# Network Service Monitor (NSM)

## Teldat Dm749-I

## Legal Notice

Warranty

This publication is subject to change.

Teldat offers no warranty whatsoever for information contained in this manual.

Teldat is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

# Table of Contents

# I Related Documents

Teldat Dm723-I DNS

Teldat Dm745-I Policy Routing

Teldat Dm775-I VRF Lite Facility

Teldat Dm786-I AFS

# Chapter 1 Introduction

## 1.1 Introducing NSM

This manual focuses on the router's Network Service Monitor (NSM) feature, which provides monitoring information on the network's level of service (through several probes) and also measures performance.

NSM is an internal router process that monitors the status of the network by measuring the response time, the time it takes to download web pages, jitters (packet delay variation), connection times, packet losses, etc.

In order to carry out these operations, the NSM feature must be installed and enabled on our router (as well as an IP device or equipment).

NSM measures the:

- Response time via Echo IP/ICMP.
- Web page download time.
- Jitter measurement between two routers.
- Connection status through a Bidirectional Forwarding Detection (BFD) session.
- Connection status of a RADIUS server.

**Note**

To apply NAT to an NSM poll, enable Advanced Firewall System (AFS). For further information on this feature, please see manual Teldat *Dm786-I AFS*.

## 1.2 TWAMP Feature

IETF defines the Two-Way Active Measurement Protocol (TWAMP) in RFC 5357. Its goal is to provide a standard for two-way measurements in IP networks. A standard was previously proposed for the measurement of round-trip delay in RFC 2681 and, in RFC 4656, the IETF One-Way Active Measurement Protocol (OWAMP) was defined to obtain one-way metrics. TWAMP broadens the OWAMP standard and facilitates a collection of protocols and methods for two-way metrics (in addition to the one-way and round-trip metrics).

Two protocols are defined in the standard: TWAMP-Control and TWAMP-Test. TWAMP-Control is used to create, start and stop sessions, whilst TWAMP-Test defines packet exchange and formats in a test session. Measurements are obtained from the IP path the test session is established over.

Four roles (or entities) are defined in the TWAMP full architecture. Behavior per role is described below:

- Control-Client: initiates the measurement process. It triggers the creation and configuration of test sessions. Since it controls the management of sessions, it does not extract or collect metrics. TWAMP-Control requires sessions to be configured from the Control-Server and prepared in the Session-Reflector for later testing. Using a non-standard protocol, the Control-Client also configures and enables test sessions in the Session-Sender.
- Server: this entity establishes a control connection to the Control-Client using the TWAMP-Control protocol. The Server receives requests from the Control-Client to configure test sessions in the Session-Reflector entity and monitor the status of said sessions.
- Session-Sender: initiates the test sessions. The Session-Sender creates measurement packets and sends them to the Session-Reflector. Responses include the measurement parameters (as defined by TWAMP-Test), which are used to calculate the network metrics. The Session-Sender extracts, processes and collects said metrics.
- Session-Reflector: receives packets sent by the Session-Sender and builds the responses with parameters defined in TWAMP-Test (used to extract the measurements). Using a non-standard protocol, the Server configures test sessions in the Session-Reflector to be used in later tests.

The following schema shows the relationship between the entities and protocols for the TWAMP's full architecture:

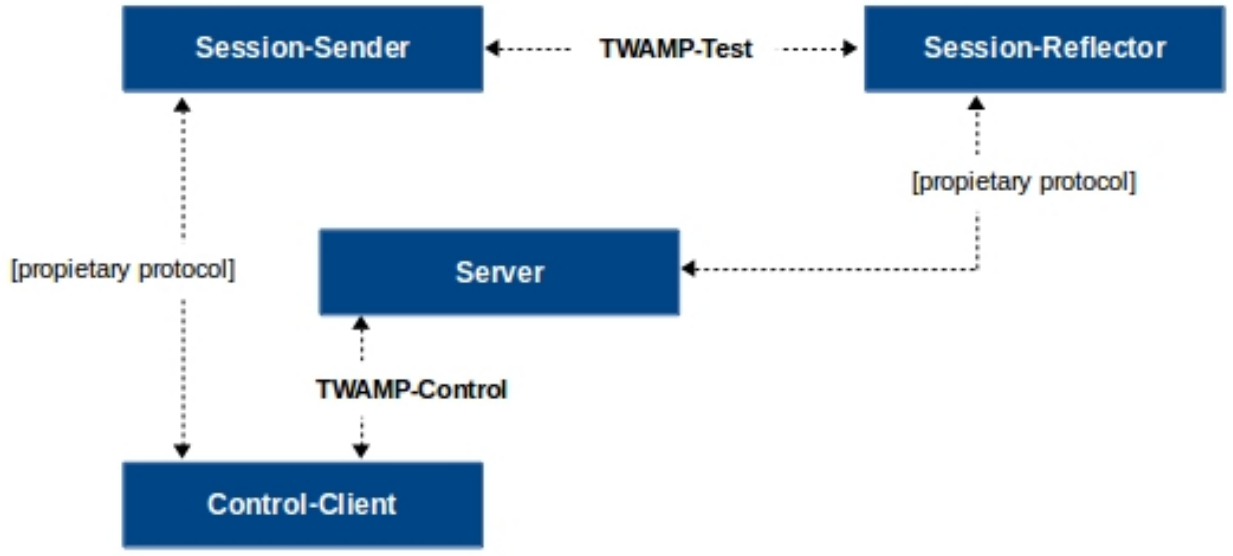



*Fig. 1: Full TWAMP architecture.*

The standard defines the possibility of implementing multiple roles in the same host. A simplified model is also proposed for the full architecture (two-host model). In said model, both the Control-Client and Session-Sender are located and run in the same host. You'll also find the Session-Reflector and the Server located and running in a different host. The following figure shows the full architecture schema with the two-host model.

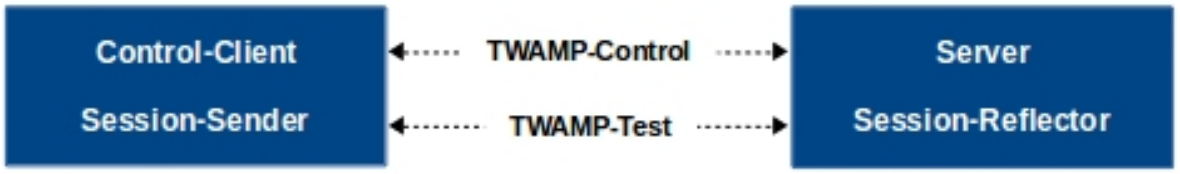



*Fig. 2: Two-host TWAMP model.*

From version 11.01.04 onwards, Teldat routers rely on a two-host model to provide the solution to the Server and Session-Reflector for a full TWAMP architecture. In this document, the term *TWAMP responder* refers to the Session-Reflector entity.

# Chapter 2 Configuration

## 2.1 Accessing the NSM Configuration menu

Enter the NSM configuration commands in the configuration menu associated with NSM (NSM *config*>). Run **feature NSM** to access the general configuration menu (*Config*>).

```
Config>FEATURE NSM
-- Network Service Monitor configuration --
NSM config>
```

Once you have accessed the NSM configuration menu, you can enter the following commands:

| Command | Function |
|---|---|
| *DESCRIPTION* | Adds a general description. |
| *LIST* | Displays information on NSM operations and status. |
| *NO* | Eliminates a configuration parameter or sets its default value. |
| *OPERATION* | Configures an NSM operation. |
| *RESET* | Eliminates the NSM configuration and all of its associated operations. |
| *RESPONDER* | Enables and configures the responder. |
| *RESPONDER*-NEXT-HOP | Configures the responder next-hop. |
| *RESPONDER*-SET-LABEL | Configures the responder label. |
| *RESPONDER*-SRC-IS-RCV-PKT-DST | Configures source is received packet destination mode in the responder. |
| *SCHEDULE* | Plans NSM operations. |
| *SERVER* | Configures an NSM server. |
| *EXIT* | Exits NSM configuration menu. |

## 2.2 Required task list to configure NSM operations

Execute the following tasks to configure an NSM operation:

- Configuring operation type (mandatory).
- Configuring common operation parameters (optional).
- Configuring specific parameters for each type of operation (optional).
- Scheduling operation execution (mandatory).
- Enabling the responder on operational targets (mandatory for certain operations).

### 2.2.1 Configuring the NSM operation type

On configuring an NSM operation, first specify an operation type. If said operation type is not configured, then none of the parameters can be modified.

The following operation types are available in our router:

(1) Echo IP/ICMP.

(2) HTTP Get.

(3) UDP Jitter.

(4) BDF.

(5) RADIUS.

### 2.2.2 Configuring common parameters

A series of parameters that allow behavior to be modified are common to all operation types:

(1) Frequency of operation execution.

(2) Next-hop IP address or interface for probe packets generated in an operation.

(3) Operation owner identification.

(4) Source IP address or interface for probe packets generated in an operation.
(5) Partial threshold for total operation time.
(6) Maximum time required to complete the operation.

### 2.2.3 Configuring specific parameters

Each operation type has a series of specific parameters:

- Echo IP/ICMP:

  Echo-request size.

  TOS (Type Of Service).

- HTTP Get:

  Source port.

- UDP Jitter:

  Interpacket delay.

  Number of packets.

  UDP packet size.

  TOS (Type Of Service).

  Control packets protocol.

  Source-port.

- BFD:

  Required transmission interval.

  Minimum reception interval supported.

  Detection multiplier.

- Radius Accounting:

  No specific parameters required.

### 2.2.4 Operation scheduling

Once an operation is configured, schedule execution so that the gathering process for the registration of statistics and error information commences.

The following parameters must be specified to schedule an operation.

- Life: operation lifetime, time during which this remains active (optional).
- Ageout: maximum time an operation is retained in the memory, without being activated, prior to deletion (optional).
- Startup time: this can be immediate or pending.

The following timeline helps explain the meaning of *Life* and *Ageout* timers:

W----------X----------Y----------Z

Where:

- W is where operation execution is planned.
- X is the beginning of the operation's lifetime (i.e. the moment this switches to an active state).
- Y is the end of a lifetime (i.e. the moment the *Life* counter times out).
- Z is the moment an operation ceases to exist in the memory.

The *Ageout* timer begins its countdown from its initial value in W and in Y, it stops between X and Y and is zeroized and then restarts at Y.

An operation may expire before execution (i.e., Z could occur before X). For this not to happen, the difference between the operation planning time and the execution start time (X and W) must be lower than the *Ageout* value.

### 2.2.5 Activating the *responder*

For UDP Jitter operations, enable a responder in a remote device where measuring is executed.

## 2.3 NSM Configuration Commands

The NSM configuration commands are as follows:

### 2.3.1 DESCRIPTION

Configures a general description. If you enter various commands, a multi-line description is created.

```
NSM config>DESCRIPTION
  <1..64 chars>    Description text
```

### 2.3.2 LIST

Displays NSM-related information for configuration and monitoring purposes.

```
NSM config>LIST
  configuration    NSM configuration
  running          NSM running info
```

#### 2.3.2.1 LIST CONFIGURATION [all] [operation-id]

Displays the NSM operations configured in a device.

*Syntax:*

```
NSM config>list configuration
  all                All NSM operations
  <1..4294967295>    Operation id number
  <cr>               Brief NSM operation list
```

##### 2.3.2.1.1 list configuration all

Consecutively displays all configured NSM operations.

##### 2.3.2.1.2 list configuration <operation-id>

Displays the specific configuration for a given operation.

*Example:*

```
NSM config>list configuration 1
Operation ID Number: 1
--------------------
Type of Operation to Perform: echo
Threshold (ms): 5000
Frequency (seconds): 60
Timeout (ms): 5000
Protocol Type: ipIcmpEcho
Target Address [Port]: 192.168.1.254 [0]
Source Address [Port]: default [0]
Packet Size (ARR data) Request/Response: 28/0
Type of Service (TOS): 0x00
Life (seconds): 3600
Operation Ageout (seconds): 3600
Owner: example.nsm
NSM config>
```

##### 2.3.2.1.3 list configuration <cr>

Displays a responder configuration status with a simplified list (identifier and type) for operations configured in a device.

*Example:*

```
NSM config>list configuration
Responder is: disabled
Jitter responder ports:
-----------------------
No jitter responder ports configured

TWAMP responder is: disabled
TWAMP responder timeout: 900 secs

TWAMP server is: disabled
TWAMP server port: 862
TWAMP server timer inactivity: 900 secs

ID          [type]
-----------------------
1           [echo      ]
2           [http      ]
3           [jitter    ]
4           [bfd       ]
5           [radius    ]
NSM config>
```

### 2.3.2.2 LIST RUNNING [all] [operation-id]

Displays information on NSM operations currently running in the device. Includes results for the latest operation, latest added statistics, various errors, lifetime, next scheduled operation, number of attempts, etc.

*Syntax:*

```
NSM config>list running
  all                 All NSM operations
  <1..4294967295>     Operation id number
  <cr>                Brief NSM operation list
```

#### 2.3.2.2.1 list running all

Consecutively displays all NSM operations that are currently running.

#### 2.3.2.2.2 list running <operation-id>

Displays specific information related to a given operation.

*Example:*

```
NSM config>list running 28622
Operation ID Number: 28622
--------------------
Owner: mapastor.teldat.es (172.24.51.5)
Type of Operation to Perform: echo
Threshold (ms): 5000
Frequency (seconds): 60
Timeout (ms): 5000
Status of Entry (SNMP RowStatus): active
Protocol Type: ipIcmpEcho
Target Address [Port]: 10.0.0.2 [0]
Source Address [Port]: default [0]
Packet Size (ARR data) Request/Response: 32/32
Type of Service (TOS): 0x00
Life (seconds): 3600
Next Scheduled Start Time: now
Operation Ageout (seconds): 60
Modification Time: 21m5s ago
Last Reset Time: never reset
Number of Octets in use: 3888
Occurred Connection-Lost/Timeout/Over-Threshold: false/false/false
Number of Operations Attempted: 22
Current Life Left (seconds): 2335
```

```
Operational State: active
Failed Operations:
  Disconnects.... 0              Timeouts....... 0
  Busies......... 0              No Connections. 0
  Drops.......... 0              Sequence Errors 0
  Verify Errors.. 0
Captured Statistics:
  Start Time: 21m6s ago
  Operations completed: 22
  Completed Over Thresholds: 0
  SumCompletion (ms): 155
  SumCompletion2 High/Low (ms): 0/1289
  Completion Time Max/min/Average (ms): Max 17 - min 5 - Avg 7
Totals Statistics:
  Elapsed Time: 21m6s
  Initiations: 22
Latest ECHO IP/ICMP Operation:
  Completion Time (ms): 5
  Return Code: ok
  Latest Start Time: 6s ago
  Target Address: 10.0.0.2
Next Start Time (seconds): 54

NSM config>
```

#### 2.3.2.2.3 list running <cr>

Displays the responder status, using a simplified list (identifier, type and operation status) for operations that are currently running.

*Example:*

```
NSM config>list running
Responder is: disabled
Jitter responder port:
----------------------
No jitter responder ports configured

TWAMP responder is: disabled
TWAMP responder timeout: 900 secs

TWAMP server is: disabled
TWAMP server port: 862
TWAMP server timer inactivity: 900 secs

ID          [type]       (operState)
---------------------------------------
3098        [jitter    ] (active       )
6930        [http      ] (active       )
28622       [echo      ] (active       )
33256       [bfd       ] (active       )
49086       [radius    ] (active       )

NSM config>
```

### 2.3.3

Accesses the configuration menu of an NSM operation.

```
NSM config>OPERATION
  <1..65535>    Operation id number
```

*Syntax:*

```
NSM config>operation <operation-id>
```

When many operations are configured, please remember polling traffic may interfere and alter results. Therefore, take great care when configuring said operations (i.e., establish a certain time separation between operations and avoid, where possible, the simultaneous deployment of several polls).

Eliminate operations through **no operation <operation-id>**.

*Example:*

```
NSM config>operation 1
-- NSM Operation configuration --
NSM operation 1>
```

### 2.3.4 RESET

Resets the NSM system. Eliminates all NSM configuration information and destroys any operations that are currently running.

```
NSM config>RESET
```

*Example:*

```
NSM config>reset
NSM config>
```

### 2.3.5 RESPONDER

Enables the responder in the device and lets you configure permanent ports to execute responder functions.

```
NSM config>RESPONDER
jitter    Set up jitter responder
twamp     Configure the TWAMP responder
<cr>
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | The **responder twamp timeout** and **responder twamp enable** commands were added as of version 11.01.04. |

#### 2.3.5.1 RESPONDER JITTER PORT <port>

Configures a port that is specifically going to act as responder, enabling it to accept and respond to UDP Jitter operation requests, provided the control packet protocol is not enabled.

```
NSM config>RESPONDER JITTER PORT
  <1..65535>    Port number
```

*Example:*

```
NSM config>responder jitter port 60000
NSM config>
```

**Note**

Once a permanent port is configured as a **responder jitter port**, you can only send UDP Jitter operations (where packet control is not executed) to said port.

To stop said port from operating as a responder for UDP Jitter operations, enter **no responder jitter port <port>**.

#### 2.3.5.2 RESPONDER TWAMP TIMEOUT <seconds>

Configures a timeout for the TWAMP responder feature. The responder will terminate a test session if no test packet is received within the time set. Default is 900 seconds.

*Syntax:*

```
NSM config>RESPONDER TWAMP TIMEOUT <seconds>
```

*Example:*

```
NSM config>responder twamp timeout 2000
NSM config>
```

Use **no responder twamp timeout** to set the default value.

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | This command was added as of version 11.01.04. |

#### 2.3.5.3 RESPONDER TWAMP ENABLE

Enables the TWAMP responder in the router. With TWAMP responder enabled, the TWAMP server can configure sessions requested by TWAMP clients for subsequent testing.

*Syntax:*

```
NSM config>RESPONDER TWAMP ENABLE
```

Use **no responder twamp enable** to disable the responder.

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | The "responder twamp enable" command was added as of version 11.01.04. |

#### 2.3.5.4 RESPONDER <cr>

Enables the responder to respond to UDP Jitter operation requests, provided the control packet protocol is enabled.

```
NSM config>RESPONDER
```

The responder listens for control packets from NSM clients on a specific port (UDP 1967). A control message contains information such as the type of operation, protocol, port, etc.

On receiving a control message, the responder enables a given port to accept requests and reply to them during a configured time.

The responder is enabled (at the remote end) for UDP Jitter operations.

Enter **no responder** to disable said responder.

### 2.3.6 RESPONDER-NEXT-HOP

Configures the **next-hop** for packets generated by the responder. This can be configured either as a numeric IP or a directly-connected interface.

**Note**

When this command is configured and another next-hop is also configured in policy routing (see Teldat manual *Dm745-I Policy Routing* ), the next-hop selected for packets via NSM prevails.

```
NSM config>RESPONDER-NEXT-HOP
  <a.b.c.d>      Ipv4 format
  <interface>    Interface name
```

*Syntax:*

```
NSM operation id>responder-next-hop <ip-address>
```

This command applies to all, control and test, jitter message types in the responder. Default is no specified next-hop.

**Command history:**

| Release | Modification |
|---|---|
| 11.00.05 | The **responder-next-hop** command was added as of version 11.00.05. |
| 11.01.00 | The **responder-next-hop** command was added as of version 11.01.00. |

### 2.3.7 RESPONDER-SET-LABEL

Configures an internal numeric label for packets generated by the responder, thus allowing other processes to identify and classify NSM packets in order to apply different policies to them.

```
NSM config>RESPONDER-SET-LABEL
  <0..99>    Label value
```

*Syntax:*

```
NSM config>responder-set-label <label-for-classification>
```

This command applies to all, control and test, jitter message types in the responder. Default is no specified label.

**Command history:**

| Release | Modification |
|---|---|
| 11.00.05 | The **responder-set-label** command was added as of version 11.00.05. |
| 11.01.00 | The **responder-set-label** command was added as of version 11.01.00. |

## 2.3.8 RESPONDER-SRC-IS-RCV-PKT-DST

Use this option to configure a new responder feature mode. This uses, as source for response packets, the same destination address as the packet received by the NSM client.

It is disabled by default. This means the address the responder uses as response source depends on the interface said response has been sent through.

Please remember this option does not enable the responder. Said option only takes effect once the responder is enabled.

```
NSM config>RESPONDER-SRC-IS-RCV-PKT-DST
```

To return to the default function and disable the new operating mode, enter **no responder-src-is-rcv-pkt-dst**

## 2.3.9 SCHEDULE

Operation scheduling is executed through the following:

```
NSM config>SCHEDULE <operation-id>
  ageout        Time to keep the operation when not active
  life          Time to execute this operation
  start-time    When to start the operation
```

### 2.3.9.1 SCHEDULE AGEOUT

Period of time an operation is retained in the memory when inactive.

*Syntax:*

```
NSM config>schedule <operation-id> ageout
  <0..2073600>    Ageout (in seconds)
  never           Never ageout (keep forever)
```

#### 2.3.9.1.1 schedule <operation-id> ageout <seconds>

Time, in seconds, an operation is retained in the memory when not actively gathering data.

Default is 3600 seconds (one hour).

#### 2.3.9.1.2 schedule <operation-id> ageout never

An operation is stored in memory indefinitely, regardless of status.

### 2.3.9.2 SCHEDULE LIFE

Time an operation is actively maintained while gathering data.

*Syntax:*

```
NSM config>schedule <operation-id> life
  <1..2147483647>    Life time (in seconds)
  forever            The operation runs forever
```

#### 2.3.9.2.1 schedule <operation-id> life <seconds>

Time, in seconds, an operation actively gathers data.

Default is 3600 seconds (one hour).

#### 2.3.9.2.2 schedule <operation-id> life forever

The operation is executed indefinitely.

### 2.3.9.3 SCHEDULE START-TIME

Specifies the time at which an operation begins to gather statistics. If no **start-time** is configured, the operation will never start.

*Syntax:*

```
NSM config>schedule <operation-id> start-time
  after      Start after the time specified
  now        Start right now
  pending    Start pending (at a later time)
```

#### 2.3.9.3.1 schedule <operation-id> start-time after <seconds>

An operation begins executing after a given time (from current time). Please remember that if you configure *ageout* with a value (in seconds) that is lower than the *time still to run* before the operation executes, the latter can never execute as it's deleted due to time out.

#### 2.3.9.3.2 schedule <operation-id> start-time now

The operation immediately begins to gather data.

*Example:*

```
NSM config>schedule 1 start-time now
NSM config>
```

#### 2.3.9.3.3 schedule <operation-id> start-time pending

The operation's start time is pending. No data is gathered until an order to do so is received. Please note that, if the time configured in *ageout* has lapsed without a start order being executed, said operation is deleted and is no longer included in the list of planned operations. Execute **start-time** to re-include it.

This is done by default.

## 2.3.10 SERVER

Accesses the NSM server configuration menu.

*Syntax:*

```
NSM config>SERVER ?
  twamp        Configure the TWAMP server
```

### 2.3.10.1 SERVER TWAMP

Accesses the TWAMP server configuration menu in the router.

*Example:*

```
NSM config>server twamp



TWAMP srv>
```

The following commands are available in the TWAMP server configuration menu:

| Command | Function |
|---|---|
| *? (HELP)* | Displays the configuration commands or their options. |
| *ENABLE* | Enables the TWAMP server. |

| | |
|---|---|
| *NO* | Configures parameters with their default values. |
| *PORT* | Configures the port for the TWAMP server. |
| *TIMER* | Configures timers for the TWAMP server. |
| *EXIT* | Exits the configuration menu. |

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | The **server twamp** command was added as of version 11.01.04. |

#### 2.3.10.1.1 ENABLE

Enables the TWAMP server in the router.

*Example:*

```
TWAMP srv>enable
```

Use **no enable** to disable the TWAMP server.

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | The "enable" command was added as of version 11.01.04. |

#### 2.3.10.1.2 NO

Use this command to configure parameters with their default values.

*Syntax:*

```
TWAMP srv>no ?
  enable    Enable the TWAMP server
  port      Configure the port for the TWAMP server
  timer     Configure timers for the TWAMP server
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | The "no" command was added as of version 11.01.04. |

#### 2.3.10.1.3 PORT <number>

Configures the TCP port the TWAMP server listens at for new Control-Client connections. Default is 862.

*Syntax:*

```
TWAMP srv>port <1..65535>
```

Use **no port** to set the default value.

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | The "port" command was added in version 11.01.04. |

#### 2.3.10.1.4 TIMER INACTIVITY <seconds>

Configures the TWAMP server inactivity timer. Said server terminates an established control connection if no packet (associated to this connection) has been received within the time set by said command. Control connection activity is suspended when a Start-Sessions command is received, and resumed after a Stop-Sessions. Default is 900 seconds.

*Syntax:*

```
TWAMP srv>timer inactivity <5..7200>
```

Use the **no timer inactivity** command to set the default value.

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | The "timer inactivity" command was added as of version 11.01.04. |

#### 2.3.10.1.5 EXIT

Exits the TWAMP server configuration menu.

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | The "exit" command was added as of version 11.01.04. |

### 2.3.11 EXIT

Exits the NSM configuration menu and returns to the main configuration menu (*Config*>).

```
NSM config>exit
```

*Example:*

```
NSM config>exit
Config>
```

## 2.4 NSM Operation Configuration Commands

The following commands are available in an NSM operation configuration menu:

```
NSM operation id>?
  bfd-interval          BFD desired transmission interval
  bfd-min-rx            BFD minimum required reception interval
  bfd-multiplier        BFD detect multiplier
  control               Enable or disable control packets
  description           Add a description text
  frequency             Frequency of the operation
  interval              Inter-packet interval
  label                 Set label for classification
  list                  Show operation parameters
  next-hop-ipaddr       Next-hop IP address
  no                    Negate a command or set its defaults
  num-packets           Number of packets to be transmitted
  owner                 Owner of operation
  request-data-size     Request data size
  source-ipaddr         Source IP address
  source-port           Source port
  threshold             Operation threshold
  timeout               Timeout of the operation
  tos                   Type of service
  type                  Type of operation
  exit
```

Not all commands are applicable to all operation types. Specific configurations for different types of operations are explained further on in this manual.

### 2.4.1 [NO] BFD-INTERVAL

**bfd-interval** establishes a minimum period for transmitting BFD packets supported by the device. If the NSM feature created the session (i.e., if BFD was not previously created by another protocol), this value prevails over the value configured in the interface where a BFD session is running. Default for a minimum interval for BFD packet transmission is 100 milliseconds. Said value must be between 50 and 999 milliseconds.

*Syntax:*

```
NSM operation 1>bfd-interval ?
  <50..999>    Interval (in milliseconds)
NSM operation 1>
```

*Example:*

```
NSM operation 1>bfd-interval 200
NSM operation 1>
```

### 2.4.2 [NO] BFD-MIN-RX

**bfd-min-rx** establishes a minimum reception period for BFD packets supported by the device. If the session was created by the NSM feature (i.e., if the BFD session was not previously created by another protocol), this value prevails over the value configured in the interface where the BFD session is running. Default for a minimum interval for reception of BFD packets is 50 milliseconds. Said value must be between 1 and 999 milliseconds.

*Syntax:*

```
NSM operation 1>bfd-min-rx ?
  <1..999>    Interval (in milliseconds)
NSM operation 1>
```

*Example:*

```
NSM operation 1>bfd-min-rx 100
NSM operation 1>
```

### 2.4.3 [NO] BFD-MULTIPLIER

**bfd-multiplier** establishes multiplier detection to calculate detection time for a BFD session. This is, basically, the number of BFD packets that need to be lost consecutively to consider the BFD session down. If the NSM feature created the session (i.e., if the BFD session was not previously created by another protocol), this value prevails over the value configured in the interface where the BFD session is running. The default value for multiplier detection is 3. Said value must be between 3 and 50.

*Syntax:*

```
NSM operation 1>bfd-multiplier ?
  <3..50>    Multiplier
NSM operation 1>
```

*Example:*

```
NSM operation 1>bfd-multiplier 5
NSM operation 1>
```

### 2.4.4 CONTROL

**Control** allows you to enable (or disable) the control packets protocol in UDP Jitter operations. If said protocol is enabled, a control packet that contains information on the type of operation, protocol, port test packets are sent to, etc. is sent before sending test packets. For this to work, the responder must be enabled at destination and listening at a specified port where the control packets are sent (1967 UDP). If said protocol isn't enabled, test packets are sent directly, which means destination must have a permanent port configured to execute responder functions where said test packets are sent.

UDP Jitter operations can be sent even if the destination doesn't have a NSM feature, but can behave like a mirror (reflecting packets that reach a given UDP port). To do this, disable the control packets protocol.

*Syntax:*

```
NSM operation 1>control ?
  disable    Disable control packets exchange
  enable     Enable control packets exchange (default)
NSM operation 1>
```

*Example:*

```
NSM operation 1>control disable
NSM operation 1>
```

Said command is exclusive to UDP Jitter operations. It is enabled by default.

### 2.4.5 [NO] DESCRIPTION

Establishes an NSM operation description.

```
NSM operation id>DESCRIPTION
  <1..64 chars>    Description text
```

*Syntax:*

```
NSM operation id>description <text>
```

### 2.4.6 FREQUENCY

Specifies how often an operation executes a probe to gather statistics.

```
NSM operation id>FREQUENCY
  <1..604800>    Frequency (in seconds)
```

*Syntax:*

```
NSM operation id>frequency <seconds>
```

This command applies to all operation types. Default is 60 seconds (one minute). Said value must be between 1 and 604.800 seconds.

We recommend using a 10-second frequency for the RADIUS operation to correctly detect the radius server.

Where a BFD operation is configured in demand mode, the **frequency** command establishes how often poll cycles are executed in a BFD session. For BFD operations in asynchronous mode, this command is irrelevant.

**Note**

A frequency value cannot be lower than the value configured for operation timeout. We strongly recommend *not* setting a frequency value lower than 60 seconds (default), except for RADIUS operations.

### 2.4.7 INTERVAL

Consecutive interpacket interval (in milliseconds) for the Jitter probe.

```
NSM operation id>INTERVAL
  <10..60000>    Interval (in milliseconds)
```

*Syntax:*

```
NSM operation id>interval <inter-packet-interval>
```

This command is exclusive to UDP Jitter operations. Default is 20 milliseconds.

### 2.4.8 LABEL

Sets an internal numeric label to probe packets for a configured operation, allowing other processes to identify and classify NSM packets and apply different policies to them.

```
NSM operation id>LABEL
  <0..99>    Label value
```

*Syntax:*

```
NSM operation id>label <label-for-classification>
```

This command applies to all operation types. Default is no specified label.

**Command history:**

| Release | Modification |
|---|---|
| 11.00.05 | The **label** command was added as of version 11.00.05. |
| 11.01.00 | The **label** command was added as of version 11.01.00. |

### 2.4.9 LIST

Displays the operation's configuration.

```
NSM operation id>LIST
```

*Example:*

```
NSM operation id>list

Operation ID Number: id
--------------------
Type of Operation to Perform: echo
Threshold (ms): 5000
Frequency (seconds): 60
Timeout (ms): 5000
Protocol Type: ipIcmpEcho
Target Address [Port]: 1.1.1.1 [0]
Source Address [Port]: default [0]
Packet Size (ARR data) Request/Response: 28/0
Echo Id policy: default
Type of Service (TOS): 0x00
Life (seconds): 3600
Operation Ageout (seconds): 3600
Owner: Teldat R&D 172.24.51.97

NSM operation id>
```

### 2.4.10 NEXT-HOP-IPADDR

Sets a specific next-hop used in probe packets generated by a configured NSM operation. This can be configured either as a numeric IP or a directly connected interface.

**Note**

When this command is configured and another next-hop is also configured in policy routing (see Teldat manual *Dm745-I Policy Routing* ), the next-hop selected for packets via NSM prevails.

This command also specifies the next-hop for multihop BFD sessions.

```
NSM operation id>NEXT-HOP-IPADDR
  <a.b.c.d>      Ipv4 format
  <interface>    Interface name
```

*Syntax:*

```
NSM operation id>next-hop-ipaddr <ip-address>
```

This command applies to all operation types. Default is no specified next-hop.

**Command history:**

| Release | Modification |
|---|---|
| 11.00.05 | The **next-hop-ipaddr** command was added as of version 11.00.05. |
| 11.01.00 | The **next-hop-ipaddr** command was added as of version 11.01.00. |

### 2.4.11 NUM-PACKETS

Number of packets used in a Jitter probe.

```
NSM operation id>NUM-PACKETS
  <1..1000>    Number of packets
```

*Syntax:*

```
NSM operation id>num-packets <number-of-packets>
```

This command is exclusive to UDP Jitter operations. Default is 10 packets.

### 2.4.12 OWNER

Specifies the operation's owner. This is an identifier text of between 1 and 200 characters.

```
NSM operation id>OWNER
  <1..200 chars>    Owner of operation
```

*Syntax:*

```
NSM operation id>owner <text>
```

*Example:*

```
NSM operation id>owner "Teldat R&D 172.24.51.97"
NSM operation id>
```

This command applies to all operation types. There is no owner by default.

### 2.4.13 REQUEST-DATA-SIZE

Payload data size for NSM operation requests.

```
NSM operation id>REQUEST-DATA-SIZE
  <1..16384>    Native payload size
```

*Syntax:*

```
NSM operation id>request-data-size <bytes>
```

This is exclusive to Echo IP/ICMP and UDP Jitter operations.

In Echo IP/ICMP operations, the values allowed range from 28 to 16384. Default is 28. An ICMP packet used by an Echo IP/ICMP probe has a total length of: IP Header (20) + ICMP Header (8) + Time stamps + request-data-size.

Values allowed in UDP Jitter operations range from 16 to 1500. Default is 32.

### 2.4.14 SOURCE-IPADDR

Sets a specific source IP address used in probe packets generated by a configured NSM operation. This address can be configured either dynamically or as a numeric IP by taking the address from a given interface.

This command also specifies the source IP address for a BFD session. One of the device interfaces must be configured with said IP address for the BFD session to be be established through the interface.

```
NSM operation id>SOURCE-IPADDR
  <a.b.c.d>      Ipv4 format
  <interface>    Interface name
```

*Syntax:*

```
NSM operation id>source-ipaddr <ip-address>
```

This command applies to all operation types. No source IP address is specified by default.

**Command history:**

| Release | Modification |
|---|---|
| 11.00.05 | The **source-ipaddr** command accepts an interface name as argument. |
| 11.01.00 | The **source-ipaddr** command accepts an interface name as argument. |

### 2.4.15 SOURCE-PORT

Sets a specific source port used in probe packets for NSM operations.

```
NSM operation id>SOURCE-PORT
  <0..65536>    Source port (in jitter operations avoid the range 50000 to 51001)
```

*Syntax:*

```
NSM operation id>source-port <port>
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.08 | Until this version, the command was only available for HTTP operations. From this version onwards, the command is also available for Jitter operations. |

## 2.4.16 THRESHOLD

Sets a partial reference threshold for total operation time.

```
NSM operation id>THRESHOLD
  <1..2147483647>    Threshold (in milliseconds)
```

*Syntax:*

```
NSM operation id>threshold <milliseconds>
```

This command applies to all operation types. Default is 5000 milliseconds.

If an operation executing a probe to collect statistics exceeds the reference threshold's total time, an indication is given and the associated statistic is updated. This determines how many successful operations (probes) surpass the reference value.

## 2.4.17 TIMEOUT

Establishes the wait time to complete an NSM operation.

```
NSM operation id>TIMEOUT
  <1000..604800000>    Timeout (in milliseconds)
```

*Syntax:*

```
NSM operation id>timeout <milliseconds>
```

This command applies to all operation types. Default is 5000 milliseconds. This value must range between 1000 and 604,800,000 milliseconds.

For HTTP Get operations, a 60-second timeout is automatically configured (recommended value). This value can be subsequently modified.

For UDP Jitter operations, this timeout is applied to each packet that makes up an operation.

Where a BFD NSM operation is configured in demand mode, the time it takes for the operation to terminate is set (i.e., a BFD Demand mode poll cycle). The optimum value is slightly higher than the time it takes to execute a BFD poll cycle (which, in the worst case scenario, is BFD's detection time for demand mode).

For RADIUS operations, a 60-second timeout is automatically configured (recommended value). This value can be subsequently modified.

**Note**

The timeout value cannot be greater than the operation frequency value configured, except for RADIUS operations. We strongly recommend using realistic timeout values (i.e., adequate for each operation type).

## 2.4.18 TOS

Configures Type Of Service (TOS) value in IP header for packets used for NSM operations.

```
NSM operation id>TOS
  <0..255>    TOS value
```

*Syntax:*

```
NSM operation id>tos <tos-value>
```

This command is exclusive to Echo IP/ICMP and UDP Jitter operations. Values allowed for TOS range from 0 to 255. Default is 0.

## 2.4.19 TYPE

Configures the operation type. This is the most important parameter and the first that needs to be specified when configuring an NSM operation. If the operation type is not set, you cannot configure any other operation parameters. If you change the operation type, then the default values will be restored. Operation types available in the router are: Echo IP/ICMP, HTTP Get, UDP Jitter, BFD and RADIUS.

BFD can be configured in two ways for NSM monitoring operations: Asynchronous and Demand.

```
NSM operation id>TYPE
  echo      Echo operation
  http      HTTP operation
  jitter    Jitter operation
  bfd       Bidirectional Forwarding Detection operation
  radius    Radius operation
```

### 2.4.19.1 TYPE ECHO IPICMP <dest-ipaddr> [ constant id / variable id]

Sets the NSM probe as Echo IP/ICMP. You must specify the destination IP address to which ICMP Echo Request frames are sent.

You can also configure an Internet hostname instead of an IP address as destination, relying on the underlaying DNS protocol to discover the target address. For further information on DNS, please see manual *Teldat Dm723-I DNS*.

*Example 1:*

```
NSM operation id>type echo ipcicmp 212.95.195.132
NSM operation id>
```

*Example 2:*

```
NSM operation id>type echo ipcicmp www.teldat.es
NSM operation id>
```

**constant-id** forces all ICMP Echo Request packets sent to take the same ICMP identifier. Similarly, **variable-id** forces ICMP Echo Requests to be sent with distinct identifiers. Neither option is specified by default: behavior depends on whether AFS (*Advanced Firewall System* ) is enabled or not. If it is enabled, ICMP Echo Requests are sent with different identifiers. If AFS is disabled, the behavior is the exact opposite. For further information on AFS, please see manual *Teldat Dm785-I AFS* .

*Example 3:*

```
NSM operation id>type echo ipcicmp 212.95.195.132 variable-id
NSM operation id>
```

**Command history:**

| Release | Modification |
|---|---|
| 11.00.05 | The **echo ipicmp** command accepts an Internet hostname as argument. |
| 11.01.00 | The **echo ipicmp** command accepts an Internet hostname as argument. |

### 2.4.19.2 TYPE HTTP GET <url>

Sets the NSM probe as HTTP Get. You must specify the URL for the probe to download.

*Example:*

```
NSM operation id>type http get http://www.teldat.com
NSM operation id>
```

Please bear in mind that DNS must be correctly configured to resolve any URL. Please see the *Teldat Dm723-I DNS* manual for further information.

**Note**

Any URL specified must start with **http://**

### 2.4.19.3 TYPE JITTER <dest-ipaddr> DEST-PORT <dest-port>

Configures the NSM probe as UDP Jitter. Destination IP address (acting as responder) and destination port must be specified.

You can also configure an Internet hostname instead of an IP address as destination, relying on the underlaying DNS protocol to discover the target address. For further information on DNS, please see manual *Teldat Dm723-I DNS*.

*Example 1:*

```
NSM operation id>type jitter 200.200.200.200 dest-port 60000
NSM operation id>
```

*Example 2:*

```
NSM operation id>type jitter www.teldat.es dest-port 60000
NSM operation id>
```

**Note**

When configuring a UDP Jitter operation destination where measurements are taken, a responder must always be enabled. If this is executed with control packets protocol enabled, simply enable the **responder** (command). Otherwise, make sure the destination has a port (where operations are sent) configured as responder (**responder jitter port**).

**Note**

The destination port used for testing must be different from 1967. The 1967 port is used for the responder to respond to NSM client petitions.

**Command history:**

| Release | Modification |
|---|---|
| 11.00.05 | The **jitter** command accepts an Internet hostname as argument in the **dest-ipaddr** option. |
| 11.01.00 | The **jitter** command accepts an Internet hostname as argument in the **dest-ipaddr** option. |

### 2.4.19.4 TYPE BFD DEMAND MODE

In demand mode, BFD only sends control packets to periodically check a line status (at given moments) when it executes poll cycles. Poll cycles are executed using a pre-configured frequency set through the **frequency** command under the NSM operations configuration.

When you enter a **type** command and type of BFD operation, the BFD mode selected is immediately followed by a BFD session IP destination address. Said destination address must be visible and directly connected to the interface that corresponds to the IP address configured through the **source-addr** command.

*Syntax:*

```
NSM operation 1>type bfd demand-mode ?
  <a.b.c.d>    Destination IP address
NSM operation 1>
```

*Example:*

```
NSM operation 1> type bfd demand-mode 172.24.80.12
NSM operation 1>
```

### 2.4.19.5 TYPE BFD ASYNC-MODE

In asynchronous mode, BFD continually sends control packets at a rhythm that marks the transmission time negotiated when establishing a BFD session. A drop is detected whenever the detection time times out without receiving a packet from the endpoint.

When you enter a **type** command, the BFD mode selected is immediately followed by a BFD session IP destination

address. Said destination address must be visible and directly connected to the interface that corresponds to the IP address configured through the **source-addr** command.

*Syntax:*

```
NSM operation 1>type bfd async-mode ?
  <a.b.c.d>    Destination IP address
NSM operation 1>
```

*Example:*

```
NSM operation 1> type bfd async-mode 172.24.80.12
NSM operation 1>
```

### 2.4.19.6 TYPE RADIUS

Radius probe packets are sent to check the status of the RADIUS server.

*Syntax:*

```
NSM operation 1>type radius ?
  <a.b.c.d>    Destination IP address
NSM operation 1> type radius 212.95.195.132 dest-port ?
  <1..65535>   Destination port
  default      Default port
NSM operation 1> type radius 212.95.195.132 dest-port default user ?
  user         User
NSM operation 1> type radius 212.95.195.132 dest-port default user <user> secret ?
  plain             Plain key
  ciphered          Ciphered key
  ciphered-unique   Unique ciphered key for this device
NSM operation 1> type radius 212.95.195.132 dest-port default user <user> secret plain <secret>
NSM operation 1>
```

*Example:*

```
NSM operation 1> type radius 212.95.195.132 dest-port default user <user> secret plain <secret>
NSM operation 1>
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.08 | The radius operation was added as of version 11.01.08. |

## 2.4.20 VRF

Allocates the operation to a VRF. This means the router sends the probe packets through VRF. For further information on the VRF facility, please see manual *Dm775-I VRF Lite Facility*.

```
NSM operation id>vrf
  <1..32 chars>    VPN Routing/Forwarding instance name
```

*Syntax:*

```
NSM operation id>vrf <vrf-name>
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | The **vrf** command was added as of version 11.01.04. |

## 2.4.21 Echo IP/ICMP Operation

Measures the end-to-end response time between a router and a device using IP. The response time is calculated by measuring the time that goes by from the moment an ICMP Echo Request is sent to a destination and an Echo Reply from said destination is received.

#### 2.4.21.1 Description of Echo IP/ICMP statistics

The following statistics are displayed for Echo IP/ICMP operations:

```
NSM config>list running 3767
Operation ID Number: 3767
--------------------
Owner: InfoVista Server on test.teldat.es (172.24.0.51)
Type of Operation to Perform: echo
Threshold (ms): 5000
Frequency (seconds): 60
Timeout (ms): 5000
Status of Entry (SNMP RowStatus): active
Protocol Type: ipIcmpEcho
Target Address [Port]: 192.168.50.2 [0]
Source Address [Port]: 172.24.78.81 [0]
Next-hop Address: 172.24.78.3
Echo Id policy: variable
Packet Size (ARR data) Request/Response: 32/32
Type of Service (TOS): 0x00
Internet hostname: example.teldat.es
Life (seconds): 3600
Next Scheduled Start Time: now
Operation Ageout (seconds): 60
Modification Time: 52m31s ago
Last Reset Time: never reset
Number of Octets in use: 3888
Occurred Connection-Lost/Timeout/Over-Threshold: false/false/false
Number of Operations Attempted: 3533
Current Life Left (seconds): 448
Operational State: active
Failed Operations:
  Disconnects.... 0              Timeouts....... 0
  Busies......... 0              No Connections. 0
  Drops.......... 0              Sequence Errors 0
  Verify Errors.. 0
Captured Statistics:
  Start Time: 48m23s ago
  Operations completed: 48
  Completed Over Thresholds: 0
  SumCompletion (ms): 4175
  SumCompletion2 High/Low (ms): 0/1929913
  Completion Time Max/min/Average (ms): Max 858 - min 21 - Avg 86
  DNS Sum (ms): 192
  DNS Timeouts/Errors: 0/0
Totals Statistics:
  Elapsed Time: 48m23s
  Initiations: 48
Latest ECHO IP/ICMP Operation:
  Completion Time (ms): 78
  Return Code: ok
  Latest Start Time: 32s ago
  DNS Time (ms): 2
  ECHO IP/ICMP Transaction Time (ms): 76
  Target Address: 192.168.50.2
  Echo Id: 11270
Next Start Time (seconds): 28

NSM config>
```

##### 2.4.21.1.1 Owner

Owner of NSM operation.

##### 2.4.21.1.2 Type of Operation to Perform

Echo: Echo IP/ICMP operation type.

#### 2.4.21.1.3 Threshold

Reference for partial threshold (in milliseconds).

#### 2.4.21.1.4 Frequency

Frequency of operation (in seconds).

#### 2.4.21.1.5 Timeout

Operation timeout (in milliseconds).

#### 2.4.21.1.6 Status of Entry (SNMP RowStatus)

Administrative status of entry.

#### 2.4.21.1.7 Protocol Type

Value for Echo IP/ICMP operations: **ipIcmpEcho**

#### 2.4.21.1.8 Target Address [Port]

Target IP address (destination) for Echo IP/ICMP operation. Port not applied.

#### 2.4.21.1.9 Source Address [Port]

Source IP address (or interface where said address is taken from) for Echo IP/ICMP operation. Port not applied.

#### 2.4.21.1.10 Next-hop Address

Next-hop IP address (or interface) for Echo IP/ICMP operation is displayed if **next-hop** command is configured.

#### 2.4.21.1.11 Echo Id Policy

Behavior configured for ICMP identifier in ICMP Echo Requests.

#### 2.4.21.1.12 Packet Size (ARR data) Request/Response

Payload data size in requests/responses.

#### 2.4.21.1.13 Type of Service (TOS)

TOS field value in IP header.

#### 2.4.21.1.14 Internet hostname

Internet hostname for Echo IP/ICMP operation.

Only displayed if destination address is configured as an Internet hostname.

#### 2.4.21.1.15 Life

Operation lifetime (in seconds).

#### 2.4.21.1.16 Next Scheduled Start Time

Scheduling next operation startup.

#### 2.4.21.1.17 Operation Ageout

Time (in seconds) statistics are stored in the memory once an operation becomes inactive.

#### 2.4.21.1.18 Modification Time

Time of the latest configuration modification (SNMP only: once it has been launched, operation configuration cannot be modified using the commands line).

#### 2.4.21.1.19 Last Reset Time

Latest reset time for an operation (SNMP only).

#### 2.4.21.1.20 Number of Octets in use

Number of memory octets used by an operation.

#### 2.4.21.1.21 Occurred Connection-Lost/Timeout/Over-Threshold

Reports if the following has occurred in the latest operation: *Connection-Lost*/*Timeout*/*Over-Threshold.*

#### 2.4.21.1.22 Number of Operations Attempted

Number of operations attempted (executions).

#### 2.4.21.1.23 Current Life Left

Current lifetime left (in seconds).

#### 2.4.21.1.24 Operational State

Operational state.

#### 2.4.21.1.25 Failed Operations

Unsuccessful operations due to:

*Disconnects:* Destination disconnected.

*Timeouts:* Maximum time for operation has timed out.

*Busies:* Operation cannot commence; previous operation has not yet finished.

*No Connections:* Connection with destination not established.

*Drops:* Internal errors.

*Sequence Errors:* Sequence errors, unexpected identifiers.

*Verify Errors:* Errors when checking data content.

#### 2.4.21.1.26 Captured Statistics

*Start Time:* Start time for the latest statistics gathering time.

*Operations completed:* Successfully completed operations.

*Completed Over Thresholds:* Operations completed over the reference threshold.

*SumCompletion:* Accumulated time for successfully completed operations.

*SumCompletion2 High*/*Low:* Accumulated squared time for successfully completed operations.

*Completion Time Max*/*min*/*Average:* Maximum, minimum operation time and average value.

*DNS sum (ms):* Total time used in DNS requests.

*DNS Timeouts*/*Errors:* Timeouts and errors in DNS requests.

**Note**

DNS-related statistics are only displayed if the destination address is configured as an Internet hostname.

#### 2.4.21.1.27 Totals Statistics

*Elapsed Time:* Time lapsed from the beginning of statistics collection.

*Initiations:* Number of operation launches.

#### 2.4.21.1.28 Latest ECHO IP/ICMP Operation

Results of latest Echo IP/ICMP operation:

*Completion Time:* Total time used in latest Echo IP/ICMP operation.

*Return Code:* Code reporting an operation result.

*Latest Start Time:* Time lapsed since latest execution.

*DNS Time:* Time used in resolving a DNS name.

*ECHO IP/ICMP Transaction Time:* Time used in RTT (Round Trip Time), Echo IP/ICMP.

*Target Address:* Destination address.

*Echo Id:* Latest ICMP identifier sent.

**Note**

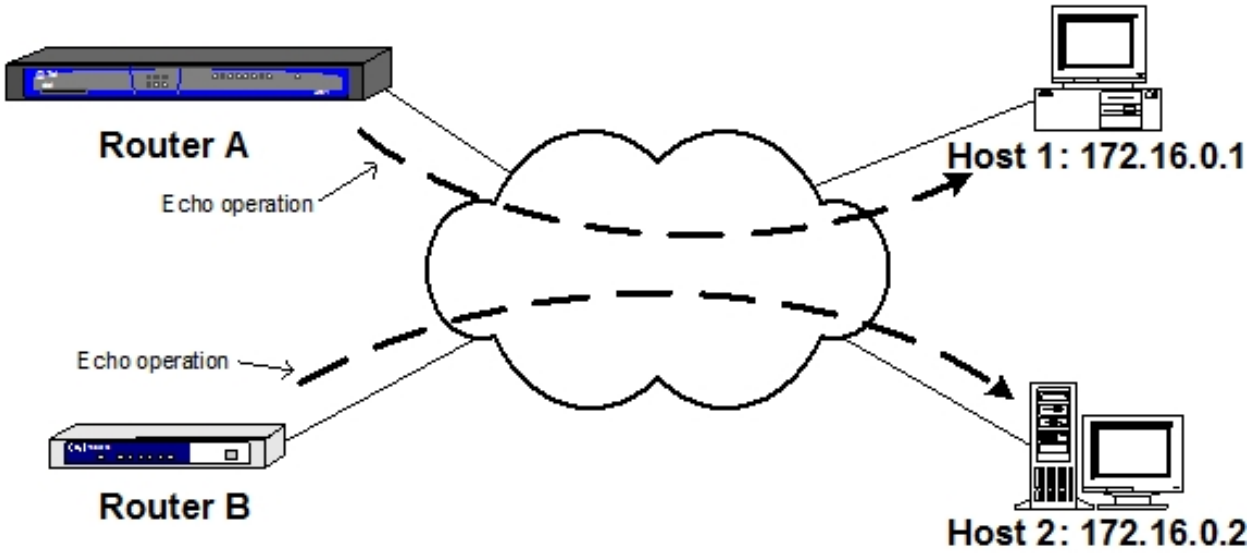
*DNS Time* and *ECHO IP/ICMP Transaction time* are only displayed if the destination address is configured as an Internet hostname. *Completion Time* is the sum of both these times.

#### 2.4.21.1.29 Next Start Time

Start time for subsequent operation execution.

### 2.4.21.2 Echo IP/ICMP operation examples

In the following example, Router A executes Echo IP/ICMP operation with default values to Host 1, while Router B executes Echo IP/ICMP to Host 2 specifying test frequency at 2 minutes, echo-request size, source IP address, timeout, indefinite duration of operation, etc.




For Router A Echo IP/ICMP operation to Host 1:

```
Router-A NSM config>operation 1
-- NSM Operation configuration --
Router-A NSM operation 1>type echo ipicmp 172.16.0.1
Router-A NSM operation 1>exit
Router-A NSM config>schedule 1 start-time now
Router-A NSM config>
```

For Router B Echo IP/ICMP operation to Host 2:

```
Router-B NSM config>operation 2
-- NSM Operation configuration --
Router-B NSM operation 2>type echo ipicmp 172.16.0.2
Router-B NSM operation 2>request-data-size 1000
Router-B NSM operation 2>source-ipaddr 10.0.0.1
Router-B NSM operation 2>timeout 10000
Router-B NSM operation 2>owner "Router B"
Router-B NSM operation 2>frequency 120
Router-B NSM operation 2>exit
Router-B NSM config>schedule 2 life forever
Router-B NSM config>schedule 2 start-time now
Router-B NSM config>
```

**Router A configuration:**

```
feature nsm
; -- Network Service Monitor configuration --
   operation 1
; -- NSM Operation configuration --
      type echo ipicmp 172.16.0.1
   exit
;
   schedule 1 start-time now
exit
;
```

**Router B configuration:**

```
feature nsm
; -- Network Service Monitor configuration --
   operation 2
; -- NSM Operation configuration --
      type echo ipicmp 172.16.0.2
      frequency 120
      owner "Router B"
      request-data-size 1000
      source-ipaddr 10.0.0.1
      timeout 10000
   exit
;
   schedule 2 life forever
   schedule 2 start-time now
exit
;
```

## 2.4.22 HTTP Get Operation

Measures the time it takes to connect and download data from an HTTP server. This calculation is made up of three parts:

- DNS Query: Time elapsed in resolving the domain name (if HTTP server IP address is directly included in the configured URL e.g., http://200.200.200.200/doc/index.html, said query is not required).
- TCP Connection: Time lapsed in opening a TCP connection with the HTTP server.
- HTTP transaction time: Time lapsed between the sending of a request (GET) and the reception of a response from the HTTP server (probe only downloads the basic HTTP page).

### 2.4.22.1 Description of HTTP Get statistics

The following statistics are displayed in HTTP Get operations:

```
NSM config>list running 9996
Operation ID Number: 9996
--------------------
Owner: InfoVista Server on test.teldat.es (172.24.0.51)
Type of Operation to Perform: http
Threshold (ms): 5000
Frequency (seconds): 60
Timeout (ms): 5000
```

```
Status of Entry (SNMP RowStatus): active
Protocol Type: httpAppl
Target Address [Port]: 172.24.78.119 [0]
Source Address [Port]: default [0]
Next-hop Address: direct-ip1
Packet Size (ARR data) Request/Response: 32/0
Type of Service (TOS): 0x00
HTTP Operation: httpGet
URL: http://mondraker.id.teldat.es/manual/mod/core.html
Life (seconds): 3600
Next Scheduled Start Time: now
Operation Ageout (seconds): 60
Modification Time: 14m35s ago
Last Reset Time: never reset
Number of Octets in use: 9072
Occurred Connection-Lost/Timeout/Over-Threshold: false/false/false
Number of Operations Attempted: 15
Current Life Left (seconds): 2724
Operational State: active
Failed Operations:
  Disconnects.... 0              Timeouts....... 0
  Busies......... 0              No Connections. 0
  Drops.......... 0              Sequence Errors 0
  Verify Errors.. 0
Captured Statistics:
  Start Time: 14m35s ago
  Operations completed: 15
  Completed Over Thresholds: 0
  SumCompletion (ms): 3066
  SumCompletion2 High/Low (ms): 0/649766
  Completion Time Max/min/Average (ms): Max 296 - min 177 - Avg 204
  DNS Sum (ms): 317
  DNS Timeouts/Errors: 0/0
Totals Statistics:
  Elapsed Time: 14m35s
  Initiations: 15
HTTP Collection Statistics:
  TCP Connection Sum (ms): 31
  HTTP Transaction Sum (ms): 2718
  TCP Timeouts: 0
  HTTP Transaction Timeouts/Errors: 0/0
Latest HTTP Operation:
  Completion Time (ms): 184
  Return Code: ok
  Latest Start Time: 36s ago
  DNS Time (ms): 5
  TCP Connection Time (ms): 1
  HTTP Transaction Time (ms): 178
  HTTP Message/Entity-Body Size (bytes): 159350/158975
  HTTP Status: 200 OK
Next Start Time (seconds): 24

NSM config>
```

#### 2.4.22.1.1 Owner

Owner of NSM operation.

#### 2.4.22.1.2 Type of Operation to Perform

Http: HTTP Get operation type.

#### 2.4.22.1.3 Threshold

Reference for partial threshold (in milliseconds).

#### 2.4.22.1.4 Frequency

Frequency of operation (in seconds).

#### 2.4.22.1.5 Timeout

Operation timeout (in milliseconds).

#### 2.4.22.1.6 Status of Entry (SNMP RowStatus)

Administrative status of entry.

#### 2.4.22.1.7 Protocol Type

Value for HTTP Get operations: **httpAppl**

#### 2.4.22.1.8 Target Address [Port]

HTTP Get operation target IP address and port. Default port is 80. Target address is filled out once the HTTP server name has been resolved through DNS.

#### 2.4.22.1.9 Source Address [Port]

HTTP Get operation source IP address (or interface where said address is taken from) and port.

#### 2.4.22.1.10 Next-hop Address

Next-hop IP address (or interface) for Echo HTTP Get operation is displayed if the **next-hop** command is configured.

#### 2.4.22.1.11 Packet Size (ARR data) Request/Response

Payload data size in requests/responses.

#### 2.4.22.1.12 Type of Service (TOS)

TOS field value in IP header.

#### 2.4.22.1.13 HTTP Operation

Executed HTTP operation: **httpGet**

#### 2.4.22.1.14 URL

URL for downloading.

#### 2.4.22.1.15 Life

Operation lifetime (in seconds).

#### 2.4.22.1.16 Next Scheduled Start Time

Scheduling next operation startup.

#### 2.4.22.1.17 Operation Ageout

Time (in seconds) statistics are stored in the memory once an operation becomes inactive.

#### 2.4.22.1.18 Modification Time

Time of the latest configuration modification (SNMP only: once it has been launched, operation configuration cannot be modified using the command line).

#### 2.4.22.1.19 Last Reset Time

Latest reset time for operation (SNMP only).

#### 2.4.22.1.20 Number of Octets in use

Number of memory octets used by an operation.

#### 2.4.22.1.21 Occurred Connection-Lost/Timeout/Over-Threshold

Reports if the following has occurred in the latest operation: *Connection-Lost*/*Timeout*/*Over-Threshold*

#### 2.4.22.1.22 Number of Operations Attempted

Number of operations attempted (executions).

#### 2.4.22.1.23 Current Life Left

Current lifetime left (in seconds).

#### 2.4.22.1.24 Operational State

Operational state.

#### 2.4.22.1.25 Failed Operations

Unsuccessful operations due to:

*Disconnects:* Destination disconnected.

*Timeouts:* Maximum time for operation has timed out.

*Busies:* Operation cannot commence; previous operation has not yet finished.

*No Connections:* Connection with destination not established.

*Drops:* Internal errors.

*Sequence Errors:* Sequence errors, unexpected identifiers.

*Verify Errors:* Errors on checking data content.

#### 2.4.22.1.26 Captured Statistics

*Start Time:* Start time for latest statistics gathering time.

*Operations completed:* Successfully completed operations.

*Completed Over Thresholds:* Operations completed over the reference threshold.

*SumCompletion:* Accumulated time for successfully completed operations.

*SumCompletion2 High*/*Low:* Accumulated squared time for successfully completed operations.

*Completion Time Max*/*min*/*Average:* Maximum, minimum operation time and average value. Total Statistics.

*Elapsed Time:* Time lapsed from the beginning of statistics collection.

*Initiations:* Number of operation initiations.

*DNS Sum:* Total time used in DNS requests.

*DNS Timeouts*/*Errors:* Timeouts and errors in DNS requests.

#### 2.4.22.1.27 HTTP Collection Statistics

HTTP Statistics.

*TCP Connection Sum:* Total time spent establishing TCP connections.

*HTTP Transaction Sum:* Total time spent downloading the URLs.

*TCP Timeouts:* Timeouts when establishing TCP connection.

*HTTP Transaction Timeouts*/*Errors:* Timeouts and errors while downloading the URL.

#### 2.4.22.1.28 Latest HTTP Operation

Results of latest HTTP Get operation:

*Completion Time:* Total time spent in latest HTTP Get operation.

*Return Code:* Code notifying result of operation.

*Latest Start Time:* Time lapsed since last execution.

*DNS Time:* Time used in resolving DNS name.

*TCP Connection Time:* Time used in establishing TCP connection with server.

*HTTP Transaction Time:* Time used in downloading URL.

*HTTP Message/Entity-Body Size:* Data received / message body.

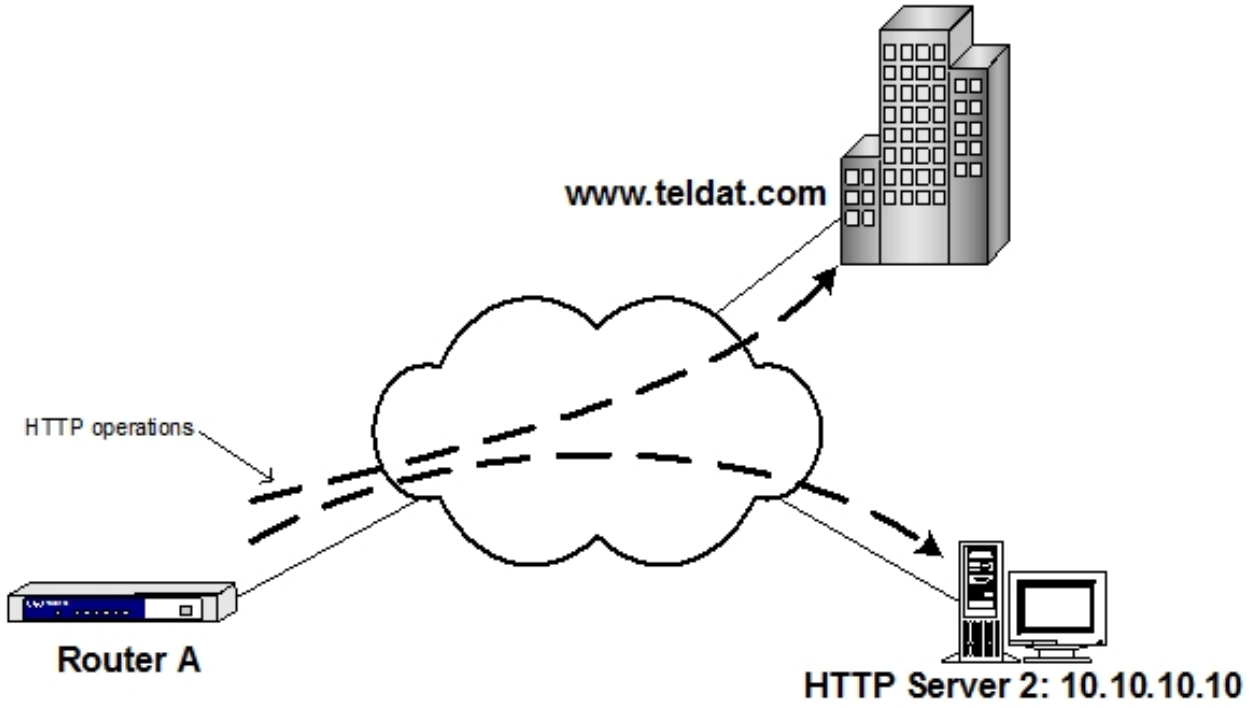
*HTTP Status:* Response (status) received from server.

#### 2.4.22.1.29 Next Start Time

Start time for subsequent operation execution.

### 2.4.22.2 HTTP Get operation examples

In the following example, Router A executes a **HTTP Ge**t from the www.teldat.com main web page and also from a test HTTP server with a known IP address.




For the www.teldat.com page:

```
Router-A NSM config>operation 3
-- NSM Operation configuration --
Router-A NSM operation 3>type http get http://www.teldat.com
Router-A NSM operation 3>exit
Router-A NSM config>schedule 3 start-time now
Router-A NSM config>
```

For an HTTP server with IP address 10.10.10.10:

```
Router-A NSM config>operation 4
-- NSM Operation configuration --
Router-A NSM operation 4>type http get http://10.10.10.10/test/testpage.html
Router-A NSM operation 4>frequency 300
Router-A NSM operation 4>exit
Router-A NSM config>schedule 4 life forever
Router-A NSM config>schedule 4 start-time now
```

```
Router-A NSM config>
```

**Router A Configuration:**

```
feature nsm
; -- Network Service Monitor configuration --
   operation 3
; -- NSM Operation configuration --
      type http get http://www.teldat.com
      timeout 60000
   exit
;
   operation 4
; -- NSM Operation configuration --
      type http get http://10.10.10.10/test/testpage.html
      frequency 300
      timeout 60000
   exit
;
   schedule 3 start-time now
   schedule 4 life forever
   schedule 4 start-time now
exit
;
```

## 2.4.23 UDP Jitter Operation

A jitter can be defined as a delay variation between two devices over time. A UDP Jitter operation aims at measuring delay, variations in said delay and packet loss.

A Jitter operation sends a series of test packets at constant intervals. Both the number of packets sent and the interval between packets can be modified. A device with an active responder must be at the other end so that, when jitter packets are received, a time stamp is given and these packets are returned to the source device.

In principle, the interval at which the device receives responses should be the same as the one at which packets were sent. When two consecutive packets are received with a greater delay than the transmission interval, this is considered positive jitter. Conversely, negative jitter is when they arrive at a shorter interval.

For example: if jitter test packets are transmitted 20 ms apart, responses are expected every 20 ms as well. If a response arrives at 22 ms, then positive jitter is 2 ms. If it arrives at 19 ms, then negative jitter is 1 ms.

High jitter values are undesirable for VoIP networks as they may degrade voice applications to the point where communication becomes unintelligible. A jitter value of 0 is ideal for all delay-sensitive networks and applications.

### 2.4.23.1 Description of UDP Jitter statistics

The following statistics are displayed for UDP Jitter operations:

```
NSM config>list running 30063
Operation ID Number: 30063
--------------------
Owner: InfoVista Server on test.teldat.es (172.24.0.51)
Type of Operation to Perform: jitter
Threshold (ms): 5000
Frequency (seconds): 60
Timeout (ms): 5000
Status of Entry (SNMP RowStatus): active
Protocol Type: jitterAppl
Target Address [Port]: 192.168.50.2 [8000]
Source Address [Port]: default [50371]
Next-hop Address: direct-ip1
Packet Size (ARR data) Request/Response: 32/0
Control Packets: true
Type of Service (TOS): 0x00
Internet hostname: example.teldat.es
Interval (ms): 20
Number of Packets: 10
Life (seconds): 3600
Next Scheduled Start Time: now
```

```
Operation Ageout (seconds): 60
Modification Time: 5m57s ago
Last Reset Time: never reset
Number of Octets in use: 3888
Occurred Connection-Lost/Timeout/Over-Threshold: false/false/false
Number of Operations Attempted: 186
Current Life Left (seconds): 3242
Operational State: active
Failed Operations:
  Disconnects.... 0              Timeouts....... 0
  Busies......... 0              No Connections. 0
  Drops.......... 0              Sequence Errors 0
  Verify Errors.. 0
Captured Statistics:
  Start Time: 5m19s ago
  Operations completed: 5
  Completed Over Thresholds: 0
  SumCompletion (ms): 956
  SumCompletion2 High/Low (ms): 0/66981680
  Completion Time Max/min/Average (ms): Max 20 - min 18 - Avg 191
  DNS Sum (ms): 45
  DNS Timeouts/Errors: 0/0
Totals Statistics:
  Elapsed Time: 5m19s
  Initiations: 5
JITTER Collection Statistics:
  JITTER Completions: 5
  Num. Of RTT: 50
  Sum Of RTT (ms): 956
  Sum2 Of RTT High/Low (ms): 0/66981680
  RTT min/Max (ms): 18/20
  Zeros SD: 40
  Positives SD: 3
    SumPosSD: 3            Sum2PosSD High/Low: 0/3
    minPosSD: 1            MaxPosSD: 1
  Negatives SD: 2
    SumNegSD: 2            Sum2NegSD High/Low: 0/4
    minNegSD: 1            MaxNegSD: 1
  Absolute average SD: 0
  Zeros DS: 35
  Positives DS: 4
    SumPosDS: 4            Sum2PosDS High/Low: 0/10
    minPosDS: 1            MaxPosDS: 1
  Negatives DS: 6
    SumNegDS: 6            Sum2NegDS High/Low: 0/10
    minNegDS: 1            MaxNegDS: 1
  Absolute average DS: 0
  Packet loss TOTAL: 0
  Packet loss SD: 0
  Packet loss DS: 0
  Packets out of sequence: 0
  Packets MIA: 0
  Packets late arrival: 0
  DNS Time (ms): 20
Latest JITTER Operation:
  Return Code: ok
  Num. Of RTT: 10
  Sum Of RTT (ms): 198
  Sum2 Of RTT (ms): 3922
  RTT min/Max (ms): 19/20
  Zeros SD: 6
  Positives SD: 1
    SumPosSD: 1      Sum2PosSD: 1      minPosSD: 1      MaxPosSD: 1
  Negatives SD: 2
    SumNegSD: 2      Sum2NegSD: 2      minNegSD: 1      MaxNegSD: 1
  Absolute average SD: 0
  Zeros DS: 4
```

```
  Positives DS: 3
    SumPosDS: 3      Sum2PosDS: 3      minPosDS: 1      MaxPosDS: 1
  Negatives DS: 2
    SumNegDS: 2      Sum2NegDS: 2      minPosDS: 1      MaxNegDS: 1
  Absolute average DS: 0
  Packet loss TOTAL: 0
  Packet loss SD: 0
  Packet loss DS: 0
  Packets out of sequence: 0
  Packets MIA: 0
  Packets late arrival: 0
  DNS Time (ms): 20
Next Start Time (seconds): 2

NSM config>
```

#### 2.4.23.1.1 Owner

Owner of the NSM operation.

#### 2.4.23.1.2 Type of Operation to Perform

Jitter: UDP Jitter operation type.

#### 2.4.23.1.3 Threshold

Reference for partial threshold (in milliseconds).

#### 2.4.23.1.4 Frequency

Frequency of operation (in seconds).

#### 2.4.23.1.5 Timeout

Operation timeout (in milliseconds).

UDP Jitter operation is only considered timed out when no test packets have been received before operation timeout expires.

#### 2.4.23.1.6 Status of Entry (SNMP RowStatus)

Entry's administrative status.

#### 2.4.23.1.7 Protocol Type

Value for UDP Jitter operations: **jitterAppl**

#### 2.4.23.1.8 Target Address [Port]

Target IP address and port used in UDP Jitter operations.

#### 2.4.23.1.9 Source Address [Port]

Source IP address for jitter operations (or interface where said address is taken from).

#### 2.4.23.1.10 Next-hop Address

Next-hop IP address (or interface) for a UDP Jitter operation is displayed if **next-hop** command is configured.

#### 2.4.23.1.11 Packet Size (ARR data) Request/Response

Payload data size in requests/responses.

#### 2.4.23.1.12 Control Packets

Control packets protocol.

#### 2.4.23.1.13 Type of Service (TOS)

TOS field value in IP header.

#### 2.4.23.1.14 Internet hostname

Internet hostname for UDP Jitter operations.

Only displayed if the destination address is configured as an Internet hostname.

#### 2.4.23.1.15 Interval

Interval between test packets used to measure jitter.

#### 2.4.23.1.16 Number of Packets

Number of test packets that make up a jitter operation.

#### 2.4.23.1.17 Life

Operation lifetime (in seconds).

#### 2.4.23.1.18 Next Scheduled Start Time

Starting time for the next scheduled operation.

#### 2.4.23.1.19 Operation Ageout

Time (in seconds) statistics are stored in memory when an operation becomes inactive.

#### 2.4.23.1.20 Modification Time

Time of latest configuration modification (SNMP only: once it has been launched, operation configuration cannot be modified using the commands line).

#### 2.4.23.1.21 Last Reset Time

Latest **reset** time for an operation (SNMP only).

#### 2.4.23.1.22 Number of Octets in use

Number of memory octets used in operation.

#### 2.4.23.1.23 Occurred Connection-Lost/Timeout/Over-Threshold

Reports if the following has occurred in the latest operation: *Connection-Lost*/*Timeout*/*Over-Threshold.*

#### 2.4.23.1.24 Number of Operations Attempted

Number of operations attempted (executions).

#### 2.4.23.1.25 Current Life Left

Current lifetime left (in seconds).

#### 2.4.23.1.26 Operational State

Operational state.

#### 2.4.23.1.27 Failed Operations

Unsuccessful operations due to:

*Disconnects:* Destination disconnected.

*Timeouts:* Maximum time for operation has timed out. Zero packets received.

*Busies:* Operation cannot commence; previous operation has not yet finished.

*No Connections:* Connection with destination not established.

*Drops:* Internal errors.

*Sequence Errors:* Sequence errors, unexpected identifiers.

*Verify Errors:* Errors on checking data content.

#### 2.4.23.1.28 Captured Statistics

*Start Time:* Start time for latest statistics gathering time.

*Operations completed:* Successfully completed operations.

*Completed Over Thresholds:* Operations completed over the reference threshold.

*SumCompletion:* Accumulated time for successfully completed operations.

*SumCompletion2 High/Low:* Accumulated squared time for successfully completed operations.

*Completion Time Max/min/Average:* Maximum, minimum operation time and average value.

*DNS sum (ms):* Total time used in DNS requests.

*DNS Timeouts/Errors:* Timeouts and errors produced in DNS requests.

**Note**

DNS-related statistics are only displayed if the destination address is configured as an Internet hostname.

#### 2.4.23.1.29 Totals Statistics

*Elapsed Time:* Time elapsed from statistics collection start time.

*Initiations:* Number of operation initiations.

#### 2.4.23.1.30 JITTER Collection Statistics

Jitter statistics:

*JITTER Completions:* Jitter operations successfully completed.

*Num. Of RTT:* Number of completed RTTs.

*Sum Of RTT:* Sum of RTT values.

*Sum2 Of RTT High/Low:* square sum of RTT values.

*RTT min/Max:* Maximum and minimum RTT.

*Zeros SD:* Null jitter values (constant delay) in Source to Destination.

*Positives SD:* Positive jitter values (delay increase) in Source to Destination.

- *SumPosSD:* Sum of positive SD jitter values.

- *Sum2PosSD High/Low:* Square sum of positive SD jitter.

- *minPosSD:* Minimum positive SD jitter value.

- *MaxPosSD:* Maximum positive SD jitter value.

*Negatives SD:* Negative jitter values (delay decrease) in Source to Destination.

- *SumNegSD*: Sum of negative SD jitter values.

- *Sum2NegSD High/Low*: Sum of squared negative SD jitter.

- *minNegSD*: Minimum negative SD jitter value.

- *MaxNegSD*: Maximum negative SD jitter value.

*Absolute average SD:* Average for the absolute jitter value in Source to Destination. To calculate this, add *SumPosSD* and *SumNegSD* and divide the result by the number of jitter values (the sum of *Zeros SD*, *Positives SD* and *Negatives SD*). The resulting value is close to the mean absolute deviation, in which jitter values are not directly considered and the average jitter value is subtracted instead. Given that the average jitter value tends to be 0, this estimation is never far off.

The concept behind DS values is the same as in SD values, but from Destination to Source.

*Packet loss TOTAL:* Global packet loss.

*Packet loss SD:* Packet loss in SD.

*Packet loss DS:* Packet loss in DS.

*Packets out of sequence:* Packets received out of sequence.

*Packets MIA:* Packet loss in which the direction cannot be determined (SD/DS).

*Packets late arrival:* Packets received after timeout.

*DNS Time:* Time used in resolving DNS name.

**Warning**

If packet control is disabled, the responder cannot determine the order of the packets received.

As a result, having packet loss statistics is meaningless for a specific direction (SD/DS):

- Loss statistics per direction are displayed as N/A (not available)

- Values obtained per direction using SNMP are also meaningless and should not be used.

Global packet loss statistics are still available.

**Note**

*DNS Time* is only displayed if the destination address is configured as an Internet hostname.

#### 2.4.23.1.31 Latest JITTER Operation

Latest UDP Jitter operation results. See previous description.

In addition to the above, the following extra statistic is displayed:

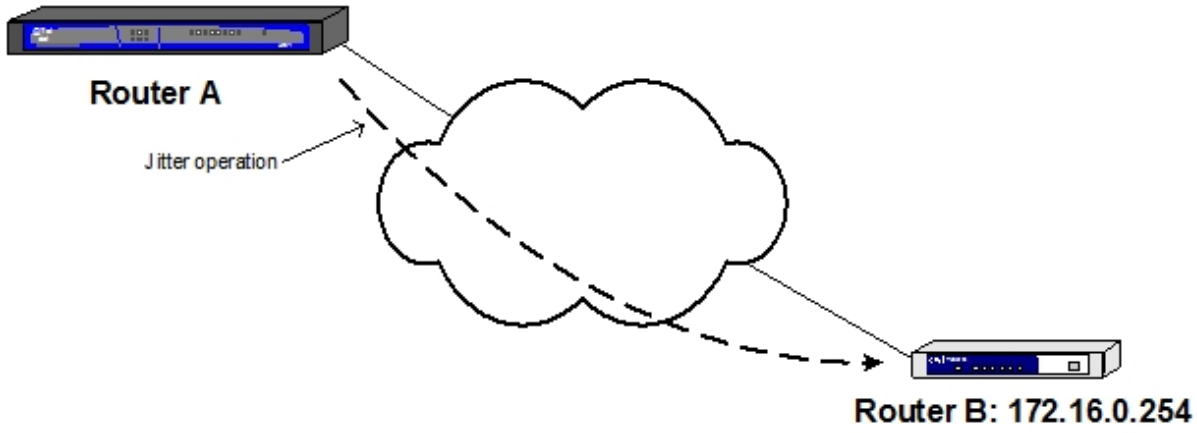
*Return Code:* Code reporting an operation result.

#### 2.4.23.1.32 Next Start Time

Start time for next operation execution.

### 2.4.23.2 UDP Jitter operation example

In the example below, Router A executes UDP Jitter measurements every 5 minutes to Router B, which acts as responder.




For Jitter operation:

```
Router-A NSM config>operation 5
-- NSM Operation configuration --
Router-A NSM operation 5>type jitter 172.16.0.254 dest-port 7000
Router-A NSM operation 5>frequency 300
Router-A NSM operation 5>exit
Router-A NSM config>schedule 5 start-time now
Router-A NSM config>
```

And in a device acting as responder:

```
Router-B NSM config>responder
Router-B NSM config>
```

**Router A Configuration:**

```
feature nsm
; -- Network Service Monitor configuration --
   operation 5
; -- NSM Operation configuration --
      type jitter 172.16.0.254 dest-port 7000
      control enable
      frequency 300
   exit
;
   schedule 5 start-time now
exit
;
```

**Router B Configuration:**

```
feature nsm
; -- Network Service Monitor configuration --
   responder
exit
;
```

## 2.4.24 BFD Operation

Bidirectional Forwarding Detection (BFD) is a protocol that helps detect drops in data communication links between two devices very quickly. As a result, alternative routes can be established in less time than through the Hello mechanisms of existing routing protocols.

BFD is a new type of operation included in the NSM feature. Within it, two subtypes can be defined: asynchronous and demand. These subtypes correspond to the BFD Asynchronous and Demand modes. Once established, the BFD session is executed in accordance with the mode defined in the NSM operation configuration.

A BFD session only has two reporting statuses: UP or DOWN (depending on whether the link that monitors BFD is up or down).

## 2.4.25 BFD statistics: Description

The following statistics are displayed for BFD operations in demand mode:

```
NSM config>list running 1
Operation ID Number: 1
--------------------
Owner: Teldat
Type of Operation to Perform: bfd
Frequency (seconds): 40
Timeout (ms): 5000
Status of Entry (SNMP RowStatus): active
Protocol Type: bfdDemand
Target Address [Port]: 10.10.44.200 [0]
Source Address [Port]: 10.10.44.205 [0]
Next-hop Address: ethernet0/0
Life (seconds): forever (never ends)
Next Scheduled Start Time: now
Operation Ageout (seconds): 3600
Modification Time: never modified
Last Reset Time: never reset
Number of Operations Attempted: 31
Current Life Left (seconds): forever (never ends)
Operational State: active
Failed Operations:
  Disconnects.... 0              Timeouts....... 0
  Busies......... 0              No Connections. 0
  Drops.......... 0              Sequence Errors 0
  Verify Errors.. 0
Captured Statistics:
  Start Time: 10m0s ago
  Operations completed: 30
Totals Statistics:
  Elapsed Time: 9m59s
  Initiations: 31
Latest BFD Operation:
  XmtTime: 50 ms   DetectTime: 150 ms
  Falls detected: 0    Diag code: No Diagnostic
  Xmtpkts: 30    Last Tx interval: 17s 405ms  min/max/avg: 312ms/20s 0ms/2s 116ms
  Rcvpkts: 30    Last Rx interval: 17s 406ms  min/max/avg: 819ms/20s 1ms/13s 435ms
Next Start Time (seconds): 20

NSM config>
```

The following statistics are displayed for BFD operations in asynchronous mode:

```
NSM config>list running 2
Operation ID Number: 2
--------------------
Owner: Teldat
Type of Operation to Perform: bfd
Status of Entry (SNMP RowStatus): active
Protocol Type: bfdAsync
Target Address [Port]: 172.24.80.10 [0]
Source Address [Port]: 172.24.80.12 [0]
Next-hop Address: direct-ip1
Life (seconds): forever (never ends)
Next Scheduled Start Time: now
Operation Ageout (seconds): 3600
Modification Time: never modified
Last Reset Time: never reset
Current Life Left (seconds): forever (never ends)
Operational State: active
Failed Operations:
  Disconnects.... 0              Timeouts....... 0
  Busies......... 0              No Connections. 0
  Drops.......... 0              Sequence Errors 0
  Verify Errors.. 0
Captured Statistics:
  Start Time: 11m20s ago
Totals Statistics:
  Elapsed Time: 11m20s
```

```
Latest BFD Operation:
  XmtTime: 50 ms   DetectTime: 150 ms
  Falls detected: 1    Diag code: Path Down
  Xmtpkts: 101    Last Tx interval: 43ms  min/max/avg: 38ms/46ms/42ms
  Rcvpkts: 102    Last Rx interval: 38ms  min/max/avg: 38ms/46ms/42ms

NSM config>
```

#### 2.4.25.1 Owner

Owner of the NSM operation.

#### 2.4.25.2 Type of Operation to Perform

**bfd**

#### 2.4.25.3 Frequency

Frequency of operation (in seconds). Only appears in BFD operations in demand mode.

#### 2.4.25.4 Timeout

Operation timeout (in milliseconds). Only appears in BFD operations in demand mode.

#### 2.4.25.5 Status of Entry (SNMP RowStatus)

Administrative status of the entry.

#### 2.4.25.6 Protocol Type

BFD operation type: **bfdDemand** or **bfdAsync**.

#### 2.4.25.7 Target Address [Port]

Target IP address (destination) for BFD operation. Port not applied.

#### 2.4.25.8 Source Address [Port]

Source IP address (or interface where address is taken from) for BFD operation. Port not applied.

#### 2.4.25.9 Next-hop Address

The next-hop IP address (or interface) for the BFD operation is displayed if the **next-hop** command is configured.

#### 2.4.25.10 Life

Operation life (in seconds).

#### 2.4.25.11 Next Scheduled Start Time

Next start time scheduled for operation purposes.

#### 2.4.25.12 Operation Ageout

Time statistics (in seconds) remain in the memory when the operation has finished.

#### 2.4.25.13 Modification Time

Time of the latest configuration modification (SNMP only: once it has been launched, operation configuration cannot be modified using the commands line).

#### 2.4.25.14 Last Reset Time

Last reset time (SNMP only).

#### 2.4.25.15 Current Life Left

Current life time left for operation (in seconds).

#### 2.4.25.16 Operational State

Operational state.

#### 2.4.25.17 Failed Operations:

Unsuccessful operations due to:

*Disconnects:* Disconnected destination.

*Timeouts:* Maximum time for operation has timed out.

*Busies:* Operation cannot commence; previous operation has not yet finished.

*No Connections:* Connection to destination has not been established.

*Drops:* Internal errors.

*Sequence Errors:* Sequence errors, unexpected identifiers.

*Verify Errors:* Errors when checking the data content.

#### 2.4.25.18 Captured Statistics

*Start Time:* Start time corresponding to the last time statistics were captured.

*Operations completed:* Successfully completed operations. Only appears for BFD operations in demand mode.

#### 2.4.25.19 Totals Statistics

*Elapsed Time:* Time lapsed since the capture of statistics started.

*Initiations:* Number of operation executions. Only appears for BFD operations in demand mode.

#### 2.4.25.20 Latest BFD Operation

Latest BFD operation results:

*XmtTime:* Transmission time for BFD packets.

*DetectTime:* Detection time for BFD packets.

*Falls detected:* Total number of drops detected by BFD.

*Diag code:* Description text on last drop detected by BFD.

*Xmtpkts*: Total number of transmitted BFD packets.

*Rcvpkts*: Total number of BFD packets received.

*Last Tx interval*: Last transmission interval: maximum, average and minimum values.

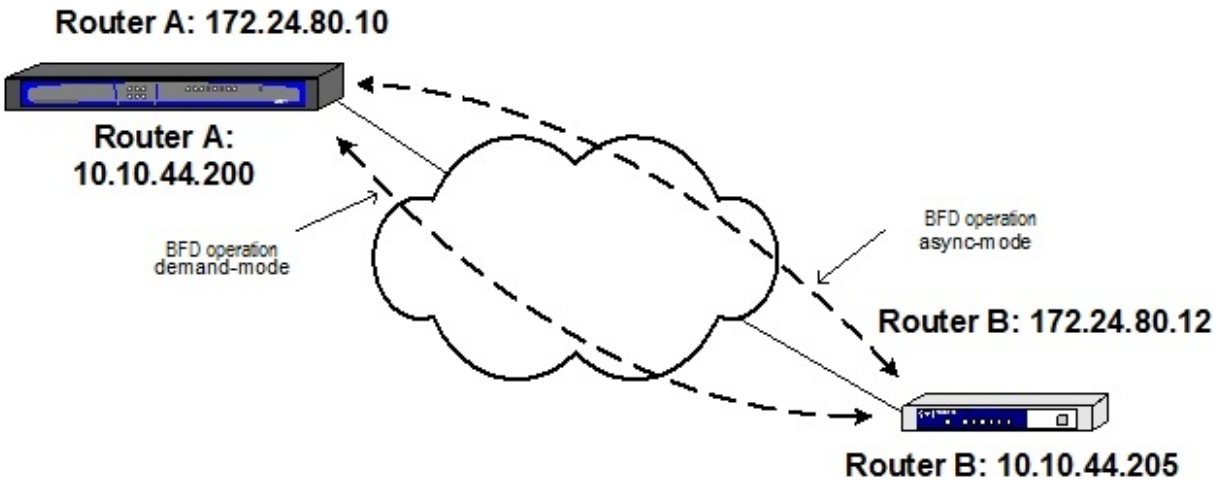
*Last Rx interval*: Last reception interval: maximum, average and minimum values.

#### 2.4.25.21 Next Start Time

Next start time for operation. Only appears for BFD operations in demand mode.

### 2.4.26 BFD operation examples

In the following example, we are going to execute a BFD operation in **demand-mode** between Router A and Router B through two of their interfaces and, at the same time, execute another BFD operation in asynchronous mode (**async-mode**) between both routers through different interfaces:




BFD operation in demand mode for Router A:

```
Router-A NSM config>operation 1
-- NSM Operation configuration --
Router-A NSM operation 1>type bfd demand-mode 10.10.44.205
Router-A NSM operation 1>bfd-interval 50
Router-A NSM operation 1>frequency 20
Router-A NSM operation 1>source-ipaddr 10.10.44.200
Router-A NSM operation 1>exit
Router-A NSM config>schedule 1 life forever
Router-A NSM config>schedule 1 start-time now
Router-A NSM config>
```

BFD operation in asynchronous mode for Router A:

```
Router-A NSM config>operation 2
-- NSM Operation configuration --
Router-A NSM operation 2>type bfd async-mode 172.24.80.12
Router-A NSM operation 2>bfd-interval 50
Router-A NSM operation 2>source-ipaddr 172.24.80.10
Router-A NSM operation 2>exit
Router-A NSM config>schedule 2 life forever
Router-A NSM config>schedule 2 start-time now
Router-A NSM config>
```

BFD operation in demand mode for Router B:

```
Router-A NSM config>operation 1
-- NSM Operation configuration --
Router-A NSM operation 1>type bfd demand-mode 10.10.44.200
Router-A NSM operation 1>bfd-interval 50
Router-A NSM operation 1>frequency 20
Router-A NSM operation 1>source-ipaddr 10.10.44.205
Router-A NSM operation 1>exit
Router-A NSM config>schedule 1 life forever
Router-A NSM config>schedule 1 start-time now
Router-A NSM config>
```

BFD operation in asynchronous mode for Router B:

```
Router-A NSM config>operation 2
-- NSM Operation configuration --
Router-A NSM operation 2>type bfd async-mode 172.24.80.10
Router-A NSM operation 2>bfd-interval 50
Router-A NSM operation 2>source-ipaddr 172.24.80.12
Router-A NSM operation 2>exit
Router-A NSM config>schedule 2 life forever
Router-A NSM config>schedule 2 start-time now
Router-A NSM config>
```

**Router A Configuration:**

```
protocol bfd
```

```
; -- Bidirectional Forwarding Detection user configuration --
   enable
  exit
;

feature nsm
; -- Network Service Monitor configuration --
   operation 1
; -- NSM Operation configuration --
      type bfd demand-mode 10.10.44.205
      bfd-interval 50
      frequency 20
      source-ipaddr 10.10.44.200
   exit
;
   operation 2
; -- NSM Operation configuration --
      type bfd async-mode 172.24.80.12
      bfd-interval 50
      source-ipaddr 172.24.80.10
   exit
;
   schedule 1 life forever
   schedule 1 start-time now
   schedule 2 life forever
   schedule 2 start-time now
exit
```

**Router B Configuration:**

```
protocol bfd
; -- Bidirectional Forwarding Detection user configuration --
   enable
  exit
;

feature nsm
; -- Network Service Monitor configuration --
   operation 1
; -- NSM Operation configuration --
      type bfd demand-mode 10.10.44.200
      bfd-interval 50
      frequency 20
      source-ipaddr 10.10.44.205
   exit
;
   operation 2
; -- NSM Operation configuration --
      type bfd async-mode 172.24.80.10
      bfd-interval 50
      source-ipaddr 172.24.80.12
   exit
;
   schedule 1 life forever
   schedule 1 start-time now
   schedule 2 life forever
   schedule 2 start-time now
exit
```

## 2.4.27 RADIUS Operation

Check the status of the RADIUS server using Radius accounting.

### 2.4.27.1 Description of RADIUS statistics

The following statistics are displayed for RADIUS operations:

```
NSM config>list running 3767
Operation ID Number: 3767
--------------------
Type of Operation to Perform: radius
Threshold (ms): 5000
Frequency (seconds): 10
Timeout (ms): 5000
Protocol Type: radiusAccounting
Target Address [Port]: 192.168.50.2 [0]
Source Address [Port]: default [0]
Life (seconds): 3600
Next Scheduled Start Time: now
Operation Ageout (seconds): 60
Number of Operations Attempted: 3533
Current Life Left (seconds): 448
Operational State: active
Failed Operations:
  Disconnects.... 0              Timeouts....... 0
  Busies......... 0              No Connections. 0
  Drops.......... 0              Sequence Errors 0
  Verify Errors.. 0
Captured Statistics:
  Start Time: 48m23s ago
  Operations completed: 48
  Completed Over Thresholds: 0
  SumCompletion (ms): 4175
  SumCompletion2 High/Low (ms): 0/1929913
  Completion Time Max/min/Average (ms): Max 858 - min 21 - Avg 86
Totals Statistics:
  Elapsed Time: 48m23s
  Initiations: 48
Next Start Time (seconds): 28

NSM config>
```

#### 2.4.27.1.1 Type of Operation to Perform

Radius: RADIUS type operation.

#### 2.4.27.1.2 Threshold

Reference for partial threshold (in milliseconds).

#### 2.4.27.1.3 Frequency

Frequency of operation (in seconds).

#### 2.4.27.1.4 Timeout

Operation timeout (in milliseconds).

#### 2.4.27.1.5 Protocol Type

Value for RADIUS operations: **radiusAccounting**

#### 2.4.27.1.6 Target Address [Port]

Target IP address and port (destination) for RADIUS operations.

#### 2.4.27.1.7 Source Address [Port]

Source IP address (or interface from which said address is taken) for RADIUS operations. Port not applied.

#### 2.4.27.1.8 Life

Operation lifetime (in seconds).

#### 2.4.27.1.9 Next Scheduled Start Time

Scheduling next operation startup.

#### 2.4.27.1.10 Operation Ageout

Time (in seconds) statistics are stored in the memory once an operation becomes inactive.

#### 2.4.27.1.11 Number of Operations Attempted

Number of operations attempted (executions).

#### 2.4.27.1.12 Current Life Left

Current lifetime left (in seconds).

#### 2.4.27.1.13 Operational State

Operational state.

#### 2.4.27.1.14 Failed Operations

Unsuccessful operations due to:

*Disconnects:* Destination disconnected.

*Timeouts:* Maximum time for operation has timed out.

*Busies:* Operation cannot commence; previous operation has not yet finished.

*No Connections:* Connection with destination not established.

*Drops:* Internal errors.

*Sequence Errors:* Sequence errors, unexpected identifiers.

*Verify Errors:* Errors when checking data content.

#### 2.4.27.1.15 Captured Statistics

*Start Time:* Start time for the latest statistics gathering time.

*Operations completed:* Successfully completed operations.

*Completed Over Thresholds:* Operations completed over the reference threshold.

*SumCompletion:* Accumulated time for successfully completed operations.

*SumCompletion2 High/Low:* Accumulated squared time for successfully completed operations.

*Completion Time Max/min/Average:* Maximum, minimum operation time and average value.

#### 2.4.27.1.16 Totals Statistics

*Elapsed Time:* Time lapsed from statistics collection start time.

*Initiations:* Number of operation initiations.

#### 2.4.27.1.17 Next Start Time

Start time for subsequent operation execution.

### 2.4.27.2 RADIUS operation examples

In the following example, Router A executes a RADIUS operation. The IP, destination port (port 1813, by default), user and secret configured in the RADIUS server are used.

For Router A Echo IP/ICMP operation to Host 1:

```
Router-A NSM config>operation 1
-- NSM Operation configuration --
Router-A NSM operation 1>type radius 172.16.0.1 dest-port default user user secret plain secret
Router-A NSM operation 1>exit
Router-A NSM config>schedule 1 life forever
Router-A NSM config>schedule 1 start-time now
```

In this example, the port on which [re] authenticated is initially authorized begins to perform [re] authentication (script 2) when the RADIUS server is detected. This way, problems are avoided when starting the router while the RADIUS server is idle. If more ports need to be authenticated, they must be added to the scripts (script 1 / script 2).

In this case, the general configuration should look like this:

**Router A configuration:**

```
   feature aaa
; -- AAA user configuration --
      enable
      radius-servers
         timeout 1
         server "Radius_1"
            key ciphered 0x212A70810217FFF5AE3AC75344FAEA74
            host <IP RADIUS SERVER>
         exit
;
;
      exit
;
      group server radius "group1"
         server Radius_1
      exit
;
;
      authentication dot1x "dot1x_list"
         method 1 group group1
         method 2 none
      exit
;
   exit
;
;
   network ethernet0/0
; -- Ethernet Interface User Configuration --
      ip address <LAN_IP> <MASK>
;
;
      repeater-switch
; -- Switch User Config --
         port 1 dot1X
; -- 802.1X User Config --
            authenticator port-control force-authorized
         exit
;
         port 2 dot1X
; -- 802.1X User Config --
            authenticator port-control force-authorized
         exit
;
         port 3 dot1X
; -- 802.1X User Config --
            authenticator port-control force-authorized
            authenticator reauth-period 60
         exit
;
      exit
;
   exit
;
```

```
;
   network ethernet0/1
; -- Ethernet Interface User Configuration --
      ip address <WAN_IP> <MASK>
;
      dot1x
; -- 802.1X User Config --
         authenticator port-control force-authorized
      exit
;
   exit
;
;
;
   protocol dot1X
; -- 802.1X User Config --
      system-auth-control
   exit
;
;
;
;
;
;
   feature nsm
; -- Network Service Monitor configuration --
      operation 1
; -- NSM Operation configuration --
         type radius <IP RADIUS SERVER> dest-port 1813 user <USER> secret plain <SECRET>
         frequency 10
      exit
;
      schedule 1 life forever
      schedule 1 start-time now
   exit
;
   feature nsla
; -- Feature Network Service Level Advisor --
      enable
;
      filter 1 nsm-op 1 rtt
      filter 1 significant-samples 1
      filter 1 activation threshold timeout
      filter 1 activation sensibility 100
      filter 1 activation stabilization-time 0
      filter 1 deactivation threshold timeout
      filter 1 deactivation sensibility 100
      filter 1 deactivation stabilization-time 0
      filter 1 initial-state active
;
      alarm 1 filter-id 1
;
      advisor 1 description "RADIUS server check"
      advisor 1 alarm-id 1
;
      advisor 2 not alarm-id 1
;
   exit
;
;
   feature management
; -- Management user configuration --
      operation 1 system script 1
      operation 1 track nsla-advisor 1
;
      operation 2 system script 2
      operation 2 track nsla-advisor 2
```

```
      script 1 commands root
      script 1 commands running-config
      script 1 commands "network ethernet0/0"
      script 1 commands repeater-switch
      script 1 commands "port 3 dot1X"
      script 1 commands "no authenticator reauthentication"
      script 1 commands root
      script 1 commands monitor
      script 1 commands "network ethernet0/0"
      script 1 commands repeater-switch
      script 1 commands "dot1X 3"
      script 1 commands "reauth-abort enable"
;
      script 2 commands root
      script 2 commands running-config
      script 2 commands "network ethernet0/0"
      script 2 commands repeater-switch
      script 2 commands "port 3 dot1X"
      script 2 commands "no authenticator port-control force-authorized"
      script 2 commands "authenticator authentication dot1x dot1x_list"
      script 2 commands "authenticator reauthentication"
      script 2 commands root
      script 2 commands monitor
      script 2 commands "network ethernet0/0"
      script 2 commands repeater-switch
      script 2 commands "dot1X 3"
      script 2 commands "reauth-abort disable"
;
;
      exit
```

# Chapter 3 Monitoring

## 3.1 Accessing the NSM monitoring menu

NSM monitoring commands must be entered in the monitoring menu associated with NSM (*NSM+*). To access said menu, use **feature NSM** found in the general monitoring menu (+).

```
+feature nsm
-- NSM console --
NSM+
```

After accessing this menu, you can enter the following commands:

| Command | Function |
|---|---|
| *CLEAR* | Clears stored statistics for an NSM operation. |
| *DELETE* | Deletes an NSM operation. |
| *LIST* | Displays information on NSM operations that are currently running. |
| *TWAMP* | Displays TWAMP information. |
| *EXIT* | Exits the NSM monitoring menu. |

**Note**

Please note that the NSM configuration menu allows you to monitor the state and the operations that are currently running (through **list running**).

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | The **twamp** command was added as of version 11.01.04. |

## 3.2 NSM Monitoring Commands

### 3.2.1 CLEAR

Clears stored statistics on the NSM being monitored.

```
NSM+clear ?
  <1..65535>    Operation id number
  <cr>          All NSM operations
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.08 | The "*clear*" command was added as of version 11.01.08. |

#### 3.2.1.1 CLEAR

Consecutively clears stored statistics on NSM operations that are currently running in a device.

*Syntax:*

```
NSM+clear
```

#### 3.2.1.2 CLEAR [<operation-id>]

Clears stored statistics on the NSM operation by specifying its id.

*Syntax:*

```
NSM+clear <operation-id>
```

*Example:*

```
NSM+clear 7
NSM+
```

### 3.2.2 DELETE

Deletes an NSM operation that is currently running.

*Syntax:*

```
NSM+delete <operation-id>
```

*Example:*

```
NSM+delete 7
NSM+
```

**Note**

When you delete an operation from the monitoring menu, the associated configuration IS NOT DELETED (when created through the command line). You can subsequently relaunch this operation by entering **schedule**.

**Command history:**

| Release | Modification |
|---|---|
| 11.00.05 | This command was obsoleted as of version 11.00.05. |
| 11.01.00 | This command was obsoleted as of version 11.01.00. |

### 3.2.3 LIST

Displays information on the NSM being monitored.

```
NSM+list ?
  <1..65535>    Operation id number
  <cr>          All NSM operations
```

#### 3.2.3.1 LIST

Consecutively displays information on NSM operations that are currently running in a device.

*Syntax:*

```
NSM+list
```

#### 3.2.3.2 LIST [<operation-id>]

Displays information on the NSM operation by specifying its id.

Depending on the operation type, certain statistics (specific to said operations) are displayed (Echo IP/ICMP, HTTP Get, BFD, UDP Jitter or Radius).

*Syntax:*

```
NSM+list <operation-id>
```

*Example:*

```
NSM+list 1
Operation ID Number: 1
--------------------
Owner: Teldat R&D Test
Type of Operation to Perform: echo
Threshold (ms): 5000
Frequency (seconds): 60
Timeout (ms): 5000
Status of Entry (SNMP RowStatus): active
```

```
Protocol Type: ipIcmpEcho
Target Address [Port]: 172.16.0.1 [0]
Source Address [Port]: default [0]
Packet Size (ARR data) Request/Response: 28/0
Type of Service (TOS): 0x00
Life (seconds): 3600
Next Scheduled Start Time: now
Operation Ageout (seconds): 3600
Modification Time: never modified
Last Reset Time: never reset
Number of Octets in use: 3888
Occurred Connection-Lost/Timeout/Over-Threshold: false/false/false
Number of Operations Attempted: 1
Current Life Left (seconds): 3590
Operational State: active
Failed Operations:
  Disconnects.... 0              Timeouts....... 0
  Busies......... 0              No Connections. 0
  Drops.......... 0              Sequence Errors 0
  Verify Errors.. 0
Captured Statistics:
  Start Time: 10s ago
  Operations completed: 1
  Completed Over Thresholds: 0
  SumCompletion (ms): 5
  SumCompletion2 High/Low (ms): 0/25
  Completion Time Max/min/Average (ms): Max 5 - min 5 - Avg 5
Totals Statistics:
  Elapsed Time: 9s
  Initiations: 1
Latest ECHO IP/ICMP Operation:
  Completion Time (ms): 5
  Return Code: ok
  Latest Start Time: 10s ago
  Target Address: 172.16.0.1
Next Start Time (seconds): 50

NSM+
```

### 3.2.4 TWAMP

Displays information on the TWAMP server and responder.

*Syntax:*

```
NSM+twamp ?
  responder    Display information on TWAMP
               responder/reflector
  server       Display information on TWAMP server
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | The "*twamp*" command was added as of version 11.01.04. |

#### 3.2.4.1 TWAMP RESPONDER SESSIONS

Displays the test sessions configured in the TWAMP responder.

*Syntax:*

```
NSM+twamp responder sessions [sender-ip <IPv4 address>]
```

Filtering options are as follows:

- **sender-ip**: option to filter through the Session-Senders IP addresses.

*Example*

```
NSM+twamp responder sessions

===================================
..::  TWAMP Responder Sessions  ::..
===================================

Conn-Id: 2, Sender IP: 192.168.2.85, Sender Port: 40000
VRF: vpn1, Receiver IP: 192.168.2.83, Receiver Port: 40000
SID: 192.168.2.83:3180294026165785737 6:480F3124
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | The "*twamp responder sessions*" command was added as of version 11.01.04. |

### 3.2.4.2 TWAMP RESPONDER STATUS

Displays information on the TWAMP responder status.

*Example:*

```
NSM+twamp responder status
TWAMP responder on VRF global is DISABLED
TWAMP responder on VRF vpn1 is ENABLED
TWAMP responder on VRF vpn2 is DISABLED
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | The "*twamp responder status*" command was added as of version 11.01.04. |

### 3.2.4.3 TWAMP SERVER CONNECTIONS

Displays information on the control connections established in the TWAMP server.

*Syntax:*

```
NSM+twamp server connections [client-ip <IPv4 address>]
```

Filtering options are as follows:

- **client-ip**: option to filter through the Control-Clients IP addresses.

*Example:*

```
NSM+twamp server connections

===================================
..::  TWAMP Server Connections  ::..
===================================

Conn-Id: 1, Client IP: 192.168.2.85, Client Port: 49445
VRF: vpn1, Mode: Unauth, Connection state: Testing
Number of test sessions (requested/active): 1/1
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | The "*twamp server connections*" command was added as of version 11.01.04. |

### 3.2.4.4 TWAMP SERVER STATUS

Displays information on the status of the TWAMP server.

*Example:*

```
NSM+twamp server status
```

```
TWAMP server on VRF global is DISABLED
TWAMP server on VRF vpn1 is ENABLED on port 862
TWAMP server on VRF vpn2 is DISABLED
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.04 | The "*twamp server status*" command was added as of version 11.01.04. |

### 3.2.5 EXIT

Exits the NSM monitoring menu and returns to the main monitoring menu (+).

*Syntax:*

```
NSM+exit
```

*Example:*

```
NSM+exit
+
```

# Chapter 4 Example

## 4.1 Multiple NSM Operations

The following configuration example shows several NSM operations, or probes, running in a given device. When a large number of operations have been programmed, you must make sure there is a time separation between executions. To do this, carefully select values for the *start-time, frequency*, *interval* and *num-packets* parameters (the last two are only applicable to UDP Jitter probes).

```
Config>show config
log-command-errors
no configuration
set data-link x25 serial0/0
set data-link x25 serial0/1
set data-link x25 serial0/2
;
network ethernet0/0
; -- Ethernet Interface User Configuration --
   ip address 172.24.78.57 255.255.0.0
;
;
;
;
exit
;
;
;
network x25-node
; -- X25-node interface configuration --
   no ip address
;
exit
;
protocol ip
; -- Internet protocol user configuration --
   internal-ip-address 10.0.0.1
;
exit
;
;
feature dns
; -- DNS resolver user configuration --
   server 172.24.0.6
exit
;
feature nsm
; -- Network Service Monitor configuration --
   operation 1
; -- NSM Operation configuration --
      type echo ipicmp 172.24.78.5
   exit
;
   operation 2
; -- NSM Operation configuration --
      type echo ipicmp 172.24.78.36
      frequency 120
      request-data-size 1000
      source-ipaddr 10.0.0.1
   exit
;
   operation 3
; -- NSM Operation configuration --
      type echo ipicmp 172.24.78.118
   exit
```

```
;
   operation 4
; -- NSM Operation configuration --
      type echo ipicmp 172.24.78.81
   exit
;
   operation 5
; -- NSM Operation configuration --
      type echo ipicmp www.teldat.es
      frequency 120
      source-ipaddr ethernet0/0
   exit
;
   operation 6
; -- NSM Operation configuration --
      type http get http://www.teldat.es
      timeout 60000
   exit
;
   operation 7
; -- NSM Operation configuration --
      type http get http://172.24.78.119/manual/mod/core.html
      frequency 120
      timeout 60000
   exit
;
   operation 8
; -- NSM Operation configuration --
      type jitter 172.24.78.1 dest-port 8000
   exit
;
   operation 9
; -- NSM Operation configuration --
      type jitter 172.24.78.2 dest-port 8000
      control enable
   exit
;
   operation 10
; -- NSM Operation configuration --
      type jitter 172.24.78.3 dest-port 8000
      control enable
   exit
;
   operation 11
; -- NSM Operation configuration --
      type bfd demand-mode 172.24.78.112
      bfd-interval 50
      frequency 20
      source ip-addr 172.24.78.57
   exit
;
   operation 12
; -- NSM Operation configuration --
      type bfd async-mode 172.24.78.115
      bfd-interval 50
      source ip-addr 172.24.78.57
   exit
   operation 13
; -- NSM Operation configuration --
      type radius 172.24.78.115 dest-port default user user        secret plain secret
      frequency 10
   exit
;
   schedule 1 start-time now
   schedule 2 life forever
   schedule 2 start-time after 1s
   schedule 3 life forever
```

```
   schedule 3 start-time after 2s
   schedule 4 start-time after 3s
   schedule 5 start-time after 4s
   schedule 6 start-time after 5s
   schedule 7 start-time after 15s
   schedule 8 life forever
   schedule 8 start-time after 25s
   schedule 9 start-time after 35s
   schedule 10 start-time after 45s
   schedule 11 life forever
   schedule 11 start-time now
   schedule 12 life forever
   schedule 12 start-time now
   schedule 13 life forever
   schedule 13 start-time now

exit
Config>
```