Network Working Group
Internet Draft

D. Katz
Juniper Networks
D. Ward
Cisco Systems

Category: Informational
June, 2003
Expires: December, 2003

Bidirectional Forwarding Detection
draft-katz-ward-bfd-00.txt

Status of this Memo

Copyright Notice

Abstract

This document describes a protocol intended to detect faults in the bidirectional path between two forwarding engines, including 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.

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

An increasingly important feature of networking equipment is the rapid detection of communication failures between adjacent systems, in order to more quickly establish alternative paths. Currently, detection can come fairly quickly in certain circumstances when data link hardware comes into play (such as SONET alarms.) However, there are media that do not provide this kind of signaling (such as Ethernet), and some media may not detect certain kinds of failures in the path, for example, failing interfaces or forwarding engine components.

Networks use relatively slow "Hello" mechanisms, usually in routing protocols, to detect failures when there is no hardware signaling to help out. The detection times available in the existing protocols are no better than a second, which is far too long for some applications and represents a great deal of lost data at gigabit rates. Furthermore, routing protocol Hellos are of no help when those routing protocols are not in use, and the semantics of detection are subtly different--they detect a failure in the path between the two routing protocol engines.

The goal of BFD is to provide low-overhead, short-duration detection of failures in the path between adjacent forwarding engines, including the interfaces, data link(s), and to the extent possible the forwarding engines themselves.

2. Design

BFD is designed to detect failures in communication with a data plane next hop. It is intended to be implemented in some component of the forwarding engine of a system, in cases where the forwarding and control engines are separated. This not only binds the protocol more to the data plane, but decouples the protocol from the fate of the routing protocol engine (making it useful in concert with various "graceful restart" mechanisms for those protocols.)

BFD operates on top of any data protocol being forwarded between two systems. It is always run in a unicast, point-to-point mode.

BFD can provide failure detection on any kind of path between systems, including direct physical links, virtual circuits, tunnels, MPLS LSPs, multihop routed paths, and unidirectional links (so long as there is some return path, of course.) Multiple BFD sessions can be established between the same pair of systems when multiple paths between them are present in at least one direction, even if the same path is used in one direction.

The BFD state machine implements a three-way handshake, both when establishing a BFD session and when tearing it down for any reason, to ensure that both systems are aware of the state change.

3. Protocol Overview

BFD is a simple, fixed-field, hello protocol that in many respects is similar to the detection components of well-known routing protocols. A pair of systems transmit BFD packets periodically over each path between the two systems, and if a system stops receiving BFD packets for long enough, some component in that particular bidirectional path to the neighboring system is assumed to have failed.

A path is only declared to be operational when two-way communication has been established between systems (though this does not necessarily mean that a bidirectional link must be used.)

A separate BFD session is created for each communications path and data protocol in use between two systems.

Each system estimates how quickly it can send and receive BFD packets in order to come to an agreement with its neighbor about how rapidly detection of failure will take place. These estimates can be modified in real time in order to adapt to unusual situations. This design also allows for fast systems on a shared medium with a slow

system to be able to more rapidly detect failures between the fast systems while allowing the slow system to participate to the best of its ability.

BFD can operate in two different modes. The first mode is known as Asynchronous mode. In this mode, each system sends a series of BFD Control packets to one another, and if a number of those packets in a row are not received by the other system, the session is declared to be down.

The second mode is known as Echo mode. In echo mode, BFD Control packets are sent at a relatively sedate rate, and additionally streams of BFD Echo packets are transmitted in each direction in such a way as to have the other system loop them back through its forwarding path. If a number of packets in a row of either the control stream or the echoed data stream are not received, the session is declared to be down.

Asynchronous mode is advantageous in that it requires half as many packets to achieve a particular detection time as does Echo mode. It is also used when Echo mode cannot be supported for some reason.

Echo mode has the advantage of truly testing only the forwarding path on the remote system, which may reduce round-trip jitter and thus allow more aggressive detection times, as well as potentially detecting some classes of failure that might not otherwise be detected.

Echo mode is enabled only when both systems signal that they are willing to do so.

4. Protocol Details

BFD packets are carried as the payload of whatever encapsulating protocol is appropriate for the medium and network. Note that many of the exact mechanisms are implementation dependent and will not affect interoperability, and are thus outside the scope of this specification. Those issues are so noted.

4.1. Timer Model

A timer is an entity that will measure an interval of time and provide a notification when that time period expires. It has two states, running and disarmed. A disarmed timer will not expire, whereas a running timer will expire after the specified interval. A

running timer can be restarted prior to its expiration to any interval; it will then not expire until the new interval has passed.

Some timers may be jittered. This is a process where a random value is subtracted from the interval (expressed as a percentage of the interval) when the timer is started. Jitter is used to avoid the self-synchronization of nominally independent timers.

4.2. State

BFD requires that a set of state elements be maintained for each session with neighboring systems. The creation of this state is outside the scope of this specification. This state description is not intended to define implementation; any equivalent method can be used.

st.SourceAddress

The source address information used when transmitting BFD Control packets for this session, appropriate to the environment. The setting of this value is outside the scope of this specification.

st.DestinationAddress

The destination address information used when transmitting BFD Control packets for this session, appropriate to the environment. The setting of this value is outside the scope of this specification.

st.EchoSourceAddress

The source address information used when transmitting BFD Echo packets for this session, appropriate to the environment, if Echo mode is supported. This address MUST be an address associated with the transmitting system, and MAY be part of a subnet other than the one over which the packet is being sent (in order to avoid the transmission of ICMP Redirects.) The setting of this value is otherwise outside the scope of this specification.

st.EchoDestinationAddress

The destination address information used when transmitting BFD Echo packets for this session, appropriate to the environment.

This address MUST be an address associated with the transmitting system, SHOULD be an address for which the remote system will route packets back on the interface over which they are received, and SHOULD be part of the subnet over which the packet is being sent (if the link is subnetted.) The setting of this value is otherwise outside the scope of this specification.

st.LocalDiscr

The local discriminator for this BFD session, used to uniquely identify it. It MUST be unique on this system, and nonzero. The value is otherwise outside the scope of this specification.

st.RemoteDiscr

The remote discriminator for this BFD session. This is the discriminator chosen by the remote system, and is totally opaque to the local system. This MUST be initialized to zero.

st.RemoteHeard

This field is set to 1 if the local system is actively receiving BFD packets from the remote system, and is set to 0 if the local system has not received BFD packets recently (within the detection time) or if the local system is attempting to tear down the BFD session. This MUST be initialized to zero.

st.SessionState

The perceived state of the session (Init, Up, Failing, or Down.) The exact action taken when the session state changes is outside the scope of this specification, though it is expected that this state change (particularly to and from Up state) is reported to other components of the system. This MUST be initialized to Down.

st.EchoModeDesired

A boolean stating whether or this system wishes to use Echo mode. The setting of this value is outside the scope of this specification.

st.EchoModeActive

A boolean tracking whether or not Echo mode is active. This MUST be initialized to FALSE.

st.LocalSessionDiagnostic

A diagnostic code specifying the reason the local session state most recently transitioned from Up to some other state. This MUST be initialized to zero.

st.RemoteSessionDiagnostic

A diagnostic code specifying the reason the remote session state most recently transitioned from Up to some other state. This MUST be initialized to zero.

st.DesiredMinAsyncTXInterval

The minimum interval, in microseconds, between transmitted BFD Control packets that this system would like to use while operating in Asynchronous mode when the session is up. The actual interval is negotiated between the two systems. This value MUST be nonzero, and is otherwise outside the scope of this specification.

st.DesiredMinSlowTXInterval

The minimum interval, in microseconds, between transmitted BFD Control packets that this system would like to use while operating in Echo mode, or when the session is not up. The actual interval is negotiated between the two systems. This value MUST be nonzero, and is otherwise outside the scope of this specification, though it is suggested that this value SHOULD be at least one second (1,000,000 usec.)

st.DesiredMinEchoTXInterval

The minimum interval, in microseconds, between transmitted BFD Echo packets that this system would like to use while operating in Echo mode. The actual interval is negotiated between the two systems. If Echo mode is supported, this value MUST be nonzero, and is otherwise outside the scope of this specification.

st.DesiredMinTXInterval

The minimum interval, in microseconds, between transmitted BFD Control packets that this system would like to use at the current time. The actual interval is negotiated between the two systems. This is set to either st.DesiredMinSlowTXInterval or st.DesiredMinAsyncTXInterval depending on the session state. This value MUST be initialized to st.DesiredMinSlowTXInterval.

st.RequiredMinRXInterval

The minimum interval, in microseconds, between received BFD Control packets that this system requires. The setting of this value is outside the scope of this specification.

st.RequiredMinEchoRXInterval

The minimum interval, in microseconds, between received BFD Echo packets that this system requires. If this system supports Echo mode, this value MUST be nonzero. If this system does not support Echo mode this value MUST be zero. The setting of this value is otherwise outside the scope of this specification.

st.TxInterval

The agreed BFD Control packet transmission interval, in microseconds, for this session. This MUST be initialized to st.DesiredMinTXInterval. Note that an independent transmit interval may be used in each direction for a single BFD session.

st.EchoTxInterval

The agreed BFD Echo packet transmission interval, in microseconds, for this session. This MUST be initialized to zero. Note that an independent transmit interval may be used in each direction for a single BFD session.

st.DetectMult

The desired detect time multiplier for BFD Control packets. The negotiated Control packet transmission interval, multiplied by this value, will be the detection time for this session (as seen by the remote system.) This value MUST be a nonzero integer, and is otherwise outside the scope of this specification.

st.EchoDetectMult

The desired detect time multiplier for BFD Echo packets. The negotiated Echo packet transmission interval, multiplied by this value, will be the detection time for this session (as seen by the local system.) This value MUST be a nonzero integer, and is otherwise outside the scope of this specification.

st.DetectionTime

The detection time of the failure of this BFD session by virtue of missing BFD Control packets, as seen by the local system, in microseconds. It MUST be initialized to zero. Note that each system determines its own detection time, and the values for each system may not be the same.

st.DetectTimer

This timer is used to keep track of session liveness by tracking the arrival of BFD Control packets. It MUST be initialized to the disarmed state. When it expires, the session is deemed to have failed.

st.EchoDetectionTime

The detection time of the failure of this BFD session by virtue of missing BFD Echo packets, as seen by the local system, in microseconds. It MUST be initialized to zero. Note that each system determines its own detection time, and the values for each system may not be the same.

st.EchoDetectTimer

This timer is used to keep track of session liveness by tracking the arrival of BFD Echo packets. It MUST be initialized to the disarmed state. When it expires, the session is deemed to have failed.

st.TransmissionTimer

This timer triggers the transmission of a BFD Control packet. It MUST be initialized to the running state, with an interval of st.DesiredMinSlowTxInterval. A jitter of 25% SHOULD be applied to

this timer.

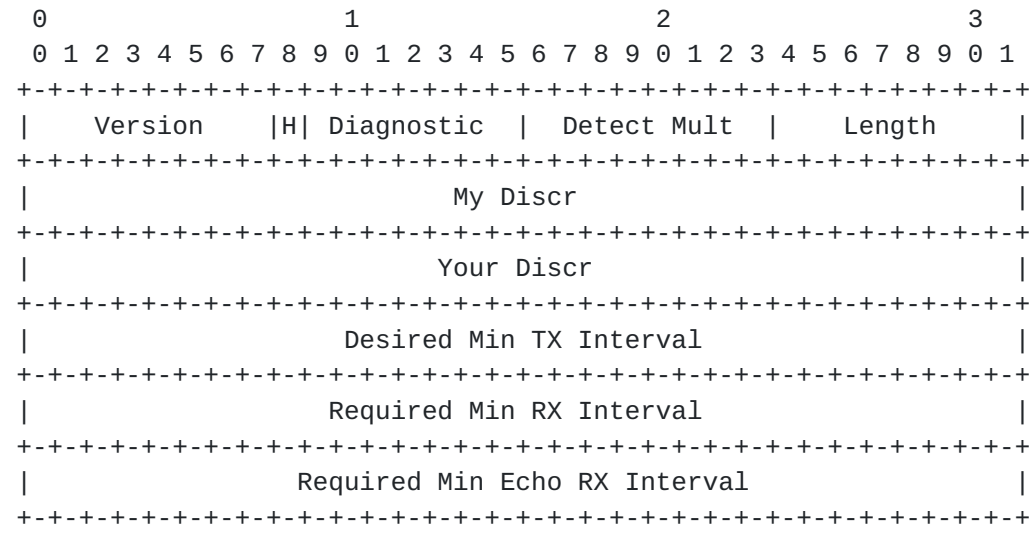
st.EchoTransmissionTimer

This timer triggers the transmission of a BFD Echo packet. It MUST be initialized to the disarmed state. A jitter of 25% SHOULD be applied to this timer.

4.3. BFD Control Packet Format

BFD Control packets are sent in an encapsulation appropriate to the environment. See "Encapsulation Specifics" below for the specifics of particular environments.

The payload of a BFD Control packet has the following format:



Version

The version number of the protocol. This document defines protocol version 0.

I Hear You (H)

This bit is set to 0 if the transmitting system either is not receiving BFD packets from the remote system, or is in the process of tearing down the BFD session for some reason (see the Elements of Procedure below for more details.)

Diagnostic

A diagnostic code specifying the local system's reason for the last transition of the session from Up to some other state. Values are:

0 -- No diagnostic
1 -- Control Detection time expired
2 -- Echo Detection time expired
3 -- Neighbor signaled session down
4 -- Forwarding plane reset

Detect Mult

Detect time multiplier. The negotiated transmission interval, multiplied by this value, provides the detection time for the transmitting system.

Length

Length of the BFD Control packet, in bytes.

My Discr

A unique, nonzero discriminator value generated by the transmitting system, used to demultiplex multiple BFD sessions between the same pair of systems.

Your Discr

The discriminator received from the corresponding remote system. This field reflects back the received value of My Discr, or is zero if that value is unknown.

Desired Min TX Interval

This is the minimum interval, in microseconds, that the local system would like to use when transmitting BFD Control packets.

Required Min RX Interval

This is the minimum interval, in microseconds, between received

BFD Control packets that this system is capable of supporting.

Required Min Echo RX Interval

This is the minimum interval, in microseconds, between received BFD Echo packets that this system is capable of supporting. If this value is zero, the transmitting system does not support BFD Echo packets.

4.4. BFD Echo Packet Format

BFD Echo packets are sent in an encapsulation appropriate to the Environment. See "Encapsulation Specifics" below for the specifics of particular environments.

The payload of a BFD Echo packet is a local matter, since only the sending system ever looks over the content. The only requirement is that sufficient information is included to demultiplex the received packet to the correct BFD session.

4.5. Elements of Procedure

4.5.1. Overview

A session begins with the periodic, slow transmission of BFD Control packets. When bidirectional communication is achieved (by virtue of the I Hear You field being nonzero, a three way handshake), the BFD session comes up.

If both systems signal that they can support Echo mode, they continue to send Control packets at the slow rate and start transmitting Echo packets at the negotiated rate.

The mechanism for detecting lost Echo packets and determining the detection time in Echo mode is outside of the scope of this specification. The only normative aspect of Echo packets is that they must not be sent more rapidly than the other system is willing to accept them (according to the advertised Required Min Echo Rx Interval.)

One possible mechanism for the handling of Echo mode is described herein. Note that if the round trip time to the remote system is greater than st.EchoDetectionTime, the algorithm described will falsely declare a session failure when Echo mode is first enabled. A system MAY decide not to negotiate Echo mode when the latency is high

relative to the detection time, or it MAY set st.EchoDetectTimer to a sufficiently large interval when it is first started (see TurnOnEchoMode below), or it MAY choose to use a different mechanism altogether (perhaps one that doesn't use timers at all) to determine whether Echo packets have not arrived. The determination of whether any of this is necessary is outside the scope of this specification.

If at least one system does not wish to or cannot support Echo mode, the systems instead send Control packets at a higher rate.

If the session fails, the transmission of Echo packets (if any) ceases, and the transmission of Control packets goes back to the slow rate.

4.5.2. Reception of BFD Control Packets

When a BFD Control packet is received, the following procedure MUST be followed, in the order specified:

If the version number is not correct (0), the packet MUST be discarded.

If the length field is less than the correct value (24), the packet MUST be discarded.

If the length field is greater than the payload of the encapsulating protocol, the packet MUST be discarded.

The appropriate BFD state block is selected based on some combination of source addressing information, the two discriminator fields, and by the interface over which the packet was received. The exact method for looking up a state block is outside the scope of this specification. If a matching session is not found, new state may be created, or the packet may be discarded. This choice is outside the scope of this specification.

If the value of st.RemoteDiscr is nonzero, it MUST match the value of My Discr. If it does not, the packet MUST be discarded.

If the value of Your Discr is nonzero, it MUST match the value of st.LocalDiscr. If it does not, the packet MUST be discarded.

If the value of st.RemoteDiscr is zero, set it to the value of My Discr.

If st.EchoModeActive is TRUE and the received Required Min Echo RX

```
Interval is zero, execute TurnOffEchoMode.

Set st.TxInterval to the greater of st.DesiredMinTxInterval and
the received Required Min Rx Interval.

Set st.EchoTxInterval to the greater of
st.DesiredMinEchoTXInterval and the received Required Min Echo Rx
Interval.

Set st.EchoDetectionTime to the value of st.EchoTxInterval
multiplied by the value of st.EchoDetectMult.

Set st.DetectionTime to the greater of st.RequiredMinRXInterval
and the received Desired Min TX Interval, multiplied by the
received Detect Multiplier.

(Re)start st.DetectTimer with an interval of st.DetectionTime.

Set st.RemoteSessionDiagnostic to the value of the received
Diagnostic.

If st.SessionState is Down
    Set st.RemoteHeard to 1
    If I Hear You is zero
        Set st.SessionState to Init
    Else
        Set st.SessionState to Up
        If st.EchoModeDesired is TRUE and Required Min Echo RX
          Interval is nonzero
            Execute TurnOnEchoMode

Else if st.SessionState is Init
    If I Hear You is nonzero
        Set st.SessionState to Up
        If st.EchoModeDesired is TRUE and Required Min Echo RX
          Interval is nonzero
            Execute TurnOnEchoMode

Else if st.SessionState is Up
    If I Hear You is zero
        Set st.LocalSessionDiagnostic to 3 (Neighbor signaled
          session down)
        Execute TakeDownSession

Else if st.SessionState is Failing
    If I Hear You is zero, set st.SessionState to Down
```

```
    TurnOffEchoMode:
        Set st.EchoModeActive to FALSE
        Disarm st.EchoDetectTimer
        Disarm st.EchoTransmissionTimer
        If st.SessionState is Up
            Set st.DesiredMinTxInterval to st.DesiredMinAsyncTXInterval
        Else
            Set st.DesiredMinTxInterval to st.DesiredMinSlowTxInterval


    TurnOnEchoMode:
        Set st.EchoModeActive to TRUE
        Set st.DesiredMinTxInterval to st.DesiredMinSlowTxInterval
        Start st.EchoDetectTimer with an interval of st.EchoDetectionTime.
          st.EchoDetectTimer MUST be started with an interval greater than
          the link round trip time;  if necessary, st.EchoDetectTimer MAY
          be started with a value greater than st.EchoDetectionTime.
        Start st.EchoTransmissionTimer with an interval of st.EchoTxInterval


    TakeDownSession:
        Disarm st.DetectTimer
        Set st.SessionState to Failing
        Set st.RemoteHeard to zero
        Execute TurnOffEchoMode
```

4.5.3. st.TransmissionTimer Expiration

When st.TransmissionTimer expires, send a BFD Control packet, and restart the timer with an interval of st.TxInterval. The packet is sent with a source address of st.SourceAddress and a destination address of st.DestinationAddress. The fields are set as follows:

Version

Set to the current version number (0).

I Hear You

Set to the value of st.RemoteHeard.

Diagnostic

Set to the value of st.LocalSessionDiagnostic.

Detect Mult

Set to the value of st.DetectMult.

My Discr

Set to st.LocalDiscr.

Your Discr

If st.SessionState is Init or Up, set to st.RemoteDiscr. Otherwise, set to zero.

Desired Min TX Interval

Set to st.DesiredMinTXInterval.

Required Min RX Interval

Set to st.RequiredMinRXInterval.

Required Min Echo RX Interval

Set to st.RequiredMinEchoRXInterval.

4.5.4. Reception of BFD Echo Packets

The processing of received Echo packets is outside of the scope of this specification. However, when a BFD Echo packet is received, the following procedure MAY be followed, in the order specified:

The appropriate BFD state block is selected based on some combination of source addressing information, data placed in the payload of the Echo packet, and the interface over which the packet was received. If a matching session is not found, discard the packet.

If st.EchoModeActive is FALSE, discard the packet.

Restart st.EchoDetectTimer with an interval of st.EchoDetectionTime.

4.5.5. st.EchoTransmissionTimer Expiration

When st.EchoTransmissionTimer expires, a BFD Echo packet MUST sent, and the timer MUST be restarted with an interval of st.EchoTxInterval. The packet is sent with a source address of st.EchoSourceAddress and a destination address of st.EchoDestinationAddress. The contents of the packet are outside the scope of this specification.

4.5.6. st.DetectTimer Expiration

When st.DetectTimer expires, set st.LocalSessionDiagnostic to 1 (Control Detection time expired), set st.RemoteDiscr to zero, and execute TakeDownSession.

4.5.7. st.EchoDetectTimer Expiration

When st.EchoDetectTimer expires, set st.LocalSessionDiagnostic to 2 (Echo Detection time expired), and execute TakeDownSession.

4.5.8. Min Rx Interval Change

When it is desired to change the rate at which BFD Control packets arrive from the remote system, st.RequiredMinRxInterval can be changed at any time to any value. The new value will be transmitted at the next st.TransmissionTimer expiration, and the remote system will adjust accordingly.

4.5.9. Min Tx Interval Change

When it is desired to change the rate at which BFD Control packets are transmitted to the remote system (subject to the requirements of the neighboring system), st.DesiredMinTxInterval can be changed at any time to any value. The new value will be transmitted at the next st.TransmissionTimer expiration. Note that st.TransmissionTimer should not be touched; it will pick up the new value (if any) at its next expiration. This is necessary when increasing the transmission interval to avoid an expiration of the neighbor's detection timer.

If the first packet containing a new, larger value of the interval is dropped, there is a chance that the detect timer will fire on the remote system and take down the BFD session. An implementation MAY continue to transmit BFD Control packets at the old, shorter interval for up to st.DetectMult packets before using the new, longer

interval.

4.5.10. Min Echo RX Interval Change

When it is desired to change the rate at which BFD Echo packets arrive from the remote system, st.RequiredMinEchoRxInterval can be changed at any time to any value. The new value will be transmitted at the next st.TransmissionTimer expiration, and the remote system will adjust accordingly.

4.5.11. Detect Multiplier Change

When it is desired to change the detect multiplier, the value of st.DetectMult can be changed to any nonzero value. The new value will be transmitted at the next st.TransmissionTimer expiration.

4.5.12. Forwarding Engine Reset

When the forwarding engine hardware is reset, set st.LocalSessionDiagnostic to 4 (Forwarding plane reset), and execute TakeDownSession.

4.5.13. Mode Change

If it is desired to switch between Async mode and Echo mode, this can be done at any time (assuming that both systems are capable of supporting Echo mode) by changing the value of st.RequiredMinEchoRXInterval to zero or nonzero accordingly. If Echo mode is enabled, Echo packets will be sent and the rate of Control packets will be reduced, and the opposite will happen if Echo mode is disabled.

4.6. Encapsulation Specifics

4.6.1. BFD for IPv4

In the case of IPv4, BFD Control packets are transmitted with source and destination UDP port <TBD1> in an IPv4 packet. The source and destination addresses MUST be associated with the local and remote systems, respectively.

BFD Echo packets are transmitted with source and destination UDP port <TBD2> in an IPv4 packet. 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.

4.6.2. BFD for IPv6

In the case of IPv6, BFD Control packets are transmitted with source and destination UDP port <TBD1> in an IPv6 packet. The source and destination addresses MUST be associated with the local and remote systems, respectively.

BFD Echo packets are transmitted with source and destination UDP port <TBD2> in an IPv6 packet. 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.

4.6.3. BFD for IEEE 802 Networks

BFD can also be used directly on top of the datalink layer in IEEE 802 networks. In this case, BFD packets are transmitted in an encapsulation appropriate for the particular IEEE 802 media, with Ether Type <TBD3>. The source and destination addresses MUST be unicast MAC addresses associated with the local and remote systems, respectively.

BFD Echo packets are transmitted in an encapsulation appropriate for the particular IEEE 802 media, with Ether Type <TBD4>. The source and destination addresses MUST both be unicast MAC addresses 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.

Note that BFD Echo mode is not likely to be appropriate for use directly over the data link layer, since most data link devices are not able to forward frames out the interface over which they were received.

Contributors

Kireeti Kompella and Yakov Rekhter of Juniper Networks were also significant contributors to this document.

Acknowledgments

This document was inspired by (and is intended to replace) the Protocol Liveness Protocol draft, written by Kireeti Kompella.

The authors would also like to thank Mike Shand, John Scudder, and Stewart Bryant for their substantive input.

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

Security Considerations

When BFD is run over network layer protocols, a significant denial-of-service risk is created, as BFD packets may be trivial to spoof. When the session is directly connected across a single link, the TTL MUST be set to the maximum on transmit, and checked to be equal to the maximum value on reception (and the packet dropped if this is not the case.) If BFD is run across multiple hops, some alternative mechanism MUST be used. One option would be to ensure that the network addresses used for BFD are not routable outside of the infrastructure in which BFD is running (and assuming there are no users connected within that network.) Another option would be to filter all packets carrying BFD's UDP ports at the edges of the network. Still another option would be to use cryptographic methods, though this is not likely to allow for very short detection times.

IANA Considerations

Two well-known UDP port numbers need to be assigned to this protocol.

IPR Notice

Full Copyright Notice

Acknowledgement

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