Network Working Group
Internet Draft

D. Katz
Juniper Networks
D. Ward
Cisco Systems

Expires: September, 2007

March, 2007

BFD for IPv4 and IPv6 (Single Hop)
draft-ietf-bfd-v4v6-1hop-06.txt

Status of this Memo

Abstract

This document describes the use of the Bidirectional Forwarding Detection protocol over IPv4 and IPv6 for single IP hops. Comments on this draft should be directed to rtg-bfd@ietf.org.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [KEYWORDS].

1. Introduction

One very desirable application for BFD [BFD] is to track IPv4 and IPv6 connectivity between directly-connected systems. This could be used to supplement the detection mechanisms in routing protocols, or to monitor router-host connectivity, among other applications.

This document describes the particulars necessary to use BFD in this environment. Interactions between BFD and other protocols and system functions are described in the BFD Generic Applications document [BFD-GENERIC].

2. Applications and Limitations

This application of BFD can be used by any pair of systems communicating via IPv4 and/or IPv6 across a single IP hop that can be associated with an incoming interface. This includes, but is not limited to, physical media, virtual circuits, and tunnels.

Each BFD session between a pair of systems MUST traverse a separate path in both directions.

If BFD is to be used in conjunction with both IPv4 and IPv6 on a particular link, a separate BFD session MUST be established for each protocol (and thus encapsulated by that protocol) over that link.

3. Initialization and Demultiplexing

In this application, there will be only a single BFD session between two systems over a given interface (logical or physical) for a particular protocol. The BFD session must be bound to this interface. As such, both sides of a session MUST take the "Active" role (sending initial BFD Control packets with a zero value of Your Discriminator) and any BFD packet from the remote machine with a zero value of Your Discriminator MUST be associated with the session bound to the remote system, interface, and protocol.

4. Encapsulation

4.1. BFD for IPv4

In the case of IPv4, BFD Control packets MUST be transmitted in UDP packets with destination port 3784, within an IPv4 packet. The source port MUST be in the range 49152 through 65535. The same UDP source port number MUST be used for all BFD Control packets associated with a particular session. The source port number SHOULD be unique among all BFD sessions on the system. If more than 16384 BFD sessions are simultaneously active, UDP source port numbers MAY be reused on multiple sessions, but the number of distinct uses of the same UDP source port number SHOULD be minimized. An implementation MAY use the UDP port source number to aid in demultiplexing incoming BFD Control packets, but ultimately the mechanisms in [BFD] MUST be used to demultiplex incoming packets to the proper session.

BFD Echo packets MUST be transmitted in UDP packets with destination UDP port 3785 in an IPv4 packet. The setting of the UDP source port is outside the scope of this specification. The destination address MUST be chosen in such a way as to cause the remote system to forward the packet back to the local system. The source address MUST be

chosen in such a way as to preclude the remote system from generating ICMP Redirect messages. In particular, the source address MUST NOT be part of the subnet bound to the interface over which the BFD Echo packet is being transmitted.

4.2. BFD for IPv6

In the case of IPv6, BFD Control packets MUST be transmitted in UDP packets with destination port 3784, within an IPv6 packet. The source port MUST be in the range 49152 through 65535. The same UDP source port number MUST be used for all BFD Control packets

associated with a particular session. The source port number SHOULD be unique among all BFD sessions on the system. If more than 16384 BFD sessions are simultaneously active, UDP source port numbers MAY be reused on multiple sessions, but the number of distinct uses of the same UDP source port number SHOULD be minimized. An implementation MAY use the UDP port source number to aid in demultiplexing incoming BFD Control packets, but ultimately the mechanisms in [BFD] MUST be used to demultiplex incoming packets to the proper session.

BFD Echo packets MUST be transmitted in UDP packets with destination UDP port 3785 in an IPv6 packet. The setting of the UDP source port is outside the scope of this specification. The source and destination addresses MUST both be associated with the local system. The destination address MUST be chosen in such a way as to cause the remote system to forward the packet back to the local system.

5. TTL/Hop Count Issues

If BFD authentication is not in use on a session, all BFD Control packets for the session MUST be sent with a TTL or Hop Count value of 255. All received BFD Control packets that are demultiplexed to the session MUST be discarded if the received TTL or Hop Count is not equal to 255. A discussion of this mechanism can be found in [GTSM].

If BFD authentication is in use on a session, all BFD Control packets MUST be sent with a TTL or Hop Count value of 255. All received BFD

Control packets that are demultiplexed the session MAY be discarded if the received TTL or Hop Count is not equal to 255.

In the context of this section, "authentication in use" means that the system is sending BFD control packets with the Authentication bit set and with the Authentication Section included, and that all unauthenticated packets demultiplexed to the session are discarded, per the BFD base specification.

6. Addressing Issues

On a subnetted network, BFD Control packets MUST be transmitted with source and destination addresses that are part of the subnet (addressed from and to interfaces on the subnet.)

On an addressed but unsubnetted point-to-point link, BFD Control packets MUST be transmitted with source and destination addresses that match the addresses configured on that link.

On an unnumbered point-to-point link, the source address of a BFD Control packet MUST NOT be used to identify the session. This means that the initial BFD packet MUST be accepted with any source address, and that subsequent BFD packets MUST be demultiplexed solely by the My Discriminator field (as is always the case.) This allows the source address to change if necessary. If the received source address changes, the local system MUST NOT use that address as the destination in outgoing BFD Control packets; rather it MUST continue to use the address configured at session creation. An implementation MAY notify the application that the neighbor's source address has changed, so that the application might choose to change the destination address or take some other action. Note that the TTL/Hop

Count check described in section 5 (or the use of authentication) precludes the BFD packets from having come from any source other than the immediate neighbor.

7. BFD for use with Tunnels

A number of mechanisms are available to tunnel IPv4 and IPv6 over arbitrary topologies. If the tunnel mechanism does not decrement the TTL or hop count of the network protocol carried within, the mechanism described in this document may be used to provide liveness detection for the tunnel. The BFD Authentication mechanism SHOULD be used and is strongly encouraged.

Normative References

[BFD] Katz, D., and Ward, D., "Bidirectional Forwarding Detection", draft-ietf-bfd-base-06.txt, March, 2007.

[BFD-GENERIC] Katz, D., and Ward, D., "Generic Application of BFD", draft-ietf-bfd-generic-03.txt, March, 2007 .

[GTSM] Gill, V., et al, "The Generalized TTL Security Mechanism (GTSM)", RFC 3682, February 2004.

[KEYWORD] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

Security Considerations

In this application, the use of TTL=255 on transmit and receive is viewed as supplying equivalent security characteristics to other protocols used in the infrastructure, as it is not trivially spoofable. The security implications of this mechanism are further discussed in [GTSM].

The security implications of the use of BFD Authentication are discussed in [BFD].

The use of the TTL=255 check simultaneously with BFD Authentication provides a low overhead mechanism for discarding a class of unauthorized packets and may be useful in implementations in which cryptographic checksum use is susceptable to denial of service attacks. The use or non-use of this mechanism does not impact interoperability.

IANA Considerations

This document has no actions for IANA.

Authors' Addresses

Dave Katz
Juniper Networks
1194 N. Mathilda Ave.
Sunnyvale, California 94089-1206 USA
Phone: +1-408-745-2000
Email: dkatz@juniper.net

Dave Ward
Cisco Systems
170 W. Tasman Dr.
San Jose, CA 95134 USA
Phone: +1-408-526-4000
Email: dward@cisco.com

Changes from the previous draft

This is a reissue of the previous version. There are only minor editorial changes.

IPR Disclaimer

Full Copyright Notice

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

This document expires in September, 2007.