VoIP and Network Quality Manager

Version 4.6
© 2019 SolarWinds Worldwide, LLC. All rights reserved.

This document may not 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 prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. 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, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or 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 or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.
# Table of Contents

**SolarWinds VNQM tips and tricks** ................................................................. 8

**How SolarWinds VNQM works** ................................................................. 9

  - Why install SolarWinds VNQM .............................................................. 9
  - What SolarWinds VNQM does .............................................................. 9

**Configure SolarWinds VNQM** ................................................................. 12

  - IP SLA management in SolarWinds VNQM ......................................... 12
  - Quality of Service and IP SLAs in SolarWinds VNQM ........................... 13
    - IP SLA Operations in VNQM ............................................................ 13
  - Quality of Service metrics in SolarWinds VNQM .................................. 14
  - Polling intervals for IP SLA operations in SolarWinds VNQM ............... 19
  - Designate paths in SolarWinds VNQM .............................................. 20
  - Understand the impact IP SLA operations have on your network ........... 21
  - Configure devices for IP SLA operations .......................................... 23
    - Configure devices for ICMP echo path operations ........................... 23
  - Add IP SLA nodes to SolarWinds VNQM ........................................... 24
    - Requirements .................................................................................... 24
    - Discover IP SLA-capable nodes automatically .................................. 24
    - Add IP SLA-capable nodes manually .............................................. 25
    - Configure CLI credentials in SolarWinds VNQM ............................... 27
  - Add IP SLA operations ........................................................................ 28
    - Add DNS IP SLA operations to devices ............................................ 28
    - Add FTP IP SLA operations to devices ............................................. 29
    - Add HTTP IP SLA operations to devices .......................................... 30
    - Add DHCP IP SLA operations to devices ......................................... 31
    - Add TCP Connect IP SLA operations to devices ................................ 32
    - Add UDP Jitter IP SLA operations to devices .................................... 34
    - Add VoIP UDP Jitter IP SLA operations to devices ............................ 35
    - Add ICMP Echo IP SLA operations to devices ................................... 36
Add UDP Echo IP SLA operations to devices ................................................................. 40
Add ICMP Path Echo operations to devices ................................................................. 41
Add ICMP Path Jitter operations to devices ................................................................. 43
Add existing operations to SolarWinds® VoIP and Network Quality Manager (VNQM) ..... 44
Edit IP SLA operations .................................................................................................. 45
Modify the SLA location ............................................................................................... 45
Rename operations in SolarWinds VNQM ..................................................................... 45
Delete IP SLA operations .............................................................................................. 46
VoIP management in SolarWinds VNQM ..................................................................... 46
Manage call managers ................................................................................................. 47
   CLI credentials ......................................................................................................... 47
   Credentials used for Cisco CallManager .................................................................. 47
   Monitor CallManager health ..................................................................................... 48
SIP monitoring on Cisco CallManagers ....................................................................... 48
Add Cisco CallManager devices to SolarWinds VNQM ................................................. 49
Add CallManager Express devices to SolarWinds VNQM ............................................ 53
Manage Avaya Call Managers ..................................................................................... 53
   Avaya CDR parameters ......................................................................................... 56
   Add Avaya Call Manager devices to SolarWinds VNQM ........................................ 57
Polling bandwidth for Avaya Communication and Media Servers ............................. 60
Add call manager devices from other manufacturers ................................................. 61
Define FTP servers ....................................................................................................... 61
Configure Cisco CallManagers for FTP ...................................................................... 61
Edit call managers ........................................................................................................ 62
Call Manager CDR/CMR Polling ................................................................................ 63
SIP Polling Settings ....................................................................................................... 63
   AXL Credentials .................................................................................................... 63
   FTP Server Settings ............................................................................................... 63
   Call Manager CDR/CQR Polling .......................................................................... 64
   Call Manager CLI Credentials ............................................................................. 64
Delete call manager devices from SolarWinds VNQM ......................................................... 65
Manage gateways in SolarWinds VNQM ........................................................................... 65
Add gateways to SolarWinds VNQM ............................................................................... 65
Edit VoIP gateways ........................................................................................................... 66
Edit CLI credentials for gateway nodes ........................................................................... 67
Remove gateways ............................................................................................................... 67
SIP monitoring on Cisco CUBE devices .......................................................................... 68
Select the VoIP infrastructure ......................................................................................... 70
Call precedence levels ..................................................................................................... 70
SolarWinds VNQM settings ............................................................................................... 71
IP SLA Management ........................................................................................................ 71
  Manage IP SLA Operations ............................................................................................ 71
  Manage IP SLA Nodes ..................................................................................................... 71
VoIP Management ............................................................................................................ 71
  Manage CallManager Nodes .......................................................................................... 72
  Manage VoIP Gateways ................................................................................................. 72
Select VoIP Infrastructure ................................................................................................. 72
Details ................................................................................................................................. 72
  Edit VoIP & Network Quality Manager Settings .......................................................... 72
  Database Details ............................................................................................................. 73
Configure SolarWinds VNQM settings ........................................................................... 73
Set the traffic precedence in SolarWinds VNQM .............................................................. 74
Use SolarWinds VNQM ...................................................................................................... 76
  Start SolarWinds VNQM ............................................................................................... 76
  SolarWinds VNQM views ............................................................................................. 76
Customize charts in SolarWinds VNQM .......................................................................... 80
  Customize chart titles in SolarWinds VNQM ............................................................... 80
  Calculated series in SolarWinds VNQM ....................................................................... 80
  Time period in SolarWinds VNQM .............................................................................. 81
  Sample interval in SolarWinds VNQM ......................................................................... 81
Chart size in SolarWinds VNQM ................................................................. .81
Data tables in SolarWinds VNQM ............................................................ .81
Font size in SolarWinds VNQM ................................................................. .82
Printing options ....................................................................................... .82
Data export options ................................................................................ .82
Advanced chart settings in SolarWinds VNQM ....................................... .82
Use custom properties for SolarWinds VNQM ...................................... .82
Advanced alerts and actions in SolarWinds VNQM ............................... .83
SolarWinds VNQM reports ...................................................................... .83
Use predefined SolarWinds VNQM reports ........................................... .83
    Historical IP SLA Operation reports .................................................. .84
    Historical VoIP reports ...................................................................... .87
    Historical SIP Trunk reports ............................................................... .87
    VNQM Connected Devices reports .................................................... .88
SolarWinds VNQM Maps ....................................................................... .88
SolarWinds VNQM map variables ........................................................... .88

**MIBs Maintained by SolarWinds VNQM** ............................................. .90

General .................................................................................................... .90
All Operations ........................................................................................ .90
DHCP Operations .................................................................................. .91
DNS Operations ..................................................................................... .91
HTTP and FTP Operations .................................................................... .91
ICMP Echo Operations .......................................................................... .91
TCP Connect Operations ....................................................................... .91
UDP Jitter Operations ........................................................................... .91
VoIP UDP Jitter Operations ................................................................... .92
VoIP Specific MIBs ................................................................................ .92

**Supported versions of Cisco Unified CallManager** ............................... .93

OIDs from the ccmTable .......................................................................... .93
OIDs from the ccmRegionTable .............................................................. .93
OIDs from the ccmGatewayTable ................................................................. 94
OIDs from the ccmProductTypeTable ............................................................ 94
OIDs from the ccmPhoneTable .................................................................... 94
OIDs from the ccmPhoneExtnTable .............................................................. 95
OIDs from the ccmH323DeviceTable .............................................................. 95

How SolarWinds VNQM creates operations ............................................... 96

Owner Field Value .................................................................................... 96

SNMP-based operations ............................................................................. 96

DHCP operations ....................................................................................... 96
DNS operations ......................................................................................... 97
FTP operations ........................................................................................ 98
HTTP operations ...................................................................................... 99
ICMP Echo operations .............................................................................. 100
TCP Connect operations ......................................................................... 101
UDP Echo operations ............................................................................... 102
UDP Jitter operations ............................................................................... 103
VoIP UDP Jitter operations ..................................................................... 104

CLI-based operations ............................................................................... 106

ICMP Path Echo operations ..................................................................... 106

IP SLA Syntax ........................................................................................ 106
IP SLA Monitor Syntax ............................................................................ 107
RTR Syntax ............................................................................................. 107

ICMP Path Jitter operations .................................................................... 108

IP SLA Syntax ........................................................................................ 108
IP SLA Monitor Syntax ............................................................................ 108
RTR Syntax ............................................................................................. 109
SolarWinds VNQM tips and tricks

- SolarWinds 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 Configure Cisco CallManagers for FTP.
- To find the necessary balance between server load and data granularity, try using different polling intervals. For more information, see Configure SolarWinds VNQM settings.
- Configure the length of time performance data is retained to balance database maintenance with IP SLA requirements. For more information, see Configure SolarWinds VNQM settings.
How SolarWinds VNQM works

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.

The following sections provide more details about the following topics:

- Why Install SolarWinds VNQM
- What SolarWinds VNQM Does

Why install SolarWinds VNQM

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. SolarWinds 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. SolarWinds VoIP and Network Quality Manager can also be used in integration with SolarWinds Network Performance Monitor, leveraging the SolarWinds NPM monitoring options to provide a better overview of your network.

What SolarWinds VNQM does

With SolarWinds VoIP and Network Quality Manager you can monitor and report both real-time and historical performance statistics for your IP SLA-capable network. SolarWinds 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

SolarWinds 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. SolarWinds VoIP and Network Quality Manager collects IP SLA data and then presents it in the easy-to-use Web Console environment. With SolarWinds 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](http://www.cisco.com/go/ipsla).
VoIP Phone Troubleshooting

SolarWinds 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 SolarWinds VoIP and Network Quality Manager, you can drill in to problem areas to start identifying the underlying problems.

Custom Charts and Gauges

SolarWinds 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 gauges of key IP SLA metrics such as jitter, latency, packet loss, and MOS. With custom charts, you can easily track the historical performance of all the paths on your network.

Custom Alerts and Actions

SolarWinds VoIP and Network Quality Manager enables you to create custom alerts for your network in the same way you create alerts and actions in SolarWinds Network Performance Monitor. Specifically, you can configure IP SLA-related alerts with a variety of corresponding actions to notify you of events on your network. For more information, see Creating and Managing Alerts.

Custom Reporting

With web-based reporting within the Orion Web Console, SolarWinds VoIP and Network Quality Manager provides real-time and historical statistics reporting for the IP SLA-specific network statistics. When you install VNQM, several predefined reports become available. 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, see Reports.

Gateway Monitoring

SolarWinds 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. SolarWinds 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 SolarWinds VoIP and Network Quality Manager, you immediately know the status of your VoIP network and all of its components at any time.

SolarWinds 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>
<tbody>
<tr>
<td>Custom MIB Pollers</td>
<td>See Monitoring MIBs with Universal Device Pollers.</td>
</tr>
<tr>
<td>Cisco CallManager supported devices</td>
<td>Search for &quot;CallManager&quot; at <a href="http://www.cisco.com">www.cisco.com</a>.</td>
</tr>
<tr>
<td>Adding Cisco CallManager devices</td>
<td>See Managing CallManagers.</td>
</tr>
<tr>
<td>Adding Avaya Call Manager devices</td>
<td>See Add Avaya Call Manager devices to SolarWinds VNQM.</td>
</tr>
<tr>
<td>Monitoring call manager devices from other manufacturers</td>
<td>See Adding call manager devices from other manufacturers.</td>
</tr>
</tbody>
</table>
Configure SolarWinds VNQM

VNQM monitors 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 in to your SolarWinds VoIP and Network Quality Manager server.
2. Start the Orion Web Console in the Orion program folder.
3. Click My Dashboards > VoIP & Network Quality.

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

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

- **IP SLA management in SolarWinds VNQM** - configuring your IP SLA devices and IP SLA operations
- **VoIP management in SolarWinds VNQM** - configuring your call managers, gateways, and defining VoIP infrastructure
- **SolarWinds VNQM settings** - configuring database, polling and monitoring settings

**IP SLA management in SolarWinds VNQM**

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 [Quality of Service and IP SLAs in SolarWinds VNQM](#).

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 [Configure devices for IP SLA operations](#).
2. Add devices that you want to monitor to your database. For more information, see [Adding Devices for Monitoring in the Web Console](#).
3. Add your devices as IP SLA nodes into VNQM. For more information, see [Add IP SLA nodes to SolarWinds VNQM](#).
4. Define IP SLA operations to be monitored by VNQM. For more information, see [Add IP SLA operations](#).
Related tasks:
- Edit IP SLA operations
- Delete IP SLA operations

Quality of Service and IP SLAs in SolarWinds VNQM

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 SolarWinds 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 SolarWinds VoIP and Network Quality Manager.

- **DHCP**: measures the response time taken to discover a DHCP server, and then obtain a leased IP address from it.
- **DNS**: measures the difference in time from when a DNS request is sent and when the reply is received.
- **FTP**: measures the response time between a Cisco device and an FTP server to retrieve a file.
- **HTTP**: measures distributed web services response times.
- **ICMP Echo**: measures round trip time between nodes on the network.
- **ICMP Path Echo**: measures round trip time hop-by-hop between nodes on the network.
- **ICMP Path Jitter**: measures WAN quality by testing connection times hop-by-hop between two devices.
- **TCP Connect**: measures WAN quality by testing connection times between two devices using a specific port.
- **UDP Echo**: measures round trip time between nodes on the network.
- **UDP Jitter**: measures WAN quality by testing connection times between two devices using a specific port number.
- **VoIP UDP Jitter**: measures call path metrics on the VoIP network.
Quality of Service metrics in SolarWinds VNQM

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

- **Latency in SolarWinds VNQM**
- **Jitter in SolarWinds VNQM**
- **Packet Loss in SolarWinds VNQM**
- **Mean Opinion Score (MOS) in SolarWinds VNQM**

Latency in SolarWinds VNQM

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 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 T1 is applied to a test packet as it leaves the source router.
2. Time stamp T2 is applied as the test packet arrives at the target router.
3. Time stamp T3 is applied as the test packet leaves the target router to return to the source.
4. Time stamp T4 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>

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.

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

```java
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

<table>
<thead>
<tr>
<th>Object</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>rttMonLatestJitterOperNumOfRTT</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.1</td>
</tr>
<tr>
<td>rttMonLatestJitterOperRTTSum</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.2</td>
</tr>
<tr>
<td>rttMonEchoAdminPrecision</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.37</td>
</tr>
<tr>
<td>rttMonLatestJitterOperOWSumSD</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.33</td>
</tr>
<tr>
<td>rttMonLatestJitterOperNumOfOW</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.41</td>
</tr>
<tr>
<td>rttMonLatestJitterOperOWSumDS</td>
<td>1.3.6.1.4.1.9.9.42.1.5.2.1.37</td>
</tr>
</tbody>
</table>

Jitter in SolarWinds VNQM

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 SolarWinds 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.

SolarWinds 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.
### CODEC  |  IP SLA OPERATION FREQUENCY (F)  |  DEFAULT NUMBER OF PACKETS (N)  |  DEFAULT PACKET SIZE (S)  |  DEFAULT INTERVAL BETWEEN PACKETS (I)
---|---|---|---|---
G.711a  |  Set on each operation as the network test interval  |  1000  |  160 + 12 RTP bytes  |  20 ms
G.711u  |  |  1000  |  160 + 12 RTP bytes  |  20 ms
G.729a  |  |  1000  |  20 + 12 RTP bytes  |  20 ms

For more information about configurable settings within SolarWinds VoIP and Network Quality Manager, see [Configure SolarWinds VNQM settings](#).

Based on the Cisco® IP SLA operations used by SolarWinds 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.

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

\[
\text{jitter}_{SD} = \frac{\text{rttMonLatestJitterOperSumOfPositives}_{SD} + \text{rttMonLatestJitterOperSumOfNegatives}_{SD}}{\text{rttMonLatestJitterOperNumOfPositives}_{SD} + \text{rttMonLatestJitterOperNumOfNegatives}_{SD}}
\]

\[
\text{jitter}_{DS} = \frac{\text{rttMonLatestJitterOperSumOfPositives}_{DS} + \text{rttMonLatestJitterOperSumOfNegatives}_{DS}}{\text{rttMonLatestJitterOperNumOfPositives}_{DS} + \text{rttMonLatestJitterOperNumOfNegatives}_{DS}}
\]

\[
\text{Jitter} = \frac{\text{rttMonLatestJitterOperSumOfPositives}_{SD} + \text{rttMonLatestJitterOperSumOfNegatives}_{SD} + \text{rttMonLatestJitterOperSumOfPositives}_{DS} + \text{rttMonLatestJitterOperSumOfNegatives}_{DS}}{\text{rttMonLatestJitterOperNumOfPositives}_{SD} + \text{rttMonLatestJitterOperNumOfNegatives}_{SD} + \text{rttMonLatestJitterOperNumOfPositives}_{DS} + \text{rttMonLatestJitterOperNumOfNegatives}_{DS}}
\]

| . | 1.3.6.1.4.1.9.9.42.1.5.2.1.9 |
| . | 1.3.6.1.4.1.9.9.42.1.5.2.1.14 |
| . | 1.3.6.1.4.1.9.9.42.1.5.2.1.8 |
| . | 1.3.6.1.4.1.9.9.42.1.5.2.1.13 |
| . | 1.3.6.1.4.1.9.9.42.1.5.2.1.19 |
| . | 1.3.6.1.4.1.9.9.42.1.5.2.1.24 |
| . | 1.3.6.1.4.1.9.9.42.1.5.2.1.18 |
SolarWinds 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 in SolarWinds VNQM

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.

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

```python
if (rttMonLatestJitterOperPacketLossSD + rttMonLatestJitterOperPacketLossDS + rttMonLatestJitterOperPacketMIA <> 0)
else
    packetLoss = 0

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

if (rttMonLatestJitterOperPacketLossDS + (rttMonLatestJitterOperPacketMIA/2) + ((rttMonLatestJitterOperPacketLateArrival + rttMonLatestJitterOperPacketOutOfSequence + rttMonLatestJitterOperNumOfRTT)/2) <> 0)
packetLossDS = (rttMonLatestJitterOperPacketLossDS +
  (rttMonLatestJitterOperPacketMIA/2) + ((rttMonLatestJitterOperPacketLateArrival
  + rttMonLatestJitterOperPacketOutOfSequence +
  rttMonLatestJitterOperNumOfRTT)) * 100 / (rttMonLatestJitterOperPacketLossDS
  + (rttMonLatestJitterOperPacketMIA/2))
else
  packetLossDS = 0

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></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>

Mean Opinion Score (MOS) in SolarWinds VNQM

MOS is an industry standard measure of call quality expressed on a scale of increasing perceived quality, from one to five. SolarWinds 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 SolarWinds 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 SolarWinds 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>COMMUNICATION SYSTEM TYPE EXAMPLES</td>
<td>MAXIMUM ADVANTAGE FACTOR VALUE</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>-------------------------------</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 SolarWinds VNQM](https://www.solarwinds.com).

For more information about SolarWinds VoIP and Network Quality Manager settings, see [Configure SolarWinds VNQM settings](https://www.solarwinds.com).

Polling intervals for IP SLA operations in SolarWinds VNQM

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

SolarWinds 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 $\leq 1$ min
- $1$ min $< $ Polling interval $\leq 3$ min
- $3$ min $< $ Polling interval $\leq 6$ min
- $6$ min $< $ Polling interval

For any given group of operations, SolarWinds 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 $\leq 1$ minute. The polling interval of Operation A is 30 seconds, and the polling interval of operation B is 1 minute. SolarWinds 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.

1. If you want to change a polling interval for an operation, you have to do it in your database.
2. 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. Click Settings > All Settings > VoIP & Quality settings.
2. Click Edit or delete operations.
3. On the Manage IP SLA Operations page, select an operation, and click Edit. You can check the polling interval in the Frequency field.

Designate paths in SolarWinds VNQM

For some of the SLA operations used by SolarWinds 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, SolarWinds VoIP and Network Quality Manager provides an easy-to-use interface for selecting paths for monitoring. When configuring IP SLA operations, SolarWinds VoIP and Network Quality Manager offers the following options for establishing monitoring:

**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.
Understand 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 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 = 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 $40 \times 39/2 = 780$ 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:

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, SolarWinds 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.

Configure devices for IP SLA operations

Cisco® IP Service Level Agreements (IP SLAs) are the primary means by which SolarWinds 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, SolarWinds VoIP and Network Quality Manager can automatically add IP SLA operations to your network devices and start monitoring those operations immediately.

Configure 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 [Cisco website](https://www.cisco.com).

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
```
Add IP SLA nodes to SolarWinds VNQM

Before you create and monitor IP SLA operations, you must add your IP SLA-capable routers to SolarWinds VoIP and Network Quality Manager.

For more information about the management information bases (MIBs) referenced by VNQM, see [MIBs Maintained by SolarWinds VNQM](#).

Requirements

- Source devices must first be added to the database before you can add them to SolarWinds VoIP and Network Quality Manager. For more information about adding nodes, see [Adding Devices for Monitoring in the Web Console](#).
- 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](#), and search for IP SLAs - DHCP Operation.

The following sections describe tasks connected with adding IP SLA Nodes to VNQM:

- [Discover IP SLA-capable nodes automatically](#)
- [Add IP SLA-capable nodes manually](#)
- [Configure CLI credentials in SolarWinds VNQM](#)

Discover IP SLA-capable nodes automatically

To add more nodes at once, complete the following procedure to automatically discover and add nodes to SolarWinds VoIP and Network Quality Manager.

1. Log in to your SolarWinds VoIP and Network Quality Manager server as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Automatically discover IP SLA capable nodes.
4. Click Start IP SLA Discovery.
5. When the discovery has finished, click No, I want to exit this wizard, and click Next.

Add IP SLA-capable nodes manually

To add individual nodes, complete the following procedure.

1. Log in to SolarWinds VNQM as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.

   ![PRODUCT SPECIFIC SETTINGS]

   Global and product specific settings such as session times, bandwidth monitoring, triggers, and more.

   - IPAM Settings
   - VoIP & Quality Settings
   - Web Console Settings

3. Click Manually Add Nodes to VoIP and Network Quality Manager.

   ![Manage IP SLA Nodes]

   Add Nodes to VoIP and Network Quality Manager. Only VoIP and Network Quality Manager license count.

   - Automatically Discover IP SLA capable nodes
   - Manually Add Nodes to VoIP and Network Quality Manager
   - Remove nodes from VoIP and Network Quality Manager

4. Select the nodes you want to add, and click Add Nodes.

   The list of nodes includes only Cisco® routers that support SNMP v2 and later. The system checks to ensure that SolarWinds VNQM can write to the node.

   In this example, the dev_ottawa_2621 router is added to SolarWinds VNQM.
5. If you are prompted to enter credentials that include write privileges:
   a. Select the node.
   b. Click Edit Credentials.
   c. If SNMP v2 is used, set the SNMP version and port number in the associated fields, enter the read/write community string, click Test, and click Save.
d. If SNMP v3 is used, select a saved credential set from the list, or enter the credentials in the provided fields, click Test, and click Save.

On the SNMP Credentials Issues page, the system displays IP SLA capability test succeeded in the Status column.

6. On the SNMP Credentials Issues page, click Add Selected Nodes.
When the system adds the node, a message is displayed.

Configure CLI credentials in SolarWinds VNQM

Some IP SLA operations require command line interface (CLI) login credentials in order to configure the operations on your routers.

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

1. Log in to your SolarWinds VoIP and Network Quality Manager server as an administrator.
2. Click Settings > All Settings > 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 click Edit Node.
5. Enter the name of the credential set in the Credentials Name field to create a new set.
6. Enter the user name and password in the associated fields.
7. Enter the enable level to use when logging in.
   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. Enter the password associated with the enable level to use when logging in.

9. Expand Advanced, and select the protocol, port number, and connection timeout you want to use when connecting to your network devices.

10. Test the credentials, and click Save.

**Add 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.

- 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 SolarWinds 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.

The following sections describe the process of adding individual operations to VNQM in detail:

- Add DNS IP SLA operations to devices
- Add FTP IP SLA operations to devices
- Add HTTP IP SLA operations to devices
- Add DHCP IP SLA operations to devices
- Add TCP Connect IP SLA operations to devices
- Add UDP Jitter IP SLA operations to devices
- Add VoIP UDP Jitter IP SLA operations to devices
- Add ICMP Echo IP SLA operations to devices
- Add UDP Echo IP SLA operations to devices
- Add ICMP Path Echo operations to devices
- Add ICMP Path Jitter operations to devices
- Add existing operations to SolarWinds® VoIP and Network Quality Manager (VNQM)

**Add DNS IP SLA operations to 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.
You cannot add operations that have been previously created with SolarWinds 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 in to your SolarWinds VoIP and Network Quality Manager server as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. In the Manage IP SLA Operations section, click Add new operations.
4. Select Create new operations, and click Next.
5. Select DNS, and click Next.
6. Select the nodes you want to add to your new DNS operations, and click Next.
   
   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](#).
7. Enter the IP Address of the DNS server and the hostname or IP address to resolve, and click Next.
8. Enter the frequency for the operation to be performed.
9. Define your warning, critical, and maximum threshold values.
10. To assign a Virtual Routing and Forwarding (VRF) name for this path, expand Advanced, and enter the VRF name.

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

   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 SolarWinds VoIP and Network Quality Manager home page.

Add FTP IP SLA operations to 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.

You cannot add operations that have been previously created with SolarWinds 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 in to your SolarWinds VoIP and Network Quality Manager server as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Add new operations in the Manage IP SLA Operations section.
4. Select Create new operations, and click Next.
5. Select FTP, and click Next.
6. Select the nodes you want to add to your new FTP operations, and click Next.
   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.
7. Enter the URL of the FTP server, and click Next.
8. Enter the frequency for the operation to be performed.
9. Define your warning, critical, and maximum threshold values.
10. To assign a type of service (ToS) or Virtual Routing and Forwarding (VRF) name for this path, expand Advanced, and enter the type of service number and VRF name.

   - 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 SolarWinds 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 Set the traffic precedence in SolarWinds VNQM.
   - 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. To rename operations or edit any other operation properties, select the operations you want to modify, and click Edit.
13. Review the operations you want to create, and click Create Operations.
   Depending on the number of operations that are being created, this process can take several minutes.
14. Click Go to VNQM Home to finish the procedure and return to the SolarWinds VoIP and Network Quality Manager home page.

Add HTTP IP SLA operations to 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.
You cannot add operations that have been previously created with SolarWinds 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 in to your SolarWinds VoIP and Network Quality Manager server as an administrator.

2. Click Settings > All Settings > VoIP & Quality Settings.

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

4. Select Create new operations, and click Next.

5. Select HTTP, and click Next.

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

   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.

7. Enter the URL of the HTTP server, and click Next.

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

9. Define your warning, critical, and maximum threshold values.

10. To assign a type of service (ToS) or Virtual Routing and Forwarding (VRF) name for this path, expand Advanced, and enter the type of service number and VRF name in the appropriate fields.

   - 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 SolarWinds 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 Set the traffic precedence in SolarWinds VNQM.
   - 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. To rename operations or edit any other operation properties, select the operations you want to modify, and click Edit.

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

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

Add DHCP IP SLA operations to 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.
You cannot add operations that have been previously created with SolarWinds 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 in to your SolarWinds VoIP and Network Quality Manager server as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Add new operations in the Manage IP SLA Operations section.
4. Select Create new operations, and click Next.
5. Select DHCP, and click Next.
6. Select the nodes you want to add to your new DHCP operations, and click Next.
   
   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.
7. Enter the IP address of the DHCP server to be tested, and click Next.
8. Enter the frequency for the operation to be performed.
9. Define your warning, critical, and maximum threshold values, and click Next.
10. To rename operations or edit any other operation properties, select the operations you want to modify, and click Edit.
11. Review the operations you want to create, and click Create Operations.
    
   Depending on the number of operations that are being created, this process can take several minutes.
12. Click Go to VNQM Home to finish the procedure and return to the SolarWinds VoIP and Network Quality Manager home page.

Add TCP Connect IP SLA operations to 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.

You cannot add operations that have been previously created with SolarWinds 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 In to your SolarWinds VoIP and Network Quality Manager server as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Add new operations in the Manage IP SLA Operations section.
4. Select Create new operations, and click Next.
5. Select TCP Connect, and click Next.
6. Select the type of path your network is configured to use. For more information, see Designate paths in SolarWinds VNQM.

7. Select the source nodes you want to add to your new TCP Connect operation, and click Next.
   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.

8. Select the target nodes you want to add to your new TCP Connect operation.

9. To create the path in only one direction, select No, create the path in just one direction.

10. To specify an external node as a target, complete the following procedure.
    a. Click Yes, use external node as a target.
    b. Enter the IP address or host name of the external node you want to add.
       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. Enter the frequency for the operation to be performed.

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

14. Define your warning, critical, and maximum threshold values.

15. 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 enter the type of service number or VRF name in the appropriate fields, or select Control enable.

   - 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 SolarWinds 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 Set the traffic precedence in SolarWinds VNQM.
   - 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. To rename operations or edit any other operation properties, select the operations you want to modify, and click Edit.

18. Review the operations you want to create, and click Create Operations.
   Depending on the number of operations that are being created, this process can take several minutes.

19. Click Go to VNQM Home to finish the procedure and return to the SolarWinds VoIP and Network Quality Manager home page.
Add UDP Jitter IP SLA operations to 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.

You cannot add operations that have been previously created with SolarWinds 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 in to your SolarWinds VoIP and Network Quality Manager server as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Add new operations in the Manage IP SLA Operations section.
4. Select Create new operations, and click Next.
5. Select UDP Jitter, and click Next.
6. Select the type of path your network is configured to use. For more information, see Designate paths in SolarWinds VNQM.
7. Select the source nodes you want to add to your new UDP Jitter operations, and click Next.
   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.
8. Select the target nodes you want to add to your new UDP Jitter operation.
9. To create the path in only one direction, select No, create the path in just one direction.
10. To specify an external node as a target, complete the following procedure.
   a. Click Yes, use external node as a target.
   b. Enter the IP address or host name of the external node you want to add.
      If you are using a host name, the source node of the operation must be able to successfully resolve the host name.
11. Enter the frequency for the operation to be performed.
12. Enter the port number to be used in the test in the Port Number field.
13. Define your warning, critical, and maximum threshold values.
14. To assign a type of service (ToS) or Virtual Routing and Forwarding (VRF) name for this path, expand Advanced, and type the type of service number and VRF name in the appropriate fields.

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 SolarWinds 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 Set the traffic precedence in SolarWinds VNQM.
15. Click Next.
16. To rename operations or edit any other operation properties, select the operations you want to modify, and click Edit.
17. Review the operations you want to create, and click Create Operations.
   Depending on the number of operations that are being created, this process can take several minutes.
18. Click Go to VNQM Home to finish the procedure and return to the SolarWinds VoIP and Network Quality Manager home page.

Add VoIP UDP Jitter IP SLA operations to 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.

You cannot add operations that have been previously created with SolarWinds 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 in to your SolarWinds VoIP and Network Quality Manager server as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Add new operations in the Manage IP SLA Operations section.
4. Select Create new operations, and click Next.
5. Select VoIP UDP Jitter, and click Next.
6. Select the type of path your network is configured to use. For more information, see Designate paths in SolarWinds VNQM.
7. Select the source nodes you want to add to your new VoIP UDP Jitter operation, and click Next.
   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.
8. Select the target nodes you want to add to your new VoIP UDP Jitter operation.
9. To create the path in only one direction, select No, create the path in just one direction.
10. To specify an external node as a target, complete the following procedure.
    a. Click Yes, use external node as a target.
    b. Enter the IP address or host name of the external node you want to add.
       If you use a host name, the source node of the operation must be able to successfully resolve the host name.
11. Enter the frequency for the operation to be performed.
12. Enter the port number to be used in the test.
13. Define your warning, critical, and maximum threshold values.
14. To assign a codec, type of service (ToS), or Virtual Routing and Forwarding (VRF) name for this path, expand Advanced, select the codec, and enter the type of service number and VRF name in the appropriate fields. For more information about codec algorithms, see Jitter in SolarWinds VNQM.

- 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 SolarWinds 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 Set the traffic precedence in SolarWinds VNQM.
- 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. To rename operations or edit any other operation properties, select the operations you want to modify, and click Edit.
17. Review the operations you want to create, and click Create Operations.
   Depending on the number of operations that are being created, this process can take several minutes.
18. Click Go to VNQM Home to finish the procedure and return to the SolarWinds VoIP and Network Quality Manager home page.

Add ICMP Echo IP SLA operations to 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.

- You may need to configure your device to successfully use ICMP Echo operations. For more information, see Configure CLI credentials in SolarWinds VNQM.
- You cannot add operations that have been previously created with SolarWinds 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 in to SolarWinds VNQM as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. In the Manage IP SLA Operations section, click Add new operations.

4. Select Create new operations, and click Next.

5. Select VoIP UDP Jitter, and click Next.

6. On the Define Paths panel, click Simple, and click Next.

   You can select other path types. See the SolarWinds VNQM Administrator Guide for more information on path types.

7. Select the source nodes you want to add to the VoIP UDP Jitter operation, and click Next.

   In this example, the source node is dev_ottawa_2621.
8. Select the target nodes you want to add to the VoIP UDP Jitter operation.

9. To create the path in only one direction, select No, create the path in just one direction. When you create a path in each direction, SolarWinds VNQM deploys the operation to the target device, which becomes the source of the second leg of the operation.

10. To specify an external node as a target, click Yes, use external node as a target. You can also target a node that you have added to SolarWinds VNQM.

11. Enter the IP address or host name of the external node you want to add, and click Next.
12. Enter the frequency for the operation to be performed. SolarWinds recommends you accept the default frequency.

13. Define your warning, critical, and maximum threshold values. SolarWinds recommends you accept the default thresholds.

14. Click Advanced and in the CODEC field, select GSM 711 ULAW. The Advanced options correspond to the type of operation you are creating. GSM 711 ULAW is the most common CODEC for VoIP UDP Jitter operations.

15. To assign a type of service (ToS) or Virtual Routing and Forwarding (VRF) name for this path, expand Advanced, and enter the type of service number and VRF name in the appropriate fields.

- 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 SolarWinds 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 Set the traffic precedence in SolarWinds VNQM.
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. Select the operation you want to create, and click Create Operations.
   Depending on the number of operations you create, this process can take several minutes.
18. Click Go to VNQM Home and review the All IP SLA Operations resource.
   It can take several minutes for the resource to populate with data. When the status icon turns green, SolarWinds VNQM is monitoring the operation.

### All IP SLA Operations

Add UDP Echo IP SLA operations to 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.

You cannot add operations that have been previously created with SolarWinds 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 in to your SolarWinds VoIP and Network Quality Manager server as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Add new operations in the Manage IP SLA Operations section.
4. Select Create new operations, and click Next.
5. Select UDP Echo, and click Next.
6. Select the type of path your network is configured to use. For more information, see Designate paths in SolarWinds VNQM.
7. Select the source nodes you want to add to your new UDP Echo operation.
   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.
8. Select the target nodes you want to add to your new UDP Echo operation.
9. To create the path in only one direction, select No, create the path in just one direction.
10. To specify an external node as a target, complete the following procedure.
   a. Click Yes, use external node as a target.
   b. Enter the IP address or host name of the external node you want to add.
      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. 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.

   - 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 SolarWinds 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 [Set the traffic precedence in SolarWinds VNQM](#).
   - 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. To rename operations or edit any other operation properties, select the operations you want to modify, and click Edit.
18. Review the operations you want to create, and click Create Operations.
   Depending on the number of operations that are being created, this process can take several minutes.
19. Click Go to VNQM Home to finish the procedure and return to the SolarWinds VoIP and Network Quality Manager home page.

Add ICMP Path Echo operations to 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.

- To add ICMP Path Echo operations, you must add CLI login credentials to your source node. For more information, see [Configure CLI credentials in SolarWinds VNQM](#).
To add ICMP Path Echo IP SLA operations to your network devices:

1. Log in to your SolarWinds VoIP and Network Quality Manager server as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Add new operations in the Manage IP SLA Operations section.
4. Select Create new operations, and click Next.
5. Select ICMP Path Echo, and click Next.
6. Select the type of path your network is configured to use. For more information, see Designate paths in SolarWinds VNQM.
7. Select the source node you want to use for your ICMP Path Echo operation.
   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.
8. If the target node is being monitored, select it from the list.
9. To create the path in only one direction, select No, create the path in just one direction.
10. To specify an external node as a target, complete the following procedure.
    a. Click Yes, use external node as a target.
    b. Enter the IP address or host name of the external node you want to add.
       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. Enter the frequency for the operation to be performed.
13. Define the warning and critical threshold values.
14. To assign a type of service (ToS) or Virtual Routing and Forwarding (VRF) name for this path, expand Advanced, and enter the type of service number and VRF name in the appropriate fields.

- 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 SolarWinds 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 Set the traffic precedence in SolarWinds VNQM.
- 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. To rename operations or edit any other operation properties, select the operations you want to modify, and click Edit.

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

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

Add ICMP Path Jitter operations to 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.

To add ICMP Path Jitter operations, you must add CLI login credentials to your source node. For more information, see Configure CLI credentials in SolarWinds VNQM.

You cannot add operations that have been previously created with SolarWinds 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 in to your SolarWinds VoIP and Network Quality Manager server as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Add new operations in the Manage IP SLA Operations section.
4. Select Create new operations, and click Next.
5. Select ICMP Path Jitter, and click Next.
6. Select the type of path your network is configured to use. For more information, see Designate paths in SolarWinds VNQM.
7. Select the source node you want to use for your ICMP Path Jitter operation, and click Next.
   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.
8. If the target node is being monitored, select it from the list.
9. To create the path in only one direction, select No, create the path in just one direction.
10. To specify an external node as a target, complete the following procedure.
   a. Click Yes, use external node as a target.
   b. Enter the IP address or host name of the external node you want to add.
      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. Enter the frequency for the operation to be performed.
13. Define the warning, critical, and maximum threshold values.
14. To assign a type of service (ToS) or Virtual Routing and Forwarding (VRF) name for this path, expand Advanced, and enter the type of service number and VRF name.

- 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 SolarWinds 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 Set the traffic precedence in SolarWinds VNQM.
- 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. To rename operations or edit any other operation properties, select the operations you want to modify, and click Edit.
17. Review the operations you want to create, and click Create Operations.
   Depending on the number of operations that are being created, this process can take several minutes.
18. Click Go to VNQM Home to finish the procedure and return to the SolarWinds VoIP and Network Quality Manager home page.

Add existing operations to SolarWinds® VoIP and Network Quality Manager (VNQM)

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

1. Log in to your SolarWinds VoIP and Network Quality Manager server as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Add new operations in the Manage IP SLA Operations section.
4. Select Monitor existing operations, and click Next.
5. If you want to automatically discover operations on your nodes, complete the following procedure.
   a. Select Automatically discover existing operations, and click Next.
   b. Select the node where the operation you want to monitor resides, and click Next.
      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 click Monitor Operations.
6. If you want to manually enter the operation numbers, expand Advanced, and complete the following procedure.
   a. Select Manually enter operation numbers, and click Next.
   b. Select the node where the operation you want to monitor resides, and click Next.
      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 click Next.
   d. Select the operation you want to monitor, and click Monitor Operations.
7. Click Go to VNQM Home to finish the procedure and return to the SolarWinds VoIP and Network Quality Manager home page.

Edit IP SLA operations

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

- Modify the SLA Location
- Rename operations in SolarWinds VNQM
- Delete IP SLA operations

Modify 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 Settings > All Settings > VoIP & Quality Settings.
2. In the Manage IP SLA operations section, click Edit or delete operations.
3. Select the operation you want to modify, and 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.

Rename operations in SolarWinds VNQM

Any operation that SolarWinds 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.

1. Click Settings > All Settings > VoIP & Quality Settings.
2. In the Manage IP SLA Operations section, click Edit or delete operations.
3. Select the operation you want to modify, and click Edit.
4. Enter the new name for the operation, and click Save.

- 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 SolarWinds NPM, the change will be reflected in the operation name unless the default naming pattern is not being used.

Delete IP SLA operations

To stop monitoring specific IP SLA operations in SolarWinds VoIP and Network Quality Manager, complete the following procedure.

Deleting manually added IP SLA operations from SolarWinds 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 SolarWinds VoIP and Network Quality Manager:

1. Log in to your SolarWinds VoIP and Network Quality Manager server as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. In the Manage IP SLA Operations section, click Edit or delete operations.
4. Select the operations you want to delete, and click Delete.
5. When prompted to confirm, click Delete to stop monitoring the selected operations.

VoIP management in SolarWinds VNQM

In SolarWinds 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.
2. Add the devices to VNQM for monitoring.
   - To monitor VoIP calls on your devices, add them as call managers. For more information, see Manage call managers.
   - To monitor the PRI trunk utilization of your devices, add them as gateways. For more information, see Manage gateways in SolarWinds VNQM.

VNQM also provides an overview of your VoIP infrastructure monitored by VNQM. For more information about configuring this resource, see Select the VoIP infrastructure.
Manage 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.

You can monitor call managers from manufacturers other than Cisco and Avaya 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 Add 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. Click Settings > All Settings > VoIP & Quality Settings.
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 Configure CLI credentials in SolarWinds VNQM.

The CLI credentials are also used for logging in to Avaya Call Managers. For more information, see Add Avaya Call Manager devices to SolarWinds VNQM.

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, SolarWinds 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. VNQM queries the database for region information. No information is modified in the database. You can create a read only AXL account specifically for VNQM.

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 Configure Cisco CallManagers for FTP.
2. Enable the AXL API. For more information, see your manufacturer's documentation.
3. Create an AXL account. For more information, see your manufacturer's documentation.
Related topics:

- Add Cisco CallManager devices to SolarWinds VNQM
- Add CallManager Express devices to SolarWinds VNQM
- Manage Avaya Call Managers
- Add Avaya Call Manager devices to SolarWinds VNQM
- Add call manager devices from other manufacturers
- Delete call manager devices from SolarWinds VNQM

Monitor CallManager health

SolarWinds 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 SolarWinds 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.

To track the performance of call managers from other manufacturers, you can use universal device pollers in connection with SolarWinds Network Performance Monitor.

After a call manager device has been added to the database for management, you can use the intuitive interface of SolarWinds 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 SolarWinds 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.

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.

SIP monitoring on Cisco CallManagers

SIP Trunking is a VoIP technology and streaming media service. A SIP Trunk provides the same service you get from a traditional analog phone line or channel (trunk) on a PRI. Instead of being a physical wire, a SIP Trunk is a virtual phone line which is provided by a SIP Trunk provider. It uses your data circuit to connect your phone system to the internet. In addition to voice calls, SIP Trunks can also carry instant messages, multimedia conferences, user presence information, enhanced 9-1-1 emergency calls, and other SIP-based, real-time communication services.

SIP Trunk monitoring provides the following benefits:
You can troubleshoot calls by analyzing CDR data, providing the associated IP SLA metrics, and giving a hop-by-hop analysis of the call path.

When integrated with SolarWinds NPM, you can view detailed network performance metrics (CPU or memory utilization) of the IP SLA source device for further troubleshooting.

VNQM provides the up and down status of the infrastructure that carries SIP Trunks and provides an alert when a SIP Trunk is down.

VNQM tracks SIP call traffic including attempted, completed, in progress, and active audio as well as attempted and completed video calls. For more information, see SolarWinds VNQM views.

You can perform advanced troubleshooting to identify the root cause of SIP call failures by correlating SIP trunk availability, call performance metrics, and corresponding network performance metrics using the Performance Analysis dashboards (PerfStack™).

There are two methods for enabling SIP Trunk monitoring in VNQM:

- Enable SIP Trunk monitoring when you add a new Cisco CallManager to VNQM.
- Enable SIP Trunk monitoring when you edit the properties of an existing Cisco CallManager in VNQM.

Add Cisco CallManager devices to SolarWinds VNQM

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

Avaya™ Call Managers can also be monitored with SolarWinds VoIP and Network Quality Manager. For more information about monitoring Avaya Call Managers, see Manage Avaya Call Managers.

Call managers from manufacturers other than Cisco and Avaya can be monitored with SolarWinds 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 Add Call Manager Devices from Other Manufacturers.

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

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Add CallManager nodes.

![Manage CallManager Nodes](image)
4. Select a vendor and call manager device, and click Next. 
   If you do not see an expected call manager device, use the Web Console to add it. You may need to enable SNMP on the call manager device.

5. Select Enable CDR/CQR polling for this call manager, and click Next.

6. To enable SIP Trunk monitoring on the CallManager, select Enable AXL SIP Trunk Polling, and enter the polling frequency for SIP Trunk Status scanning.
   If you select Add Call Manager without CDR/CQR monitoring, SolarWinds VNQM provides call manager statistics, but does not provide information about calls or call quality.
7. Click Next.

8. Select or enter the AXL credentials that SolarWinds VNQM uses to collect region and location information for call managers and phones.

   Enter AXL credentials for both publisher and subscriber call managers.

9. Make sure the VNQM AXL Application User has the following roles:
   - Standard AXL API Access
   - Standard CCM Admin Users
   - Standard SERVICEABILITY Administration

   By default, only the Standard CCM Super Users Access Control Group has the Standard SERVICEABILITY Administration role. If you don't want the users to have that much access to your Cisco CallManager, you have to create a new Access Control Group in CUCM with only the roles that the SolarWinds VNQM user actually needs. For more details, see Manage User Access in CUCM (© 2018 Cisco, available at https://www.cisco.com/, obtained on October 1, 2018).

10. Click Test to test the credentials.

11. Click Next.

12. Define the FTP server details.
   a. Enter the FTP server IP address or host name where your CDR/CMR data is stored. For more information about FTP configuration, see Configure 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 the FTP credentials.
g. Enter a number in Polling Frequency between 1 and 60 to configure how frequently you want to poll the FTP server in minutes.

h. If you want to remove the files from the FTP server, select Delete CDR/CMR files from FTP server after download.

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

Removing the files from the FTP server prevents the device from filling up with log files, and helps speed up data collection from the FTP server.

i. Click Test FTP Server Connection to test the connection.

j. Click Next.

13. On the Summary panel, review the information you entered, and click Add Call Manager.

After SolarWinds VNQM adds the call manager, the call manager is displayed on the VoIP CallManagers resource.

14. After you have added the device, you can configure it to send data.
Add CallManager Express devices to SolarWinds VNQM

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

SolarWinds 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 SolarWinds VoIP and Network Quality Manager:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Add CallManager nodes.
4. If you have not already added your CallManager devices to the database, use the Orion Web Console to add your CallManager devices before continuing.
5. Select an available CallManager Express device, and click Next.
6. If you do not see an expected CallManager Express device, use the Orion Web Console to add it.
7. Click Next, and click Add CallManager.

Manage 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. SolarWinds VNQM supports Avaya Aura® Call Manager version 6.x.

In order to collect Avaya data in VNQM, the Avaya user must have sufficient permissions to execute the following commands:

- `display system-parameters cdr`
  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 in to the Avaya Call Manager using PuTTY, TuTTY, or Avaya Manager.
2. Enter `change system-parameters cdr`, and press F3.
3. Set the Primary Output Format to customized.

4. Set the Primary Output Endpoint to CDR1, and press F7 to navigate to the next page.

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

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

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


7. Enter a name for VNQM. The name can be any name you choose.
8. Enter the IP address of the VNQM main or additional poller in the IP Address column, and press F3 to save your changes.

9. Enter change ip-services, press F3, and define the following settings:
   - Service Type: CDR1
   - Local Node: procr
   - Remote Node: \[vnqm\] where \[vnqm\] is the name you specified in Step 7.
   - Remote Port: 50000

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

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 in to the Avaya Call Manager using PuTTY, TuTTY, or Avaya Manager.
2. Enter `change system-parameters ip-options`, press F3, and 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. Enter `change ip-network-region [x]` where [x] is the region number, and 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 SolarWinds 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:

- 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.

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.

Add Avaya Call Manager devices to SolarWinds VNQM

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

When you add an Avaya call manager device, SolarWinds VoIP and Network Quality Manager uses the value of the OID 1.3.6.1.2.1.1.1 (sysDescr) to identify an Avaya Communication and Media Server.

Add an Avaya Communication and Media Server to VNQM

The following procedure adds an Avaya Communication and Media Server device to SolarWinds VoIP and Network Quality Manager.

Call managers from manufacturers other than Cisco® and Avaya can be monitored with SolarWinds 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 Add call manager devices from other manufacturers.

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

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Add CallManager Nodes.

   VoIP Management

   Manage CallManager Nodes

   Add, delete and manage Call Managers
   > Add CallManager nodes
   > Manage CallManager Nodes

4. Select a vendor and a call manager device, and click Next.

   If you do not see an expected call manager device, use the Orion Web Console to add it. Make sure that you enable SNMP on the call manager device.

   Add Call Manager

   SELECT NODES WHAT TO MONITOR SUMMARY

   Select a Call Manager

   Choose the call manager you want to add from the list below.
   Cisco CallManager nodes must be running the Cisco CallManager SNMP Service.

   To fully benefit from monitoring Avaya Call Managers, they must be configured with the correct SNMP information.

   If you don’t see your nodes below, you may need to add your nodes to VoIP and Network Quality Manager.

   GROUP BY:
   Vendor

   Avaya Communication
   Cisco

   Node Name
   USAUS-AVAYA-ACM-01

5. Select Enable CDR/CQR polling for this call manager, and click Next.

   If you select Add Call Manager without CDR/CQR monitoring, SolarWinds VNQM provides call manager statistics, but does not provide information about calls or call quality.
6. Select or enter the CLI credentials that SolarWinds VNQM uses to collect region and location information for call managers and phones.

7. Click Test to test the credentials.

   If the SAT account has a PIN code defined for additional authentication, the CLI credential test will fail. PINs are not supported by SolarWinds 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, and click Add Call Manager.

   After SolarWinds adds the call manager, the call manager is displayed in the VoIP CallManagers resource.
9. After you have added the device, you can configure it to send data.

Restrictions:

- 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 SolarWinds VoIP and Network Quality Manager.
- SolarWinds 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.

Polling bandwidth for Avaya Communication and Media Servers

The average bandwidth requirements of Avaya™ Communication and Media Servers vary 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.
Add 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.

- 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.

For more information about setting up universal device pollers for call managers from other manufacturers, see Monitoring MIBs with Universal Device Pollers.

For more information about adding call managers from other manufacturers to SolarWinds VoIP and Network Quality Manager, see Select the VoIP infrastructure.

Define 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 SolarWinds VoIP and Network Quality Manager can download and process the data. For more information about FTP configuration, see Configure 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 SolarWinds VoIP and Network Quality Manager tries to download CDR/CMR data. If you have a large amount of data or if SolarWinds 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.

Configure 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 in 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.

If you want to change the time interval for collecting CDR/CMR data, click System > Enterprise Parameters, modify the CDR File Time Interval, and click OK.

5. Log in 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.

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

Edit call managers

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

For more information about editing node properties, see Edit node properties.

To edit call manager specific settings:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Manage CallManager Nodes.
4. Select the call manager node you want to modify, and 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® CallManagers:**

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

**SIP Polling Settings**
Select Enable AXL SIP Trunk Polling for this Call Manager to collect information about SIP Trunks on this CallManager.

**AXL Credentials**
Select the appropriate settings from the Select AXL Credentials list or define new credentials. Make sure the VNQM AXL Application User has the following roles:

- Standard AXL API Access
- Standard CCM Admin Users
- Standard SERVICEABILITY Administration

By default, only the Standard CCM Super Users Access Control Group has the Standard SERVICEABILITY Administration role. If you don't want the users to have that much access to your Cisco CallManager, you have to create a new Access Control Group in CUCM with only the roles that the SolarWinds VNQM user actually needs. For more details, see Manage User Access in CUCM (© 2018 Cisco, available at https://www.cisco.com/, obtained on October 1, 2018).

**FTP Server Settings**
Enter or edit details about the FTP server where your CDR/CMR data is stored. For more information about FTP configuration, see [Configure Cisco CallManagers for FTP](#).
FTP Server
Enter or edit the FTP server IP address.

Port
Enter 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
Enter or edit these details if appropriate.

FTP Credentials:
Add or edit your FTP credentials.

To define a new set of FTP Credentials:
- Enter a name in Select FTP Credentials.
- Enter the user name in FTP Username.
- Enter the password in FTP Password.

Polling Frequency: Enter 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.

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:
- Enter 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 click Submit.
Delete call manager devices from SolarWinds VNQM

The following procedure provides the steps required to delete a call manager device from SolarWinds VoIP and Network Quality Manager

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Manage Call Manager nodes.
4. Select the Call Manager-hosting devices you want to delete, and click Remove Call Managers.
5. Click OK to confirm.

Manage gateways in SolarWinds VNQM

Managing gateways in SolarWinds 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. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Manage gateways.

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

Related tasks:

- Add gateways to SolarWinds VNQM
- Edit VoIP gateways
- Edit CLI credentials for gateway nodes
- Remove gateways

Add gateways to SolarWinds VNQM

To monitor your gateways with SolarWinds 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 SolarWinds VoIP and Network Quality Manager as a gateway. Gateway nodes require CLI credentials.

To add a gateway device to SolarWinds VoIP and Network Quality Manager:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Add gateways.
4. Select VoIP Gateways to Add: Select one or more available nodes which you want to add to VNQM as gateways.
   If you do not see an expected device, click Add your nodes to add it to the SolarWinds Orion database, and repeat Steps 1 - 3. For more information about adding nodes to the SolarWinds Orion database, see Adding Devices for Monitoring in the Web Console.

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.

   i. 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 click Finish to add the selected gateways.

Edit 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 Settings > All Settings > VoIP & Quality Settings.
3. Click Manage gateways.

4. Select one or more available gateways that you want to edit.

   - If you do not see an expected device, click Add your nodes to add it to the Orion database, and repeat Steps 1 - 3. For more information about adding nodes to the SolarWinds Orion database, see Add devices for monitoring in the Web Console.

5. Edit the appropriate properties of the selected gateway node. For more information about editing nodes, see Edit node properties.

6. Click Submit to apply your changes.

**Edit CLI credentials for gateway nodes**

For monitoring gateway nodes, VNQM uses CLI credentials.

To edit CLI credentials, complete the following steps:

1. Log in to your SolarWinds VoIP and Network Quality Manager server as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Manage Gateways.
4. Select the node you want to edit, and 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, provide the following details:
   
   - Select Credentials
     Enter the name of the new credential set.
   
   - Username
   
   - Password
   
   - Enable Level
     Select the enable level to use when logging in.

     The enable level must have privileges to execute terminal commands. SolarWinds 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
     Enter the password associated with the enable level to use when logging in.

6. Expand Advanced, and 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.

**Remove gateways**

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 Settings > All Settings > VoIP & Quality Settings.
3. Click Manage gateways.
4. Select the gateways you want to remove.
5. Click Remove Gateways, and click OK to confirm.

SIP monitoring on Cisco CUBE devices

As of version 4.6, SolarWinds VoIP and Network Quality Manager (VNQM) supports gateway SIP monitoring on Cisco Unified Border Element (CUBE) devices. You can review the list of SIP trunks on the device, including dial peer number, description, and keep alive status. You can also poll keep alive status, call activity, and utilization metrics for each SIP trunk.

You can also review the SIP trunk statistics for Cisco CUBE devices in the Performance Analysis charts (PerfStack™) in the Orion Web Console.

Enable SIP trunk monitoring for a new Cisco CUBE gateway

In order to poll SIP-related, SolarWinds VNQM requires CLI credentials with enable mode.

You can specify the CLI credentials when you add a new gateway to SolarWinds VNQM:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Add gateways.
4. Select VoIP Gateways to Add: Select the Cisco CUBE node which you want to add to VNQM as a gateway.
5. Click Next.
6. The CLI Credentials Issues dialog pops up. Modify CLI credentials to solve the issues:
   a. Select the Cisco CUBE device whose CLI credentials you want to edit.
   b. Click Edit Credentials.
      - Define a new set of credentials in the Username and Password fields.
      - Select Enable from the Enable Level drop-down.
      - Enter the password associated with the enable level in the Enable Password field.
- Click Save to apply your CLI credential settings on the selected nodes.

![CLI Credentials Issues](image)

**e.** Click Select Successful to select the Cisco CUBE node whose CLI credentials have been updated successfully.

**f.** Click Continue to add the selected Cisco CUBE node to VNQM as a gateway node.

7. Review the information, and click Finish to add the selected gateway.

SIP trunk monitoring on Cisco CUBE devices starts automatically as soon as CLI credentials are validated and saved. For more information, see Add Gateways to SolarWinds VNQM.

Enable SIP trunk monitoring for an existing Cisco CUBE gateway

If you have already added the gateway to SolarWinds VNQM, you can enable SIP trunk monitoring through the Manage Gateways page:

1. Log in to your SolarWinds VoIP and Network Quality Manager server as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.
3. Click Manage Gateways.
4. Select the Cisco CUBE node you want to edit, and 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, provide the following details:

- **Select Credentials**
  - Enter the name of the new credential set.
- **Username**
- **Password**
- **Enable Level**
  - Select Enable.
- **Enable Password**
  - Enter the password associated with the enable level to use when logging in.
6. Expand Advanced, and 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.

SIP trunk monitoring on Cisco CUBE devices starts automatically as soon as CLI credentials are validated and saved. For more information, see Manage Gateways in SolarWinds VNQM.

Select the VoIP infrastructure

In SolarWinds 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 Settings > All Settings > VoIP & Quality Settings.
3. In the VoIP Management group, click Select VoIP nodes.
4. Expand the names 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.

   - If you do not see an expected VoIP-related device or interface in the list, use the Orion Web Console to add the device to the database. For more information, see Adding Devices for Monitoring in the Web Console.
   - 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.

<table>
<thead>
<tr>
<th>CALL PRECEDENCE LEVEL</th>
<th>CALL PRIORITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Flash override</td>
</tr>
<tr>
<td>1</td>
<td>Flash</td>
</tr>
<tr>
<td>2</td>
<td>Immediate</td>
</tr>
<tr>
<td>3</td>
<td>Priority</td>
</tr>
</tbody>
</table>
SolarWinds VNQM settings

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

To access this page:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings > VoIP & Quality Settings.

The following settings of SolarWinds 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 SolarWinds VNQM.

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.

- 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, click Research Features, select Search by feature, and 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 SolarWinds VoIP and Network Quality Manager. For more information, see Add IP SLA nodes to SolarWinds VNQM.

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 SolarWinds VNQM.
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.

Only nodes added to the database are available for SolarWinds 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.

SolarWinds 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. SolarWinds 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 Add IP SLA nodes to SolarWinds VNQM.

For more information about alerts and reports in SolarWinds VoIP and Network Quality Manager, see Use SolarWinds VNQM.

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 SolarWinds VoIP and Network Quality Manager. From the SolarWinds VoIP and Network Quality Manager Settings page, you can configure the following:

- The port through which SolarWinds VoIP and Network Quality Manager sends simulated traffic.
- The jitter codec that SolarWinds VoIP and Network Quality Manager simulates on your network.
- The interval at which SolarWinds 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 SolarWinds 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 Configure SolarWinds VNQM settings.

Database Details

The SolarWinds 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.

Configure SolarWinds VNQM settings

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

SolarWinds 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 Settings > All Settings > VoIP & Quality Settings.
3. Click Edit VoIP & Network Quality Manager settings in the Details section.
4. To use a port other than the default for simulated VoIP traffic, enter 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 SolarWinds VNQM.
6. Enter a CallManager Polling Interval in minutes to specify how often you want to collect your call manager data.

SolarWinds VoIP and Network Quality Manager measures the performance of your network by periodically sending test packets over defined paths. SolarWinds VoIP and Network Quality Manager measures the performance of your network in transmitting these test packets. 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. Enter the period of time, in days, to retain IP SLA operation statistics in the IP SLA Data Retention field.

SolarWinds 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. Enter a value for the MOS Advantage Factor.

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 SolarWinds VNQM.

9. Provide a value for the Type of Service (ToS) octet to set the precedence of VoIP traffic on your network.

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 VNQM 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 Set the traffic precedence in SolarWinds VNQM.

10. Select Operations in running configurations to view all new operations created by VNQM in the running configurations on Cisco devices. You cannot view VNQM operations created with CLI credentials.

11. Enter 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 Add Avaya Call Manager devices to SolarWinds VNQM. If you use a load balancer, it is recommended that you disable this option, and add the load balancer directly to VNQM.

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

15. Enter 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. Enter 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 Save after you have finished configuring your settings.

Set the traffic precedence in SolarWinds VNQM

In SolarWinds 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. SolarWinds VoIP and Network Quality Manager employs a decimal Type of Service value specified on the SolarWinds VoIP and Network Quality Manager Settings page. For more information, see Configure SolarWinds VNQM settings.
The Type of Service value used by SolarWinds 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:

<table>
<thead>
<tr>
<th>ToS Value (decimal)</th>
<th>DSCP Value (decimal)</th>
<th>DSCP Precedence</th>
<th>Flow Control</th>
<th>PHB</th>
<th>Drop Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best Effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Default</td>
</tr>
<tr>
<td>Class Selector</td>
<td>32</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>16</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>96</td>
<td>24</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>32</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>160</td>
<td>40</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>192</td>
<td>48</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>224</td>
<td>56</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Assured Forwarding</td>
<td>40</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>48</td>
<td>12</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>56</td>
<td>14</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>72</td>
<td>18</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>80</td>
<td>20</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>88</td>
<td>22</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>104</td>
<td>26</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>112</td>
<td>28</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>120</td>
<td>30</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>136</td>
<td>34</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>144</td>
<td>36</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>152</td>
<td>38</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Expedited Forwarding</td>
<td>184</td>
<td>46</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
Use SolarWinds VNQM

SolarWinds 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 SolarWinds VNQM
- Exploring SolarWinds VNQM Views
- Customizing Charts in SolarWinds VNQM
- Using custom properties for SolarWinds VNQM
- Using alerts and actions in SolarWinds VNQM
- SolarWinds VNQM reports
- Maps in SolarWinds VNQM

Start SolarWinds VNQM

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

1. Log in to your SolarWinds VoIP and Network Quality Manager server.
2. Start the Orion Web Console in the Orion program folder.
3. Click My Dashboards > VoIP & Network Quality.

You can also open SolarWinds 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:

SolarWinds VNQM views

SolarWinds 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 Use and Configuring Subviews.

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 Customize Web Console Menu Bars.
- 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 SolarWinds 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 customization, see Customize Views.

The following views are provided with SolarWinds 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

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.

CallManager SIP Trunks View

Displays a list of all available trunks on a single CallManager.

<table>
<thead>
<tr>
<th>CallManager SIP Trunks</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>DESCRIPTION</td>
<td>DEVICEPOOL</td>
<td>STATUS</td>
<td></td>
</tr>
<tr>
<td>DevLab-11Sts10S-SIP-Trunk</td>
<td>Calls between 11.5 and 10.5 cluster</td>
<td>Default</td>
<td>Registered</td>
<td></td>
</tr>
<tr>
<td>DevLab-11Sts11-SIP-Trunk</td>
<td>Calls between 11.5 and 11 cluster</td>
<td>DevLab-Trunk-DP</td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>DevLab-11Sts91-SIP-Trunk</td>
<td>Calls between 11.5 and 9.1 cluster</td>
<td>DevLab-Trunk-DP</td>
<td>Registered</td>
<td></td>
</tr>
<tr>
<td>Gateway-11-S5-SIP-Trunk</td>
<td>SIP Trunk to 10.199.196.1 for PSTN</td>
<td>DevLab-Trunk-DP</td>
<td>Registered</td>
<td></td>
</tr>
</tbody>
</table>

SIP Trunk Details View

Displays detailed information about a single SIP Trunk on a call manager, including SIP Trunk Destinations. The view provides charts for trunk availability and audio and video call 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.
• 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.

Customize charts in SolarWinds VNQM

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

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

- Customize chart titles in SolarWinds VNQM
- Calculated series in SolarWinds VNQM
- Time period in SolarWinds VNQM
- Sample interval in SolarWinds VNQM
- Chart size in SolarWinds VNQM
- Customize chart titles in SolarWinds VNQM
- Data tables in SolarWinds VNQM
- Font size in SolarWinds VNQM
- Printing options
- Data export options
- Advanced chart settings in SolarWinds VNQM

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

Customize chart titles in SolarWinds VNQM

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

SolarWinds Network Performance Monitor might provide default chart titles and subtitles. If you edit any of the Chart Titles fields on the Custom Chart page, you can restore the default titles and subtitles by clearing the respective fields, and clicking Submit.

Calculated series in SolarWinds VNQM

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.

Only the options applicable for the particular resource are available.

**Time period in SolarWinds VNQM**

Designate a predefined or custom time period for your chart by using any of the following methods:

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

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.

Data within the defined sample is summarized automatically.

**Sample interval in SolarWinds VNQM**

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.

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

**Chart size in SolarWinds VNQM**

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 in SolarWinds VNQM**

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

You might 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 in SolarWinds VNQM

Generated charts have variable font sizes. Use the Font Size option to select a small, medium, or large size font for chart labels and text.

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

Printing options

To print a customized chart, click Printable Version. A printable version of the customized chart is displayed in the browser.

Data export options

Exportable chart data is also available from selected charts in the Display Data from Chart area. 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 chart settings in SolarWinds VNQM

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

To modify the chart title and subtitle, expand Advanced, and enter the Chart title and Chart subtitle.

SolarWinds 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.

Use custom properties for SolarWinds 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 SolarWinds 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 SolarWinds VoIP and Network Quality Manager, see Creating a Custom Property.

**Advanced alerts and actions in SolarWinds VNQM**

As of Orion Platform 2015.1 (VNQM version 4.2.2), alerts are no longer created with the desktop-based, Advanced Alerts Manager or Basic Alerts Manager. Alerts are instead created and managed in the SolarWinds Orion Web Console. See Create and Manage Alerts for more information.

**SolarWinds VNQM reports**

SolarWinds provides a web-based reporting feature as a quick and easy way for you to extract data from your database. Because SolarWinds 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 Reports in the Orion Web Console. You can create and edit reports using VNQM data directly in the Orion Web Console.

A number of predefined IP SLA-specific reports is available with your installation of SolarWinds VoIP and Network Quality Manager. The web-based Reports feature 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 SolarWinds VoIP and Network Quality Manager web interface and print them with the click of a button.

For more information about predefined IP SLA Reports, see Use predefined VNQM reports.

Report scheduling is available within the Reports feature in the Orion Web Console. This feature schedules automatic email reports that can be sent to individual users or groups of users.

**Use predefined SolarWinds VNQM reports**

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

To access predefined reports:

1. Start the Orion Web Console.
2. Click Report > All Reports.
3. Click the report you want to display.

To edit a report:

1. Click the report you want to modify.
2. Click Edit Report.
3. After editing, review the Summary, and Click Submit.

Historical IP SLA Operation reports

SolarWinds 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.

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

SolarWinds 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 - 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.

**PRI Gateway Utilization - Last 24 Hours**
Displays PRI Utilization for VoIP gateways over the last 24 hours.

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

Historical SIP Trunk reports

SolarWinds VNQM includes predefined reports for SIP Trunk statuses.

**SIP Trunk Status Availability - Last 7 Days**
Displays the percentage of SIP Trunk status durations over the last 7 days.

**SIP Trunk Status Availability - Last Month**
Displays the percentage of SIP Trunk status durations that occurred last month.

**SIP Trunk Status Availability - This Month**
Displays the percentage of SIP Trunk status durations that occurred this month.
VNQM Connected Devices reports

**Connected Phones Report**

Displays all connected phones for a call manager, including their name, extension, IP address, region, status, and license status.

**Connected Gateways Report**

Displays all connected gateways for a call manager, including their name, IP address, status, and region.

**SolarWinds VNQM Maps**

SolarWinds 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.

**SolarWinds VNQM 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>IpSlaOperationNumber</td>
<td>The internal number of the operation</td>
</tr>
<tr>
<td>VARIABLE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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>OperationType</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.
MIBs Maintained by SolarWinds VNQM

SolarWinds 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 SolarWinds VoIP and Network Quality Manager, according to the settings of your SolarWinds VoIP and Network Quality Manager implementation, as it conducts IP SLA operations:

- General
- All Operations
- DHCP Operations
- DNS Operations
- HTTP and FTP Operations
- ICMP Echo Operations
- TCP Connect Operations
- UDP Jitter Operations
- VoIP UDP Jitter Operations
- VoIP Specific MIBs

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
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
- rttMonLatestJitterOperSumOfNegativesDS
- rttMonLatestJitterOperNumOfPositivesSD
- rttMonLatestJitterOperNumOfPositivesDS
- rttMonLatestJitterOperNumOfNegativesSD
- rttMonLatestJitterOperNumOfNegativesDS
- rttMonLatestJitterOperPacketLossSD
VoIP UDP Jitter Operations

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

VoIP Specific MIBs

- rttMonEchoAdminSourceAddress
- rttMonCtrlAdminFrequency
- rttMonEchoAdminCodecType
- rttMonEchoAdminCodecPayload
- rttMonEchoAdminCodecNumPackets
- rttMonEchoAdminCodecInterval
- rttMonEchoAdminICPFAvFactor
- rttMonScheduleAdminRttLife
- rttMonScheduleAdminRttStartTime
Supported versions of Cisco Unified CallManager

SolarWinds VoIP and Network Quality Manager uses the CISCO-CCM-MIB and supports Cisco® Unified Communications Manager (CallManager) versions 6, 7, 8, 9, 10, 11, and 12.

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 CallManager server.

The following table lists the OIDs used for CallManager.

<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>ccmlNetAddressType</td>
<td>1.3.6.1.4.1.9.9.156.1.1.2.1.6</td>
</tr>
<tr>
<td>ccmlNetAddress</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

<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><code>ccmGatewayName</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.3.1.1.2</code></td>
</tr>
<tr>
<td><code>ccmGatewayDescription</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.3.1.1.4</code></td>
</tr>
<tr>
<td><code>ccmGatewayStatus</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.3.1.1.5</code></td>
</tr>
<tr>
<td><code>ccmGatewayInetAddressType</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.3.1.1.7</code></td>
</tr>
<tr>
<td><code>ccmGatewayInetAddress</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.3.1.1.8</code></td>
</tr>
<tr>
<td><code>ccmGatewayTimeLastStatusUpdt</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.3.1.1.11</code></td>
</tr>
<tr>
<td><code>ccmGatewayTimeLastRegistered</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.3.1.1.12</code></td>
</tr>
<tr>
<td><code>ccmGatewayProductTypeIndex</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.3.1.1.15</code></td>
</tr>
</tbody>
</table>

## OIDs from the `ccmProductTypeTable`

<table>
<thead>
<tr>
<th>NAME</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ccmProductType</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.1.8.1.2</code></td>
</tr>
<tr>
<td><code>ccmProductName</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.1.8.1.3</code></td>
</tr>
<tr>
<td><code>ccmProductCategory</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.1.8.1.4</code></td>
</tr>
</tbody>
</table>

## OIDs from the `ccmPhoneTable`

<table>
<thead>
<tr>
<th>NAME</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ccmPhoneIndex</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.2.1.1.1</code></td>
</tr>
<tr>
<td><code>ccmPhonePhysicalAddress</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.2.1.1.2</code></td>
</tr>
<tr>
<td><code>ccmPhoneDescription</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.2.1.1.4</code></td>
</tr>
<tr>
<td><code>ccmPhoneIpAddress</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.2.1.1.6</code></td>
</tr>
<tr>
<td><code>ccmPhoneStatus</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.2.1.1.7</code></td>
</tr>
<tr>
<td><code>ccmPhoneTimeLastRegistered</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.2.1.1.8</code></td>
</tr>
<tr>
<td><code>ccmPhoneE911Location</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.2.1.1.9</code></td>
</tr>
<tr>
<td><code>ccmPhoneProductTypeIndex</code></td>
<td><code>1.3.6.1.4.1.9.9.156.1.2.1.1.18</code></td>
</tr>
<tr>
<td>NAME</td>
<td>OID</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>ccmPhoneName</td>
<td>1.3.6.1.4.1.9.9.156.1.2.1.1.20</td>
</tr>
</tbody>
</table>

**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>
<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>
How SolarWinds VNQM creates operations

The following sections detail how SolarWinds VoIP and Network Quality Manager creates new operations on your network devices:

- Owner Field Value
- SNMP-Based Operations
- CLI-Based Operations

Owner Field Value

SolarWinds 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
- 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;opNum&lt;br&gt;ber&gt;</td>
<td>11 (Dhcp)</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>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 “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>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>
<tr>
<td>rttMonScheduleAdminRttStart</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>1.3.6.1.4.1.9.9.42.1.2.1.1.4.&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>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>
</tbody>
</table>
### MIB NAME | OID NUMBER | VALUE
--- | --- | ---
rttMonEchoAdminTargetAddressString | 1.3.6.1.4.1.9.9.42.1.2.2.1.11.<opNumber> | Host name to resolve
rttMonEchoAdminNameServer | 1.3.6.1.4.1.9.9.42.1.2.2.1.12.<opNumber> | DNS server IP
rttMonEchoAdminVrfName | 1.3.6.1.4.1.9.9.42.1.2.2.1.26.<opNumber> | VRF name (only if specified)
rttMonCtrlAdminThreshold | 1.3.6.1.4.1.9.9.42.1.2.1.1.5.<opNumber> | MAX (WarningRttThreshold,CriticalRttThreshold)
rttMonCtrlAdminFrequency | 1.3.6.1.4.1.9.9.42.1.2.1.1.6.<opNumber> | Frequency (s)
rttMonCtrlAdminTimeout | 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)

### FTP operations

### MIB NAME | OID NUMBER | VALUE
--- | --- | ---
rttMonCtrlAdminRttType | 1.3.6.1.4.1.9.9.42.1.2.1.1.4.<opNumber> | 12 (Ftp)
rttMonEchoAdminProtocol | 1.3.6.1.4.1.9.9.42.1.2.2.1.1.<opNumber> | 30 (FtpAppl)
rttMonCtrlAdminOwner | 1.3.6.1.4.1.9.9.42.1.2.1.1.2.<opNumber> | See “OWNER Field Value”
rttMonCtrlAdminNvgen | 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)
<table>
<thead>
<tr>
<th>MIB NAME</th>
<th>OID NUMBER</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<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>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>rttMonScheduleAdminRttStart</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>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>1.3.6.1.4.1.9.9.42.1.2.2.1.16.&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>MIB NAME</td>
<td>OID NUMBER</td>
<td>VALUE</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------</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.&lt;opNumber&gt;</td>
<td>2 (IplcmpEcho)</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>1.3.6.1.4.1.9.9.42.1.2.2.1.16.&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>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>rttMonScheduleAdminRttStart</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**

<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.&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>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>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;opNum&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;opNum&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;opNum&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;opNum&gt;</td>
<td>Forever</td>
</tr>
<tr>
<td>rttMonScheduleAdminRttStart</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.2.&lt;opNum&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;opNum&gt;</td>
<td>Create &amp; Go (activation)</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>rttMonCtrlAdminRttType</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.4.&lt;opNum&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.&lt;opNum&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;opNum&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;opNum&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;opNum&gt;</td>
<td>VRF name (only if specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminSourceAddr</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.6.&lt;opNum&gt;</td>
<td>Source IP (only if specified)</td>
</tr>
<tr>
<td>rttMonEchoAdminTargetAddr</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.2.&lt;opNum&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;opNum&gt;</td>
<td>Target port</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>rttMonScheduleAdminRttStart</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>

**UDP Jitter 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>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>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>MIB NAME</td>
<td>OID NUMBER</td>
<td>VALUE</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>rttMonEchoAdminTOS</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.9.\langle opNumber\rangle</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.\langle opNumber\rangle</td>
<td>100</td>
</tr>
<tr>
<td>rttMonEchoAdminNumPackets</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.18.\langle opNumber\rangle</td>
<td>100</td>
</tr>
<tr>
<td>rttMonEchoAdminInterval</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.17.\langle opNumber\rangle</td>
<td>20</td>
</tr>
<tr>
<td>rttMonCtrlAdminThreshold</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.5.\langle opNumber\rangle</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.\langle opNumber\rangle</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.\langle opNumber\rangle</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.\langle opNumber\rangle</td>
<td>Forever</td>
</tr>
<tr>
<td>rttMonScheduleAdminRttStartTime</td>
<td>1.3.6.1.4.1.9.9.42.1.2.5.1.2.\langle opNumber\rangle</td>
<td>Now</td>
</tr>
<tr>
<td>rttMonCtrlAdminStatus</td>
<td>1.3.6.1.4.1.9.9.42.1.2.1.1.9.\langle opNumber\rangle</td>
<td>Create &amp; Go (activation)</td>
</tr>
</tbody>
</table>

VoIP UDP Jitter 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.\langle opNumber\rangle</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.\langle opNumber\rangle</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.\langle opNumber\rangle</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.\langle opNumber\rangle</td>
<td>1</td>
</tr>
<tr>
<td>rttMonEchoAdminVrfName</td>
<td>1.3.6.1.4.1.9.9.42.1.2.2.1.26.\langle opNumber\rangle</td>
<td>VRF name (only if specified)</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>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>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>
</tbody>
</table>
### MIB NAME | OID NUMBER | VALUE
--- | --- | ---
rttMonCtrlAdminFrequency | 1.3.6.1.4.1.9.9.42.1.2.1.1.6.<opNumber> | Frequency (s)
rttMonCtrlAdminTimeout | 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)

### 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**

configure terminal
ip sla <opNumber>
path-jitter <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 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
ip sla monitor schedule <opNumber> life forever start-time now
exit
RTR Syntax

configure terminal
rtr <opNumber>
type pathJitter dest-addr <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