Copyright © 1995-2015 SolarWinds Worldwide, LLC. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SOLARWINDS and SOLARWINDS & Design marks are the exclusive property of SolarWinds Worldwide, LLC and its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks, registered or pending registration in the United States or in other countries. All other trademarks mentioned herein are used for identification purposes only and may be or are trademarks or registered trademarks of their respective companies.

VoIP and Network Quality Manager Version 4.2, revised 12/3/2018
About SolarWinds

SolarWinds, Inc develops and markets an array of IT management, monitoring, and discovery tools to meet the diverse requirements of today’s IT management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in IT management and discovery technology. The SolarWinds customer base includes over 85 percent of the Fortune 500 and customers from over 170 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

<table>
<thead>
<tr>
<th>Team</th>
<th>Contact information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales</td>
<td>1.866.530.8100</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.solarwinds.com">www.solarwinds.com</a></td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="http://www.solarwinds.com/support">www.solarwinds.com/support</a></td>
</tr>
<tr>
<td>User Forums</td>
<td><a href="http://www.thwack.com">www.thwack.com</a></td>
</tr>
</tbody>
</table>

Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Specifying</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Window items, including buttons and fields.</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>Book and CD titles, variable names, new terms</td>
</tr>
<tr>
<td><strong>Fixed font</strong></td>
<td>File and directory names, commands and code examples, text typed by you</td>
</tr>
</tbody>
</table>
### Convention Specifying

<table>
<thead>
<tr>
<th>Convention</th>
<th>Specifying</th>
</tr>
</thead>
<tbody>
<tr>
<td>Straight brackets, as in [value]</td>
<td>Optional command parameters</td>
</tr>
<tr>
<td>Curly braces, as in {value}</td>
<td>Required command parameters</td>
</tr>
<tr>
<td>Logical OR, as in value1</td>
<td>value2</td>
</tr>
</tbody>
</table>

### SolarWinds VoIP and Network Quality Manager Documentation Library

The following documents are included in the SolarWinds VoIP and Network Quality Manager documentation library:

<table>
<thead>
<tr>
<th>Document</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SolarWinds VoIP and Network Quality Manager Administrator Guide</td>
<td>Provides detailed setup, configuration, and conceptual information.</td>
</tr>
<tr>
<td>Page Help</td>
<td>Provides help for every window in the SolarWinds VoIP and Network Quality Manager user interface.</td>
</tr>
<tr>
<td>Release Notes</td>
<td>Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at <a href="http://www.solarwinds.com">www.solarwinds.com</a></td>
</tr>
</tbody>
</table>

The following documents supplement the SolarWinds VoIP and Network Quality Manager documentation library with information about Network Performance Monitor:
<table>
<thead>
<tr>
<th>Document</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Performance Monitor Administrator Guide</td>
<td>Provides detailed setup, configuration, and conceptual information.</td>
</tr>
<tr>
<td>Page Help</td>
<td>Provides help for every window in the Network Performance Monitor user interface.</td>
</tr>
<tr>
<td>Release Notes</td>
<td>Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at <a href="http://www.solarwinds.com">www.solarwinds.com</a>.</td>
</tr>
</tbody>
</table>
# Table of Contents

Tips and Tricks .................................................................................................................. 13

Introduction ...................................................................................................................... 14
  Why Install SolarWinds VoIP and Network Quality Manager ........................................ 14
  What SolarWinds VoIP and Network Quality Manager Does .......................................... 14
  How SolarWinds VoIP and Network Quality Manager Works ......................................... 17

Installing SolarWinds VoIP and Network Quality Manager ................................................ 19
  SolarWinds VNQM Licensing .......................................................................................... 19
    IP SLA Sites .................................................................................................................. 20
    IP Phones .................................................................................................................... 20
    Nodes ............................................................................................................................ 20
    Licensing example ........................................................................................................ 20
  Installation Requirements ............................................................................................... 20
  SolarWinds VoIP and Network Quality Manager Requirements ...................................... 21
  SQL Server Requirements .............................................................................................. 22
  Installing SolarWinds VNQM ......................................................................................... 24

Additional Polling Engine and Web Console ..................................................................... 27
  Installing an Additional Polling Engine ......................................................................... 28
  Installing an Additional Web Console ............................................................................ 30

Upgrading VNQM ............................................................................................................. 32

Uninstalling VNQM .......................................................................................................... 33

Configuring VoIP and Network Quality Manager ............................................................. 34
  IP SLA Management ....................................................................................................... 34
# Understanding Quality of Service and IP SLAs

- **IP SLA Operations in VNQM** .................................................. 36
- **Quality of Service Metrics** ......................................................... 37
  - Latency .................................................................................. 37
  - Jitter ..................................................................................... 39
  - Packet Loss ........................................................................... 41
  - Mean Opinion Score (MOS) ..................................................... 42
- **Understanding Polling Intervals for IP SLA Operations** ................. 44
- **Designating Paths** ................................................................ 45
- **Understanding the Impact IP SLA Operations Have on Your Network** ...................................................... 46
- **Dangers of Overusing IP SLA Operations** ................................... 47
- **Strategies for the Proper Use of IP SLA Operations** ......................... 47
- **Configuring Devices for IP SLA Operations** ................................ 49
  - Configuring devices for ICMP echo path operations .......... 49
- **Adding IP SLA Nodes to VoIP and Network Quality Manager** ........ 50
- **Discovering IP SLA-Capable Nodes Automatically** .................... 51
- **Adding IP SLA-Capable Nodes Manually** ..................................... 51
- **Configuring CLI Credentials** .................................................. 52
- **Adding IP SLA Operations** ........................................................ 53
- **Adding DNS IP SLA Operations to Your Devices** ....................... 53
- **Adding FTP IP SLA Operations to Your Devices** ....................... 55
- **Adding HTTP IP SLA Operations to Your Devices** ...................... 57
- **Adding DHCP IP SLA Operations to Your Devices** ..................... 58
- **Adding TCP Connect IP SLA Operations to Your Devices** ............ 60
- **Adding UDP Jitter IP SLA Operations to Your Devices** ............... 62
- **Adding VoIP UDP Jitter IP SLA Operations to Your Devices** ........ 64
- **Adding ICMP Echo IP SLA Operations to Your Devices** .............. 66
- **Adding UDP Echo IP SLA Operations to Your Devices** ............... 69
- **Adding ICMP Path Echo Operations to Your Devices** .................. 71
- **Adding ICMP Path Jitter Operations to Your Devices** ................... 73
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding Existing Operations to VoIP and Network Quality Manager</td>
<td>76</td>
</tr>
<tr>
<td>Editing IP SLA Operations</td>
<td>77</td>
</tr>
<tr>
<td>Modifying the SLA Location</td>
<td>77</td>
</tr>
<tr>
<td>Renaming Operations in VoIP and Network Quality Manager</td>
<td>78</td>
</tr>
<tr>
<td>Deleting IP SLA Operations from VoIP and Network Quality Manager</td>
<td>78</td>
</tr>
<tr>
<td>VoIP Management</td>
<td>79</td>
</tr>
<tr>
<td>Managing Call Managers</td>
<td>80</td>
</tr>
<tr>
<td>CLI Credentials</td>
<td>80</td>
</tr>
<tr>
<td>Credentials Used for Cisco CallManager</td>
<td>81</td>
</tr>
<tr>
<td>Monitoring Call Manager Health</td>
<td>81</td>
</tr>
<tr>
<td>Adding Cisco CallManager Devices to VoIP and Network Quality Manager</td>
<td>82</td>
</tr>
<tr>
<td>Adding CallManager Express Devices to VoIP and Network Quality Manager</td>
<td>85</td>
</tr>
<tr>
<td>Managing Avaya Call Managers</td>
<td>85</td>
</tr>
<tr>
<td>Avaya CDR parameters</td>
<td>92</td>
</tr>
<tr>
<td>Adding Avaya Call Manager Devices</td>
<td>93</td>
</tr>
<tr>
<td>Requirements</td>
<td>93</td>
</tr>
<tr>
<td>Adding an Avaya Communication and Media Server to VNQM</td>
<td>93</td>
</tr>
<tr>
<td>Requirements for Handling RTCP Data</td>
<td>95</td>
</tr>
<tr>
<td>Bandwidth Requirements for Avaya Communication and Media Servers</td>
<td>96</td>
</tr>
<tr>
<td>Adding Call Manager Devices from Other Manufacturers</td>
<td>96</td>
</tr>
<tr>
<td>Defining FTP Servers</td>
<td>97</td>
</tr>
<tr>
<td>Configuring Cisco CallManagers for FTP</td>
<td>97</td>
</tr>
<tr>
<td>Editing Call Managers</td>
<td>98</td>
</tr>
<tr>
<td>Call Manager CDR/CMR Polling</td>
<td>99</td>
</tr>
<tr>
<td>AXL Credentials</td>
<td>99</td>
</tr>
<tr>
<td>FTP Server Settings</td>
<td>100</td>
</tr>
<tr>
<td>Call Manager CDR/CQR Polling</td>
<td>101</td>
</tr>
<tr>
<td>Call Manager CLI Credentials</td>
<td>101</td>
</tr>
<tr>
<td>Deleting Call Manager Devices from VoIP and Network Quality Manager</td>
<td>101</td>
</tr>
<tr>
<td>Managing Gateways</td>
<td>102</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Adding Gateways</td>
<td>102</td>
</tr>
<tr>
<td>Editing VoIP Gateways</td>
<td>103</td>
</tr>
<tr>
<td>Editing CLI Credentials for Gateway Nodes</td>
<td>104</td>
</tr>
<tr>
<td>Removing Gateways</td>
<td>105</td>
</tr>
<tr>
<td>Selecting VoIP and Network Quality Manager Infrastructure</td>
<td>105</td>
</tr>
<tr>
<td>Call Precedence Levels</td>
<td>106</td>
</tr>
<tr>
<td>VoIP and Network Quality Manager Settings</td>
<td>107</td>
</tr>
<tr>
<td>VNQM Settings Overview</td>
<td>107</td>
</tr>
<tr>
<td>IP SLA Management</td>
<td>107</td>
</tr>
<tr>
<td>Manage IP SLA Operations</td>
<td>107</td>
</tr>
<tr>
<td>Manage IP SLA Nodes</td>
<td>108</td>
</tr>
<tr>
<td>VoIP Management</td>
<td>108</td>
</tr>
<tr>
<td>Manage CallManager Nodes</td>
<td>108</td>
</tr>
<tr>
<td>Manage VoIP Gateways</td>
<td>108</td>
</tr>
<tr>
<td>Select VoIP Infrastructure</td>
<td>108</td>
</tr>
<tr>
<td>Details</td>
<td>109</td>
</tr>
<tr>
<td>Edit VoIP &amp; Network Quality Manager Settings</td>
<td>109</td>
</tr>
<tr>
<td>Database Details</td>
<td>110</td>
</tr>
<tr>
<td>Configuring VoIP and Network Quality Manager Settings</td>
<td>110</td>
</tr>
<tr>
<td>Setting Traffic Precedence</td>
<td>113</td>
</tr>
<tr>
<td>Using VoIP and Network Quality Manager</td>
<td>114</td>
</tr>
<tr>
<td>Starting VNQM</td>
<td>114</td>
</tr>
<tr>
<td>Exploring VNQM Views</td>
<td>115</td>
</tr>
<tr>
<td>VoIP CallManager View</td>
<td>116</td>
</tr>
<tr>
<td>Customizing Charts in VNQM</td>
<td>118</td>
</tr>
<tr>
<td>Chart Titles</td>
<td>118</td>
</tr>
<tr>
<td>Calculated Series</td>
<td>119</td>
</tr>
<tr>
<td>Time Period</td>
<td>119</td>
</tr>
<tr>
<td>Sample Interval</td>
<td>120</td>
</tr>
<tr>
<td>Chart Size</td>
<td>120</td>
</tr>
</tbody>
</table>
Table of Contents

Data Tables ......................................................................................................................... 120
Font Size ............................................................................................................................. 120
Printing Options ................................................................................................................... 120
Data Export Options .......................................................................................................... 121
Advanced ............................................................................................................................. 121
Using Custom Properties for VNQM ................................................................................ 121
Using Advanced Alerts and Actions in VNQM ................................................................. 122
VNQM Reports .................................................................................................................... 124
 Using Predefined VNQM Reports .................................................................................... 125
     Historical IP SLA Reports ............................................................................................... 125
     Historical VoIP Reports ................................................................................................. 129
VNQM Maps ....................................................................................................................... 129
VolIP and Network Quality Manager Map Variables ....................................................... 130

Appendix A: Software License Key .................................................................................... 132
    Maintaining Licenses with License Manager ............................................................... 133
    Installing License Manager ......................................................................................... 133
    Using License Manager ............................................................................................... 133

Appendix B: MIBs Maintained by VolIP and Network Quality Manager ......................... 135
    General ........................................................................................................................... 135
    All Operations ................................................................................................................. 135
    DHCP Operations ........................................................................................................... 136
    DNS Operations ............................................................................................................ 136
    HTTP and FTP Operations ............................................................................................. 136
    ICMP Echo Operations ................................................................................................. 136
    TCP Connect Operations ............................................................................................... 136
    UDP Jitter Operations .................................................................................................... 136
    VoIP UDP Jitter Operations .......................................................................................... 137
    VoIP Specific MIBs ......................................................................................................... 137

Appendix C: Supported Versions of Cisco Unified Call Manager .................................... 139
    OIDs from the ccmTable ............................................................................................. 139
OIDs from the ccmRegionTable .................................................................139
OIDs from the ccmGatewayTable .............................................................140
OIDs from the ccmProductTypeTable .........................................................140
OIDs from the ccmPhoneTable .................................................................140
OIDs from the ccmPhoneExtnTable .............................................................141
OIDs from the ccmH323DeviceTable ...........................................................141

Appendix D: How VoIP and Network Quality Manager Creates Operations ..........143
  Owner Field Value ..............................................................................143
  SNMP-Based Operations .....................................................................143
    DHCP Operations .............................................................................144
    DNS Operations .............................................................................145
    FTP Operations .............................................................................146
    HTTP Operations ...........................................................................147
    ICMP Echo Operations .....................................................................148
    TCP Connect Operations .................................................................149
    UDP Echo Operations .....................................................................151
    UDP Jitter Operations .....................................................................152
    VoIP UDP Jitter Operations ..............................................................153
  CLI-Based Operations .........................................................................156
    ICMP Path Echo Operations .............................................................156
      IP SLA Syntax .............................................................................156
      IP SLA Monitor Syntax ................................................................156
      RTR Syntax .................................................................................157
    ICMP Path Jitter Operations ..............................................................157
      IP SLA Syntax .............................................................................157
      IP SLA Monitor Syntax ................................................................158
      RTR Syntax .................................................................................158

Appendix E: Database Maintenance ..........................................................160
  Running Database Maintenance ...........................................................160
Tips and Tricks

- Network Performance Monitor provides default chart titles and subtitles. To restore the default values, clear the respective fields when editing chart titles, and then click Submit.
- To display gauges and charts for the opposite direction call path between the same two endpoints, click View reverse call path.
- The time interval for collecting CDR and CMR data can be modified during the configuration of Cisco call managers. For more information, see Configuring Cisco CallManagers for FTP.
- To find the necessary balance between server load and data granularity, try using different polling intervals. For more information, see Configuring VoIP and Network Quality Manager Settings.
- Configure the length of time performance data is retained to balance database maintenance with IP SLA requirements. For more information, see Configuring VoIP and Network Quality Manager Settings.
**Introduction**

SolarWinds VoIP and Network Quality Manager offers an easy-to-use, scalable IP SLA network monitoring solution that can integrate seamlessly with other SolarWinds products on the Orion platform.

**Why Install SolarWinds VoIP and Network Quality Manager**

Internet Protocol Service Level Agreement (IP SLA) technology offers a cost-effective and efficient response to the needs of enterprises of all sizes. As a network manager, you face more than the simple question of whether your network is up or down. You need to know specific quality of service measurements for your network. VoIP and Network Quality Manager gives you the tools to quickly test the fitness of your current network, and then determine and track quality of service on your network over time.

SolarWinds VoIP and Network Quality Manager collects IP SLA-specific data and provides presentation tools that enable IP SLA network monitoring and real-time status reporting. VoIP and Network Quality Manager can also be used in integration with SolarWinds Network Performance Monitor, leveraging the NPM monitoring options to provide a better overview of your network.

**What SolarWinds VoIP and Network Quality Manager Does**

With VoIP and Network Quality Manager you can monitor and report both real-time and historical performance statistics for your IP SLA-capable network. VoIP and Network Quality Manager offers the following features to help you manage your entire network:
Quality of Service (QoS) Monitoring with Cisco IP SLA Operations

VoIP and Network Quality Manager uses Cisco IP SLA operations to measure network performance. Specifically, IP SLA operations provide immediate insight into network Quality of Service (QoS), including packet loss, latency, jitter, and mean opinion score (MOS) metrics. VoIP and Network Quality Manager collects IP SLA data and then presents it in the easy-to-use Web Console environment. With VoIP and Network Quality Manager and IP SLA operations, you know at a glance exactly how well your network is and has been performing. For more information about Cisco IP SLA operations, see www.cisco.com/go/ipsla.

VoIP Phone Troubleshooting

VoIP and Network Quality Manager uses Call Detail Records (CDR) and Call Management Records (CMR) data from your call managers to help you identify possible affected calls and patterns of affected calls. CDR/CMR data provides region information per call record in addition to the call source and destination, MOS, latency, packet loss, termination call code, and more. With VoIP and Network Quality Manager, you can drill in to problem areas to start identifying the underlying problems.

Custom Charts and Gauges

VoIP and Network Quality Manager provides easy-to-read charts and gauges that you can customize to suit your monitoring requirements. You can quickly determine the current status and performance of your network using custom VoIP and Network Quality Manager gauges of key IP SLA metrics such as jitter, latency, packet loss, and MOS. With custom VoIP and Network Quality Manager charts, you can easily track the historical performance of all the paths on your network.

Custom Alerts and Actions

VoIP and Network Quality Manager enables you to create custom alerts for your network in the same way you create advanced alerts and actions in Network Performance Monitor. Specifically, VoIP and Network Quality Manager enables you to configure IP SLA-related alerts with a variety of corresponding actions to notify you of events on your network. These IP SLA alerts are filtered from existing alerts and presented separately within VoIP and Network Quality Manager. For more information about using Advanced Alerts in VoIP and Network Quality Manager, see "Using Advanced Alerts and Actions" in the VoIP and Network Quality Manager Administrator Guide.
**Custom Reporting**

With Orion Report Writer, VoIP and Network Quality Manager provides real-time and historical statistics reporting for the IP SLA-specific network statistics. When you install VoIP and Network Quality Manager, several predefined reports become available within Report Writer. By using custom properties, you can also generate custom reports to specifically communicate the historical condition of your network. For more information about data reporting in VoIP and Network Quality Manager, see "Creating VoIP and Network Quality Manager Reports" in the [VoIP and Network Quality Manager Administrator Guide](#).

**Gateway Monitoring**

VoIP and Network Quality Manager provides comprehensive resources that enable you to monitor your VoIP gateways, giving you an overview of individual PRI trunks of your gateways.

**Call Manager Monitoring**

Call manager devices are scalable call processing solutions for managing IP-based telecommunications networks. These devices provide VoIP networks with the features and functions of more traditional telephony. VoIP and Network Quality Manager uses the SNMP and ICMP monitoring technology and the AXL API of Cisco to interact with call managers and to persistently track call manager performance. With the addition of VoIP and Network Quality Manager, you immediately know the status of your VoIP network and all of its components at any time.

VoIP and Network Quality Manager comes with presets that allow you to monitor Cisco CallManager and CallManager Express, and Avaya Call Manager devices. You can also define custom Management Information Base (MIB) pollers to monitor call managers from other manufacturers. Call managers by other manufacturers are monitored like other nodes and cannot be added as call managers. For more information, consult the following table:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Reference</th>
</tr>
</thead>
</table>
How SolarWinds VoIP and Network Quality Manager Works

SolarWinds VoIP and Network Quality Manager builds upon the proven technology of the SolarWinds Orion platform to give you monitoring, alerting, and reporting abilities for your network. After installation and initial configuration, VoIP and Network Quality Manager deploys Cisco IP SLA operations to generate various types of network traffic including DNS requests, DHCP IP allocation, FTP and HTTP requests, TCP connect, ICMP and UDP Echo, and simulated VoIP traffic between devices on your network using the jitter codec you specify. Cisco IP SLAs provide real-time and historical performance statistics that VoIP and Network Quality Manager presents in the readily customizable Web Console. VoIP and Network Quality Manager downloads CDR/CMR data from your Cisco call manager and uses your AXL credentials to pull region information to provide detailed call record information about every call in your network.

You can also monitor Avaya Communication and Media Server devices with VoIP and Network Quality Manager. VNQM intercepts the CDR packets sent by the TCP protocol, as well as the RTCP data sent through UDP, and based on these data, it provides information about the call details and the call quality.
How SolarWinds VoIP and Network Quality Manager Works

IP SLA operations VoIP and Network Quality Manager only work with Cisco IOS devices that support the RTT MIB. For more information about the MIBs VoIP and Network Quality Manager uses, see "MIBs Maintained by VoIP and Network Quality Manager" in the VoIP and Network Quality Manager Administrator Guide.

Note: For VoIP statistics, VoIP and Network Quality Manager uses simulated VoIP traffic, instead of real VoIP traffic. This ensures the continuous collection of performance statistics so you can know the state of your network at any time, regardless of whether the network is actually being used to complete a call.
Installing SolarWinds VoIP and Network Quality Manager

SolarWinds VoIP and Network Quality Manager provides a simple, wizard-driven installation process.

The installation is powered by the following tools:

1. **VNQM Installation Wizard** installs VNQM and launches the installation of the corresponding .NET framework requirements.
2. **VNQM Licence Activation Wizard** deals with the activation of your license, you can temporarily skip this step.
3. **SolarWinds Configuration Wizard** takes care of the basic configuration of VNQM.

You can find more installation related details in the following sections:

- VNQM Licensing
- Installation Requirements
- Installing SolarWinds VNQM
- Additional Polling Engine and Web Console
- Upgrading VNQM
- Uninstalling VNQM

**SolarWinds VNQM Licensing**

SolarWinds VoIP and Network Quality Manager uses four different license types and is licensed on the IP SLA site level, the IP Phone level, and the node level.

The following license types are available:

- SLA 5 – 5 IP SLA sites, 300 IP Phones, and 40 nodes
- SLA 25 – 25 IP SLA sites, 1500 IP Phones, and 200 nodes
Installing SolarWinds VoIP and Network Quality Manager

- SLA 50 – 50 IP SLA sites, 3000 IP Phones, and 400 nodes
- SLA X – Unlimited IP SLA sites, unlimited IP Phones, and 1000 nodes

**IP SLA Sites**

Any device that has at least one monitored operation counts toward your IP SLA site count.

**IP Phones**

Any IP phone connected to your network when the network is polled counts toward your IP Phone count. Phones can be registered or unregistered. Registered phones are connected, take precedence over unregistered phones, and count toward your license. Unregistered phones are disconnected and do not count toward your license. If you have more registered IP phones than the number granted to you by your license, only the latest registered phones will be monitored, up to the number of phones granted by your license. Registered and unregistered phones after that number will not be monitored.

**Nodes**

Any SNMP-enabled device that you monitor counts toward your node count. Each monitored call manager typically consumes a node license.

Each source node counts towards your node count. In a bidirectional setup, each node is both a source and target node, and they both count towards your license.

**Licensing example**

If your network uses four IP SLA sites, 45 nodes, and 700 IP Phones, you may decide to purchase the smallest license.

The number of IP SLA sites fall within your license count, but the number of nodes and IP Phones do not. When you configure VoIP and Network Quality Manager, you must choose 40 out of your 45 nodes to monitor, including the call managers you want to monitor. VoIP and Network Quality Manager automatically monitors only 300 registered IP Phones at a time of the 700 on your network. Each time your network is polled, a different 300 registered IP Phones may be monitored.

**Installation Requirements**
The following requirements are based on a minimum installation of VoIP and Network Quality Manager with SQL Server on a separate database server. If you are installing VoIP and Network Quality Manager with SolarWinds Network Performance Monitor, the server that you use to host VoIP and Network Quality Manager must also support an installation of NPM.

**Note:** To optimize database scalability, we recommend that you maintain your SQL Server installation on its own server, separate from the server on which you are hosting SolarWinds Network Performance Monitor and VoIP and Network Quality Manager. If you must host your SQL server on the same server, we recommend a quad-processor, 2.67 GHz, 64-bit CPU and at least 16 GB of RAM.

### SolarWinds VoIP and Network Quality Manager Requirements

<table>
<thead>
<tr>
<th>Hardware or software</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Environment</strong></td>
<td>VoIP and Network Quality Manager supports IP SLA for Cisco IP SLA capable devices. It is possible to monitor Cisco CallManager, CallManager Express, and Avaya Communication and Media Server devices with VoIP and Network Quality Manager.</td>
</tr>
<tr>
<td><strong>CPU</strong></td>
<td>Dual processor, 3GHz</td>
</tr>
<tr>
<td><strong>RAM</strong></td>
<td>8 GB</td>
</tr>
<tr>
<td><strong>Hard drive space</strong></td>
<td>20 GB</td>
</tr>
<tr>
<td><strong>Operating system</strong></td>
<td>Windows Server 2003 SP2 (32-bit), Enterprise edition or higher, including R2, with IIS installed</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 SP2 (64-bit), including R2, with IIS installed, running in 32-bit mode</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 (32-bit), Enterprise Edition or higher, with IIS installed</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 (64-bit), with IIS installed, running in 32-bit mode</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012</td>
</tr>
</tbody>
</table>
## Installing SolarWinds VoIP and Network Quality Manager

**Hardware or software** | **Requirements**
--- | ---
.NET Framework | Version 4.0
Web browser | Internet Explorer version 8 or later
Mozilla Firefox - two most recent versions
Google Chrome - two most recent versions

### SQL Server Requirements

<table>
<thead>
<tr>
<th>Hardware or software</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| CPU | Dual processor, 3 GHz  
Quad-processor, 2.67 GHz, 64-bit (for large networks) |
| RAM | 8 GB  
16 GB (for large networks) |
| Hard drive space | 20 GB |
| Database | SQL Server 2008 Express, Standard, or Enterprise  
SQL Server 2012 Express, Standard, or Enterprise  
SQL Server 2012 SP1 |

### Notes:
- If you anticipate six million standard, device to device calls per month with a peak hour of 20,000 calls, we recommend using a dedicated SQL server with a 64-bit, 2.67 GHz quad-processor CPU and 16 GB of RAM. We do not support more than six million calls per month.
If you are installing VoIP and Network Quality Manager with SolarWinds NPM, see "Orion NPM Requirements" in the SolarWinds Network Performance Monitor Administrator Guide.
Installing SolarWinds VoIP and Network Quality Manager

Installing SolarWinds VNQM

SolarWinds VoIP and Network Quality Manager employs an intuitive wizard to guide your installation.

To install VNQM:

1. Log on as an administrator to the server you will use to monitor your IP SLA network.
2. Launch the executable file.
   - If you downloaded the product from the SolarWinds website, navigate to your download location, and then launch the executable file. You may need to run the executable file as an administrator.
   - If you received physical media, browse to the executable file, and then launch the executable file. You may need to run the executable file as an administrator.
3. If you are prompted to install requirements, click Install, and then complete the installation, including a reboot, if required.

Notes:

- Downloading and installing the Microsoft .NET Framework 4.0 may take more than 20 minutes, depending on your existing system configuration.
- If a reboot is required, after restart, click Install to resume the installation, and then click Next on the Welcome window.
4. If you want to use the Orion Improvement Program to send anonymous data about your product usage to SolarWinds, click Yes, send data.
5. Review the Welcome text, and then click Next.
6. Select your preferred language, and then click Next.
   Note: This selection cannot be changed later.
7. **If the Setup Wizard detects that Microsoft Internet Information Services (IIS) is not installed**, select **Suspend installation to manually install IIS**, click **Finish**, quit setup, and then install IIS.

   **Note:** The Web Console requires that Microsoft IIS is installed on the VoIP and Network Quality Manager server. If you do not install IIS at this point, you must install IIS later, and then configure a website for the Web Console to use. For more information about IIS, see [Enabling IIS](#).

8. Accept the license agreement, and then click **Next**.

9. Click **Next** to confirm the default Destination Location.

   **If you want to install to a destination folder other than the default given**, click **Browse**, select an installation folder, and then click **OK**.

10. Read the Start Copying Files information, and if you are satisfied with your settings, click **Next** to continue.

11. Click **Finish** to close the Installation Wizard.

12. Select one of the available licensing options.

   - **If you want to buy a license**, click **Buy Now**.

   - **If this is a new installation of SolarWinds VoIP and Network Quality Manager**, click **Enter Licensing Information**, and then complete the license registration process. For more information about software license keys, see "Software License Key" in the [VoIP and Network Quality Manager Administrator Guide](#).

     Click **Continue** when the license is successfully installed.

   - **If you want to evaluate VNQM**, click **Continue Evaluation**.

13. The Orion Configuration Wizard launches automatically. Click **Next** on the Welcome screen to continue the basic configuration.

    **Note:** **If the Configuration Wizard does not start automatically**, start the **Configuration Wizard** in the SolarWinds Orion folder.
14. Define your SQL server settings, and then click **Next**.
   a. Select or fill in your **SQL Server** instance.
   b. Define the authentication used on the server:
      - *If you want to use your Windows credentials*, select Use Windows Authentication.
      - *If you want to use your SQL server credentials*, select Use SQL Server Authentication.

   **Note:** The selected instance must support mixed mode or SQL authentication with strong passwords. For more information, see the page on the Microsoft Developer Network about [authentication modes](#).

15. Specify your SQL database settings:
   - *If you are creating a new database*, select Create a new database, provide a name for the new database, and then click Next.
   - *If you are using an existing database*, select Use an existing database, type or select the database name, and then click Next.

   **Note:** If you are using an existing database or SQL account, the user account must be a member of the db_owner database role.

16. Specify the SQL server account for Orion:
   a. *If you want the polling engine and web console to use a new SQL account for accessing the database*, select Create a new account, provide a new account name and confirmed password, and then click Next.

   **Note:** If you are creating a new SQL account for use with VoIP and Network Quality Manager, the account must be a member of the db_securityadmin database role.
   b. *If you want the polling engine and web console to use an existing SQL account for accessing the database*, select the existing account, provide the appropriate password, and then click Next.
17. Specify the website settings:

a. Provide the IP address of the server used for the web console.
   
   **Note:** Consider retaining the default IP address setting of All Unassigned, unless your environment requires the designation of a specific IP address for your Web Console.

b. Specify both the port through which you want to access the web console, and the volume and folder in which you want to install the web console files, and then click **Next**.
   
   **Note:** If you specify any port other than 8787, the default port for evaluations, you must include that port in the URL used to access the web console. For example, if you specify an IP address of 192.0.2.1 and port 8080, the URL used to access the web console is http://192.0.2.1:8080.

c. **If you are prompted to create a new directory,** click **Yes**.

d. **If you are prompted to create a new website,** click **Yes**.
   
   **Note:** Choosing to overwrite an existing website does not result in the deletion of any previously applied custom NPM website settings.

18. Confirm that the services you want to install are selected on the Service Settings window, and then click **Next**.

19. **If you are prompted to disable the SNMP Trap Service**, click **Yes**.

20. Review the final configuration items, and then click **Next**.

21. Click **Finish** on the Completing the Orion Configuration Wizard dialog. The Orion Web Console is launched automatically.
Installing additional pollers and Web Consoles helps you extend your SolarWinds VoIP and Network Quality Manager implementation. You can install additional polling engines to aid you in load balancing and configure additional websites to ensure redundant access through more than one web server. By sharing the same database, you can also share a unified user interface, making the addition of polling engines transparent to your staff.

The additional polling engines and Web Consoles are available as separate installers from your main installation.

These components are licensed and purchased separately from your main VoIP and Network Quality Manager. For more information about purchasing licenses, contact your sales representative (sales@solarwinds.com) or customer service.

**Installing an Additional Polling Engine**

Download the special installation package for the VoIP and Network Quality Manager additional polling engines to the server where you want to install the additional polling engine:

```
SolarWinds-Orion-VNQM-vx.y.z-Poller.exe
```

where \( x \) is the major release number, \( y \) is the minor release number, and \( z \) is the point release number.

**Note:** After completing the following procedure, VoIP and Network Quality Manager polling engines emulate the same behavior as NPM additional polling engines. They monitor only applications on nodes associated with the VoIP and Network Quality Manager additional polling engine.

**To install the additional polling engine:**

1. Log on with a Windows administrator account to the server where you want to install the additional polling engine.
2. Run the installer for the VoIP and Network Quality Manager Poller.
3. **If you are prompted to install requirements**, click **Install**, and then complete the installation, including a reboot, if required.

   **Notes:**
   - Downloading and installing the Microsoft .NET Framework 4.0 may take more than 20 minutes, depending on your existing system configuration.
   - If a reboot is required, click **Install** after the restart to resume the installation, and then click **Next** on the Welcome window.

4. **If you want to use the Orion Improvement Program to send anonymous data about your product usage to SolarWinds**, click **Yes, send data**.

5. Type your VoIP and Network Quality Manager server host name or IP address, the administrator user name, and the administrator password. Click **Next** to verify that you are installing the correct version of the polling engine for your server.

6. Review the Welcome page, and then click **Next**.

7. Accept the license agreement, and then click **Next**.

8. Choose a destination location, or accept the default location, and then click **Next**.

9. Click **Next** to start copying files.

10. Click **Finish** to complete the Installation Wizard.

11. Click **Enter Licensing Information** to enter your license, or click **Continue Evaluation**.

12. Review the Configuration Wizard Welcome page, and then click **Next**.

13. Configure the database for your environment by selecting the appropriate **SQL Server** database and **Authentication** information, and then click **Next**.

14. Configure the database by selecting **Use an existing database**, and then selecting the name of the **SQL Server** database for the VoIP and Network Quality Manager server, and then click **Next**.

15. Select whether to **Create a new account**, or **Use an existing account**, enter the account information, and then click **Next**.
Installing SolarWinds VoIP and Network Quality Manager

16. **If the Website Settings page is displayed**, configure the IP Address, Port, and Website Root Directory as appropriate, select whether you want to enable automatic login, and then click Next.

17. Ensure that all the services displayed in the Service Settings page are selected, including the Job Engine Plugin, and then click Next.

18. Review the Configuration Wizard Summary page, and then click Next.

19. Click Finish to complete the Configuration Wizard.

You can assign nodes to the polling engines by selecting the polling engine you want in the Add Node wizard.

You can also perform poller load balancing using Node Management to assign nodes to polling engines.

**To assign nodes to polling engines:**

1. Log on to the web console as a user with node management rights.
2. Click Home.
3. In the All Nodes resource on the Orion Summary Home view, click Manage Nodes.
4. Select the nodes you want to change, and then click More Actions > Change Polling Engine.
5. Select the new polling engine, and then click Submit.

**Installing an Additional Web Console**

Download the special installation package for VoIP and Network Quality Manager additional web consoles to the server where you want to install the additional web console:

SolarWinds-Orion-VNQM-vx.y.z-WebOnly.exe

where x is the major release number, y is the minor release number, and z is the point release number.

TCP port 17777 must be open on both the VoIP and Network Quality Manager server and the website.

Ensure you schedule an appropriate maintenance window in which to install the additional Web Console.
Installing an Additional Web Console

To install the additional Web Console:

1. Log on to your current VoIP and Network Quality Manager additional Web Console server with a Windows administrator account.
2. Run the VoIP and Network Quality Manager installer.
3. If you are prompted to install requirements, click Install, and then complete the installation, including a reboot, if required.

   Notes:
   - Downloading and installing the Microsoft .NET Framework 4.0 may take more than 20 minutes, depending on your existing system configuration.
   - If a reboot is required, click Install after the restart to resume the installation, and then click Next on the Welcome window.
4. If you want to use the Orion Improvement Program to send anonymous data about your product usage to SolarWinds, click Yes, send data.
5. Type your VoIP and Network Quality Manager server host name or IP address, the administrator user name, and the administrator password. Click Next to verify that you are installing the correct version of the polling engine for your server.
6. Review the Welcome page, and then click Next.
7. Accept the license agreement, and then click Next.
8. Choose a destination location, or accept the default location, and then click Next.
9. Click Next to start copying files.
10. Click Finish to complete the Installation Wizard.
11. Review the Configuration Wizard Welcome window, and then click Next.
12. Specify the appropriate information on the Database Settings window, and then click Next.
13. Specify the appropriate database to use, and then click Next. Ensure you have stopped your polling engines before continuing.
14. Specify the appropriate database account on the Database Account window, and then click Next.
15. Select the IP address, port, and website root directory on the Website Settings window, and then click Next.
16. Review the configuration summary, and then click Next.
17. Click Finish to complete the Configuration Wizard.

**Upgrading VNQM**

Upgrading VNQM does not require you to uninstall your current installation. However, you must follow certain upgrade paths according to the version you are upgrading VNQM from.

Until VoIP and Network Quality Manager 4.0, the application required the installation of SolarWinds Network Performance Monitor. Since version 4.0, VNQM has been a stand-alone application which can but does not have to be installed together with NPM.

For more details about upgrading VNQM, see the KB article "Compatibility of SolarWinds Orion Products for Installation and Upgrade."

**Notes:**

- Back up your database before you start the upgrade to ensure none of your data is lost during the upgrade.
- None of your historical data or customized settings will be lost in the process.
- If you have a large amount of VoIP and CallManager data, the upgrade may take 30 minutes to an hour to complete.

**To upgrade VoIP and Network Quality Manager:**

1. Follow the appropriate upgrade path.
2. Install VoIP and Network Quality Manager normally. For more information about installing VNQM, see "Installing VoIP and Network Quality Manager" in the VoIP and Network Quality Manager Administrator Guide.

**If you use IP SLA Manager 3.5.1:**

1. Upgrade NPM to version 10.5.
2. Upgrade to VoIP and Network Quality Manager 4.0, 4.0.1 or 4.1, and then upgrade from any of these versions to VNQM 4.2.
If you use VNQM 4.0 or above:

1. Upgrade to VoIP and Network Quality Manager 4.2.

**Uninstalling VNQM**

The uninstallation procedure for VNQM consists of removing the SolarWinds VoIP and Network Quality Manager application in the Control Panel. However, configuration files, database entries and registry keys are not removed by this procedure.

To completely uninstall VNQM, contact SolarWinds Technical Support for assistance.
Configuring VoIP and Network Quality Manager

VNQM monitors your IP SLA operations and VoIP infrastructure. Configuring VNQM means adding your devices to VNQM, defining what you are going to monitor, and how often you want to poll data from your devices.

You can configure VNQM in the Orion Web Console.

To start VNQM:

1. Log on to your VoIP and Network Quality Manager server.
2. Start the Orion Web Console in the Orion program folder.
3. Click the VoIP and Network Quality tab.

After establishing your basic VoIP infrastructure and adding IP SLA operations, you can change your settings at any time to further customize VoIP and Network Quality Manager for your network. For example, you can add IP SLA devices, designate paths, and configure polling options. VoIP and Network Quality Manager uses a wizard-based application to guide you through the process of configuring VoIP and Network Quality Manager for your network.

The following sections provide detailed instructions for configuring the various aspects of VoIP and Network Quality Manager for your network.

- **IP SLA Management** - configuring your IP SLA devices and IP SLA operations
- **VoIP Management** - configuring your CallManagers, gateways, and defining VoIP infrastructure
- **VNQM Details** - configuring database, polling and monitoring settings

### IP SLA Management

By using VNQM you can monitor IP SLA operations that are set on your devices. Designing a tailored set of IP SLA operations for monitoring your devices is a complex task.
For more information about IP SLA operations and quality of service metrics in VNQM, see "Understanding Quality of Service and IP SLAs" in the VoIP and Network Quality Manager Administrator Guide.

After you have designed a set of IP SLA operations to be used for monitoring your devices, complete the following steps:

1. Configure your devices for IP SLA operations. For more information, see "Configuring Devices for IP SLA Operations" in the VoIP and Network Quality Manager Administrator Guide.

2. Add devices that you want to monitor to your database. For more information, see "Adding Devices for Monitoring in the Web Console" in the SolarWinds Orion Core Administrator Guide.

3. Add your devices as IP SLA nodes into VNQM. For more information, see "Adding IP SLA nodes to VoIP and Network Quality Manager" in the VoIP and Network Quality Manager Administrator Guide.

4. Define IP SLA operations to be monitored by VNQM. For more information, see "Adding IP SLA Operations" in the VoIP and Network Quality Manager Administrator Guide.

Related tasks:

- Editing IP SLA operations
- Deleting IP SLA operations

**Understanding Quality of Service and IP SLAs**

IP Service Level Agreements (IP SLAs) are a diagnostic method developed by Cisco that generates and analyzes traffic between Cisco IOS devices on your network. By using VoIP and Network Quality Manager to implement IP SLA operations between your network devices, you can acquire real-time and historical statistics that give you accurate Quality of Service (QoS) measurements over designated network paths between a source device and a target device.

For a better understanding of individual quality of service and IP SLAs, it is necessary to understand the following concepts:

**Source**

A device that creates and inserts IP SLA packets into the network. The source is where all IP SLA operation tests are initiated.
Target
The ultimate destination of the packets created and sent by the source.

Operation
The type of test being performed on the network.

IP SLA Operations in VNQM
The following operations are supported by VoIP and Network Quality Manager.

DHCP
Dynamic Host Configuration Protocol (DHCP) IP SLA operations measure the response time taken to discover a DHCP server, and then obtain a leased IP address from it.

DNS
Domain Name Server (DNS) IP SLA operations measure the difference in time from when a DNS request is sent and when the reply is received.

FTP
File Transfer Protocol (FTP) IP SLA operations measure the response time between a Cisco device and an FTP server to retrieve a file.

HTTP
Hypertext Transfer Protocol (HTTP) IP SLA operations measure distributed web services response times.

ICMP Echo
Internet Control Message Protocol (ICMP) Echo IP SLA operations measure round trip time between nodes on the network.

ICMP Path Echo
ICMP Echo IP SLA operations measure round trip time hop-by-hop between nodes on the network.

ICMP Path Jitter
ICMP Path Jitter IP SLA operations measure WAN quality by testing connection times hop-by-hop between two devices.

TCP Connect
Transmission Control Protocol (TCP) Connect IP SLA operations measure WAN quality by testing connection times between two devices using a specific port.
UDP Echo

User Datagram Protocol (UDP) Echo IP SLA operations measure round trip time between nodes on the network.

UDP Jitter

UDP Jitter IP SLA operations measure WAN quality by testing connection times between two devices using a specific port number.

VoIP UDP Jitter

Voice over Internet Protocol (VoIP) UDP Jitter IP SLA operations measure call path metrics on the VoIP network.

Quality of Service Metrics

The quality of service in VNQM is measured by using the following metrics:

- Latency
- Jitter
- Packet Loss
- Mean Opinion Score

Latency

With respect to VoIP, latency is a measure of the difference in time between when one caller speaks and when the other caller hears what the first has said. Excessive network latency can cause noticeable gaps and synchronization loss in transmitted conversations, particularly when VoIP is used with other types of data, as in a video conference. If these gaps become large enough, callers may find that they will inadvertently interrupt each other while conversing.

IP SLA operations measure latency by sequentially applying four different time stamps to a single test packet in the following way:

1. Time stamp $T_1$ is applied to a test packet as it leaves the source router.
2. Time stamp $T_2$ is applied as the test packet arrives at the target router.
3. Time stamp $T_3$ is applied as the test packet leaves the target router to return to the source.
4. Time stamp $T_4$ is applied when the test packet returns to the source.
IP SLA operations provide four separate measures of latency by computing differences among the four time stamps in the following way.

<table>
<thead>
<tr>
<th>Latency measure</th>
<th>Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Round trip time</td>
<td>T4 – T1</td>
</tr>
<tr>
<td>Source-to-target latency</td>
<td>T2 – T1</td>
</tr>
<tr>
<td>Target processing latency</td>
<td>T3 – T2</td>
</tr>
<tr>
<td>Target-to-source latency</td>
<td>T4 – T3</td>
</tr>
</tbody>
</table>

**Note:** Latency is computed for both source-to-target and target-to-source directions to account for asynchronous network behavior, providing a more detailed picture of the overall network latency.

VoIP and Network Quality Manager calculates latency in the following way:

```python
if (rttMonLatestJitterOperNumOfRTT <> 0)
delay = (convert rttMonLatestJitterOperRTTSum to milli/microseconds depending on rttMonEchoAdminPrecision) / rttMonLatestJitterOperNumOfRTT
else
delay = 0
if (micro/milli second convert value of rttMonLatestJitterOperOWSumSD and rttMonLatestJitterOperNumOfOW has value and rttMonLatestJitterOperNumOfOW <> 0)
delaySD = micro/milli second convert value of rttMonLatestJitterOperOWSumSD / rttMonLatestJitterOperNumOfOW
else
if (micro/milli second convert value of rttMonLatestJitterOperOWSumDS and rttMonLatestJitterOperNumOfOW has value and rttMonLatestJitterOperNumOfOW <> 0)
delayDS = micro/milli second convert value of rttMonLatestJitterOperOWSumDS / rttMonLatestJitterOperNumOfOW
else
delaySD & delayDS = null
```
Jitter

Jitter is a measure of the variation in network latency that results in a loss of synchronization over time. In VoIP phone calls, users experience jitter as distracting noise, clicks, and pops. To ensure acceptable quality of service, network jitter should be located, isolated, and addressed. By using VoIP and Network Quality Manager you can identify areas of your network that may be experiencing synchronization difficulties, and then you can take the necessary action to ensure maximum quality of service on your VoIP network.

VoIP and Network Quality Manager requires you to select a jitter codec to properly configure IP SLAs for your VoIP network. Codecs compute jitter by specifying that IP SLA operations send a number of packets \( n \), each with a specific size \( s \), at a set interval \( i \) between packets, at a determined frequency \( f \), as shown in the following table.

<table>
<thead>
<tr>
<th>Codec</th>
<th>IP SLA operation frequency ( f )</th>
<th>Default number of packets ( n )</th>
<th>Default packet size ( s )</th>
<th>Default interval between packets ( i )</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711a</td>
<td>Set on each operation as the network test interval</td>
<td>1000</td>
<td>160 + 12 RTP bytes</td>
<td>20 ms</td>
</tr>
<tr>
<td>G.711u</td>
<td></td>
<td>1000</td>
<td>160 + 12 RTP bytes</td>
<td>20 ms</td>
</tr>
<tr>
<td>G.729a</td>
<td></td>
<td>1000</td>
<td>20 + 12 RTP bytes</td>
<td>20 ms</td>
</tr>
</tbody>
</table>

### Table of IP SLA Operations

<table>
<thead>
<tr>
<th>IP SLA Operation</th>
<th>(f)</th>
<th>(n)</th>
<th>(s)</th>
<th>(i)</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonLatestJitterOperNumOfRTT</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rttMonLatestJitterOperRTTSum</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rttMonEchoAdminPrecision</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.37</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rttMonLatestJitterOperOWSumSD</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.33</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rttMonLatestJitterOperNumOfOW</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.41</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rttMonLatestJitterOperOWSumDS</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.37</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
For more information about configurable settings within VoIP and Network Quality Manager, see "Configuring VoIP and Network Quality Manager Settings" in the VoIP and Network Quality Manager Administrator Guide.

**Note:** Based on the Cisco IP SLA operations used by VoIP and Network Quality Manager, jitter codecs G.711a and G.711u can achieve a peak MOS of 4.34. On the same basis, jitter codec G.729a can achieve a peak MOS of 4.06.

VoIP and Network Quality Manager calculates jitter in the following way:

\[
\text{jitterSD} = \frac{\text{rttMonLatestJitterOperSumOfPositivesSD} + \text{rttMonLatestJitterOperSumOfNegativesSD}}{\text{rttMonLatestJitterOperNumOfPositivesSD} + \text{rttMonLatestJitterOperNumOfNegativesSD}}
\]

\[
\text{jitterDS} = \frac{\text{rttMonLatestJitterOperSumOfPositivesDS} + \text{rttMonLatestJitterOperSumOfNegativesDS}}{\text{rttMonLatestJitterOperNumOfPositivesDS} + \text{rttMonLatestJitterOperNumOfNegativesDS}}
\]

\[
\text{Jitter} = \frac{\text{rttMonLatestJitterOperSumOfPositivesSD} + \text{rttMonLatestJitterOperSumOfPositivesDS} + \text{rttMonLatestJitterOperSumOfNegativesSD} + \text{rttMonLatestJitterOperSumOfNegativesDS}}{\text{rttMonLatestJitterOperNumOfPositivesSD} + \text{rttMonLatestJitterOperNumOfPositivesDS} + \text{rttMonLatestJitterOperNumOfNegativesSD} + \text{rttMonLatestJitterOperNumOfNegativesDS}}
\]

<table>
<thead>
<tr>
<th>Variable</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonLatestJitterOperSumOfPositivesSD</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.9</td>
</tr>
<tr>
<td>rttMonLatestJitterOperSumOfNegativesSD</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.14</td>
</tr>
<tr>
<td>rttMonLatestJitterOperNumOfPositivesSD</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.8</td>
</tr>
<tr>
<td>rttMonLatestJitterOperNumOfNegativesSD</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.13</td>
</tr>
<tr>
<td>rttMonLatestJitterOperSumOfPositivesDS</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.19</td>
</tr>
<tr>
<td>rttMonLatestJitterOperSumOfNegativesDS</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.24</td>
</tr>
<tr>
<td>rttMonLatestJitterOperNumOfPositivesDS</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.18</td>
</tr>
<tr>
<td>rttMonLatestJitterOperNumOfNegativesDS</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.23</td>
</tr>
</tbody>
</table>
Configuring VoIP and Network Quality Manager

**Note:** VoIP and Network Quality Manager reads one jitter value at a given time, which is calculated based on the SNMP poll. This is an average value. The CLI command is not necessarily executed at the same moment. For this reason, the output of the current CLI commands is not the same as the values displayed in the VNQM charts or in the historical data.

**Packet Loss**

Packet loss is a quantitative measure of information loss over a given network connection. Though packet loss is inevitable in any network environment, the goal is always to identify where packets are lost in transmission so you can act to minimize information loss and maintain high QoS for your services.

VoIP and Network Quality Manager calculates packet loss in the following way:

```plaintext
if (rttMonLatestJitterOperPacketLossSD +
    rttMonLatestJitterOperPacketLossDS +
    rttMonLatestJitterOperPacketMIA <> 0)
    packetLoss =
        ((rttMonLatestJitterOperPacketLossSD +
          rttMonLatestJitterOperPacketLossDS +
          rttMonLatestJitterOperPacketMIA) * 100) /
            (rttMonLatestJitterOperPacketLossSD +
             rttMonLatestJitterOperPacketLossDS +
             rttMonLatestJitterOperPacketMIA +
             rttMonLatestJitterOperPacketLateArrival +
             rttMonLatestJitterOperPacketOutOfSequence +
             rttMonLatestJitterOperNumOfRTT)
else
    packetLoss = 0
if (rttMonLatestJitterOperPacketLossSD +
    (rttMonLatestJitterOperPacketMIA/2) +
    ((rttMonLatestJitterOperPacketLateArrival +
      rttMonLatestJitterOperPacketOutOfSequence +
      rttMonLatestJitterOperNumOfRTT)/2) <> 0)
```

41
\[
\text{packetLossSD} = \frac{(\text{rttMonLatestJitterOperPacketLossSD} + (\text{rttMonLatestJitterOperPacketMIA}/2) + ((\text{rttMonLatestJitterOperPacketLateArrival} + \text{rttMonLatestJitterOperPacketOutOfSequence} + \text{rttMonLatestJitterOperNumOfRTT}/2)) \times 100}{\text{rttMonLatestJitterOperPacketLossSD} + (\text{rttMonLatestJitterOperPacketMIA}/2)}
\]

\text{else if \ (rttMonLatestJitterOperPacketLossDS + (rttMonLatestJitterOperPacketMIA)/2 + ((rttMonLatestJitterOperPacketLateArrival + \text{rttMonLatestJitterOperPacketOutOfSequence} + \text{rttMonLatestJitterOperNumOfRTT}/2) <> 0)}

\[
\text{packetLossDS} = \frac{(\text{rttMonLatestJitterOperPacketLossDS} + (\text{rttMonLatestJitterOperPacketMIA}/2) + ((\text{rttMonLatestJitterOperPacketLateArrival} + \text{rttMonLatestJitterOperPacketOutOfSequence} + \text{rttMonLatestJitterOperNumOfRTT}/2)) \times 100}{\text{rttMonLatestJitterOperPacketLossDS} + (\text{rttMonLatestJitterOperPacketMIA}/2)}
\]

\text{else}

\text{packetLossDS} = 0

<table>
<thead>
<tr>
<th>Metric</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonLatestJitterOperPacketLossSD</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.26</td>
</tr>
<tr>
<td>rttMonLatestJitterOperPacketLossDS</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.27</td>
</tr>
<tr>
<td>rttMonLatestJitterOperPacketMIA</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.29</td>
</tr>
<tr>
<td>rttMonLatestJitterOperPacketLateArrival</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.30</td>
</tr>
<tr>
<td>rttMonLatestJitterOperPacketOutOfSequence</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.28</td>
</tr>
<tr>
<td>rttMonLatestJitterOperNumOfRTT</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.1</td>
</tr>
</tbody>
</table>
MOS is an industry standard measure of call quality expressed on a scale of increasing perceived quality, from one to five. VoIP and Network Quality Manager reports MOS as computed by a standard International Telecommunications Union (ITU) algorithm involving the codec for your VoIP network and values of latency, jitter, packet loss, and MOS advantage factor. Jitter, latency, and packet loss are variable quantities that are measured by VoIP and Network Quality Manager in real time. Generally, MOS reflects call quality as shown in the following table.

<table>
<thead>
<tr>
<th>Call quality</th>
<th>MOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very satisfied</td>
<td>4.3-5.0</td>
</tr>
<tr>
<td>Satisfied</td>
<td>4.0-4.3</td>
</tr>
<tr>
<td>Some users satisfied</td>
<td>3.6-4.0</td>
</tr>
<tr>
<td>Many users dissatisfied</td>
<td>3.1-3.6</td>
</tr>
<tr>
<td>Nearly all users dissatisfied</td>
<td>2.6-3.1</td>
</tr>
<tr>
<td>Not recommended</td>
<td>1.0-2.6</td>
</tr>
</tbody>
</table>

Both the MOS advantage factor and the codec algorithm are selected for your specific network on the VoIP and Network Quality Manager Settings page. The following table provides guidance for how the advantage factor is determined for your application.

<table>
<thead>
<tr>
<th>Communication system type examples</th>
<th>Maximum advantage factor value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conventional wired network</td>
<td>0</td>
</tr>
<tr>
<td>Wireless network within a building</td>
<td>5</td>
</tr>
<tr>
<td>Outdoor wireless network (cellular phones)</td>
<td>10</td>
</tr>
<tr>
<td>Remote communications by satellite</td>
<td>20</td>
</tr>
</tbody>
</table>
For more information about MOS calculations, see the ITU-T Recommendation G.107.

For more information about codec algorithms, see "Jitter" in the VoIP and Network Quality Manager Administrator Guide.

For more information about VoIP and Network Quality Manager settings, see "Configuring VoIP and Network Quality Manager Settings" in the VoIP and Network Quality Manager Administrator Guide.

Understanding Polling Intervals for IP SLA Operations

VNQM polls IP SLA operations at a certain frequency. This frequency is defined by polling intervals set in your database.

VoIP and Network Quality Manager divides all monitored operations on a node into groups based on their polling frequency. The polling frequency is divided by two for the polling interval, which occurs twice as fast as the polling frequency.

The polling interval groups are the following:

- Polling interval <= 1min
- 1min < Polling interval <= 3min
- 3min < Polling interval <= 6min
- 6min < Polling interval

For any given group of operations, VoIP and Network Quality Manager finds the operation with the most frequent polling interval in the group and uses that interval to poll the entire group. Consider the following example:

Five operations are being monitored on a single node. These operations have the following polling frequencies:

- Operation A: 1 minute
- Operation B: 2 minutes
- Operation C: 4 minutes
- Operation D: 5 minutes
- Operation E: 14 minutes
Operations A and B would be put in the same group because their polling intervals are both <= 1 minute. The polling interval of Operation A is 30 seconds, and the polling interval of operation B is 1 minute. VoIP and Network Quality Manager will poll both of these operations simultaneously every 30 seconds because the more frequent of the two operations is 1 minute, and VNQM polls twice that frequency.

Operations C and D are in a different group because their polling intervals are 2 minutes and 2.5 minutes, which are <= 3 minutes and greater than 1 minute. VNQM will poll both of these operations simultaneously every 2 minutes because the more frequent of the two operations is 4 minutes, and VNQM polls twice that frequency.

Operation E is in a different group because its polling interval is 7 minutes.

Notes:

- If you want to change a polling interval for an operation, you have to do it in your database.
- VNQM does not support the polling of several hundred operations at 5 second polling interval.

To check the currently set polling interval in VNQM:

1. Go to VoIP & Network Quality settings.
2. Click Edit or delete operations.
3. On the Manage IP SLA Operations page, select the appropriate operation, and then click Edit. You can check the polling interval in the read-only Frequency field.

Designating Paths

For some of the SLA operations used by VoIP and Network Quality Manager, performance statistics are collected by sending traffic over paths between sites that you define. These network paths are defined by your IP routing protocol. Because large networks can quickly become complicated, VoIP and Network Quality Manager provides an easy-to-use interface for selecting paths for monitoring. When configuring IP SLA operations, VoIP and Network Quality Manager offers the following options for establishing monitoring:
Understanding the Impact IP SLA Operations Have on Your Network

**Simple**
A simple path contains one source node and only one destination node. The path can be tested bidirectionally.

**Fully Meshed**
A Fully Meshed path configuration connects every node you define over distinct call paths to every other node selected.

**Hub and Spoke**
A Hub and Spoke call path configuration allows you to designate specific nodes as hubs. Each hub is then connected to all other nodes, with paths representing spokes.

**Custom**
The Custom call path configuration option allows you to define your own paths. All defined nodes are listed under this option, and expanding each node displays a list of all other nodes. You can use the check boxes to define paths to best suit your monitoring requirements.

**Understanding the Impact IP SLA Operations Have on Your Network**
When configured properly, IP SLA operations have a minimal impact on your overall network health. However, problems can arise when configurations force operations to be tested too frequently, or when too many overlapping operations are being performed across similar paths.

Most problems occur when using IP SLA operations on a fully meshed network. For example, in a fully meshed network with seven devices, a simple ICMP Echo operation would require 42 operations to test each link in each direction. The number of links is calculated in the following way:

- Hub-and-Spoke Links = \( N - 1 \)
- Full Mesh Links = \( \frac{N(N - 1)}{2} \)

\( N \) is the number of devices on the network. Therefore, the number of links in a seven device fully meshed network would be \( 7(7 - 1)/2 \), or \( 7(6)/2 \), or 21.

To test each link bi-directionally, twice as many operations are needed. The number of bi-directional links is found using the following calculation:

- Hub-and-Spoke Links = \( (N - 1)^2 \)
- Full Mesh Links = \( N(N - 1) \)
Therefore the total number of operations for the seven site hub-and-spoke and seven site full mesh are as follows:

Hub-and-Spoke Operations = (7 - 1)² = 12
Full Mesh Operations = 7(7 - 1) = 42

Adding three more operations to that network would increase the operations from 36 to 144 (36 x 4). 144 operations will not have a significant impact on this small network.

When looking at a typical mid-sized network with 30 devices, the number of operations begins to quickly increase, according to the following calculation:

Links = 30 x 29/2 = 435
Total Operations = 435 x 2 x 4 = 3480

The number of operations grows at an exponential rate. Here is the same arithmetic for a 180 device network:

Links = 180 x 179/2 = 16,110
Total Operations = 16,110 x 2 x 4 = 128,800

**Dangers of Overusing IP SLA Operations**

By continuing to add operations and devices to any network, especially in a fully meshed environment, overall network performance will start to degrade. In addition to burdening the network with test packets, a large number of IP SLA operations can cause the following effects:

- Several thousand test results stored every five minutes can create a large database affecting other services on the database.
- Chances are that most of the historical results will never be examined due to the large number of results to filter.
- Adding thousands of IP SLA operations could add a significant burden to the SNMP poller.

**Strategies for the Proper Use of IP SLA Operations**

IP SLA operations can negatively affect network performance when they are implemented improperly. To avoid affecting the performance of your network, use the following strategies:
Keep Local Tests Local

Not all test types are used to test WAN services (DHCP is one example). A large network may have several distributed DHCP servers. If each site has a local DHCP server, users at that site would receive IP addresses from the local server if it is available. For 40 sites you could accomplish DHCP testing by deploying an operation from the local switch or router of each site to the local DHCP server of the site. This creates only 40 tests with 40 results to poll and store every five minutes. You might also add tests for some secondary DHCP servers and have around 50 tests in total. If you added all DHCP testing to all sites to all servers you would have approximately $40^2$, or 1600 tests. Most of these tests are for DHCP requests to remote sites, which will never actually be what the users request when obtaining an IP address.

Test Paths Only for Supported Traffic

For this example, UDP jitter, a common IP SLA test, will be used. On an MPLS 40-site network, the UDP jitter operation is implemented between five sites that use UDP to deliver video conferencing. Because video conferencing is sensitive to network jitter and delay, implementing jitter operations between these sites is recommended. Using the formula for a full mesh network such as an MPLS network, we need to set up ten operations. However, if full mesh is deployed to test the links between all sites, there would be $40 \times \frac{39}{2} = 780$ tests, and only 1.3% of the tests would be for valid video paths. Therefore, a custom deployment of the operations is the recommended option in this scenario.

Consider Decreasing the Test Frequency When Possible

Decreasing or increasing the test frequency has a significant impact on the network load. For example, decreasing the test frequency from 300 seconds to 360 seconds will lessen the test impact on the source device and network by ten percent. Increasing the frequency to 150 seconds will increase the load by one hundred percent.

Avoid Overlapping Tests

It is possible to deploy a DNS test to an internal DNS server, an HTTP test to an intranet page, a ping test to the HTTP server, and a TCP connect to the HTTP server from a local switch. While there are four individual operations testing four services, there are now three redundant tests overlapping each other. The HTTP operation performs the following:
Configuring VoIP and Network Quality Manager

1. Resolves the URL to an IP address using the DNS server.
2. Performs a TCP port 80 request to the HTTP server.
3. Requests the HTTP and detects a successful page load.
4. Records the DNS resolve time, TCP open time, and page load time.
   Using the HTTP test, the other three tests can be eliminated because they yield the same results.

To prevent overloading the network with IP SLA operations, VoIP and Network Quality Manager limits the number of operations that can be created at one time to 306, or 18 nodes in a fully meshed environment.

For more detailed information about IP SLA operation configurations and deployment strategies, see the New to Networking Volume 2: The Basics of Cisco IP SLA technical reference.

**Configuring Devices for IP SLA Operations**

Cisco IP Service Level Agreements (IP SLAs) are the primary means by which VoIP and Network Quality Manager acquires information about the performance of your network. The process of configuring a device for IP SLA can involve numerous command line operations on each router. To help you easily configure your devices, VoIP and Network Quality Manager can automatically add IP SLA operations to your network devices and start monitoring those operations immediately.

**Configuring devices for ICMP echo path operations**

Devices where you want to monitor ICMP echo path operations must be manually configured. VNQM reads hop results from history data. Therefore, the operation needs to be configured to save data to the history table.

To enable history data support, configure the following items:

- History filter (all)
- Number of buckets kept (min value: 1)
- Number of samples kept (max value: 30)
- Lives of history kept (min value: 1)
To configure history data support, follow the directions based on your IOS version on the following Cisco links:

- [Configuring an ICMP Path Echo Operation with Optional Parameters on the Source Device](#)
- [Configuring and Scheduling an ICMP Path Echo Operation with Optional Parameters on the Source Device](#)
- [Setting History Characteristics](#)

To check history configuration, use one of the following commands (depending on your IOS version):

```
sh ip sla history full
sh ip sla monitor history full
sh rtr history full
```

When history is properly configured, the output resembles the following:

```
Entry number: 55
Life index: 1
Bucket index: 4
Sample index: 1
Sample time: *08:08:19.278 UTC Tue Aug 24 1993
RTT (milliseconds): 5
Response return code: OK
Target address: 10.199.254.5

Life index: 1
Bucket index: 4
Sample index: 2
Sample time: *08:08:19.286 UTC Tue Aug 24 1993
RTT (milliseconds): 1
Response return code: OK
Target address: 10.199.254.2

Life index: 1
Bucket index: 4
Sample index: 3
Sample time: *08:08:19.286 UTC Tue Aug 24 1993
RTT (milliseconds): 1
Response return code: OK
Target address: 10.199.2.3
```
Before you can start creating and monitoring IP SLA operations, you must add your IP SLA-capable routers to VoIP and Network Quality Manager.

For more information about the management information bases (MIBs) referenced by VNQM, see "MIBs Maintained by VoIP and Network Quality Manager Devices" in the VoIP and Network Quality Manager Administrator Guide.

Requirements

- Source devices must first be added to the database before you can add them to VoIP and Network Quality Manager. For more information about adding nodes, see "Adding Devices for Monitoring in the Web Console" in the SolarWinds Orion Core Administrator Guide.

- The devices must be Cisco devices and must support SNMP v2 or v3. To confirm that the Cisco IOS release for your device supports IP SLA operations, visit the Cisco Feature Navigator, click Research Features, select Search by Feature, and then select IP SLAs - DHCP Operation.

Discovering IP SLA-Capable Nodes Automatically

If you want to add more nodes at once, complete the following procedure to automatically discover and add nodes to VoIP and Network Quality Manager.

To automatically discover and add nodes to VoIP and Network Quality Manager:

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.
2. Click VoIP & Network Quality in the Modules menu bar, and then click VoIP & Quality Settings at the top right of the view.
3. Click Automatically discover IP SLA capable nodes.
4. Click Start IP SLA Discovery.
5. After the discovery has finished, click No, I want to exit this wizard, and then click Next.

Adding IP SLA-Capable Nodes Manually

If you want to add individual nodes, complete the following procedure.
To manually add nodes to VoIP and Network Quality Manager:

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.
2. Click **VoIP & Network Quality** in the Modules menu bar, and then click **VoIP & Quality Settings** at the top right of the view.
3. Click **Manually Add Nodes to VoIP and Network Quality Manager**.
4. Select the nodes you want to add to VoIP and Network Quality Manager, and then click **Add Nodes**.
5. **If you are prompted to enter credentials that include write privileges**, complete the following procedure:
   a. Click **Edit Node Details**.
   b. Click **Edit Credentials**.
6. **If SNMP v2 is used**, set the SNMP version and port number in the associated fields, type the read/write community string, and then click **Test**.
7. **If SNMP v3 is used**, select a saved credential set from the list, or type the credentials in the provided fields, and then click **Test**.
8. Click **Add Selected Nodes**.

**Configuring CLI Credentials**

Some IP SLA operations require command line interface (CLI) login credentials in order to configure the operations on your routers. Complete the following procedure to add CLI credentials to your VoIP and Network Quality Manager nodes.

To add CLI credentials to your VoIP and Network Quality Manager nodes:

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.
2. Click **VoIP & Network Quality** in the Modules menu bar, and then click **VoIP & Quality Settings** at the top right of the view.
3. Click **Manage IP SLA Nodes**.
4. Select the node you want to edit, and then click **Edit Node**.
Configuring VoIP and Network Quality Manager

5. Type the name of the credential set in the **Credentials Name** field to create a new set.
6. Type the user name and password in the associated fields.
7. Type the enable level to use when logging in.
   **Note:** The enable level must have privileges to execute configure terminal commands as well as be able to configure IP SLA operations. For information about configuring network devices, see your manufacturer’s documentation.
8. Type the password associated with the enable level to use when logging in.
9. Expand **Advanced**, and then select the protocol, port number, and connection timeout you want to use when connecting to your network devices.
10. Test the credentials, and then click **Save** when you have finished.

**Adding IP SLA Operations**

The following sections detail how to add each type of operation SolarWinds VoIP and Network Quality Manager supports. Complete the associated procedures to start monitoring your IP SLA operations.

You can either create new IP SLA operations and add them to your devices, or you can add operations existing on your devices to VNQM.

**Notes:**

- When SolarWinds VoIP and Network Quality Manager creates IP SLA operations on your network devices, the numbers used to identify the operations start at 40000. This way you can easily identify the operations created by VoIP and Network Quality Manager.
- If there are operations defined on your devices, it is strongly recommended that you back up your device settings before you start adding new operations.

**Adding DNS IP SLA Operations to Your Devices**
Domain Name Server (DNS) IP SLA operations measure the difference in time from when a DNS request is sent and when the reply is received. These operations ensure that your DNS servers are operational and are performing as expected.

**Note:** You cannot add operations that have been previously created with VoIP and Network Quality Manager. If you have already created an operation with the same operation number, you must manually remove the operation from the device.

**To add DNS IP SLA operations to your network devices:**

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.
2. Click the VoIP & Network Quality tab in the Modules menu bar, and then click **VoIP & Quality Settings** at the top right of the view.
3. Click **Add new operations** in the Manage IP SLA Operations section.
4. Select **Create new operations**, and then click **Next**.
5. Select **DNS**, and then click **Next**.
6. Select the nodes you want to add to your new DNS operations, and then click **Next**.
   
   **Note:** If you do not see your IP SLA routers in the list, you must add the devices before you can continue. For more information, see "Adding Devices for Monitoring in the Web Console" in the SolarWinds Network Performance Monitor Administrator Guide.

7. Type the IP Address of the DNS server and the hostname or IP address to resolve, and then click **Next**.
8. Type the frequency for the operation to be performed.
9. Define your warning, critical, and maximum threshold values in the associated fields.
10. **If you want to assign a Virtual Routing and Forwarding (VRF) name for this path**, expand Advanced, and then type the VRF name.

   **Note**: VRFs only exist on provider edge routers (PE). A VRF is a routing and forwarding table instance, and you can have more than one VRF per PE. The VRF includes routes that are available to a certain set of sites. A VRF is named based on the VPNs it services and on the role of the customer edge (CE) router in the topology.

11. Click **Next**.

12. **If you want to rename operations or edit any other operation properties**, select the operations you want to modify, and then click **Edit**.

13. Review the operations you want to create, and then click **Create Operations**.

   **Note**: Depending on the number of operations that are being created, this process can take several minutes to complete.

14. Click **Go to VNQM Home** to finish the procedure and return to the VoIP and Network Quality Manager home page.

**Adding FTP IP SLA Operations to Your Devices**

File Transfer Protocol (FTP) IP SLA operations measure the response time between a device and an FTP server to retrieve a file. These operations run on Cisco IP SLA capable devices, and they ensure that your FTP servers are operational and performing as expected.

**Note**: You cannot add operations that have been previously created with VoIP and Network Quality Manager. If you have already created an operation with the same operation number, you must manually remove the operation from the device.

**To add FTP IP SLA operations to your network devices:**

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.
2. Click **VoIP & Network Quality** in the Modules menu bar, and then click **VoIP & Quality Settings** at the top right of the view.
3. Click **Add new operations** in the Manage IP SLA Operations section.
4. Select **Create new operations**, and then click **Next**.
5. Select FTP, and then click **Next**.

6. Select the nodes you want to add to your new FTP operations, and then click **Next**.

   **Note:** If you do not see your IP SLA routers in the list, you must add the devices before you can continue. For more information, see "Adding Devices for Monitoring in the Web Console" in the *SolarWinds Network Performance Monitor Administrator Guide*.

7. Type the URL of the FTP server, and then click **Next**.

8. Type the frequency for the operation to be performed.

9. Define your warning, critical, and maximum threshold values in the associated fields.

10. If you want to assign a type of service (ToS) or Virtual Routing and Forwarding (VRF) name for this path, expand **Advanced**, and then type the type of service number and VRF name in the appropriate fields.

**Notes:**

- The ToS octet is a decimal value (0-255) that sets the precedence for VoIP traffic monitored with Cisco IP SLA operations. The default ToS value used by VoIP and Network Quality Manager is 184, corresponding to Expedited Forwarding (EF) per hop behavior (PHB) and a Differentiated Service Code Point (DSCP) value of 46. For more information about the ToS octet, see "Setting Traffic Precedence" in the *VoIP and Network Quality Manager Administrator Guide*.

- VRFs only exist on provider edge routers (PE). A VRF is a routing and forwarding table instance, and you can have more than one VRF per PE. The VRF includes routes that are available to a certain set of sites. A VRF is named based on the VPNs it services and on the role of the CE in the topology.

11. Click **Next**.

12. If you want to rename operations or edit any other operation properties, select the operations you want to modify, and then click **Edit**.
13. Review the operations you want to create, and then click **Create Operations**.

   **Note:** Depending on the number of operations that are being created, this process can take several minutes to complete.

14. Click **Go to VNQM Home** to finish the procedure and return to the VoIP and Network Quality Manager home page.

### Adding HTTP IP SLA Operations to Your Devices

Hypertext Transfer Protocol (HTTP) IP SLA operations measure distributed web services response times. These operations ensure that your HTTP servers are operational and performing as expected.

**Note:** You cannot add operations that have been previously created with VoIP and Network Quality Manager. If you have already created an operation with the same operation number, you must manually remove the operation from the device.

**To add HTTP IP SLA operations to your network devices:**

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.
2. Click **VoIP and Network Quality** in the Modules menu bar, and then click **VoIP & Quality Settings** at the top right of the view.
3. Click **Add new operations** in the Manage IP SLA Operations section.
4. Select **Create new operations**, and then click **Next**.
5. Select **HTTP**, and then click **Next**.
6. Select the nodes you want to add to your new HTTP operations, and then click **Next**.
   
   **Note:** If you do not see your IP SLA routers in the list, you must add the devices before you can continue. For more information, see "**Adding Devices for Monitoring in the Web Console**" in the *SolarWinds Network Performance Monitor Administrator Guide*.

7. Type the URL of the HTTP server, and then click **Next**.
8. Type the frequency for the operation to be performed.
9. Define your warning, critical, and maximum threshold values in the associated fields.

10. *If you want to assign a type of service (ToS) or Virtual Routing and Forwarding (VRF) name for this path*, expand **Advanced**, and then type the type of service number and VRF name in the appropriate fields.

**Notes:**

- The ToS octet is a decimal value (0-255) that sets the precedence for VoIP traffic monitored with Cisco IP SLA operations. The default ToS value used by VoIP and Network Quality Manager is 184, corresponding to Expedited Forwarding (EF) per hop behavior (PHB) and a Differentiated Service Code Point (DSCP) value of 46. For more information about the ToS octet, see "*Setting Traffic Precedence*" in the *VoIP and Network Quality Manager Administrator Guide*.

- VRFs only exist on provider edge routers (PE). A VRF is a routing and forwarding table instance, and you can have more than one VRF per PE. The VRF includes routes that are available to a certain set of sites. A VRF is named based on the VPNs it services and on the role of the CE in the topology.

11. Click **Next**.

12. *If you want to rename operations or edit any other operation properties*, select the operations you want to modify, and then click **Edit**.

13. Review the operations you want to create, and then click **Create Operations**.

   **Note:** Depending on the number of operations that are being created, this process can take several minutes to complete.

14. Click **Go to VNQM Home** to finish the procedure and return to the VoIP and Network Quality Manager home page.

**Adding DHCP IP SLA Operations to Your Devices**

Dynamic Host Configuration Protocol (DHCP) IP SLA operations measure the time taken to discover a DHCP server and then obtain a leased IP address from it. These operations ensure that your DHCP servers are operational and performing as expected.
Configuring VoIP and Network Quality Manager

Note: You cannot add operations that have been previously created with VoIP and Network Quality Manager. If you have already created an operation with the same operation number, you must manually remove the operation from the device.

To add DHCP IP SLA operations to your network devices:

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.
2. Click VoIP & Network Quality in the Modules menu bar, and then click VoIP & Quality Settings at the top right of the view.
3. Click Add new operations in the Manage IP SLA Operations section.
4. Select Create new operations, and then click Next.
5. Select DHCP, and then click Next.
6. Select the nodes you want to add to your new DHCP operations, and then click Next.
   
   Note: If you do not see your IP SLA routers in the list, you must add the devices before you can continue. For more information, see "Adding Devices for Monitoring in the Web Console" in the SolarWinds Network Performance Monitor Administrator Guide.

7. Type the IP address of the DHCP server to be tested, and then click Next.
8. Type the frequency for the operation to be performed.
9. Define your warning, critical, and maximum threshold values in the associated fields.
10. Click Next.
11. If you want to rename operations or edit any other operation properties, select the operations you want to modify, and then click Edit.
12. Review the operations you want to create, and then click Create Operations.
   
   Note: Depending on the number of operations that are being created, this process can take several minutes to complete.

13. Click Go to VNQM Home to finish the procedure and return to the VoIP and Network Quality Manager home page.
Adding TCP Connect IP SLA Operations to Your Devices

Transmission Control Protocol (TCP) Connect IP SLA operations measure WAN quality by testing connection times between two devices using a specific port. These operations ensure that your WAN is operational and performing as expected.

**Note:** You cannot add operations that have been previously created with VoIP and Network Quality Manager. If you have already created an operation with the same operation number, you must manually remove the operation from the device.

**To add TCP Connect IP SLA operations to your network devices:**

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.
2. Click **VoIP & Network Quality** in the Modules menu bar, and then click **VoIP & Quality Settings** at the top right of the view.
3. Click **Add new operations** in the Manage IP SLA Operations section.
4. Select **Create new operations**, and then click **Next**.
5. Select **TCP Connect**, and then click **Next**.
6. Select the type of path your network is configured to use. For more information, see "Designating Paths" in the VoIP and Network Quality Manager Administrator Guide.
7. Select the source nodes you want to add to your new TCP Connect operation, and then click **Next**.
   **Note:** If you do not see your IP SLA routers in the list, you must add the devices before you can continue. For more information, see "Adding Devices for Monitoring in the Web Console" in the SolarWinds Network Performance Monitor Administrator Guide.
8. Select the target nodes you want to add to your new TCP Connect operation.
9. If you want to create the path in only one direction, select **No, create the path in just one direction**.
10. If you want to specify an external node as a target, complete the following procedure.
   
a. Click **Yes, use external node as a target**.
   
b. Type the IP address or host name of the external node you want to add.
   
   **Note:** If you use a host name, the source node of the operation must be able to successfully resolve the host name.

11. Click **Next**.

12. Type the frequency for the operation to be performed.

13. Type the port number to be used in the test in the **Port Number** field.

14. Define your warning, critical, and maximum threshold values in the associated fields.

15. If you want to assign a type of service (ToS), Virtual Routing and Forwarding (VRF) name for this path, or enable the target node to act as a controller, expand **Advanced**, and then type the type of service number or VRF name in the appropriate fields, or select **Control enable**.

   **Notes:**
   
   - The ToS octet is a decimal value (0-255) that sets the precedence for VoIP traffic monitored with Cisco IP SLA operations. The default ToS value used by VoIP and Network Quality Manager is 184, corresponding to Expedited Forwarding (EF) per hop behavior (PHB) and a Differentiated Service Code Point (DSCP) value of 46. For more information about the ToS octet, see "Setting Traffic Precedence" in the **VoIP and Network Quality Manager Administrator Guide**.
   
   - VRFs only exist on provider edge routers (PE). A VRF is a routing and forwarding table instance, and you can have more than one VRF per PE. The VRF includes routes that are available to a certain set of sites. A VRF is named based on the VPNs it services and on the role of the CE in the topology.

16. Click **Next**.

17. If you want to rename operations or edit any other operation properties, select the operations you want to modify, and then click **Edit**.
18. Review the operations you want to create, and then click **Create Operations**.

   **Note:** Depending on the number of operations that are being created, this process can take several minutes to complete.

19. Click **Go to VNQM Home** to finish the procedure and return to the VoIP and Network Quality Manager home page.

### Adding UDP Jitter IP SLA Operations to Your Devices

User Datagram Protocol (UDP) Jitter IP SLA operations measure WAN quality by testing connection times between two devices using a specific port number. These operations ensure that your WAN is operational and performing as expected.

**Note:** You cannot add operations that have been previously created with VoIP and Network Quality Manager. If you have already created an operation with the same operation number, you must manually remove the operation from the device.

**To add UDP Jitter IP SLA operations to your network devices:**

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.

2. Click **VoIP & Network Quality** in the Modules menu bar, and then click **VoIP & Quality Settings** at the top right of the view.

3. Click **Add new operations** in the Manage IP SLA Operations section.

4. Select **Create new operations**, and then click **Next**.

5. Select **UDP Jitter**, and then click **Next**.

6. Select the type of path your network is configured to use. For more information, see "**Designating Paths**" in the *VoIP and Network Quality Manager Administrator Guide*.

7. Select the source nodes you want to add to your new UDP Jitter operations, and then click **Next**.

   **Note:** If you do not see your IP SLA routers in the list, you must add the devices before you can continue. For more information, see "**Adding Devices for Monitoring in the Web Console**" in the *SolarWinds Network Performance Monitor Administrator Guide*.
8. Select the target nodes you want to add to your new UDP Jitter operation.

9. If you want to create the path in only one direction, select **No, create the path in just one direction**.

10. **If you want to specify an external node as a target**, complete the following procedure.
   
   a. Click **Yes, use external node as a target**.
   
   b. Type the IP address or host name of the external node you want to add.
   
   **Note**: If you are using a host name, the source node of the operation must be able to successfully resolve the host name.

11. Type the frequency for the operation to be performed.

12. Type the port number to be used in the test in the **Port Number** field.

13. Define your warning, critical, and maximum threshold values in the associated fields.

14. **If you want to assign a type of service (ToS) or Virtual Routing and Forwarding (VRF) name for this path**, expand **Advanced**, and then type the type of service number and VRF name in the appropriate fields.

**Notes:**

- The ToS octet is a decimal value (0-255) that sets the precedence for VoIP traffic monitored with Cisco IP SLA operations. The default ToS value used by VoIP and Network Quality Manager is 184, corresponding to Expedited Forwarding (EF) per hop behavior (PHB) and a Differentiated Service Code Point (DSCP) value of 46. For more information about the ToS octet, see "Setting Traffic Precedence" in the *VoIP and Network Quality Manager Administrator Guide*.

- VRFs only exist on provider edge routers (PE). A VRF is a routing and forwarding table instance, and you can have more than one VRF per PE. The VRF includes routes that are available to a certain set of sites. A VRF is named based on the VPNs it services and on the role of the CE in the topology.

15. Click **Next**.
16. **If you want to rename operations or edit any other operation properties**, select the operations you want to modify, and then click **Edit**.

17. Review the operations you want to create, and then click **Create Operations**.

   **Note:** Depending on the number of operations that are being created, this process can take several minutes to complete.

18. Click **Go VNQM Home** to finish the procedure and return to the VoIP and Network Quality Manager home page.

---

**Adding VoIP UDP Jitter IP SLA Operations to Your Devices**

VoIP UDP Jitter IP SLA operations measure call path metrics on your VoIP network. These operations ensure that your VoIP network is operational and performing as expected.

**Note:** You cannot add operations that have been previously created with VoIP and Network Quality Manager. If you have already created an operation with the same operation number, you must manually remove the operation from the device.

**To add VoIP UDP Jitter IP SLA operations to your network devices:**

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.

2. Click **VoIP & Network Quality** in the Modules menu bar, and then click **VoIP & Quality Settings** at the top right of the view.

3. Click **Add new operations** in the Manage IP SLA Operations section.

4. Select **Create new operations**, and then click **Next**.

5. Select **VoIP UDP Jitter**, and then click **Next**.

6. Select the type of path your network is configured to use. For more information, see "**Designating Paths**" in the **VoIP and Network Quality Manager Administrator Guide**.
7. Select the source nodes you want to add to your new VoIP UDP Jitter operation, and then click **Next**.
   
   **Note**: If you do not see your IP SLA routers in the list, you must add the devices before you can continue. For more information, see "Adding Devices for Monitoring in the Web Console" in the *SolarWinds Network Performance Monitor Administrator Guide*.

8. Select the target nodes you want to add to your new VoIP UDP Jitter operation.

9. **If you want to create the path in only one direction**, select **No, create the path in just one direction**.

10. **If you want to specify an external node as a target**, complete the following procedure.

    a. Click **Yes, use external node as a target**.
    
    b. Type the IP address or host name of the external node you want to add.

    **Note**: If you use a host name, the source node of the operation must be able to successfully resolve the host name.

11. Type the frequency for the operation to be performed.

12. Type the port number to be used in the test in the **Port Number** field.

13. Define your warning, critical, and maximum threshold values in the associated fields.
14. If you want to assign a codec, type of service (ToS), or Virtual Routing and Forwarding (VRF) name for this path, expand Advanced, select the codec, and then type the type of service number and VRF name in the appropriate fields. For more information about codec algorithms, see "Jitter" in the VoIP and Network Quality Manager Administrator Guide.

Notes:

- The ToS octet is a decimal value (0-255) that sets the precedence for VoIP traffic monitored with Cisco IP SLA operations. The default ToS value used by VoIP and Network Quality Manager is 184, corresponding to Expedited Forwarding (EF) per hop behavior (PHB) and a Differentiated Service Code Point (DSCP) value of 46. For more information about the ToS octet, see "Setting Traffic Precedence" in the VoIP and Network Quality Manager Administrator Guide.

- VRFs only exist on provider edge routers (PE). A VRF is a routing and forwarding table instance, and you can have more than one VRF per PE. The VRF includes routes that are available to a certain set of sites. A VRF is named based on the VPNs it services and on the role of the CE in the topology.

15. Click Next.

16. If you want to rename operations or edit any other operation properties, select the operations you want to modify, and then click Edit.

17. Review the operations you want to create, and then click Create Operations.

   Note: Depending on the number of operations that are being created, this process can take several minutes to complete.

18. Click Go to VNQM Home to finish the procedure and return to the VoIP and Network Quality Manager home page.

Adding ICMP Echo IP SLA Operations to Your Devices

Internet Control Message Protocol (ICMP) Echo IP SLA operations measure round trip time between nodes on your network. These operations ensure that your network devices are operational and performing as expected.

Notes:
You may need to configure your device to successfully use ICMP Echo operations. For more information, see "Configuring CLI Credentials" in the VoIP and Network Quality Manager Administrator Guide.

You cannot add operations that have been previously created with VoIP and Network Quality Manager. If you have already created an operation with the same operation number, you must manually remove the operation from the device.

To add ICMP Echo IP SLA operations to your network devices:

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.
2. Click VoIP & Network Quality in the Modules menu bar, and then click VoIP & Quality Settings at the top right of the view.
3. Click Add new operations in the Manage IP SLA Operations section.
4. Select Create new operations, and then click Next.
5. Select ICMP Echo, and then click Next.
6. Select the type of path your network is configured to use. For more information, see "Designating Paths" in the VoIP and Network Quality Manager Administrator Guide.
7. Select the source nodes you want to add to your new ICMP Echo operation, and then click Next.
   
   **Note:** If you do not see your IP SLA routers in the list, you must add the devices before you can continue. For more information, see "Adding Devices for Monitoring in the Web Console" in the SolarWinds Network Performance Monitor Administrator Guide.

8. Select the target nodes you want to add to your new ICMP Echo operation.
9. If you want to create the path in only one direction, select No, create the path in just one direction.
10. If you want to specify an external node as target, complete the following procedure.
   a. Click **Yes, use external node as a target**.
   b. Type the IP address or host name of the external node you want to add.
      
      **Note**: If you use a host name, the source node of the operation must be able to successfully resolve the host name.

11. Click **Next**.

12. Type the frequency for the operation to be performed.

13. Define your warning, critical, and maximum threshold values in the associated fields.

14. If you want to assign a type of service (ToS) or Virtual Routing and Forwarding (VRF) name for this path, expand **Advanced**, and then type the type of service number and VRF name in the appropriate fields.

   **Notes**:
   
   - The ToS octet is a decimal value (0-255) that sets the precedence for VoIP traffic monitored with Cisco IP SLA operations. The default ToS value used by VoIP and Network Quality Manager is 184, corresponding to Expedited Forwarding (EF) per hop behavior (PHB) and a Differentiated Service Code Point (DSCP) value of 46. For more information about the ToS octet, see "Setting Traffic Precedence" in the VoIP and Network Quality Manager Administrator Guide.
   
   - VRFs only exist on provider edge routers (PE). A VRF is a routing and forwarding table instance, and you can have more than one VRF per PE. The VRF includes routes that are available to a certain set of sites. A VRF is named based on the VPNs it services and on the role of the CE in the topology.

15. Click **Next**.

16. If you want to rename operations or edit any other operation properties, select the operations you want to modify, and then click **Edit**.
17. Review the operations you want to create, and then click **Create Operations**.
   
   **Note:** Depending on the number of operations that are being created, this process can take several minutes to complete.

18. Click **Go to VNQM Home** to finish the procedure and return to the VoIP and Network Quality Manager home page.

**Adding UDP Echo IP SLA Operations to Your Devices**

UDP Echo IP SLA operations measure round trip time between nodes on your network. These operations ensure that your network devices are operational and performing as expected.

**Note:** You cannot add operations that have been previously created with VoIP and Network Quality Manager. If you have already created an operation with the same operation number, you must manually remove the operation from the device.

**To add UDP Echo IP SLA operations to your network devices:**

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.
2. Click **VoIP & Network Quality** in the Modules menu bar, and then click **VoIP & Quality Settings** at the top right of the view.
3. Click **Add new operations** in the Manage IP SLA Operations section.
4. Select **Create new operations**, and then click **Next**.
5. Select **UDP Echo**, and then click **Next**.
6. Select the type of path your network is configured to use. For more information, see "Designating Paths" in the *VoIP and Network Quality Manager Administrator Guide*.
7. Select the source nodes you want to add to your new UDP Echo operation.
   
   **Note:** If you do not see your IP SLA routers in the list, you must add the devices before you can continue. For more information, see "Adding Devices for Monitoring in the Web Console" in the *SolarWinds Network Performance Monitor Administrator Guide*. 
8. Select the target nodes you want to add to your new UDP Echo operation.

9. If you want to create the path in only one direction, select No, create the path in just one direction.

10. If you want to specify an external node as a target, complete the following procedure.
   a. Click Yes, use external node as a target.
   b. Type the IP address or host name of the external node you want to add.
      
      Note: If you use a host name, the source node of the operation must be able to successfully resolve the host name.

11. Click Next.

12. Type the frequency for the operation to be performed.

13. Type the port number to be used in the test.

14. Define your warning and critical threshold values in the associated fields.

15. If you want to assign a type of service (ToS) or Virtual Routing and Forwarding (VRF) name for this path or enable the target node to act as a controller, expand Advanced, and then type the type of service number or VRF name in the appropriate fields or select Control enable.

Notes:

- The ToS octet is a decimal value (0-255) that sets the precedence for VoIP traffic monitored with Cisco IP SLA operations. The default ToS value used by VoIP and Network Quality Manager is 184, corresponding to Expedited Forwarding (EF) per hop behavior (PHB) and a Differentiated Service Code Point (DSCP) value of 46. For more information about the ToS octet, see "Setting Traffic Precedence" in the VoIP and Network Quality Manager Administrator Guide.

- VRFs only exist on provider edge routers (PE). A VRF is a routing and forwarding table instance, and you can have more than one VRF per PE. The VRF includes routes that are available to a certain set of sites. A VRF is named based on the VPNs it services and on the role of the CE in the topology.
16. Click **Next**.

17. **If you want to rename operations or edit any other operation properties**, select the operations you want to modify, and then click **Edit**.

18. Review the operations you want to create, and then click **Create Operations**.

   **Note:** Depending on the number of operations that are being created, this process can take several minutes to complete.

19. Click **Go to VNQM Home** to finish the procedure and return to the VoIP and Network Quality Manager home page.

**Adding ICMP Path Echo Operations to Your Devices**

ICMP Path Echo IP SLA operations measure round trip time between each node on a designated path on your network. Round trip time is measured hop-by-hop. These operations ensure that your network devices are operational and performing as expected.

**Notes:**

- To add ICMP Path Echo operations, you must add CLI login credentials to your source node. For more information, see "**Configuring CLI Credentials**" in the *VoIP and Network Quality Manager Administrator Guide*.

- You cannot add operations that have been previously created with VoIP and Network Quality Manager. If you have already created an operation with the same operation number, you must manually remove the operation from the device.

**To add ICMP Path Echo IP SLA operations to your network devices:**

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.

2. Click **VoIP & Network Quality** in the Modules menu bar, and then click **VoIP & Quality Settings** at the top right of the view.

3. Click **Add new operations** in the Manage IP SLA Operations section.

4. Select **Create new operations**, and then click **Next**.

5. Select **ICMP Path Echo**, and then click **Next**.
6. Select the type of path your network is configured to use. For more information, see "Designating Paths" in the VoIP and Network Quality Manager Administrator Guide.

7. Select the source node you want to use for your ICMP Path Echo operation.
   **Note:** If you do not see your IP SLA routers in the list, you must add the devices before you can continue. For more information, see "Adding Devices for Monitoring in the Web Console" in the SolarWinds Network Performance Monitor Administrator Guide.

8. **If the target node is being monitored**, select it from the list.

9. **If you want to create the path in only one direction**, select No, create the path in just one direction.

10. **If you want to specify an external node as a target**, complete the following procedure.
    a. Click Yes, use external node as a target.
    b. Type the IP address or host name of the external node you want to add.
       **Note:** If you use a host name, the source node of the operation must be able to successfully resolve the host name.

11. Click Next.

12. Type the frequency for the operation to be performed.

13. Define your warning and critical threshold values in the associated fields.
14. If you want to assign a type of service (ToS) or Virtual Routing and Forwarding (VRF) name for this path, expand **Advanced**, and then type the type of service number and VRF name in the appropriate fields.

**Notes:**

- The ToS octet is a decimal value (0-255) that sets the precedence for VoIP traffic monitored with Cisco IP SLA operations. The default ToS value used by VoIP and Network Quality Manager is 184, corresponding to Expedited Forwarding (EF) per hop behavior (PHB) and a Differentiated Service Code Point (DSCP) value of 46. For more information about the ToS octet, see "Setting Traffic Precedence" in the *VoIP and Network Quality Manager Administrator Guide*.

- VRFs only exist on provider edge routers (PE). A VRF is a routing and forwarding table instance, and you can have more than one VRF per PE. The VRF includes routes that are available to a certain set of sites. A VRF is named based on the VPNs it services and on the role of the CE in the topology.

15. Click **Next**.

16. If you want to rename operations or edit any other operation properties, select the operations you want to modify, and then click **Edit**.

17. Review the operations you want to create, and then click **Create Operations**.

**Note:** Depending on the number of operations that are being created, this process can take several minutes to complete.

18. Click **Go to VNQM Home** to finish the procedure and return to the VoIP and Network Quality Manager home page.

**Adding ICMP Path Jitter Operations to Your Devices**

ICMP Path Jitter IP SLA operations take call path measurements between each node on a designated path on your VoIP network. Round trip time is measured hop-by-hop. These operations ensure that your VoIP network is operational and performing as expected.

**Notes:**
To add ICMP Path Jitter operations, you must add CLI login credentials to your source node. For more information, see "Configuring CLI Credentials" in the VoIP and Network Quality Manager Administrator Guide.

You cannot add operations that have been previously created with VoIP and Network Quality Manager. If you have already created an operation with the same operation number, you must manually remove the operation from the device.

To add ICMP Path Jitter IP SLA operations to your network devices:

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.
2. Click VoIP & Network Quality in the Modules menu bar, and then click VoIP & Quality Settings at the top right of the view.
3. Click Add new operations in the Manage IP SLA Operations section.
4. Select Create new operations, and then click Next.
5. Select ICMP Path Jitter, and then click Next.
6. Select the type of path your network is configured to use. For more information, see "Designating Paths" in the VoIP and Network Quality Manager Administrator Guide.
7. Select the source node you want to use for your ICMP Path Jitter operation, and then click Next.
   
   **Note:** If you do not see your IP SLA routers in the list, you must add the devices before you can continue. For more information, see "Adding Devices for Monitoring in the Web Console" in the SolarWinds Network Performance Monitor Administrator Guide.
8. If the target node is being monitored, select it from the list.
9. If you want to create the path in only one direction, select No, create the path in just one direction.
10. If you want to specify an external node as a target, complete the following procedure.
   a. Click Yes, use external node as a target.
   b. Type the IP address or host name of the external node you want to add.
      
      Note: If you use a host name, the source node of the operation must be able to successfully resolve the host name.

11. Click Next.

12. Type the frequency for the operation to be performed.

13. Define your warning, critical, and maximum threshold values in the associated fields.

14. If you want to assign a type of service (ToS) or Virtual Routing and Forwarding (VRF) name for this path, expand Advanced, and then type the type of service number and VRF name in the appropriate fields.

   Notes:
   
   - The ToS octet is a decimal value (0-255) that sets the precedence for VoIP traffic monitored with Cisco IP SLA operations. The default ToS value used by VoIP and Network Quality Manager is 184, corresponding to Expedited Forwarding (EF) per hop behavior (PHB) and a Differentiated Service Code Point (DSCP) value of 46. For more information about the ToS octet, see "Setting Traffic Precedence" in the VoIP and Network Quality Manager Administrator Guide.
   
   - VRFs only exist on provider edge routers (PE). A VRF is a routing and forwarding table instance, and you can have more than one VRF per PE. The VRF includes routes that are available to a certain set of sites. A VRF is named based on the VPNs it services and on the role of the CE in the topology.

15. Click Next.

16. If you want to rename operations or edit any other operation properties, select the operations you want to modify, and then click Edit.
Adding Existing Operations to VoIP and Network Quality Manager

17. Review the operations you want to create, and then click Create Operations.
   **Note:** Depending on the number of operations that are being created, this process can take several minutes to complete.

18. Click Go to VNQM Home to finish the procedure and return to the VoIP and Network Quality Manager home page.

Adding Existing Operations to VoIP and Network Quality Manager

With VoIP and Network Quality Manager you can monitor operations that are already configured on a device. To do so, add these operations to VNQM.

**To add an operation configured on your device to VNQM:**

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.

2. Click VoIP & Network Quality in the Modules menu bar, and then click VoIP & Quality Settings at the top right of the view.

3. Click Add new operations in the Manage IP SLA Operations section.

4. Select Monitor existing operations, and then click Next.

5. **If you want to automatically discover operations on your nodes,**
   complete the following procedure.
   a. Select Automatically discover existing operations, and then click Next.
   b. Select the node where the operation you want to monitor resides, and then click Next.
      **Note:** If you have not entered valid CLI credentials for the selected node, you may be prompted to enter credentials. You do not have to provide credentials to the node.
   c. Select the operation you want to monitor, and then click Monitor Operations.
6. **If you want to manually enter the operation numbers**, expand **Advanced**, and then complete the following procedure.

   a. Select **Manually enter operation numbers**, and then click **Next**.
   b. Select the node where the operation you want to monitor resides, and then click **Next**.
   
   **Note:** If you have not entered valid CLI credentials for the selected node, you may be prompted to enter credentials. You do not have to provide credentials to the node.

   c. Enter the operation number, and then click **Next**.
   d. Select the operation you want to monitor, and then click **Monitor Operations**.

7. Click **Go to VNQM Home** to finish the procedure and return to the VoIP and Network Quality Manager home page.

**Editing IP SLA Operations**

The following sections provide more details about editing IP SLA operations monitored by VoIP and Network Quality Manager:

- **Modifying the SLA Location**
- **Renaming Operations in VNQM**

**Note:** Modifying operations created with VNQM is possible only by using VNQM. If you modify an operation created by VNQM directly on the device, the changes will be overwritten by the IP SLA operation settings from VNQM.

**Modifying the SLA Location**

You can add or modify location information for any IP SLA operation by completing the following procedure.

**To edit the SLA location:**

1. Click **VoIP & Network Quality** in the Modules menu bar, and then click **VoIP & Quality Settings** at the top right of the view.
2. Click **Edit or delete operations** in the Manage IP SLA Operations section.
3. Select the operation you want to modify, and then click **Add/Edit SLA Location**.
4. Select the Origin Location or Cisco CallManager ID.
5. Select the Target Location or Cisco CallManager ID.
6. Click **Save**.

**Renaming Operations in VoIP and Network Quality Manager**

Any operation that VoIP and Network Quality Manager monitors is given a default name using the following pattern: SourceNodeName -> TargetNodeName, where SourceNodeName is the name of the source node and TargetNodeName is the name of the target node. To change the name of an operation, complete the following procedure.

**To rename an operation:**

1. Click **VoIP & Network Quality** in the Modules menu bar, and then click **VoIP & Quality Settings** at the top right of the view.
2. Click **Edit or delete operations** in the Manage IP SLA Operations section.
3. Select the operation you want to modify, and then click **Edit**.
4. Type the new name for the operation in the **Operation Name** field, and then click **Save**.

**Notes:**

- Leaving the **Operation Name** field blank results in the operation being named using the default naming pattern.
- *If you change the name of a node in NPM*, the change will be reflected in the operation name unless the default naming pattern is not being used.

**Deleting IP SLA Operations from VoIP and Network Quality Manager**

If you decide to stop monitoring specific IP SLA operations in VoIP and Network Quality Manager, complete the following procedure.
Configuring VoIP and Network Quality Manager

**Note:** Deleting manually added IP SLA operations from VoIP and Network Quality Manager only removes the operations from the list of monitored operations. The operations will still exist on your network devices. You must manually remove operations from your devices to completely remove the operations. If you do not remove the operations, you will not be able to add other operations with the same number.

**To delete IP SLA Operations from VoIP and Network Quality Manager:**

1. Log on to your SolarWinds VoIP and Network Quality Manager server using an account with administrator privileges.
2. Click **VoIP & Network Quality** in the Modules menu bar, and then click **VoIP & Quality Settings** at the top right of the view.
3. Click **Edit or delete operations** in the Manage IP SLA Operations section.
4. Select the operations you want to delete, and then click **Delete**.
5. When prompted to confirm, click **Delete** to stop monitoring the selected operations.

**VoIP Management**

In VoIP and Network Quality Manager you can monitor your call managers, VoIP gateways and define your VoIP infrastructure for a quick overview in the VoIP Infrastructure resource.

To configure your devices for monitoring in VNQM, complete the following steps:

1. Add the devices to your database. For more information, see "Adding Devices for Monitoring in the Web Console" in the SolarWinds Orion Core Administrator Guide.
2. Add the devices to VNQM for monitoring.

- If you want to monitor VoIP calls on your devices, add them as call managers. For more information, see "Managing Call Managers" in the VoIP and Network Quality Manager Administrator Guide.
If you want to monitor the PRI trunk utilization of your devices, add them as gateways. For more information, see "Managing Gateways" in the VoIP and Network Quality Manager Administrator Guide.

VNQM also provides an overview of your VoIP infrastructure monitored by VNQM. For more information about configuring this resource, see "Selecting VoIP Infrastructure" in the VoIP and Network Quality Manager Administrator Guide.

Managing Call Managers

Call Manager devices are managed on the Manage Call Manager Nodes page.

The Manage Call Manager Nodes page provides a list of Cisco CallManager, CallManager Express, and Avaya Communication and Media Server devices that are currently monitored by VNQM.

**Note:** Call managers from manufacturers other than Cisco and Avaya can be monitored with VoIP and Network Quality Manager if you use a custom management information base (MIB) poller specifically configured for your call manager from other manufacturers. You cannot monitor call manager specific data, such as VoIP phones, region information, or call data. For more information, see "Adding Call Manager Devices from Other Manufacturers".

To access the Manage Call Manager Nodes page:

1. Log in to the Orion Web Console as an administrator.
2. Select the VoIP and Network Quality tab, and then click **VoIP & Quality Settings** in the top right of the page.
3. Click **Manage CallManager Nodes**.

**CLI Credentials**

Command line interface (CLI) credentials are used to log in to any device, such as a call manager, a gateway, a router, and so on, that accepts commands through a command line interface. You can provide text input through the command line, and receive text output after the execution of the command. For more information about CLI credentials and their usage, see "Configuring CLI Credentials".
Configuring VoIP and Network Quality Manager

The CLI credentials are also used for logging in to Avaya Call Managers. For more information, see "Adding Avaya Call Manager Devices".

Credentials Used for Cisco CallManager

To exercise the full benefits of monitoring Cisco CallManager devices, you can provide AXL credentials and FTP credentials to the CDR/CMR data. By downloading CDR/CMR data from CallManager devices, VoIP and Network Quality Manager can track the region information of each call made through your monitored Cisco CallManager device.

AXL refers to the Administration XML API of Cisco, which provides a mechanism to receive and modify data in the database of the call manager. VoIP and Network Quality Manager queries the database for region information. No information is modified in the database. You can create a read only AXL account specifically for VoIP and Network Quality Manager.

**Note:** To monitor CDR/CMR data, perform the following tasks to both publisher and subscriber Cisco CallManager Devices.

1. Configure the Cisco CallManager to monitor calls. For more information, see "Configuring Cisco CallManagers for FTP".
2. Enable the AXL API. For more information, see the online tutorial "Enable AXL on CUCM."
3. Create an AXL account. For more information, see the online tutorial "Enable AXL on CUCM."

Monitoring Call Manager Health

VoIP and Network Quality Manager references the Cisco Management Information Base (MIB) CISCO-CCM-MIB to provide out-of-the-box monitoring capability for Cisco CallManager and CallManager Express devices.

You can also monitor Avaya Communication and Media Server devices with VoIP and Network Quality Manager. VNQM intercepts the CDR packets sent by the TCP protocol, as well as the RTCP data sent through UDP, and based on these data, it provides information about the call details and the call quality.

**Note:** If you want to track the performance of call managers from other manufacturers, you can use universal device pollers in connection with SolarWinds Network Performance Monitor. For more information, see "Monitoring MIBs with Universal Device Pollers" in the *SolarWinds Network Performance Monitor Administrator Guide*. 

81
Adding Cisco CallManager Devices to VoIP and Network Quality Manager

After a call manager device has been added to the database for management, you can use the intuitive interface of VoIP and Network Quality Manager to track and report call-processing performance statistics for your VoIP network.

Only Cisco CallManager, CallManager Express, and Avaya Communication and Media Server devices can be added to VoIP and Network Quality Manager as CallManager nodes. Call management devices from other manufacturers can only be monitored as a part of your VoIP infrastructure. For more information about adding call management devices from other manufacturers than Cisco and Avaya, see "Adding Call Manager Devices from Other Manufacturers" in the VoIP and Network Quality Manager Administrator Guide.

**Note:** Cisco CallManager, CallManager Express, and Avaya Communication and Media Server devices provide a different level of details:

- For Cisco CallManagers, you can see all information from the device Call Detail Records, such as the call source, destination, duration, or the call quality indicators.
- For Cisco CallManager Express devices, the information about CDR is not available, thus giving you only the details about the device status and its phone devices count.
- For Avaya Communication and Media Server devices, you can see information such as the call source, destination, duration, and certain call quality indicators.

**Adding Cisco CallManager Devices to VoIP and Network Quality Manager**

The following procedure adds a Cisco CallManager device to VoIP and Network Quality Manager.

**Note:** Avaya Call Managers can also be monitored with VoIP and Network Quality Manager. For more information about monitoring Avaya Call Managers, see "Managing Avaya Call Managers". Call managers from manufacturers other than Cisco and Avaya can be monitored with VoIP and Network Quality Manager if you use a custom management information base (MIB) poller specifically configured for your call manager from other manufacturers. You cannot monitor call manager specific data, such as VoIP phones, region information, or call data. For more information, see "Adding Call Manager Devices from Other Manufacturers" in the VoIP and Network Quality Manager Administrator Guide.
To add a Cisco CallManager device to VoIP and Network Quality Manager:

1. Log in to the Orion Web Console as an administrator.
2. Select the VoIP and Network Quality tab, and then click VoIP & Quality Settings in the top right of the page.
3. Click Add CallManager nodes.
4. Select an available CallManager-hosting device, and then click Next.
   **Note:** If you do not see an expected CallManager device, use the Web Console to add it. You may need to enable SNMP on the CallManager device.
5. Decide whether you want to collect information about calls on this call manager.
   - **If you want to collect information about calls on this call manager**, select Enable CDR/CMR polling for this Call Manager, and then click Next.
   - **If you do not want to collect call information from this call manager**, select Add Call Manager without CDR/CMR monitoring, click Next, and then click Add Call Manager.
6. Define your AXL credentials by either selecting an existing credential set from the Select AXL credentials list or by creating a new set.
   
   To create a new set, complete the following procedure:
   
   a. Type a name in Select AXL credentials.
   b. Type the user name in AXL Username.
   c. Type the password in AXL Password.
   **Notes:**
   - Enter AXL credentials for both publisher and subscriber call managers.
   - AXL credentials must be accurate. VoIP and Network Quality Manager tests the credentials before continuing to the next step.
Adding Cisco CallManager Devices to VoIP and Network Quality Manager

7. Click **Next**.
8. Define the FTP server details.
   a. Type the **FTP server** IP address or host name where your CDR/CMR data is stored. For more information about FTP configuration, see "Configuring Cisco CallManagers for FTP".
   b. Enter the **FTP port number**.
   c. Select **Passive mode** to connect to the FTP server in passive mode.
   d. **If you connect to an SFTP site**, select **Secure connection**.
   e. Enter the CDR/CMR file path if applicable.
   f. Enter your FTP credentials by either selecting an existing credential set from the **Select FTP credentials** list or by creating a new set.
      To create a new set, complete the following procedure.
      - Type a name in **Select FTP credentials**.
      - Type the user name in **FTP Username**.
      - Type the password in **FTP Password**.
      - Click **Test FTP server connection** to test the credentials.
   g. Type a number in **Polling Frequency** between 1 and 60 to configure how frequently you want to poll the FTP server in minutes.
   h. Select **Delete CDR/CMR files from FTP server after download** if you want to remove the files from the FTP server.
      **Warning**: Deleting CDR/CMR files from the FTP server may cause serious data loss. Ensure that your backups are running successfully before selecting this option.
      **Note**: Removing the files from the FTP server is advisable to prevent the device from filling up on logs, or in the case when you want to speed up data collection from the FTP server.
   i. Click **Next**.
9. Review the information, and then click **Add Call Manager**, or click **Back** to make changes.

**Adding CallManager Express Devices to VoIP and Network Quality Manager**

The following procedure adds a Cisco CallManager Express device to VoIP and Network Quality Manager.

**Note:** VoIP and Network Quality Manager does not collect call data information or region information from CallManager Express devices and does not support phone polling on the devices.

To add a CallManager Express device to VoIP and Network Quality Manager:

1. Log in to the Orion Web Console as an administrator.
2. Select the VoIP and Network Quality tab, and then click **VoIP & Quality Settings** in the top right of the page.
3. Click **Add new CallManager nodes**.
4. **If you have not already added your CallManager devices to the database,** use the Web Console to add your CallManager devices before continuing.
5. Select an available CallManager Express device, and then click **Next**.
   **Note:** If you do not see an expected CallManager Express device, use the Web Console to add it.
6. Click **Next**.
7. Review the information, and then click **Add Call Manager**, or click **Back** to make changes.

**Managing Avaya Call Managers**

To exercise the full benefits of monitoring an Avaya Call Manager, the device must be configured to emit CDRs and quality data.

In order to collect Avaya data in VNQM, the Avaya user must have sufficient permissions to execute the following commands:
to set up an Avaya call manager to emit CDR and quality data.

- **list station**: to display a list of phone devices.
- **list media-gateway**: to display a list of gateways.
- **list ip-network-region monitor**: to display a list of regions.
- **status station**: to display the details of phones, including status information.
- **display station [x]**, where [x] is the extension number of the phone: to display the details of phones. The extension number of the phone can be obtained by using the list station command.
- **display media-gateway [y]**, where [y] is the gateway number: to display the details of gateways. The gateway number can be obtained by using the list media-gateway command.

**To set up an Avaya Call Manager to emit CDRs:**

1. Log on to the Avaya Call Manager using PuTTY, TuTTY, or Avaya Manager.
2. Type **change system-parameters cdr**, and then press F3.
3. Set the **Primary Output Format** to customized.
4. Set the **Primary Output Endpoint** to CDR1, and then press F7 to navigate to the next page.

   **Note:** If the Primary Output is already in use, you can use the Secondary Output for these settings.

![CDR System Parameters](image)

5. Define the customized CDR format according to the details in the following illustration, and then press F3 to save your changes.

   **Note:** Instead of the calling-num parameter, you can also use the clg-num/in-tac parameter.

![CDR System Parameters](image)
6. Type `change node-names ip`, and then press F3.

7. Type a name for VNQM. The name can be any name you choose.

8. Type the IP address of the VNQM main or additional poller in the **IP Address** column, and then press F3 to save your changes.
9. Type \texttt{change ip-services}, press \texttt{F3}, and then define the following settings:
   - Service Type: \texttt{CDR1}
   - Local Node: \texttt{procr}
   - Remote Node: \texttt{[vnqm]} where \texttt{[vnqm]} is the name you specified in Step 7.
   - Remote Port: \texttt{50000}

10. Press \texttt{F7} to navigate to the next page.
11. Set the **Reliable Protocol** to \( n \), and then press F3.

![Image of Avaya Call Manager settings](image)

**Note:** After changing a setting, press F3 to save it, or press F1 to discard your changes.

**To set up an Avaya Call Manager to emit quality data:**

1. Log on to the Avaya Call Manager using PuTTY, TuTTY, or Avaya Manager.
2. Type `change system-parameters ip-options`, press F3, and then define the following settings:
   - Server IPV4 Address: The IP address of the VNQM main or additional poller
   - RTCP Report Period in seconds
   - IPV4 Server Port: 5005

3. Press F3 to save your changes.

4. Type `change ip-network-region [x]` where [x] is the region number, and then press F3.

5. Use F7 to navigate to the IP Network Region page.
6. Define the following settings:
   - RTCP Reporting Enabled: y
   - Use Default Server Parameters: y

7. Press F3 to save your changes.

Avaya CDR parameters

To take advantage of CDR polling in VoIP and Network Quality Manager, at least the following Avaya CDR parameters must be configured:

- dialed-num
- calling-num, or clg-num/in-tac
- start-date(4d) or start-date
- start-time
- end-date(4d), end-date, or date
- end-time, or time
- cond-code

If your Avaya setup makes it necessary, you can substitute certain parameters with different ones, and use them in the following way:
Configuring VoIP and Network Quality Manager

- Instead of the `start-time` parameter, you can use the `time` and `sec-dur` parameters.
- Instead of the `start-time` parameter, you can use the `end-time` and `sec-dur` parameters.
- Instead of the `end-time` parameter, you can use the `start-time` and `sec-dur` parameters.
- Instead of the `time` parameter, you can use the `start-time` and `sec-dur` parameters.

The order in which you configure CDR parameters is not relevant.

**Notes:**

- To be able to use the `start-date`, `start-date(4d)`, `end-date(4d)`, `start-time`, and `end-time` CDR custom fields, you must enable the SA8201-Start Time and the 4-Digit Year CDR Custom fields special application.
- You must also enable the SA8202-Intra-switch CDR by COS special application.

**Adding Avaya Call Manager Devices**

**Requirements**

Before adding Avaya Communication and Avaya Media Server devices to VNQM, make sure that you configure the device for VNQM. For detailed information, see "Managing Avaya Call Managers".

When you add an Avaya call manager device, VoIP and Network Quality Manager uses the value of the OID 1.3.6.1.2.1.1.1.1 `{sysDescr}` to identify an Avaya Communication and Media Server.

**Adding an Avaya Communication and Media Server to VNQM**

The following procedure adds an Avaya Communication and Media Server device to VoIP and Network Quality Manager.
**Note:** Call managers from manufacturers other than Cisco and Avaya can be monitored with VoIP and Network Quality Manager if you have SolarWinds Network Performance Monitor installed, and use a custom management information base (MIB) poller specifically configured for your call manager from other manufacturers. You cannot monitor call manager specific data, such as VoIP phones, region information, or call data. For more information, see "Adding Call Manager Devices from Other Manufacturers" in the *VoIP and Network Quality Manager* Administrator Guide.

**To add an Avaya Call Manager device to VoIP and Network Quality Manager:**

1. Log in to the Orion Web Console as an administrator.
2. Select the VoIP and Network Quality tab, and then click **VoIP & Quality Settings** in the top right of the page.
3. Click **Add CallManager nodes** in the **VoIP Management > Manage CallManager Nodes** section.
4. Select an available CallManager-hosting device, and then click **Next**.
   
   **Note:** If you do not see an expected call manager device, use the Web Console to add it. Make sure that you enable SNMP on the call manager device.

5. Decide whether you want to collect information about calls on this call manager.

   - **If you want to collect information about calls on this call manager,** select **Enable CDR/CQR polling for this Call Manager**, and then click **Next**.
   
   - **If you do not want to collect information about calls on this call manager,** select **Add Call Manager without CDR/CQR monitoring**, and then click **Next**.
     
     For information about the configuration of the necessary CDR parameters, see "Avaya CDR parameters".

6. Define the CLI credentials that let you log in to the SAT console of the Avaya Call Manager by either selecting an existing credentials set from the **Select Credentials** list, or by creating a new set.

   To create a new set, complete the following procedure:
Configuring VoIP and Network Quality Manager

a. Type the user name and password in the appropriate fields.
b. Select the enable level from the list.
c. Type the enable password.
d. In the Advanced section, select either the Telnet or the SSH protocol from the list.
e. Specify the Connection Timeout.

7. Click Test to test the credentials.

Note: If the SAT account has a PIN code defined for additional authentication, the CLI credential test will fail. PINs are not supported by VoIP and Network Quality Manager. Disable the PIN in the Avaya Call Manager, or use a credential set for which a PIN code is not defined.

8. Click Next.

9. Review the information, and then click Add Call Manager, or click Back to make changes.

Notes:

- The Avaya CDR/CQR Polling configuration grouping describes the configuration settings that are applicable to the Avaya Call Manager. To emit CDR or CQR (RTCP) data, use the listening ports that are displayed. The port numbers cannot be further configured through the user interface of VoIP and Network Quality Manager.

- VoIP and Network Quality Manager does not support the usage of survivable processors on Avaya. If you have set up survivable processors on your Avaya Communication and Media Server, VNQM does not accept CDR data.

- Use an NTP server to synchronize the time settings of the Avaya Communication and Media Server and the VNQM pollers. The synchronization is necessary to make sure that the CDR data and the call quality data match each other. If the time settings of the call manager and the VNQM pollers are not synchronized, the call quality data may not be displayed.

Requirements for Handling RTCP Data
If VNQM does not handle RTCP data correctly, the following causes are possible. Make sure that you fix these issues in order for VNQM to be able to process RTCP data.

- RTCP is already pointing to a different target than your VNQM instance.
- Both channels for CDR data are already occupied.
- You are using a customized data format for the CDR channel, which does not comply with the requirements of VNQM.

**Bandwidth Requirements for Avaya Communication and Media Servers**

This topic provides information about the average bandwidth requirements of Avaya Communication and Media Servers with different traffic levels.

This section assumes that the default polling interval of five seconds is used.

If an Avaya Communication and Media Server handles 20,000 calls simultaneously, the bandwidth necessary for polling RTCP data can be up to 18 Mbps.

If an Avaya Communication and Media Server handles one-sixth of this amount, that is, around 3,000 calls simultaneously, the bandwidth necessary for polling RTCP data is up to 3 Mbps.

Based on the previous calculations, a bandwidth of 5 Mbps suits most needs.

**Adding Call Manager Devices from Other Manufacturers**

VNQM also allows limited monitoring of other call manager devices. You can add them as VoIP network nodes and monitor their status in the VoIP Infrastructure resource. To do so, use a universal device poller configured for your call manager from other manufacturers. To take advantage of this option, SolarWinds Network Performance Monitor must also be installed.

**Notes:**

- Call managers from manufacturers other than Cisco and Avaya are added as VoIP network nodes, and thus are not displayed in the CallManagers resource.
- No CDR/CMR data are collected.
Configuring VoIP and Network Quality Manager

For more information about setting up universal device pollers for call managers from other manufacturers, see "Monitoring MIBs with Universal Device Pollers" in the SolarWinds Network Performance Monitor Administrator Guide.

For more information about adding call managers from other manufacturers to VoIP and Network Quality Manager, see "Adding VoIP Infrastructure" in the VoIP and Network Quality Manager Administrator Guide.

**Defining FTP Servers**

When you set up your Cisco CallManager device to collect CDR/CMR data, you can also designate an FTP server where the data is stored so that other applications, such as VoIP and Network Quality Manager, can download and process the data. For more information about FTP configuration, see "Configuring Cisco CallManagers for FTP".

**If you are unsure of your FTP server settings**, check your Cisco Billing Application Server parameters.

The **Polling Frequency** refers to how frequently VoIP and Network Quality Manager tries to download CDR/CMR data. If you have a large amount of data or if VoIP and Network Quality Manager experiences frequent timeouts, you should extend the amount of time between polls.

**Deleting CDR/CMR data** can cause serious data loss, but can be useful in certain circumstances. Do not select this option unless you successfully run verified backups of your data.

**Configuring Cisco CallManagers for FTP**

Complete the following procedure to configure your Cisco CallManager device to save CDR/CMR data to an FTP server.

You will need administrator access to your Cisco Unified Communications Manager and Cisco Unified Serviceability pages.

1. Log on to your Cisco Unified Communications Manager Administration page with an account that has administrative privileges.
2. Click **System > Service Parameters**.
3. On the Service Parameter page, set the **CDR Enabled Flag** to True.
4. Click **OK**.
To change the time interval for collecting CDR/CMR data, click **System > Enterprise Parameters**, modify the **CDR File Time Interval**, and then click **OK**.

5. Log on to the Cisco Unified Serviceability page with an account that has administrative privileges.
6. Click **Tools > CDR Management**.
7. Click the plus sign to add a new application billing server.
8. Enter the following information:
   - Host or IP address - the application billing server to which you want to send CDRs
   - User Name - the user name of the application billing server who has write permissions to the directory to which you send the CDR data
   - Password - the FTP password
   - Protocol - the protocol used to send CDR data to the application billing server
   - Directory Path - the path to which you want to send CDR data
9. Click **Add**.

   **Note**: This information is used when configuring your CCM when you want to monitor CDR/CMR data in VoIP and Network Quality Manager.

**Editing Call Managers**

In VoIP and Network Quality Manager you can edit the properties of your call manager nodes.

You can edit the following properties:

- Node name and polling address
- Polling Details (polling method, polling intervals and engines, CDR/CMR polling settings)
- Dependencies
- Custom properties
Configuring VoIP and Network Quality Manager

- Call Manager specific details (AXL credentials, FTP server settings, polling frequency)
- Alerting thresholds

For more information about editing node properties, see "Edit Properties" in the SolarWinds Network Performance Monitor Administrator Guide.

To edit call manager specific settings:

1. Log in to the Orion Web Console as an administrator.
2. Click VoIP & Network Quality in the Modules menu bar, and then click VoIP & Quality Settings at the top right of the view.
3. Click Manage CallManager Nodes in the VoIP Management section.
4. Select the call manager node you want to modify, and then click Edit CallManagers. This opens the Edit Properties page where you can edit the following call manager specific details, depending on the type of call manager.

   - For Cisco Call Managers:

   **Call Manager CDR/CMR Polling**

   Select Enable CDR/CMR polling for this Call Manager to collect information about calls on this CallManager.

   **AXL Credentials**

   Select the appropriate settings from the Select AXL Credentials list or define new credentials.

   To define a new set of AXL Credentials:

   - Type a name in Select AXL Credentials.
   - Type the user name in AXL Username.
FTP Server Settings

- Type the password in **AXL Password**.

**Notes:**

- Enter AXL credentials for both publisher and subscriber call managers.
- AXL credentials must be accurate. VoIP and Network Quality Manager tests the credentials before continuing to the next step.

**FTP Server Settings**

Fill in or edit details about the FTP server where your CDR/CMR data is stored. For more information about FTP configuration, see "Configuring Cisco CallManagers for FTP".

**FTP Server:** Fill in or edit the FTP server IP address.

**Port:** Fill in or edit the FTP port number.

**Passive mode:** Select this option to connect to the FTP server in passive mode.

**Secure Connection:** Select this option if you connect to an SFTP site.

**CDR/CMR file path:** Fill in or edit these details if appropriate.

**FTP Credentials:** Add or edit your FTP credentials.

**To define a new set of FTP Credentials:**

- Type a name in **Select FTP Credentials**.
- Type the user name in **FTP Username**.
- Type the password in **FTP Password**.

**Polling Frequency:** Type a number between 1
and 60 to configure how frequently you want to poll the FTP server in minutes.

**Delete CDR/CMR files from FTP server after download:** Select this option to delete CDR/CMR files from the FTP server if the hard drive is becoming full or if you need to speed up data collection from the FTP server.

**Warning:** Deleting CDR/CMR files from the FTP server may cause serious data loss. Ensure that your backups are running successfully before selecting this option.

- For Avaya Communication and Media Servers:

  **Call Manager CDR/CQR Polling**

  Select **Enable CDR/CQR polling for this Call Manager** to collect information about calls on this Call Manager.

  **Call Manager CLI Credentials**

  Select the appropriate settings from the **Select Credentials** list, or define new credentials.

  **To define a new set of CLI Credentials:**

  - Type the user name and password in the associated fields.
  - In the Advanced section, you can define the protocol, the port number, and the connection timeout.

  5. Edit the appropriate details, and then click **Submit**.

**Deleting Call Manager Devices from VoIP and Network Quality Manager**

The following procedure provides the steps required to delete a Call Manager device from VoIP and Network Quality Manager.
To delete a Call Manager device from VoIP and Network Quality Manager:

1. Log in to the Orion Web Console as an administrator.
2. Select the VoIP and Network Quality tab, and then click **VoIP & Quality Settings** in the top right of the page.
3. Click **Manage CallManager nodes**.
4. Select the CallManager-hosting devices you want to delete, and then click **Remove CallManagers**.
5. Click **OK** to confirm.

**Managing Gateways**

Managing gateways in VoIP and Network Quality Manager is done on the Manage Gateways page. This page provides a list of all gateway nodes monitored by VNQM.

**To access the Manage Gateway Nodes page:**

1. Log in to the Orion Web Console as an administrator.
2. Select the VoIP and Network Quality tab, and then click **VoIP & Quality Settings** in the top right of the page.
3. Click **Manage gateways** in the **VoIP Management** grouping.

**Notes:**

- For polling gateway details, VNQM requires valid CLI credentials.
- For adding gateway nodes to VNQM, the nodes already have to be in your database.

**Adding Gateways**

If you want to monitor your gateways with VoIP and Network Quality Manager, you have to add them to VNQM as gateway nodes first.

The Add VoIP Gateway page provides a wizard which helps you to add a gateway node to VoIP and Network Quality Manager as a gateway. Gateway nodes require CLI credentials.
To add a gateway device to VoIP and Network Quality Manager:

1. Log in to the Orion Web Console as an administrator.
2. Select the VoIP and Network Quality tab, and then click VoIP & Quality Settings in the top right of the page.
3. Click Add gateways in the VoIP Management grouping.
4. **Select VoIP Gateways to Add:** Select one or more available nodes which you want to add to VNQM as gateways. 
   
   **Note:** If you do not see an expected device, click add your nodes to add it to the Orion database, and then repeat Steps 1 - 3. For more information about adding nodes to the Orion database, see "Adding Devices for Monitoring in the Web Console" in the SolarWinds Network Performance Monitor Administrator Guide.

5. Click Next.
6. The CLI Credentials Issues dialog pops up with details about CLI credential issues on the nodes you are adding. Modify CLI credentials to solve the issues:
   a. Select the node or nodes whose CLI credentials you want to edit.
      
      **Note:** If you want to use the same CLI credentials for all nodes with issues, click Select Errors. All nodes will be selected.
   b. Click Edit Credentials.
      
      - Select valid credentials in the Select Credentials list or define a new set of credentials in the Username and Password fields.
      - Click Save to apply your CLI credential settings on the selected nodes.
   c. Click Select Successful to select nodes whose CLI credentials have been updated successfully.
   d. Click Continue to add the selected nodes to VNQM as gateway nodes.

7. Review the information, and then click Finish to add the selected gateways, or click Back to make changes.

**Editing VoIP Gateways**
You can edit the gateway node details, such as the node name, polling details, dependencies or custom properties.

**To edit gateway node properties:**

1. Log in to the Orion Web Console as an administrator.
2. Click **VoIP & Quality Settings** in the top right of the VoIP and Network Quality tab.
3. Click **Manage gateways**.
4. Select one or more available gateways that you want to edit.

   **Note:** If you do not see an expected device, click add your nodes to add it to the Orion database, and then repeat Steps 1 - 3. For more information about adding nodes to the Orion database, see "Adding Devices for Monitoring in the Web Console" in the SolarWinds Network Performance Monitor Administrator Guide.

5. Edit the appropriate properties of the selected gateway node. For more information about editing nodes, see "Editing Object Properties" in the SolarWinds Network Performance Monitor Administrator Guide.
6. Click **Submit** to apply your changes.

**Editing CLI Credentials for Gateway Nodes**

For monitoring gateway nodes, VNQM uses CLI credentials.

**To edit CLI credentials, complete the following steps:**

1. Log on to your VoIP and Network Quality Manager server using an account with administrator privileges.
2. Click **VoIP & Quality Settings** in the top right of the VoIP and Network Quality tab.
3. Click **Manage Gateways**.
4. Select the node you want to edit, and then click **Edit CLI Credentials**.
5. Select the appropriate settings from the **Select Credentials** list or define new credentials.

**To define a new set of CLI credentials:**
Configuring VoIP and Network Quality Manager

- **Select Credentials**: Type the name of the new credential set.
- **Username**: Type the user name.
- **Password**: Type the password.
- **Enable Level**: Select the enable level to use when logging in.
  
  **Note**: The enable level must have privileges to execute terminal commands. VoIP and Network Quality Manager uses Show commands to fetch and display data from the gateway. For information about configuring network devices, see your manufacturer’s documentation.

- **Enable Password**: Type the password associated with the enable level to use when logging in.

6. Expand **Advanced**, and then select the **Protocol, Port Number**, and **Connection Timeout** you want to use when connecting to your network devices.

7. Click **Test** to test the credentials.

8. Click **Save** to apply your changes.

**Removing Gateways**

If you want to stop monitoring the PRI trunk utilization of a gateway, remove the gateway from VNQM.

**To remove gateway nodes from VNQM:**

1. Log in to the Orion Web Console as an administrator.

2. Click **VoIP & Quality Settings** in the top right of the VoIP and Network Quality tab.

3. Click **Manage gateways**.

4. Select one or more gateways that you want to remove.

5. Click **Remove Gateways**, and then click **OK** to confirm.

**Selecting VoIP and Network Quality Manager Infrastructure**
In VoIP and Network Quality Manager you can monitor the health and status of your IP SLA and VoIP devices in the VoIP Infrastructure resource on the VoIP Summary View page. To use this resource, select VoIP nodes which form the VoIP infrastructure.

**To specify VoIP infrastructure for VNQM:**

1. Log in to the Orion Web Console as an administrator.
2. Click **VoIP & Quality Settings** in the top right of the VoIP and Network Quality tab.
3. Click **Select VoIP nodes**.
4. Click the + in front of the name of manufacturers to see the available devices.
5. Make sure you only select the nodes that you want to see in the VoIP Infrastructure resource.

**Notes:**

- **If you do not see an expected VoIP-related device or interface in the list**, use the Web Console to add the device to the database. For more information, see "Adding Devices for Monitoring in the Web Console" in the SolarWinds Network Performance Monitor Administrator Guide.

- **If you are adding a VoIP simulation node and you want VNQM to automatically discover its IP SLA operation configuration**, you must provide an SNMP read/write community string when you add the device.

6. When you have selected all nodes that are a part of your VoIP infrastructure, click **OK** to confirm your settings.

**Call Precedence Levels**

The priority of a call is indicated by the call precedence level. The following table contains the list of possible call precedence levels.
VoIP and Network Quality Manager Settings

The following sections provide information about the settings you can define in VoIP and Network Quality Manager.

- **VNQM Settings Overview**
- **Configuring VNQM (Example Workflow)**
- **Setting Traffic Precedence**

**VNQM Settings Overview**

The VoIP and Network Quality Manager Settings page gives an overview of the configuration pages within VoIP and Network Quality Manager.

**To access this page:**

1. Log in to the Orion Web Console as an administrator.
2. Click **VoIP & Quality Settings** in the top right of the VoIP and Network Quality tab.

The following settings of VoIP and Network Quality Manager can be configured from this page.

**IP SLA Management**

This section provides links for managing IP SLA nodes and operations. For more information, see "**IP SLA Management**" in the *VoIP and Network Quality Manager Administrator Guide*.

**Manage IP SLA Operations**
By using the links in this section you can add, edit or delete IP SLA operations on your network. Each IP SLA operation on your network is associated with a designated simulation node.

**Notes:**

- IP SLA operations are limited to locations where there is an existing, Cisco IP SLA-compatible router or switch to serve as a simulation node. For more information about Cisco IP SLA-capable routers and switches, go to [www.cisco.com/go/fn](http://www.cisco.com/go/fn), click Research Features, select Search by feature, and then select IP SLAs – UDP Based VoIP Operation.
- Only nodes added to the database are available for IP SLA Manager monitoring.

**Manage IP SLA Nodes**

By using the links in this section you can add, edit and remove IP SLA devices from VoIP and Network Quality Manager. For more information, see "Adding Nodes to VoIP and Network Quality Manager" in the *VoIP and Network Quality Manager Administrator Guide*.

**VoIP Management**

By using the links in this section you can manage your VoIP network: call managers, gateways, and VoIP infrastructure.

For more information, see "VoIP Management" in the *VoIP and Network Quality Manager Administrator Guide*.

**Manage CallManager Nodes**

By using the links in this section you can specify and manage the devices on your VoIP network that are Cisco CallManager, CallManager Express, and Avaya Communication and Media Server devices.

**Note:** Only nodes added to the database are available for VoIP and Network Quality Manager monitoring.

**Manage VoIP Gateways**

By using the links in this section you can specify and manage devices on your VoIP network that are gateways.

**Select VoIP Infrastructure**
By using the Select VoIP nodes link you can select VoIP-related nodes and interfaces from your database and then display them in the VoIP Infrastructure resource.

VoIP and Network Quality Manager can monitor any node that is relevant to your VoIP network, provided you have first added the node. By expanding the given node trees, you can choose to monitor VoIP traffic down to the interface level. VoIP and Network Quality Manager provides a number of default alerts, reports, and resources with which you can constantly monitor all of your VoIP devices.

For more information about adding devices and interfaces, see "Adding Nodes to VoIP and Network Quality Manager" in the VoIP and Network Quality Manager Administrator Guide.

For more information about alerts and reports in VoIP and Network Quality Manager, see "Using VoIP and Network Quality Manager" in the VoIP and Network Quality Manager Administrator Guide.

Details

By using the options in this section you can configure general VNQM options, and view database details.

**Edit VoIP & Network Quality Manager Settings**

Links in this section present general options regarding your configuration of VoIP and Network Quality Manager. From the VoIP and Network Quality Manager Settings page, you can configure the following:

- The port through which VoIP and Network Quality Manager sends simulated traffic.
- The jitter codec that VoIP and Network Quality Manager simulates on your network.
- The interval at which VoIP and Network Quality Manager collects data about your network.
- The length of time that the collected data is retained in the database.
- The MOS advantage factor that appropriately characterizes your VoIP network for the purpose of determining the Mean Opinion Score (MOS).
- The Type of Service (ToS) octet allows you to set precedence levels for VoIP traffic and IP SLA operations.
Whether you can view operations created by VoIP and Network Quality Manager in the running configurations on your Cisco devices.

Which calls are successfully completed.

The timeout period of CDR/CMR data collection.

Whether you want to enable automatic Avaya Call Manager detection.

For more information, see "Configuring VoIP and Network Quality Manager Settings" in the VoIP and Network Quality Manager Administrator Guide.

Database Details

The VoIP and Network Quality Manager Database Details page provides installation and memory sizing information for your database. From this view you can read statistics concerning individual tables within your database.

Select a table from the list to see a count of rows and memory usage by data and indexes, respectively.

**Configuring VoIP and Network Quality Manager Settings**

The following steps guide you through the process of configuring VNQM on the VoIP and Network Quality Manager Settings page.

**Note:** VoIP and Network Quality Manager maintains default values for these settings. If you want to use the default settings, click **Restore Defaults**.

**To edit VoIP & Quality Settings:**

1. Log in to the Orion Web Console as an administrator.
2. Click **VoIP & Quality Settings** in the top right of the VoIP and Network Quality tab.
3. Click **Edit VoIP & Network Quality Manager settings** in the Details section.
4. **If you want to use a port other than the default for simulated VoIP traffic**, type your preferred port in the VoIP UDP Port field.
5. Select the **VoIP Jitter Codec** you are using for your VoIP network. For more information about jitter codecs, see "Jitter" in the VoIP and Network Quality Manager Administrator Guide.
6. Type a **CallManager Polling Interval** in minutes to specify how often you want to collect your call manager data.

VoIP and Network Quality Manager measures the performance of your network by periodically sending test packets over defined paths. The period between measurements is referred to as the polling interval. As network sizes and VoIP server performance vary, you may have to try a number of different intervals to achieve the necessary balance between server processing load and data resolution.

7. Type the period of time, in days, to retain IP SLA operation statistics in the **IP SLA Data Retention** field.

VoIP and Network Quality Manager stores statistics regarding the performance of your VoIP network in your database. The length of time this data is retained is configurable, allowing you to balance database maintenance with IP SLA requirements. As network sizes and VoIP server performance vary, you may have to try different retention periods to achieve the necessary balance between database memory allocation and data retention.

8. Type a value for the **MOS Advantage Factor**.

**Note:** The advantage factor measures on a scale of 0 to 20 the willingness of VoIP network users to trade call quality for convenience. For example, a cellular telephone is more convenient than a wired telephone, so some loss of call quality due to compression over a cellular phone network, as compared to call quality over a wired phone network, is acceptable to most users. This distinction is reflected in a higher advantage factor for a cellular phone network than for a wired phone network. For more information, see "Mean Opinion Score (MOS)" in the *VoIP and Network Quality Manager Administrator Guide.*
9. Provide a value for the **Type of Service** (ToS) octet to set the precedence of VoIP traffic on your network.

   **Note:** The ToS octet is a decimal value (0-255) that sets the precedence for VoIP traffic monitored with Cisco IP SLA operations. The default ToS value used by VoIP and Network Quality Manager is 184, corresponding to Expedited Forwarding (EF) per hop behavior (PHB) and a Differentiated Service Code Point (DSCP) value of 46. For more information about the ToS octet, see "Setting Traffic Precedence" in the *VoIP and Network Quality Manager Administrator Guide*.

10. Select **Operations in running configurations** to view all new operations created by VoIP and Network Quality Manager in the running configurations on Cisco devices. You cannot view VoIP and Network Quality Manager operations created with CLI credentials.

11. Type in the call termination codes that you want to represent successfully completed calls in **Successful call termination codes**.

12. Enter the time period that you want to wait before ending the CDR/CMR job in hh:mm:ss format in the **CDR/CMR job timeout** field.

13. Select whether you want to enable the detection of Avaya Call Managers. If the **Avaya Call Manager Detection** option is enabled, VNQM automatically detects Avaya Call Managers when you add call managers through the Add Call Manager wizard. For more information about adding Avaya Call Managers, see *Adding Avaya Call Manager Devices*. If you use a load balancer, it is recommended that you disable this option, and add the load balancer directly to VNQM.

14. Type in the **VoIP Gateway Polling Interval** in minutes to specify how often the status of your VoIP gateways and their calls should be checked.

15. Type in a value for the **VoIP Gateway Critical Threshold** in percent to specify when you want to be warned that the channel utilization of your gateways is critical.

16. Type in a value for the **VoIP Gateway Warning Threshold** in percent to specify when you want to be warned that the channel utilization of your gateways is high.

17. Specify how long your VoIP gateway statistics should be retained in the **VoIP Gateway Retention Period** field.
18. Click **OK** after you have finished configuring your VoIP and Network Quality Manager settings.

**Setting Traffic Precedence**

In VoIP and Network Quality Manager you can set the precedence, or packet priority, of your network traffic. Setting precedence levels for your traffic enables you to better ensure high quality of service on your network. VoIP and Network Quality Manager employs a decimal Type of Service value specified on the VoIP and Network Quality Manager Settings page. For more information, see "[Configuring VoIP&Network Quality Settings](#) in the *VoIP and Network Quality Manager Administrator Guide*. The Type of Service value used by VoIP and Network Quality Manager corresponds to the per hop behavior (PHB) and the Differentiated Service Code Point (DSCP) values as shown in the following table.

![Traffic Precedence Table](image)

<table>
<thead>
<tr>
<th>ToS Value (decimal)</th>
<th>DSCP Value (decimal)</th>
<th>IP Precedence</th>
<th>Flow Control</th>
<th>PHB</th>
<th>Drop Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best Effort</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Default</td>
</tr>
<tr>
<td>Class Selector (Backward Compatibility with IP Precedence)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>CS1</td>
</tr>
<tr>
<td>64</td>
<td>16</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>CS2</td>
</tr>
<tr>
<td>96</td>
<td>24</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>CS3</td>
</tr>
<tr>
<td>128</td>
<td>32</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>CS4</td>
</tr>
<tr>
<td>160</td>
<td>40</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>CS5</td>
</tr>
<tr>
<td>192</td>
<td>48</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>CS6</td>
</tr>
<tr>
<td>224</td>
<td>56</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>CS7</td>
</tr>
<tr>
<td>Assured Forwarding</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>AF11 Low</td>
</tr>
<tr>
<td>48</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>AF12 Medium</td>
</tr>
<tr>
<td>56</td>
<td>14</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>AF13 High</td>
</tr>
<tr>
<td>72</td>
<td>18</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>AF21 Low</td>
</tr>
<tr>
<td>80</td>
<td>20</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>AF22 Medium</td>
</tr>
<tr>
<td>88</td>
<td>22</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>AF23 High</td>
</tr>
<tr>
<td>104</td>
<td>26</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>AF31 Low</td>
</tr>
<tr>
<td>112</td>
<td>28</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>AF32 Medium</td>
</tr>
<tr>
<td>120</td>
<td>30</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>AF33 High</td>
</tr>
<tr>
<td>136</td>
<td>34</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>AF41 Low</td>
</tr>
<tr>
<td>144</td>
<td>36</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>AF42 Medium</td>
</tr>
<tr>
<td>152</td>
<td>38</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>AF43 High</td>
</tr>
<tr>
<td>Expedited Forwarding</td>
<td></td>
<td>184</td>
<td>1</td>
<td>0</td>
<td>EF</td>
</tr>
</tbody>
</table>
Using VoIP and Network Quality Manager

VoIP and Network Quality Manager focuses on the IP SLA operations and VoIP infrastructure of your network.

The following sections introduce basic tasks you can accomplish with VNQM:

- Starting VNQM
- Exploring VNQM Views
- Customizing Charts in VNQM
- Using Custom Properties
- Using VNQM Alerts
- Using VNQM Reports
- Using VNQM Maps

Starting VNQM

VoIP and Network Quality Manager opens in a web browser. The default Home tab provides a selection of the most relevant resources for monitoring your network.

To start VoIP and Network Quality Manager:

1. Log on to your VoIP and Network Quality Manager server.
2. Start the Orion Web Console in the Orion program folder.
3. Click the VoIP and Network Quality tab.

Note: You can also open VoIP and Network Quality Manager in a web browser by filling in the name or IP address of the server with your VNQM installation, such as http://oriondemo.solarwinds.com/Orion/.
If you use another port than the default 80, you need to add it to the address. If port 8080 is used, the address opening your VNQM in a web browser looks like the following:

Exploring VNQM Views

VoIP and Network Quality Manager presents current network performance metrics in easy-to-review tables, graphs, and charts.

VNQM data is provided in resources that are displayed on views.

A View is a web page providing a framework for displaying information about your VoIP calls and IP SLA operations in relation to individual nodes. Views contain resources. You can customize which resources you want to have on a view.

Selected views offer optional, fully customizable subviews that allow you to more extensively organize the resources that are available in your web console. For more information about subviews, see "Using and Configuring Subviews" in the SolarWinds Network Performance Monitor Administrator Guide.

The following two basic types of views are available:

- **Summary views** show VoIP or IP SLA details on all nodes and operations managed by VNQM. You can access your summary views in the VoIP and Network Quality menu bar. For more information about customizing the menu bar, see "Customizing Web Console Menu Bars" in the SolarWinds Network Performance Monitor Administrator Guide.

- **Detail views** show traffic information about individual objects in your IP SLA and VoIP infrastructure. You can access your detail views by opening a summary view and clicking the object whose details you want to see.

Resources are displayed on your views as a box and provide information about different aspects of your VoIP infrastructure or IP SLA operations usually in a chart and a table.
Some resources are meant to be used on summary views, some are suitable for detail views, and some can be useful on both view types. The information shown pertains to either all devices VoIP and Network Quality Manager monitors (if used on a summary view) or to the selected object (if used on a detail view for a node, interface, gateway or call manager, or other object).

For more information about customizing VoIP and Network Quality Manager views, see "Customizing Views" in the SolarWinds Network Performance Monitor Administrator Guide.

The following views are provided with VoIP and Network Quality Manager:

**IP SLA Operation Details View**
- Provides information about a single IP SLA operation instance. This view provides troubleshooting information for that instance.

**IP SLA Summary View**
- Provides an overview of the entire network, including resources that present information about IP SLA operations, IP SLA network maps, events and alerts, and overall performance metrics.

**IP SLA Top 10 View**
- Provides several resources containing lists of the top ten operations by category. These lists provide a quick overview of potential problem areas on your network.

**IP SLA Web Summary View**
- Provides an overview of your web-based operations, including resources that present information about web operations, events and alerts, and overall performance metrics.

**VoIP Call Details View**
- Displays detailed information about a single call.

**VoIP Call Path View**
- Displays information about a single VoIP call path. This provides information about the originating VoIP site of the call path.

**VoIP Call Manager Gateway View**
- Displays information about a gateway which has been registered with a call manager.

**VoIP CallManager View**
Using VoIP and Network Quality Manager

Provides information about a single call manager instance, including information about the server or router that hosts the call manager instance.

**VoIP Gateway View**

Provides detailed information about a single VoIP gateway or endpoint.

**Location View**

Displays information about a single VoIP location.

**VoIP Phone Details View**

Displays information about a single VoIP CCM Phone.

**VoIP Site View**

Displays information about a single VoIP Site. A VoIP Site is an IP SLA node with an operation.

**VoIP Summary View**

Provides an overview of your entire VoIP network, including resources that present information about VoIP devices, VoIP-related events and alerts, call paths, and overall performance metrics.

**VoIP and Quality Subview**

This subview is shown as the left navigation tab VoIP and Quality for node detail views which are provided by SolarWinds Network Performance Monitor.

It provides VNQM-relevant information pertaining to a selected node directly from the node view. The displayed information depends on how the node was added to VNQM:

- **Gateway**

  The subview provides information about the node from the gateway point of view. Resources shown here include Data Distribution, Failed Calls, Top 10 Quality and Trunk Utilization.

- **Call Manager**

  The subview provides information relevant for the node as a Call Manager. Here you can find resources such as Call Manager Stats, Failed Calls, Registered and Unregistered Phones chart, Disconnect Causes, and Connected Phones.
Customizing Charts in VNQM

- **IP SLA node**
  The subview displays the IP SLA Operations resource which provides information about IP SLA operations created on the selected node.

- **Gateway and IP SLA**
  If a node has been added to VNQM as both a gateway node and an IP SLA node, the VoIP and Quality subview displays both gateway and IP SLA operations relevant for the selected node, that is, Data Distribution, Failed Calls, Top 10 Quality Issues, Trunk Utilization, and IP SLA Operations.

**Customizing Charts in VNQM**

Charts produced within the Orion Web Console are customizable. To customize a chart, click **Edit** in the top right corner of the appropriate resource and use the customization options available on the corresponding Edit Resource page.

The following sections describe options that are available on the Customize Chart page to modify the presentation of a selected chart:

- **Chart Titles**
- **Calculated Series**
- **Time Period**
- **Sample Interval**
- **Chart Size**
- **Data Tables**
- **Font Size**
- **Printing Options**
- **Data Export Options**
- **Advanced**

**Note:** Click **Refresh** at any time while customizing a chart to review the changes you have made.

**Chart Titles**
**Chart Titles** are displayed at the top center of a generated chart. In the **Chart Titles** area you can modify the title and subtitles of your generated chart.

Network Performance Monitor provides default chart titles and subtitles. To restore the default values, clear the respective fields when editing chart titles, and then click **Submit**.

**Calculated Series**

In your graphs, you can display markers calculated from historical data. By using these markers, you can compare the current situation with the calculated series.

**To display markers in the graph, select the appropriate options:**

- **Show a trend line** displays the trend line, allowing you to see potential future results as they are extrapolated from collected historical data.
- **Show the sum of all data series** displays a line showing the total of all objects graphed.
- **Show the 95th percentile line** displays the 95th percentile marker. For more information, see "95th Percentile Calculations" in the SolarWinds Orion Core Administrator Guide.

**Note:** Only the options applicable for the particular resource are available.

**Time Period**

You can designate a predefined or custom time period for your chart by using any of the available methods:

- Select a predefined time period from the time period list.
- Select the **Select custom period** option, and then provide custom **Start** and **Ending Dates/Times** in the appropriate fields.

Some charts define the time period they show using the following options:

- **Default zoom range:** Select the time period to be displayed in the graph or chart per default. You can see this information by default below the chart title.
- **Amount of historical data to load**: Select the time period for which the data should be loaded. You can display this data dynamically using the slider below the chart.

- **Sample interval**: Select the time interval which you want to see in the graph as a single point or bar.
  
  **Note**: Data within the defined sample is summarized automatically.

### Sample Interval

The sample interval dictates the precision of your generated chart. A single point or bar is plotted for each sample interval. If a sample interval spans multiple polls, polled data is automatically summarized and plotted as a single point or bar on the chart.

**Note**: Due to limits of memory allocation, some combinations of time periods and sample intervals may require too much system resources to display, due to the large number of polled data points. As a result, charts may not be displayed if the time period is too long or if the sample interval is too small.

### Chart Size

Chart size options configure the width and height, in pixels, of the chart. You can maintain the same aspect ratio, or scale the chart in size, by entering a width, and then entering 0 for the height.

### Data Tables

The **Data Table Below Chart** option displays a table of the charted data points below the chart.

**Note**: You may not be able to read individual data points if you select a small sample interval. Select a larger sample interval to more easily read data points.

### Font Size

Generated charts have variable font sizes. By using the Font Size option you can select a small, medium, or large size font for your chart labels and text.

**Note**: Font size selections are maintained in the printable version of your chart.

### Printing Options

To print your customized chart, click **Printable Version**. A printable version of your customized chart is displayed in the browser.
Data Export Options

Exportable chart data is also available from selected charts in the Display Data Export Options. Data can be exported as Microsoft Excel-compatible Raw Data or as HTML-formatted Chart Data.

To export chart data, click Raw Data, and then follow the prompts to open or save the resulting raw data file.

Advanced

By using this option you can modify the title and subtitle of your generated chart. Chart titles are displayed at the top center of a generated chart.

To modify the chart title and subtitle:

1. Click + next to Advanced.
2. Fill in the appropriate Chart title or Chart subtitle.

Note: Orion may provide default chart titles and subtitles. If you edit any of them, you can restore the default titles and subtitles by clearing the respective fields, and then clicking Submit.

Using Custom Properties for VNQM

By using the Orion Custom Property Editor, you can simplify the task of monitoring your network. By using the Custom Property Editor you can define custom properties, such as country, building, asset tag, and serial number. These properties may apply to any device or operation that you have stored in the SolarWinds VoIP and Network Quality Manager database. After properties are added, they are available for display and filtering within any Orion application. A few examples of how custom properties can be used are as follows:

- Add a custom property and display it as an annotation on a chart.
- Add a custom property to interfaces to display a custom description.
- Add a custom property that is used as an account limitation on sites.
- Add additional information to sites, such as contact, owner, or support contract number.
- Add a notification property to sites that can configure the alerts feature to send an email to a computer named within the custom property.
• Add a custom property to routers and interfaces for grouping them on the web or in a report.
• Add a custom property of billing codes or customer IDs.

In the Custom Property Editor you can choose from a collection of commonly used properties, or you can build your own custom properties. After your custom property is defined, you can use the Custom Property Editor to populate your custom property with appropriate values or you can use the Import Wizard to populate the new property from either a text file or a comma-delimited file. For more information about creating custom properties for VoIP and Network Quality Manager, see "Creating a Custom Property" in the SolarWinds Network Performance Monitor Administrator Guide.

Using Advanced Alerts and Actions in VNQM

VoIP and Network Quality Manager provides a number of IP SLA-specific alerts you can use with Advanced Alert Manager to actively monitor and respond to detected issues. By using the Advanced Alerts Manager you can also designate actions for VoIP and Network Quality Manager alerts.

Note: Only advanced alerts can be used for IP SLA-specific purposes. Basic alerts cannot be configured to trigger on VoIP conditions or events.

To view your alerts:

1. Start the Orion Web Console in your Orion program folder.
2. Go to the Home tab, and then select the Alerts tab.

To edit alerts:

1. Start the Advanced Alert Manager in your SolarWinds Orion program folder (for example through Start > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager).
2. Click Configure Alerts.
3. In the Manage Alerts popup window, you can add, activate and edit your VNQM alerts. For more information, see "Using Orion Advanced Alerts" in the SolarWinds Orion Core Administrator Guide.
Using VoIP and Network Quality Manager

**Note:** In general, you can keep the alert evaluation frequency to one minute. Depending on the amount of operations and CDR/CMR polling, and the amount of data returned, you may need to increase the amount of time between each alert evaluation.

The following section contains the list of VoIP and Network Quality Manager specific alerts.

- Alert me when a managed node has not been polled during the last 5 minutes
- Alert me when a managed node last poll time is 10 minutes old
- Alert me when an IP SLA operation fails
- Alert me when an IP SLA operation goes into warning or critical state
- Alert me when the call manager’s failed call percentage is over 25% within the last 30 minutes
- Alert me when the call manager’s jitter is over 50 within the last 30 minutes
- Alert me when the call manager’s latency is over 150 within the last 30 minutes
- Alert me when the call manager's MOS is under 3.5 within the last 30 minutes
- Alert me when the call manager’s packet loss is over 5 within the last 30 minutes
- Alert me when the phone’s failed call percentage is over 25% within the last 30 minutes
- Alert me when the phone’s jitter is over 50 within the last 30 minutes
- Alert me when the phone’s latency is over 150 within the last 30 minutes
- Alert me when the phone’s MOS is under 3.5 within the last 30 minutes
- Alert me when the phone’s packet loss is over 5 within the last 30 minutes
- Alert me when the region’s jitter is over 50 within the last 30 minutes
- Alert me when the region’s latency is over 150 within the last 30 minutes
- Alert me when the region's MOS is under 3.5 within the last 30 minutes
- Alert me when the region's packet loss is over 5 within the last 30 minutes
- VoIP - Infrastructure Node is Down
- VoIP - Rejected Gateways > 5%
- VoIP - Rejected Phones > 5%
- VoIP - Unregistered Gateways > 5%
- VoIP - Unregistered Phones > 5%

You can configure other alerts by following the procedures in the SolarWinds Network Performance Monitor Administrator Guide and by using variables available in NPM and the Advanced Alert Manager.


**VNQM Reports**

SolarWinds provides Report Writer as a quick and easy way for you to extract data from your database. Because VoIP and Network Quality Manager is an integrated module of the Orion platform, information that you collect about your IP SLA-capable network is easily presented in a variety of formats using Report Writer.

A number of predefined IP SLA-specific reports is available with your installation of VoIP and Network Quality Manager. Report Writer also enables custom IP SLA report creation, as necessary, using criteria and conditions you choose. When you have finished editing your reports, you can view them through the VoIP and Network Quality Manager web interface and print them with the click of a button.

**Note:** VNQM 4.2 does not support managing reports directly within the Orion Web Console.

For more information about predefined IP SLA Reports, see "Using Predefined IP SLA Reports" in the VoIP and Network Quality Manager Administrator Guide.

For more information about using Report Writer, see "Creating and Modifying Reports" in the SolarWinds Orion Core Administrator Guide.
Using VoIP and Network Quality Manager

A report scheduling application is available to all customers with a current maintenance agreement. This tool schedules automatic email reports that can be sent to individual users or groups of users. Log in to the customer portal of www.solarwinds.com and download the Report Scheduler from the Additional Components for Orion area.

Report Writer capabilities are further enhanced when they are used with the Custom Property Editor. Custom properties are available for report sorting and filtering. For more information, see "Creating Custom Properties for VoIP and Network Quality Manager" in the VoIP and Network Quality Manager Administrator Guide.

Using Predefined VNQM Reports

The following VNQM reports are provided with a VoIP and Network Quality Manager installation.

To access predefined reports:

1. Start the Orion Web Console in your SolarWinds Orion program folder.
2. Go to the Home tab, and then select the Reports tab.
3. Double-click the report you want to display.

To edit a report, open it in the Report Writer:


For more information about customizing reports to suit your reporting needs, see "Creating and Modifying Reports" in the SolarWinds Orion Core Administrator Guide.

Historical IP SLA Reports

VoIP and Network Quality Manager includes predefined reports for IP SLA operations on your network.

DHCP – Last 7 Days

Displays the average round trip time, maximum round trip time, and total failed requests over the last 7 days.
DHCP – Last Month
Displays the average round trip time, maximum round trip time, and total failed requests that occurred last month.

DHCP – This Month
Displays the average round trip time, maximum round trip time, and total failed requests that occurred this month.

DNS – Last 7 Days
Displays the average round trip time and maximum round trip time for DNS requests over the last 7 days.

DNS – Last Month
Displays the average round trip time and maximum round trip time for DNS requests that occurred last month.

DNS – This Month
Displays the average round trip time and maximum round trip time for DNS requests that occurred this month.

FTP – Last 7 Days
Displays the average round trip time and maximum round trip time for FTP requests over the last 7 days.

FTP – Last Month
Displays the average round trip time and maximum round trip time for FTP requests that occurred last month.

FTP – This Month
Displays the average round trip time and maximum round trip time for FTP requests that occurred this month.

HTTP – Last 7 Days
Displays the minimum and average round trip time for HTTP, DNS, and TCP Connect requests as well as the total failed requests over the last 7 days.

HTTP – Last Month
Displays the minimum and average round trip time for HTTP, DNS, and TCP Connect requests as well as the total failed requests that occurred last month.
HTTP – This Month
Displays the minimum and average round trip time for HTTP, DNS, and TCP Connect requests as well as the total failed requests that occurred this month.

ICMP Echo – Last 7 Days
Displays the average round trip time and maximum round trip time for ICMP Echo requests over the last 7 days.

ICMP Echo – Last Month
Displays the average round trip time and maximum round trip time for ICMP Echo requests that occurred last month.

ICMP Echo – This Month
Displays the average round trip time and maximum round trip time for ICMP Echo requests that occurred this month.

ICMP Path Echo – Last 7 Days
Displays the average round trip time and maximum round trip time hop-by-hop over the last 7 days.

ICMP Path Echo – Last Month
Displays the average round trip time and maximum round trip time hop-by-hop that occurred last month.

ICMP Path Echo – This Month
Displays the average round trip time and maximum round trip time hop-by-hop that occurred this month.

ICMP Path Jitter – Last 7 Days
Displays the average MOS for operations defined on your network between listed source and destination sites hop-by-hop over the last 7 days.

ICMP Path Jitter – Last Month
Displays the average MOS for operations defined on your network between listed source and destination sites hop-by-hop that occurred last month.

ICMP Path Jitter – This Month
Displays the average MOS for operations defined on your network between listed source and destination sites hop-by-hop this month.
TCP Connect – Last 7 Days
Displays the average round trip time and maximum round trip time for TCP Connect requests over the last 7 days.

TCP Connect – Last Month
Displays the average round trip time and maximum round trip time for TCP Connect requests that occurred last month.

TCP Connect – This Month
Displays the average round trip time and maximum round trip time for TCP Connect requests that occurred this month.

UDP Echo – Last 7 Days
Displays the average round trip time and maximum round trip time for UDP Echo requests over the last 7 days.

UDP Echo – Last Month
Displays the average round trip time and maximum round trip time for UDP Echo requests that occurred last month.

UDP Echo – This Month
Displays the average round trip time and maximum round trip time for UDP Echo requests that occurred this month.

UDP Jitter – Last 7 Days
Displays the average MOS for operations defined on your network between listed source and destination sites over the last 7 days.

UDP Jitter – Last Month
Displays the average MOS for operations defined on your network between listed source and destination sites that occurred last month.

UDP Jitter – This Month
Displays the average MOS for operations defined on your network between listed source and destination sites that occurred this month.

VoIP UDP Jitter – Last 7 Days
Displays minimum, maximum, and average VoIP metrics for the simulated VoIP traffic between listed source and destination sites over the last 7 days.
Using VoIP and Network Quality Manager

**VoIP UDP Jitter – Last Month**
Displays minimum, maximum, and average VoIP metrics for the simulated VoIP traffic between listed source and destination sites that occurred last month.

**VoIP UDP Jitter – This Month**
Displays minimum, maximum, and average VoIP metrics for the simulated VoIP traffic between listed source and destination sites that occurred this month.

**Historical VoIP Reports**
VoIP and Network Quality Manager includes predefined reports for VoIP-enabled devices on your network.

**Calls in Last 24 Hours**
Displays the call details of all calls on your network between listed source and destination sites over the last 24 hours.

**Jitter – Last 30 Days**
Displays the average jitter for call paths defined on your network between listed source and destination sites over the last 30 days.

**Latency – Last 30 Days**
Displays the average latency for call paths defined on your network between listed source and destination sites over the last 30 days.

**MOS Score – Last 30 Days**
Displays the average MOS for call paths defined on your network between listed source and destination sites over the last 30 days.

**Packet Loss – Last 30 Days**
Displays the average packet loss for call paths between listed source and destination sites, as defined on your network, over the last 30 days.

**VoIP Nodes Availability – Last 30 Days**
Displays the average availability for all VoIP-enabled nodes designated on your network over the last 30 days.

**VNQM Maps**
VoIP and Network Quality Manager allows you to display your IP SLA operations on customizable maps produced within the Orion Web Console. You can create new maps or modify any existing map to include IP SLA operations. The operation status is displayed on the map in the same fashion as nodes, interfaces, or volumes.

For more information about using maps, see the SolarWinds Network Atlas Administrator Guide.

To add SolarWinds VoIP and Network Quality Manager operations to your map:

1. Start the Network Atlas in your SolarWinds program folder.
2. Locate the source node in the left pane containing the IP SLA operations you want to add.
3. Click [+ ] next to the node name.
4. Click [+ ] next to IP SLA Operations.
5. Drag the operation you want to the drawing area.

VoIP and Network Quality Manager Map Variables

The following list of variables can be used when creating labels for your map objects.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DateChangedUtc</td>
<td>The last time the operation information was updated</td>
</tr>
<tr>
<td>Deleted</td>
<td>Indicates if the operation has been deleted from VoIP and Network Quality Manager</td>
</tr>
<tr>
<td>Description</td>
<td>A user defined explanation of the operation</td>
</tr>
<tr>
<td>DetailsUrl</td>
<td>Link to the detail page</td>
</tr>
<tr>
<td>DisplaySource</td>
<td>The source node</td>
</tr>
<tr>
<td>DisplayTarget</td>
<td>The target node</td>
</tr>
<tr>
<td>Frequency</td>
<td>How often the operation is performed</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IpSlaOperationNumber</td>
<td>The internal number of the operation</td>
</tr>
<tr>
<td>IsAutoConfigured</td>
<td>This value is True if it was created by VoIP and Network Quality Manager, False if it was created by the user</td>
</tr>
<tr>
<td>LifetimeUtc</td>
<td>The timeframe of when the operation is executed</td>
</tr>
<tr>
<td>NodeID</td>
<td>The ID of the node</td>
</tr>
<tr>
<td>OperationInstanceId</td>
<td>The internal ID of the operation</td>
</tr>
<tr>
<td>OperationName</td>
<td>The name of the operation as it appears in the database</td>
</tr>
<tr>
<td>OperationResultID</td>
<td>The ID of the results of the operation</td>
</tr>
<tr>
<td>OperationResultRecordTime</td>
<td>The timestamp of when the operation was performed</td>
</tr>
<tr>
<td>OperationStateID</td>
<td>The ID of the operation state</td>
</tr>
<tr>
<td>OperationStatusID</td>
<td>The ID of the operation status</td>
</tr>
<tr>
<td>OperationTypeID</td>
<td>The value of the operation type</td>
</tr>
<tr>
<td>OperationTypeID</td>
<td>The ID of the operation type</td>
</tr>
<tr>
<td>SourceNodeID</td>
<td>The node ID of the source node</td>
</tr>
<tr>
<td>StatusMessage</td>
<td>A message that describes the status value</td>
</tr>
<tr>
<td>TargetNodeID</td>
<td>The node ID the operation is targeting</td>
</tr>
</tbody>
</table>

For more information about creating maps, see the [SolarWinds Network Atlas Administrator Guide](#).
Appendix A: Software License Key

After installing the application, the setup program displays the licensing window. Complete the following procedure to enable your software license key.

To enable a software license key:

1. Click Enter Licensing Information.
2. If the computer on which you installed VoIP and Network Quality Manager is connected to the Internet, complete the following procedure.
   a. Click I want to activate my license over the Internet.
   c. Log in to the customer portal using your CustomerID and password.
   d. Click License Management.
   e. Browse to SolarWinds VoIP and Network Quality Manager, and then locate the unregistered licenses list.
   f. Copy your unregistered VoIP and Network Quality Manager activation key to the clipboard, and then paste it into the Activation Key field on the Activate Toolset window.
   g. If you use a proxy server to access the Internet, select the Proxy Server option, and then type the proxy address and port number.
   h. Click Next.

3. If the computer on which you are installing VoIP and Network Quality Manager is not connected to the Internet, complete the following procedure.
   a. Click I want to activate my license through the Customer Portal.
   b. Complete the procedure described on the Activate Toolset window to complete the registration.
Maintaining Licenses with License Manager

SolarWinds License Manager is an easy-to-install, free utility with which you can migrate VoIP and Network Quality Manager licenses from one computer to another without contacting SolarWinds Customer Service. The following sections provide procedures for installing and using License Manager:

- Installing License Manager
- Using License Manager

Installing License Manager

Install License Manager on the computer from which you are migrating currently licensed products.

**Note:** You must install License Manager on a computer with the correct time. If the time on the computer is off by as little as 5 minutes, in either direction, from Greenwich Mean Time (GMT), you will be unable to reset licenses without calling SolarWinds Customer Service. Time zone settings do not affect and do not cause this issue.

**To install License Manager:**

1. Start **SolarWinds License Manager Setup** in the SolarWinds folder.
2. Click **I Accept** to accept the SolarWinds EULA.
3. If you are prompted to install the SolarWinds License Manager application, click **Install**.

Using License Manager

You must run License Manager on the computer where the currently licensed SolarWinds product is installed before you can migrate licenses to a new installation. The following procedure deactivates currently installed licenses that can then be transferred to a new installation.

**To deactivate currently installed licenses:**

1. Start **SolarWinds License Manager** in the SolarWinds folder.
2. Select the products you want to deactivate on this computer, and then click **Deactivate**.
3. Specify your SolarWinds Customer ID and password when prompted, and then click **Deactivate**.

**Note:** Deactivated licenses are now available for activation on a new computer.

After you have successfully deactivated your products, log on to the computer on which you want to install your products, and then begin installation. When asked to specify your licenses, provide the appropriate information. The license you deactivated earlier is then assigned to the new installation.
Appendix B: MIBs Maintained by VoIP and Network Quality Manager

VoIP and Network Quality Manager continually updates CISCO-RTTMON-MIB in order to maintain IP SLA operations between devices. The following OID names are maintained by VoIP and Network Quality Manager, according to the settings of your VoIP and Network Quality Manager implementation, as it conducts IP SLA operations:

**General**

- SysContactOID
- RttMonApplVersion
- RttMonApplResponder (Read/Write)
- RttMonCtrlAdminStatus (Read/Write)
- RttMonCtrlAdminRttType (Read/Write)
- RttMonCtrlAdminOwner (Read/Write)
- RttMonCtrlAdminNvgen (Read/Write)
- RttMonEchoAdminProtocol (Read/Write)
- RttMonEchoAdminTOS

**All Operations**

- rttMonCtrlAdminRttType
- rttMonEchoAdminProtocol
- rttMonLatestRttOperSense
- rttMonLatestRttOperSense
- rttMonLatestRttOperApplSpecificSense
- rttMonLatestRttOperSenseDescription
- rttMonLatestRttOperTime
Appendix B: MIBs Maintained by VoIP and Network Quality Manager

DHCP Operations

- rttMonEchoAdminTargetAddress (Read/Write)

DNS Operations

- rttMonEchoAdminTargetAddressString (Read/Write)
- rttMonEchoAdminNameServer (Read/Write)

HTTP and FTP Operations

- rttMonLatestHTTPOperRTT
- rttMonLatestHTTPOperDNSRTT
- rttMonLatestHTTPOperTCPConnectRTT
- rttMonLatestHTTPOperTransactionRTT
- rttMonEchoAdminURL (Read/Write)
- rttMonEchoAdminOperation (Read/Write)

ICMP Echo Operations

- rttMonEchoAdminTargetAddress (Read/Write)

TCP Connect Operations

- rttMonCtrlAdminTimeout (Read/Write)
- rttMonEchoAdminControlEnable (Read/Write)
- rttMonEchoAdminTargetAddress (Read/Write)
- rttMonEchoAdminTargetPort (Read/Write)

UDP Jitter Operations

- rttMonLatestJitterOperSumOfPositivesSD
- rttMonLatestJitterOperSumOfPositivesDS
- rttMonLatestJitterOperSumOfNegativesSD
VoIP UDP Jitter Operations

- rttMonLatestJitterOperSumOfNegativesDS
- rttMonLatestJitterOperNumOfPositivesSD
- rttMonLatestJitterOperNumOfPositivesDS
- rttMonLatestJitterOperNumOfNegativesSD
- rttMonLatestJitterOperNumOfNegativesDS
- rttMonLatestJitterOperPacketLossSD
- rttMonLatestJitterOperPacketLossDS
- rttMonLatestJitterOperPacketMIA
- rttMonLatestJitterOperPacketLateArrival
- rttMonLatestJitterOperPacketOutOfSequence
- rttMonLatestJitterOperRTTSum
- rttMonLatestJitterOperNumOfRTT
- rttMonLatestJitterOperOWSumSD
- rttMonLatestJitterOperOWSumDS
- rttMonLatestJitterOperNumOfOW

VoIP UDP Jitter Operations

- rttMonLatestJitterOperMOS
- rttMonEchoAdminSourceAddress
- RttMonEchoAdminSourcePort
- RttMonEchoAdminTargetAddress
- RttMonEchoAdminTargetPort
- RttMonEchoAdminVrfName
- RttMonEchoAdminTOS
- RttMonEchoAdminTOS
- RttMonEchoAdminInterval

VoIP Specific MIBs
Appendix B: MIBs Maintained by VoIP and Network Quality Manager

- `rttMonEchoAdminSourceAddress`
- `rttMonCtrlAdminFrequency`
- `rttMonEchoAdminCodecType`
- `rttMonEchoAdminCodecPayload`
- `rttMonEchoAdminCodecNumPackets`
- `rttMonEchoAdminCodecInterval`
- `rttMonEchoAdminICPIFAAdvFactor`
- `rttMonScheduleAdminRttLife`
- `rttMonScheduleAdminRttStartTime`
Appendix C: Supported Versions of Cisco Unified Call Manager

VoIP and Network Quality Manager uses the CISCO-CCM-MIB and supports Cisco Unified Call Manager versions 6, 7, 8, 9 and 10.

**Note:** If you have multiple polling engines, you must install the same version of IP SLA Manager on all polling engines before you will be able to add a Call Manager server.

The following table lists the OIDs used for Call Manager.

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccmRegisteredPhones</td>
<td>1.3.6.1.4.1.9.9.156.1.5.5.0</td>
</tr>
<tr>
<td>ccmUnregisteredPhones</td>
<td>1.3.6.1.4.1.9.9.156.1.5.6.0</td>
</tr>
<tr>
<td>ccmRejectedPhones</td>
<td>1.3.6.1.4.1.9.9.156.1.5.7.0</td>
</tr>
<tr>
<td>ccmRegisteredGateways</td>
<td>1.3.6.1.4.1.9.9.156.1.5.8.0</td>
</tr>
<tr>
<td>ccmUnregisteredGateways</td>
<td>1.3.6.1.4.1.9.9.156.1.5.9.0</td>
</tr>
<tr>
<td>ccmUnregisteredGateways</td>
<td>1.3.6.1.4.1.9.9.156.1.5.10.0</td>
</tr>
</tbody>
</table>

**OIDs from the ccmTable**

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccmVersion</td>
<td>1.3.6.1.4.1.9.9.156.1.1.2.1.4</td>
</tr>
<tr>
<td>ccmInetAddressType</td>
<td>1.3.6.1.4.1.9.9.156.1.1.2.1.6</td>
</tr>
<tr>
<td>ccmInetAddress</td>
<td>1.3.6.1.4.1.9.9.156.1.1.2.1.7</td>
</tr>
<tr>
<td>ccmClusterId</td>
<td>1.3.6.1.4.1.9.9.156.1.1.2.1.8</td>
</tr>
</tbody>
</table>

**OIDs from the ccmRegionTable**
Appendix C: Supported Versions of Cisco Unified Call Manager

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccmRegionIndex</td>
<td>1.3.6.1.4.1.9.9.156.1.1.4.1.1</td>
</tr>
<tr>
<td>ccmRegionName</td>
<td>1.3.6.1.4.1.9.9.156.1.1.4.1.2</td>
</tr>
</tbody>
</table>

**OIDs from the ccmGatewayTable**

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccmGatewayName</td>
<td>1.3.6.1.4.1.9.9.156.1.3.1.1.2</td>
</tr>
<tr>
<td>ccmGatewayDescription</td>
<td>1.3.6.1.4.1.9.9.156.1.3.1.1.4</td>
</tr>
<tr>
<td>ccmGatewayStatus</td>
<td>1.3.6.1.4.1.9.9.156.1.3.1.1.5</td>
</tr>
<tr>
<td>ccmGatewayInetAddressType</td>
<td>1.3.6.1.4.1.9.9.156.1.3.1.1.7</td>
</tr>
<tr>
<td>ccmGatewayInetAddress</td>
<td>1.3.6.1.4.1.9.9.156.1.3.1.1.8</td>
</tr>
<tr>
<td>ccmGatewayTimeLastStatusUpdt</td>
<td>1.3.6.1.4.1.9.9.156.1.3.1.1.11</td>
</tr>
<tr>
<td>ccmGatewayTimeLastRegistered</td>
<td>1.3.6.1.4.1.9.9.156.1.3.1.1.12</td>
</tr>
<tr>
<td>ccmGatewayProductTypeIndex</td>
<td>1.3.6.1.4.1.9.9.156.1.3.1.1.15</td>
</tr>
</tbody>
</table>

**OIDs from the ccmProductTypeTable**

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccmProductType</td>
<td>1.3.6.1.4.1.9.9.156.1.1.8.1.2</td>
</tr>
<tr>
<td>ccmProductName</td>
<td>1.3.6.1.4.1.9.9.156.1.1.8.1.3</td>
</tr>
<tr>
<td>ccmProductCategory</td>
<td>1.3.6.1.4.1.9.9.156.1.1.8.1.4</td>
</tr>
</tbody>
</table>

**OIDs from the ccmPhoneTable**
## OIDs from the ccmPhoneExtnTable

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccmPhoneExtnIndex</td>
<td>1.3.6.1.4.1.9.9.156.1.2.5.1.1</td>
</tr>
<tr>
<td>ccmPhoneExtn</td>
<td>1.3.6.1.4.1.9.9.156.1.2.5.1.2</td>
</tr>
</tbody>
</table>

## OIDs from the ccmH323DeviceTable

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccmH323DevName</td>
<td>1.3.6.1.4.1.9.9.156.1.11.1.1.2</td>
</tr>
<tr>
<td>ccmH323DevDescription</td>
<td>1.3.6.1.4.1.9.9.156.1.11.1.1.4</td>
</tr>
<tr>
<td>ccmH323DevInetAddressType</td>
<td>1.3.6.1.4.1.9.9.156.1.11.1.1.5</td>
</tr>
<tr>
<td>ccmH323DevInetAddress</td>
<td>1.3.6.1.4.1.9.9.156.1.11.1.1.6</td>
</tr>
<tr>
<td>ccmH323DevStatus</td>
<td>1.3.6.1.4.1.9.9.156.1.11.1.1.21</td>
</tr>
</tbody>
</table>
## Appendix C: Supported Versions of Cisco Unified Call Manager

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccmH323DevStatusReason</td>
<td>1.3.6.1.4.1.9.9.156.1.11.1.1.22</td>
</tr>
<tr>
<td>ccmH323DevTimeLastStatusUpdt</td>
<td>1.3.6.1.4.1.9.9.156.1.11.1.1.23</td>
</tr>
<tr>
<td>ccmH323DevTimeLastRegistered</td>
<td>1.3.6.1.4.1.9.9.156.1.11.1.1.24</td>
</tr>
<tr>
<td>ccmH323DevProductTypeIndex</td>
<td>1.3.6.1.4.1.9.9.156.1.11.1.1.31</td>
</tr>
</tbody>
</table>
Appendix D: How VoIP and Network Quality Manager Creates Operations

The following sections detail how VoIP and Network Quality Manager creates new operations on your network devices:

- **Owner Field Value**
- **SNMP-Based Operations**
- **CLI-Based Operations**

**Owner Field Value**

VoIP and Network Quality Manager sets the Owner field value using the following naming scheme:

```
SW.IpSla.<pollerMachineName>.<dbCatalogName>
```

Where:

- `<pollerMachineName>` is the name of the server that is running the primary or additional poller assigned to a node that is a source node for an IP SLA operation.
- `<dbCatalogName>` is the name of the database on the database server.

**SNMP-Based Operations**

The following tables list the OIDs and values that are used to create new SNMP-based operations:

- **DHCP Operations**
- **DNS Operations**
- **FTP Operations**
- **HTTP Operations**
- **ICMP Echo Operations**
- **TCP Connect Operations**
Appendix D: How VoIP and Network Quality Manager Creates Operations

- **UDP Echo Operations**
- **UDP Jitter Operations**
- **VoIP UDP Jitter Operations**

### DHCP Operations

<table>
<thead>
<tr>
<th>MIB name</th>
<th>OID number</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonCtrlAdminRttType</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.4.&lt;opNumber&gt;</td>
<td>11 (Dhcp)</td>
</tr>
<tr>
<td>rttMonEchoAdminProtocol</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.1.&lt;opNumber&gt;</td>
<td>29 (DhcpAppl)</td>
</tr>
<tr>
<td>rttMonCtrlAdminOwner</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.2.&lt;opNumber&gt;</td>
<td>See &quot;OWNER Field Value&quot;</td>
</tr>
<tr>
<td>rttMonCtrlAdminNonce</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.10.&lt;opNumber&gt;</td>
<td>1</td>
</tr>
<tr>
<td>rttMonEchoAdminSourceAddress</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.6.&lt;opNumber&gt;</td>
<td>Source IP (only if specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminTargetAddress</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.2.&lt;opNumber&gt;</td>
<td>DHCP IP</td>
</tr>
<tr>
<td>rttMonCtrlAdminThreshold</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.5.&lt;opNumber&gt;</td>
<td>MAX (WarningRttThreshold,CriticalRttThreshold)</td>
</tr>
<tr>
<td>rttMonCtrlAdminFrequency</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.6.&lt;opNumber&gt;</td>
<td>Frequency (s)</td>
</tr>
<tr>
<td>rttMonCtrlAdminTimeout</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.7.&lt;opNumber&gt;</td>
<td>Frequency * 0.6 (ms)</td>
</tr>
<tr>
<td>rttMonScheduleAdminRttLife</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.1.&lt;opNumber&gt;</td>
<td>Forever</td>
</tr>
</tbody>
</table>
### DNS Operations

<table>
<thead>
<tr>
<th>MIB name</th>
<th>OID number</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonScheduleAdmin inRttStartTime</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.2.&lt;opNumber&gt;</td>
<td>Now</td>
</tr>
<tr>
<td>rttMonCtrlAdminStatus</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.9.&lt;opNumber&gt;</td>
<td>Create &amp; Go (activation)</td>
</tr>
</tbody>
</table>

### DNS Operations

<table>
<thead>
<tr>
<th>MIB name</th>
<th>OID number</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonCtrlAdminRttType</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.4.&lt;opNumber&gt;</td>
<td>8 (Dns)</td>
</tr>
<tr>
<td>rttMonEchoAdminProtocol</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.1.&lt;opNumber&gt;</td>
<td>26 (DnsAppl)</td>
</tr>
<tr>
<td>rttMonCtrlAdminOwner</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.2.&lt;opNumber&gt;</td>
<td>See “OWNER Field Value”</td>
</tr>
<tr>
<td>rttMonCtrlAdminOwner</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.2.&lt;opNumber&gt;</td>
<td>See “OWNER Field Value”</td>
</tr>
<tr>
<td>rttMonCtrlAdminOwner</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.10.&lt;opNumber&gt;</td>
<td>1</td>
</tr>
<tr>
<td>rttMonEchoAdminTargetAddressString</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.11.&lt;opNumber&gt;</td>
<td>Host name to resolve</td>
</tr>
<tr>
<td>rttMonEchoAdminNameServer</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.12.&lt;opNumber&gt;</td>
<td>DNS server IP</td>
</tr>
<tr>
<td>rttMonEchoAdminVrfName</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.12.&lt;opNumber&gt;</td>
<td>VRF name (only if specified)</td>
</tr>
<tr>
<td>rttMonCtrlAdminThreshold</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.5.&lt;opNumber&gt;</td>
<td>MAX (WarningRttThreshold,CriticalRttThreshold)</td>
</tr>
<tr>
<td>rttMonCtrlAdminFrequency</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.6.&lt;opNumber&gt;</td>
<td>Frequency (s)</td>
</tr>
</tbody>
</table>
# Appendix D: How VoIP and Network Quality Manager Creates Operations

<table>
<thead>
<tr>
<th>MIB name</th>
<th>OID number</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonCtrlAdminTime out</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.7.&lt;opNumber&gt;</td>
<td>Frequency * 0.6 (ms)</td>
</tr>
<tr>
<td>rttMonScheduleAdminRttLife</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.1.&lt;opNumber&gt;</td>
<td>Forever</td>
</tr>
<tr>
<td>rttMonScheduleAdminRttStartTime</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.2.&lt;opNumber&gt;</td>
<td>Now</td>
</tr>
<tr>
<td>rttMonCtrlAdminStatus</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.9.&lt;opNumber&gt;</td>
<td>Create &amp; Go (activation)</td>
</tr>
</tbody>
</table>

## FTP Operations

<table>
<thead>
<tr>
<th>MIB name</th>
<th>OID number</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonCtrlAdminRttType</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.4.&lt;opNumber&gt;</td>
<td>12 (Ftp)</td>
</tr>
<tr>
<td>rttMonEchoAdminProtocol</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.1.&lt;opNumber&gt;</td>
<td>30 (FtpAppl)</td>
</tr>
<tr>
<td>rttMonCtrlAdminOwner</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.2.&lt;opNumber&gt;</td>
<td>See “OWNER Field Value”</td>
</tr>
<tr>
<td>rttMonCtrlAdminNvgen</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.10.&lt;opNumber&gt;</td>
<td>1</td>
</tr>
<tr>
<td>rttMonEchoAdminVrfName</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.26.&lt;opNumber&gt;</td>
<td>VRF name (only if specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminSourceAddress</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.6.&lt;opNumber&gt;</td>
<td>Source IP (only if specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminOperation</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.13.&lt;opNumber&gt;</td>
<td>3 (FtpGet)</td>
</tr>
<tr>
<td>rttMonEchoAdminURL</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.15.&lt;opNumber&gt;</td>
<td>Target URL</td>
</tr>
<tr>
<td>MIB name</td>
<td>OID number</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>rttMonCtrlAdminThreshold</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.5.&lt;opNumber&gt;</td>
<td>MAX (WarningRttThreshold,CriticalRttThreshold)</td>
</tr>
<tr>
<td>rttMonCtrlAdminFrequency</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.6.&lt;opNumber&gt;</td>
<td>Frequency (s)</td>
</tr>
<tr>
<td>rttMonCtrlAdminTimeout</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.7.&lt;opNumber&gt;</td>
<td>Frequency * 0.6 (ms)</td>
</tr>
<tr>
<td>rttMonScheduleAdminRttLife</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.1.&lt;opNumber&gt;</td>
<td>Forever</td>
</tr>
<tr>
<td>rttMonScheduleAdminRttStartTime</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.2.&lt;opNumber&gt;</td>
<td>Now</td>
</tr>
<tr>
<td>rttMonCtrlAdminStatus</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.9.&lt;opNumber&gt;</td>
<td>Create &amp; Go (activation in fact)</td>
</tr>
</tbody>
</table>

**HTTP Operations**

<table>
<thead>
<tr>
<th>MIB name</th>
<th>OID number</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonCtrlAdminRttType</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.4.&lt;opNumber&gt;</td>
<td>7 (Http)</td>
</tr>
<tr>
<td>rttMonEchoAdminProtocol</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.1.&lt;opNumber&gt;</td>
<td>25 (HttpAppl)</td>
</tr>
<tr>
<td>rttMonCtrlAdminOwner</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.2.&lt;opNumber&gt;</td>
<td>See “OWNER Field Value”</td>
</tr>
<tr>
<td>rttMonCtrlAdminVgenre</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.10.&lt;opNumber&gt;</td>
<td>1</td>
</tr>
<tr>
<td>rttMonEchoAdminVrfName</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.26.&lt;opNumber&gt;</td>
<td>VRF name (only if specified)</td>
</tr>
</tbody>
</table>
**Appendix D: How VoIP and Network Quality Manager Creates Operations**

<table>
<thead>
<tr>
<th>MIB name</th>
<th>OID number</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonEchoAdminSourceAddress</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.6.&lt;opNumber&gt;</td>
<td>Source IP (only if specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminOperation</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.13.&lt;opNumber&gt;</td>
<td>1 (HttpGet)</td>
</tr>
<tr>
<td>rttMonEchoAdminURL</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.15.&lt;opNumber&gt;</td>
<td>Target URL</td>
</tr>
<tr>
<td>rttMonCtrlAdminThreshold</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.5.&lt;opNumber&gt;</td>
<td>MAX (WarningRttThreshold,CriticalRttThreshold)</td>
</tr>
<tr>
<td>rttMonCtrlAdminFrequency</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.6.&lt;opNumber&gt;</td>
<td>Frequency (s)</td>
</tr>
<tr>
<td>rttMonCtrlAdminTimeout</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.7.&lt;opNumber&gt;</td>
<td>Frequency * 0.6 (ms)</td>
</tr>
<tr>
<td>rttMonScheduleAdminRttLife</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.1.&lt;opNumber&gt;</td>
<td>Forever</td>
</tr>
<tr>
<td>rttMonScheduleAdminRttStartTime</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.2.&lt;opNumber&gt;</td>
<td>Now</td>
</tr>
<tr>
<td>rttMonCtrlAdminStatus</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.9.&lt;opNumber&gt;</td>
<td>Create &amp; Go (activation)</td>
</tr>
</tbody>
</table>

**ICMP Echo Operations**

<table>
<thead>
<tr>
<th>MIB name</th>
<th>OID number</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonCtrlAdminRttType</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.4.&lt;opNumber&gt;</td>
<td>1 (Echo)</td>
</tr>
<tr>
<td>rttMonEchoAdminProtocol</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.1.1.&lt;opNumber&gt;</td>
<td>2 (IPlcmpEcho)</td>
</tr>
<tr>
<td>MIB name</td>
<td>OID number</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>rttMonCtrlAdminOwner</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.2.&lt;opNumber&gt;</td>
<td>See “OWNER Field Value”</td>
</tr>
<tr>
<td>rttMonCtrlAdminNeighbor</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.10.&lt;opNumber&gt;</td>
<td>1</td>
</tr>
<tr>
<td>rttMon Echo Admin VrfName</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.26.&lt;opNumber&gt;</td>
<td>VRF name (only if specified)</td>
</tr>
<tr>
<td>rttMon Echo Admin SourceAddress</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.6.&lt;opNumber&gt;</td>
<td>Source IP (only if specified)</td>
</tr>
<tr>
<td>rttMon Echo Admin TargetAddress</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.2.&lt;opNumber&gt;</td>
<td>Target IP</td>
</tr>
<tr>
<td>rttMonCtrlAdminThreshold</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.5.&lt;opNumber&gt;</td>
<td>MAX (WarningRttThreshold,CriticalRttThreshold)</td>
</tr>
<tr>
<td>rttMonCtrlAdminFrequency</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.6.&lt;opNumber&gt;</td>
<td>Frequency (s)</td>
</tr>
<tr>
<td>rttMonCtrlAdminTimeout</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.7.&lt;opNumber&gt;</td>
<td>Frequency * 0.6 (ms)</td>
</tr>
<tr>
<td>rttMonScheduleAdminInRttLife</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.1.&lt;opNumber&gt;</td>
<td>Forever</td>
</tr>
<tr>
<td>rttMonScheduleAdminInRttStartTime</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.2.&lt;opNumber&gt;</td>
<td>Now</td>
</tr>
<tr>
<td>rttMonCtrlAdminStatus</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.9.&lt;opNumber&gt;</td>
<td>Create &amp; Go (activation in fact)</td>
</tr>
</tbody>
</table>

TCP Connect Operations
# Appendix D: How VoIP and Network Quality Manager Creates Operations

<table>
<thead>
<tr>
<th>MIB name</th>
<th>OID number</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonCtrlAdminRttType</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.4.&lt;opNumber&gt;</td>
<td>6 (TcpConnect)</td>
</tr>
<tr>
<td>rttMonEchoAdminProtocol</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.1.1.&lt;opNumber&gt;</td>
<td>24 (IpTcpConn)</td>
</tr>
<tr>
<td>rttMonCtrlAdminOwner</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.2.&lt;opNumber&gt;</td>
<td>See “OWNER Field Value”</td>
</tr>
<tr>
<td>rttMonCtrlAdminNvgene</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.10.&lt;opNumber&gt;</td>
<td>1</td>
</tr>
<tr>
<td>rttMonEchoAdminVrfName</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.26.&lt;opNumber&gt;</td>
<td>VRF name (only if specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminSourceAddress</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.6.&lt;opNumber&gt;</td>
<td>Source IP (only if specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminTargetAddress</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.2.&lt;opNumber&gt;</td>
<td>Target IP</td>
</tr>
<tr>
<td>rttMonEchoAdminTargetPort</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.25.&lt;opNumber&gt;</td>
<td>Target port</td>
</tr>
<tr>
<td>rttMonCtrlAdminThreshold</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.5.&lt;opNumber&gt;</td>
<td>MAX (WarningRttThreshold,CriticalRttThreshold)</td>
</tr>
<tr>
<td>rttMonCtrlAdminFrequency</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.6.&lt;opNumber&gt;</td>
<td>Frequency (s)</td>
</tr>
<tr>
<td>rttMonCtrlAdminTimeout</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.7.&lt;opNumber&gt;</td>
<td>Frequency * 0.6 (ms)</td>
</tr>
<tr>
<td>rttMonScheduleAdminRttLife</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.1.&lt;opNumber&gt;</td>
<td>Forever</td>
</tr>
<tr>
<td>rttMonScheduleAdminRttStartTime</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.2.&lt;opNumber&gt;</td>
<td>Now</td>
</tr>
</tbody>
</table>
### UDP Echo Operations

<table>
<thead>
<tr>
<th>MIB name</th>
<th>OID number</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonCtrlAdminStatus</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.9.&lt;opNumber&gt;</td>
<td>Create &amp; Go (activation)</td>
</tr>
</tbody>
</table>

#### MIB name Operations

<table>
<thead>
<tr>
<th>MIB name</th>
<th>OID number</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonCtrlAdminRttType</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.4.&lt;opNumber&gt;</td>
<td>5 (UdpEcho)</td>
</tr>
<tr>
<td>rttMonEchoAdminProtocol</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.1.1.&lt;opNumber&gt;</td>
<td>3 (IpUdpEchoAppl)</td>
</tr>
<tr>
<td>rttMonCtrlAdminOwner</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.2.&lt;opNumber&gt;</td>
<td>See “OWNER Field Value”</td>
</tr>
<tr>
<td>rttMonCtrlAdminNvgen</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.10.&lt;opNumber&gt;</td>
<td>1</td>
</tr>
<tr>
<td>rttMonEchoAdminVrfName</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.26.&lt;opNumber&gt;</td>
<td>VRF name (only if specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminSourceAddress</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.6.&lt;opNumber&gt;</td>
<td>Source IP (only if specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminTargetAddress</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.2.&lt;opNumber&gt;</td>
<td>Target IP</td>
</tr>
<tr>
<td>rttMonEchoAdminTargetPort</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.5.&lt;opNumber&gt;</td>
<td>Target port</td>
</tr>
<tr>
<td>rttMonCtrlAdminThreshold</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.5.&lt;opNumber&gt;</td>
<td>MAX (WarningRttThreshold,CriticalRttThreshold)</td>
</tr>
<tr>
<td>rttMonCtrlAdminFrequency</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.6.&lt;opNumber&gt;</td>
<td>Frequency (s)</td>
</tr>
</tbody>
</table>
## Appendix D: How VoIP and Network Quality Manager Creates Operations

### MIB name | OID number | Value
--- | --- | ---
rttMonCtrlAdminTim | 1.3.6.1.4.1.9.9.42.1.2.1.1.7.<opNumber> | Frequency * 0.6 (ms)
rttMonScheduleAdminRttLife | 1.3.6.1.4.1.9.9.42.1.2.5.1.1.<opNumber> | Forever
rttMonScheduleAdminRttStartTime | 1.3.6.1.4.1.9.9.42.1.2.5.1.2.<opNumber> | Now
rttMonCtrlAdminStatus | 1.3.6.1.4.1.9.9.42.1.2.1.1.9.<opNumber> | Create & Go (activation in fact)

### UDP Jitter Operations

| MIB name | OID number | Value |
--- | --- | ---
rttMonCtrlAdminRttType | 1.3.6.1.4.1.9.9.42.1.2.1.1.4.<opNumber> | 9 (Jitter)
rttMonEchoAdminProtocol | 1.3.6.1.4.1.9.9.42.1.2.2.1.1.<opNumber> | 27 (JitterAppl)
rttMonCtrlAdminOwner | 1.3.6.1.4.1.9.9.42.1.2.1.1.2.<opNumber> | See “OWNER Field Value”
rttMonCtrlAdminVrgeen | 1.3.6.1.4.1.9.9.42.1.2.1.1.10.<opNumber> | 1
rttMonEchoAdminVrfName | 1.3.6.1.4.1.9.9.42.1.2.2.1.26.<opNumber> | VRF name (only if specified)
rttMonEchoAdminSourceAddress | 1.3.6.1.4.1.9.9.42.1.2.2.1.6.<opNumber> | Source IP (only if specified)
rttMonEchoAdminSourcePort | 1.3.6.1.4.1.9.9.42.1.2.2.1.7.<opNumber> | Source port
rttMonEchoAdminTargetAddress | 1.3.6.1.4.1.9.9.42.1.2.2.1.2.<opNumber> | Target IP
<table>
<thead>
<tr>
<th>MIB name</th>
<th>OID number</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonEchoAdminTargetPort</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.5.&lt;opNumber&gt;</td>
<td>Target port</td>
</tr>
<tr>
<td>rttMonEchoAdminTOS</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.9.&lt;opNumber&gt;</td>
<td>Type Of Service (if specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminPktDataRequestSize</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.3.&lt;opNumber&gt;</td>
<td>100</td>
</tr>
<tr>
<td>rttMonEchoAdminNumPackets</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.18.&lt;opNumber&gt;</td>
<td>100</td>
</tr>
<tr>
<td>rttMonEchoAdminInterval</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.17.&lt;opNumber&gt;</td>
<td>20</td>
</tr>
<tr>
<td>rttMonCtrlAdminThreshold</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.5.&lt;opNumber&gt;</td>
<td>MAX (WarningRttThreshold,CriticalRttThreshold)</td>
</tr>
<tr>
<td>rttMonCtrlAdminFrequency</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.6.&lt;opNumber&gt;</td>
<td>Frequency (s)</td>
</tr>
<tr>
<td>rttMonCtrlAdminTimeOut</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.7.&lt;opNumber&gt;</td>
<td>Frequency * 0.6 (ms)</td>
</tr>
<tr>
<td>rttMonScheduleAdminRttLife</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.1.&lt;opNumber&gt;</td>
<td>Forever</td>
</tr>
<tr>
<td>rttMonScheduleAdminRttStartTime</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.2.&lt;opNumber&gt;</td>
<td>Now</td>
</tr>
<tr>
<td>rttMonCtrlAdminStatus</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.9.&lt;opNumber&gt;</td>
<td>Create &amp; Go (activation)</td>
</tr>
</tbody>
</table>

VoIP UDP Jitter Operations
## Appendix D: How VoIP and Network Quality Manager Creates Operations

<table>
<thead>
<tr>
<th>MIB name</th>
<th>OID number</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonCtrlAdminRttType</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.4.&lt;opNumber&gt;</td>
<td>9 (Jitter)</td>
</tr>
<tr>
<td>rttMonEchoAdminProtocol</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.1.&lt;opNumber&gt;</td>
<td>27 (JitterAppl)</td>
</tr>
<tr>
<td>rttMonCtrlAdminOwner</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.2.&lt;opNumber&gt;</td>
<td>See “OWNER Field Value”</td>
</tr>
<tr>
<td>rttMonCtrlAdminNgegen</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.10.&lt;opNumber&gt;</td>
<td>1</td>
</tr>
<tr>
<td>rttMonEchoAdminVrfName</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.26.&lt;opNumber&gt;</td>
<td>VRF name (only if specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminSourceAddress</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.6.&lt;opNumber&gt;</td>
<td>Source IP (only if specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminSourcePort</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.7.&lt;opNumber&gt;</td>
<td>Source port</td>
</tr>
<tr>
<td>rttMonEchoAdminTargetAddress</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.2.&lt;opNumber&gt;</td>
<td>Target IP</td>
</tr>
<tr>
<td>rttMonEchoAdminTargetPort</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.5.&lt;opNumber&gt;</td>
<td>Target port</td>
</tr>
<tr>
<td>rttMonEchoAdminTOS</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.9.&lt;opNumber&gt;</td>
<td>Type Of Service (if specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminCodecType</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.27.&lt;opNumber&gt;</td>
<td>Codec type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 = NA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = G711ULAW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 = G711ALAW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 = G729A</td>
</tr>
<tr>
<td>MIB name</td>
<td>OID number</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>rttMonEchoAdminCodecPayload</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.29.&lt;opNumber&gt;</td>
<td>100 (if codec specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminPktDataRequestSize</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.3.&lt;opNumber&gt;</td>
<td>100 (if no codec specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminCodecNumPackets</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.30.&lt;opNumber&gt;</td>
<td>100 (if codec specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminNumPackets</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.18.&lt;opNumber&gt;</td>
<td>100 (if no codec specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminCodecInterval</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.28.&lt;opNumber&gt;</td>
<td>20 (if codec specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminInterval</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.17.&lt;opNumber&gt;</td>
<td>20 (if no codec specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminICPIFAdvFactor</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.31.&lt;opNumber&gt;</td>
<td>0 by default, configurable internally</td>
</tr>
<tr>
<td>rttMonCtrlAdminThreshold</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.5.&lt;opNumber&gt;</td>
<td>MAX (WarningRttThreshold,CriticalRttThreshold)</td>
</tr>
<tr>
<td>rttMonCtrlAdminFrequency</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.6.&lt;opNumber&gt;</td>
<td>Frequency (s)</td>
</tr>
<tr>
<td>rttMonCtrlAdminTimeout</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.7.&lt;opNumber&gt;</td>
<td>Frequency * 0.6 (ms)</td>
</tr>
<tr>
<td>rttMonScheduleAdminRttLife</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.1.&lt;opNumber&gt;</td>
<td>Forever</td>
</tr>
<tr>
<td>rttMonScheduleAdminRttStartTime</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.2.&lt;opNumber&gt;</td>
<td>Now</td>
</tr>
<tr>
<td>rttMonCtrlAdminStatus</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.9.&lt;opNumber&gt;</td>
<td>Create &amp; Go (activation in fact)</td>
</tr>
</tbody>
</table>
Appendix D: How VoIP and Network Quality Manager Creates Operations

**CLI-Based Operations**

The following examples list the commands that are used to create new CLI-based operations:

- **ICMP Path Echo Operations**
- **ICMP Path Jitter Operations**

**ICMP Path Echo Operations**

**IP SLA Syntax**

```plaintext
configure terminal
ip sla <opNumber>
path-echo <dest_IP> [source-ip <source_IP>]
owner <swIdentifier>
threshold <threshold> # MAX(WarningRttThreshold, CriticalRttThreshold)
frequency <frequencyMs>
vrf <vrfName> # VRF name (only if specified)
tos <typeOfService> # Type Of Service (only if specified)
history filter all
history buckets-kept 1
history lives-kept 1
samples-of-history-kept 30
exit
ip sla schedule <opNumber> life forever start-time now
exit
```

**IP SLA Monitor Syntax**
configure terminal
ip sla monitor <opNumber>
type pathEcho protocol ipIcmpecho <dest_IP> [source-ipaddr <source_IP>]
owner <swIdentifier>
threshold <threshold> MAX(WarningRttThreshold, CriticalRttThreshold)
frequency <frequencyMs>
vrf <vrfName> VRF name (only if specified)
tos <typeOfService> Type Of Service (only if specified)
filter-for-history all
buckets-of-history-kept 1
lives-of-history-kept 1
samples-of-history-kept 30
exit
ip sla monitor schedule <opNumber> life forever start-time now
exit

RTR Syntax

configure terminal
rtr <opNumber>
type pathEcho protocol ipIcmpecho <dest_IP> [source-ipaddr <source_IP>]
owner <swIdentifier>
threshold <threshold> MAX(WarningRttThreshold, CriticalRttThreshold)
frequency <frequencyMs>
vrf <vrfName> VRF name (only if specified)
tos <typeOfService> Type Of Service (only if specified)
filter-for-history all
buckets-of-history-kept 1
lives-of-history-kept 1
samples-of-history-kept 30
exit
rtr schedule <opNumber> life forever start-time now
exit

ICMP Path Jitter Operations

IP SLA Syntax
Appendix D: How VoIP and Network Quality Manager Creates Operations

configure terminal
ip sla <opNumber>
path-jitter <dest_IP> [source-ip <source_IP>]
owner <swIdentifier>
threshold <threshold># MAX(WARNING RTT THRESHOLD, CRITICAL RTT THRESHOLD)
frequency <frequencyMs>
vrf <vrfName># VRF name (only if specified)
tos <typeOfService># Type Of Service (only if specified)
history filter all
history buckets-kept 1
history lives-kept 1
samples-of-history-kept 30
exit
ip sla schedule <opNumber> life forever start-time now
exit

IP SLA Monitor Syntax

configure terminal
ip sla monitor <opNumber>
type pathJitter dest-ipaddr <dest_IP> [source-ipaddr <source_IP>]
owner <swIdentifier>
threshold <threshold># MAX(WARNING RTT THRESHOLD, CRITICAL RTT THRESHOLD)
frequency <frequencyMs>
vrf <vrfName># VRF name (only if specified)
tos <typeOfService># Type Of Service (only if specified)
filter-for-history all
buckets-of-history-kept 1
lives-of-history-kept 1
samples-of-history-kept 30
exit
ip sla monitor schedule <opNumber> life forever start-time now
now
exit

RTR Syntax
configure terminal
rtr <opNumber>
type pathJitter dest-ipaddr <dest_IP> [source-ipaddr <source_IP>]
owner <swIdentifier>
threshold <threshold> MAX(WarningRttThreshold, CriticalRttThreshold)
frequency <frequencyMs>
vrf <vrfName> VRF name (only if specified)
tos <typeOfService> Type Of Service (only if specified)
filter-for-history all
buckets-of-history-kept 1
lives-of-history-kept 1
samples-of-history-kept 30
exit
rtr schedule <opNumber> life forever start-time now
exit
Appendix E: Database Maintenance

The primary tasks that are available for maintaining an SQL database are data summarization and database compaction. Data summarization occurs automatically as part of the nightly maintenance program. You can also run database maintenance on demand from the Windows Start menu.

Running Database Maintenance

Database maintenance performs a series of data summarizations that help you optimize the size of your database. Data summarization consists of gathering all the collected network data for a defined period of time, calculating statistics from the data, and then discarding the data itself while retaining the statistics. By regularly running database maintenance, you can realize significant space savings and performance improvements.

Database maintenance can either be run directly from the Start menu, or scheduled for a set Archive Time and initiated from the Poller Settings view in the Web Console. In either case, after it is started, database maintenance normally proceeds without further attention. The following procedure provides the steps to perform Database Maintenance.

**Note:** Administrative privileges are required to run Database Maintenance.

**To run the Database Maintenance utility:**

1. **If you want to run database Maintenance from the Web Console,** complete the following steps:
   a. Click **Settings** in the top right of the web console, and then click **Poller Settings** in the Settings group.
   b. Click **Perform Maintenance Now** in the Database Settings area.

2. **If you want to run database Maintenance from the Start menu,** click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Maintenance**, and then click **Start**.