BFD

Summary

Bidirectional Forwarding Detection (BFD) is a low-overhead and short-duration protocol intended to detect faults in the bidirectional path between two forwarding engines, including physical interfaces, sub-interfaces, data link(s), and to the extent possible the forwarding engines themselves, with potentially very low latency. It operates independently of media, data protocols, and routing protocols.

BFD is basically a hello protocol for checking bidirectional neighbor reachability. It provides sub-second link failure detection support. BFD is not routing protocol specific, unlike protocol hello timers or such.

BFD Control packets are transmitted in UDP packets with destination port 3784, BFD also uses port 4784 for multihop paths. The source port is in the range 49152 through 65535. And BFD Echo packets are encapsulated in UDP packets with destination port 3785.

Standards and Technologies:

- RFC 5880 Bidirectional Forwarding Detection (BFD)
- RFC 5881 BFD for IPv4 and IPv6
- RFC 5882 Generic Application of BFD
- RFC 5883 Bidirectional Forwarding Detection (BFD) for Multihop Paths

Features not yet supported

- echo mode
- enabling BFD for ip route gateways
- authentication

Configuration

Allowing or forbidding BFD sessions can be done from the `/routing bfd configuration` menu. For example:

```
/routing bfd configuration
add interfaces=sfp12 forbid-bfd=yes
add interfaces=static
```

Configuration entries are order sensitive, which means that in the example above we are forbidding BFD sessions explicitly on the "sfp12" interface and allowing on the rest of the interfaces belonging to the "static" interface list.

To be able to filter multi-hop sessions, `addresses` or `address-list` properties can be used to match the destination, as well as the appropriate VRF, if a session is not running in the "main" VRF.

```
/ip firewall address-list
add address=10.155.255.183 list=bgp_allow_bfd
add address=10.155.255.217 list=bgp_allow_bfd

/routing bfd configuration
add addresses=111.111.0.0/16 vrf=vrf1
add address-list=bgp_allow_bfd
```

Everything else that is not explicitly listed in the configuration by default is forbidden.

BFD with BGP

To enable the use of BFD for BGP sessions, enable `use-bfd` for required entries in `/routing bgp connection` menu.

A useful feature is that the BGP session will show that the BFD session for that particular BGP session is down:

```
[admin@dr_02_BGP_MUM] /routing/bgp/session> print
Flags: E - established
 0 E ;;; BFD session down
     name="ovpn_test1-1"
     remote.address=111.111.11.11@vrf1 .as=65530 .id=10.155.101.217
     .capabilities=mp,rr,as4 .hold-time=infinity .messages=40717
     .bytes=3436281 .eor=""
     local.address=111.111.11.12@vrf1 .as=555 .id=111.111.11.12
     .capabilities=mp,rr,gr,as4 .messages=1 .bytes=19 .eor=""
     output.procid=20
     input.procid=20 .filter=bgp-in ebgp
     hold-time=infinity use-bfd=yes uptime=3s210ms
     last-started=2023-05-19 09:54:04 prefix-count=3853
```

BFD with OSPF

To enable the use of BFD for OSPF neighbors, enable `use-bfd` for required entries in `/routing ospf interface-template` menu.

Session Status

The status of the currently available sessions can be observed from `/routing bfd session` menu:

```
[admin@dr_02_BGP_MUM] /routing/bfd/session> print
Flags: U - up, I - inactive
 0 I ;;; BFD forbidden for destination address
     multihop=yes remote-address=10.155.101.183 local-address="" desired-tx-interval=0ms required-min-rx=0ms
     multiplier=0

 1   multihop=no remote-address=111.111.11.11%ovpn-out1@vrf1 local-address=111.111.11.12@vrf1 state=down
     state-changes=0 desired-tx-interval=200ms required-min-rx=200ms remote-min-rx=1us multiplier=5
     packets-rx=0 packets-tx=7674
```

BFD is picking the highest value between the local tx interval and remote minimum rx interval as desired transmit interval. If the session is not established then desired minimum tx interval is set to 1 second.