Configuring BFD with DHCP and Other Musings
draft-vinokour-bfd-dhcp-01

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."


This Internet-Draft will expire on November 10, 2008.

Abstract

This document defines a method for configuring Bidirectional Forwarding Detection (BFD) by an IP Edge device using DHCPv4 or DHCPv6. It provides motivation for the new functionality, defines new DHCP options to assist with the task and outlines the rules for configuring BFD on an IP endpoint for different network topologies. The document also discusses endpoint behavior upon BFD failure. Comments on this draft should be directed to rtg-bfd@ietf.org.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "MAY", "OPTIONAL", "MUST OR MAY", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY NOT", "NOT RECOMMENDED", "MUST NOT IF", and "SHALL NOT IF" are used in this document to describe Requirements Language. The word 'implementation' is used to distinguish amongst the configuration options available in an implementation, the configuration options that must be supported, and the configuration options that need not be supported.

These key words and their usage are borrowed from RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels".
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in RFC 2119 [RFC2119].

Table of Contents

1. Introduction ........................................... 3
2. BFD Provisioning on IP Endpoint .......................... 3
   2.1. New DHCP Options Inserted by Client .................. 4
   2.2. New DHCP Options Inserted by Server .................. 5
   2.3. BFD Configuration Parameters ........................ 7
   2.4. Operation with DHCP Relay Agent ..................... 9
3. BFD Provisioning and Management on IP Edge ............... 12
4. BFD and IP Address Lifecycle ............................ 13
   4.1. BFD and DHCPv4 Client States ....................... 13
   4.2. BFD and DHCPv6 Client .............................. 13
5. BFD Failure and DHCP Client .............................. 14
6. Other BFD Initialization Methods ........................ 14
7. IANA Considerations ..................................... 15
8. Security Considerations .................................. 15
9. Acknowledgements ......................................... 16
10. Normative References .................................... 16
Authors’ Addresses ......................................... 17

Intellectual Property and Copyright Statements ............... 18
1. Introduction

A particularly useful application for BFD [I-D.ietf-bfd-base] is to track IP connectivity between dynamically configured endpoints (e.g. hosts or CPE) and their IP Edge device (BRAS, BNG etc.) While IP connectivity is typically enabled on endpoints using DHCP [RFC2131] or DHCPv6 [RFC3315], there is currently no well-defined procedure for autoconfiguring BFD on IP devices to enable forwarding plane failure detection.

BFD runs over IPv4 or IPv6 and can only be initiated on dynamically configured endpoints after DHCP configuration is successfully completed, for two reasons. First, an endpoint lacks an IP address until configured by DHCP and thus can’t be identified by IP network and receive BFD packets. Second, an endpoint lacks knowledge of its peer IP devices (e.g. default gateway) and thus can’t send BFD packets to them.

The first reason suggests that BFD can not be started up until after unconfigured DHCP client obtains a valid network address. The second one implies that BFD requires configuration parameters supplied by DHCP for its operation. Thus, BFD startup must be coordinated with DHCP which also supplies BFD parameters. In short, BFD must be provisioned by DHCP on DHCP-configured endpoints.

In turn, BFD can be used to enhance behavior of DHCP client by notifying it about loss of IP connectivity with IP Edge. While DHCP client operation upon L2 link failure is well-defined and is designed to verify network configuration as soon as connectivity is restored, similar functionality is absent for loss of L3. Ability by a DHCP client to initiate negotiation upon detecting an IP connectivity failure can be very useful in broadband scenarios. The document discusses a BFD-based mechanism to that effect.

2. BFD Provisioning on IP Endpoint

BFD is a light-weight protocol that has no auto-bootstrapping facility and no discovery mechanism. It is fully reliant on a client application for configuration as described in [I-D.ietf-bfd-generic]. In current deployments, BFD is used in conjunction with routing protocols and is configured locally on both endpoints of the connection. In such scenarios applications or the operator configuring BFD are implicitly aware of BFD capabilities of the system and need neither discovery nor transport mechanism to bring up the protocol instance.

In contrast, supporting BFD auto-configuration on a remote host
requires a BFD bootstrapping application compliant with
[I-D.ietf-bfd-generic] to provide full BFD configuration to the host.
The application should also provide a mechanism for detecting BFD
capability of the host and supply BFD configuration that is
consistent with this capability. Such requirements on the
bootstrapping application stem from basic principles of BFD design
and are based on the premise that BFD never runs "standalone" but
always in the context of client applications.

No mechanism is currently defined for DHCP-assisted BFD configuration
on an IP endpoint. BFD can only be enabled if BFD parameters are
hard-wired (pre-provisioned) on a device or provided by some out-of-
band mechanism like the one specified in DSLF TR-069 [TR-069]. To
enable DHCP-based BFD bootstrapping, we suggest defining two sets of
DHCP options. Options in the first set (one for DHCPv4, one for
DHCPv6) is inserted by the client and advertise BFD capability of the
remote endpoint. Options in the second set would carry BFD specific
configuration parameters and allow DHCP client to bootstrap BFD
locally.

2.1. New DHCP Options Inserted by Client

Option TBD_1 MAY be used by DHCPv4 client in DHCPDISCOVER,
DHCPREQUEST or DHCPINFORM packets to advertise BFD support on an IP
endpoint. The format of the option TBD_1 is:

```
+-----------------+-----------------+-----------------+-----------------+
|     Code (TBD_1)   |   Length    |Vers |Reserved | Num Auth Types|
+-----------------+-----------------+-----------------+-----------------+
|       A1      |      A2       |  ...                          |
+-----------------+-----------------+-----------------+-----------------+
```

An equivalent option TBD_2 MAY be used by DHCPv6 client in SOLICIT,
REQUEST, CONFIRM, RENEW, REBIND, and INFORMATION_REQUEST packets to
advertise BFD support on an IP endpoint. The format of the option
TBD_2 is:

```
+-----------------+-----------------+-----------------+-----------------+
|     Code (TBD_2)   |   Length    |Vers |Reserved | Num Auth Types|
+-----------------+-----------------+-----------------+-----------------+
|       A1      |       A2   |  ...                                |
+-----------------+-----------------+-----------------+-----------------+
```
In both options TBD_1 and TBD_2 "Vers" stands for the version of BFD supported on the endpoint running DHCP client. BFD version should be currently set to 1 according to [I-D.ietf-bfd-base]. "Num Auth Types" is the number of BFD Authentication types supported by the IP endpoint. If client does not support BFD Authentication, the field MUST be set to 0. Finally, A1, A2, etc are the codes of BFD Authentication types supported by the endpoint as defined in [I-D.ietf-bfd-base].

2.2. New DHCP Options Inserted by Server

When a DHCPv4 packet containing option TBD_1 is received by a DHCPv4 server, the server MAY configure BFD on the endpoint running the client if it supports version of BFD requested by the client. If DHCP server cannot supply BFD configuration for BFD version that IP endpoint is running, the server SHOULD NOT configure BFD on the endpoint. To deliver BFD configuration to the endpoint, the server inserts option TBD_3 into DHCPOFFER and DHCPACK packets. The format of the option TBD_3 is:

```
| Code (TBD_3) | Length | Vers | E | R | C | A | D | Detect Mult |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Local Discriminator                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Desired Min TX Interval                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Required Min RX Interval                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Required Min Echo RX Interval              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Remote IP address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

If option TBD_1 specifies support for BFD Authentication, the server MAY supply an Authentication Section. The format of Authentication Section is as follows:
Here "Auth Len" is the length of Authentication Section and "Num Keys" is the number of authentication keys to be used during the session. Then follows the authentication key definition in a modified TLV format - in addition to Type an Authentication Key ID is provided for each key. Codes for Authentication types MUST be consistent with [I-D.ietf-bfd-base]. If Authentication Section is present it MUST immediately follow Remote IP Address field.

If "Num Auth Types" field in option TBD_1 is set to 0, the server SHOULD NOT supply Authentication Section in option TBD_3. The server SHOULD only configure Authentication types that the endpoint supports.

Likewise, when a DHCPv6 server receives a packet containing option TBD_2, it MAY choose to configure BFD on the endpoint if it supports version of BFD requested by the client. To deliver BFD configuration to the endpoint the server inserts option TBD_4 into ADVERTISE, REPLY, or RECONFIGURE packets. The format of the option TBD_4 is:
2.3. BFD Configuration Parameters

BFD parameters defined in options TBD_3 and TBD_4, along with recommended (default) values are as follows:

Vers is BFD version 1
Enable (E) 1
Role (R) is Active vs Passive Passive
Control Plane Independent Bit (C) 0
Authentication Present Bit (A) 0
Local Demand Mode Bit (D) 0
Detect Multiplier 3
Local Discriminator No default value
Desired Min TX Interval 10000 (ms)
Required Min RX Interval 1000 (ms)
Required Min Echo RX Interval 0 (ms)
Remote IP address No default value
Authentication data None

Definitions of all parameters (except for remote IP address) can be found in [I-D.ietf-bfd-base].

In order for BFD configuration in option TBD_3 or TBD_4 to be
accepted by an IP endpoint, BFD Version field MUST match BFD version supported by the endpoint and provided to DHCP server in option TBD_1 or TBD_2. If BFD versions do not match configuration MUST be discarded by the endpoint. Currently the version should be set to 1 according to [I-D.ietf-bfd-base].

Enable bit (E) set to 1 indicates that BFD on the endpoint SHOULD be enabled. If Enable bit is set to 0, BFD MUST NOT be initiated. If BFD is already running, it SHOULD be disabled.

Default values define an IP endpoint as a passive BFD peer running in Asynchronous mode without Authentication. Authentication Present Bit (A) set to 1 indicates the presence of the optional Authentication Section. Asynchronous mode is selected as default because Demand mode requires some mechanism outside of BFD to generate polls toward the peer. Numeric values of Detect Multiplier and Desired Min TX interval are selected as being consistent with PPP keepalive default values that are relevant for broadband scenarios. Required Min RX intervals are set to 1 second as sub-second detection times are not currently expected in broadband scenarios. The failure detection time of 3 seconds (given the suggested default Detect Multiplier value) on IP Edge would represent an order of magnitude improvement over the current industry default of 30s (the typical failure detection time for PPP).

Value 0 for Required min Echo RX Interval indicates that Echo mode is not supported by an endpoint. This reflects the expectation that Echo mode is not typically used in broadband scenarios.

C-bit value depends on BFD implementation on an endpoint; the default value of 0 assumes that the endpoint’s control plane and forwarding plane share fate.

Remote IP address cannot be initialized with a meaningful default value. As explained in Section 4 (Section 4), BFD operation is undefined until DHCP negotiation is completed at which point remote IP address will be set to a value extracted from option TBD_3 or TBD_4.

Authentication data is not supplied by default. If Authentication Section is present, IP endpoint MUST discard configuration for BFD Authentication types that it does not support.

Note that these parameters can be pre-provisioned or configured by some out-of-band mechanism as well as by DHCP. Therefore, precedence rules must be defined to resolve conflicts when a device is configured by several methods at once. Section 6 (Section 6) defines and discusses these rules.
When DHCP client receives DHCPACK with a properly formed option TBD_3, or REPLY or RECONFIGURE with a properly formed option TBD_4, the BFD parameters in the respective option MUST be used to initialize and start up BFD on the endpoint according to [I-D.ietf-bfd-base] and [I-D.ietf-bfd-v4v6-1hop] and using precedence rules specified in Section 6 (Section 6), provided Enable bit is set 1 and BFD version in the configuration matches BFD version supported by the endpoint. BFD state is initially set to Down, and destination IP address for BFD packets is set to the Remote IP address from option TBD_3 or TBD_4. Subsequent BFD operation on the endpoint is fully defined by BFD state machine as described in [I-D.ietf-bfd-base].

2.4. Operation with DHCP Relay Agent

In some deployments, IP Edge device serving as BFD endpoint is configured as a DHCPv4 relay agent. In this case, it may be preferable for an operator to program BFD endpoint configuration on the DHCP relay rather than the server. Relay agent can not insert BFD configuration into DHCP packets directly: the only manipulations a relay agent is allowed to perform on DHCP packets is setting giaddr and inserting relay-agent-info option. Therefore, in order to allow DHCP relay to provide an IP endpoint BFD configuration to the server, there is a need to extend the relay-agent-info option ([RFC3046]) with a new sub-option, the bfd-endpoint sub-option. The new sub-option has the same format as option TBD_3, except it employs a different code (TBD_5):

```
+-------------+-----------+-----------+-----------+----------+----------+
| 0           | 1         | 2         | 3         |
+-------------+-----------+-----------+-----------+----------+----------+
| Code (TBD_5)| Length    | Vers      | R|C|A|D|E|  Detect Mult |
|-------------+-----------+-----------+-----------+----------+----------+
| Local Discriminator | | | | | |
+-------------+-----------+-----------+-----------+----------+----------+
| Desired Min TX Interval | | | | | |
+-------------+-----------+-----------+-----------+----------+----------+
| Required Min RX Interval | | | | | |
+-------------+-----------+-----------+-----------+----------+----------+
| Required Min Echo RX Interval | | | | | |
+-------------+-----------+-----------+-----------+----------+----------+
| Remote IP address | | | | | |
```

The relay agent MAY insert the bfd-endpoint sub-option into DHCPDISCOVER or DHCPREQUEST packet from an IP endpoint if it would like the server to use its BFD configuration to configure BFD on the endpoint. If the server supports BFD provisioning and detects bfd-
endpoint sub-option it MUST use BFD configuration from the sub-option in option TBD_3 that it inserts into DHCPOFFER and DHCPACK packets.

DHCPv4 server MAY be configured to supply BFD configuration to the client only if bfd-endpoint sub-option is present in a DHCPDISCOVER or DHCPREQUEST packet. However, in a general case, the presence of the sub-option does not directly influence the server’s decision to insert option TBD_3 in a packet; rather it places a requirement on the content of the option if the server chooses to insert it. For example, whether or not bfd-endpoint sub-option is present in DHCPDISCOVER or DHCPREQUEST, the server MUST NOT insert option TBD_3 in DHCPOFFER or DHCPACK if option TBD_1 was not supplied by the client. This is consistent with usage of other sub-options of relay-agent-info option.

Below is a sample call flow with DHCPv4 relay agent:
Similarly, an operator may wish to program BFD endpoint configuration on a DHCPv6 relay agent rather than the server. To enable DHCPv6 server to use BFD endpoint configuration provided by a relay agent, the relay agent MAY insert option TBD_4 into RELAY_FORW packet that it sends to the server upon receiving SOLICIT, REQUEST, CONFIRM, RENEW, REBIND, or INFORMATION_REQUEST packet from an IP endpoint. If a server detects option TBD_4 in RELAY_FORW it MUST insert it unchanged into respective client message that is subsequently appended to RELAY_REPL packet, provided option TBD_2 is present in the original client packet. Relay agent then transparently passes ADVERTISE, REPLY, or RECONFIGURE message with embedded option TBD_4 to the client.

Below is a sample call flow with DHCPv6 relay agent:
DHCPv6 client / IP Endpoint
IP Edge acting as DHCPv6 relay

--SOLICIT ------> (TBD_2)
IP Edge inserts option TBD_4 into RELAY_FORW

--RELAY_FORW ----> (TBD_4, TBD_2 embedded in SOLICIT msg)
Server copies TBD_4 into RELAY message and inserts the RELAY into REPLY_REPL

<--REPLY --------> (TBD_4)
IP Edge extracts REPLY and relays it transparently to the client

<--RELAY_REPL--- (TBD_4 embedded in REPLY msg)
Server sends RELAY_REPL to IP Edge

--REQUEST -------> (TBD_2)
IP Edge inserts option TBD_4 into RELAY_FORW

<--RELAY_FORW ---> (TBD_2 + TBD_4)
Server copies TBD_4 into RELAY message and inserts the RELAY into REPLY_REPL

<--REPLY --------> (TBD_4)
IP Edge extracts REPLY and relays it transparently to the client

<--RELAY_REPL--- (TBD_4 embedded in REPLY msg)
Server sends RELAY_REPL to IP Edge

<--BFD poll------ IP Edge initiates BFD polling
--BFD response->

<BFD poll------
--BFD response->

3. BFD Provisioning and Management on IP Edge

BFD provisioning on IP Edge is not done via DHCP; it is a responsibility of IP Edge operator and is out of scope of this document. Likewise, DHCP is not responsible for configuring Remote IP address provided to IP endpoint in option TBD_3 or TBD_4 on IP Edge.

IP Edge is expected to be the active BFD peer (BFD role on the endpoint is Passive by default, see Section 2.3 (Section 2.3)). If BFD on an endpoint is provisioned via DHCP, IP Edge configured as DHCP server or relay agent can initiate BFD session with the endpoint immediately after completion of DHCP messaging. This is an
additional benefit of the DHCP based BFD configuration: any other provisioning method, e.g. via an ACS server ([TR-069]) is asynchronous with IP connectivity establishment between IP Edge and the endpoint and does not give IP Edge any an indication of BFD availability on the endpoint.

While DHCP module on IP Edge MAY assist with the timing of BFD session initiation, it is not a bootstrapping or management client of BFD. BFD does not inform DHCP server or relay of BFD failures and thus does not influence the state of IP address lease by the endpoint.

4. BFD and IP Address Lifecycle

4.1. BFD and DHCPv4 Client States

BFD can operate on an endpoint for as long as IP address lease by DHCP client is valid. If lease renewal fails for some reason and DHCPv4 client transitions to DHCP INIT state, BFD MUST be disabled. Subsequently, BFD can only be re-enabled upon successful DHCP renegotiation and DHCP transitioning into BOUND state.

BFD MAY be initiated by DHCP client upon its transitioning into BOUND state provided a valid option TBD_3 is received by the client in a DHCPv4 packet. BFD is disabled by DHCP client when the DHCPv4 client transitions into INIT state.

Thus, BFD can run on an IP endpoint configured by DHCP when DHCP client is in BOUND, RENEWING, REBINDING, INIT-REBOOT and REBOOTING states only. In DHCP INIT, SELECTING and REQUESTING states BFD operation is undefined.

4.2. BFD and DHCPv6 Client

DHCPv6 does not have a formal state machine like DHCPv4. Therefore, BFD operation on an IPv6 endpoint running DHCPv6 client is best described in relation to the lifecycle of IPv6 address lease. As with DHCPv4, BFD can only run on an IPv6 endpoint with a valid IPv6 address. If IP address lease expires BFD MUST be disabled. BFD MAY be enabled when a configuration with a valid IPv6 address is applied on the endpoint, provided BFD configuration is supplied in option TBD_4 or by some other means.

It is possible that IPv6 endpoints running DHCPv6 client use SLAAC to obtain their network address. Such endpoints could still use DHCPv6 for BFD configuration. Specifically, once an endpoint is configured with an IPv6 address, it MAY send an INFORMATION-REQUEST message with
an option TBD_2. Processing by the server or relay agent should be the same in this case as for a regular DHCPv6 client. The contents of Section 2 (Section 2) fully applies to this situation.

5. BFD Failure and DHCP Client

If BFD on an IP endpoint is configured using DHCP options TBD_3 or TBD_4, DHCP client is a client application of BFD in the sense of [I-D.ietf-bfd-generic]. Thus, BFD events, e.g. unplanned BFD failures SHOULD be reported to DHCP client. If BFD on an endpoint detects a planned failure, e.g. the BFD peer transition to AdminDown state, DHCP client SHOULD NOT be informed. Decision of whether or not to inform DHCP MAY be based on BFD Diag code.

Modern Access and Aggregation networks connecting dynamically configured endpoints and their IP Edge device can be quite complex and have non-trivial redundancy behavior designed to minimize service interruptions. Given that DHCP packets are often used for subscriber line authentication and session establishment, some self-healing network designs may rely on DHCP message exchange initiated upon connectivity interruption between IP Edge and an endpoint. However, DHCP exchanges initiated by DHCP servers are typically disallowed in broadband scenarios for security reasons and a mechanism informing DHCP client of IP connectivity loss with the network is currently missing.

BFD running on an endpoint provides such mechanism. Unplanned BFD failure on an endpoint indicates loss of IP connectivity with IP Edge. Therefore, indication of unplanned BFD failure can be used by DHCP client to react to interruptions in IP connectivity in the same way as is currently specified for L2 loss.

If IP endpoint is running DHCPv4 client, the client MAY transition into INIT-REBOOT state upon receiving a notification of BFD failure. If IP endpoint is running DHCPv6 client, the client MAY consider loss of BFD to be equivalent to loss of L2, and initiate a Confirm messages exchange as described in section 18.1.2 of [RFC3315]. The exact behavior of DHCP client upon receiving unplanned BFD failure notification is determined by the operator and is outside the scope of this document.

6. Other BFD Initialization Methods

BFD on an IP endpoint can be pre-provisioned or configured by mechanisms other than DHCP, e.g. manually or via ACS per DSLF TR-069 [TR-069]. As DHCP-based BFD configuration is initiated by the
endpoint using DHCP option TBD_1 or TBD_2, it is expected that, once this provisioning mode is selected, no other mechanisms to configure BFD will be used.

If BFD has been pre-provisioned on an IP endpoint, DHCP-based configuration SHOULD override pre-provisioned BFD configuration with the exception of Control Plane Independent (C) Bit. Proper setting of C bit requires knowledge of BFD implementation on the endpoint and thus pre-provisioned value is more reliable than the one supplied by DHCP. Likewise, BFD initialization information in option TBD_3 or TBD_4 SHOULD override any BFD configuration present on an IP endpoint at the time of DHCP negotiation, with the exception of C-bit, no matter what its origin is.

In particular, if Enable bit in the option TBD_3 or TBD_4 in a DHCP packet received by the endpoint is set to 0, BFD MUST NOT be initiated even if BFD configuration has been pre-provisioned by other means. In case BFD is already running by the time options TBD_3 or TBD_4 are received with Enable bit set to 0, BFD SHOULD be disabled no matter what the origin of its configuration is.

7.  IANA Considerations

This document requests IANA to allocate option and sub-option codes for newly defined DHCP options and sub-options as described in the text.

Note to RFC Editor: this section may be removed on publication as an RFC.

8.  Security Considerations

The configuration of BFD by DHCP is subject to the same security concerns as is the configuration of an endpoint by DHCP in general; these are outlined in [RFC2131]. Potentially, a malicious user snooping on DHCP interaction between IP Edge and an endpoint can retrieve BFD discriminator values and hijack the BFD session. This can lead to temporary disruption of IP connectivity for the endpoint.

In the networks with high security risk, BFD authentication SHOULD be enabled for BFD running between IP endpoints. To ensure security of authentication keys, DHCP messages containing options TBD_3 or TBD_4 with BFD authentication information MUST be authenticated using the procedures described in [RFC3118]. Messages failing the authentication should be silently discarded by the client.
An alternative DHCP based authentication mechanism has been proposed in [I-D.pruss-dhcp-auth-dsl]. The progress of that document in DHCP WG will be closely followed, and this draft will be updated accordingly.

9. Acknowledgements

Authors would like to thank Ralph Droms for reviewing the document prior to publication and providing many insightful comments.

10. Normative References

[I-D.ietf-bfd-base]

[I-D.ietf-bfd-generic]

[I-D.ietf-bfd-v4v6-1hop]

[I-D.pruss-dhcp-auth-dsl]


Authors’ Addresses

Vitali Vinokour
Cisco Systems
1414 Massachusetts Ave
Boxborough, MA  01719
USA

Phone: +1-978-936-0774
Fax:
Email: vvinokou@cisco.com

Dave Ward
Cisco Systems
170 W. Tasman Dr.
San Jose, CA  95134
USA

Phone: +1-408-526-4000
Fax:
Email: dward@cisco.com
URI:
Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.