BFD Protocol

Teldat-Dm 779-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-Dm 749-I NSM Feature

Chapter 1 BFD Protocol

1.1 Introduction

Bidirectional Forwarding Detection (BFD) is a protocol designed to provide fast detection of drops in data communication links between two devices. Fast detection allows you to establish alternative routes quicker than by using the existing 'Hello' mechanisms in routing protocols.

Routing protocol detection should take, at least, 1 second. However, this amount of time proves excessive for certain applications and could entail an excessive loss of data for gigabit transfer rates. BFD aims at detecting drops in data communication fast, generating little overload and occupying the line for a short amount of time. Problem detection in the line, interfaces and is the forwarder for each router is carried out in the link that joins the two neighboring devices. Additionally, the BFD protocol aims at standardizing detection methods so that they work for all types of mediums, links and protocols. To do this, it uses programmable detection times and adapts them to the routing features of devices.

This document focuses on protocol characteristics and explains how to use then in different scenarios and for several applications. It also details the protocol configuration and monitoring.

1.2 Protocol Description

Our routers support BFD implementation over the IPv4 protocol and with unicast packets (i.e. in point-to-point mode between two routers). The BFD protocol often encapsulates UDP with destination port 3784 (4784 for multihop sessions) and source port between 49152 and 65535. The source port is unique for each BFD session.

The BFD protocol basically transmits packets at a continuous rate between the two devices at the two ends of the link being monitored. An incident is detected when packets stop being received at one of the two ends for a given period of time.

For each link being monitored, a new BFD session is created. During negotiation between the two devices to establish the BFD session, both devices set their limitations on packet transmission and reception. This way, the faster device adapts to the slower one and the transmission and detection times for each device are defined.

The routing protocols register in the BFD session that monitors the desired link. The session notifies the routing protocols registered in the session about changes in the link status. There is only one BFD session for each link to be monitored.

1.2.1 Operating Modes

The BFD protocol has three different operating modes: *Asynchronous*, *Demand* and *Echo*.

1.2.1.1 Asynchronous Mode

The *Asynchronous* mode transmits packets in accordance with a fixed transmission period, but one end is independent from the other. This means that a device can set a transmission period that is totally different from the one chosen by the device at the other end of the link. Each transmission period is negotiated when establishing the session. Problems are detected when packets from the remote end are not received within a time period that exceeds the detection interval negotiated while the session was established.

1.2.1.2 Demand Mode

The *Demand* mode only checks the line status at given times, when the registered protocol wants to know the link status. Whenever this is the case, a poll sequence is executed and (save for the negotiation prior to establishing the session) it is here where there is BFD packet transmission on the line. This operating mode prevents any type of line overloading, but restricts detection to poll intervals. The *Demand* mode should not be used when the return time on the link is greater than the detection time.

1.2.1.3 Echo Mode

The *Echo* mode allows a device to send packets and has the remote device forwarder return the packets to the local device. Problems are detected when return packets are not received within the detection time set. Sent packets are defined as echo packets. This mode helps you detect problems in the remote device forwarder, and allows for more aggressive detection times by reducing the jitter on the return path. This mode can only be enabled at one of the two link ends, although both ends must agree.

1.2.2 BFD Releases

Currently, there are two BFD releases: version 0 and version 1. Our devices support both versions and, by default, operate in the highest version supported by the remote device being used to negotiate the session establishment process. You can, however, force operations in version 0 through configuration.

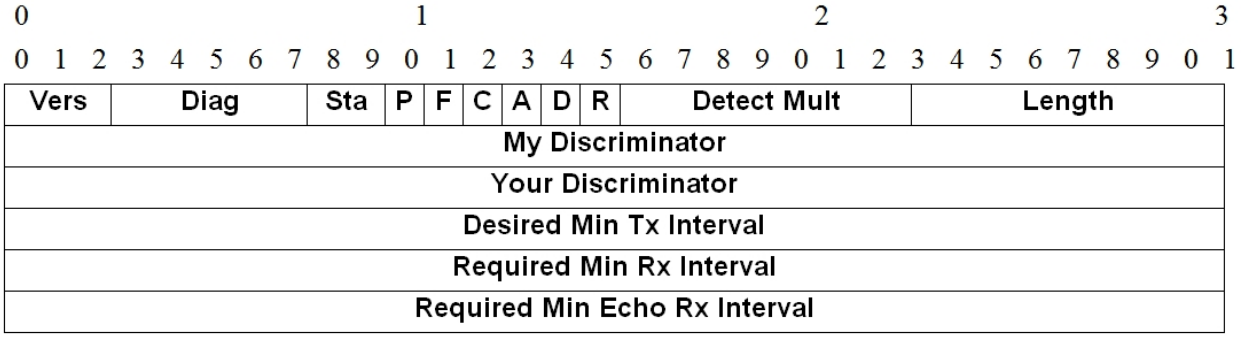
The implementation of this protocol follows IETF recommendations: Bidirectional Forwarding Detection (BFD) [RFC5880], Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop) [RFC5881] and Bidirectional Forwarding Detection (BFD) for Multihop Paths [RFC 5883].

1.2.3 BFD Packet Format

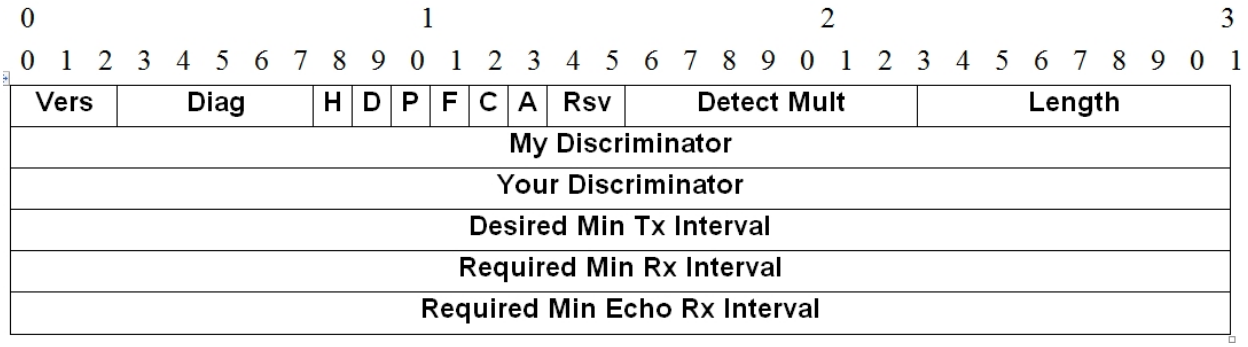
The BFD packet has a mandatory section and an optional authentication section. Singlehop sessions are not authenticated. For security purposes, only IPv4 packets whose TTL field is equal to 255 are accepted. Multihop sessions support the following authentication types: Keyed MD5, Meticulous Keyed MD5, Keyed SHA1 and Meticulous Keyed SHA1.

The mandatory section of BFD packets has the following format:

1.2.3.1 Version 1



1.2.3.2 Version 0



The only difference between both versions is the *State* field, which does not exist in version 0 and is used to replace the *I Hear You* field.

The meaning of each packet field is as follows:

- **Version (Vers):**

  BFD protocol version.
- **Diagnostic (Diag):**

  Numerical code indicating the reason for the last drop detected in the device that sends the packet. The values that this can take are as follows:

  0 – No Diagnostic

  1 – Control Detection Time Expired

  2 – Echo Function Failed

  3 – Neighbor Signaled Session Down

  4 – Forwarding Plane Reset

5 – Path Down

6 – Concatenated Path Down

7 – Administratively Down

8 – Reverse Concatenated Path Down

9-31 – Reserved for future use

- **I Hear You (H) (this only exists in version 0):**

  This bit is 0 if the device does not receive packets from the remote end or if it is in the process of considering the session as down. The bit is 1 when the session is established and packets are being received from the remote device.

- **State (Sta) (this only exists in version 1):**

  This is the current state of the states machine for the device protocol that transmits the packet. These values can be:

  0 – AdminDown

  1 – Down

  2 – Init

  3 – Up

- **Poll (P):**

  If this value is 1, the device transmitting the packet is requesting communication verification (Demand Mode) or parameter renegotiation.

- **Final (F):**

  If this is 1, the device transmitting is responding to a packet with a Poll bit set to 1.

- **Control Plane Independent (C):**

  This is not used, and its value should be 0.

- **Authentication Present (A):**

  If this is 1, the packet contains the optional authentication section. If it is 0, then the packet goes without authentication.

- **Demand (D):**

  If this is 1, the device transmitting the packet is requesting to operate in *Demand* Mode. If this is 0, the device is either incapable or unwilling to operate in *Demand* Mode.

- **Reserved (R):**

  This is not used, and its value should be 0.

- **Detect Mult:**

  This is the detection interval multiplier. This is the number used to multiply the negotiated transmission interval to obtain the detection interval.

- **Length:**

  Length of the BFD packets, in bytes. Without authentication this is 24 and with authentication it is 24 plus the size of the authentication section.

- **My Discriminator:**

  Value that identifies the session in the device transmitting the packet. This value is randomly generated when the session is created.

- **Your Discriminator:**

  Value that identifies the session in the device receiving the packet. This reflects the value received in the My Discriminator field in the previous packet. If this is 0 then the identifier is unknown as a packet from the remote device has not been received yet.

- **Desired Min Tx Interval:**

  This is the minimum time interval in microseconds that the device transmitting the packet wishes to exist between transmitted BFD packets.

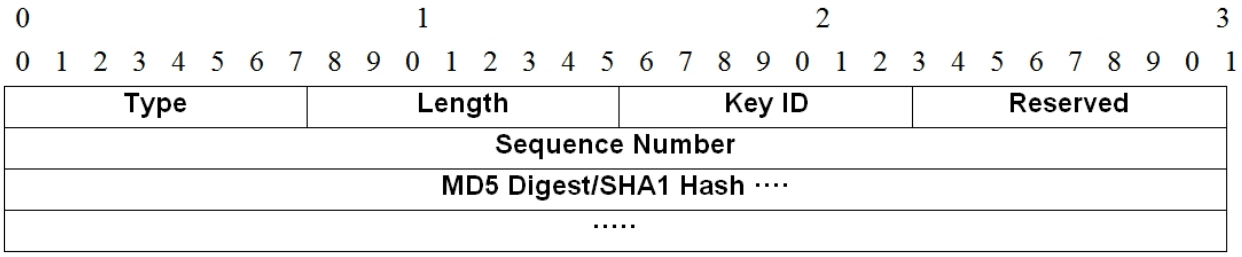
- **Required Min Rx Interval:**

This is the minimum time interval in microseconds between received BFD packets that the device transmitting the packets can support.

- **Required Min Echo Rx Interval:**

  This is the minimum time interval in microseconds between received ECHO packets that the device transmitting the packet can support. If this value is 0, this indicates that the device transmitting the packet does not admit reception of ECHO packets. In the case of our devices, this value is 0.

1.2.3.3 Authentication Section



The Authentication section is optional and is only present if the Authentication Present (A) bit is activated in the mandatory part of the BFD packet.

- **Type:**

  Type of authentication. 1 Simple Password (not supported), 2 Keyed MD5, 3 Meticulous Keyed MD5, 4 Keyed SHA1, Meticulous Keyed SHA1.

- **Length:**

  Length of the authentication section, in bytes. This is 24 for MD5 authentication types and 28 for SHA1 authentication types.

- **Key ID:**

  The key ID used to generate the MD5 digest or the SHA1 hash. This enables the use of multiple keys with the Key Chain feature. The value is 0 if only one key is configured.

- **Reserved:**

  This must be set to 0 on transmit and ignored on receipt.

- **Sequence Number:**

  The sequence number used in authentication. For meticulous authentication, this value is incremented for each successive packet transmitted. For non-meticulous authentication, this value is incremented when the session state changes. The range of valid sequence numbers accepted at the receiving end for Keyed MD5 and Keyed SHA1 authentication types is from RecAuthSeqNum to RecAuthSeqNum + 3 * DetectTime included. For Meticulous Keyed MD5 and Meticulous Keyed SHA1 authentication types, packets between RecAuthSeqNum + 1 and RecAuhtSeqNum + 3 * DetectTime included, are accepted.

- **MD5 Digest/SHA1 Hash:**

  This field contains the result of applying the MD5 or SHA1 function to the whole BFD packet after copying the key used to this field and padding it out with zeros when it is shorter than the size of the field. The field size is 16 bytes for MD5 and 20 bytes for SHA1 (i.e. the maximum key sizes that can be used).

1.2.4 Negotiating the timers

During the last part of session establishment, the timers negotiation is carried out. This is used by each device to detect problems in the communication link monitoring the BFD session.

The times negotiated are the **transmission time** (XmtTime) and the **detection time** (DetectTime). The transmission time is, as the name suggests, the time in which a device transmits BFD packets in *Asynchronous* mode. The detection time is the maximum period of time the device waits without receiving a packet from the remote end before stating that there is a problem. If a BFD packet is not received during a time period greater than the detection time, the session is considered lost.

During session negotiation, each device transmits its limitations on packet transmission and reception. The values transmitted by each device are entered through configuration and are as follows:

- **Desired Min Tx Interval (DesMinTx)**
- **Required Min Rx Interval (ReqMinRx)**
- **Detect Multiplier (DetectMult)**

The times in each device is negotiated with these three values. The equations used are as follows:

- **XmtTime = max(DesMinTx, Recv ReqMinRX)**
- **DetectTime = Recv DetectMult * max (ReqMinRx, Recv DesMinTx)**

In *Demand* mode, the detection time is calculated differently and depends on the BFD protocol version:

- **Version 1: DetectTime = DetectMult * (DesMinTx, Recv ReqMinRX)**
- **Version 0: DetectTime = DetectMult * (ReqMinRX, Recv DesMinTx)**

When the session is lost, and prior to the timers negotiation, the devices transmit with a time period of 1 second. Therefore, if the link is down for a long time, the BFD protocol does not penalize devices that send packets at low transmission periods.

1.2.5 Support for IPv6 addresses

From version 11.01.04 onwards, support for IPv6 has been added for the BGP protocol.

BFD for NSM does not currently support IPv6 addresses.

IPv6 addresses are also supported in multihop sessions.

Chapter 2 BFD Protocol Configuration

2.1 Introduction

BFD protocol configuration is performed in different setup menus. These include the BFD protocol global configuration menu; the single hop session parameters configuration menu belonging to the interface associated with the session; and finally, the session configuration menu found under routing protocols.

- The BFD protocol global configuration menu allows you to enable or disable the protocol. It also allows you to configure profiles for multihop sessions, in which you define the parameters to be used for these sessions. It lets you define multihop sessions and assign the corresponding profile.
- The parameters for negotiating BFD session timers are configured on each interface. This is only true for single hop sessions. The parameters for negotiating multihop sessions are defined in the profiles in the BFD protocol menu.
- In the configuration for each protocol, you associate the routing protocol with a BFD session, identified by the remote device address with which you establish the session.

Note

The NSM feature is a special case. In the case of single hop sessions, the BFD session configured from NSM has its own parameters and is independent of the parameters configured in the interface associated with the BFD session. The BFD negotiation parameters for multihop sessions will be those defined in the associated profile.

2.2 BFD Protocol Global Configuration

The BFD protocol is enabled and disabled by means of the protocol global configuration menu. The profiles for negotiating multihop sessions are also defined here. Any authentication and session negotiation parameters that you wish to use are defined in these profiles. You can also specify the source/destination address pairs that define a multihop session, assigning them the profile desired for the session. In order to access the BFD protocol configuration, you must run the following sequence of commands in the device's configuration console:

```
*config
Config>protocol BFD
-- Bidirectional Forwarding Detection user configuration --
BFD config>
```

You can also gain access through the dynamic configuration menu:

```
*running-config
Config$protocol BFD
-- Bidirectional Forwarding Detection user configuration --
BFD config$
```

The configuration commands available in the BFD protocol configuration menu are as follows:

```
BFD config$?
  enable     Enable BFD protocol
  list       List BFD configuration
  no         Negate a command or set its defaults
  profile    BFD profile configuration
  session    BFD multihop session configuration
  exit
BFD config$
```

Command	Function
? (HELP)	Displays the available commands or options.
ENABLE	Enables the BFD protocol in the router.
LIST	Displays the current configuration for the BFD protocol.
NO	Configures the default value for a given option that disables parameters or deletes previously added configuration elements.
PROFILE	Allows you to define a profile with the BFD negotiation and authentication para-

	meters.
SESSION	Configures a multihop BFD session defined by the source/destination address pairs and the profile that defines the BFD negotiation and authentication parameters.
EXIT	Exits the BFD protocol configuration.

Note

If you use the dynamic configuration menu, the first thing to do when configuring the BFD protocol is to enable it by executing the **ENABLE** command. Subsequently, you need to configure the parameters for each session and the sessions.

2.2.1 ENABLE

The **ENABLE** command allows you to enable the BFD protocol. When configuring BFD sessions in a router, this is the first command you need to enter. This enables the protocol to start up so everything is ready to establish BFD sessions. By default, the BFD protocol is disabled.

Syntax:

```
BFD config$enable
```

2.2.2 NO ENABLE

The **NO ENABLE** command allows you to disable the BFD protocol. By default the BFD protocol is disabled.

Syntax:

```
BFD config$no enable
```

2.2.3 PROFILE

The **PROFILE** command lets you specify negotiation and authentication parameters to be used in multihop BFD sessions. A profile can be assigned to various multihop sessions, allowing you to save configuration lines.

Syntax:

```
BFD config$profile <name> min-tx <min-tx-value> min-rx <min-rx-value> mult
<multiplier> [md5|met-md5|sha1|met-sha1 key-chain|key-string <string>]
```

Parameter	**Definition**
<name>	A word between 1 and 15 characters in length that defines the profile name.
<min-tx-value>	Value between 50 and 999 milliseconds that establishes the desired minimum transmit interval.
<min-rx-value>	Value between 1 and 999 milliseconds that establishes the required minimum receive interval.
<multiplier>	Value between 3 and 50 that establishes the multiplier used to calculate the detection time.
<string>	A word between 1 and 20 characters for the key-string option and between 1 and 16 characters for the key-chain option. Establishes the key that will be used for authentication in the key-string option; establishes the Key Chain name that will be used for authentication in the key-chain option.

Note

Keyed MD5 and Meticulous Keyed MD5 authentication types support key lengths of between 1 and 16 characters. Keyed SHA1 and Meticulous Keyed SHA1 authentication types support key lengths of between 1 and 20 characters.

Example:

```
BFD config$profile sampleprof min-tx 600 min-rx 750 mult 10 sha1 key-string samplekeyword
```

2.2.4 NO PROFILE

The **NO PROFILE** command deletes the configuration of a profile identified by its profile name.

Note

When deleting a BFD profile, all BFD sessions assigned that profile will be automatically deleted.

Syntax:

```
BFD config$no profile <name>
```

Example:

```
BFD config$no profile sampleprof
```

2.2.5 SESSION

The **SESSION** command lets you configure a multihop BFD session defined by the source/destination address pairs and the BFD profile that you want to assign to the session.

Syntax:

```
BFD config$session src <source-ip> dst <destination-ip> <profile-name>
```

Parameter	Definition
<source-ip>	The session's IPv4 or IPv6 source address.
<destination-ip>	The session's IPv4 or IPv6 destination address, commonly known as peer address.
<name>	Word between 1 and 15 characters that defines the profile name assigned to this session.

Example 1:

```
BFD config$session src 192.168.1.1 dst 172.24.1.1 sampleprof
```

Example 2:

```
BFD config$session src 2001:db8::1000:2 dst 1001:db8:2000:4 test_profile
```

Command history:

Release	Modification
11.01.04	IPv6-compatible option added as of version 11.01.04

2.2.6 NO SESSION

The **NO SESSION** command allows you to delete a multihop BFD session defined by the source/destination address pairs and the BFD profile assigned to the session.

Syntax:

```
BFD config$no session src <source-ip> dst <destination-ip> <profile-name>
```

Parameter	Definition
<source-ip>	The session's IPv4 or IPv6 source address.
<destination-ip>	The session's IPv4 or IPv6 destination address, commonly known as peer address.
<name>	Word between 1 and 15 characters that defines the name of the profile assigned to this session.

Example 1:

```
BFD config$no session src 192.168.1.1 dst 172.24.1.1 sampleprof
```

Example 2:

```
BFD config$no session src 2001:db8::1000:2 dst 1001:db8:2000:4 test_profile
```

Command history:

Release	Modification
11.01.04	IPv6-compatible option added as of version 11.01.04

2.3 Configuring the parameters for a BFD session

The single hop BFD session parameters are configured in the configuration menu for the interface through which you are going to establish the BFD session. To access the configuration menu for an interface, you need enter the following sequence of commands from the router's console root menu. We are going to use the ethernet0/0 interface as an example:

```
*config
Config>network ethernet0/0
-- Ethernet Interface User Configuration --
ethernet0/0 config>
```

You can also gain access through the dynamic configuration menu:

```
*running-config
Config$network ethernet0/0
-- Ethernet Interface User Configuration --
ethernet0/0 config$
```

The configuration commands relative to the BFD protocol available in the configuration menu for an interface are preceded by the word bfd and are as follows:

```
ethernet0/0 config$?
  bfd             Interface Bidirectional Forwarding Detection config commands
  description     Enter interface description
  ip              Interface Internet Protocol config commands
  no              Negate a command or set its defaults
  shutdown        Change state to administratively down
  update          Update a level indicator
  exit
ethernet0/0 config$bfd ?
  interval        Set desired minimum transmit interval
  list            List BFD configuration
  min-rx          Set required minimum receive interval
  multiplier      Set desired detect time multiplier
  version         Set desired BFD protocol version

ethernet0/0 config$
```

Command	Function
? (HELP)	Displays the available commands or options.
INTERVAL	Establishes the minimum required transmission interval.
LIST	Displays the current configuration for the BFD protocol parameters.
MIN-RX	Establishes the minimum reception interval supported.
MULTIPLIER	Establishes the multiplier in order to calculate the detection time.
VERSION	Allows you to configure the BFD protocol version.

Note

The interfaces currently supported by BFD are those where IP configuration is supported.

2.3.1 BFD INTERVAL

The **BFE INTERVAL** command defines the minimum timer period wanted for packet transmission. It indicates the minimum time the device needs to transmit BFD packets. This must be configured bearing in mind the device load and the number of BFD sessions it needs to support, so the BFD protocol does not involve a load that affects the performance of the rest of the protocols. The value entered must be in milliseconds and the default value is 100 milliseconds. The value entered must be between 50 and 999 milliseconds.

Syntax:

```
ethernet0/0 config$bfd interval ?
  <50..999>    milliseconds
ethernet0/0 config$
```

Example:

```
ethernet0/0 config$bfd interval 200
ethernet0/0 config$
```

2.3.2 BFD MIN-RX

The **BFD MIN-RX** command defines the minimum timer period supported for packet reception. This time indicates the minimum time during which the device can receive BFD packets. This must be configured bearing in mind the device load and the number of BFD sessions it needs to support, so the device can deal with all the received BFD packets and so link drops which have not occurred are not detected. The value entered must be in milliseconds and is 50 by default. The value entered must be between 1 and 999 milliseconds.

Syntax:

```
ethernet0/0 config$bfd min-rx ?
  <1..999>    milliseconds
ethernet0/0 config$
```

Example:

```
ethernet0/0 config$bfd min-rx 70
ethernet0/0 config$
```

2.3.3 BFD MULTIPLIER

The **BFD MULTIPLIER** command defines the multiplier value used when calculating the detection time. This value represents the number of consecutive packets that have to be lost in order to assume the BFD session is down. Default value is 3 and the entered value must be between 3 and 50.

Syntax:

```
ethernet0/0 config$bfd multiplier ?
  <3..50>    multiplier
ethernet0/0 config$
```

Example:

```
ethernet0/0 config$bfd multiplier 5
ethernet0/0 config$
```

2.3.4 BFD VERSION

The **BFD VERSION** command allows you to configure the device to operate with BFD protocol version 0. By default the device operates BFD protocol version 1, although this mode allows you to establish sessions with devices that only support version 0.

If the device is configured to operate with BFD version 1, the device will try and establish sessions with the highest version supported by the remote device. If the remote device begins transmitting packets in the 0 version, the local device establishes the session with version 0. If the former begins to transmit packets using version 1, then the local device establishes the session with version 1.

In a scenario where you previously needed to operate in version 0 and you configure the device through the **BFD VERSON 0** command, if you wish to migrate to version 1 in the future, you need to execute the **BFD VERSION 1**, disable the sessions administratively and re-enable them once you've passed to version 1.

Syntax:

```
ethernet0/0 config$bfd version ?
  <0..1>    protocol version
ethernet0/0 config$
```

Example:

```
ethernet0/0 config$bfd version 0
ethernet0/0 config$
```

2.3.5 BFD LIST

The **BFD LIST** command displays the current BFD parameters configuration for the interface, including the default values.

Syntax:

```
ethernet0/0 config$bfd list
```

Example:

```
ethernet0/0 config$bfd list
BFD version: 0
Minimun desired transmit interval: 200 ms
Minimun required receive interval: 70 ms
Detect time multiplier: 5
ethernet0/0 config$
```

2.4 Configuring BFD in the BGP protocol

In the Border Gateway Protocol (BGP) configuration menu, you can register a BGP peer in a BDF session. This way, the BFD session informs the BGP protocol of any event occurring in the BFD session.

It is in the configuration menu for a BGP group where you can associate a BGP peer to a BFD session. The command is a modifier for the **PEER** command and is known as **BFD-SESSION**. By executing this command, a BFD session is created (if it did not previously exist) as soon as BGP communications are established with the *peer*. If the session already exists, the BGP protocol registers in it. In cases where an existing BFD session stops having registered protocols, it stops existing as it is no longer necessary.

To access this menu, follow the steps shown in the following example. The BGP autonomous system number (peer-as 100) is an example. It must be the specific autonomous system for the group you wish to configure, just like the peer IP address (*172.24.80.12*):

```
*config
Config>protocol bgp
-- Border Gateway Protocol user configuration --
BGP config>group type external peer-as 100
-- BGP group configuration --
BGP config>peer 172.24.80.12
BGP config>peer 172.24.80.12 ?
  anal-retentive         Warn when receiving questionable BGP updates
  gateway                Next hop router for received routes
  hold-time              BGP holdtime value to use when negotiating the connection
  ignore-first-as-hop    Allow routes from route servers that don't prepend their own ashop
  in-delay               Amount of time a learned route must be stable before accepting it
  in-route-map           Configure inbound route-map associated to this neighbor
  keep                   Learned routes to be retained
  keepalives-always      Always send keepalives
  local-addr             Address to be used on the local end of the TCP connection
  local-as               Local autonomous system
  log-up-down            Log BGP peers entering or leaving the ESTABLISHED state
  metric-out             Primary metric for sent routes
  next-hop-self          Disable the next hop calculation for this neighbor
  no-aggregator-id       Specify the routerid in the aggregator attribute as zero
  no-auth-check          Do not check authentication field
  no-shared-interface    Allow connections to not directly connected peers
  no-v4-as-loop          Prevent routes with looped AS paths from being
                         advertised to version 4 external peers
```

```
  out-delay              Amount of time a route must be present in the routing
                         database before exporting it
  out-route-map          Set outbound route-map associated to this neighbor
  passive                Do not attempt active OPENs
  preference             Preference used for learned routes
  preference2            Tie breaker in the case of a preference tie
  recv-buffer            Receive buffering
  remove-private-as      Remove private as numbers from updates
  route-to-peer          Allow routing to directly peers
  send-buffer            Send buffering
  send-community         Send communities attribute to this peer
  set-pref               Set preference from/to localpref
  ttl                    Time to Live to be used on TCP connection
  v3-as-loop-okay        Advertise routes whose AS path is looped to version 3  external peers

 bfd-session             Register the peer in a BFD session

  <cr>
BGP config> peer 172.24.80.12 bfd-session

BGP config>
```

You can also access through the dynamic configuration menu.

```
*running-config
Config$protocol bgp
-- Border Gateway Protocol user configuration --
BGP config$group type external peer-as 100
-- BGP group configuration --
BGP config$peer 172.24.80.12
BGP config$peer 172.24.80.12 bfd-session

BGP config$
```

To deregister the peer in the BFD session BGP protocol, simply execute the same command preceded by the command **NO** (as shown in the following example).

```
BGP config>no peer 172.24.80.12 ?
  anal-retentive         Warn when receiving questionable BGP updates
  gateway                Next hop router for received routes
  hold-time              BGP holdtime value to use when negotiating the connection
  ignore-first-as-hop    Allow routes from route servers that don't prepend
                         their own ashop
  in-delay               Amount of time a learned route must be stable before accepting it
  in-route-map           Configure inbound route-map for this neighbor
  keep                   Learned routes to be retained
  keepalives-always      Always send keepalives
  local-addr             Address to be used on the local end of the TCP connection
  local-as               Local autonomous system
  log-up-down            Log BGP peers entering or leaving the ESTABLISHED state
  metric-out             Primary metric for sent routes
  next-hop-self          Disable the next hop calculation for this neighbor
  no-aggregator-id       Specify the routerid in the aggregator attribute as zero
  no-auth-check          Do not check authentication field
  no-shared-interface    Allow connections to not directly connected peers
  no-v4-as-loop          Prevent routes with looped AS paths from being
                         advertised to version 4 external peers
  out-delay              Amount of time a route must be present in the routing
                         database before exporting it
  out-route-map          Configure outbound route-map for this neighbor
  passive                Do not attempt active OPENs
  preference             Preference used for learned routes
  preference2            Tie breaker in the case of a preference tie
  recv-buffer            Receive buffering
  remove-private-as      Remove private as numbers from updates
  route-to-peer          Allow routing to directly peers
  send-buffer            Send buffering
  send-community         Disable the community attribute for outgoing routes
```

```
  set-pref               Set preference from/to localpref
  ttl                    Time to Live to be used on TCP connection
  v3-as-loop-okay        Advertise routes whose AS path is looped to version 3 external peers
  bfd-session            Unregister the peer from a BFD session
  <cr>
BGP config>no peer 172.24.80.12 bfd-session

BGP config>
```

2.5 Configuring BFD in the NSM feature

We are now going to explain how to configure the NSM feature (Network Service Monitor) to monitor the status of a line connection through a BFD session.

We define the BFD protocol as a new type of NSM feature operation. Within this type of BFD operation we define two subtypes: asynchronous and demand. These two subtypes correspond to the BFD protocol's *Asynchronous* and *Demand* modes. The BFD session establishes according to the mode defined in the NSM operation configuration.

Here you can see how to access the NSM feature configuration menu and how to create a BFD operation:

```
*config
Config$feature nsm
-- Network Service Monitor configuration --
NSM config>operation 1
-- NSM Operation configuration --
NSM operation 1>
```

In the operation menu you can see the commands that take effect when configuring the type of BFD operation in the NSM feature:

```
NSM operation 1>

   bfd-interval         BFD desired transmission interval
   bfd-min-rx           BFD minimum required reception interval
   bfd-multiplier       BFD detect multiplier
   frequency            Frequency of the operation
   interval             Inter-packet interval
   list                 Show operation parameters
   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
NSM operation 1>
```

Below, you will find a brief description of the commands that affect the BFD configuration and the NSM operation. For further information on the rest of the commands and any other details on the NSM feature, please see the manual on the NSM feature Teldat- *Dm749-I*.

Command	**Function**
? (HELP)	Displays the available commands or their options.
BFD-INTERVAL	Establishes the minimum transmission period required for BFD.
BFD-MIN-RX	Establishes the minimum reception period supported for BFD.
BFD-MULTIPLIER	Establishes the multiplier to calculate the detection time for BFD.
FREQUENCY	Sets the frequency for the poll cycles for a BFD session executed in Demand mode.
LIST	Displays the current configuration for the NSM operation.
SOURCE-IPADDR	Establishes the source address for the BFD session.
TIMEOUT	Establishes the poll cycles timeout for a BFD operation in Demand mode.
TYPE	Establishes the type of NSM operation and the destination IP address for the BFD session.

EXIT	Exits the BFD protocol configuration.

Note

If the NSM feature creates the BFD session, and if it is a single hop BFD session, the BFD session parameters are obtained from the NSM operation configuration and the parameters configured in the interface through which the BFD session is established are ignored.

Note

If a multihop session is defined for the source/destination address pairs of the NSM operation, the session parameters used in the negotiation will be those defined in the profile assigned to the multihop session.

2.5.1 BFD-INTERVAL

The **BFD-INTERVAL** command establishes the minimum period for BFD packet transmission supported by the device. This value prevails over the value configured in the interface over which the BFD session is established if the NSM feature created the session (i.e. if the BFD session had not been previously created by any other protocol). The default value for the minimum interval for the BFD packet transmission is 100 milliseconds. The value entered 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>
```

2.5.2 BFD-MIN-RX

The **BFD-MIN-RX** command establishes the BFD packet reception minimum period supported by the device. The value prevails over that configured on the interface over which the BFD session is established if the NSM feature created the session (i.e. if the BFD session had not been previously created by a different protocol). The default value for the BFD packet reception minimum interval is 50 milliseconds. The value entered 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>
```

2.5.3 BFD-MULTIPLIER

The **BFD-MULTIPLIER** establishes the detection multiplier used to calculate the BFD session detection time. Basically, this is the number of consecutive BFD packets that must be lost before considering the BFD session as down. The value prevails over that configured on the interface over which the BFD session is established if the NSM feature created the session (i.e. if the BFD session had not been previously created by a different protocol). The default value for the detection multiplier is 3. The introduced 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>
```

2.5.4 FREQUENCY

In cases of configuring a BFD operation in *Demand* mode, the **FREQUENCY** command establishes the frequency the BFD session poll cycles are executed. This command has no effect for BFD operations in *Asynchronous* mode. The default value for the poll cycle frequency is 60 seconds. The value entered must be between 1 and 604.800 seconds.

Syntax:

```
NSM operation 1>frequency ?
  <1..604800>    Frequency (in seconds)
NSM operation 1>
```

Example:

```
NSM operation 1>frequency 5
NSM operation 1>
```

2.5.5 LIST

The **LIST** command displays the current configuration of the operation including the default values for the non-configured parameters. Depending on the type of operation, only the values that prove useful for said operation appear. We're going to see two examples; example 1 displays the configuration of a BFD operation in *Asynchronous* mode and example 2, a BFD operation in *Demand* mode.

Syntax:

```
NSM operation 1>list
```

Example 1:

```
NSM operation 1>list

Operation ID Number: 1
--------------------
Type of Operation to Perform: bfd
Protocol Type: bfdAsync

Target Address [Port]: 172.24.80.12 [0]
Source Address [Port]: 172.24.80.10 [0]
Life (seconds): forever (never ends)
Operation Ageout (seconds): 3600
Owner:
BFD Desired Min Tx interval (ms): 200
BFD Required Min Rx interval (ms): 100
BFD Detect Multiplier: 5

NSM operation 1>
```

Example 2:

```
NSM operation 1>list

Operation ID Number: 1
--------------------
Type of Operation to Perform: bfd
Frequency (seconds): 5
Timeout (ms): 2000
Protocol Type: bfdDemand
Target Address [Port]: 172.24.80.12 [0]
Source Address [Port]: 172.24.80.10 [0]
Life (seconds): forever (never ends)
Operation Ageout (seconds): 3600
Owner:
BFD Desired Min Tx interval (ms): 200
BFD Required Min Rx interval (ms): 100
BFD Detect Multiplier: 5
```

```
NSM operation 1>
```

2.5.6 SOURCE-IPADDR

The **SOURCE-IPADDR** command specifies the source IP address for the BFD session. Some of the device interfaces have to be configured with this IP address so that the BFD session can establish over this interface.

Syntax:

```
NSM operation 1>source-ipaddr ?
  <a.b.c.d>    Source IP address
NSM operation 1>
```

Example:

```
NSM operation 1>source ipaddr 172.24.80.10
NSM operation 1>
```

2.5.7 TIMEOUT

The **TIMEOUT** command, in cases where you are configuring a BFD NSM operation in *Demand* mode, establishes the time the operation takes to finish (i.e. a poll cycle for the BFD in *Demand* mode). By default, this value is 5.000 milliseconds (5 seconds). You must configure a value that is below the frequency value over which the poll cycles are executed, entered through the **FREQUENCY** command. The optimum value should be slightly above the one it takes to execute a BFD poll cycle, which in the worst case is the BFD detection time for the *Demand* mode. The value should be between 1000 and 604.800.000 milliseconds.

Syntax:

```
NSM operation 1>timeout ?
  <1000..604800000>    Timeout (in milliseconds)
NSM operation 1>
```

Example:

```
NSM operation 1>timeout 2000
NSM operation 1>
```

2.5.8 TYPE

Here we are going to describe the **TYPE** command for cases involving BFD operation configuration.

Syntax:

```
NSM operation 1>type ?
  echo      Echo operation
  http      HTTP operation
  jitter    Jitter operation
  bfd       Bidirectional Forwarding Detection operation

NSM operation 1>type bfd ?
  demand-mode BFD Demand Mode
  async-mode  BFD Asynchronous Mode

NSM operation 1>
```

There are two modes in which we can configure BFD for the NSM monitoring operation: *Asynchronous* and *Demand.*

2.5.8.1 DEMAND MODE

In *Demand* mode, the BFD protocol only sends control packets to check the status of the line whenever a poll cycle is carried out. Poll cycles are executed at the frequency configured with the **FREQUENCY** command in the NSM operation configuration.

On entering the **TYPE** command and the type of BFD operation, the selected BFD mode is followed by the destination IP address for the BFD session. In the case of single hop BFD sessions, the destination IP address must be visible and directly connected to the interface corresponding to the IP address entered with 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>
```

2.5.8.2 ASYNC-MODE

In *Asynchronous* mode, the BFD protocol continuously sends control packets at the same pace indicated by the transmission time negotiated when establishing the BFD session. A drop is detected when the detection time has timed out without having received a packet from the remote end.

On entering the **TYPE** command, the selected BFD mode is followed by the destination IP address for the BFD session. In the case of single hop BFD sessions, the destination IP address must be visible and directly connected to the interface corresponding to the IP address entered with 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>
```

2.6 NSLA recommended configuration for BFD NSM

We are going to establish a configuration recommended for the NSLA feature (Network Service Level Advisor) when using information received from a BFD NSM operation.

You need to bear in mind that the BFD session only communicates two states, UP or DOWN, if the link monitoring the BFD is up or down. Consequently, you need to set the activation and deactivation threshold to 0 and the significant number of samples to 1. The activation and deactivation sensitivity is set at 100% so that every time an event occurs, an alarm is generated. You have a free hand when it comes to selecting the establishment times.

Below, you can see how to access the NSLA feature menu:

```
*config
Config>feature nsla
-- Feature Network Service Level Advisor --
NSLA config>
```

A NSLA feature configuration example for a BFD NSM operation:

```
NSLA config>show config
; Showing Menu and Submenus Configuration for access-level 15 ...
        enable
;
        filter 1 nsm-op 1 bfd
        filter 1 significant-samples 1
        filter 1 activation threshold 0
        filter 1 activation sensibility 100
        filter 1 activation stabilization-time 5
        filter 1 deactivation threshold 0
        filter 1 deactivation sensibility 100
        filter 1 deactivation stabilization-time 5
;
      alarm 1 filter-id 1
;
      advisor 1 alarm-id 1
;
NSLA config>
```

Chapter 3 Monitoring the BFD Protocol

3.1 BFD Monitoring Menu Commands

The BFD protocol has its own monitoring menu and, in cases where NSM is used with a BFD operation, you can check some BFD statistics associated with the NSM operation through the NSM monitoring menu.

We are now going to see how to access the BFD protocol monitoring menu:

```
*monitor
+protocol bfd
-- BFD Protocol Monitor --
BFD+
```

The following commands are available in the BFD protocol monitoring menu.

```
BFD+
  clear      Clear BFD session statistics
  disable    Disable BFD sessions
  enable     Enable BFD sessions
  list       Show BFD session statistics
  stop       Stop and delete BFD sessions
  vrf        Enter BFD VRF monitor
  exit
BFD+
```

What follows is a brief description of each command:

Command	Function
? (HELP)	Displays the commands or available options.
CLEAR	Allows you to initialize the statistics for one or all the BFD sessions.
DISABLE	Allows you to administratively disable one or all the BFD sessions.
ENABLE	Administratively enables one or all the BFD sessions.
LIST	Shows statistics for the BFD sessions. These can be presented either as abbreviated or in detail for one or all sessions.
STOP	Allows you to stop one or all the BFD sessions. The sessions are eliminated and no longer exist in the device.
VRF	Enters the BFD monitor menu of a VRF.
EXIT	Exits the BFD protocol monitoring menu.

3.1.1 CLEAR

The **CLEAR** command allows you to initialize the statistics for one or all the BFD session in the device. On executing this, all counters on sent and received packets are switched to zero (together with the packet reception and transmission times and the counter for down sessions detected).

There are two options for the **CLEAR** command:

```
BFD+clear ?
  all     Clear statistics of all BFD sessions
  peer    Clear statistics of the BFD session with the peer
BFD+
```

3.1.1.1 CLEAR ALL

The **CLEAR ALL** command allows you to initialize the statistics for all the BFD sessions present in the device.

Example:

```
BFD+clear all
BFD+
```

3.1.1.2 CLEAR PEER

The **CLEAR PEER** command allows you to initialize the statistics for a determined session. The session is identified through the remote device IP address.

Syntax:

```
BFD+clear peer ?
  <a.b.c.d>    Ipv4 format
  <a::b>       Ipv6 address
BFD+
```

Example:

```
BFD+clear peer 172.24.80.12
BFD+
```

Command history:

Release	Modification
11.01.04	Support for BGP IPv6 peers was introduced as of version 11.01.04

3.1.2 DISABLE

The **DISABLE** command allows you to administratively disable one or all the device BFD sessions. The administratively disabled session continues to send BFD packets but the session is down. This mode can be used to check that the BFD protocol is operating, without needing to stop the data link, by disabling the session at one end and checking that the other end has detected it is down.

There are two options for the **DISABLE** command:

```
BFD+disable ?
  all     Disable all BFD sessions
  peer    Disable the BFD session with the peer
BFD+
```

3.1.2.1 DISABLE ALL

The **DISABLE ALL** command administratively disables all the device BFD sessions (i.e. puts them in ADMINDOWN state) .

Example:

```
BFD+disable all
BFD+
```

3.1.2.2 DISABLE PEER

The **DISABLE PEER** command disables a specific session identified by the remote device IP address with which the BFD session is established.

Syntax:

```
BFD+disable peer ?
  <a.b.c.d>    Ipv4 format
  <a::b>       Ipv6 address
BFD+
```

Example:

```
BFD+disable peer 172.24.80.12
BFD+
```

Command history:

Release	Modification
11.01.04	Support for BGP IPv6 peers was introduced as of version 11.01.04

3.1.3 ENABLE

The **ENABLE** command allows you to administratively enable one or all the device BFD sessions. Only sessions that are administratively disabled are affected by this command.

There are two options for the ENABLE command:

```
BFD+enable ?
  all     Enable all BFD sessions
  peer    Enable the BFD session with the peer
BFD+
```

3.1.3.1 ENABLE ALL

The **ENABLE ALL** command administratively enables (removes from the ADMINDOWN state) all the device BFD sessions that are administratively disabled.

Example:

```
BFD+enable all
BFD+
```

3.1.3.2 ENABLE PEER

The **ENABLE PEER** command administratively enables a specific session identified by the remote IP address of the device used to establish the BFD session. For this command to take effect, the session must have been administratively disabled previously.

Syntax:

```
BFD+enable peer ?
  <a.b.c.d>    Ipv4 format
  <a::b>       Ipv6 address
BFD+
```

Example:

```
BFD+enable peer 172.24.80.12
BFD+
```

Command history:

Release	Modification
11.01.04	Support for BGP IPv6 peers was introduced as of version 11.01.04

3.1.4 LIST

The **LIST** command displays all the BFD session statistics present in the device. You can list a summary of all the sessions in a table or display one or all of the existing sessions in detail.

There are various options for the **LIST** command:

```
BFD+list ?
  all        Show all sessions detailed statistics
  peer       Show detailed statistics of the session with the peer
  summary    Show a summary of all sessions
BFD+
```

3.1.4.1 LIST ALL

The **LIST ALL** command displays the statistics for all the device BFD sessions in detail.

Syntax:

```
BFD+list all
```

Example:

```
BFD+list all
```

```
    MyDisc: 0x688a5826  ReDisc: 0x94d1dde1
    Myaddr: 172.24.80.10  Peer: 172.24.80.12  Infc: ethernet0/0
    State: Up    Uptime: 17s    Created: 3m 45s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM BGP
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled
    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms   XmtTime: 50 ms   DetectTime: 150 ms
    Xmtpkts: 421    Last Tx interval: 46ms  min/max/avg: 38ms/46ms/42ms
    Rcvpkts: 420    Last Rx interval: 45ms  min/max/avg: 37ms/47ms/42ms
    MyDisc: 0xbc27ef2c  ReDisc: 0x23708d77
    Myaddr: 10.10.44.200  Peer: 10.10.44.205  Infc: ethernet0/1
    State: Up    Uptime: 7s    Created: 3m 45s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM BGP
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled
    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms   XmtTime: 50 ms   DetectTime: 150 ms
    Xmtpkts: 178    Last Tx interval: 43ms  min/max/avg: 38ms/46ms/42ms
    Rcvpkts: 178    Last Rx interval: 46ms  min/max/avg: 37ms/47ms/42ms

BFD+
```

The meaning of each section is as follows:

3.1.4.1.1 MyDisc

(My Discriminator): This is the session's local identifier. The session is identified in the device through this value.

3.1.4.1.2 ReDisc

(Remote Discriminator): This is the session's remote identifier. The session in the remote device is identified with this value.

3.1.4.1.3 Myaddr

Local interface IP address through which the BFD session is established.

3.1.4.1.4 Peer

Remote device interface IP address through which the BFD session is established.

3.1.4.1.5 Infc

Name of the local interface through which the BFD session is established with the remote device. *Multihop session* will appear in the case of multihop sessions, as they are not assigned to any interface.

3.1.4.1.6 State

Current status of the BFD session in the local device.

3.1.4.1.7 Uptime

Indicates the time the session has been in an UP state; this is 0 seconds if it's not UP.

3.1.4.1.8 Created

Indicates the time elapsed since the session was created.

3.1.4.1.9 Falls detected

This is the number of falls in the BFD session since it was created or since the last time the statistics were restarted.

3.1.4.1.10 Diag code

(Diagnostic code): Indicates the cause of the last BFD session fall detected in the local device.

3.1.4.1.11 Registered protocols

List of the protocols registered in the BFD session. All registered protocols are notified of any event generated in a session.

3.1.4.1.12 BFD version

This is the BFD protocol version number with which the session is operating. There are currently only two versions: 0 and 1.

3.1.4.1.13 Demand mode

This shows if the *Demand* mode is active for the session.

3.1.4.1.14 Authentication Type

Displays the type of authentication used in the session or *Disabled* if authentication is not enabled.

3.1.4.1.15 MinTx

(Minimum desired transmission interval): This is the minimum transmission interval configured in the local device.

3.1.4.1.16 MinRx

(Minimum required reception interval): This is the minimum reception interval supported by the local device you have configured.

3.1.4.1.17 Mult

(Detect multiplier): This is the detection multiplier used by the device to calculate the detection time. This shows the value configured in the local device.

3.1.4.1.18 ActiveMinTx

(Active minimum desired transmission interval): This is the value for the minimum desired transmission interval being used by the device. Before the timers' negotiation, and while the session is down, the ActiveMinTx value is different to the MinTx value and is 1000 milliseconds.

3.1.4.1.19 XmtTime

(Transmit Time): This is the transmission interval negotiated with the remote device. It is the time it takes the remote device to send BFD control packets in *Asynchronous* mode.

3.1.4.1.20 DetectTime

Detection time negotiated with the remote device. This is the maximum time the device waits without receiving packets before it assumes the BFD session is down.

3.1.4.1.21 Xmtpkts

(Transmitted packets): Number of transmitted packets since the BFD session was established or since the statistics were last restarted. This value initializes when the session switches to an UP state.

3.1.4.1.22 Last Tx Interval

Transmission interval for the last transmitted packet and the minimum, maximum and average values of this value for the total number of transmitted packets (Xmtpkts).

3.1.4.1.23 Rcvpkts

(Received packets): Number of packets received since the BFD session was established or since the the statistics were last restarted. This value initializes when the session switches to an UP state.

3.1.4.1.24 Last Rx Interval

Reception interval for the last received packet and the minimum, maximum and average values of this value for the total number of received packets (Rcvpkts).

3.1.4.2 LIST PEER

Displays detailed statistics for a specific session identified by the remote device IP address with which the BFD session was established.

Syntax:

```
BFD+list peer ?
  <a.b.c.d>    Ipv4 format
  <a::b>       Ipv6 address
BFD+
```

Example:

```
BFD+list peer 172.24.80.12
    MyDisc: 0x688a5826  ReDisc: 0x94d1dde1
    Myaddr: 172.24.80.10  Peer: 172.24.80.12  Infc: ethernet0/0
    State: Up    Uptime: 2m 27s    Created: 5m 55s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM BGP
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled
    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms   XmtTime: 50 ms   DetectTime: 150 ms
    Xmtpkts: 3457    Last Tx interval: 42ms  min/max/avg: 38ms/48ms/41ms
    Rcvpkts: 3456    Last Rx interval: 43ms  min/max/avg: 37ms/47ms/41ms
BFD+
```

Command history:

Release	Modification
11.01.04	Support for BGP IPv6 peers was introduced as of version 11.01.04

3.1.4.3 LIST SUMMARY

Displays a summary in table format of all the BFD sessions that are in the device. The most relevant data for each BFD session appears in this table.

Syntax:

```
BFD+list summary
```

Example:

```
BFD+list summary

MyDisc      ReDisc      MyIP          Peer          State  XmtTime  DetectTime  Falls  Uptime
-------------------------------------------------------------------------------------------
0x688a5826  0x94d1dde1  172.24.80.10  172.24.80.12  Up     50   ms  150  ms     0      4m 42s
0xbc27ef2c  0x23708d77  10.10.44.200  10.10.44.205  Up     50   ms  150  ms     0      4m 31s
BFD+
```

3.1.5 STOP

Allows you to stop and delete a specific BFD session from the device or all the BFD sessions that are in the device.

There are two options for the **STOP** command:

```
BFD+stop ?
  all     Stop and delete all BFD sessions
  peer    Stop and delete the BFD session with the peer
BFD+
```

3.1.5.1 STOP ALL

Stops and deletes all the BFD sessions present in the device. Consequently, sessions do not generate any further events in any of the protocols that were registered in them

Example:

```
BFD+stop all
BFD+
```

3.1.5.2 STOP PEER

Stops and deletes a specific BFD session identified by the remote device IP address with which the BFD session was established. If there no session with a remote device interface has the IP address entered, the command returns an error message.

Syntax:

```
BFD+stop peer ?
  <a.b.c.d>    Ipv4 format
  <a::b>       Ipv6 address
BFD+
```

Example:

```
BFD+stop peer 172.24.80.12
BFD+
```

Command history:

Release	Modification
11.01.04	Support for BGP IPv6 peers was introduced as of version 11.01.04

3.1.6 VRF

This option allows you to access the monitor menu of the BFD sessions that belong to a VRF by entering the VRF identifier after the **VRF** command. The menu is the same as the root BFD monitor menu, but the **VRF** option is not present.

Example:

```
BFD+vrf ?
  <1..32 chars>    VPN Routing/Forwarding instance name
BFD+vrf MXONE



BFD vrf+
BFD vrf+?
  clear      Clear BFD session statistics
  disable    Disable BFD sessions
  enable     Enable BFD sessions
  list       Show BFD session statistics
  stop       Stop and delete BFD sessions
  exit
BFD vrf+
```

Command history:

Release	Modification
11.01.04	This command was introduced as of version 11.01.04

Chapter 4 BFD Configuration Examples

4.1 Configuration example for BFD with NSM and NSLA

Below, you will see a configuration example between two Atlas 250 devices connected to two different networks through their Ethernet0/0 and Ethernet0/1 interfaces.

Device: PRUEBAS-BFD-1:

```
; Showing System Configuration for access-level 15 ...

log-command-errors
no configuration
set hostname PRUEBAS-BFD-1
;
network ethernet0/0
; -- Ethernet Interface User Configuration --
   ip address 172.24.80.10 255.255.0.0
;
exit
;
;
network ethernet0/1
; -- Ethernet Interface User Configuration --
   ip address 10.10.44.200 255.255.255.0
;
exit
;
;
protocol bfd
; -- Bidirectional Forwarding Detection user configuration --
  enable
exit
;
protocol ip
; -- Internet protocol user configuration --
   router-id 172.24.80.10
;
   route 0.0.0.0 0.0.0.0 172.24.0.98
;
   classless
;
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
;
feature nsla
; -- Feature Network Service Level Advisor --
   enable
;
   filter 1 nsm-op 1 bfd
   filter 1 significant-samples 1
   filter 1 activation threshold 0
   filter 1 activation sensibility 100
   filter 1 activation stabilization-time 5
   filter 1 deactivation threshold 0
   filter 1 deactivation sensibility 100
   filter 1 deactivation stabilization-time 5
;
   filter 2 nsm-op 2 bfd
   filter 2 significant-samples 1
   filter 2 activation threshold 0
   filter 2 activation sensibility 100
   filter 2 activation stabilization-time 5
   filter 2 deactivation threshold 0
   filter 2 deactivation sensibility 100
   filter 2 deactivation stabilization-time 5
;
   alarm 1 filter-id 1
;
   alarm 2 filter-id 2
;
   advisor 1 alarm-id 1
;
   advisor 2 alarm-id 2
;
exit
;
dump-command-errors
end
; --- end ---
```

Device: PRUEBAS-BFD-3:

```
; Showing System Configuration for access-level 15 ...

log-command-errors
no configuration
set hostname PRUEBAS-BFD-3
;
network ethernet0/0
; -- Ethernet Interface User Configuration --
   ip address 172.24.80.12 255.255.0.0
;
exit
;
;
network ethernet0/1
; -- Ethernet Interface User Configuration --
   ip address 10.10.44.205 255.255.255.0
;
exit
;
;
protocol bfd
; -- Bidirectional Forwarding Detection user configuration --
   enable
exit
;
protocol ip
; -- Internet protocol user configuration --
```

```
   router-id 172.24.80.12
;
   route 0.0.0.0 0.0.0.0 172.24.0.6
;
   classless
;
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
;
dump-command-errors
end
; --- end ---
```

Once the two sessions are established, everything we can see under the monitoring lists in the PRUEBAS-BFD-1 device is shown below:

```
PRUEBAS-BFD-1 BFD+list all

    MyDisc: 0x72c206be  ReDisc: 0xd0bee79c
    Myaddr: 172.24.80.10  Peer: 172.24.80.12  Infc: ethernet0/0
    State: Up    Uptime: 27s    Created: 30s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms XmtTime: 50 ms DetectTime: 150 m
    Xmtpkts: 639    Last Tx interval: 44ms  min/max/avg: 38ms/47ms/42ms
    Rcvpkts: 640    Last Rx interval: 46ms  min/max/avg: 37ms/48ms/42ms

    MyDisc: 0xbba08211  ReDisc: 0x7267556c
    Myaddr: 10.10.44.200  Peer: 10.10.44.205  Infc: ethernet0/1
    State: Up    Uptime: 28s    Created: 31s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM
    BFD version: 1  Demand mode: ON
    Authentication Type: Disabled    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms XmtTime: 50 ms DetectTime: 150 ms
    Xmtpkts: 4    Last Tx interval: 295ms  min/max/avg: 295ms/16s 667ms/8s 481ms
    Rcvpkts: 4    Last Rx interval: 296ms  min/max/avg: 296ms/16s 667ms/8s 481ms

PRUEBAS-BFD-1 BFD+
```

This corresponds to the PRUEBAS-BFD-3 device:

```
PRUEBAS-BFD-3 BFD+list all
```

```
    MyDisc: 0xd0bee79c  ReDisc: 0x72c206be
    Myaddr: 172.24.80.12  Peer: 172.24.80.10  Infc: ethernet0/0
    State: Up    Uptime: 1m 0s    Created: 1m 4s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms XmtTime: 50 ms DetectTime: 150 ms
    Xmtpkts: 1412    Last Tx interval: 42ms  min/max/avg: 38ms/47ms/42ms
    Rcvpkts: 1411    Last Rx interval: 45ms  min/max/avg: 37ms/47ms/42ms

    MyDisc: 0x7267556c  ReDisc: 0xbba08211
    Myaddr: 10.10.44.205  Peer: 10.10.44.200  Infc: ethernet0/1
    State: Up    Uptime: 1m 1s    Created: 1m 4s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM
    BFD version: 1  Demand mode: ON
    Authentication Type: Disabled    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms XmtTime: 50 ms DetectTime: 150 ms
    Xmtpkts: 8    Last Tx interval: 306ms  min/max/avg: 295ms/19s 705ms/9s 496ms
    Rcvpkts: 8    Last Rx interval: 306ms  min/max/avg: 295ms/19s 705ms/9s 496ms

PRUEBAS-BFD-3 BFD+
```

If we simulate a drop in the 10.10.44.0 network, for instance by disconnecting the network cable from the PRUEBAS-BFD-3 Ethernet0/1 interface (as this is in *Demand* mode) the interface, in this case, will drop before the BFD is capable of detecting it and consequently the *Diagnostic Code* is *Path Down*. BFD would have detected the drop in the next poll cycle. It's as if we had executed the *shutdown* command on the PRUEBAS-BFD-3 device's Ethernet0/1 interface:

```
PRUEBAS-BFD-1 BFD+list all

    MyDisc: 0x72c206be  ReDisc: 0xd0bee79c
    Myaddr: 172.24.80.10  Peer: 172.24.80.12  Infc: ethernet0/0
    State: Up    Uptime: 3m 6s    Created: 3m 9s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms XmtTime: 50 ms DetectTime: 150 ms
    Xmtpkts: 4355    Last Tx interval: 44ms  min/max/avg: 38ms/47ms/41ms
    Rcvpkts: 4356    Last Rx interval: 46ms  min/max/avg: 37ms/48ms/41ms

    MyDisc: 0xbba08211  ReDisc: 0x7267556c
    Myaddr: 10.10.44.200  Peer: 10.10.44.205  Infc: ethernet0/1

    State: Down    Uptime: 0s    Created: 3m 10s

     Falls detected: 1 Diag code: Control Detection Time Expired
     Registered protocols: NSM
     BFD version: 1 Demand mode: OFF
     Authentication Type: Disabled    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
     ActiveMinTx: 1000 ms XmtTime: 1000 ms DetectTime: 150 ms
     Xmtpkts: 34    Last Tx interval: 920ms  min/max/avg: 21ms/20s 0ms/5s 843ms
     Rcvpkts: 18    Last Rx interval: 332ms  min/max/avg: 296ms/19s 699ms/9s 810ms

PRUEBAS-BFD-1 BFD+
PRUEBAS-BFD-3 BFD+list all

    MyDisc: 0xd0bee79c  ReDisc: 0x72c206be
    Myaddr: 172.24.80.12  Peer: 172.24.80.10  Infc: ethernet0/0
    State: Up    Uptime: 3m 55s    Created: 3m 58s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms XmtTime: 50 ms DetectTime: 150 ms
```

```
    Xmtpkts: 5497    Last Tx interval: 38ms  min/max/avg: 38ms/47ms/41ms
    Rcvpkts: 5496    Last Rx interval: 42ms  min/max/avg: 37ms/48ms/41ms

    MyDisc: 0x7267556c  ReDisc: 0xbba08211
    Myaddr: 10.10.44.205  Peer: 10.10.44.200  Infc: ethernet0/1
    State: Admindown    Uptime: 0s    Created: 3m 58s
    Falls detected: 1 Diag code: Path Down
    Registered protocols: NSM
    BFD version: 1 Demand mode: OFF
    Authentication Type: Disabled    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 1000 ms XmtTime: 1000 ms DetectTime: 150 ms
    Xmtpkts: 43    Last Tx interval: 810ms  min/max/avg: 21ms/19s 705ms/4s 747ms
    Rcvpkts: 18    Last Rx interval: 331ms  min/max/avg: 295ms/19s 705ms/9s 812ms

PRUEBAS-BFD-3 BFD+
```

4.2 Configuration example for BFD with NSM, NSLA and BGP

Below, you will see a configuration example between two Atlas 250 devices connected to two different networks through their Ethernet0/0 and Ethernet0/1 interfaces.

Device: PRUEBAS-BFD-1:

```
; Showing System Configuration for access-level 15 ...

log-command-errors
no configuration
set hostname PRUEBAS-BFD-1
;
network ethernet0/0
; -- Ethernet Interface User Configuration --
   ip address 172.24.80.10 255.255.0.0
;
   bfd interval 50
   bfd min-rx 50
   bfd multiplier 3

exit
;
;
network ethernet0/1
; -- Ethernet Interface User Configuration --
   ip address 10.10.44.200 255.255.255.0
;
   bfd interval 65
   bfd min-rx 55
   bfd multiplier 4

exit
;
;
protocol bfd
; -- Bidirectional Forwarding Detection user configuration --
   enable
exit
;
protocol ip
; -- Internet protocol user configuration --
   router-id 172.24.80.10
;
   route 0.0.0.0 0.0.0.0 172.24.0.98
;
   classless
;
exit
;
;
```

```
protocol bgp
; -- Border Gateway Protocol user configuration --
   enable
;
   as 100
   export as 200 prot all all
;
   export as 300 prot all all
;
   group type external peer-as 300
; -- BGP group configuration --
      peer 10.10.44.205
      peer 10.10.44.205 bfd-session
      peer 172.24.80.12
      peer 172.24.80.12 bfd-session
   exit
;
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
;
feature nsla
; -- Feature Network Service Level Advisor --
   enable
;

   filter 1 nsm-op 1 bfd
   filter 1 significant-samples 1
   filter 1 activation threshold 0
   filter 1 activation sensibility 100
   filter 1 activation stabilization-time 5
   filter 1 deactivation threshold 0
   filter 1 deactivation sensibility 100
   filter 1 deactivation stabilization-time 5
;
   filter 2 nsm-op 2 bfd
   filter 2 significant-samples 1
   filter 2 activation threshold 0
   filter 2 activation sensibility 100
   filter 2 activation stabilization-time 5
   filter 2 deactivation threshold 0
   filter 2 deactivation sensibility 100
   filter 2 deactivation stabilization-time 5
;
   alarm 1 filter-id 1
;
```

```
   alarm 2 filter-id 2
;
   advisor 1 alarm-id 1
;
   advisor 2 alarm-id 2
;
exit
;
dump-command-errors
end
; --- end ---
```

Device: PRUEBAS-BFD-3:

```
; Showing System Configuration for access-level 15 ...

log-command-errors
no configuration
set hostname PRUEBAS-BFD-3
;
network ethernet0/0
; -- Ethernet Interface User Configuration --
   ip address 172.24.80.12 255.255.0.0
;
   bfd interval 50
   bfd min-rx 50
   bfd multiplier 3
exit
;
;
network ethernet0/1
; -- Ethernet Interface User Configuration --
   ip address 10.10.44.205 255.255.255.0
;
   bfd interval 65
   bfd min-rx 55
   bfd multiplier 5
exit
;
;
   protocol bfd
; -- Bidirectional Forwarding Detection user configuration --
   enable
exit
;
protocol ip
; -- Internet protocol user configuration --
   router-id 172.24.80.12
;
   route 0.0.0.0 0.0.0.0 172.24.0.6
;
   classless
;
exit
;
;
protocol bgp
; -- Border Gateway Protocol user configuration --
   enable
;
   as 300
   export as 100 prot all all
;
   group type external peer-as 100
; -- BGP group configuration --
      peer 10.10.44.200
      peer 10.10.44.200 bfd-session
      peer 172.24.80.10
```

```
      peer 172.24.80.10 bfd-session
   exit
;
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
;
dump-command-errors
end
; --- end ---
```

Once both sessions are established, everything we see under the monitoring lists in the PRUEBAS-BFD-1 device is shown below:

```
PRUEBAS-BFD-1 BFD+list all

    MyDisc: 0x571485c1  ReDisc: 0x75c455d1
    Myaddr: 172.24.80.10  Peer: 172.24.80.12  Infc: ethernet0/0
    State: Up    Uptime: 1m 43s    Created: 1m 46s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM BGP
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms XmtTime: 50 ms DetectTime: 150 ms
    Xmtpkts: 2426    Last Tx interval: 40ms  min/max/avg: 38ms/47ms/42ms
    Rcvpkts: 2427    Last Rx interval: 45ms  min/max/avg: 37ms/47ms/42ms

    MyDisc: 0xd2512e7a  ReDisc: 0x6675e700
    Myaddr: 10.10.44.200  Peer: 10.10.44.205  Infc: ethernet0/1
    State: Up    Uptime: 1m 44s    Created: 1m 47s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM BGP
    BFD version: 1  Demand mode: ON
    Authentication Type: Disabled    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms XmtTime: 50 ms DetectTime: 150 ms

    Xmtpkts: 12    Last Tx interval: 285ms  min/max/avg: 265ms/19s 730ms/9s 693ms
    Rcvpkts: 12    Last Rx interval: 285ms  min/max/avg: 265ms/19s 730ms/9s 693ms

PRUEBAS-BFD-1 BFD+
```

The following corresponds to the PRUEBAS-BFD-3 device:

```
PRUEBAS-BFD-3 BFD+list all

    MyDisc: 0x75c455d1  ReDisc: 0x571485c1
    Myaddr: 172.24.80.12  Peer: 172.24.80.10  Infc: ethernet0/0
```

```
    State: Up    Uptime: 2m 26s    Created: 2m 29s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM BGP
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms XmtTime: 50 ms DetectTime: 150 ms
    Xmtpkts: 3418    Last Tx interval: 42ms  min/max/avg: 38ms/47ms/41ms
    Rcvpkts: 3417    Last Rx interval: 45ms  min/max/avg: 37ms/47ms/41ms

    MyDisc: 0x6675e700  ReDisc: 0xd2512e7a
    Myaddr: 10.10.44.205  Peer: 10.10.44.200  Infc: ethernet0/1
    State: Up    Uptime: 2m 27s    Created: 2m 29s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM BGP
    BFD version: 1  Demand mode: ON
    Authentication Type: Disabled    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms XmtTime: 50 ms DetectTime: 150 ms
    Xmtpkts: 16    Last Tx interval: 296ms  min/max/avg: 266ms/19s 734ms/9s 783ms
    Rcvpkts: 16    Last Rx interval: 295ms  min/max/avg: 265ms/19s 735ms/9s 783ms

PRUEBAS-BFD-3 BFD+
```

If the the BFD session is created by means of the NSM feature, the BFD parameters are taken from the NSM operation configuration. Those that have been configured in the interface where the session has been established are ignored.

If we simulate a drop in the 10.10.44.0 network, for instance by disconnecting the network cable from the PRUEBAS-BFD-3 Ethernet0/1 interface, what you will see is the same as in the previous example (i.e., a drop when the device detects that its interface has been disconnected):

```
PRUEBAS-BFD-1 BFD+list all

    MyDisc: 0x571485c1  ReDisc: 0x75c455d1
    Myaddr: 172.24.80.10  Peer: 172.24.80.12  Infc: ethernet0/0
    State: Up    Uptime: 11m 37s    Created: 11m 41s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM BGP
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled
    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms XmtTime: 50 ms DetectTime: 150 ms
    Xmtpkts: 16312    Last Tx interval: 46ms  min/max/avg: 38ms/47ms/41ms
    Rcvpkts: 16312    Last Rx interval: 45ms  min/max/avg: 37ms/47ms/41ms

    MyDisc: 0xd2512e7a  ReDisc: 0x6675e700
    Myaddr: 10.10.44.200  Peer: 10.10.44.205  Infc: ethernet0/1
    State: Down    Uptime: 0s    Created: 11m 41s
    Falls detected: 1 Diag code: Control Detection Time Expired
    Registered protocols: NSM BGP
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled
    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 1000 ms XmtTime: 1000 ms DetectTime: 150 ms
    Xmtpkts: 77    Last Tx interval: 790ms  min/max/avg: 21ms/20s 0ms/9s 317ms
    Rcvpkts: 70    Last Rx interval: 435ms  min/max/avg: 265ms/19s 730ms/9s 954ms

PRUEBAS-BFD-1 BFD+
PRUEBAS-BFD-3 BFD+list all

    MyDisc: 0x75c455d1  ReDisc: 0x571485c1
    Myaddr: 172.24.80.12  Peer: 172.24.80.10  Infc: ethernet0/0
    State: Up    Uptime: 12m 22s    Created: 12m 25s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM BGP
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled
    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms XmtTime: 50 ms DetectTime: 150 ms
```

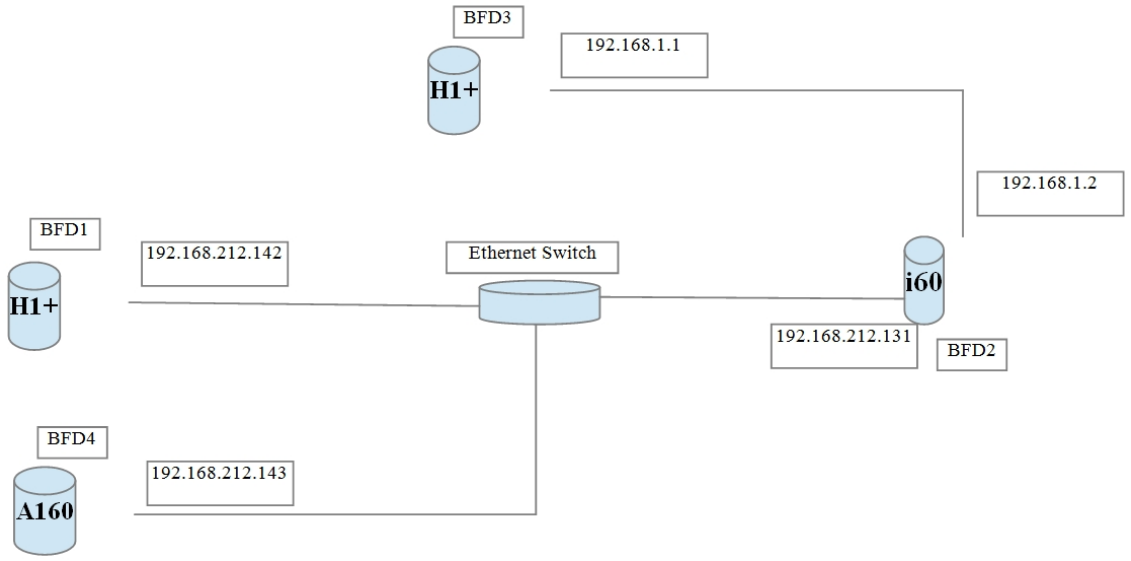
```
    Xmtpkts: 17326    Last Tx interval: 41ms  min/max/avg: 38ms/47ms/41ms
    Rcvpkts: 17326    Last Rx interval: 46ms  min/max/avg: 37ms/48ms/41ms

    MyDisc: 0x6675e700  ReDisc: 0xd2512e7a
    Myaddr: 10.10.44.205  Peer: 10.10.44.200  Infc: ethernet0/1
    State: Admindown    Uptime: 0s    Created: 12m 25s
    Falls detected: 1 Diag code: Path Down
    Registered protocols: NSM BGP
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled
    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
     ActiveMinTx: 1000 ms XmtTime: 1000 ms DetectTime: 150 ms
    Xmtpkts: 70    Last Tx interval: 435ms  min/max/avg: 266ms/19s 734ms/9s 957ms
    Rcvpkts: 70    Last Rx interval: 434ms  min/max/avg: 265ms/19s 735ms/9s 957ms

PRUEBAS-BFD-3 BFD+
```

4.3 Configuration example for multihop BFD sessions with NSM

The following configuration example shows multiple devices connected in accordance with the scheme detailed.



Both multihop and singlehop sessions are configured in the example. It includes sessions with and without authentication, and even some with the Key Chain feature.

BFD-1 device:

```
; Showing Menu and Submenus Configuration for access-level 15 ...

   log-command-errors
   no configuration
   set hostname BFD1
   set inactivity-timer disabled
   add device loopback 1
   set data-link at cellular0/0
   set data-link at cellular0/1
   set data-link at cellular1/0
   set data-link at cellular1/1
;
   network ethernet0/0
; -- Ethernet Interface User Configuration --
      ip address 192.168.212.142 255.255.254.0
;
   exit
;
;
   network loopback1
; -- Loopback interface configuration -
      ip address 192.168.2.1 255.255.255.0
```

```
;
   exit
;
;
;
;
;
   protocol bfd
; -- Bidirectional Forwarding Detection user configuration --
      enable
;
      profile test min-tx 450 min-rx 450 mult 7 md5 key-string pablito
;
      session src 192.168.212.142 dst 192.168.1.1 test
   exit
;
;
   protocol ip
; -- Internet protocol user configuration --
      route 192.168.1.0 255.255.255.0 192.168.212.131
;
      classless
   exit
;
;
   feature ntp
; -- NTP Protocol user configuration --
      peer address 1 192.168.212.14
   exit
;
   feature nsm
; -- Network Service Monitor configuration --
      operation 1
; -- NSM Operation configuration --
         type bfd async-mode 192.168.1.1
         source-ipaddr 192.168.212.142
      exit
;
      operation 2
; -- NSM Operation configuration --
         type bfd async-mode 192.168.212.131
            bfd-interval 450
            bfd-min-rx 470
            bfd-multiplier 7
            source-ipaddr 192.168.212.142

      exit
;
      schedule 1 life forever
      schedule 1 start-time now
      schedule 2 life forever
      schedule 2 start-time now
   exit
;
   dump-command-errors
   end
```

BFD-2 device:

```
; Showing Menu and Submenus Configuration for access-level 15 ...

   log-command-errors
   no configuration
   set hostname BFD2
   set data-link at cellular0/0
   set data-link at cellular0/1
;
   network ethernet0/0
```

```
; -- Ethernet Interface User Configuration --
      ip address 192.168.212.131 255.255.254.0
;
   exit
;
;
   network ethernet0/1
; -- Ethernet Interface User Configuration --
      ip address 192.168.1.2 255.255.255.0
;
   exit
;
   event
; -- ELS Config --
      enable trace subsystem BFD ALL
   exit
;
;
;
;
;
    protocol bfd
; -- Bidirectional Forwarding Detection user configuration --
    enable
;
;
   exit
;
;
   feature nsm
; -- Network Service Monitor configuration --
      operation 1
; -- NSM Operation configuration --
         type bfd async-mode 192.168.212.142
         bfd-interval 480
         bfd-min-rx 300
         source-ipaddr 192.168.212.131
      exit
;
      schedule 1 life forever
      schedule 1 start-time now
   exit
;
   dump-command-errors
   end
```

BFD-3 device:

```
; Showing Menu and Submenus Configuration for access-level 15 ...

   log-command-errors
   no configuration
   set hostname BFD3
   set inactivity-timer disabled
   set data-link at cellular0/0
   set data-link at cellular0/1
   set data-link at cellular1/0
   set data-link at cellular1/1
   feature key-chain
; -- Key Chain user configuration --
      key-chain sha1tests
         key 1 key-string sha1keyfortesting
         key 1 accept-lifetime 00:00:00 1 jan 2013 17:30:00 24 jan 2013
         key 1 send-lifetime 00:00:00 1 jan 2013 17:30:00 24 jan 2013
;
         key 2 key-string sha1keyfortesting2
         key 2 accept-lifetime 17:30:00 24 jan 2013 infinite
         key 2 send-lifetime 17:30:00 24 jan 2013 infinite
```

```
;
      exit
;
   exit
;
;
   network ethernet0/0
; -- Ethernet Interface User Configuration --
      ip address 192.168.1.1 255.255.255.0
;
   exit
;
;
;
;
;
   protocol bfd
; -- Bidirectional Forwarding Detection user configuration --
      enable
;
      profile test min-tx 450 min-rx 450 mult 6 md5 key-string pablito
      profile test2 min-tx 450 min-rx 450 mult 6
      profile test3 min-tx 950 min-rx 950 mult 20 sha1 key-chain sha1tests
;
      session src 192.168.1.1 dst 192.168.212.142 test
      session src 192.168.1.1 dst 192.168.212.143 test3         exit
;
;
   protocol ip
; -- Internet protocol user configuration --
      route 192.168.212.0 255.255.254.0 192.168.1.2
;
   exit
;
;
   feature ntp
; -- NTP Protocol user configuration --
      protocol
      peer address 1 192.168.212.14
   exit
;
   feature nsm
; -- Network Service Monitor configuration --
      operation 1
; -- NSM Operation configuration --
         type bfd async-mode 192.168.212.142
         source-ipaddr 192.168.1.1
     exit
;
      operation 2
; -- NSM Operation configuration --
         type bfd async-mode 192.168.212.143
         source-ipaddr 192.168.1.1
      exit
;
      schedule 1 life forever
      schedule 1 start-time now
      schedule 2 life forever
      schedule 2 start-time now
   exit
;
   dump-command-errors
   end
```

BFD-4 device:

```
; Showing Menu and Submenus Configuration for access-level 15 ...
```

```
   log-command-errors
   no configuration
   set hostname BFD4
   feature key-chain
; -- Key Chain user configuration --
      key-chain sha1tests
      key 1 key-string sha1keyfortesting
      key 1 accept-lifetime 00:00:00 1 jan 2013 17:30:00 24 jan 2013
      key 1 send-lifetime 00:00:00 1 jan 2013 17:30:00 24 jan 2013
;
      key 2 key-string sha1keyfortesting2
      key 2 accept-lifetime 17:30:00 24 jan 2013 infinite
      key 2 send-lifetime 17:30:00 24 jan 2013 infinite
;
      exit
;
   exit
;
;
   network ethernet0/0
; -- Ethernet Interface User Configuration --
      ip address 192.168.212.143 255.255.254.0
;
   exit
;
;
;
;
;
   protocol bfd
; -- Bidirectional Forwarding Detection user configuration --
      enable
;
      profile test min-tx 900 min-rx 950 mult 20 sha1 key-chain sha1tests
;
      session src 192.168.212.143 dst 192.168.1.1 test
   exit
;
;
   protocol ip
; -- Internet protocol user configuration --
      route 192.168.1.0 255.255.255.0 192.168.212.131
;
      classless
   exit
;
;
   feature nsm
; -- Network Service Monitor configuration --
      operation 1
; -- NSM Operation configuration --
         type bfd async-mode 192.168.1.1
         source-ipaddr 192.168.212.143
      exit
;
      schedule 1 life forever
      schedule 1 start-time now
   exit
;
   dump-command-errors
   end
```

Once the sessions have been established, the monitoring lists in the BFD-1 device show the following:

```
BFD1 BFD+list all

    MyDisc: 0x534ef075  ReDisc: 0x79986c65
    Myaddr: 192.168.212.142  Peer: 192.168.212.131  Infc: ethernet0/0
```

```
    State: Up    Uptime: 2d 6h 39m 39s    Created: 5d 16h 19m 36s
    Falls detected: 4    Diag code: Control Detection Time Expired
    Registered protocols: NSM
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled
    MinTx: 450 ms   MinRx: 470 ms   Mult: 7
    ActiveMinTx: 450 ms XmtTime: 450 ms DetectTime: 1440 ms
    Xmtpkts: 498977    Last Tx interval: 352ms  min/max/avg: 337ms/543ms/392ms
    Rcvpkts: 467925    Last Rx interval: 365ms  min/max/avg: 202ms/1s 297ms/419ms

    MyDisc: 0xf6776c5d  ReDisc: 0x6931e5db
    Myaddr: 192.168.212.142  Peer: 192.168.1.1  Infc: Multihop session
    State: Up   Uptime: 2d 6h 39m 40s    Created: 5d 16h 19m 37s
    Falls detected: 5    Diag code: Control Detection Time Expired
    Registered protocols: NSM
    BFD version: 1  Demand mode: OFF
    Authentication Type: Keyed MD5
    MinTx: 450 ms   MinRx: 450 ms   Mult: 7
    ActiveMinTx: 450 ms XmtTime: 450 ms DetectTime: 2700 ms
    Xmtpkts: 498913    Last Tx interval: 400ms  min/max/avg: 337ms/671ms/393ms
    Rcvpkts: 498546    Last Rx interval: 347ms  min/max/avg: 3ms/1s 225ms/392ms

BFD1 BFD+
```

This corresponds to the BFD-2 device:

```
BFD2 BFD+list all

    MyDisc: 0x79986c65  ReDisc: 0x534ef075
    Myaddr: 192.168.212.131  Peer: 192.168.212.142  Infc: ethernet0/0
    State: Up    Uptime: 2d 7h 52m 21s    Created: 2d 7h 52m 25s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled
    MinTx: 480 ms   MinRx: 300 ms   Mult: 3
    ActiveMinTx: 480 ms XmtTime: 480 ms DetectTime: 3150 ms
    Xmtpkts: 478677    Last Tx interval: 389ms  min/max/avg: 360ms/659ms/419ms
    Rcvpkts: 509790    Last Rx interval: 152ms  min/max/avg: 0ms/1s 495ms/393ms

BFD2 BFD+
```

This is what shows up for the BFD-3 device:

```
BFD3 BFD+list all

    MyDisc: 0x58f8f4bc  ReDisc: 0xf515d2db
    Myaddr: 192.168.1.1  Peer: 192.168.212.143  Infc: Multihop session
    State: Up    Uptime: 6m 9s    Created: 5d 17h 31m 41s
    Falls detected: 3    Diag code: Control Detection Time Expired
    Registered protocols: NSM
    BFD version: 1  Demand mode: OFF
    MinTx: 950 ms   MinRx: 950 ms   Mult: 20
    ActiveMinTx: 950 ms XmtTime: 950 ms DetectTime: 19000 ms
    Xmtpkts: 444    Last Tx interval: 808ms  min/max/avg: 712ms/947ms/830ms
    Rcvpkts: 444    Last Rx interval: 720ms  min/max/avg: 58ms/1s 603ms/831ms

    MyDisc: 0x6931e5db  ReDisc: 0xf6776c5d
    Myaddr: 192.168.1.1  Peer: 192.168.212.142  Infc: Multihop session
    State: Up    Uptime: 2d 7h 52m 58s    Created: 5d 17h 31m 41s
    Falls detected: 4    Diag code: Control Detection Time Expired
    Registered protocols: NSM
    BFD version: 1  Demand mode: OFF
    Authentication Type: Keyed MD5
    MinTx: 450 ms   MinRx: 450 ms   Mult: 6
    ActiveMinTx: 450 ms XmtTime: 450 ms DetectTime: 3150 ms
    Xmtpkts: 510236    Last Tx interval: 356ms  min/max/avg: 337ms/479ms/393ms
    Rcvpkts: 509681    Last Rx interval: 571ms  min/max/avg: 0ms/1s 359ms/393ms
```

```
BFD BFD+
```

And for BFD-4:

```
BFD4 BFD+list all

    MyDisc: 0xf515d2db  ReDisc: 0x58f8f4c
    Myaddr: 192.168.212.143  Peer: 192.168.1.1  Infc: Multihop session
    State: Up    Uptime: 6m 51s    Created: 7m 35s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: NSM
    BFD version: 1  Demand mode: OFF
    Authentication Type: Keyed SHA1
    MinTx: 900 ms   MinRx: 950 ms   Mult: 20
    ActiveMinTx: 900 ms XmtTime: 950 ms DetectTime: 19000 ms
    Xmtpkts: 495    Last Tx interval: 893ms  min/max/avg: 712ms/946ms/831ms
    Rcvpkts: 495    Last Rx interval: 875ms  min/max/avg: 712ms/947ms/830ms

BFD4 BFD+
```

4.4 Configuration example for BFD with BGP and IPv6 addressing

Below, you can see a configuration example involving two devices connected to a switch.

Configuration for device 1:

```
   log-command-errors
   no configuration
   set data-link at cellular0/0
   set data-link at cellular1/0
   set data-link nic cellular0/1
   set data-link nic cellular1/1
   set hostname PRUEBAS-BFD-1_6
   network ethernet0/0
; -- Ethernet Interface User Configuration --
      ipv6 address 2001:db8:1000::1/64
      ipv6 nd ra suppress
      bfd interval 50
;
   exit
;
   network ethernet0/1
; -- Ethernet Interface User Configuration --
      bfd interval 65
      bfd min-rx 55
      bfd multiplier 4
   exit
;
   network ethernet2/0
; -- Ethernet Interface User Configuration --
      no auto-negotiation
      duplex full
      speed 1000mbps
   exit
;
   event
; -- ELS Config --
      enable trace subsystem BGP ALL
      enable trace subsystem BFD ALL
      enable trace subsystem DEBUG ALL
   exit
;
;
;
;
```

```
   protocol bfd
; -- Bidirectional Forwarding Detection user configuration --
      enable
;
;
   exit
;
;
;
   protocol bgp
; -- Border Gateway Protocol user configuration --
      enable
;
      as 100
      router-id 192.168.214.155
;
      address-family ipv6
; -- BGP IPv6 address family configuration --
         export as 300 prot all all
;
      exit
;
      group type external peer-as 300
; -- BGP group configuration --
         peer 2001:db8:1000::2
         peer 2001:db8:1000::2 bfd-session
         peer 2001:db8:1000::2 address-family ipv6 unicast
      exit
;
   exit
;
```

Configuration for the second device:

```
   log-command-errors
   no configuration
   set data-link at cellular0/0
   set data-link at cellular1/0
   set data-link nic cellular0/1
   set data-link nic cellular1/1
   set hostname PRUEBAS-BFD-2_6
   network ethernet0/0
; -- Ethernet Interface User Configuration --
      ipv6 address 2001:db8:1000::2/64
      ipv6 nd ra suppress
      bfd interval 50
;
   exit
;
   network ethernet0/1
; -- Ethernet Interface User Configuration --
      bfd interval 65
      bfd min-rx 55
      bfd multiplier 4
   exit
;
   event
; -- ELS Config --
      enable trace subsystem BGP ALL
      enable trace subsystem BFD ALL
      enable trace subsystem DEBUG ALL
   exit
;
;
;
;
   protocol bfd
; -- Bidirectional Forwarding Detection user configuration --
```

```
      enable
;
;
   exit
;
;
;
   protocol bgp
; -- Border Gateway Protocol user configuration --
      enable
;
      as 300
      router-id 192.168.214.157
;
      address-family ipv6
; -- BGP IPv6 address family configuration --
         export as 300 prot all all
;
      exit
;
      group type external peer-as 100
; -- BGP group configuration --
         peer 2001:db8:1000::1
         peer 2001:db8:1000::1 bfd-session
         peer 2001:db8:1000::1 address-family ipv6 unicast
      exit
;
   exit
;
;
```

Once the sessions have been established, the following appears under the monitoring lists in the PRUEBAS-BFD-1_6 device:

```
PRUEBAS-BFD-1_6 BFD+list summary

MyDisc      ReDisc      MyIP             Peer             State      XmtTime  DetectTime  Falls       Uptime
-------------------------------------------------------------------------------------------------------------------------------
0x3ee9b38b  0x7a911131  2001:db8:1000::1  2001:db8:1000::2  Up         50   ms  150  ms     0           13m 5s
```

```
PRUEBAS-BFD-1_6 BFD+list all

    MyDisc: 0x3ee9b38b  ReDisc: 0x7a911131
    Myaddr: 2001:db8:1000::1  Peer: 2001:db8:1000::2  Infc: ethernet0/0
    State: Up    Uptime: 13m 32s    Created: 13m 33s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: BGP
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled
    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms   XmtTime: 50 ms   DetectTime: 150 ms
    Xmtpkts: 18887    Last Tx interval: 45ms  min/max/avg: 37ms/46ms/41ms
    Rcvpkts: 18887    Last Rx interval: 38ms  min/max/avg: 37ms/46ms/41ms
```

This is what we get if we simulate a drop in the network disconnecting a link:

```
PRUEBAS-BFD-2_6 BFD+li all

    MyDisc: 0x7a911131  ReDisc: 0x0
    Myaddr: 2001:db8:1000::2  Peer: 2001:db8:1000::1  Infc: ethernet0/0
    State: Down    Uptime: 0s    Created: 15m 0s
    Falls detected: 1    Diag code: Control Detection Time Expired
    Registered protocols: BGP
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled
    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 1000 ms   XmtTime: 1000 ms   DetectTime: 150 ms
    Xmtpkts: 20896    Last Tx interval: 780ms  min/max/avg: 19ms/780ms/41ms
    Rcvpkts: 20891    Last Rx interval: 41ms  min/max/avg: 37ms/46ms/41ms
```

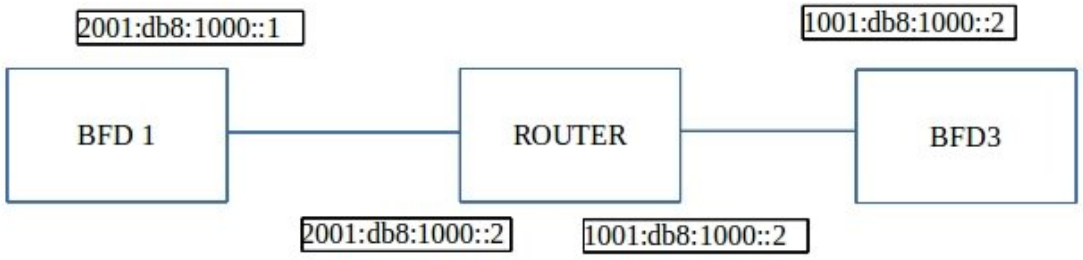
After connecting the cable again:

```
PRUEBAS-BFD-2_6 BFD+li all

    MyDisc: 0x7a911131  ReDisc: 0x3ee9b38b
    Myaddr: 2001:db8:1000::2  Peer: 2001:db8:1000::1  Infc: ethernet0/0
    State: Up    Uptime: 6s    Created: 15m 32s
    Falls detected: 1    Diag code: Control Detection Time Expired
    Registered protocols: BGP
    BFD version: 1  Demand mode: OFF
    Authentication Type: Disabled
    MinTx: 50 ms   MinRx: 50 ms   Mult: 3
    ActiveMinTx: 50 ms   XmtTime: 50 ms   DetectTime: 150 ms
    Xmtpkts: 138    Last Tx interval: 40ms  min/max/avg: 37ms/46ms/43ms
    Rcvpkts: 139    Last Rx interval: 44ms  min/max/avg: 37ms/46ms/43ms
```

4.5 Configuration example for multihop BFD sessions with BGP and IPv6

Below, you will see an example of two devices connected to a middle router. Each device belongs to a different network.



Configuration for the BFD1 device:

```
   log-command-errors
   no configuration
   set data-link at cellular0/0
   set data-link at cellular1/0
   set data-link nic cellular0/1
   set data-link nic cellular1/1
   set hostname PRUEBAS-BFD-1_6
   network ethernet0/0
; -- Ethernet Interface User Configuration --
      ipv6 address 2001:db8:1000::1/64
      ipv6 nd ra suppress
      bfd interval 50
;
   exit
;
   network ethernet0/1
; -- Ethernet Interface User Configuration --
      bfd interval 65
      bfd min-rx 55
      bfd multiplier 4
   exit
;
   event
; -- ELS Config --
```

```
      enable trace subsystem BGP ALL
      enable trace subsystem BFD ALL
      enable trace subsystem DEBUG ALL
   exit
;
;
;
;
   protocol bfd
; -- Bidirectional Forwarding Detection user configuration --
      enable
;
      profile test min-tx 450 min-rx 450 mult 7 md5 key-string pablito
;
      session src 2001:db8:1000::1 dst 1001:db8:1000::1 test
   exit
;
   protocol ipv6
; -- IPv6 user configuration --
      route 1001:db8:1000::/64 2001:db8:1000::4
   exit
;

;
;
   protocol bgp
; -- Border Gateway Protocol user configuration --
      enable
;
      as 100
      router-id 192.168.214.155
;
      address-family ipv6
; -- BGP IPv6 address family configuration --
         export as 200 prot all all
;
         export as 300 prot all all
;
      exit
;
      group type external peer-as 300
; -- BGP group configuration --
         peer 1001:db8:1000::1
         peer 1001:db8:1000::1 local-interface ethernet0/0
         peer 1001:db8:1000::1 no-shared-interface
         peer 1001:db8:1000::1 bfd-session
      exit
;
   exit
;
;
```

Configuration for the middle router:

```
  log-command-errors
   no configuration
   set data-link at cellular0/0
   set data-link at cellular1/0
   set data-link nic cellular0/1
   set data-link nic cellular1/1
;
   network ethernet0/0
; -- Ethernet Interface User Configuration --
      ip address 192.168.214.154 255.255.252.0
;
      ipv6 address 2001:db8:1000::4/64
      ipv6 nd ra suppress
;
```

```
   exit
;
   network ethernet0/1
; -- Ethernet Interface User Configuration --
      ipv6 address 1001:db8:1000::2/64
      ipv6 nd ra suppress
   exit
;
;
;
;
;
;
   protocol ipv6
; -- IPv6 user configuration --
      unicast-routing
   exit
;
;
;
;
```

Configuration for the BFD3 device:

```
   log-command-errors
   no configuration
   set data-link at cellular0/0
   set data-link at cellular1/0
   set data-link nic cellular0/1
   set data-link nic cellular1/1
   set hostname PRUEBAS-BFD-3_6
   network ethernet0/0
; -- Ethernet Interface User Configuration --
      ipv6 address 1001:db8:1000::1/64
      ipv6 nd ra suppress
      bfd interval 50
;
   exit
;
   network ethernet0/1
; -- Ethernet Interface User Configuration --
      bfd interval 65
      bfd min-rx 55
      bfd multiplier 5
   exit
;
   event
; -- ELS Config --
      enable trace subsystem BGP ALL
      enable trace subsystem BFD ALL
      enable trace subsystem DEBUG ALL
   exit
;
;
;
;
   protocol bfd
; -- Bidirectional Forwarding Detection user configuration --
      enable
;
      profile test min-tx 450 min-rx 450 mult 6 md5 key-string pablito
;
      session src 1001:db8:1000::1 dst 2001:db8:1000::1 test
   exit
;
   protocol ipv6
; -- IPv6 user configuration --
      route 2001:db8:1000::/64 1001:db8:1000::2
```

```
   exit
;
;
;
   protocol bgp
; -- Border Gateway Protocol user configuration --
      enable
;
      as 300
      router-id 192.168.214.157
;
      address-family ipv6
; -- BGP IPv6 address family configuration --
         export as 100 prot all all
;
      exit
;
      group type external peer-as 100
; -- BGP group configuration --
         peer 2001:db8:1000::1
         peer 2001:db8:1000::1 local-interface ethernet0/0
         peer 2001:db8:1000::1 no-shared-interface
         peer 2001:db8:1000::1 bfd-session
      exit
;
   exit
;
;
```

Once the sessions have been established, the following appears under the monitoring lists in the BFD1 device:

```
PRUEBAS-BFD-1_6 BFD+list all

    MyDisc: 0x4bc08c10  ReDisc: 0xf9c3d297
    Myaddr: 2001:db8:1000::1  Peer: 1001:db8:1000::1  Infc: Multihop session
    State: Up    Uptime: 32s    Created: 33s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: BGP
    BFD version: 1  Demand mode: OFF
    Authentication Type: Keyed MD5
    MinTx: 450 ms   MinRx: 450 ms   Mult: 7
    ActiveMinTx: 450 ms   XmtTime: 450 ms   DetectTime: 2700 ms
    Xmtpkts: 78    Last Tx interval: 446ms  min/max/avg: 337ms/446ms/405ms
    Rcvpkts: 78    Last Rx interval: 445ms  min/max/avg: 337ms/446ms/405ms
```

This is what we get for the BFD3 device:

```
PRUEBAS-BFD-3_6 BFD+list all

    MyDisc: 0xf9c3d297  ReDisc: 0x4bc08c10
    Myaddr: 1001:db8:1000::1  Peer: 2001:db8:1000::1  Infc: Multihop session
    State: Up    Uptime: 1m 25s    Created: 1m 25s
    Falls detected: 0    Diag code: No Diagnostic
    Registered protocols: BGP
    BFD version: 1  Demand mode: OFF
    Authentication Type: Keyed MD5
    MinTx: 450 ms   MinRx: 450 ms   Mult: 6
    ActiveMinTx: 450 ms   XmtTime: 450 ms   DetectTime: 3150 ms
    Xmtpkts: 212    Last Tx interval: 337ms  min/max/avg: 337ms/446ms/396ms
    Rcvpkts: 212    Last Rx interval: 409ms  min/max/avg: 337ms/446ms/396ms
```