e-mail your comments to the Comments Hotline (comments@alcatel-lucent.com).

1 Overview

Overview

Purpose

This document provides important information about the contents of Lucent DHCP 5.4 B45. It covers new and enhanced features, system requirements, product installation and upgrades, and known issues. The document is meant to be read by all customers who plan on using Lucent DHCP 5.4 B45. Please read this document carefully and completely before installing and using Lucent DHCP 5.4 B45.

Important! The content of this document is cumulative: it contains information already published to support previous builds of Lucent DHCP 5.4. Resolved customer issues, for example, are organized by the build in which the fix occurred.

2 Release components

Overview

Purpose

This chapter describes software and documentation deliverables included in this release.

Contents

This chapter covers these topics.

Software deliverables

Software included in this release

The following table lists the software that comprises the Lucent DHCP 5.4 B45 release.

Table 2.1 Software deliverables

Type	Platform	Directory	File
Lucent DHCP Software	AIX 5.2	/vitalqip/LucentDHCP/5.4/aix/LucentDHCP5.4-aix.52-b45	*dhcpd*
	HPUX.11	/vitalqip/LucentDHCP/5.4/hpux/LucentDHCP5.4-hpux.11x-b45	*dhcpd*
	Linux	/vitalqip/LucentDHCP/5.4/linux/LucentDHCP5.4-linux-b45	*dhcpd*
	Solaris	/vitalqip/LucentDHCP/5.4/solaris/LucentDHCP5.4-solaris.2x-b45	*dhcpd*
	Windows 2008 Enterprise and Standard Editions	/vitalqip/LucentDHCP/5.4/w2k/LucentDHCP5.4-w2k-b45	*DHCPService.exe*
	Windows 2003	/vitalqip/LucentDHCP/5.4/w2k/LucentDHCP5.4-w2k-b45	*DHCPService.exe*

How to obtain software

VitalQIP Lucent DHCP 5.4 B45 installation files are available for download via Alcatel-Lucent Electronic Delivery (ALED) services. ALED uses secure HTTP and FTP to download files and documentation. In order to use ALED, you must be registered with Alcatel-Lucent Global Support.

If you are not registered with Alcatel-Lucent Global Support, visit https://market.lucent.com/release/SPRegistrantTypeSvlt. If you need assistance in registering, contact the Alcatel-Lucent Customer Support Services:

- Inside the United States: 1 (866) 582-3688, prompt 7
- Outside the United States: 1 (630) 218-7688

You must have SSH installed and configured before downloading installation files. For more information about setting up secure FTP, visit https://download.support.lucent.com/cgi-bin/ssh_ftp.cgi. After you have set up secure FTP, you can connect via secure FTP and access the **Product|Version|Platform** directory to download the product's files. To download the product via secure HTTP, follow these steps:

1 If you have not registered, register at https://market.lucent.com/release/SPRegistrantTypeSvlt.

2 Open a browser and go to https://support.lucent.com/portal/olcsHome.do.

3 Log in with your user name and password. The Customer Center is displayed.

4 Under Technical Support, click **Downloads**.

5 Click **U-Z**.

6 Under V, click on **VitalQIP®**.

7 Under Documentation and downloads, click **Downloads: Electronic Delivery**.

8 Select **LucentDHCP** and click **Next**.

9 Select **5.4** and click **Next**.

10 Select the appropriate platform and click **Next**.

11 Select the file to download and click **Next**.

12 Specify the download directory on your local machine.

13 Click **Download** to use the legacy download agent, or **Download Plus** to use the GetPlus® download agent.

END OF STEPS

Documentation deliverables

Documentation available for this release

The following table lists the available documentation for the Lucent DHCP 5.4 B45 release.

Table 2.2 Documentation deliverables

Type	Directory	File
Release Notes	/vitalqip/LucentDHCP/5.4/aix/ DHCP5.4ReleaseNotes-aix.52 /vitalqip/LucentDHCP/5.4/hpux/ DHCP5.4ReleaseNotes-hpux.11x /vitalqip/LucentDHCP/5.4/linux/ DHCP5.4ReleaseNotes-linux /vitalqip/LucentDHCP/5.4/solaris/ DHCP5.4ReleaseNotes-solaris.2x /vitalqip/LucentDHCP/5.4/w2k/ DHCP5.4ReleaseNotes-w2k	LDHCP54B45RN.pdf

To obtain documentation from OnLine Customer Support

In addition to the ALED site, VitalQIP product documentation is available to customers through OnLine Customer Support (OLCS). To navigate to OLCS, follow these steps:

1. Go to https://support.lucent.com/portal/productIndexByCat.do.
2. Select the product category for which you require documentation. For example, for VitalQIP documentation, select **Network, Service Management and OSS**.
3. To obtain manuals, select **Manuals and Guides**. To obtain release notes, select **Release Information**.

END OF STEPS

3 New features

Overview

Purpose

The following sections identify the new features and/or capabilities contained in this release.

Contents

This chapter covers these topics.

Windows 2008 support with VitalQIP 7.1 PR2

Feature ID

LDHCP00001273

Release

5.4 build 43

Description

Added support for Windows 2008 Enterprise and Standard Editions to the DHCP server. This change allows the DHCP server executable to operate effectively with all currently supported versions of the Windows OS. Build 42 and earlier DHCP 5.4 Servers will not function in the Windows 2008 environment.

The code changes affect only Windows platforms. This patch does not need to be applied to UNIX systems.

Note: VitalQIP 7.1 PR2 is also required to support Windows 2008 on VitalQIP Remote Servers.

RFC 4833 time zone options support

Feature ID

LDHCP00000679

Release

5.4 build 42

Description

Added support to the DHCP server for time zone options 100 and 101 as specified in RFC 4833.

Client Class support at the subnet level

Feature ID

LDHCP00000687

Release

5.4 build 42

Description

The DHCP server can now support client classes (user, vendor, device) at both the server level and the subnet level. This expanded feature allows options and policies defined in the address independent client classes to now be unique according to the subnet that they are assigned to. This feature will provide an easy way to assign the same option value(s) to all clients of a particular user class or vendor class in a subnet, without the need define separate address ranges in the subnet, differentiated by user or vendor class.

Note: VitalQIP 7.1 does not currently provide the capability to assign client classes at the subnet level. In order to utilize this feature in the DHCP server, a DHCP generation user exit must be employed.

Vendor and User Class exclusions at the scope level

Feature ID

LDHCP00001074

Release

5.4 build 42

Description

The DHCP server has the capability to exclude vendor and/or user classes from receiving a lease from a particular address range or scope. This feature is utilized through the use of two new scope level configuration file policies, excluded-vendor-classes and excluded-user-classes. Multiple values can be specified for each policy, and a trailing wildcard asterisk (*) is supported.

The syntax is :

```
policy excluded-vendor-classes “value1”,”optional-value2”;
policy excluded-user-classes “value1”,”optional-value2”;
```

Note This feature will be supported beginning in VitalQIP 7.1, Patch Release 2. Earlier versions of VitalQIP must utilize a DHCP generation user exit to insert the policy statements in the DHCP configuration file.

DHCP last known good configuration support

Feature ID

LDHCP00000613

Release

5.4 build 39

Description

The DHCP server attempts to parse *dhcpd.conf*, and if it is successful, it copies *dhcpd.conf* to *dhcpd.conf.lastgood*. If a syntax error is detected within *dhcpd.conf*, the server attempts to parse *dhcpd.conf.lastgood*. If it can parse the backup file, it copies *dhcpd.conf.lastgood* to *dhcpd.conf*. If both files are corrupt, the server exits. If *dhcpd.conf* is valid, it is copied to *dhcpd.conf.lastgood*.

DHCP failover configuration verification

Feature ID

LDHCP00000630

Release

5.4 build 39

Description

The DHCP Server verifies that the failover information contained in the *dhcpd.conf* and *dhcpd.pcy* file is consistent. Server logic was added to verify that when the primary-server tag occurs in the *dhcpd.conf* file, that the failover server type is secondary and that the specified IP address in the tag is identified in the *dhcpd.pcy* file as a partner primary. When the tag erroneously occurs in a primary/standalone server's configuration file, or when there is no matching primary partner in the policy file, ignore the new configuration file and attempt to use the backup configuration file (see LDHCP000000613) instead.

DHCP release API callout

Feature ID

LDHCP00000554

Release

5.4 build 34

Description

This is a new API callout that is called after the DHCP server releases an IP address as a result of processing a DHCPRELEASE message from a DHCP client.

ACKRENEWFORUNUSEDADDRESS DHCP server policy

Feature ID

LDHCP00000559

Release

5.4 build 34

Description

When this policy is set, the DHCP server will ACK a Renew Request for an IP address that is not in the server's active lease table, provided that this address is in the server's managed ranges. The default value of this policy is off.

OFFERONLYAPIREQUESTEDADDRESS DHCP server policy

Feature ID

LDHCP00000560

Release

5.4 build 34

Description

A capability to force the DHCP server to only offer the address that is specified by the discover API callout in the requested IP address parameter (typically from, but not restricted to, Vital Access), is provided. If the address is not available for any reason (unmanaged, in use, forceClass mismatch, etc.), the discover message will be dropped and an Info level message written to the DHCP log. This capability will allow service provider environments to only offer/ack IP addresses specified by Vital Access. The default value of this new policy is off.

LOGDHCPMSGTRAFFIC DHCP server policy functionality extended

Feature ID

LDHCP00000573

Release

5.4 build 34

Description

Added remote id to relay agent info that is written to syslog when LogDhcpMsgTraffic policy is enabled for incoming DHCP message types.

Enhanced DHCP API callout libraries for VA Extension Service failover

Feature ID

None

Release

5.4 build 28

Description

The Extension Service communication retry and failover functionality was added to the API callout (for VitalAccess 2.1). These policies were added:

- RetryExistingSocket – The server retries to send the message to the current Extension Service socket following a communication error.
- ProcessLevelFailover – The server threads automatically close their existing socket connections to a “failed” Extension Service and creates new socket connections to the most recently connected “failover” Extension Service.
- AttemptPrimaryReconnect – When connected to a failover Extension Service, The DHCP server periodically attempts to reestablish a connection with the primary Extension Service.

DHCP server differentiates between vendor classes in many to one failover environment

Feature ID

None

Release

5.4 build 28

Description

Added support for associating client class data in a failover server to the primary server that it is defined under in the DHCP server configuration file. This change guarantees that a failover server offers the option values as defined in the client class associated with the primary server from which the offered address is assigned when there are multiple client classes with the same identifier, originating in different primary servers in a many-to-one failover configuration.

This change is effective for these types of client classes:

- vendor class
- user class
- device class

Reduction in the number of duplicate messages sent to database

Feature ID

None

Release

5.4 build 28

Description

Support was added for a policy to define a time period during which the DHCP server does not send “duplicate” ADD type update messages to the Message Service. This policy can be used to reduce the update message queuing problems seen in some customer sites. In particular, where there are redundant relays configured.

The policy defaults to zero, which disables the new logic. Any value specified that exceeds a maximum limit value of 60 seconds is overridden with the maximum limit. The name of the new policy is UpdatePreclusionDuration.

Supports RFC 3361 SIP server option

Feature ID

R.LUDHCP5.4-00900

Release

5.4 build 28

Description

Support was added in the server for the SIP Server option (option 120). This option must be in the DHCP configuration file in the sub-option format – hex data enclosed in square brackets. The option string identifier for the configuration file is “sip-server”. The DHCP server supports long option encoding for this option.

Supports RFC 4280 broadcase and multicast service (BCMCS) options

Feature ID

R.LUDHCP5.4-01200

Release

5.4 build 28

Description

Support was added for the Broadcast and Multicast Controller options (88 and 89) defined in RFC 4280. Two new options, broadcast-multicast-service-domain and broadcast-multicast-service-address, are the names of options 88 and 89, respectively. Option 88 has long option encoding available.

New policies for LDRM support

Feature ID

None

Release

5.4 build 21

Description

Five new server level policies have been added to support the interface to the Lucent DHCP Rules Manager (LDRM):

- UseLDRMCallout – when set to true (1) in the DHCP policy file, will cause the server to load and initialize the LDRM Callout library
- PacketReceiptLDRMCallout – when set to true, will cause the server to invoke an LDRM Callout API following the receipt and parsing of every DHCP packet
- DiscoverLDRMCallout – when set to true, will cause the server to invoke an LDRM Callout API prior to processing a DHCPDISCOVER packet
- RequestLDRMCallout – when set to true, will cause the server to invoke an LDRM Callout API prior to processing a DHCPREQUEST packet
- BootpRequestLDRMCallout – when set to true, will cause the server to invoke an LDRM Callout API prior to processing a BOOTPREQUEST packet
- AckLDRMCallout – when set to true, will cause the server to invoke an LDRM Callout API after sending a DHCPACK packet (Note: LDRM does not currently provide any functionality associated with this callout.)

These policies must be defined in the “Additional Policies” section of the server profile in VitalQIP 6.1SP1. For VitalQIP 6.2 and VitalQIP 7.x, these policies are predefined

under DHCP Server Policies on the Server Profile display. The default value for each of these policies is false (0).

Conditional processing of DHCPINFORM packets

Feature ID

None

Release

5.4 build 10

Description

A new server level policy, DropAllDhcpInformPackets, has been created, which when set to true (1) in the DHCP policy file, will cause the server to preclude the processing of any DHCPINFORM packet, beyond the parsing of the incoming packet. This policy will allow administrators to configure the DHCP server to ignore inform packets, when the processing of the same is not required. The default value for the policy is false (0). This policy must be defined in the "Additional Policies" section of the server profile in VitalQIP.

Ping response received trap

Feature ID

None

Release

5.4 build 10

Description

A new SNMP trap has been created, titled dhcpServerPingResponseReceived, which will be issued when a ping response is received by the DHCP server. This trap will contain the IP address that generated the ping response.

Dynamic DNS override options

Feature ID

None

Release

5.4 build 10

Description

A new server level policy, DDNSOverrideOption, has been created, which allows for the specification of a user defined option, that when present in the applicable configuration data in dhcpd.conf (host and/or client class) will specify an override value to be used in the Dynamic DNS flag field of the lease update message, which is sent to VitalQIP and the DNS Update Service. The valid values for the user defined option are ‘a’, ‘ptr’, ‘both’, and ‘none’. This value identifies which resource records are to be updated, and if present, will override the value provided in DHCP option 81 (client FQDN). This policy must be defined in the “Additional Policies” section of the server profile in VitalQIP.

Option 82 support in active lease file

Feature ID

R.DHCP-00035

Release

5.4 build 5

Description

The active lease file, *dhcp.db*, has an additional field. The Lucent DHCP 5.4 server tracks DHCP Relay Agent Information (option 82) for each lease. All Option 82 data is written to the Active Lease file as an ASCII representation of the hexadecimal data, so the Active Lease Service can support its display. The option 82 information is also communicated to a failover server if one is present.

As a result of this feature, all active lease services and CLIs must be upgraded to VitalQIP 6.1 SP1 to work correctly.

Option 82 Support for device class suboption

Feature ID

R.DHCP-00050

Release

5.4 build 5

Description

The Lucent DHCP 5.4 server supports the device class suboption of the relay agent information option as defined in RFC 3256. DHCP options associated with a specific device class in the DHCP configuration file will be assigned to clients whose discover packet contains that device class, in a manner similar to the user and vendor client classes that were introduced in the DHCP 5.2 server. Configuration parameters associated with a device class will take precedence over the same configuration options with different values specified in user or client classes.

Option 82 support for subnet (LINK) section suboption

Feature ID

R.DHCP-00045

Release

5.4 build 5

Description

The Lucent DHCP 5.4 server supports the subnet selection suboption of the relay agent information option. This suboption is also referred to as the link selection suboption. The server offers an IP address within the subnet specified by this suboption. This option is similar to the subnet selection option (option 118) that originates from a

DHCP client. This option is overridden by the Link Selection suboption if both are present. This option takes precedence over the Subnet Selection Option, if both are present.

Enhanced debug level control

Feature ID

R.DHCP-00075, R.DHCP-00080

Release

5.4 build 5

Description

The Lucent DHCP 5.4 server supports requests via the VitalQIP Network Services display to clear the debug log, stop logging altogether, or change the debug level, all without restarting the server. Clearing the debug log forces a rollover of the log file. Several new debug features are also supported in the Lucent DHCP 5.4 server, as documented in the *VitalQIP Administrator Reference Manual*.

SNMP trap enhancements

Feature ID

R.DHCP-00100, R.DHCP-00130

Release

5.4 build 5

Description

The Lucent DHCP 5.4 server supports two additional traps. The subnet unavailable descent threshold trap will be issued when the percentage of leases unavailable in a subnet falls below a configurable threshold value. The threshold value can be specified for each subnet in the DHCP configuration file using the subnet-unavailable-descent-threshold subnet level policy. Alternatively, a default value can be specified

for all subnets with the DefaultDescentThreshold server policy. This trap is only issued when a non-zero threshold value is in effect for a subnet.

The drop unknown client trap will be issued when a client request is explicitly dropped by the server because its MAC address is either in a MAC exclusion pool, or the MAC is not in an inclusion pool. This capability must be enabled through a new server policy, IssueDropUnknownClientTrap.

Note: You need to upgrade SNMP Modules to SNMP version 2.1, build 8 or higher to implement this feature.

Wildcard support for user and vendor classes

Feature ID

R.DHCP-00120

Release

5.4 build 5

Description

The Lucent DHCP 5.4 server supports the capability to match client provided user class and vendor class values with values containing wildcards, that are provided in either an address scope or client class construct within the DHCP configuration file. The wildcard character is an asterisk (*) and is treated as a trailing wildcard, meaning that any additional characters following the wildcard character will be ignored.

RFC 3396 support

Feature ID

R.DHCP-00140

Release

5.4 build 5

Description

The Lucent DHCP 5.4 server supports RFC 3396, which provides the capability to split options that exceed 255 bytes (the maximum size of a single option) into multiple instances for outgoing packets and to concatenate multiple instances of the same option number that appear in incoming packets.

RFC 3442 support

Feature ID

R.DHCP-00150

Release

5.4 build 5

Description

The Lucent DHCP 5.4 server supports RFC 3442, which allows the use of the classless static route option.

RFC 3397 support

Feature ID

R.DHCP-00160

Release

5.4 build 5

Description

The Lucent DHCP 5.4 server supports RFC 3397, which allows the use of the domain search option.

RFC 3495 support

Feature ID

R.DHCP-00170

Release

5.4 build 5

Description

The Lucent DHCP 5.4 server supports RFC 3495, which allows the use of the CableLabs client configuration option.

New server policies

Feature ID

None

Release

5.4 build 5

Description

The following server policies are new. They are documented in detail in the *VitalQIP User's Guide*.

- SupportRelayAgentDeviceClass
- IssueDropUnknownClientTrap
- DefaultDescentThreshold
- DropZeroMacAddressPackets
- SendServerIdLast
- SupportEncodingLongOptions
- MaxOutgoingDhcpMessageSize

New configuration policies

Feature ID

None

Release

5.4 build 5

Description

The following configuration policies are new.

Policy name: subnet-unavailable-descent-threshold

Values: Numeric

Default value: 0

Description: Specifies the percentage when an SNMP dhcpServerSubnetThresholdDescent trap is issued when addresses become available on a subnet. For example, if the value of this policy is set to 80, and the number of used addresses on the subnet falls below 80%, the SNMP trap is issued. If this value is set to 0, no dhcpServerSubnetThresholdDescent trap is issued for this subnet. If this value is not specified, the server level policy value, DefaultDescentThreshold, is used.

Policy name: subnet-unavailable-threshold

Values: Numeric

Default value: 0

Description: Specifies the percentage when an SNMP dhcpServerSubnetThresholdExceeded trap is issued when addresses become unavailable on a subnet. For example, if the value of this policy is set to 80, and the number of used addresses on the subnet goes above 80%, the SNMP trap is issued. If this value is set to 0, no dhcpServerSubnetThresholdExceeded trap is issued for this subnet. If this value is not specified, the server level policy value, DefaultUnavailableThreshold, is used.

4 Changes to interfaces, alarms, and messages

Overview

Purpose

This chapter is not pertinent to the Lucent DHCP 5.4 B45 release.

5 Resolved issues

Overview

Purpose

This chapter describes resolved issues in this release.

Contents

This chapter covers these topics.

Resolved issues in Lucent DHCP 5.4 B45

The following table identifies the customer reported issues that were fixed in Lucent DHCP 5.4 B45.

Table 5.1 Resolved issues in Lucent DHCP 5.4 B45

Fault ID	AR ID	Description of issue
LDHCP00000662	1-1718957	Documentation: DHCP 5.4 B39 RN confusing.
LDHCP00001782	1-1880002, 1-1872665	Use of “siaddr=sname” does not correctly specify IP address of FQDN from value of DHCP Option 66.
LDHCP00002008		Documentation: Remove invalid note from DHCP B45 Release Notes.

Resolved issues in Lucent DHCP 5.4 B42

The following table identifies the customer reported issues that were fixed in Lucent DHCP 5.4 B42.

Table 5.2 Resolved issues in Lucent DHCP 5.4 B42

Fault ID	AR ID	Description of issue
LDHCP00000655	1-1686683	A large number of virtual interfaces will prevent the DHCP server from binding to the interfaces.
LDHCP00000693		Misleading DHCP log entries when Discover or Request messages are not processed are removed.

Resolved issues in Lucent DHCP 5.4 B39

The following table identifies the customer reported issues that were fixed in Lucent DHCP 5.4 B39.

Table 5.3 Resolved issues in Lucent DHCP 5.4 B39

Fault ID	AR ID	Description of issue
LDHCP00000440	1-1639191	DHCP has memory leak during reliability test.
LDHCP00000605		Long option 82 fields cause server to crash.
LDHCP00000624		DHCP PID hangs at shutdown while running with SNMP 2.2.
LDHCP00000629		Vulnerability on RedHat 4.4 where server may stop responding.
LDHCP00000630	1-1630454	DHCP server unable to process messages when configuration files are not correct.
LDHCP00000641	1-1646413	5.4 B34 crashing due to renew on MDHCP object during renew address shuffle.

Resolved issues in Lucent DHCP 5.4 B34

The following table identifies the customer reported issues that were fixed in Lucent DHCP 5.4 B34.

Table 5.4 Resolved issues in Lucent DHCP 5.4 B34

Fault ID	AR ID	Description of issue
LDHCP00000529	1-1407227	Have problem with Epson projector obtaining IP address from LDHCP.
LDHCP00000555	1-1393156	DHCP Server cores when dhcp stats and file generation are done at same time.
LDHCP00000566	1-1506958	DHCP 5.4 Bld 30 crashes when renew request received for unknown lease.

Fault ID	AR ID	Description of issue
LDHCP00000582		DHCP needs to perform the hostname processing on the value returned from LDRM,according to the ClientHostNameProcessing server policy value.
LDHCP00000584		Long options are corrupted when LeaveBootPParametersInOptions policy set.
LDHCP00000586	1-1547582	Lucent DHCP is sending corrupted DHCPNak due to Option 82.
LDHCP00000588	1-1546315	DHCP 5.4 server cored during the processing of a DHCPINFORM message.
LDHCP00000276	1-1019216	DHCP Server cannot open an interface name longer than eight characters. According to the *Sun GigaSwift Ethernet Adaptor Installation and User's Guide*, the naming scheme of ce1920000 is exclusively used for virtual LAN (VLAN) interface naming. The Lucent DHCP server is not currently designed to support VLAN interfaces. This is a technical limitation of the server and the server is presently working as designed.
LDHCP00000553		In a many-to-one failover configuration, the secondary DHCP server does not correctly assign failover policy values other than the pollDelay policy. The policy values will be applied to the first primary listed in the secondary's policy file (as identified with the PrimaryIpAddr policy label), but all remaining primary servers in the secondary's policy file will use the default values assigned by the DHCP server.
LDHCP00000556		Seeing a "^B" following the circuit id in the *dhcpd.log* file when the circuit id consists of a HEX 25 or ASCII "%" sign.
LDHCP00000557		Long Options Encoding has a Memory Leak.
LDHCP00000558		Memory Leak When Using LDRM Discover/Request Callouts.
LDHCP00000561		The Linux DHCP server will SigSegV and exit if the snmp library is in place and the SNMP master agent is not running.
LDHCP00000570		Time conversion routine unnecessarily called for grant/renew lease at levelInfo.
LDHCP00000571		DHCP server logging causes unnecessary performance impact.

Fault ID	AR ID	Description of issue
LDHCP00000573		Need policy to log either CircuitID or RemoteID when "LogDhcpMsgTraffic=all".
LDHCP00000576		UpdateQIP <> delete will still send message to msg service.
LDHCP00000578		IP Address does not get marked as available once it is flagged as unavailable.

Resolved issues in Lucent DHCP 5.4 B28

The following table identifies the customer reported issues that were fixed in Lucent DHCP 5.4 B28.

Table 5.5 Resolved issues in Lucent DHCP 5.4 B28

Fault ID	AR ID	Description of issue
LDHCP00000322		DHCP Server is sending a 0.0.0.0 IP Address in the QIP Update packet under certain circumstances.
LDHCP00000335	1-1159879	DHCP Server is not populating SIAddr properly when a vendor class is being used.
LDHCP00000438	1-1214045	DHCP server sends its first address in the delete lease message in a multi-NIC environment.
LDHCP00000446	1-1261062	The DHCP Server sets both the Release and Autorelease bits in the UpdateQIP policy when UpdateQIP=autorelease.
LDHCP00000452		DHCP server offers a different IP address than the requested IP address when that address is already in a pending state.
LDHCP00000470		DHCP Failover Hangs during send of SNMP trap.
LDHCP00000472		IP address is being unreserved when another device has this IP.
LDHCP00000473		Client requested IP is being NAKed when host record does not match requested IP.

Fault ID	AR ID	Description of issue
LDHCP00000474		LeaseExpirationSleepTime and ThresholdMonitorSleepTime policies require upper limit.
LDHCP00000476		Client is being NAKed after roaming from static to dynamic and then back to static.
LDHCP00000477	1-1264635	DHCP server stops without error message.
LDHCP00000479		Server hangs after receiving HEX 25 - ASCII percent sign (%) in option 82 packet.
LDHCP00000480	1-1323390	DHCP INFORM failed to response on QIP DHCP Server.

Resolved issues in Lucent DHCP 5.4 B22

The following table identifies the customer reported issues that were fixed in Lucent DHCP 5.4 B22.

Table 5.6 Resolved issues in Lucent DHCP 5.4 B22

Fault ID	AR ID	Description of issue
LDHCP00000332	1-1161425	DHCP daemon will not start on flat subnet.
LDHCP00000333	1-1161817	Update QIP Delete option when set to false not working.

Resolved issues in Lucent DHCP 5.4 B21

The following table identifies the customer reported issues that were fixed in Lucent DHCP 5.4 B21.

Table 5.7 Resolved issues in Lucent DHCP 5.4 B21

Fault ID	AR ID	Description of issue
LDHCP00000316		DHCP crash error using java dhcp emulator when scope becomes depleted.
LDHCP00000368		Segmentation faults on startup.
LDHCP00000388		DHCP Server initializes with SNMP Module but then stops talking to it.

Resolved issues in Lucent DHCP 5.4 B11

The following table identifies the customer reported issues that were fixed in Lucent DHCP 5.4 B11.

Table 5.8 Resolved issues in Lucent DHCP 5.4 B11

Fault ID	AR ID	Description of issue
LDHCP00000314		In the policy declaration section of the log, the state of the IssueDropUnknownClientsTrap policy is being reported as the value of the DefaultDescentThreshold policy and vice versa.
LDHCP00000315		HP only. Problem processing Option 82 suboptions. When configured with a device class, the DHCP server is not supplying the additional device class options when the device class criteria are met. This issue also affects the processing of the subnet link selection suboption.

Resolved issues in Lucent DHCP 5.4 B10

The following table identifies the customer reported issues that were fixed in Lucent DHCP 5.4 B10.

Table 5.9 Resolved issues in Lucent DHCP 5.4 B10

Fault ID	AR ID	Description of issue
LDHCP00000169		Bus Error occurs in ping receive thread, shutting down server.
LDHCP00000194		Option 82 Data is not properly written to active lease file. When an incoming DHCP packet with relay agent information data (option 82) contains individual bytes with hex values greater than 0x7f, the server does not correctly write this byte or any subsequent byte of the option 82 data for this client to the active lease file.
LDHCP00000195		Change debug level feature of enhanced logging control does not work on Windows. When a Change Debug Level request (without restart) is sent from the VitalQIP GUI to a DHCP server running on Windows, the server fails to properly change the debug level. The Clear Debug Log and Stop Debug Log features do perform the requested operation.
LDHCP00000196		Failover sync binding operation may drop a lease.
LDHCP00000197		Log rolling under stress hangs Sun9 boxes.
LDHCP00000201	1-0806167	QDHCP 5.3 b8 “Dr. Watson-ed” and died after a DHCP generation or delete active lease.
LDHCP00000204	1-1006569	The DHCP BootP API does not authorize a Bootp request.
LDHCP00000208		Server hang (from delete lease during initialization).
LDHCP00000209		PostAckServerAddrOverride does not work for bootp clients.
LDHCP00000255	1-1021067	DHCP sync between Master and Failover problem.
LDHCP00000259	1-1043222	DHCP Server core dumps when attempting to send the binding updates from a primary to a restarting secondary server when there are no subnets configured.
LDHCP00000270		Force-Class policy does not correctly process similar strings.

Resolved issues in Lucent DHCP 5.4 B5

The following table identifies the customer reported issues that were fixed in Lucent DHCP 5.4 B5.

Table 5.10 Resolved issues in Lucent DHCP 5.4 B5

Fault ID	AR ID	Description of issue
LDHCP00000086		Solaris dhcpd crashes with “Debug=All FeatureTimeStamp”.
LDHCP00000110		Stop trap is not being generated when Failover server stops.
LDHCP00000129	1-0820239	DHCP server can Core or stop responding if receiving DORA traffic contains an all zero MAC address.
LDHCP00000135	1-0847285	Sending DHCP option 40 with debug enabled crashes DHCP.
LDHCP00000147	1-0882455	Configuring a global MAC pool causes server startup time to increase considerably.

6 Known issues

Overview

Purpose

This chapter describes known issues and workarounds if available for DHCP 5.4 releases.

Contents

This chapter covers these topics.

Known issues and workarounds in Lucent DHCP 5.4

The following table includes a list of known issues that were identified as customer impacting and/or outstanding customer problems not yet resolved in Lucent DHCP 5.4 B45 release.

Table 6.1 Known issues and workarounds

Fault ID	AR ID	Description of issue	Workaround
LDHCP00000522		HPUX is not logging long options.	

Known vendor issues

The following table includes a list of known vendor issues that have been identified as customer impacting problems.

Table 6.2 Known vendor issues

Fault ID	Vendor	Description of issue	Workaround
LDHCP00001781	Microsoft	Vendor Specific Info Option Order Affects Windows XP SP3 DHCP Client	Microsoft has published their Knowledgebase article and the hotfix for this issue. Refer to Article ID 953761 for more information: http://support.microsoft.com/kb/953761/en-us

7 System requirements

Overview

Purpose

This chapter describes software and hardware requirements and compatibility restrictions.

Contents

This chapter covers these topics.

Supported platforms

Lucent DHCP 5.4 B45 runs on VitalQIP 6.2, 7.0, and 7.1 remote servers. The following table lists the platforms that are supported in Lucent DHCP 5.4 B45.

Important! Platform support is dependant upon the VitalQIP Remote Server version. Reference the corresponding version of VitalQIP Release Notes for supported platforms.

Important! Support for Windows 2000 SP3 was discontinued along with the vendor. Microsoft end-of-life for Windows 2000 SP3 was June 2005.

Table 7.1 Supported platforms

VitalQIP component	Platform
VitalQIP 7.1 Remote Server	Red Hat Enterprise Linux (AS, ES – 32 bit) 4.0 –x86 platforms only Solaris 9 UltraSPARC Solaris 10 UltraSPARC Windows 2003 Standard and Enterprise Server (32 bit only) Windows 2008 Standard and Enterprise Server (32 bit and 64 bit). Requires VitalQIP 7.1 PR2.
VitalQIP 7.0 Remote Server	Red Hat Enterprise Linux (AS, ES – 32 bit) 4.0 –x86 platforms only Solaris 9 and 10 UltraSPARC Windows 2003 Standard and Enterprise Server (32 bit only)
VitalQIP 6.2 Remote Server	Windows 2000 Advanced Server SP4 Windows 2003 Enterprise Server (32 bit only) Windows 2003 Standard Server (32 bit only) Solaris 8 UltraSPARC (SPARC32PLUS only) Solaris 9 UltraSPARC Red Hat Enterprise Linux ES Release 3.0 (x86) HP-UX 11.11 (RISC Version 2.0) AIX 5.2

System patches

Ensure the appropriate operating system patches are applied before you upgrade to Lucent DHCP 5.4 B45.

The following table describes the patches to install for each platform.

Table 7.2 Platform patches

Platform	Required Patches
Linux RedHat 4.0 x86	• Ensure the Linux Developers Kit is installed. Sybase installation on Linux requires the Developers Kit to run the installation or the installation fails. • Install the Red Hat Linux patch, *compat-libstdc++-7.3-2.96.128.i386.rpm*. Visit http://www.redhat.com to download the patch.
Solaris 9 UltraSPARC	Recommended Patch Set 3/07 or newer and PatchID# 111711-16, 111712-16 and 111722-05 (or superseded patch#).
Solaris 10 UltraSPARC	Recommended Patch Set 2/07 or newer.
Windows 2003	Recommended Patch SP2.

Software requirements

The section lists the software requirements for Lucent DHCP 5.4 B45. Please note if you are not currently running on the supported platform version, you are strongly encouraged to upgrade to the supported version.

Important! You must select UNICODE and UTF-8 support, as well as the desired languages during the Solaris Operating System and Database installation. This step is mandatory. (VQIP00017643)

The following table lists the software requirements for Lucent DHCP 5.4.

Table 7.3 Software requirements

Software	Version	Description/comments
VitalQIP	7.1	Lucent DHCP 5.4 B34 is delivered with VitalQIP 7.1.

Software	Version	Description/comments
VitalQIP	7.0	Lucent DHCP 5.4, Build 28 is delivered with VitalQIP 7.0 (Oct 2006 Release).
VitalQIP	6.2	DHCP 5.4, Build 21 is delivered with VitalQIP 6.2. This is the minimum version for use with VitalQIP 6.2. DHCP 5.4, Build 22 or greater of the DHCP server includes LDRM support. For more information on LDRM and supported platforms, see the LDRM Release Notes.

Hardware requirements

The following table lists the hardware requirements for Lucent DHCP 5.4 B45.

Table 7.4 Hardware requirements

Component	Windows/Linux	UNIX
VitalQIP Remote Server	500 Mhz Pentium processor, or higher	300 Mhz processor
	256 MB memory, minimum	256 memory minimum per processor, more is strongly recommended
	300 MB of disk space	300 MB of disk space

Compatibility restrictions

VitalQIP 7.1 supports DNS/DHCP Generation and message compatibility with pre-VitalQIP 7.1 remote servers for the following versions of VitalQIP when they are on the most current patch level:

- VitalQIP 6.2
- VitalQIP 7.0

Important! Contact Technical Support before upgrading from VitalQIP 6.1 SP1 (or earlier release) to VitalQIP 7.1 to determine if a direct upgrade is possible.

Third-party or other hardware/software requirements

VMware support policy

Customers, who choose to run VitalQIP or any VitalQIP add-ons under VMware, will be supported as follows:

If an AR (Assistance Request) is opened with Alcatel-Lucent Support, customers must clearly state whether they are running the VitalQIP software in a VMware environment. It will be generally assumed that the issue being reported is common between the VMware environment and a native supported platform, and support will make every effort to resolve the problem, however respond-only objectives will apply if the issue is Vmware related. In the event it becomes impossible to determine whether the problem exists with VitalQIP software or VMware, Alcatel-Lucent support reserves the right to request that the customer reproduce the issue in a native environment before further troubleshooting is attempted.

Certified performance numbers on the officially certified platforms may not hold true under VMware.

Solaris 10 Container support policy

Customers who choose to run VitalQIP components in a Solaris 10 environment will be supported as follows:

- VitalQIP Enterprise Server or Remote Server (DNS Only) will run in a Solaris 10 Container environment. The DHCP server cannot support the virtual interfaces in a container on Solaris 10.
- The customer must reproduce any problems on a native Solaris 10 platform. If the problem is reproducible in the native environment, then the customer can enter a ticket with Alcatel-Lucent Support.
- Be sure to explain that this system is running in a Solaris 10 container environment but that the problem was replicated in a supported environment. Include the version of VitalQIP you are running.
- If the problem is not reproducible in the native Solaris 10 platform, the customer must open a support request with Sun Microsystems.

8 Installation and upgrade notes

Overview

Purpose

This chapter covers the upgrade of the Lucent DHCP Service, versions 5.4 build 5 and higher to Lucent DHCP 5.4 B45. The instructions in this chapter cover upgrades on Windows and UNIX platforms. Be aware that the failover/secondary servers must be upgraded before the primary partner servers are upgraded.

Contents

This chapter covers these topics.

Upgrade to Lucent DHCP 5.4 B45 on Windows

Upgrade procedure for Windows

To upgrade to Lucent DHCP 5.4 B45, follow these steps:

1. Open the VitalQIP Service Controller by accessing **Start | Programs | VitalQIP | Service Controller**. The Service Controller window appears.
2. Stop the Lucent DHCP Service. Right-click **Lucent DHCP Service** and select **Stop**.
3. In Windows Explorer, copy the new DHCP executable **`dhcpservice.exe`** to *%QIPHOME%/dhcp*.
4. Start the Lucent DHCP Service. In the VitalQIP Service Controller, right-click the **Lucent DHCP Service** and select **Start**.

END OF STEPS

Upgrade to Lucent DHCP 5.4 B45 on UNIX

UNIX only: pre-upgrade requirement

Before you upgrade to Lucent DHCP 5.4 B45 on UNIX, the environment variables must be set. The environment variables will need to be set each time you start Lucent DHCP 5.4 B45. Environment variables and their values are stored in *$QIPHOME/etc/shrc* or *$QIPHOME/etc/cshrc*.

To set your environmental variables, issue the following commands:

```
#cd <VitalQIP_directory>/etc
#. ./shrc OR source cshrc
```

Upgrade procedure for UNIX

To upgrade to Lucent DHCP 5.4 B45, follow these steps:

1. Find the process ID (PID) of DHCP Server by running:
   ```
   ps -ef | egrep dhcpd
   ```
2. Run kill ***<PID>*** for Lucent DHCP Server (**`dhcpd`**).

3 Copy the executable **`dhcpd`** to *$QIPHOME/usr/bin*.

4 Start the VitalQIP DHCP Server by running:

```
$QIPHOME/usr/bin/dhcpd –f$QDHCPCONFIG
```

END OF STEPS