



VitalQIP

DNS/DHCP & IP MANAGEMENT SOFTWARE | VitalQIP DHCP

Release 6.0, Build 67
RELEASE NOTES

Nokia and the Nokia logo are trademarks of Nokia. All other trademarks are the property of their respective owners.

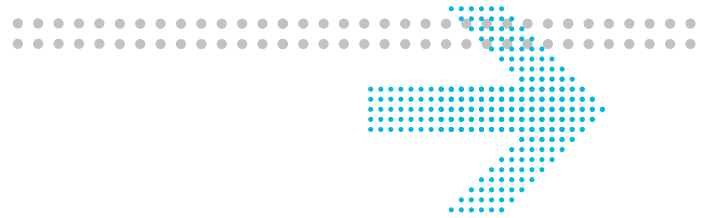
The information presented is subject to change without notice. Nokia assumes no responsibility for inaccuracies contained herein.

Copyright © 2021 Nokia. All Rights Reserved.

Licenses

Refer to Appendix B, “Third party software license statements” in the *Nokia Release 21 Installation Guide* (9YZ093320001RJZZA) for a complete description of all software licenses used to develop this product.

Contents



About this document

Purpose	v
Reason for reissue	v
Conventions used	ix
Related information	ix
Technical support	x

1 Release components

Software deliverables	1-2
How to obtain software	1-2
Document deliverables	1-4
To obtain documentation	1-4

2 New features

New features	2-2
Nokia DHCPv4 MIB variables	2-18
Trap object IDs (OIDs)	2-32

3 Test results

4 Changes to interfaces, alarms, and messages

5 Resolved issues

Resolved issues in Nokia DHCPv4 6.0, Build 67	5-3
Resolved issues in Nokia DHCPv4 6.0, Build 64	5-4
Resolved issues in Nokia DHCPv4 6.0, Build 60	5-5
Resolved issues in Nokia DHCPv4 6.0, Build 56	5-6
Resolved issues in Nokia DHCPv4 6.0, Build 51	5-7
Resolved issues in Nokia DHCPv4 6.0, Build 50	5-8
Resolved issues in Nokia DHCPv4 6.0, Build 49	5-9
Resolved issues in VitalQIP DHCPv4 6.0, Build 46	5-10
Resolved issues in VitalQIP DHCPv4 6.0, Build 37	5-12
Resolved issues in VitalQIP DHCPv4 6.0, Build 30	5-13

	Resolved issues in VitalQIP DHCPv4 6.0, Build 28	5-14
	Resolved issues in VitalQIP DHCPv4 6.0, Build 27	5-15
	Resolved issues in VitalQIP DHCPv4 6.0, Build 24	5-16
	Resolved issues in VitalQIP DHCPv4 6.0, Build 20	5-17
	Resolved issues in VitalQIP DHCPv4 6.0, Build 14	5-18
	Resolved issues in VitalQIP DHCPv4 6.0, Build 11	5-19
	Resolved issues in VitalQIP DHCPv4 6.0, Build 10	5-20
6	Known issues	
	Known issues and workarounds	6-2
	Known vendor issues	6-4
7	System requirements	
	Supported platforms	7-2
	Software requirements	7-2
	Hardware requirements	7-3
	Compatibility restrictions	7-3
8	Installation and upgrade notes	
	Performing first-time installation	8-2
	Upgrade to VitalQIP DHCPv4 6.0 on Windows	8-2
	Upgrade to VitalQIP DHCPv4 6.0 on UNIX	8-3
	Upgrade Nokia DHCPv4 in a failover configuration	8-4
	Enable Client ID	8-5
	Configuring SNMP 3.0 on Linux	8-6
	Configuring SNMP log rotation on Unix	8-8
	Configuring SNMP 3.0 (using Net-SNMP) on Windows	8-15
	Configuring SNMP Traps for all platforms	8-16
	CONFIGURATION	8-17
	VERIFICATION	8-19

About this document



Purpose

This document provides important information about the contents of VitalQIP DHCPv4 6.0 Build 67. It covers new features, system requirements, product installation and upgrades, as well as resolved problems and known issues.

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

Reason for reissue

The following table shows the revision history of this document

Issue	Feature name	Description	Feature impact
21	New features	Added 3 new features.	“Nokia DHCPv4 6.0, Build 67 New features” (p. 2-2)
21	Resolved issues	Added 4 resolved issues.	“ARs resolved in Build 67 release” (p. 5-3)
20	New features	Added 3 new features.	“Nokia DHCPv4 6.0, Build 64 New features” (p. 2-3)
20	Resolved issues	Added 1 resolved issues.	“Resolved issues in Nokia DHCPv4 6.0, Build 64” (p. 5-4)
20	Supported platforms	Added Windows 2016 Standard Server.	“Supported platforms” (p. 7-2)
19	Resolved issues	Added 4 resolved issues.	“Resolved issues in Nokia DHCPv4 6.0, Build 60” (p. 5-5)
19	New features	Added 3 new features.	“Nokia DHCPv4 6.0, Build 60 New features” (p. 2-4)
19	Known issues	Removed LDHCP00013019 from known issues.	Table 6-1, “Known issues and workarounds” (p. 6-2)
18	Known issues	Added LDHCP00013019 to known issues.	Table 6-1, “Known issues and workarounds” (p. 6-2)

Issue	Feature name	Description	Feature impact
18	Resolved issues	Added 2 resolved issues.	“Resolved issues in Nokia DHCPv4 6.0, Build 56” (p. 5-6)
18	New features	Added 3 new features.	“Nokia DHCPv4 6.0, Build 56 New features” (p. 2-5)
18	Supported platforms	Removed Solaris support.	“Supported platforms” (p. 7-2)
17	Resolved issues	Added 2 resolved issues.	“Resolved issues in Nokia DHCPv4 6.0, Build 51” (p. 5-7)
16	Known issues	Added LDHCP00012998 to known issues.	Table 6-1, “Known issues and workarounds” (p. 6-2)
16	Resolved issues	Added 4 resolved issues.	“Resolved issues in Nokia DHCPv4 6.0, Build 50” (p. 5-8)
16	New features	Added 3 new features.	“Nokia DHCPv4 6.0, Build 50 New features” (p. 2-6)
15	Resolved issues	Added 4 resolved issues.	“Resolved issues in Nokia DHCPv4 6.0, Build 49” (p. 5-9)
14	Supported platforms	Added Red Hat Enterprise Linux (AS,ES) 7.1 into supported platforms list.	“Supported platforms” (p. 7-2)
14	Known issues	Added issue LDHCP00012831.	Table 6-1, “Known issues and workarounds” (p. 6-2)
14	New features	DHCPv4 stats are generated on a periodic basis in an XML format.	Table 2-7, “VitalQIP DHCPv4 6.0, Build 46 New features” (p. 2-9)
14	Resolved issues	Added 7 resolved issues.	“Resolved issues in VitalQIP DHCPv4 6.0, Build 46” (p. 5-10)
13	New features	Renamed PostAckServerAddrOverride policy to DhcpLeaseUpdateServerAddress	Table 2-8, “VitalQIP DHCPv4 6.0, Build 37 New features value” (p. 2-10)
13	Resolved issues	Added 3 resolved issues.	“Resolved issues in VitalQIP DHCPv4 6.0, Build 37” (p. 5-12)
12	New features	<ul style="list-style-type: none"> Added support for DHCPv4 SNMP log rotation. Added support for zero MAC when assigning manual DHCPv4 by client ID addresses. 	“VitalQIP DHCPv4 6.0, Build 30 New features” (p. 2-11)
12	Known vendor issues	Removed issue LDHCP00002014.	“Known vendor issues” (p. 6-4)
12	Known issues	Removed Issue LDHCP00012061.	Table 6-1, “Known issues and workarounds” (p. 6-2)

Issue	Feature name	Description	Feature impact
12	Resolved Issues	Added 5 resolved issues.	“Resolved issues in VitalQIP DHCPv4 6.0, Build 30” (p. 5-13)
11	New features	<ul style="list-style-type: none"> Added new ThresholdTrapMinimumScopeSize server policy. Added new DHCPv4 server policy DhcpSyslogLevel. Added new Ipv6UpdateMessageTransport policy. Added support for new update-qip configuration file policy for both subnet and scope levels. 	“VitalQIP DHCPv4 6.0, Build 28 New features” (p. 2-12)
11	Known issues	Added Issue LDHCP00012061.	Table 6-1, “Known issues and workarounds” (p. 6-2)
11	Resolved issues	Added 2 resolved issues.	Table 5-11, “ARs resolved in Build 28 release” (p. 5-14)
10	New features	<ul style="list-style-type: none"> Added new ShareManualBootpAndManualDHCP policy. Added SupportVirtualInterfaces and FailoverVirtualAddress policies to support use of virtual interfaces on Linux and Solaris. 	“New features in previous releases” (p. 2-13)
10	Resolved issues	Added 4 resolved issues.	Table 5-12, “ARs resolved in Build 27 release” (p. 5-15)
9	New features	<ul style="list-style-type: none"> Ability to assign Client Classes to Scope or Object not just Subnet or Server level. Allow the DHCPv4 Server Policy SupportClientId to be configurable on the Subnet Level. 	“New features in previous releases” (p. 2-13)
9	Resolved issues	Added 5 resolved issues.	Table , “Resolved issues in VitalQIP DHCPv4 6.0, Build 24” (p. 5-16)
8	Resolved issues	Added 6 resolved issues.	Table , “Resolved issues in VitalQIP DHCPv4 6.0, Build 20” (p. 5-17)
8	Known issues	Removed LDHCP0003212 from Known issues.	Table 6-1, “Known issues and workarounds” (p. 6-2)

Issue	Feature name	Description	Feature impact
8	New features	<ul style="list-style-type: none"> Minimum Client ID length requirement when SupportClientId enabled. Add support for a new option-class client class. Client ID option in DHCPOFFER, DHCPACK and DHCPNAK. Multiple destinations for SNMP traps in DHCPv4 6.0. 	“New features in previous releases” (p. 2-13)
7	Resolved Issues	<ul style="list-style-type: none"> Added LDHCP00011894. Updates for LDHCP00011969. 	<ul style="list-style-type: none"> Table , “Resolved issues in VitalQIP DHCPv4 6.0, Build 14” (p. 5-18) “Upgrade to VitalQIP DHCPv4 6.0 on Windows” (p. 8-2) and “Upgrade to VitalQIP DHCPv4 6.0 on UNIX” (p. 8-3)
6	Resolved Issues	Added 5 resolved issues.	Table , “Resolved issues in VitalQIP DHCPv4 6.0, Build 14” (p. 5-18)
5	Resolved Issues	Added LDHCP00009060.	Table , “Resolved issues in VitalQIP DHCPv4 6.0, Build 11” (p. 5-19)
4	Resolved Issues	Added LDHCP00009056.	Table , “Resolved issues in VitalQIP DHCPv4 6.0, Build 10” (p. 5-20)
3	New features	<ul style="list-style-type: none"> Added new feature “DHCPv4 server support for adhering to option 57, maximum message size”. Added new feature “Ping preclusion policy”. Added new feature “Support for new MinimumRequestedLeaseTime policy”. Added new feature “Support for new DropInformsWhenNotActive policy”. Added new feature “Support for DHCPv4 on Solaris 10 Zones/Containers”. 	“New features in previous releases” (p. 2-13)
3	Resolved Issues	Added 5 resolved issues.	“Resolved issues in VitalQIP DHCPv4 6.0, Build 10” (p. 5-20)

Issue	Feature name	Description	Feature impact
2	Known vendor issue	Added Issue LDHCP00002014	“Issues raised by customers are tracked by the Technical Support team. For more information about these issues, contact “Technical support” (p. 1-x).” (p. 6-3)
1	Known vendor Issues	Added Issue LDHCP00003209	“Issues raised by customers are tracked by the Technical Support team. For more information about these issues, contact “Technical support” (p. 1-x).” (p. 6-3)

Conventions used

This document uses the following typographical conventions:

Appearance	Description
<i>Italicized text</i>	<ul style="list-style-type: none"> File and directory names Titles of publications A value that the user supplies
<i>Bold italicized text</i>	<ul style="list-style-type: none"> Emphasized information
graphic user interface text or key name	<ul style="list-style-type: none"> Text that is displayed in a graphical user interface or in a hardware label The name of a key on the keyboard
input text	Command names and text that the user types or selects as input to a system
<input variable>	Input variable for which you must substitute another value. The angle brackets also indicate the value is a variable.
output text	Text that a system displays or prints

Related information

The following documents are referenced in these release notes:

- *VitalQIP Administrator Reference Manual* (part number: 9YZ-08807-0001-RKZZA)
This guide describes planning and configuring your network, information about the VitalQIP interface, advanced DNS and DHCPv4 configurations, and troubleshooting.
- *VitalQIP Installation Guide* (part number: 9YZ-08807-0001-RJZZA)
This guide describes how to install the VitalQIP product.
- *VitalQIP Command Line Interface User's Guide* (part number: 9YZ-08807-0002-TCZZA)
This guide discusses and describes how to use the *VitalQIP Command Line Interface*.
- *VitalQIP Web Client User's Guide* (part number: 9YZ-08807-0001-TCZZA)
This guide describes how to use the web client interface.

Technical support

If you need assistance with Nokia, you can contact the Technical Assistance Center for your region. Contact information is provided in the following table.

Region	Contact information
North America	Phone 1-866-LUCENT (582-3688) Option 1, Option 2 E-mail: support@nokia.com Web: https://customer.nokia.com/support/s/
Other Regions	E-mail: support@nokia.com Web: https://customer.nokia.com/support/s/ Select your country for telephone contact information.



1 Release components

Overview

Purpose

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

Contents

This chapter covers these topics.

Software deliverables	1-2
How to obtain software	1-2
Document deliverables	1-4
To obtain documentation	1-4

Software deliverables

The following table lists the software that comprises the VitalQIP DHCPv4 6.0 Build 67 release.

Table 1-1 Software deliverables

Type	Platform	Directory	File
Nokia DHCPv4 6.0 Software	Linux	<i>VitalQIP/LDHCP/DHCP6.0/Linux/DHCP6.0B67-Linux</i>	<i>DHCP6.0.67-linux-gcc3.tar</i>
	Windows	<i>VitalQIP/LDHCP/DHCP6.0/Windows/DHCP6.0B67-Windows</i>	<i>DHCP6.0.67-w2k.zip</i>

Note: SNMP plugin(sub agent) is delivered along with VitalQIP DHCPv4 server software.

How to obtain software

VitalQIP DHCPv4 6.0 Build 67 installation files are available for download via Nokia OnLine Customer Support (OLCS) services. OLCS uses secure HTTP and FTP to download files and documentation. In order to use OLCS, you must be registered with Nokia Global Support.

If you are not registered with Nokia Global Support, visit <https://customer.nokia.com/support/s/>. If you need assistance in registering, contact the Nokia 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-na.support.nokia.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://online.networks.nokia.com/newaccount/email.faces>
- 2 Once registered, open a browser and go to <https://customer.nokia.com/support/s/>

-
- 3 Log in with your user name and password. The Nokia support portal is displayed.
 - 4 In the **Software Downloads** drop down list, select **VitalQIP** and click **Submit**.
 - 5 Under the line “**Please navigate through the hierarchy to download:**”, select **LDHCP**.
 - 6 Select **DHCPv4** and then the desired Operating System.
 - 7 Select the build(s) you wish to download from the list and then click Next.
 - 8 Specify the download directory on your local machine.
 - 9 Click **Download** to use the legacy download agent, or **Download Plus** to use the GetPlus[®] download agent.

END OF STEPS

Downloading Net-SNMP (Master Agent)

Table 1-2 Net-SNMP downloading locations

Type	Platform	Directory
Net-SNMP	Linux	http://net-snmp.sourceforge.net/download.html
	Windows	http://www.net-snmp.org

Note: The above table gives the possible ways to get the SNMP master agent.

Document deliverables

Documentation available for this release

The following table lists the available documentation for the VitalQIP DHCPv4 6.0 Build 67 release.

Table 1-3 Documentation list

Document ID	Document title
190-409-114R6.0	Nokia DHCPv4 6.0 Release Notes

To obtain documentation

In addition to the OLCS site, VitalQIP product documentation is available to customers through OnLine Customer Support (OLCS).

To navigate OLCS, follow these steps:

-
- 1 If you have not registered, register at <https://online.networks.nokia.com/newaccount/email.faces>
 - 2 Open a browser and go to <https://support.alcatel-lucent.com/portal/olcsHome.do>.
 - 3 Log in with your user name and password. The Customer Center is displayed.
 - 4 In the **Software Downloads** drop down list, select **VitalQIP** and click **Submit**.
-

-
- 5 Under the line “**Please navigate through the hierarchy to download:**”, select **LDHCP**.
 - 6 Select **DHCPv4** and then select **Docs**.
 - 7 Select documents from the **Please select one or more Downloads** check list and click **Next**.
 - 8 Specify the download directory on your local machine.
 - 9 Click **Download** to use the legacy download agent, or **Download Plus** to use the GetPlus[®] download agent.

END OF STEPS



2 New features

Overview

Purpose

The following sections identify the new features and/or capabilities contained in VitalQIP DHCPv4 6.0.

Contents

This chapter covers these topics.

New features	2-2
Nokia DHCPv4 MIB variables	2-18
Trap object IDs (OIDs)	2-32

New features

Following are new features included in Nokia DHCPv4 6.0, Build 67

Table 2-1 Nokia DHCPv4 6.0, Build 67 New features

Feature ID	Feature Name	Description
LDHCP00013051	Include Org ID in scope utilization alert message	Included the org ID associated with the DHCPv4 server in the scope utilization alert message from the DHCPv4 server in order to support the VitalQIP requirement to email the DHCP scope utilization alert.
LDHCP00013053	SuppressActiveLeasePing enhancement	Enhanced SuppressActiveLeasePing logic, when processing a DISCOVER message, to preclude the ping when lease status is PENDING for less than MaxPendingSeconds. This change is intended to accommodate the rare case where a client with an active lease sends back to back DISCOVER messages, both with ciAddr=0.0.0.0, due to the first DISCOVER being lost on the network.
LDHCP00013049	Support for new IPv6-Only Preferred option	Added support for the IPv6-Only Preferred option (RFC 8925). The DHCPv4 server will now include the new option (108) in DHCPOFFER and DHCPREQUEST messages, which specifies a wait time, when requested by the DHCPv4 client. The wait time, in seconds, can be configured at the server level (Ipv6OnlyPreferredWaitTime) or at the subnet level and specifies the number of seconds for which the client should disable DHCPv4 processing. This feature is intended to be utilized in dual stack networks and can be used to indicate that a host supports an IPv6-only mode and is willing to forgo obtaining an IPv4 address.

Following are new features included in Nokia DHCPv4 6.0, Build 64

Table 2-2 Nokia DHCPv4 6.0, Build 64 New features

Feature ID	Feature Name	Description
LDHCP00013035	Option Class Client Class enhancement to allow User Class (77) and Vendor Class (60) option numbers	Changed configuration file option class client class processing to allow for option class client classes to be defined for option 77 (user class) and option 60 (vendor class). Previously, these were not allowed, due to the existing capability to utilize the user class and vendor class client class types. This change will allow for more flexibility in defining which options are sent to a client in the DHCP offer and ack messages when multiple option class client classes are defined which include option 60 and/or 77. Client class options will be offered to the DHCP client using whichever matching option class client class occurs first in the server's configuration file, within the current option class client class precedent ordering of object, followed by subnet, followed by server level.
LDHCP00013038	Enhanced the DHCP server syslog/event log information	Enhanced the DHCP server syslog/event log information for each of the following scenarios: <ol style="list-style-type: none"> 1. For each ping response received, indicating a target address already in use, included the requesting client MAC and XID in the log message. 2. For each DHCP packet dropped due to the subnet the client is on not being served, logged the event, including the client MAC and XID. 3. When the secondary failover server determines that a partner primary is not running, included the primary's IP address in the log message.

Feature ID	Feature Name	Description
LDHCP00013039	DHCP scope utilization alerts	The DHCP scope utilization feature has been enhanced to support the sending of a new DHCP scope utilization alert message type to the QIP Update Service when the scope percent utilization exceeds the configured threshold. Support for unique scope threshold values assigned to individual scopes in the DHCP configuration file has been added as well, using a new scope level configuration policy, named scope-unavailable-threshold. The DHCP server will also send the new DHCP scope utilization alert message when scope utilization exceeds the subnet-unavailable-threshold and the scope size exceeds the previously implemented ThresholdTrapMinimumScopeSize server policy, but only if there is no scope-unavailable-threshold policy assigned to the scope. In other words, the scope-unavailable-threshold policy will take precedence for a scope when both threshold policies are specified.

Following are new features included in Nokia DHCPv4 6.0, Build 60

Table 2-3 Nokia DHCPv4 6.0, Build 60 New features

Feature ID	Feature Name	Description
LDHCP00013024	DHCPv4 server policy to send grant type lease update to VitalQIP for init-reboot requests	A new server level policy, SendGrantUpdateForInitReboot, will specify the type of lease update request that is sent to qip-qipupdated after ACK-ing an init-reboot from a DHCP client. When the policy is TRUE/enabled, the grant type update request message is sent, otherwise the renew type update request message is sent. The default is FALSE/disabled, retaining the preexisting server behavior.

Feature ID	Feature Name	Description
LDHCP00013026	DHCPv4 server policy to preclude writing of client vendor class values to the active lease file	A new server level policy, PrecludeVendorClassDbWrite, provides the capability to preclude writing DHCP client vendor class values to the active lease file when the policy is set to TRUE (default is FALSE/disabled). This feature can be used to reduce the size of the active lease file when storage of the vendor class is not necessary or to eliminate malformed entries when client provided vendor class strings contain non-printable character values.
LDHCP00013030	DHCPv4 server and subnet level excluded fingerprints	The DHCPv4 server will support the specification of excluded fingerprint tables in the server's configuration file, at both the server and subnet levels. When a DHCP client fingerprint matches an excluded fingerprint from the server level table, or the appropriate subnet table, the DHCP client request will be dropped and an informational debug log entry written. The excluded fingerprint processing, as well as the previously provided scope level fingerprint policy processing, must be enabled by setting the DhcpFingerprinting server policy to TRUE (default is FALSE/disabled). Logging of excluded DHCP client requests can be precluded by setting the LogExcludedFingerprints to FALSE (default is TRUE).

Following are new features included in Nokia DHCPv4 6.0, Build 56

Table 2-4 Nokia DHCPv4 6.0, Build 56 New features

Feature ID	Feature Name	Description
LDHCP00012991 (AR-1-6486855)	DHCP should automatically create a new subnet if it receives a Dynamic MDHCP update for an address which is not in an existing subnet	Added support for dynamically creating a subnet when a dynamic MDHCP update specifies an IP address not in a currently defined subnet.

Feature ID	Feature Name	Description
LDHCP00013004	DHCPv4 server should support DHCP fingerprinting to control address scope assignment	The DHCPv4 server now provides a new feature that utilizes the client DHCP fingerprint to determine what address scope(s) are valid for address assignment. The DHCP fingerprint is defined to be the exact sequence of DHCP options specified in the client's parameter request list (option 55), contained in the DHCPDISCOVER message. This feature is enabled with a server level policy (DhcpFingerprinting default=off) and utilizes a new DHCP scope level configuration file policy, dhcp-fingerprint, which specifies the exact sequence of DHCP options that must be in the client's parameter request list in order for an address from the scope to be assigned.
LDHCP00013015	Dynamic MDHCP update success status improvement	Added improved success status determination of dynamic MDHCP updates and the reintroduction of all dynamic MDHCP updates received since the last DHCP generation, when the server is stopped and restarted (ie. cold started). The DHCP server will accomplish this by performing a copy/append of the contents of the dhcpd_update.conf file into a new journal file, dhcpd_update.conf.journal after each successful dynamic MDHCP update. On a cold start, the updates in the journal file, if it exists, will be read into the server's internal configuration. On a DHCP server HUP/reload, which occurs with a DHCP generation, the journal file will be removed, since the MDHCP objects it contains should now be in the normal config file, dhcpd.conf, received from VitalQIP as a result of the DHCP generation.

There is no new feature in Nokia DHCPv4 6.0, Build 51.

Following are new features included in Nokia DHCPv4 6.0, Build 50

Table 2-5 Nokia DHCPv4 6.0, Build 50 New features

Feature ID	Feature Name	Description
LDHCP00012983 (AR 1-6430145)	DHCP should not assign ping threads based on MAC address if SupportClientID is True	Added support for an alternative semaphore to ensure synchronous processing of packets from a particular client. This semaphore will replace the use of the MAC based semaphore, and be enabled with the new AlternateSemaphoreForCID policy (default=0). This policy is designed to support DHCP servers with client ID lease tracking enabled (SupportClientId=1) and where a security appliance is overriding the clients' MAC address with it's own MAC address in DHCPDISCOVER packets. DHCP servers using such a security appliance should use this feature in order to ensure timely processing of DHCP traffic from all clients whose packets pass through the appliance.
LDHCP00012988	Chart stats should include counts for dropped not serving subnet and a thread pool busy count	Added additional fields to the chart stats file output for thread pool busy count and dropped not serving subnet count. The thread pool busy count is incremented by the DHCP server when a new DHCP client message has been read from the UDP port and all pool threads are currently busy processing other client messages. The new message will be processed as soon as a pool thread is available. Also the minimum ChartStatsFrequency policy value has been changed to 15 seconds. The default remains 300 seconds and a value of zero disables the generation of the chartstats file.
LDHCP00012993	DHCP chartstats file should eliminate the xml format	Converted the chart stats file from an XML format to a plain text file and changed the name to dhcpd_chart.stats.

Following are new features included in Nokia DHCPv4 6.0, Build 49

Table 2-6 Nokia DHCPv4 6.0, Build 49 New features

Feature ID	Feature Name	Description
LDHCP00012974	DHCPv4 support for rapid commit option - RFC 4039	Added support for the rapid commit option (80) that is defined in RFC 4039. This feature will only be allowed when the DHCP client includes the rapid commit option in the DHCPDISCOVER message and the feature is enabled with the RapidCommitEnabled server level policy or the object/range level policy (rapid-commit-enabled). The default value for these policies is FALSE (0) and the object/range value, when explicitly configured, will override the server level setting.
LDHCP00012975	New counters to support DHCP analytics	Added new counters to the chartstats output in order to support DHCP analytics. Also converted the leases per second variables (current and max) to a floating point number to provide two decimal places of precision. The new counters are as follows: dropped-depleted-subnet-client-count, abusive-client-count, ping-response-received-count, dropped-unregistered-client-count, dropped-excluded-client-count, dropped-zero-MAC-addr-client-count.
LDHCP00012981 (AR 1-6214902)	New Allow_Underscores value for ClientHostNameProcessing server policy	The DHCP server ClientHostNameProcessing feature supports a new setting that allows underscores in a label while still correcting other non-rfc compliant characters. This setting will accomodate Windows clients that allow for underscores in the hostname.

Following is new feature included in VitalQIP DHCPv4 6.0, Build 46

Table 2-7 VitalQIP DHCPv4 6.0, Build 46 New features

Feature ID	Feature Name	Description
LDHCP00012837	DHCP stats should be generated on a periodic basis in an xml format for display.	The DHCP server can now generate a statistics file at a periodic frequency, specified by the ChartStatsFrequency server policy value, in an xml format.

Following is new feature included in VitalQIP DHCPv4 6.0, Build 37:

Table 2-8 VitalQIP DHCPv4 6.0, Build 37 New features value

Feature ID	Feature Name	Description
LDHCP00012116	Renamed PostAckServerAddrOverride policy to DhcpLeaseUpdateServerAddress	The DhcpLeaseUpdateServerAddress policy defines the DHCP server address that will be included in each lease update message. This value is included in the lease update sent to Nokia in order to support a forthcoming (VitalQIP 8.0PR6) lease audit feature by DHCP server address.

Following are new features included in VitalQIP DHCPv4 6.0, Build 30:

Table 2-9 VitalQIP DHCPv4 6.0, Build 30 New features

Feature ID	Feature Name	Description
LDHCP00011961	Added support for DHCPv4 SNMP log rotation.	The DHCPv4 SNMP log rotation is controlled by the following policies residing in the DHCPv4 server policy file: SnmppDebugRotateFilesize, SnmppDebugRotateInterval, SnmppDebugRotateMaxDepth. For how to configure it, refer to “Configuring SNMP log rotation on Unix” (p. 8-8).
LDHCP00012105	Allow zero MAC when assigning manual DHCP addresses by client ID.	The DHCPv4 SupportClientId feature will allow DHCP client packets that contain a zero MAC address to be offered/assigned manual DHCP addresses based upon the client ID.

Following are new features included in VitalQIP DHCPv4 6.0, Build 28:

Table 2-10 VitalQIP DHCPv4 6.0, Build 28 New features

Feature ID	Feature Name	Description
	Added new ThresholdTrapMinimumScopeSize server policy.	<p>The ThresholdTrapMinimumScopeSize policy provides support for scope level lease threshold processing and trap issuance. When the policy value is zero (default=0), scope level threshold processing will not be performed. If the policy is set to a non-zero value less than 10, the server will override the policy value to 10. The ThresholdTrapMinimumScopeSize does NOT specify the threshold percentage, but rather the minimum scope size for which a scope threshold trap will be issued. When this policy is not set, scope traps will not be issued. The scope level threshold processing uses the applicable subnet threshold policy values if defined or the server level policy values when there is no subnet value defined.</p> <p>Note: Either the DefaultUnavailableThreshold or DefaultDescentThreshold server level policy must be set to a non-zero value to enable threshold processing.</p>
	Added the new DHCP server policy DhcpSyslogLevel.	<p>The DhcpSyslogLevel policy specifies the level of messages that will be written to syslog/event log. The policy can be set to none, error, warning, or info and defines the minimum level that will be written to the log. When set to "none", the server will not log any messages. The default value for the policy is "info", which specifies all messages are logged.</p>
	Added new Ipv6UpdateMessageTransport policy.	<p>The Ipv6UpdateMessageTransport policy is used to enable the lease updates to the message service to be sent via IPv6. The default value for this policy is 0 (disabled), so that the default behavior of the DHCPv4 server is to continue sending lease update messages as it historically has done, using IPv4 transport.</p>

Feature ID	Feature Name	Description
	Added support for new update-qip configuration file policy for both subnet and scope levels.	A scope level setting will override any subnet and server settings. A subnet level setting will override the server policy. The available scope and subnet values are the same as those available at the server policy level (ie. all, none, grant, renew, release, decline, delete, expiration, autorelease, bootp). Multiple values may be specified in a single policy statement, separated by a space.

Following are new features included in the previous releases.

Table 2-11 New features in previous releases

Feature ID	Feature Name	Description
	Added new ShareManualBootpAndManualDHCP policy.	The ShareManualBootpAndManualDhcp policy, when enabled in the DHCP server policy file, will allow for the sharing of the two different types of manual objects by the DHCP server when assigning addresses.
	Added SupportVirtualInterfaces and FailoverVirtualAddress policies to support use of virtual interfaces on Linux and Solaris.	The SupportVirtualInterfaces policy will allow the DHCP server to bind to virtual interfaces with a colon (:) in the interface name. The FailoverVirtualAddress policy will explicitly define the IP address that the failover socket will bind to for communication with the partner server. When not specified, the default behavior for the failover socket is to bind to INADDR_ANY (0.0.0.0). The virtual interface support is only available on Linux and Solaris systems. The SupportVirtualInterfaces policy must be enabled to use the FailoverVirtualAddress policy. With the SupportVirtualInterface policy enabled, the DHCP server will listen for client DHCP traffic on any configured virtual interface. The FailoverVirtualAddress policy allows for either failover partner in a failover configuration to listen on the specific interface address specified.

Feature ID	Feature Name	Description
	Ability to assign Client Classes to Scope or Object not just Subnet or Server level.	<p>Added support to recognize client class specified at the manual object and DHCP scope levels within the DHCP server configuration file.</p> <p>This feature allows one or more option class, user class and/or vendor class client classes to be included in any manual DHCP objects, automatic DHCP scope, or dynamic DHCP scope.</p> <p>The purpose of this feature is to allow for more flexibility when defined DHCP option that client will receive, utilizing the conditional assignment logic that the various client classes provide.</p>
	Allow the DHCP Server Policy SupportClientId to be configurable on the Subnet Level.	<p>Added support for a subnet level configuration file policy, support-client-id, that can be set to “on” or “off”, which overrides the server level SupportClientid policy, and determines whether the DHCP server will track leases by client ID within the subnet.</p>
	Minimum Client ID length requirement when SupportClientId enabled.	<ul style="list-style-type: none"> Added support for new <i>MinimumClientIdLength</i> policy (default = 7). Used to ensure uniqueness for lease tracking. When <i>SupportClientId</i> is enabled and a client specifies an option 61 (clientId) value whose length is less than this policy value, the client packet will be dropped.

Feature ID	Feature Name	Description
	Add support for a new option-class client class	<p>Added support for new option-class client class, which allows options to be sent in the offer and ack messages based upon client provided option values in the discover and request messages.</p> <p>This feature allows option values to be assigned based on client provided option(s), other than the currently supported vendor and user classes. One such application is for PXE clients that provide a client system architecture type option (option 93) that require a specific bootfile name (e.g.. uefi/bootx64.efi for system type 0007 - EFI BC).</p>
	Client ID option in DHCPOFFER, DHCPACK and DHCPNAK	<p>Added a new feature to include the client ID option (option 61) in server response messages (DHCPOFFER, DHCPACK, and DHCPNAK), controlled by a new server level policy, IncludeClientIdInServerResponses, whose default value will be FALSE, in order to maintain the current behavior of the DHCP server.</p>
	Multiple destinations for SNMP traps in DHCPv4 6.0	<p>Changed the SNMP trap sending mechanism in the SNMP library utilizing the Agentx protocol, in order to support multiple trap destinations. With these changes, the SnmpTrapCommunity and SnmpTrapPeer server policies are now obsolete.</p>

Feature ID	Feature Name	Description
	DHCP server support for adhering to option 57, maximum message size.	<ul style="list-style-type: none"> The new <i>IgnoreClientMaximumMessageSize server</i> policy, when FALSE (default), directs the server to log a warning message to the sys/event and server debug logs and drop the discover/request packet if the outgoing packet size exceeds the option 57 value specified by the client. When the policy is set to TRUE, the DHCP server responds to the packet regardless of the client's option 57 value. The DHCP server uses the minimum legal value of 576 bytes (according to RFC 2132), if the client specifies a lesser value in option 57.
	Ping preclusion policy when client has active lease but does not indicate with a non zero <i>ciaddr</i> .	Added support for <i>SuppressActiveLeasePing</i> policy. When it is TRUE, the system directs the server to bypass the ping for both manual and dynamic objects that currently have a lease status as active (2), but do not send their client address in the <i>ciaddr</i> field of the discover packet.
	Support for new <i>MinimumRequestedLeaseTime</i> server policy and minimum-requested-lease-time scope/subnet level policy.	<ul style="list-style-type: none"> Define the <i>MinimumRequestedLeaseTime</i> server level policy and the minimum-requested-lease-time subnet and scope level policies, which can be used to specify a lease time in seconds, which is the minimum lease time (option 51) value a dynamic DHCP client can request and be offered. A subnet level policy value will take precedence over the server policy value. <i>HonorRequestedLeaseTime</i> legacy policy behavior should not be altered.

Feature ID	Feature Name	Description
	Support for new <i>DropInformsWhenNotActive</i> policy to enable/disable DHCPACK's for DHCPINFORM message on DHCP servers in failover configuration.	<ul style="list-style-type: none">Define new <i>DropInformsWhenNotActive</i> server policy – when it is TRUE, directs server to preclude the processing of DHCPINFORM messages. When it is FALSE (default), directs server to process DHCPINFORM messages regardless of failover status.Also moved the increment of the inform count for DHCP statistics prior to the check for the <i>DropAllDhcpInformPackets</i> policy.
	Support for DHCP on Solaris 10 Zones/Containers.	<ul style="list-style-type: none">Increase the supported interface name length to handle zone naming convention.Add logic to properly recognize the longer I/F name as unique (and not a duplicate) for Solaris.

Nokia DHCPv4 MIB variables

The Nokia DHCPv4 server optionally supports SNMP on all platforms. The statistical information gathered by the DHCPv4 server through normal operations can be accessed through the DHCPv4 MIB variables.

Portions of the DHCPv4 MIB objects defined by the DHCP Working Group of the Internet Engineering Task Force (IETF) in a proposed draft have been implemented. In particular, there is support for Bootp and DHCP counter and statistics groups. The supported DHCPv4 server MIB variables are grouped in categories listed in the following tables. Refer to [Table 2-12](#) for a description of each variable.

Table 2-12 Summary of SNMP MIB variables for the VitalQIP DHCPv4 server

Function	MIB Variable(s)	Description
System information:		
Server Information	<i>dhcpServSystemDescr</i>	Provides a textual description of the server. This value includes the full name and version identification of the server. Example: <i>Version 6.0 Build 67-VitalQIP DHCP Server</i>
Server Status	<i>dhcpServSystemStatus</i>	Status of the DHCPv4 server: <ul style="list-style-type: none"> • 0 – Starting server up • 1 – Server is running • 2 – Server is stopping • 3 – Server is halted • 4 – Server is reloading its configuration Note: Once the server has been completely stopped, no status can be returned from this variable.
Number of seconds since service was started	<i>dhcpServSystemUpTime</i>	This value is the time elapsed (in seconds) since it started.
Number of seconds since service was last reset (config files were re-read)	<i>dhcpServSystemResetTime</i>	This value is the time elapsed (in seconds) since the last time the name server was “reset”.
Counter information by server:		

Function	MIB Variable(s)	Description
Number of Used Subnets (in use)	<i>dhcpServCountUsedSubnets</i>	The number of subnets managed by the server (for example, configured), from which the server has issued at least one lease.
Number of Unused Subnets (not in use)	<i>dhcpServCountUnusedSubnets</i>	The number of subnets managed by the server, from which the server has issued no leases.
Number of exhausted/full Subnets	<i>dhcpServCountFullSubnets</i>	The number of subnets managed by the server, in which all defined addresses have been leased to clients. Subnets containing unavailable leases are not represented in this counter.
Counter information for Bootp packets:		
Number of Bootp Request Packets received	<i>dhcpServBootpCountRequests</i>	The number of packets received that contain a Message Type of 1 (BOOTREQUEST) in the first octet and do not contain option number 53 (DHCPv4 Message Type) in the options.
Number of Invalid Bootp Request Packets received	<i>dhcpServBootpCountInvalids</i>	The number of packets received that do not contain a Message Type of 1 (BOOTREQUEST) in the first octet or are not valid BOOTP packets (for example, too short, invalid field in packet header)
Number of Bootp Packets sent	<i>dhcpServBootpCountReplies</i>	The number of packets sent that contain a Message Type of 2 (BOOTREPLY) in the first octet and do not contain option number 53 (DHCPv4 Message Type) in the options.
Number of Bootp Packets dropped with unknown clients	<i>dhcpServBootpCountDroppedUnknownClients</i>	The number of BOOTP packets dropped due to the server not recognizing or not providing service to the hardware address received in the incoming packet.
Number of Bootp packets dropped because this server cannot serve addresses to this subnet	<i>dhcpServBootpCountDroppedNotServingSubnet</i>	The number of BOOTP packets dropped due to the server not being configured or not able to serve addresses on the subnet from which this message was received.
Counter information for DHCP packets:		

Function	MIB Variable(s)	Description
Number of DHCPv4 Discover Packets received	<i>dhcpServDhcpCountDiscovers</i>	The number of DHCPDISCOVER (option 53 with value 1) packets received.
Number of DHCPv4 Request Packets received	<i>dhcpServDhcpCountRequests</i>	The number of DHCPREQUEST (option 53 with value 3) packets received.
Number of DHCPv4 Release Packets received	<i>dhcpServDhcpCountReleases</i>	The number of DHCPRELEASE (option 53 with value 7) packets received.
Number of DHCPv4 Decline Packets received	<i>dhcpServDhcpCountDeclines</i>	The number of DHCPDECLINE (option 53 with value 4) packets received.
Number of DHCPv4 Inform Packets received	<i>dhcpServDhcpCountInforms</i>	The number of DHCPINFORM (option 53 with value 8) packets received.
Number of Invalid DHCPv4 packets received	<i>dhcpServDhcpCountInvalids</i>	The number of DHCP packets received whose DHCP message type (option 53) is not understood or handled by the server.
Number of DHCPv4 Offers sent	<i>dhcpServDhcpCountOffers</i>	The number of DHCP OFFER (option 53 with value 2) packets sent.
Number of DHCPv4 Acks sent	<i>dhcpServDhcpCountAcks</i>	The number of DHCPACK (option 53 with value 5) packets sent.
Number of DHCPv4 Nacks sent	<i>dhcpServDhcpCountNacks</i>	The number of DHCPNACK (option 53 with value 6) packets sent.
Number of DHCPv4 Packets dropped with unknown clients	<i>dhcpServDhcpCountDroppedUnknownClient</i>	The number of DHCP packets dropped due to the server not recognizing or not providing service to the client ID and/or hardware address received in the incoming packet.
Number of DHCPv4 Packets dropped because this server cannot serve addresses to this subnet	<i>dhcpServDhcpCountDroppedNotServingSubnet</i>	The number of DHCP packets dropped due to the server not being configured or not able to serve addresses on the subnet from which this message was received.
Statistical/performance information for Bootp packets:		

Function	MIB Variable(s)	Description
Minimum Amount of Time between receiving two Bootp packets	<i>dhcpServBootpStatMinArrivalInterval</i>	The minimum amount of time between receiving two BOOTP messages. A message is received at the server when the server is able to begin processing the message. This typically occurs immediately after the message is read into server memory. If no messages have been received, or the time interval is less than 1 ms, this object contains a zero value. The value is in milliseconds.
Maximum Amount of Time between receiving two Bootp packets	<i>dhcpServBootpStatMaxArrivalInterval</i>	The maximum amount of time between receiving two BOOTP messages. A message is received at the server when the server is able to begin processing the message. This typically occurs immediately after the message is read into server memory. If no messages have been received, this object contains a zero value. The value is in milliseconds.
Number of Seconds since the last Bootp Packet was received	<i>dhcpServBootpStatLastArrivalTime</i>	The number of seconds since the last valid BOOTP message was received by the server. Invalid messages do not cause this value to change. If no valid messages have been received, this object contains a zero value.

Function	MIB Variable(s)	Description
Minimum Response Time to Bootp packets	<i>dhcpServBootpStatMinResponseTime</i>	The smallest time interval measured as the difference between the arrival of a BOOTP message at the server and the successful transmission of the response to that message. A message is received at the server when the server is able to begin processing the message. A message is transmitted after the server has no further use for the message. Note that the operating system may still have the message queued internally. The operating system queue time is not to be considered as part of the response time. Invalid messages do not cause this value to change. If no valid messages have been received, or the interval is less than 1 ms, this object contains a zero value. The value is in milliseconds.
Maximum Response Time to Bootp packets	<i>dhcpServBootpStatMaxResponseTime</i>	The largest time interval measured as the difference between the arrival of a BOOTP message at the server and the successful transmission of the response to that message. A message is received at the server when the server is able to begin processing the message. A message is transmitted after the server has no further use for the message. Note that the operating system may still have the message queued internally. The operating system queue time is not to be considered as part of the response time. Invalid messages do not cause this value to change. If no valid messages have been received, this object contains a zero value. The value is in milliseconds.

Function	MIB Variable(s)	Description
Sum of the Response Times for Bootp packets	<i>dhcpServBootpStatSumResponseTime</i>	The sum of the response time intervals (in milliseconds), where a response time interval is measured as the difference between the arrival of a BOOTP message at the server and the successful transmission of the response to that message. A message is received at the server when the server is able to begin processing the message. A message is transmitted after the server has no further use for the message. Note that the operating system may still have the message queued internally. The operating system queue time is not to be considered as part of the response time. Invalid messages do not cause this value to change. If no valid messages have been received, this object contains a zero value. The value is in milliseconds.
Statistical/performance information for DHCP packets:		
Minimum Amount of Time between receiving two DHCPv4 packets	<i>dhcpServDhcpStatMinArrivalInterval</i>	The minimum amount of time between receiving two DHCP messages. A message is received at the server when the server is able to begin processing the message. This typically occurs immediately after the message is read into server memory. If no messages have been received, or the interval is less than 1 ms, this object contains a zero value. The value is in milliseconds.
Maximum Amount of Time between receiving two DHCPv4 packets	<i>dhcpServDhcpStatMaxArrivalInterval</i>	The maximum amount of time between receiving two DHCP messages. A message is received at the server when the server is able to begin processing the message. This typically occurs immediately after the message is read into server memory. If no messages have been received, this object contains a zero value. The value is in milliseconds.

Function	MIB Variable(s)	Description
Number of Seconds since the last DHCPv4 Packet was received	<i>dhcpServDhcpStatLastArrivalTime</i>	The number of seconds since the last valid DHCP message was received by the server. Invalid messages do not cause this value to change. If no valid messages have been received, this object contains a zero value.
Minimum Response Time to DHCPv4 packets	<i>dhcpServDhcpStatMinResponseTime</i>	The smallest time interval measured as the difference between the arrival of a DHCP message at the server and the successful transmission of the response to that message. A message is received at the server when the server is able to begin processing the message. A message is transmitted after the server has no further use for the message. Note that the operating system may still have the message queued internally. The operating system queue time is not to be considered as part of the response time. Invalid messages do not cause this value to change. If no valid messages have been received, or the interval is less than 1 ms, this object contains a zero value. The value is in milliseconds.
Maximum Response Time to DHCPv4 packets	<i>dhcpServDhcpStatMaxResponseTime</i>	The largest time interval measured as the difference between the arrival of a DHCP message at the server and the successful transmission of the response to that message. A message is received at the server when the server is able to begin processing the message. A message is transmitted after the server has no further use for the message. Note that the operating system may still have the message queued internally. The operating system queue time is not to be considered as part of the response time. Invalid messages do not cause this value to change. If no valid messages have been received, this object contains a zero value. The value is in milliseconds.

Function	MIB Variable(s)	Description
Sum of the Response Times for DHCPv4 packets	<i>dhcpServDhcpStatSumResponseTime</i>	The sum of the response time intervals (in milliseconds), where a response time interval is measured as the difference between the arrival of a DHCP message at the server and the successful transmission of the response to that message. A message is received at the server when the server is able to begin processing the message. A message is transmitted after the server has no further use for the message. Note that the operating system may still have the message queued internally. The operating system queue time is not to be considered as part of the response time. Invalid messages do not cause this value to change. If no valid messages have been received, this object contains a zero value. value is in milliseconds.
DHCPv4 and Bootp statistics by subnet and/or address pool:		
	<pre> <i>dhcpServRangeEntry</i> ::= SEQUENCE { <i>dhcpServRangeSubnetAddr</i>, <i>dhcpServRangeSubnetMask</i>, <i>dhcpServRangeStart</i>, <i>dhcpServRangeEnd</i>, <i>dhcpServRangeInUse</i>, <i>dhcpServRangeOutstandingOffers</i>, <i>dhcpServRangeUnavailable</i>, <i>dhcpServRangeType</i>, <i>dhcpServRangeUnused</i> } </pre>	Note that a table is provided that will allow all of the following information to be accessed not only by subnet, but also by address pool (scope).
Subnet Address of the Address Pool (scope) of the table entry that is being referenced	<i>dhcpServRangeSubnetAddr</i>	The IP address defining this subnet.

Function	MIB Variable(s)	Description
Subnet Mask of the Address Pool (scope) of the table entry that is being referenced	<i>dhcpServRangeSubnetMask</i>	The subnet mask associated with this subnet.
Starting IP Address of the Address Pool of the table entry that is being referenced	<i>dhcpServRangeStart</i>	The starting IP Address of the Address pool range for this entry within the table.
Ending IP Address of the Address Pool of the table entry that is being referenced	<i>dhcpServRangeEnd</i>	The ending IP Address of the Address pool range for this entry within the table.
Number of Addresses in this range (of the table entry) that are Used (in use)	<i>dhcpServRangeInUse</i>	The number of addresses in this range that are currently in use. This number includes address leases that have not expired, and addresses that have been reserved (by the server through configuration).
Number of Addresses in this range (of the table entry) that have outstanding Offers pending	<i>dhcpServRangeOutstandingOffers</i>	The number of outstanding DHCP OFFER messages for this range is reported with this value. An offer is outstanding if the server has sent a DHCP OFFER message to a client, but has not yet received a DHCP REQUEST message from the client, nor has the server-specific time-out (limiting the time in which a client can respond to the offer message) for the offer message expired.
Number of Addresses in this range (of the table entry) that are unavailable	<i>dhcpServRangeUnavailable</i>	The number of IP Addresses within this range that are marked by the DHCP server as unavailable. An address is marked as unavailable by the DHCPv4 server when an acknowledgement of the address conflict detection (PING) is received. In addition, the DHCP server will mark leases as unavailable if a DHCP DECLINE is received from the DHCP client.

Function	MIB Variable(s)	Description
The Type of (IP) Address range of the table entry	<i>dhcpServRangeType</i>	DHCPv4 Server Client Lease Type: <ul style="list-style-type: none"> • 1 – Manual Bootp • 2 – Automatic Bootp • 3 – Manual DHCP • 4 – Automatic DHCP • 5 – Dynamic DHCP
Number of Addresses in this range (of the table entry) that are unused or available for assignment	<i>dhcpServRangeUnused</i>	The number of addresses in this range that are currently unused. This number excludes address leases that have not expired, and addresses that have been reserved (by the server through configuration).
DHCPv4 Server Failover Configuration:		
Note: These MIB variables are only available when you have a DHCPv4 Failover server configuration.		
Indicates the IP address of the partner server.	<i>dhcpServFailoverPartnerAddr</i>	Shows the failover server IP address for a queried primary server, or the primary server IP address for a queried failover server. If no failover server is defined, this has a null value.
Indicates the function of the partner server	<i>dhcpServFailoverPartnerType</i>	The type of partner server. The following values indicate the type of partner server: <ul style="list-style-type: none"> • primary (1) - The partner server is a primary server. • secondary (2) - The partner server is a secondary server.

Function	MIB Variable(s)	Description
Indicates the status of the partner server	<i>dhcpServFailoverPartnerStatus</i>	<p>This variable indicates the last known state of the queried server's partner. The following values indicate the status of the partner server:</p> <ul style="list-style-type: none"> • unknown (0) - The status of the partner server identified in the <i>dhcpServFailoverPartnerAddr</i> variable, as defined in this server's <i>dhcpd.pcy</i> file, is unknown. This value is valid for primary and secondary partner servers. • syncing (1) - The partner server identified in the <i>dhcpServFailoverPartnerAddr</i> variable is exchanging lease data with the server maintaining the partner MIB variables. This value is valid for primary and secondary partner servers. • active (2) - The partner server identified in the <i>dhcpServFailoverPartnerAddr</i> variable is running and is giving out leases on its configured subnets. This value is only valid when querying a secondary server for the status of its primary partner.

Function	MIB Variable(s)	Description
	<i>dhcpServFailoverPartnerStatus</i> (continued)	<ul style="list-style-type: none"> inactive (3) - The partner server identified in the <i>dhcpServFailoverPartnerAddr</i> variable is not responding to poll messages and not giving out leases on its configured subnets. This value is only valid when querying a secondary server for the status of its primary partner. <p>When querying a primary server for the status of its secondary partner, only the 0 and 1 values are used. The primary server does not poll the secondary server. As a result, the primary server does not know if the secondary server is running after the primary server has synchronized with the secondary server. After the primary server has synchronized with the secondary server, the partner status value for the secondary server is set to the unknown (0) status.</p>
Indicates the time of the last poll or response	<i>dhcpServFailoverPartnerPolltime</i>	A timestamp documenting the time of receipt for the last poll message from a secondary partner server or last poll response from each primary server.
DHCPv4 server SNMP traps:		
The DHCPv4 server has started	<i>dhcpServerStarted</i>	The DHCP server has been started.
The DHCPv4 server has stopped	<i>dhcpServerStopped</i>	The DHCP server has been stopped.
The DHCPv4 server has reloaded its configuration	<i>dhcpServerReload</i>	The DHCP server has been told to reload its configuration.

Function	MIB Variable(s)	Description
The DHCPv4 server has determined that a subnet has been depleted of addresses that satisfy the configured ForceClass server policy value.	<i>dhcpServerSubnetDepleted</i>	The DHCP server has used all the addresses within a subnet that satisfy the configured ForceClass server policy value, and has received a discover request for which it cannot offer a lease. This trap will be generated for each such discover request that cannot be offered a lease. The address of the depleted subnet is included in the trap text.
The DHCPv4 server receives a bad packet.	<i>dhcpServerBadPacket</i>	The DHCP server has received a malformed packet.
The DHCPv4 Failover server has taken control of some address space	<i>dhcpServerFailoverActive</i>	This trap is issued by the secondary server. A primary server is down and its scopes will be serviced by this failover server.
The DHCPv4 Failover server has returned control to the primary server for some address space	<i>dhcpServerFailoverReturnedControl</i>	This trap is issued by the secondary server. The failover server has returned control to its primary partner.
Indicates the number of leases issued by the server has exceeded the specified threshold value set for the subnet.	<i>dhcpServerSubnetThresholdExceeded</i>	The trap is issued by the LucentDHCP server when the percentage of used addresses in a subnet has exceeded the value of the threshold defined for the subnet or global server threshold, assuming that a subnet-specific value is not specified with a subnet in the server configuration file.
Indicates the number of leases issued by the server fallen below the threshold value set for the subnet.	<i>dhcpServerSubnetThresholdDescent</i>	The trap is issued by the LucentDHCP server when the percentage of used addresses in a subnet has fallen below the value of the threshold defined for the subnet or global server threshold, assuming that a subnet-specific value is not specified with a subnet in the server configuration file.
Indicates the lease request is from an unknown client.	<i>dhcpServerDropUnknownClient</i>	The trap is issued when an unregistered client attempts to obtain a DHCP lease.

Function	MIB Variable(s)	Description
Indicates the address for which the server wants to provide a lease is unavailable.	dhcpServerPingResponseReceived	The address that the server wanted to provide is not available as indicated by a ping response. This can indicate unauthorized use of the address or the network.

Trap object IDs (OIDs)

Purpose

This section describes the components that comprise an SNMP trap. The VitalQIP enterprise-specific trap contents are defined by the following:

- DHCPv4: **vitalqipDhcpTrapEntry**

Similar trap variables are defined for DHCP, as shown in the following table.

Table 2-13 Trap variables

vitalqipDhcpTrapEntry in qdhcp.mib	Type	Description
vitalqipDhcpTrIndex	Integer	Indicates which trap is received for <i>qdhcp.mib</i> : 1 = dhcpServerStarted 2 = dhcpServerStopped 3 = dhcpServerReload 4 = dhcpServerSubnetDepleted 5 = dhcpServerBadPacket 6 = dhcpServerFailoverActive 7 = dhcpServerFailoverReturnedControl 8 = dhcpServerSubnetThresholdExceeded 9 = dhcpServerSubnetThresholdDescent 10 = dhcpServerDropUnknownClient 11 = dhcpServerPingResponseReceived For a description of the DHCP traps, refer to the DHCP server SNMP traps in Table 2-12 .
vitalqipDhcpTrSequence	Counter	Indicates how many times a specific trap is received. This number is a counter that will increment every time a specific trap is received. Such counters are only reset by DHCP Starts or by a DHCP Restart.
vitalqipDhcpTrId	Integer	Indicates the application that generated the alarm. Currently, all traps are generated by the Monitor. The value is always 1.
vitalqipDhcpTrText	80-char string	An ASCII string describing the alarm condition/cause, for example: Nokia DHCP stopped Nokia DHCP started

vitalqipDhcpTrapEntry in qdhcp.mib	Type	Description
vitalqipDhcpTrPriority	Integer	Indicates the priority level as set on the agent for this class and type of trap. The DHCP servers send traps with the following priorities: <ol style="list-style-type: none"> 1 (inform) for start, stop, reload, failover returned control, subnet threshold descended, and ping response received. 2 (warning) a bad packet is received. Used when a bad DHCP packet is received that either contains an invalid DHCP magic cookie (see RFC 2131, Sec 3) or DHCP option data with invalid length(s). 3 (minor) when a subnet threshold is exceeded. 4 (major) when a subnet is depleted. 5 (critical) when a failover is activated.
vitalqipDhcpTrClass	Integer	This is not used and is set to the value of vitalqipDhcpTr Index (DHCP).
vitalqipDhcpTrType	Integer	This is not used and is set to the value of vitalqipDhcpTr Index (DHCP).
vitalqipDhcpTrTime	Counter	Indicates the time when the trap has occurred. It contains the number of seconds since UNIX epoch (midnight UTC of January 1, 1970). For example, the local time of the sub-agent host is: 1238788125 (which translates to Fri Apr 3 15:48:45 2009)
vitalqipDhcpTrSuspect	32-char string	The hostname where the sub-agent (<i>named</i> or <i>dhcpd</i>) is running.
vitalqipDhcpTrDiagId	Integer	This is not used and is set to the value of vitalqipDhcpTr Index (DHCP).
vitalqipDhcpTrIteration	Integer	Indicates the total number of traps sent so far.

Sample DHCP traps

The following is sample output from a trap receiver utility. The definitions of the vitalqipDhcpTr family of values are in the above table.

```
Received SNMPv2c Trap:
Community: public
From: 127.0.0.1
sysUpTime.0 = 2 days, 03:56:26.29
snmpTrapOID.0 = dhcpServerSubnetThresholdExceeded
vitalqipDhcpTrIndex = 8
```

```

vitalqipDhcpTrSequence = 1
vitalqipDhcpTrId = monitor(1)
vitalqipDhcpTrText = Nokia DHCP Subnet Threshold exceeded for
    subnet 10.51.0.0
vitalqipDhcpTrPriority = minor(3)
vitalqipDhcpTrClass = 8
vitalqipDhcpTrType = 8
vitalqipDhcpTrTime = 1184876862
vitalqipDhcpTrSuspect = qa2k342
vitalqipDhcpTrDiagId = 8
vitalqipDhcpTrIteration = 1

Received SNMPv2c Trap:
Community: public
From: 127.0.0.1
sysUpTime.0 = 2 days, 04:01:15.06
snmpTrapOID.0 = dhcpServerSubnetDepleted vitalqipDhcpTrIndex = 4
vitalqipDhcpTrSequence = 1
vitalqipDhcpTrId = monitor(1)
vitalqipDhcpTrText = Nokia DHCP Subnet Depleted for subnet
    10.51.0.0
vitalqipDhcpTrPriority = major(4)
vitalqipDhcpTrClass = 4
vitalqipDhcpTrType = 4
vitalqipDhcpTrTime = 1184877151
vitalqipDhcpTrSuspect = qa2k342
vitalqipDhcpTrDiagId = 4
vitalqipDhcpTrIteration = 1

```

Querying vitalqipDhcpTrapEntry tables and variables

An administrator can query the DHCP trap tables by using the `snmptable` or other SNMP client utility. An administrator can also query a specific component of a thrown trap using `snmpget` or other SNMP client utility. For example,

vitalqipDhcpTrText.15

would return the text value of the 15th trap in the `vitalqipDhcpTrapEntry` table.

Trap table rolling

The `vitalqipDhcpTrapTable` can only hold up to 32 entries each. When the 33rd DHCP trap is thrown, the `TrapTable` overwrites the 1st trap with the 33rd trap. The 34rd trap will replace the 2nd trap and the table will continue in a FIFO manner, overwriting the oldest trap in the table with the newest trap.



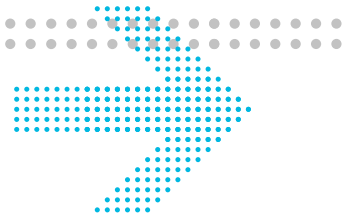
3 Test results

Overview

Purpose

This chapter is not pertinent to the VitalQIP DHCPv4 6.0

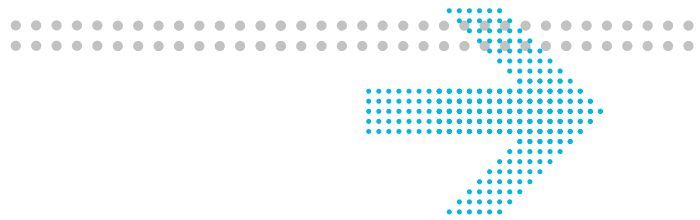
4 Changes to interfaces, alarms, and messages



Overview

Purpose

This chapter is not pertinent to the VitalQIP DHCPv4 6.0



5 Resolved issues

Overview

Purpose

This chapter describes resolved issues in this release.

Contents

This chapter covers these topics.

Resolved issues in Nokia DHCPv4 6.0, Build 67	5-3
Resolved issues in Nokia DHCPv4 6.0, Build 64	5-4
Resolved issues in Nokia DHCPv4 6.0, Build 60	5-5
Resolved issues in Nokia DHCPv4 6.0, Build 56	5-6
Resolved issues in Nokia DHCPv4 6.0, Build 51	5-7
Resolved issues in Nokia DHCPv4 6.0, Build 50	5-8
Resolved issues in Nokia DHCPv4 6.0, Build 49	5-9
Resolved issues in VitalQIP DHCPv4 6.0, Build 46	5-10
Resolved issues in VitalQIP DHCPv4 6.0, Build 37	5-12
Resolved issues in VitalQIP DHCPv4 6.0, Build 30	5-13
Resolved issues in VitalQIP DHCPv4 6.0, Build 28	5-14
Resolved issues in VitalQIP DHCPv4 6.0, Build 27	5-15
Resolved issues in VitalQIP DHCPv4 6.0, Build 24	5-16
Resolved issues in VitalQIP DHCPv4 6.0, Build 20	5-17
Resolved issues in VitalQIP DHCPv4 6.0, Build 14	5-18

Resolved issues in VitalQIP DHCPv4 6.0, Build 11	5-19
Resolved issues in VitalQIP DHCPv4 6.0, Build 10	5-20

Resolved issues in Nokia DHCPv4 6.0, Build 67

The following table identifies issues that have been resolved in Nokia DHCPv4 6.0 Build 67.

Table 5-1 ARs resolved in Build 67 release

Fault ID	AR number	Severity	Description of issue
LDHCP00013053		3: Medium	Updated DHCPv4 SNMP MIB to correct parsing errors, warnings and updated Support contact info.
LDHCP00013058		3: Medium	Added logic during renew processing to preclude the client ID match check for MDHCP by MAC objects when the host record's clientIdTracked flag is set to FALSE. This change will allow for the renew request by a MDHCP by MAC to proceed regardless of whether or not a client ID is provided by the client in option 61.
LDHCP00013061		4: Low	Changed the default for the IncludeClientIdInServerResponses DHCP server policy to True, in order to be compliant with RFC 6842.
LDHCP00013063		3: Medium	Added logic during DHCPDECLINE processing to only send the lease update message to VitalQIP when the server is the currently active server in a failover configuration, in order to eliminate redundant lease update messages in a failover configuration.

Resolved issues in Nokia DHCPv4 6.0, Build 64

The following table identifies issues that have been resolved in Nokia DHCPv4 6.0 Build 64.

Table 5-2 ARs resolved in Build 64 release

Fault ID	AR number	Severity	Description of issue
LDHCP00013041		3: Medium	Added logic to check for a valid thread ID when stopping/restarting the server prior to calling pthread_join() for certain threads that were not previously checked, specifically the expiredLeaseDelete, reconfigure, and failover polling (serverFSM) threads. This change will eliminate the segmentation fault in the rare case when a thread create fails, since the pthread_join will be bypassed during stop/restart processing.

Resolved issues in Nokia DHCPv4 6.0, Build 60

The following table identifies issues that have been resolved in Nokia DHCPv4 6.0 Build 60.

Table 5-3 ARs resolved in Build 60 release

Fault ID	AR number	Severity	Description of issue
LDHCP00013019		3: Medium	Certain long concatenation requiring options (88, 119, and 122) may prevent the DHCP server from successfully starting when present in the server configuration file and longer than 357 bytes. Limit checking of long option data lengths during option logging has been added to prevent buffer overflows that may cause the server to terminate.
LDHCP00013029	1-7292865	3: Medium	DHCP Server may on extremely rare occasion, incur a SIGSEGV crash on server HUP. Added logic to preclude joining a thread during shutdown/restart processing if the thread was not successfully created during initialization.
LDHCP00013036	1-7480912	3: Medium	DHCP Server may intermittently incur a SIGSEGV crash on Linux only, when SiAddr=sname policy is set and TFTP server name option does not successfully translate into an IP address for siAddr field in outgoing DHCPOFFER/DHCPACK. Added code to preclude call to free address information when translation was unsuccessful.
LDHCP00013022		4: Low	The -v option for the DHCP server on Linux returns outdated copyright information.

Resolved issues in Nokia DHCPv4 6.0, Build 56

The following table identifies issues that have been resolved in Nokia DHCPv4 6.0 Build 56.

Table 5-4 ARs resolved in Build 56 release

Fault ID	AR number	Severity	Description of issue
LDHCP00013003		3: Medium	Replaced the deprecated function gethostbyname with getaddrinfo to determine the siAddr from the sname value (dhcp-tftp-server option) and added an error level log message when not successful. This change will preclude the negative server performance observed when the dhcp-tftp-server option is improperly configured.
LDHCP00013017	1-7090100	3: Medium	Added logic to zero the lastAddUpdateTime field in the host record when an address is selected for reuse by the server during Discover message processing or when released by the server during release, autorelease, delete lease, or expiration processing. This change fixes the issue where a lease update is erroneously precluded due to the previous lease owner releasing the lease shortly after it being granted or renewed.

Resolved issues in Nokia DHCPv4 6.0, Build 51

The following table identifies issues that have been resolved in Nokia DHCPv4 6.0 Build 51.

Table 5-5 ARs resolved in Build 51 release

Fault ID	AR number	Severity	Description of issue
LDHCP00012996		4: Low	Classless static route destination descriptor invalid for 0 length subnet mask.
LDHCP00012998		3: Medium	DHCPv4 Access Control callout library requires 32-bit QSI and QIP libraries on 8.1.2 remotes.

Resolved issues in Nokia DHCPv4 6.0, Build 50

The following table identifies issues that have been resolved in Nokia DHCPv4 6.0 Build 50.

Table 5-6 ARs resolved in Build 50 release

Fault ID	AR number	Severity	Description of issue
LDHCP00012984	1-6388598	4: Low	Increased the buffer size for call to <code>gethostbyname_r()</code> in order to correctly populate the <code>siAddr</code> field in the BOOTPREPLY when the <code>SiAddr=sname</code> server policy is set and the name is resolved by DNS.
LDHCP00012985		3: Medium	Added logic to identify the Primary DHCP server address in a new manual table record created when processing a dynamic manual DHCP update. This change will preclude the Secondary server from responding to a discover received from the client identified in the dynamic manual DHCP update when the Primary is active. This change was required after changes were made to VitalQIP to push dynamic manual updates to both the Primary and Secondary servers in a failover configuration.
LDHCP00012990		4: Low	Added logic to the Linux <code>signal_handler</code> to resolve a thread synchronization issue at cold start that resulted in failure to write the PID file. This issue only occurred in test environments with an empty configuration file and no SNMP library to be loaded.
LDHCP00012994	1-6496515	4: Low	Changed client DHCP maximum message size variables from signed to unsigned short in order to support option 57 values from clients up to 65536.

Resolved issues in Nokia DHCPv4 6.0, Build 49

The following table identifies issues that have been resolved in Nokia DHCPv4 6.0 Build 49.

Table 5-7 ARs resolved in Build 49 release

Fault ID	AR number	Severity	Description of issue
LDHCP00012831	1-5717237, 1-5431564, 1-5330694	3: Medium	Added 'doNotRetainNotificationLogs yes' directive to the snmpd.conf file (including sample_snmpd.conf) to preclude server memory growth with NetSNMP
LDHCP00012972		3: Medium	Replaced call to IsIPAddrValid() with call to inet_addr() when processing siAddr value for outgoing packet to eliminate potential memory leak when SiAddr policy set to "sname". The leak will only occur when the TFTP server option to be sent in an offer or ack message is a hostname/FQDN and the size of the leak is the number of bytes in the hostname/FQDN.
LDHCP00012973		4: Low	When ListenOnLoopback is enabled, which is required when using the appliance DHCPv4 probe, bypass opening a dummy socket for the loopback interface so that the server is able to read and process DHCP client messages from the probe.
LDHCP00012979		3: Medium	Changed infinite lease time option value conversion for Windows to fix issue with invalid expiration time in the active lease file and update messages.

Resolved issues in VitalQIP DHCPv4 6.0, Build 46

The following table identifies issues that have been resolved in VitalQIP DHCPv4 6.0, Build 46.

Table 5-8 ARs resolved in Build 46 release

Fault ID	AR number	Severity	Description of issue
LDHCP00012119		3: Medium	Added logic to the failover state machine to delay sending any failover messages until the server is ready to handle incoming messages from the partner server. This change will preclude the rare occurrence of binding updates not getting processed on a newly started server (primary or secondary).
LDHCP00012133		3: Medium	The DHCP server does not have an API callout library to support the Access Control feature on Windows, starting with build 37.
LDHCP00012134		3: Medium	During the binding update operation for a lease tracked by client ID, a redundant memory allocation is performed, resulting in the leak of 255 bytes per lease. This leak will only occur for a new lease, not for an existing lease renewal.
LDHCP00012141		4: Low	The option value data for a single option that is printed in the server debug log for an incoming or outgoing packet may be printed noncontiguously, making it very difficult to read. This is observed when thread context switching occurs during the printing of the option data due to multiple different client packets getting processed simultaneously. This can occur on any platform, but is most pronounced on Solaris due to the thread scheduling algorithm.
LDHCP00012832		3: Medium	With ActiveLeaseExpiration enabled, the DHCP server may hang during the restart associated with DHCP generation. This is a very rare occurrence that is more likely to occur on a machine with multiple processors.

Fault ID	AR number	Severity	Description of issue
LDHCP00012840		4: Low	When the SupportClientId policy is false and a manual-dhcp-clientid object resides in the dhcpd.conf file that contains one or more client classes (option-class, user-class, vendor-class), the DHCP server does not properly ignore the entire manual-dhcp-clientid object and flags the configuration file as bad, resulting in the use of the last known good file and a QIP DHCP generation error.
LDHCP00012843		3: Medium	The DHCP statistics variable for the delete lease count is not incremented when a lease is deleted.
LDHCP00012844	1-5993568	3: Medium	Description of DHCP Trap vitalqipDhcpTrPriority warning information in release notes is not correct.

Resolved issues in VitalQIP DHCPv4 6.0, Build 37

The following table identifies issues that have been resolved in VitalQIP DHCPv4 6.0, Build 37.

Table 5-9 ARs resolved in Build 37 release

Fault ID	AR number	Severity	Description of issue
LDHCP00012114		3: Medium	Changed SNMP log rotation policy print logic to print default policy values when invalid values are specified.
LDHCP00012123		2: High	Corrected length calculation for an active lease file record so that records requiring 192 bytes of data do not have bytes truncated. Truncated records may result in a server crash during binding update exchanges with a partner failover server. Also added checks for a valid client ID length when building binding updates to a partner failover server in order to preclude server crashes during binding update exchanges.
LDHCP00012124		4: Low	Corrected abusive client check to only increment the individual client's warning count once per message by precluding the increment that could occur for each scope within the target subnet. This change will eliminate the false positive abusive client warnings that occur for DHCPDISCOVER and DHCPREQUEST messages from clients that are assigned dynamic addresses from subnets with many scopes.

Resolved issues in VitalQIP DHCPv4 6.0, Build 30

The following table identifies issues that have been resolved in VitalQIP DHCPv4 6.0, Build 30.

Table 5-10 ARs resolved in Build 30 release

Fault ID	AR number	Severity	Description of issue
LDHCP00012060	1-4839522	3: Medium	The DHCPv4 server with <i>LogDhcpMsgTraffic=all</i> sometimes writes bogus characters to the log and then stops writing to log all together.
LDHCP00012076	1-2891051	3: Medium	The 25 value is not supported as <i>AbusiveClientWarningCount</i> .
LDHCP00012095	1-5117072	3: Medium	ICMP udp port bootps unreachable messages.
LDHCP00012108		3: Medium	Object level (both manual and scope) client classes may result in memory leaks during a HUP/restart.
LDHCP00012113	1-5346189	2: High	DHCP crashes, occurs about twice a week since upgraded from DHCPv4 6.0B6 to DHCPv4 6.0 B28.

Resolved issues in VitalQIP DHCPv4 6.0, Build 28

The following table identifies issues that have been resolved in VitalQIP DHCPv4 6.0, Build 28.

Table 5-11 ARs resolved in Build 28 release

Fault ID	AR number	Severity	Description of issue
LDHCP00012031	1-4727387 1-4687902	3: Medium	The 6.0/Linux dhcpd cores if SNMP call collides with SIGHUP.
LDHCP00012051	1-4856959	2: High	Nonprintable data contained in a DHCPv4 client provided option 61 (client ID) value can cause unpredictable logging behavior, including dhcpd crashes.

Resolved issues in VitalQIP DHCPv4 6.0, Build 27

The following table identifies issues that have been resolved in VitalQIP DHCPv4 6.0, Build 27.

Table 5-12 ARs resolved in Build 27 release

Fault ID	AR number	Severity	Description of issue
LDHCP00012016	1-4464338	3: Medium	dhcpServDhcpStatLastArrivalTime MIB variable shows incorrect value.
LDHCP00012020	1-2872642	3: Medium	Correct the primary/failover binding synchronization in appliances that are initially installed/started with a default null configuration file and then HUP'd with the first valid configuration file.
LDHCP00012023		3: Medium	At server start/restart, when the configuration file specifies a manual-dhcp-clientid object with a different client ID value for the IP address compared to what is in the active lease file, the active lease entry should be ignored and the server configuration file manual client ID entry definition should take precedence.
LDHCP00012029	1-4641653 1-4641517	2: High	When SupportClientId policy is True, DHCP client renew sometimes NACKd even though active lease with same clientid and requested IP exists.

Resolved issues in VitalQIP DHCPv4 6.0, Build 24

The following table identifies issues that have been resolved in VitalQIP DHCPv4 6.0, Build 24.

Table 5-13 ARs resolved in Build 24 release

Fault ID	AR number	Severity	Description of issue
LDHCP00011999	1-4188534	3: Medium	Option 157 not recognized by qdhcp 6.0.14.
LDHCP00012007	1-4186199	3: Medium	Server crash at initialization when option class client class value is hex data type.
LDHCP00012008		3: Medium	Identical client classes at subnet and server levels not processed for option inclusion.
LDHCP00012009	1-4371611	3: Medium	LDHCP Acks DHCP-Request for duplicate address with different Client ID.
LDHCP00012011	1-4410198	2: High	Worker threads hung by small MaxUnavailableTime policy value in depleted subnet.

Resolved issues in VitalQIP DHCPv4 6.0, Build 20

The following table identifies issues that have been resolved in VitalQIP DHCPv4 6.0, Build 20.

Table 5-14 ARs resolved in Build 20 release

Fault ID	AR number	Severity	Description of issue
LDHCP00011962	1-3887758	3: Medium	Client ID is not verified while processing a DHCP RELEASE. DHCP should verify the Client ID before doing the DHCP Release.
LDHCP00011972	1-4037824	2: High	DHCP server crashes when it is processing a discover message without the client ID.
LDHCP00011974		1: Critical	Dynamically added M-DHCP is not used when more than one scope is defined.
LDHCP00011900	1-3608237	3: Medium	DHCPINFORM from client out of scope kills the DHCP server.
LDHCP00011993	1-4158641	3: Medium	DHCPD stops handing out leases. It continues to process expired leases and SNMP statistics.
LDHCP00011994		3: Medium	String type manual-dhcp-clientid values get wrong addresses.

Resolved issues in VitalQIP DHCPv4 6.0, Build 14

The following table identifies issues that have been resolved in VitalQIP DHCPv4 6.0, Build 14.

Table 5-15 ARs resolved in Build 14 release

Fault ID	AR number	Severity	Description of issue
LDHCP00010406	1-3429557	3: Medium	DHCP crashes on the primary and failover DHCP servers.
LDHCP00011893	1-3544739	1: Critical	RFE: Timeout should be implemented in the CheckTransactionID feature.
LDHCP00011894	1-3566153	3: Medium	DHCP service stops on the appliance version 2.0, when SNMP is enabled, due to an issue with the memory. This happens on both LDHCP 6.0 and LDHCP 5.4 versions.
LDHCP00011896		3: Medium	The DHCPRELEASE message fails for an address that was obtained using subnet selection when the subnet selection option is not in the DHCPRELEASE message.
LDHCP00011897		3: Medium	A capability to dynamically update the DHCP server configuration is required, specifically to define new manual objects in the existing subnets.
LDHCP00011898	1-3712324	2: High	Problems with NAK for offers based on ClientID.

Resolved issues in VitalQIP DHCPv4 6.0, Build 11

The following table identifies issues that have been resolved in VitalQIP DHCPv4 6.0, Build 11.

Table 5-16 ARs resolved in Build 11 release

Fault ID	AR number	Severity	Description of issue
LDHCP00009060	1-2604777	2: High	LDHCP service failing during "sendBindingChangeToBackupServers():"

Resolved issues in VitalQIP DHCPv4 6.0, Build 10

The following table identifies issues that have been resolved in VitalQIP DHCPv4 6.0, Build 10.

Table 5-17 ARs resolved in Build 10 release

Fault ID	AR number	Severity	Description of issue
LDHCP00009056		2: High	DHCP generation and collecting SNMP statistics around the same time cause DHCP server 5.6 build 9 to crash.



6 Known issues

Overview

Purpose

This chapter describes known issues and workarounds if available for VitalQIP DHCPv4 6.0 Build 60.

Contents

This chapter covers these topics.

Known issues and workarounds	6-2
Known vendor issues	6-4

Known issues and workarounds

The following table includes a list of known issues that were identified as customer impacting and/or outstanding customer problems that have not yet been resolved.

Table 6-1 Known issues and workarounds

Fault ID	AR Number	Severity	Description of issue	Workaround
LDHCP00003105		3: Medium	LeaseQuery for D-DHCP objects by id or mac when SupportClientId policy is set always returns lease unknown.	SupportClientId policy should not be enabled when Leasequery functionality is utilized.
LDHCP00003119		3: Medium	Start and stop of DHCP does not log a stop message. The log message that is missing is: "The service was stopped."	The missing stop event appears to be intermittent and machine dependent.
LDHCP00003123		3: Medium	Stats Dump will crash Server configured with large number of subnets (over 32767 subnets)	

Fault ID	AR Number	Severity	Description of issue	Workaround
LDHCP00011996		4: Low	When SupportClientId and SupportAutoRelease are both enabled and multiple clients specify the same client ID value, the worker thread pool in the server may experience a lock out situation which can eventually lead to the server being unable to respond to client messages. Defensive code was added under LDHCP00011993 to specify a MinimumClientIdLength policy, which defaults to 7, so that the server can drop packets when SupportClientId is enabled and the client ID (option 61) length from the client is less than the policy value. This issue can still occur when longer length, non-unique client ID values are specified by multiple DHCP clients, within a very short time frame (< 1 sec) on multiple subnets.	When this client behavior, which is non-conforming with RFC 2132 and RFC 4361, is expected to occur, the workaround is to set the server policy SupportClientId to False.

Note: Issues raised by customers are tracked by the Technical Support team. For more information about these issues, contact [“Technical support”](#) (p. 1-x).

For the latest list of Known Issues, refer to the “Known Problems List” in the following link <https://infoproducts.alcatel-lucent.com/aces/cgi-bin/dbaccessproddoc.cgi.edit?entryId=1-0000000001457&doctype=TLNT>

Known vendor issues

There are currently no known vendor issues affecting Nokia DHCPv4 running on supported platforms

7 System requirements



Overview

Purpose

This chapter describes software and hardware requirements and compatibility restrictions.

Contents

This chapter covers these topics.

Supported platforms	7-2
Software requirements	7-2
Hardware requirements	7-3
Compatibility restrictions	7-3

Supported platforms

Nokia DHCPv4 6.0 is supported on the following platforms.

- Red Hat Enterprise Linux (AS,ES) 7.x (64bit)

Note: The *compat-libcap1* is required.

- Red Hat Enterprise Linux (AS,ES) 8.x (64bit)

Note: The *compat-libcap1* is required.

Note: DHCP lease per second (LPS) performance verification on RHEL8 is planned.

- Windows 2016 Standard Server
- Windows 2019 Standard Server

Note: In order to run the DHCPv4 6.0 server on Windows, starting with build (B41), the Microsoft Visual C++ 2013 Redistributable Package (x86) must be installed. This can be obtained from Microsoft (<https://www.microsoft.com/en-us/download/details.aspx?id=40784>).

Note: Nokia DHCPv4 6.0 is 32 bit on all platforms.

Each release of DHCP is certified against a specific release of an operating system. Additional point releases of that operating system are considered supported.

As an example, VitalQIP DHCPv4 6.0 is certified with RHEL 8.2, which means that VitalQIP DHCPv4 6.0 will support RHEL 8.x

Software requirements

Nokia DHCPv4 6.0 Build 67 was certified with VitalQIP 21.

Important! Platform support is dependent upon the VitalQIP Remote Server version.

Note: Customers that install DHCPv4 6.0 Build 67 and use the Access Control feature, must also upgrade the remote server where the DHCPv4 6.0 B67 server resides to QIP 20 or later. This is due to the introduction of the 32 bit shared libraries (libqiprw32.so, libqsinet32.so, libqsicommon32.so), which are required when DHCPv4 6.0 Build 67 is configured to dynamically load Qdhcplib_AC.so using the APICalloutLibrayName server policy.

Nokia DHCPv4 6.0 is also supported on VitalQIP 8.1.5 and VitalQIP 20 Remote Servers running on operating systems that support VitalQIP 21 platforms. For detailed information about supported platforms, refer to the corresponding version of VitalQIP Release Notes.

Hardware requirements

Refer to “VitalQIP 21 Release Notes” for more information on hardware requirements for VitalQIP remote servers to run Nokia DHCPv4 6.0.

Compatibility restrictions

Nokia DHCPv4 6.0 has the following compatibility restrictions.

Table 7-1 Product compatibility

Product	Compatibility
VitalQIP	VitalQIP DHCPv4 6.0 is supported with VitalQIP 8.1.5 and above.
SNMP Module	SNMP Module 3.0 is supported only with DHCPv4 6.0 on VitalQIP 7.3 remote servers and above.
VitalQIP AM appliance	AM 3.0.1 PR01 and above.

Note: The above mentioned compatibility does not override product life cycle. If a product version listed above is sunset or in the process of being sunset, any issues found may require the customer to upgrade to a current release.

8 Installation and upgrade notes



Overview

Purpose

This chapter contains notes on installation of VitalQIP DHCPv4 6.0 Build 67.

Contents

This chapter covers these topics.

Performing first-time installation	8-2
Upgrade to VitalQIP DHCPv4 6.0 on Windows	8-2
Upgrade to VitalQIP DHCPv4 6.0 on UNIX	8-3
Upgrade Nokia DHCPv4 in a failover configuration	8-4
Enable Client ID	8-5
Configuring SNMP 3.0 on Linux	8-6
Configuring SNMP log rotation on Unix	8-8
Configuring SNMP 3.0 (using Net-SNMP) on Windows	8-15
Configuring SNMP Traps for all platforms	8-16

Performing first-time installation

If you are installing VitalQIP DHCPv4 6.0 for the first time, ensure that you have met the system requirements described in the *VitalQIP 21 Release Notes* and then refer to the *VitalQIP Installation Guide* for instructions on remote server installation. This manual is available on the OLCS site as well as the documentation area of OLCS.

Upgrade to VitalQIP DHCPv4 6.0 on Windows

Note: For DHCPv4 6.0 Build 67, the Windows service name will remain “Lucent DHCP Service” to allow for interoperability with the current version of VitalQIP at the time of DHCPv4 6.0 Build 67 release

To upgrade to VitalQIP DHCPv4 6.0 from DHCPv4 5.4, 5.5 or 5.6:

-
- 1 Back up the *DHCPService.exe* file before upgrading DHCPv4 6.0.
 - 2 Unzip the *dhcp6.0.67-w2k.zip* file and copy to a temporary directory.
 - 3 Open the Windows Service Controller and Stop the Lucent DHCP Service.
 - 4 In Windows Explorer, copy the new DHCP executable *dhcbservice.exe* to %QIPHOME%\dhcp. Copy the SNMP plug-in library file *qdhcp_snmp.dll* to %QIPHOME%\lib. Optionally, copy the AC cache library *Qdhcplib_AC.dll* to %QIPHOME%\lib, if you are using the Access Control feature and running the Cache service.
 - 5 If you are using the Access Control feature in 64-bit VitalQIP 21 environments, copy *qiprw32.dll*, *QSICommon32.dll* and *QSIINet32.dll* to %QIPHOME%\lib with *Qdhcplib_AC.dll*.
 - 6 Start the Lucent DHCP Service. In the Windows Service Controller, click the Lucent DHCP Service and select Start. DHCPv4 6.0 automatically converts the DHCPv4 5.4, 5.5 or 5.6 format dhcp.db file to the new format if necessary.
-

Note: SNMP 3.0 users must obtain a new plug-in file to support VitalQIP DHCPv4 6.0. Refer to [Configuring SNMP 3.0 \(using Net-SNMP\) on Windows](#) for instructions.

END OF STEPS

Upgrade to VitalQIP DHCPv4 6.0 on UNIX

UNIX only: pre-upgrade requirement

Before you upgrade to VitalQIP DHCPv4 6.0 from DHCPv4 5.4, 5.5, or 5.6 on UNIX, the environment variables must be set. The environment variables will need to be set each time you start VitalQIP DHCPv4 6.0. 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
```

To upgrade to Nokia DHCPv4 6.0 from VitalQIP DHCPv4 5.4, 5.5, or 5.6:

-
- 1 Back up the *dhcpcd* file before upgrading Nokia DHCPv4.
 - 2 Untar the *dhcpc6.0.67-linux-gcc3.tar* file and copy to a temporary directory.
 - 3 Find the process ID (PID) of DHCPv4 Server by running:

```
ps -ef | egrep dhcpcd
```
 - 4 Run `kill <PID>` for VitalQIP DHCPv4 Server (dhcpcd), for example:

```
kill `cat $QIPHOME/etc/dhcpcd.pid`
```
 - 5 Copy the executable *dhcpcd* to *\$QIPHOME/usr/bin*. Copy the SNMP plug-in library (*libqdhcp_snmp.so*) to *\$QIPHOME/usr/lib*. Optionally, copy the AC cache library (*Qdhcplib_AC.so*) to *\$QIPHOME/usr/lib* if you are using the Access Control feature and running the Cache service.
-

-
- 6 If you are using the Access Control feature in 64-bit VitalQIP 8.1.x environments, copy *libqiprw32.so*, *libqsicommon32.so.11*, and *libqsinet32.so.11* to *\$QIPHOME/usr/lib* with *Qdhcplib_AC.so*.
-

- 7 Start the Nokia DHCPv4 Server by running:

```
$QIPHOME/usr/bin/dhcpd -f$QdhcpCONFIG
```

VitalQIP DHCPv4 6.0 automatically converts the DHCPv4 5.4, 5.5, and 5.6 format *DHCPv4.db* file to the new format if necessary.

END OF STEPS

Upgrade Nokia DHCPv4 in a failover configuration

Often DHCP server downtime is more critical than VitalQIP downtime or downtime of any one DNS server. The effects of a DHCP server being down can be reduced if a DHCP failover server is configured. If a DHCP primary server is down during an upgrade, the DHCP failover server hands out addresses instead.

However, a DHCP failover makes upgrade of the Nokia DHCP version more complicated because the failover synchronization can work correctly only if the DHCPv4 primary and DHCP failover are the same DHCP version. If there are multiple DHCP primaries for one failover, all DHCP primaries must be the same version as the DHCP failover.

The recommended procedure for upgrading the Nokia DHCP version in a primary-failover configuration is as follows:

-
- 1 Ensure that “PingDelay” is configured to a non-zero value in the *dhcpd.pcy* of both the primary and failover DHCP servers to prevent duplicate IP addresses on the network in case of any synchronization issues. Also, be certain that no DHCP Generation is scheduled during the time of the upgrade.
-
- 2 Shut down the DHCP failover first and upgrade it to the new DHCP version.

- 3 Be sure that the *dhcp.db* file is still in place on the DHCP failover. Nokia DHCPv4 6.0 automatically converts the DHCPv4 5.4, 5.5, or 5.6 format *dhcp.db* file to the new format if necessary.
- 4 Restart DHCP on the failover, and stop DHCP on the primary. If there are multiple DHCP primaries, stop DHCP on all of them.
- 5 Upgrade the first DHCP primary server to the new DHCP version, and then restart it. At that time, it synchronizes with the DHCP failover and starts handing out addresses for its subnets.
- 6 If there are multiple DHCP primary servers for one failover, upgrade each of them and bring them online, one at a time.
- 7 If the servers were upgraded from DHCPv4 5.4, 5.5 or 5.6 update all the DHCP Server Profiles in VitalQIP. Change the Server Type to Nokia DHCPv4 6.0. Check the other parameters to ensure they did not get reset. Especially, check the Managed Range, Use Failover Server, and Ping Delay.
- 8 When all Server Profiles are correct in VitalQIP, you can do DHCP Generation, but you do not need to do so if the original *dhcpd.conf* and *dhcpd.pcy* files are still on all the servers and are already correct.

END OF STEPS

Enable Client ID

Transitioning to VitalQIP DHCPv4 5.6 or Nokia DHCPv4 6.0 and enabling the SupportClientID policy requires additional consideration for D-DHCP and additional steps for A-DHCP address scopes.

If a previous Nokia DHCPv4 server exists and is being upgraded with SupportClientID policy set to true, then the following should be noted.

- For D-DHCP scopes, adequate leases should be available to ensure that the new leases can be granted, while old leases are left to expire. The reason is that if a client already has a lease in the DHCP database, it was tracked by MAC address with a previous server and the new server with the SupportClientID policy enabled does not recognize the existing lease during a DHCP Discover. However, if the client issues a renew, the renew is granted based on the original MAC/IP but no client id is written for this lease (no tracking by client id available for this lease).
- For A-DHCP scopes, renews work as with D-DHCP, but a Discover from a client that already has an infinite lease from an A-DHCP scope will result in a new lease and the old lease will remain and will not be reused. The old lease should therefore be manually deleted by the administrator.

Configuring SNMP 3.0 on Linux

To configure SNMP Module 3.0 on Linux, follow these steps:

- 1 Make sure there is no old snmp (snmpdm) running).
- 2 Install snmp package if not installed already.
- 3 Get packages for RH 5.2 x64 (*net-snmp-5.3.1-24.el5.x86_64.rpm*, *net-snmp-utils-5.3.1-24.el5.x86_64.rpm*, *lm_sensors-2.10.0-3.1.x86_64.rpm*).
- 4 Install libsensors (net-snmp dependency)

```
# rpm -iv /cdrom/Server/lm_sensors-2.10.0-3.1.x86_64.rpm
Preparing packages for installation...
lm_sensors-2.10.0-3.1
```
- 5 Install snmp master agent (server)

```
# rpm -iv /cdrom/Server/net-snmp-5.3.1-24.el5.x86_64.rpm
Preparing packages for installation...
net-snmp-5.3.1-24.el5
```

6 Install snmp utilities (clients)

```
# rpm -iv /cdrom/Server/net-snmp-utils-5.3.1-24.el5.x86_64.rpm
Preparing packages for installation...
net-snmp-utils-5.3.1-24.el5
```

Note: In RH, yum should be used to install packages. yum can figure out dependencies. For master agent, the package net-snmp is needed and for the tools (snmpget, snmpwalk etc), the package net-snmp-utils is needed. Example on RH 5.3 system:

```
# yum search net-snmp
net-snmp.x86_64 : A collection of SNMP protocol tools and
libraries.
net-snmp-devel.i386 : The development environment for the NET-SNMP
project.
net-snmp-devel.x86_64 : The development environment for the NET-
SNMP project.
net-snmp-libs.i386 : The NET-SNMP runtime libraries.
net-snmp-libs.x86_64 : The NET-SNMP runtime libraries.
net-snmp-perl.x86_64 : The perl NET-SNMP module and the mib2c
tool.
net-snmp-utils.x86_64 : Network management utilities using SNMP,
from the NET-
: SNMP project.

# yum install net-snmp.x86_64
# yum install net-snmp-utils.x86_64
```

7 Copy the *qdhcp.mib* file to the */usr/share/snmp/mibs* directory.

8 If present, remove the old *dhcp.mib* from */usr/share/snmp/mibs* if it is there.

9 Modify the */etc/snmp/snmpd.conf* file to include the information from the supplied *sample_snmpd.conf* file.

```
##
# Minimal configuration file for Net-SNMP master agent snmpd.
# For more details on configuring the master agent and tools,
# pls refer to the Net-SNMP website (http://www.net-snmp.org).
rocommunity public

##
```

```
# Enable AgentX protocol.
# It is necessary for Alcatel-Lucent DNS and DHCP server SNMP sub
  agents.
# For more details on configuring the master agent for AgentX
  support,
# please refer to the Net-SNMP website (http://www.net-snmp.org).
master agentx

##
# Disable trap log retention
#
doNotRetainNotificationLogs yes
```

- 10 Modify `/etc/snmp/snmp.conf` file by adding the following line to automatically load/translate the enterprise DHCPv4 mibs.

```
mibs +QDHCP-SERVER-MIB
```

- 11 Stop and start `snmpd` by typing:

```
# /etc/init.d/snmpd restart
# /etc/init.d/snmptrapd restart

END OF STEPS
```

Configuring SNMP log rotation on Unix

To configure SNMP log rotation on Unix, follow these steps:

- 1 Log in to **VitalQIP**.
-

- 2 Select the **DHCP Servers** from the **DHCP>IPv4** menu.

Result: The DHCPv4 Server Filter Table opens.

- 3 Select the DHCPv4 server that you need to add SNMP log rotation policies.

Result: The DHCPv4 Server page opens.

The screenshot shows a web interface for configuring a DHCPv4 Server. At the top, there are tabs for 'DHCP Server', 'ActiveLease', 'MAC Pool', and 'Reports'. Below the tabs, there are buttons for 'Save', 'Delete', 'Actions', and 'Refresh', along with 'previous' and 'next' navigation links. The main content area is divided into two sections: 'Server Properties' and 'Server Parameters'.

Server Properties

*Host Name:	server1	*Domain Name:	us.schp.com
IPv4 Address:	192.168.88.7	IPv6 Transport Address:	
*Server Type:	LUCENT DHCP 6.0	Failover Server:	

Server Parameters

Name	Value
Failover Server Type	Standalone/Primary
Managed Range	Corporation
* Default Directory	/opt/qip/dhcp
* DHCP Template	general
Accept Client Names	True
Additional Policies	

- 4 Select the **Additional Policies** parameter.

Result: The Additional Policies field appears.

The screenshot shows the 'DHCP Server' configuration window. The 'Server Properties' section includes fields for Host Name (server1), Domain Name (us.schp.com), IPv4 Address (192.168.88.7), IPv6 Transport Address, Server Type (LUCENT DHCP 6.0), and Failover Server. The 'Server Parameters' section is a table with columns 'Name' and 'Value'. The 'Additional Policies' row is highlighted. Below the table is a large empty text area labeled 'Additional Policies'.

Name	Value
Fallover Server Type	Standalone/Primary
Managed Range	Corporation
* Default Directory	/opt/qip/dhcp
* DHCP Template	general
Accept Client Names	True
Additional Policies	

- 5 In the Additional Policies field, enter the name and value of the SNMP log rotation policies. Refer to [Table 8-1, “Log rotation policies”](#) (p. 8-10) for detailed.

Table 8-1 Log rotation policies

Policy name	Default value	value range	Description
SnmppDebugRotateFileSize	0	0 - 1610612736 bytes (10KB - 1.5GB) Note: values from 1-11023 bytes will be automatically reset to the default value.	The maximum debug file size. Supported value formats: <number> : in Byte(s) <number>k : in Kilobyte(s) <number>m : in Megabyte(s). Note: Upper-case letters "K" and "M" may also be used. Note: The zero value is used to disable this function.

Policy name	Default value	value range	Description
<code>SnmpDebugRotateInterval</code>	0	0 - 63072000 seconds (60 second - 2 years) Note: values from 1-59 seconds will be automatically reset to the default value.	The interval time to create a debug file. Supported value formats: <number> : in second(s) <number>m : in minute(s) <number>h : in hour(s) <number>d : in day(s) <number>w : in week(s) <number>y : in year(s) Note: Upper-case letters "M", "H", "D", "W", and "Y" may also be used. Note: The zero value is used to disable this function.
<code>SnmpDebugRotateMaxDepth</code>	1	0 - 9 Note: values greater than 10 will be automatically reset to the default value.	The number of backup debug files to be kept when rotation intervals or max file sizes are reached. Note: Enter zero to disable this function.

Note: The default is used if entered value exceeds the maximum.

Result: The added policy appears in the Policy area.

The screenshot shows a 'Server Parameters' configuration window. It contains a table with 'Name' and 'Value' columns. The 'Additional Policies' row is highlighted in blue. Below the table, there is a section titled 'Additional Policies' containing a text area with the following text:

Name	Value
Failover Server Type	Standalone/Primary
Managed Range	Corporation
* Default Directory	/opt/qip/dhcp
* DHCP Template	general
Accept Client Names	True
Additional Policies	SnmpDebugRotateFileSize=10000 SnmpDebugRotateInterval=60000 SnmpDe...
Client Class	
Debug Information	
Dynamic MDHCP Update	False
Remote Server Proxy	

Additional Policies

```
SnmpDebugRotateFileSize=10000
SnmpDebugRotateInterval=60000
SnmpDebugRotateMaxDepth=2
```

6 Click **Save**.

Result: A Saved Successfully message appears.

7 Select **Actions**, then click **Generation**.

Result: The Generate DHCP Configuration File page opens.

The DHCP server information appears in the upper portion of this page. The fields on the remaining portion of this page are as follows.

Table 8-2 DHCPv4 configuration setup fields

Field	Description
Type	<p>Required. Check the radio button to specify where you want the files to go. Allowable values are:</p> <ul style="list-style-type: none"> • Server – Perform DHCPv4 generation (default). • Preview - Preview the generated DHCP. • Debug – Change the Debug options for this server. This option is only available if the server is a Lucent DHCP server.

Field	Description
Debug Options	<p>If Type is set to Debug, you can select one of the following options for this server:</p> <ul style="list-style-type: none"> • Change Debug Level - Changes the debug level. This option enables Debug Level options when selected. • Clear Debug Log - Clears the debug log • Stop Debug Log - Stops debugging.
Debug Level	<p>If Debug is set to Change Debug Level, you can select one of the following options for the debug level for this server:</p> <ul style="list-style-type: none"> • LevelCritical – The default value. A critical error is one that shuts down the program. Only critical messages are logged. • LevelError – An error has occurred, but the program should continue. Critical messages are included. • LevelWarning – The program has encountered an unexpected issue but continues. Errors and critical messages are included with these warnings. • LevelInfo – These are informational messages about the program events and flow. These messages include critical messages, errors and warnings. • LevelDebug – Indicates that all levels should be logged. <p>Note: The current debug level for the server is the one that is initially selected when you open the Generate DHCP Configuration File page.</p>

8 In the **Scheduler** area, select a schedule for DHCP configuration file generation.

9 Click **Submit**.

10 In the console mode, go to the `$QIPHOME`.

1. Stop the running dhcpv4 server by finding the daemon's process ID and using the `kill <process_ID>` command or by using the `pkill dhcpv4` command.

Note: To find the dhcpv4 process ID, use this command:

```
ps -ef | grep dhcp
```

2. Start the dhcpv4 server by:

```
/opt/qip/usr/bin/dhcp -f /opt/qip/dhcpv4/dhcp.conf
```

```
END OF STEPS
```

Configuring SNMP 3.0 (using Net-SNMP) on Windows

Installation

OpenSSL

If choosing the ssl-enabled installation of Net-SNMP, download or build the openssl binaries:

- 1 Download the latest 32-bit OpenSSL binary from <http://www.slproweb.com/products/Win32OpenSSL.html> (Win32 OpenSSL v0.9.8k Light).
- 2 If running the install produces a warning about runtime libraries, you may need to install the 32-bit runtime redistributables found at the same location (Visual C++ 2008 Redistributables).
- 3 Install the package to *c:\OpenSSL*.
- 4 Choose the copy the binaries to the OpenSSL (/bin) directory, rather than the default Windows directory, unless you are sure you know the impact.
- 5 Set the PATH system environment variable to include “*C:\Openssl\bin*” if you chose the recommended copy location instead of the default (Windows) location.

```
END OF STEPS
```

Net-SNMP

- 1 Download and install SNMP from Net-SNMP website.

-
- 2 Use 32-bit version with or without ssl.
 - 3 Use the default installation options (This is the tested configuration, although integration with Microsoft SNMP is optional).
 - 4 If you desire to run the master agent (snmpd.exe) or trap daemon (snmptrapd.exe) as services:
 - **Run, Start Menu -> Programs -> Net-SNMP -> Service -> Register Agent Service** to “daemonize” the master agent.
 - **Run, Start Menu -> Programs -> Net-SNMP -> Service -> Register Trap Service** to “daemonize” the trap service.
 - You can remove the services by choosing the corresponding “**Unregister**” selection at the same start menu location.

END OF STEPS

Configuring SNMP Traps for all platforms

The VitalQIP DHCP server uses AgentX protocol for sending traps. The following policies are used in *snmpd.conf* file for configuration of traps:

```
;
; For sending v2 traps to localhost
trap2sink 127.0.0.1 public
; For sending v2 traps to destination 10.10.4.2
trap2sink 10.10.4.2:162 public
; For sending v2 traps to destination 10.10.4.16
trap2sink 10.10.4.16:162 public
; For sending v1 traps to destination 10.10.4.1
trapsink 10.10.4.1:162 public
;You can send traps to multiple destinations. Add each destination
seperately.
;trap2sink 10.10.4.2 public also can be used.Default port will be
used.
```

SNMP Trap Receiver

- 1 Create a *snmptrapd.conf* file in the *<path_of_net-snmp>\etc\snmp* directory and add the following lines:

```
disableAuthorization yes
authCommunity log public
```

- 2 Start the trap receiver.

END OF STEPS

Note: The Configuring SNMP Traps and SNMP Trap Receiver procedures are common for all operating systems.

CONFIGURATION

SNMP Master Agent

- 1 Copy the *sample_snmpd.conf* file (provided with DHCPv4) to *<path_of_net-snmp>\etc\snmp\snmpd.conf* file.
-

- 2 Ensure the following lines are in the *snmpd.conf* file:

```
master agentx
agentxSocket tcp:localhost:705
```

- 3 Start the master agent.

END OF STEPS

SNMP Trap Receiver

- 1 Create a *snmptrapd.conf* file in the *<path_of_net-snmp>\etc\snmp* directory and add the following lines:

```
disableAuthorization yes
authCommunity log public
```

- 2 Start the trap receiver.

END OF STEPS

SNMP Plugins

By default Net-SNMP master agent talks AgentX protocol through Unix domain socket. However Windows does not have domain sockets. Therefore, the server plugins require a configuration file:

- 1 qdhcp_snmp_agent.conf in <path_of_net-snmp>\etc\snmp directory with the text lines below:

```
##
# Talk to snmpd using TCP at port 705.
# snmpd has to be configured to listen to the same port.
agentxSocket tcp:localhost:705.
```

Ensure the plugin is in the %QIPHOME%\lib directory.

- 2 Start the server.

END OF STEPS

SNMP Utilities

- 1 Copy the qdhcp.mib file to the <path_of_net-snmp>\share\snmp\mibs directory.

- 2 Remove our old *dhcp.mib* if it is there.

- 3 By default Net-SNMP utilities do not load the enterprise DHCP server mibs. Configure the general snmp config file (<path_of_net-snmp>\etc\snmp\snmp.conf) by adding the appropriate lines below:

mibs +QDHCP-SERVER-MIB

VERIFICATION

Master Agent

Successful configuration will log something like the following in *<path_of_net-snmp>\log\snmpd.log*.

Turning on AgentX master support.

NET-SNMP version 5.7.3

NET-SNMP version 5.7.3 Plugins

Successful DHCP plugin connection to master agent will log something like the following in the *%QIPHOME%\log\qdhcp_snmp.log*:

```
2016-06-21 15:10:55 qdhcp_snmp_agent QDHCP SNMP module 3.0 Build
56 Starting
2016-06-21 15:10:55 SNMP Policies:
2016-06-21 15:10:55 SnmpOn=True
2016-06-21 15:10:55 SnmpLogFile=/opt/qip/log/qdhcp_snmp.log
2016-06-21 15:10:55 SnmpTruncateLog=True
2016-06-21 15:10:55 SnmpThrottleBadPacketTraps=True
2016-06-21 15:10:55 SnmpThrottleSubnetDepletionTraps=True
2016-06-21 15:10:55 SnmpUpdateRangeTable=True
2016-06-21 15:10:55 SnmpDebugRotateFileSize=0
2016-06-21 15:10:55 SnmpDebugRotateInterval=0
2016-06-21 15:10:55 SnmpDebugRotateMaxDepth=1
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing agent
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing snmp
2016-06-21 15:10:55 MIB search path:
/root/.snmp/mibs:/netapp/buildtools/net-snmp/5.7.3/linux-gcc3-
32bit/share/snmp/mibs
2016-06-21 15:10:55 Cannot find module (SNMPv2-MIB): At line 0 in
(none)
2016-06-21 15:10:55 Cannot find module (IF-MIB): At line 0 in
(none)
2016-06-21 15:10:55 Cannot find module (IP-MIB): At line 0 in
(none)
2016-06-21 15:10:55 Cannot find module (TCP-MIB): At line 0 in
(none)
2016-06-21 15:10:55 Cannot find module (UDP-MIB): At line 0 in
(none)
```

```
2016-06-21 15:10:55 Cannot find module (HOST-RESOURCES-MIB): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (NOTIFICATION-LOG-MIB): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (DISMAN-EVENT-MIB): At line
0 in (none)
2016-06-21 15:10:55 Cannot find module (DISMAN-SCHEDULE-MIB): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (UCD-SNMP-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (UCD-DEMO-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (SNMP-TARGET-MIB): At line
0 in (none)
2016-06-21 15:10:55 Cannot find module (NET-SNMP-AGENT-MIB): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (HOST-RESOURCES-TYPES): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (SNMP-MPD-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (SNMP-USER-BASED-SM-MIB):
At line 0 in (none)
2016-06-21 15:10:55 Cannot find module (SNMP-FRAMEWORK-MIB): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (SNMP-VIEW-BASED-ACM-MIB):
At line 0 in (none)
2016-06-21 15:10:55 Cannot find module (SNMP-COMMUNITY-MIB): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (IPV6-ICMP-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (IPV6-MIB): At line 0 in
(none)
2016-06-21 15:10:55 Cannot find module (IPV6-TCP-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (IPV6-UDP-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (IP-FORWARD-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (NET-SNMP-PASS-MIB): At
line 0 in (none)
```

```
2016-06-21 15:10:55 Cannot find module (NET-SNMP-EXTEND-MIB): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (UCD-DLMOD-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (SNMP-NOTIFICATION-MIB): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (SNMPv2-TM): At line 0 in
(none)
2016-06-21 15:10:55 Cannot find module (NET-SNMP-VACM-MIB): At
line 0 in (none)
2016-06-21 15:10:55 NET-SNMP version 5.7.3 AgentX subagent
connected
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing dhcpServSystem
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
dhcpServSubnetCounters
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
dhcpServBootpCounters
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
dhcpServDhcpCounters
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
dhcpServBootpStatistics
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
dhcpServDhcpStatistics
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
dhcpServRangeTable
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
dhcpServFailoverTable
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing trap data
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
vitalqipDhcpTrapTable
2016-06-21 15:10:55 qdhcp snmp agent Created 14 rows in range
table
2016-06-21 15:10:55 qdhcp snmp agent Created 0 rows in failover
table
```

If not, you may see a line like the following, indicating an error in the configuration files.

```
2009-08-06 15:28:01 Warning: Failed to connect to the agentx
master agent ([NIL]):
```

Trap Receiver

Successful configuration will log something like the following in `<path_of_net-snmp>/log/snmpd.log`.

NET-SNMP version 5.7.3

If not, you may see the following in `<path_of_net-snmp>/log/snmptrapd.log`.

Warning: *no access control information configured.*

This receiver will not accept any incoming notifications.

NET-SNMP version 5.7.3

Utilities

Successful DHCP mib loading and translation will look something like the following when running the `snmptranslate -Tp -IR dhcpServSystem` command.

```
+---dhcpServSystem(1)
+-- -R-- String dhcpServSystemDescr(1)
|       Textual Convention: DisplayString
|       Size: 0..255
+-- -R-- EnumVal dhcpServSystemStatus(2)
|       values: starting(0), running(1), stopping(2),
stopped(3), reload(4)
+-- -R-- Gauge dhcpServSystemUpTime(3)
+-- -R-- Gauge dhcpServSystemResetTime(4)
```

If not, you may see a line like the following, indicating an error.

Unknown object identifier: dhcpServSystem

ALU Appliance

There are 2 packages for the appliance. (the `qdhcp` server and the `qdhcp-snmp` plugin, with mib).

Remove the old proxy statements from `/etc/snmp/snmpd.conf` file.

Modify `/etc/snmp/snmpd.conf` file by adding the following line to enable AgentX master agent support.

Note: The `snmp` package will have all the default setting, so there should not be any need to modify anything.

master agentx

agentXPerms 755 755 qip qip

stop and start snmpd

Running dhcpd:

Make sure path of libqdhcpd_snmp.so is in LD_LIBRARY_PATH environment variable
make sure QIPHOME environment variable is set.

Look at dhcpdd.pcy file to make sure debugging is on and path of log file is correct.

start dhcpdd:

Successful DHCP plugin connection to master agent will log something like the following
in the %QIPHOME%\log\qdhcp_snmp.log.

```
2016-06-21 15:10:55 qdhcp_snmp_agent QDHCP SNMP module 3.0 Build
56 Starting
2016-06-21 15:10:55 SNMP Policies:
2016-06-21 15:10:55 SnmpOn=True
2016-06-21 15:10:55 SnmpLogFile=/opt/qip/log/qdhcp_snmp.log
2016-06-21 15:10:55 SnmpTruncateLog=True
2016-06-21 15:10:55 SnmpThrottleBadPacketTraps=True
2016-06-21 15:10:55 SnmpThrottleSubnetDepletionTraps=True
2016-06-21 15:10:55 SnmpUpdateRangeTable=True
2016-06-21 15:10:55 SnmpDebugRotateFileSize=0
2016-06-21 15:10:55 SnmpDebugRotateInterval=0
2016-06-21 15:10:55 SnmpDebugRotateMaxDepth=1
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing agent
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing snmp
2016-06-21 15:10:55 MIB search path:
/root/.snmp/mibs:/netapp/buildtools/netsnmp/5.7.3/linux-gcc3-
32bit/share/snmp/mibs
2016-06-21 15:10:55 Cannot find module (SNMPv2-MIB): At line 0 in
(none)
2016-06-21 15:10:55 Cannot find module (IF-MIB): At line 0 in
(none)
2016-06-21 15:10:55 Cannot find module (IP-MIB): At line 0 in
(none)
2016-06-21 15:10:55 Cannot find module (TCP-MIB): At line 0 in
(none)
2016-06-21 15:10:55 Cannot find module (UDP-MIB): At line 0 in
(none)
2016-06-21 15:10:55 Cannot find module (HOST-RESOURCES-MIB): At
line 0 in (none)
```

```
2016-06-21 15:10:55 Cannot find module (NOTIFICATION-LOG-MIB): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (DISMAN-EVENT-MIB): At line
0 in (none)
2016-06-21 15:10:55 Cannot find module (DISMAN-SCHEDULE-MIB): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (UCD-SNMP-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (UCD-DEMO-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (SNMP-TARGET-MIB): At line
0 in (none)
2016-06-21 15:10:55 Cannot find module (NET-SNMP-AGENT-MIB): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (HOST-RESOURCES-TYPES): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (SNMP-MPD-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (SNMP-USER-BASED-SM-MIB):
At line 0 in (none)
2016-06-21 15:10:55 Cannot find module (SNMP-FRAMEWORK-MIB): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (SNMP-VIEW-BASED-ACM-MIB):
At line 0 in (none)
2016-06-21 15:10:55 Cannot find module (SNMP-COMMUNITY-MIB): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (IPV6-ICMP-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (IPV6-MIB): At line 0 in
(none)
2016-06-21 15:10:55 Cannot find module (IPV6-TCP-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (IPV6-UDP-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (IP-FORWARD-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (NET-SNMP-PASS-MIB): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (NET-SNMP-EXTEND-MIB): At
line 0 in (none)
```

```
2016-06-21 15:10:55 Cannot find module (UCD-DLMOD-MIB): At line 0
in (none)
2016-06-21 15:10:55 Cannot find module (SNMP-NOTIFICATION-MIB): At
line 0 in (none)
2016-06-21 15:10:55 Cannot find module (SNMPv2-TM): At line 0 in
(none)
2016-06-21 15:10:55 Cannot find module (NET-SNMP-VACM-MIB): At
line 0 in (none)
2016-06-21 15:10:55 NET-SNMP version 5.7.3 AgentX subagent
connected
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing dhcpServSystem
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
dhcpServSubnetCounters
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
dhcpServBootpCounters
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
dhcpServDhcpCounters
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
dhcpServBootpStatistics
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
dhcpServDhcpStatistics
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
dhcpServRangeTable
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
dhcpServFailoverTable
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing trap data
2016-06-21 15:10:55 qdhcp_snmp_agent Initializing
vitalqipDhcpTrapTable
2016-06-21 15:10:55 qdhcp snmp agent Created 14 rows in range
table
```

If not, you may see a line like the following, indicating an error in the configuration files.

```
2009-08-06 15:28:01 Warning: Failed to connect to the agentx
master agent ([NIL]):
```

Testing SNMP queries

At this point, it is assumed that dhcp sub agents have successfully connected to master agent (snmpd). That means SNMP queries by DHCP OID should succeed. For example, to send a query for the dhcpServSystem MIB variable:

```
$ snmpwalk -v2c -c public 192.168.89.135
.1.3.6.1.4.1.1751.1.48.0.1.1.1.1
```

```

QDHCP-SERVER-MIB::dhcpServSystemDescr.0 = STRING: " (Version: 6.0
Build 56- VitalQIP DHCP Server) "
QDHCP-SERVER-MIB::dhcpServSystemStatus.0 = INTEGER: running(1)
QDHCP-SERVER-MIB::dhcpServSystemUpTime.0 = Gauge32: 522
QDHCP-SERVER-MIB::dhcpServSystemResetTime.0 = Gauge32: 522

```

However, it is convenient to send queries by using MIB variables than OIDs. There are many ways to make MIB files available to Net-SNMP applications. For details, please look at the document [TUT:Using and loading MIBS](#).

To verify that the MIB files are available to Net-SNMP clients, type the following:

```
$ snmptranslate -Tp -IR dhcpServSystem
```

You should see the following:

```

+--dhcpServSystem(1)
  +-- -R-- String dhcpServSystemDescr(1)
  |       Textual Convention: DisplayString
  |       Size: 0..255
  +-- -R-- EnumVal dhcpServSystemStatus(2)
  |       values: starting(0), running(1), stopping(2),
stopped(3), reload(4)
  +-- -R-- Gauge dhcpServSystemUpTime(3)
  +-- -R-- Gauge dhcpServSystemResetTime(4)

```

Now send some SNMP queries:

```

$ snmpwalk -v2c -c public 127.0.0.1 dhcpServSystem
QDHCP-SERVER-MIB::dhcpServSystemDescr.0 = STRING: " (Version: 6.0
Build 56 - VitalQIP DHCP Server) "
QDHCP-SERVER-MIB::dhcpServSystemStatus.0 = INTEGER: running(1)
QDHCP-SERVER-MIB::dhcpServSystemUpTime.0 = Gauge32: 72
QDHCP-SERVER-MIB::dhcpServSystemResetTime.0 = Gauge32: 72

```

```

$ snmpget -v2c -c public 127.0.0.1 dhcpServSystemDescr.0
QDHCP-SERVER-MIB::dhcpServSystemDescr.0 = STRING: " (Version: 6.0
Build 56 - VitalQIP DHCP Server) "

```

```
$ snmpwalk -v2c -c public 127.0.0.1 vitalqipDhcpTrapTable
```

```

QDHCP-SERVER-MIB::vitalqipDhcpTrIndex.1 = INTEGER: 1
QDHCP-SERVER-MIB::vitalqipDhcpTrIndex.2 = INTEGER: 2
QDHCP-SERVER-MIB::vitalqipDhcpTrSequence.1 = Counter32: 1
QDHCP-SERVER-MIB::vitalqipDhcpTrSequence.2 = Counter32: 1
QDHCP-SERVER-MIB::vitalqipDhcpTrId.1 = INTEGER: monitor(1)
QDHCP-SERVER-MIB::vitalqipDhcpTrId.2 = INTEGER: monitor(1)
QDHCP-SERVER-MIB::vitalqipDhcpTrText.1 = STRING: "VitalQIP DHCP
started"
QDHCP-SERVER-MIB::vitalqipDhcpTrText.2 = STRING: "VitalQIP DHCP
Re-initialized"
QDHCP-SERVER-MIB::vitalqipDhcpTrPriority.1 = INTEGER: inform(1)
QDHCP-SERVER-MIB::vitalqipDhcpTrPriority.2 = INTEGER: inform(1)
QDHCP-SERVER-MIB::vitalqipDhcpTrClass.1 = INTEGER: 1
QDHCP-SERVER-MIB::vitalqipDhcpTrClass.2 = INTEGER: 3
QDHCP-SERVER-MIB::vitalqipDhcpTrType.1 = INTEGER: 1
QDHCP-SERVER-MIB::vitalqipDhcpTrType.2 = INTEGER: 3
QDHCP-SERVER-MIB::vitalqipDhcpTrTime.1 = Counter32: 1466014734
QDHCP-SERVER-MIB::vitalqipDhcpTrTime.2 = Counter32: 1466014946
QDHCP-SERVER-MIB::vitalqipDhcpTrSuspect.1 = STRING: "qipsun34"
QDHCP-SERVER-MIB::vitalqipDhcpTrSuspect.2 = STRING: "qipsun34"
QDHCP-SERVER-MIB::vitalqipDhcpTrDiagId.1 = INTEGER: 1
QDHCP-SERVER-MIB::vitalqipDhcpTrDiagId.2 = INTEGER: 3
QDHCP-SERVER-MIB::vitalqipDhcpTrIteration.1 = INTEGER: 1
QDHCP-SERVER-MIB::vitalqipDhcpTrIteration.2 = INTEGER: 2

```

Use snmptable to see the exact number of rows in the table.

```

#
SNMP table: QDHCP-SERVER-MIB::vitalqipDhcpTrapTable
vitalqipDhcpTrIndex vitalqipDhcpTrSequence vitalqipDhcpTrId
vitalqipDhcpTrText vitalqipDhcpTrPriority vitalqipDhcpTrClass
vitalqipDhcpTrType vitalqipDhcpTrTime vitalqipDhcpTrSuspect
vitalqipDhcpTrDiagId vitalqipDhcpTrIteration 1 1 monitor
"VitalQIP DHCP started" inform 1 1 1466014972 "qipsun34"

```

Policies for SNMP Plugin

The sample dhcpd.pcy file:

```

QIPOrgID=1
debug=all
debugfile=/opt/dhcp_test_netsnmp/data/dhcpd.log

```

```
; Primary
;SecondaryIPAddr=192.168.0.1
; one to one Failover
;PrimaryIPAddr=192.168.0.2
; many to one Failover
PrimaryIPAddr1=10.52.0.5
PrimaryIPAddr2=192.168.0.3
PrimaryIPAddr3=192.168.0.4
;
; Policies for SNMP plugin
;;
; SnmpOn=boolean. The valid value is: true, false, yes, no, 1, 0,
;   on, off.
; If false, the dhcp server will not attempt to load the snmp
;   plugin.
; The default is true.
SnmpOn=true
;;
; SnmpLogFile=<path>
; There are four special LogFile names: syslog, stdout, stderr
; If the name is syslog, stdout or stderr, the log messages will
;   be written to
;   Syslog, stdout and stderr respectively.If the policy is
;   commented out,
; the plugin will try to write log to $QIPHOME/log/qdhcp_snmp.log,
; if the directory does not exists, it will try
; to write log to Syslog otherwise.
;SnmpLogFile=/var/log_qdhcp_snmp.log
;;
; Truncate it the log if true. The value is: true, false, yes, no,
;   1, 0, on, off.
; This policiy is significant for logging to a file only. The
;   default is true.
SnmpTruncateLog=true
; As the DHCP server can send streams for traps, it is possible to
; throttle those traps. If the value is yes (default), the bad
;   packet
; traps will be sent only if the trap is older than 2 seconds.
;   SnmpThrottleBadPacketTraps=Yes
; If the value is yes (default), the Subnet Depletion traps will
;   be
; sent only if the trap is older than 2 seconds.
;   SnmpThrottleSubnetDepletionTraps=Yes
```

Note: If *SnmpLogFile* is set to Syslog on server running Windows, the log will be redirected to application event logs.

Frequently Asked Questions

- **It does not work, what should I do?**

Look at the `qdhcp_snmp_agent.log` file. Make sure the sub agent is connected to the master agent using AgentX protocol. Run the master agent in foreground to watch the log to stderr: `snmpd -f -Dagetnx -L`.

- **Sub agent is connected to master agent but none of the dhcp mib variables are returned, what should I do?**

The `snmpd.conf` file has some kind of access control set which is preventing the master agent to serve OIDs below certain configured OID. To verify that, replace the `snmpd.conf` file with the `sample_snmpd.conf` file or create a minimal conf file (read next question), restart `snmpd` and see if it works.

Note: On RH 5.x, the default `/etc/snmp/snmpd.conf` file restricts snmp queries to `system + hrSystem`. So, after dhcp sub agent is connected to master agent, if you query for any dhcp MIB variable you get a message saying No more variables left in this MIB View.

- **What does a minimal snmpd.conf file looks like?**

```
# The simplest snmpd.conf file without any sort of real access control
rocommunity public
master agentx
```

- **Most of the time snmp queries to the DHCP server is timing out. What can I do?**

The DHCP server populates statistics data structure if the data is older than 120 seconds. If the `dhcpd.conf` file is such that it has lot of scopes or options and if it takes longer to populate statistics data structure, snmp query will time out if the query triggers the server to populate the statistics data. The snmp code in DHCPv4 6.0 tries to increase the statistics update time if it takes longer than 120 seconds to generate. For example, if it takes say 130 seconds to update the statistics data, it will try to update it again if the data is older than 130 seconds and so on. But even with that snmp query will timeout if the query triggers an update of the statistics data. Look at the dhcp server's log file to see how long it is taking to generate the statistics data.

- **How do I know that I am using the latest MIB files?**

The MIB definitions are changed to QDHCP-SERVER-MIB for dhcp servers. So look at the output of the `snmpget` or `snmpwalk` and check the first word for the MIB definition.

