

Configuration Guide

Network Quality Monitoring

This configuration guide helps users understand and configure ADTRAN Operating System (AOS) network quality monitoring (NQM) feature. This document includes an overview of NQM components, common applications, and detailed descriptions of Web-based graphical user interface (GUI) menus, and step-by-step configuration. There is a troubleshooting section that outlines proper use and interpretation of collected data on the AOS product(s).

For detailed CLI NQM commands, refer to the *AOS Command Reference Guide* (CRG) available online at <https://supportforums.adtran.com>.

Prerequisites to completely understanding this feature and configuration guide assumes the user has previous knowledge of data and voice network components, quality of service (QoS), and Network Time Protocol (NTP).

This guide consists of the following sections:

- *NQM Overview on page 2*
- *Hardware and Software Requirements and Limitations on page 4*
- *Configuring NQM on page 5*
- *Creating Probes and Tracks on page 6*
- *Configuring the Probe Responder on page 9*
- *Configuring NQM Using the CLI on page 12*
- *Troubleshooting on page 19*

NQM Overview

NQM is a collection of tools used to measure or verify the service level or quality of a network in real time by measuring and grading a network's path from an AOS device to another device. Network elements such as congestion and improper configuration can cause problems, such as packet loss, inter-packet delay variance, and latency, that can degrade network traffic between two endpoints. Voice and video network traffic is more sensitive to errors such as inter-packet delay variance and packet loss. Depending upon the results of the test(s) or probe(s), the AOS device can be configured to take actions to assist in network backup (via the route table). Therefore, NQM provides valuable information about the condition of the network that allows administrators to be aware of network issues, service quality, bandwidth utilization, and available resources by testing the quality between two endpoints.

Service Level Agreements (SLA), a contract purchased by the end user (administrator's company) that guarantees a certain QoS on the network, can be verified or tested using NQM probes. NQM enables administrators to examine network traffic to be proactive in maintaining a robust network.

Understanding Network Monitor Probes and Tracks

A network probe is a facility that can actively measure certain parameters across a network path. A network probe may optionally use the measured results and configured thresholds of performance to declare a pass or fail status related to the probe. ADTRAN's NQM feature consists of two new network monitor probe clients that generate test packets towards a probe endpoint and a network monitor probe server that responds to probe packets. The test traffic is generated at a source host and is sent to a target host with a participating traffic responder. Synchronized and accurate clock sources are only needed for proper functionality and measurement of the one-way delay on the network. The NTP server feature is used to provide synchronized timing to source and target remote devices to obtain credible performance results for one-way delay. Round-trip loss, delay, and Inter Packet Delay Variance (IPDV), do not require clock synchronization. A network probe can assist in troubleshooting, analyzing, or managing quality service levels.

A track is an object created to monitor a network probe for changes of state. The track can be configured to perform a specific action based upon the probe state detected. Association between a track and a probe occurs through referencing the probe in the track's configuration. Once the track is registered with the probe, whenever a change occurs with the probe's state, an event is sent to the track. Tracks are optional, and typically not used when solely collecting statistics on current network performance and quality.

Two-way Active Measurement Probe

The first of these two probes is called two-way active measurement protocol (TWAMP) probe. This probe uses methodology and architecture of the One-Way Active Measurement Protocol (OWAMP) to define an open protocol for measuring two-way or round-trip metrics. It uses a TCP control protocol to negotiate test sessions with a TWAMP server and generates UDP test traffic to take measurements. Use of this probe type requires that both endpoints have a properly synchronized time source to measure one-way delay and the far end must be running a TWAMP responder.



Use NTP on the platforms participating in TWAMP measurements in order to achieve valuable information. Incorrect or incomplete NTP configurations can cause unexpected TWAMP measurements.

ICMP Timestamp Probe

Internet Control Message Protocol (ICMP) timestamp probe, **icmp-timestamp**, is a **probe** type that generates ICMP timestamp request packets and listens for the corresponding reply packets. This allows the probe to measure one-way delay and inter-packet delay variance, two-way delay and inter-packet delay variance, and two-way packet loss. This probe type will provide a mechanism for testing loss, latency, and inter-packet delay variance across many different platforms (i.e., non-ADTRAN products) because it uses standard ICMP timestamp packets. Use of this probe type will require both probe endpoints to have synchronized (to at least a millisecond accuracy) time sources if one-way inter-packet delay variance measurements are desired. The ICMP timestamp probe type does not use a control protocol to set up test sessions. The probe's far end must simply respond to ICMP timestamp reply messages. The ICMP timestamp packet format limits the accuracy of delay measurements to +/-1 millisecond.



Use NTP on the platforms participating in ICMP timestamp probes in order to achieve valuable information. Incorrect or incomplete NTP configurations can cause unexpected ICMP timestamp measurements. The ICMP timestamp probe is not capable of reporting any information on the system clock status.

Probe Responder

The probe responder is the general term used for a variety of server applications that respond to certain network monitor probe types. The TWAMP probe responder encompasses the responder side of the TWAMP-Control protocol by responding to TWAMP-Control messages and acting as a remote endpoint for test packets. The ICMP-timestamp probe responder responds to ICMP timestamp request packets so that it can act as a remote endpoint for ICMP timestamp probes. The UDP-Echo probe responder responds to udp-echo request packets.

NQM Functionality on the Router

NQM can detect network issues affecting the quality of voice on the network by testing the connectivity between two endpoints. In [Figure 1](#), a probe is sent from Site A to Site B to test the network for the service quality provided from the carrier. Issues detected on the network are typically the service provider's responsibility, but misconfigurations and network load can cause inter-packet delay variance, latency, and packet loss. Site A is the originator of the probe and Site B is the responder. The timestamps between $t1$ and $t3$ ([Figure 1](#)) are the measurements between the endpoints that are used to calculate performance metrics. If the probe fails, tracks can be used to take appropriate action to manage the network for optimal performance. $T2$ minus $T1$ is the delay from probe to responder and $T3$ minus $T4$ is the delay from the responder to the probe initiator. Various computations involving these times allow the determination of delays involved. Comparing these times from a given packet to the next packet are used to determine inter-packet delay variance values.

Test Protocol Timestamps

$T1$ is the point in time that the test packet left the probe going towards the responder.

$T2$ is the point in time the test packet was received at the responder.

$T3$ is the point in time that the test packet was sent from the responder back to the probe.

$T4$ is the point in time that the test packet was received by the probe.

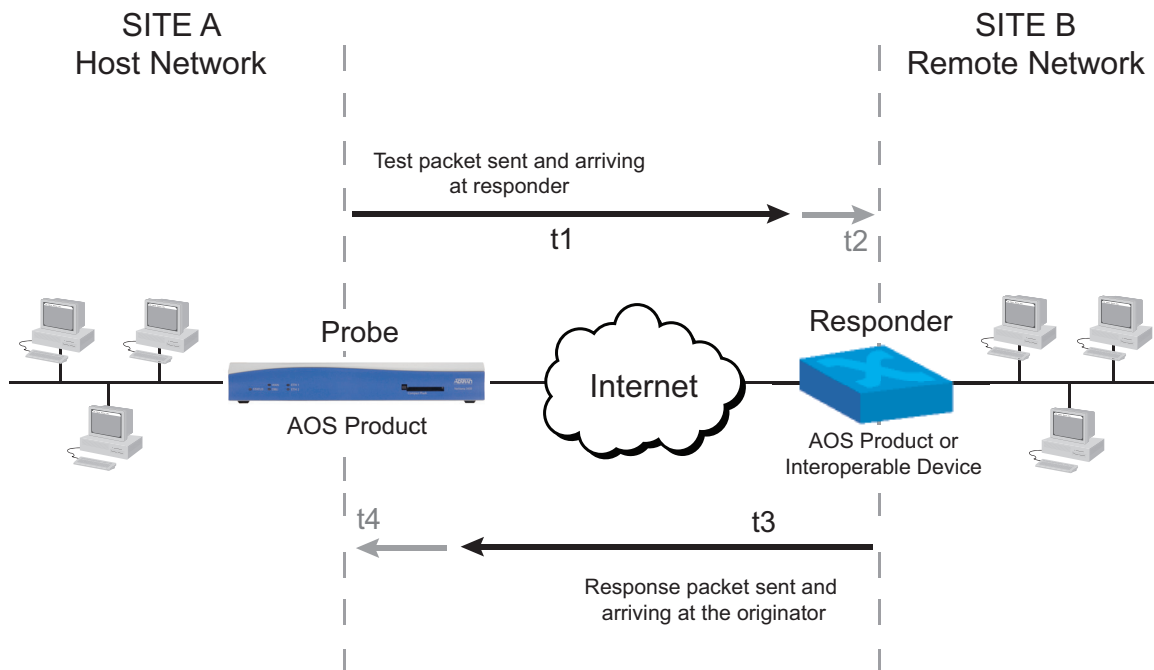


Figure 1. Example of Basic NQM Applications

NQM Usage Scenarios

An administrator can set up probes without tracks to continuously verify a network's compliance with desired network criteria or an SLA. When the configured thresholds are exceeded, the probe change state (pass or fail) and the track will take action, notifying the administrator that something is below average. The user interface(s) will display the results of the latest probe operation and optionally a circular history of the latest probe operations. This type of data may be useful when troubleshooting problems with network applications such as voice over IP (VoIP) or multimedia streaming.

Administrators can setup a network monitor probe and track to cause the automatic switchover to a backup link if the primary link's measurements fall outside of a defined range of acceptable values. This would permit proactive restoration of service levels.

Use of a two-way ping utility may be used as real time troubleshooting tool during initial installs of a router or network to help characterize and troubleshoot network performance issues.

Hardware and Software Requirements and Limitations

NQM was introduced in firmware AOS 17.2 for AOS products as outlined in the *AOS Product Feature Matrix*, available online at <https://supportforums.adtran.com>.

As of AOS firmware release R11.2.0, virtual routing and forwarding (VRF) is supported by the NQM feature. Probes that support VRF functionality are HTTP Request, ICMP Echo, ICMP Timestamp, TCP Connect, and TWAMP probes. Responders that support VRF functionality are ICMP Timestamp, TWAMP, and UDP Echo responders. When VRFs are configured, the probe or responder service is limited to the specified VRF. If no VRF is configured, the service is limited to the default (unnamed) VRF. When

VRF is configured for probe responders, multiple source interfaces can be specified, resulting in one source interface for each VRF. For more information about VRF configuration, and its use in AOS products, refer to the guide [Configuring Multi-VRF in AOS](https://supportforums.adtran.com) available online at <https://supportforums.adtran.com>.

Configuring NQM

The following steps are required to implement NQM in AOS:

- Configure the probe (destination)
- (Optional) Configure the track (failure action)
- Configure the responder (remote device)

Setting up NQM Using the GUI

Access the GUI from any Web browser on your network by following these steps:

1. Connect the unit to your PC using the first Ethernet port on the unit with a 10/100BaseT Ethernet cable.
2. Set your PC to obtain an IP address automatically via Dynamic Host Configuration Protocol (DHCP), or change your PC to a fixed IP address of 10.10.10.2. If you cannot change the PC's IP address, you will need to change the unit's IP address using the CLI.
3. Enter the unit's IP address in your browser's address line. The default IP address is 10.10.10.1. You will then be prompted for the user name and password (the default settings are **admin** and **password**). After entering the correct user name and password, the initial GUI menu will appear.

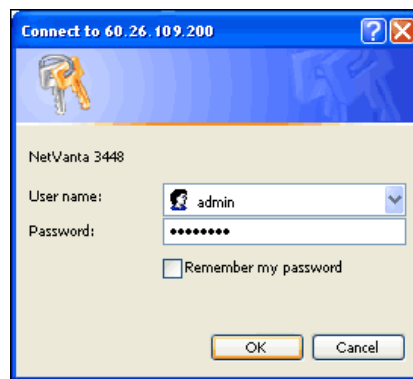



Figure 2. GUI Login Screen



While navigating the GUI, you will notice question mark  symbols that indicate additional information is available. Simply place your cursor over the symbol to view the additional information.



Updated configurations must be saved to nonvolatile memory (NVRAM) to retain new changes after a loss of power or a reboot. To quickly save your configuration at any time while in the GUI, select **SAVE** at the top right of your current menu.

Creating Probes and Tracks

Use the following steps to manually configure tracks and probes using the GUI.

1. Navigate to **Data > Network Monitor > Probes/Tracks** from the main menu to manually create and configure a new probe and track.

Enter a name for the probe and select the **Type** of probe to create. Next, select the **Create** button to proceed to the configuration menu.

Figure 3. NQM Create Probe Menu

2. Enable the probe by selecting the **Enable** check box. Modify the default settings and enter the **Destination** information to complete the probe configuration.

"Probe HSV to ACK" Configuration

Warning: ICMP Timestamp and Two-way Active Measurement (TWAMP) probes require NTP time server. Please go to the ["Time Server"](#) page to configure the unit to use NTP time server.

Configuration | **Advanced**

Edit the information for probe HSV to ACK below.

Enable:	<input checked="" type="checkbox"/>	Enable the probe.
Probe Period:	60 (secs)	Time between probe test attempts. (1-65535)
Timeout:	2000 (msecs)	Time to wait before declaring test failed. Must be less than the probe-period. (1-4,294,967,295)
Send Schedule:	20 (msecs)	Time between start of an individual packet send operation. (5-5000)
DSCP:	0	Specify the diffServ code value. (0-63)
Number of Packets:	10	Number of packets to send and receive during one probe operation. (1-1000)
History Depth (optional):	1	Number of probe operation results to keep. (1-120)
Tolerance:	Mode: None	Configure the tolerance and its specifications for probe state transitions. ?
Payload Size:	0	Specify payload size. (0-1462)
Payload Data:	Data Type: Zeroes	Configure the payload data. ?
Destination:	IP/Hostname: 208.61.209.10 Port: 0	Enter destination IP address or a hostname and a port number (optional). (1-65535)
Source (optional):	IP: 208 . 61 . 209 . 220 Port: 0	Enter source IP address and a source port. Source port value of 0 means auto-select the source port. (0-65535)

Reset Apply

If you have not configured the unit to use a NTP time server, do so at this time by selecting **Time Server**.

Advanced settings allow you to set up more complex threshold values for probe states to transition between pass and fail.

Select the **Advanced** tab to configure the probe to measure Inter Packet Delayed Variation (IPDV-abs) values (difference between two test packets, delay values, and packet loss for probe state transitions. Passing and failing values for IPDV-abs and delay values are in milliseconds.

Enter the **Destination** IP address or host name of the remote site to test the connectivity from end to end.

Figure 4. NQM Probe Configuration Menu

- Optional. Navigate to **Data > Network Monitor > Probes/Tracks** once the probe is created and select the link (Probe name) to modify the probe or to view its statistics and configuration.

NQM Track Configuration

- Optional. To manually create and configure a new track, return to the main NQM menu, **Data > Network Monitor > Probes/Tracks**. Enter a name for the track and select **Create** to proceed with the track configuration. The track requires configured thresholds on the associated probe in order to be effective. Refer to the **Advanced** tab in [Figure 4](#).

System

- Data**
 - Router / Bridge
 - Default Gateway
 - Routing
 - Route table
 - IP Interfaces
 - Loopback Interfaces
 - GRE Tunnels
 - QoS Wizard
 - QoS Maps
 - Bridging
 - Spanning Tree
 - UDP Relay
 - Demand Routing
 - VRRP
- Firewall**
 - Firewall Wizard
 - Firewall / ACLs
 - Security Zones
- Wireless**
 - AC / AP Discovery
 - APs / Radios / VAPs
 - Clients
 - MAC Access List
 - AP Firmware
- VPN**
 - VPN Wizard
 - VPN Peers
 - Certificates
- Network Monitor**
 - Wizard
 - Probes / Tracks
 - Probe Responder
- URL Filtering**
 - URL Filters
 - Top Websites

Create probes

Use this form to create and delete probes. Click on the link below on an appropriate probe name to modify the probe or to view its statistics and configuration.

Probe Name: *Enter probe name.*

Type: *Specify the probe type.*

<input type="checkbox"/>	Probe	Type	Status
<input type="checkbox"/>	CorporatePing	ICMP Echo	Enabled
<input type="checkbox"/>	HSV to ACK	ICMP Timestamp	Disabled

Create Tracks

Use this form to create, configure and delete tracks. To edit an existing track, click on the track name listed below.

Create a "track action" by associating tracks with [routes](#) or [interfaces](#).

WARNING: Modifying an existing track will replace the configuration for that track.

Track Name: *Enter track name.*

<input type="checkbox"/>	Track	Status	Test Logic
<input type="checkbox"/>	CorporatePing	Enabled	No Operation

Enter a name for the track and select the **Create** button to proceed to the configuration menu.

Figure 5. NQM Create Tracks Menu

5. Enable the track by selecting the **ENABLE** check box. The track can be associated with a combination of up to five objects (probes and schedules).

"Track HSV Backup" Configuration

Enter the appropriate information below to create a track.

Enable: *Enable the track.*

Dampening-interval: *Specify the dampening-interval in seconds. (1-4,294,967,295)*

Set Test Objects:

Logical Operator:

Object Type	Object	Negate
Probe	HSV to ACK	<input type="checkbox"/>
Probe	Orlando Sit...	<input type="checkbox"/>
<Select>		
<Select>		
<Select>		

Execute TCL:

If you want to negate the object in the logic, check the **Negate** check box. The logical operator describes how the objects should be evaluated logically.

Optionally, set a track action using a TCL script based on the result(s) of the probe(s). TCL files must have a .tcl extension for it to show up on the list. The **Track State** and **Script** option will appear when the **Execute TCL** option is checked.

Figure 6. NQM Track Configuration Menu

6. Navigate to **Data > Network Monitor > Probes/Tracks** once the track is created and select the link (**Track name**) to modify the track or to view its statistics and configuration.

Configuring the Probe Responder

Use this section to configure the target (or remote) unit(s) to respond to a probe (UDP echo packets, ICMP timestamp packets, or TWAMP packets).

1. To create a responder, navigate to **Data > Network Monitor > Probe Responder** to assign a **Packet Type**, and select **Create** to proceed with the responder configuration.

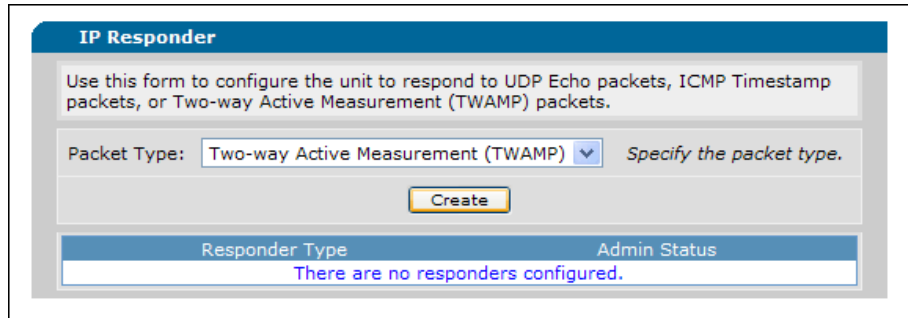


Figure 7. NQM Create Responder Menu

2. Enable the responder by selecting the **Enable** check box and select the **Source Interface**.

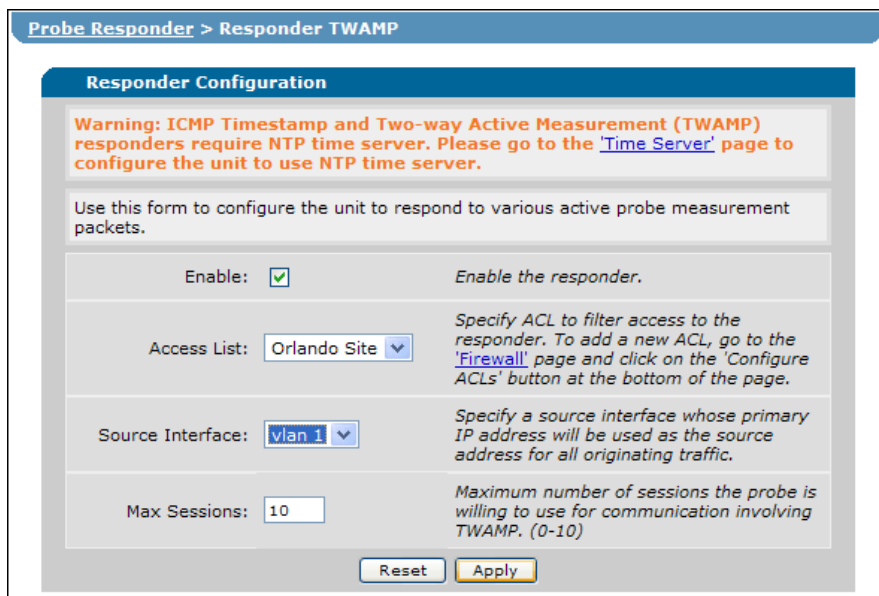


Figure 8. NQM Responder Configuration Menu

3. Navigate to **Data > Network Monitor > Probes Responder** once the responder has been created and select the link (**Responder Type**) to access the responder configuration or to view its statistics (**Responder Statistics**).

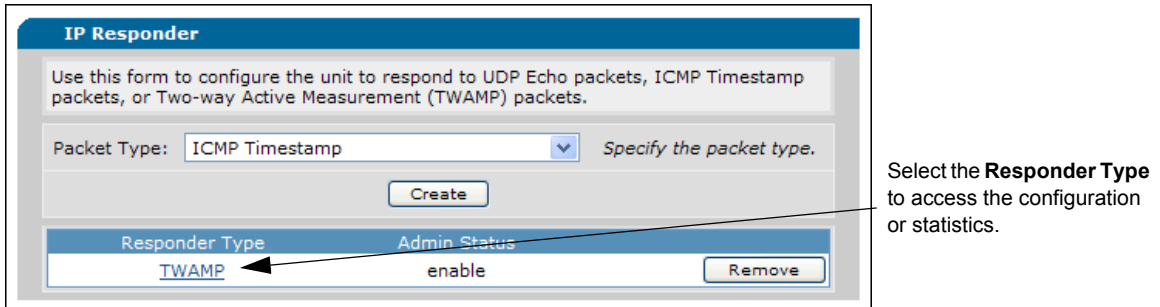


Figure 9. NQM IP Responder Type menu

4. Use the menu below to modify the configuration or view the **Responder Statistics**.

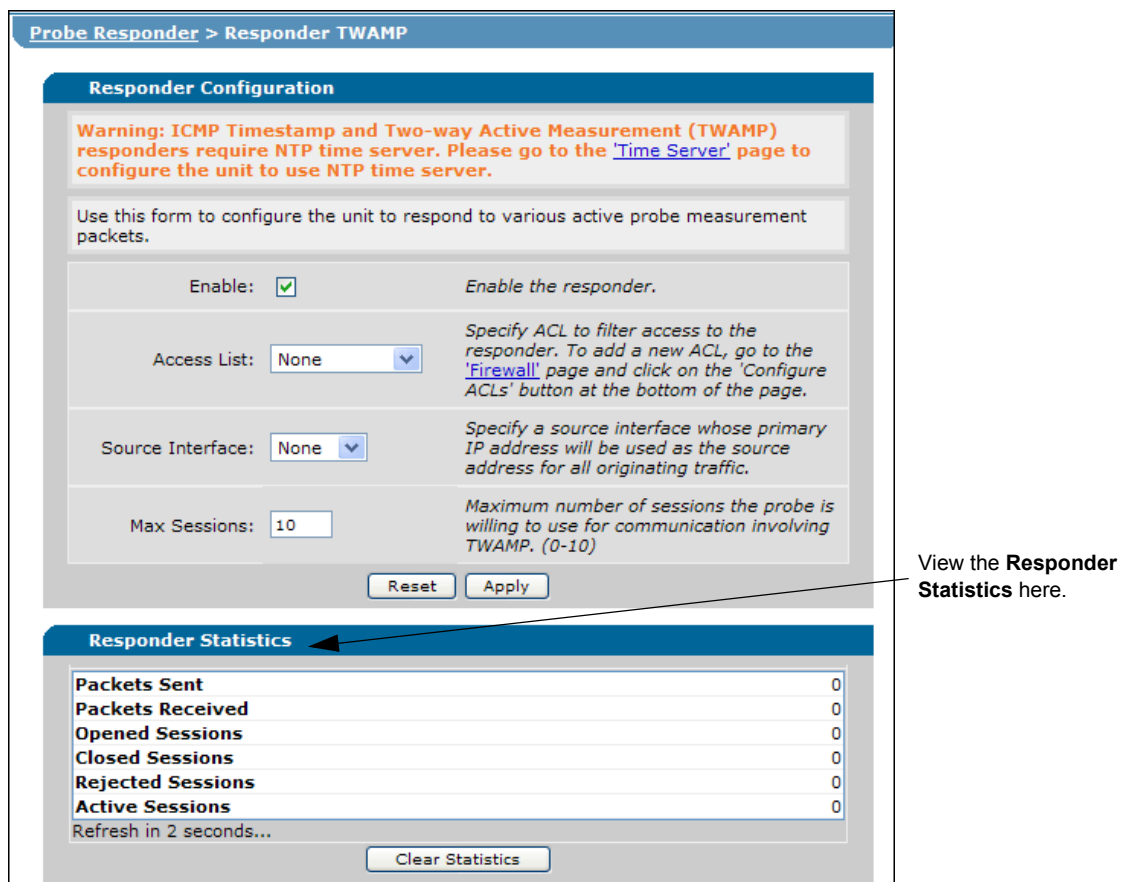


Figure 10. NQM Responder Statistics Menu

Executing a TWAMP Ping

Use two-way ping utility to execute a TWAMP session towards a remote responder that measures packet loss, delay, and inter-packet delay variance.

Navigate to **Utilities > System > Two-way Ping** to test the connectivity to the specified destination. Select **Start Ping** to begin the test.

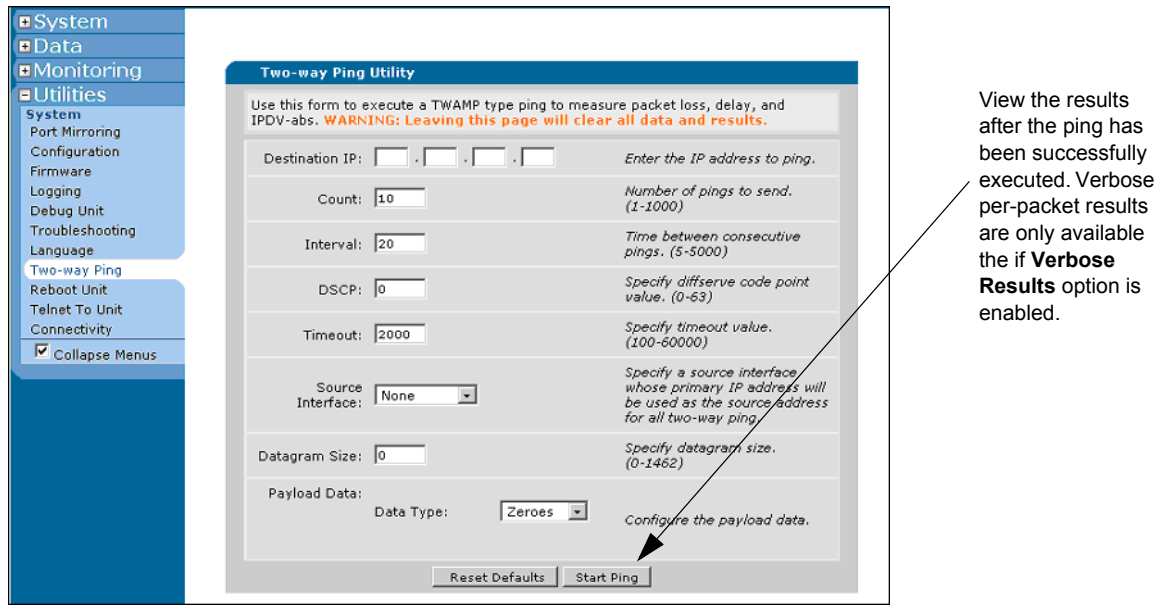


Figure 11. Two-Way Ping Utility Menu

Configuring NQM Using the CLI



*The configuration parameters used in the example are for instructional purposes only. Please replace all underlined entries (example) with your specific parameters to configure your application. For detailed information on specific commands and advanced options, refer to the *AOS Command Reference Guide* provided online at <https://supportforums.adtran.com>.*

The NQM feature requires the use of NTP to provide accurate real time clock data to the devices. The command appears as follows:

```
(config)#ntp server <IP address> [prefer | source | version]
```

<IP address> Specifies the host name or IP address of the server with the NTP system.

prefer Defines the specified server's synchronization as preferred over all other configured NTP servers.

source Specifies the source interface to use for this particular server.

version Specifies the version number for outgoing NTP packets.

Step 1: Create the Probe

The *Example Configurations on page 16* demonstrate how to create a TWAMP probe and responder. This same method is very similar for creating other probe types. The command appears as follows:

```
(config)#probe <name> [icmp-timestamp | twamp]
```

<name> Specifies the alphanumeric description or identity of the probe. Use the **no** form of this command to delete the probe and the setting associated with the probe.

Optional. Use the **source-address** command to specify the IP address of the host device sending the probe. The command appears as follows:

```
(config)#source-address <ip address>
```

<ip address> Specifies the host device by entering the host name or IP address.

Next, use the **destination** command to specify the IP address or host name of the target device. Only one **destination** is allowed per probe. The command appears as follows:

```
(config)#destination <ip address> port <value>
```

<host name | IP address> Specifies the target device by entering the host name or IP address.

port <value> Optional. Specifies the port number. The default is **0**. The range is **0** to **65535**.

Command Syntax

The following command settings are optional for the basic setup because default settings are loaded in your unit prior to factory release:

```
(config-probe-Houston)#vrf <name>
```

<name> Specifies the VRF in which the probe operates. If no VRF is specified, the probe operates within the default (unnamed) VRF.

```
(config-probe-Houston)#history-depth <value>
```

<value> Specifies the amount of probe results to store in the history. The default is **1**. The range is **1** to **120**.

```
(config-probe-Houston)#num-packets <value>
```

<value> Specifies the number of test packets to send during the one probe operation. The use of two or more test packets is required to obtain measurements of packet loss and delay. The default is **10**. The range is **1** to **1000**.

```
(config-probe-Houston)#period <value>
```

<value> Specifies the time (in seconds) between probe test attempts. The default is **60** seconds. The range is **1** to **65535**.

```
(config-probe-Houston)#threshold ipdv-abs [in | out | round-trip] [avg | max | min] <fail value>
<pass value>
```

[in | out | round-trip] Specifies the inbound, outbound, or round trip absolute IPDV.

[avg | max | min] Specifies the average, maximum, or minimum absolute IPDV.

<fail value> Specifies the failing threshold (in milliseconds) for the absolute IPDV values measured by the probe. The probe test is considered a failure if the absolute IPDV crosses this threshold and subsequent probe tests will not be considered successful until they cross the passing threshold. The default is **4294967295**. The range is **0** to **4294967295**.

<pass value> Specifies the passing threshold (in milliseconds) for the absolute IPDV values measured by the probe. Once the absolute IPDV value of a probe test crosses the failing threshold, later probe tests will not be considered successful until they cross the passing threshold. The default is **4294967295**. The range is **0** to **4294967295**.

```
(config-probe-Houston)#threshold packet-loss round-trip <fail value> <pass value>
```

<fail value> Specifies the number of packets allowed to be lost before triggering a failed state change in the probe. The probe test is considered a failure if the round-trip packet loss crosses this threshold and subsequent probe tests will not be considered successful until they cross the passing threshold. The default is **1000**. The range is **1** to **1000**.

<pass> Specifies the lower number of packets allowed to be lost before triggering a passed state change in the probe. Once the round-trip packet loss of a probe test crosses the failing threshold, later probe tests will not be considered successful until they cross the passing threshold. The default is **1000**. The range is **1** to **1000**.

```
(config-probe-Houston)#timeout <value>
```

<value> Specifies the amount of time (in milliseconds) that the probe will wait for the response to a test packet before considering it lost. The default is **2000**. The range is **1** to **900000**.

```
(config-probe-Houston)#tolerance [consecutive | rate] fail <value> [of <value> | pass <value>]
```

[consecutive | rate] Specifies the tolerance conditions for the probe's pass or fail states.

fail <value> Specifies the number of failures that must occur before transitioning the probe to the FAIL state. The default is **1**. The range is **1** to **254**.

of <value> Specifies a number of test probes changes during the specified limit before triggering a failed change of state in the probe. The default is **1**. The range is **1** to **255**.

pass <value> Specifies a number of positive changes before triggering a passed change of state in the probe. The default is **1**. The range is **1** to **255**.

Issue a **no shutdown** to enable the probe that is **shutdown** by default. The command appears as follows:

```
(config-probe-Houston)#no shutdown
```

Step 2: Create the AOS Responder (Remote Device)

The target device must be configured to respond to the probe requests. Use the example below to configure an AOS device to respond to ICMP timestamp, TWAMP, or UDP echo probes. The command appears as follows:

```
(config)#probe responder [icmp-timestamp | twamp | udp-echo]
```

[icmp-timestamp | twamp | udp-echo] Specifies the device to respond to ICMP timestamp, TWAMP, or UDP echo packets respectively.

Optional. Configure the source interface with the primary IP address to use as the source address for all responder traffic originated from the device. The command appears as follows:

```
(config-responder-twamp)#[vrf <name>] source interface <name>
```

vrf <name> Optionally specifies the VRF in which the responder operates. If no VRF is specified, the responder operates within the default (unnamed) VRF.

<name> Specifies the interface used for all responder traffic responses.



*The **[vrf <name>] source interface <name>** command is only available on TWAMP and UDP-Echo responders.*

Optional. Use an access control list (ACL) to restrict access to the probe responder. The command appears as follows:

```
(config-responder-twamp)#access-class <name> in [vrf <name>]
```

<name> Specifies the ACL to use manage to responder responses.

vrf <name> Specifies the VRF in which the ACL is used to use manage to responder responses. If no VRF is specified, the default (unnamed) VRF is used.

Optional and only available on TWAMP responders. Specify the maximum number of simultaneous responder type control sessions allowed to be in use. The command appears as follows:

```
(config-responder-twamp)#max-sessions <value>
```

<value> Specifies the maximum number of simultaneous sessions allowed.

Issue a **no shutdown** to enable the responder that is **shutdown** by default. The command appears as follows:

```
(config-responder-twamp)#no shutdown
```

Example Configurations

The following examples are designed to enhance the understanding of CLI configuration of NQM on AOS products:

Example AOS NTP Server Configuration (Host and Remote)

Note: The NTP server configuration is only required for accurate one-way delay measurements.

```
>enable
#configure terminal
(config)#ntp server 208.61.209.244 prefer
(config)#ntp server 208.61.209.211
(config)#
2008.03.22 04:39.59 NTP 4.2.4p0
```

Example TWAMP (Host Device) Configuration

```
>enable
#configure terminal
(config)#probe Houston twamp
(config-probe-Houston)#destination 208.61.209.223
(config-probe-Houston)#history-depth 50
(config-probe-Houston)#num-packets 100
(config-probe-Houston)#period 90
(config-probe-Houston)#threshold ipdv-abs in max 200 150
(config-probe-Houston)#threshold packet-loss round-trip 100 100
(config-probe-Houston)#timeout 2000
(config-probe-Houston)#tolerance consecutive fail 3 pass 10
(config-probe-Houston)#no shutdown
(config-probe-Houston)#exit
(config)#
```

Example AOS TWAMP Responder (Remote Device) Configuration

```
>enable
#configure terminal
(config)#probe responder twamp
(config-responder-twamp)#source interface vlan 1
(config-responder-twamp)#access-class PERMIT_ANY in
(config-responder-twamp)#max-sessions 10
(config-responder-twamp)#no shutdown
(config-responder-twamp)#exit
(config)#
```


CLI Configuration Command Summary

Table 1. Command Summary Table

Step	Command	Explanation
Step 1	(config)#ntp server <IP address> [prefer source version]	Specifies the NTP server that will provide synchronized timing. Use the no form of this command to delete the NTP sever setting. By default, no NTP servers are configured.
	(config)#probe <name> [icmp-timestamp twamp]	Specifies a OWAMP or TWAMP probe. Use the no form of this command to delete the probe and the setting associated with the probe. By default, no probes are configured.
	(config-probe-name)#data [pattern [hex ascii] <string> zero random]	Specifies the data type used to pad a measurement packet if needed by setting the size command. Use the no form of this command to restore the default setting. The default value is zero .
	(config-probe-name)#vrf <name>	Specifies the VRF in which the probe operates. If no VRF is specified, the probe operates within the default (unnamed) VRF.
	(config-probe-name)#destination [<host name> <ip address>] [port <value>]	Specifies the destination of the probe by entering the IP address or host name and the port number. The address and port number are required. Only one destination can be configured per probe. Use the no form of this command to remove the destination information from the probe.
	(config-probe-name)#dscp <value>	Specifies the DiffServe code point value to be placed in the test packets. The range is 0 to 63 . Use the no form of this command to restore the default setting. The default DSCP value is 0 .
	(config-probe-name)#size <value>	Specifies the payload packet size. The range is 0 to 1462 . Use the no form of this command to restore the default setting. The default value is 0 .
	(config-probe-name)#source-address <ip address>	Specifies the source port of the TWAMP probe packets by assigning an IP address. Use the no form of this command to command removes the source address from the probe.

Table 1. Command Summary Table (Continued)

Step	Command	Explanation
	(config-probe-name)# source-port <value>	Specifies the source port of the TWAMP probe packets by assigning a port number between 0 and 65534 . Use the no form of this command to remove the source port setting. The default settings for the source port is 0 .
	(config-probe-name)# num-packets <packet-count>	Specifies the number of packets to send and receive during one probe operation. The range is 1 to 1000 . Use the no form of this command to restore the default setting. The default value is 10 .
	(config-probe-name)# history-depth <value>	Specifies the amount of probe test results to store in the history. The default is 1 . The range is 1 to 120 .
	(config-probe-name)# period <value>	Specifies the time between each test probe attempt. Use the no form of this command to restore the default setting. The default is 60 seconds. The range is 1 to 65535 .
	(config-probe-name)# send-schedule periodic <schedule-time>	Specifies the schedule type and time in milliseconds between each individual packet send operation. Use the no form of this command to restore the default setting. The default value is schedule type is periodic (only option at this time) and the schedule time is 20 . The schedule time range is 5 to 5000 .
	(config-probe-name)# threshold ipdv-abs [in out round-trip] [min avg max] <fail value> <pass value>	Specifies the criteria for a probe to be declared as passing or failing for the delay or latency values determined by the probe. Fail and pass values are expressed as milliseconds. Use the no form of this command to remove the specified criteria. The default value is 4294967295 for the passing and failing values. The range for the passing and failing latency is 0 to 4294967295 .
	(config-probe-name)# threshold packet-loss round-trip <fail value> <pass value>	Specifies the criteria for a probe to be declared as passing or failing for the amount of round trip packet loss measured by the probe. Use the no version of this command to remove the criteria. The default is 1000 for passing and failing the probe. The range is 1 to 1000 .

Table 1. Command Summary Table (Continued)

Step	Command	Explanation
Step 2	(config)# probe responder [icmp-timestamp twamp udp-echo]	Specifies an ICMP timestamp, TWAMP, or UDP echo probe responder. Use the no form of this command to delete the responder and the setting associated with the responder. By default, no responders are configured.
	(config-responder-type)# access-class <name> in [vrf <name>]	Specifies an ACL to filter access to the responder. The optional vrf parameter specifies the VRF in which the responder operates. If no VRF is specified, the default (unnamed) VRF is used. Use the no form of this command to delete the ACL.
	(config-responder-type)# max-sessions <value>	Specifies the maximum number of simultaneous responder type control session allowed in use. Use the no form of this command to return to the default number of sessions. The default is 10 . The range is 1 to 10 .
	(config-responder-type)#[vrf <name>] source-interface <address>	Specifies an interface whose primary IP address will be used as the source address when responding to probe requests. The optional vrf parameter specifies the VRF in which the responder operates. If no VRF is specified, the default (unnamed) VRF is used. Use the no form of this command to delete the source interface setting.
	(config-responder-type)# no shutdown	Enables the device to respond to probe packets. Use shutdown to disable the responder. The responder is shutdown by default.



For a complete list of NQM commands, refer to the *AOS Command Reference Guide* available online at <https://supportforums.adtran.com>.

Troubleshooting


NQM is primarily a monitoring and troubleshooting tool. The *Example of Basic NQM Applications on page 4* illustrates using NQM to help identify round-trip delay, one-way delay, inter-packet delay variance, packet loss, and echo connectivity between two endpoints. Use probes and responders to narrow down the path(s) of network problem(s) causing VoIP issues. If poor metrics are discovered on the WAN (public) interface packets, check the physical WAN interface for configuration and connectivity issues prior to contacting your service provider.

Check the public interface for errors, discards, or throttles to eliminate the AOS device as the source of any network issues. It is possible for the AOS device to drop packets due to interface errors, network load issues, or incorrect speed/duplex negotiations. If there are no dropped packets, errors, or throttles, and the speed and duplex settings are correct, the AOS device can be cleared in the troubleshooting exercise. Also test the endpoint(s) for proper connectivity, functionality, and configuration.

The administrator can use the circular history to search for the source of the lost packets and inter-packet delay variance. Using this technique can quickly identify specific paths or endpoints with errors. If only one direction or endpoint has errors, that particular endpoint or connection is faulty. If multiple endpoints have errors, the problem is most likely a general issue with the uplink to the ISP (network congestion due to provisioning or other errors). A **traceroute** can be performed from the AOS device to the endpoint to determine which portion of the network is experiencing the problem. Also, refer to [NQM Usage Scenarios on page 4](#) for description on how to troubleshoot using NQM.

Troubleshooting Command Summary

After configuring NQM in the CLI, several different commands can be issued from the Enable mode prompt to assist in troubleshooting VoIP issues. Use the summary of **show** commands in [Table 2](#).



NOTE *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

Table 2. AOS NQM Troubleshooting Commands

Command	Explanation
#show probe [<probe-name> responder [twamp icmp-timestamp udp-echo] [realtime] statistics [history]]	Displays the probe status. Specify a probe name to display only information pertaining to that probe. This command will not display any statistics when NQM is disabled.
>twping [<dest-ip>] [port <port> interval <value> count <value> dscp <value> timeout <value> size <value>]	Executes a Two-Way Active Measurement Protocol test with a cooperating responder to measure the packet loss, delay and inter-packet delay variance on the network path between this device and the responder. The statistics are also displayed after the test ping.
>debug twping	Debugs the TWAMP control and test client associated with the two-way ping utility.

Sample Output

The following is sample output from the **show probe <name>** command:

```
# show probe Houston
0-----1-----2-----3-----4-----5-----6-----7-----8
1234567890123456789012345678901234567890123456789012345678901234567890
Probe Houston:
Current State: PASS Admin. Status: UP
Type: TWAMP Period: 60 Timeout: 1500
Source: 192.168.1.255:17001 Destination: 10.10.20.254:17000
Data Size: 14 Num-packets 100 DSCP: 0
Data pad: Zero
Send-schedule: 20 msec Type: periodic
Authentication Mode: open Key: not set
Tracked by: Nothing
Tests Run: 194 Failed: 1
Tolerance: not set
Time in current state: 1 days, 2 hours, 50 minutes, 7 seconds
Packet Loss          fail          pass
Round Trip          1000          1000
```

The following is sample output from the **show probe <name> statistics** command:

```
# show probe Houston statistics
0-----1-----2-----3-----4-----5-----6-----7-----8
1234567890123456789012345678901234567890123456789012345678901234567890
Probe Houston:
Start Time: 2008/02/31 12:42:36.345
End Time: 2008/02/31 12:42:38.754
Local Clock: Sync, Error Est 3.5 ms
Remote Clock: Sync, Error Est 3.5 ms
Packets Sent: 100
Packet Loss
round-trip num = 0
Delay
round-trip min/avg/max = 84 101 121 ms
num/sum/sum2 = 10 1017 104774 ms
out min/avg/max = 52 52 52 ms
num/sum/sum2 = 10 521 27164 ms
in min/avg/max = 32 49 69 ms
num/sum/sum2 = 10 496 25892 ms
IPDV-abs
round-trip min/avg/max = 0 9 17 ms
num/sum/sum2 = 9 89 1208 ms
out min/avg/max = 0 0 0 ms
num/sum/sum2 = 9 0 0 ms
in min/avg/max = 0 9 17 ms
num/sum/sum2 = 9 89 1208 ms
IPDV-pos
round-trip min/avg/max = 0 8 17 ms
num/sum/sum2 = 4 32 432 ms
out min/avg/max = 0 0 0 ms
num/sum/sum2 = 6 0 0 ms
in min/avg/max = 4 10 17 ms
num/sum/sum2 = 3 32 432 ms
IPDV-neg
round-trip min/avg/max = 3 11 17 ms
num/sum/sum2 = 5 57 775 ms
out min/avg/max = 0 0 0 ms
num/sum/sum2 = 3 0 0 ms
in min/avg/max = 0 9 17 ms
num/sum/sum2 = 6 57 775 ms
```

The following is sample output from the **show probe responder twamp** command:

#show probe responder twamp

```
0-----1-----2-----3-----4-----5-----6-----7-----8
1234567890123456789012345678901234567890123456789012345678901234567890
TWAMP-Test: 360 rcvd, 360 sent
TWAMP-Control: 20 sessions opened, 18 sessions closed,
                3 sessions rejected, 2 sessions active
```

The following is sample output from the **show probe responder icmp-timestamp** command:

#show probe responder icmp-timestamp

```
0-----1-----2-----3-----4-----5-----6-----7-----8
1234567890123456789012345678901234567890123456789012345678901234567890
ICMP Timestamp: 125 rcvd, 125 sent
```

The following is sample output from the **show probe responder udp-echo** command:

#show probe responder udp-echo

```
Admin. Status: UP
Rcvd  Sent  FFE Hits  Drops
41    41    N/A       N/A
N/A   N/A    19        0
```



*Output from the **show probe responder udp-echo** command can vary depending on whether the hardware fast forward engine (FFE) feature is enabled or disabled on the AOS device. When hardware FFE is enabled, the **Rcvd** and **Sent** columns of the command output appear as **N/A**, and the **FFE Hits** and **Drops** columns of the output display current packet FFE and drop information. When hardware FFE is disabled, the command output displays current received (**Rcvd**) and sent (**Sent**) packet information and displays **N/A** for the **FFE Hits** and **Drops** columns.*

The following is sample output from the **twping 208.61.209.221** command:

```
# twping 208.61.209.221 verbose
0-----1-----2-----3-----4-----5-----6-----7-----8
1234567890123456789012345678901234567890123456789012345678901234567890
Type CTRL+C to abort. Test will complete in approximately 7 seconds.
--- twping statistics from [208.61.209.1]:1292 to [208.61.209.221]:1081

SID: 000000053000000000
Seq #   Delay      Delay      Local Clock      Remote Clock
      out, ms   in, ms   status, err in mS   status, err in mS

0       1         0       sync 0.001907       sync  0.503540
1       2         0       sync 0.001907       sync  0.503540
2       2         0       sync 0.001907       sync  0.503540
3       1         0       sync 0.001907       sync  0.503540
4       2         0       sync 0.001907       sync  0.503540
5       1         0       sync 0.001907       sync  0.503540
6       1         0       sync 0.001907       sync  0.503540
7       1         0       sync 0.001907       sync  0.503540
8       2         0       sync 0.001907       sync  0.503540

10 sent, 0 lost (0.000%)

Delay
round-trip  min/avg/max =          2          2          2 ms
            num/sum/sum2 =          9         20         45 ms

out         min/avg/max =          1          2          2 ms
            num/sum/sum2 =          9         18         39 ms

in          min/avg/max =          0          0          0 ms
            num/sum/sum2 =          9          1          0 ms

IPDV-abs
round-trip  min/avg/max =          0          0          0 ms
            num/sum/sum2 =          8          2          1 ms

out         min/avg/max =          0          0          0 ms
            num/sum/sum2 =          8          2          1 ms

in          min/avg/max =          0          0          0 ms
            num/sum/sum2 =          8          0          0 ms

IPDV-pos
round-trip  min/avg/max =          0          0          0 ms
            num/sum/sum2 =          4          1          0 ms

out         min/avg/max =          0          0          0 ms
            num/sum/sum2 =          6          1          0 ms

in          min/avg/max =          0          0          0 ms
            num/sum/sum2 =          1          0          0 ms

IPDV-neg
round-trip  min/avg/max =          0          0          0 ms
            num/sum/sum2 =          4          1          0 ms

out         min/avg/max =          0          0          0 ms
            num/sum/sum2 =          2          0          0 ms

in          min/avg/max =          0          0          0 ms
            num/sum/sum2 =          7          0          0 ms

clock error
local = sync, 0.001907 ms
remote = sync, 0.503540 ms
```