

Network Working Group  
Internet Draft  
Expires: May 2008  
Intended Status: Informational

S. Poretsky  
Reef Point Systems

R. Papneja  
Isocore

J. Karthik  
S. Vapiwala  
Cisco Systems

November 2007

**Benchmarking Terminology for Protection Performance**  
**<[draft-ietf-bmwg-protection-term-03.txt](#) >**

Intellectual Property Rights (IPR) statement:

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](#).

Status of this Memo

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."

The list of current Internet-Drafts can be accessed at  
<http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at  
<http://www.ietf.org/shadow.html>.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document provides common terminology and metrics for benchmarking the performance of sub-IP layer protection mechanisms. The performance benchmarks are measured at the IP-Layer, so avoid dependence on specific sub-IP protection mechanisms. The benchmarks and terminology can be applied in methodology documents for different sub-IP layer

protection mechanisms such as Automatic Protection Switching (APS), Virtual Router Redundancy Protocol (VRRP), Stateful High Availability (HA), and Multi-Protocol Label Switching Fast Reroute (MPLS-FRR).

## Table of Contents

<a href="#">1. Introduction.....</a>	<a href="#">3</a>
<a href="#">2. Existing definitions.....</a>	<a href="#">4</a>
<a href="#">3. Test Considerations.....</a>	<a href="#">5</a>
<a href="#">3.1. Path.....</a>	<a href="#">5</a>
<a href="#">3.1.1. Path.....</a>	<a href="#">5</a>
<a href="#">3.1.2. Working Path.....</a>	<a href="#">6</a>
<a href="#">3.1.3. Primary Path.....</a>	<a href="#">6</a>
<a href="#">3.1.4. Protected Primary Path.....</a>	<a href="#">6</a>
<a href="#">3.1.5. Backup Path.....</a>	<a href="#">7</a>
<a href="#">3.1.6. Standby Backup Path.....</a>	<a href="#">8</a>
<a href="#">3.1.7. Dynamic Backup Path.....</a>	<a href="#">8</a>
<a href="#">3.1.8. Disjoint Paths.....</a>	<a href="#">8</a>
<a href="#">3.1.9. Shared Risk Link Group (SRLG).....</a>	<a href="#">9</a>
<a href="#">3.2. Protection.....</a>	<a href="#">9</a>
<a href="#">3.2.1. Protection Switching System.....</a>	<a href="#">9</a>
<a href="#">3.2.2. Link Protection.....</a>	<a href="#">10</a>
<a href="#">3.2.3. Node Protection.....</a>	<a href="#">10</a>
<a href="#">3.2.4. Path Protection.....</a>	<a href="#">10</a>
<a href="#">3.2.5. Backup Span.....</a>	<a href="#">11</a>
<a href="#">3.2.6. Protected Interface.....</a>	<a href="#">11</a>
<a href="#">3.3. Protection Switching.....</a>	<a href="#">12</a>
<a href="#">3.3.1. Failover Event.....</a>	<a href="#">12</a>
<a href="#">3.3.2. Failure Detection.....</a>	<a href="#">12</a>
<a href="#">3.3.3. Failover.....</a>	<a href="#">13</a>
<a href="#">3.3.4. Restoration.....</a>	<a href="#">13</a>
<a href="#">3.3.5. Reversion.....</a>	<a href="#">14</a>
<a href="#">3.4. Nodes.....</a>	<a href="#">14</a>
<a href="#">3.4.1. Protection-Switching Node.....</a>	<a href="#">14</a>
<a href="#">3.4.2. Non-Protection Switching Node.....</a>	<a href="#">14</a>
<a href="#">3.4.3. Failover Node.....</a>	<a href="#">15</a>
<a href="#">3.4.4. Merge Node.....</a>	<a href="#">15</a>
<a href="#">3.4.5. Point of Local repair (PLR).....</a>	<a href="#">16</a>
<a href="#">3.4.6. Head-end Failover Node.....</a>	<a href="#">16</a>
<a href="#">3.5. Benchmarks.....</a>	<a href="#">17</a>
<a href="#">3.5.1. Failover Packet Loss.....</a>	<a href="#">17</a>
<a href="#">3.5.2. Reversion Packet Loss.....</a>	<a href="#">17</a>
<a href="#">3.5.3. Failover Time.....</a>	<a href="#">18</a>
<a href="#">3.5.4. Reversion Time.....</a>	<a href="#">18</a>
<a href="#">3.5.5. Additive Backup Latency.....</a>	<a href="#">19</a>
<a href="#">3.6. Failover Time Calculation Methods.....</a>	<a href="#">19</a>
<a href="#">3.6.1. Time-Based Loss Method.....</a>	<a href="#">19</a>
<a href="#">3.6.2. Packet-Loss Based Method.....</a>	<a href="#">20</a>
<a href="#">3.6.3. Timestamp-Based Method.....</a>	<a href="#">21</a>
<a href="#">4. Acknowledgments.....</a>	<a href="#">22</a>
<a href="#">5. IANA Considerations.....</a>	<a href="#">22</a>
<a href="#">6. Security Considerations.....</a>	<a href="#">22</a>
<a href="#">7. References.....</a>	<a href="#">22</a>

8. Author's Address.....	<a href="#">23</a>
--------------------------	--------------------

Poretsky, Papneja, Karthik, Vapiwala      Expires May 2008      [Page 2]

## 1. Introduction

The IP network layer provides route convergence to protect data traffic against planned and unplanned failures in the internet. Fast convergence times are critical to maintain reliable network connectivity and performance. Technologies that function at sub-IP layers can be enabled to provide further protection of IP traffic by providing the failure recovery at the sub-IP layers so that the outage is not observed at the IP-layer. Such technologies includes High Availability (HA) stateful failover. Virtual Router Redundancy Protocol (VRRP), Automatic Link Protection (APS) for SONET/SDH, Resilient Packet Ring (RPR) for Ethernet, and Fast Reroute for Multi-Protocol Label Switching (MPLS-FRR) [8].

Benchmarking terminology have been defined for IP-layer route convergence [7]. New terminology and methodologies specific to benchmarking sub-IP layer protection mechanisms are required. This will enable different implementations of the same protection mechanisms to be benchmarked and evaluated. In addition, different protection mechanisms can be benchmarked and evaluated. The metrics for benchmarking the performance of sub-IP protection mechanisms are measured at the IP layer, so that the results are always measured in reference to IP and independent of the specific protection mechanism being used. The purpose of this document is to provide a single terminology for benchmarking sub-IP protection mechanisms. It is intended that there can exist unique methodology documents for each sub-IP protection mechanism. The sequence of events is as follows:

1. Failover Event - Primary Path fails
2. Failure Detection- Failover Event is detected
3. Failover - Backup Path becomes the Working Path due to Failover Event
4. Restoration - Primary Path recovers from a Failover Event
5. Reversion (optional) - Primary Path becomes the Working Path

These terms are further defined in this document. Figure 1 shows the fundamental model that is to be used in benchmarking sub-IP protection mechanisms. A Protection Switching consists of a minimum of two Protection-Switching Nodes with a Primary Path and a Backup Path. A Failover Event occurs along the Primary Path. A Tester is set outside the two nodes as it sends and receives IP traffic along the Working Path. The Working Path is the Primary Path prior to the Failover Event and the Backup Path after the Failover Event. If Reversion is supported then the Working Path is the Primary Path after Restoration (Failure Recovery) of the Primary Path. The tester MUST record the IP packet sequence numbers, departure time, and arrival time so that the metrics of Failover Time, Additive Latency,

Packet Reordering, Duplicate Packets, and Reversion Time can be measured. The Tester may be a single device or a test system.

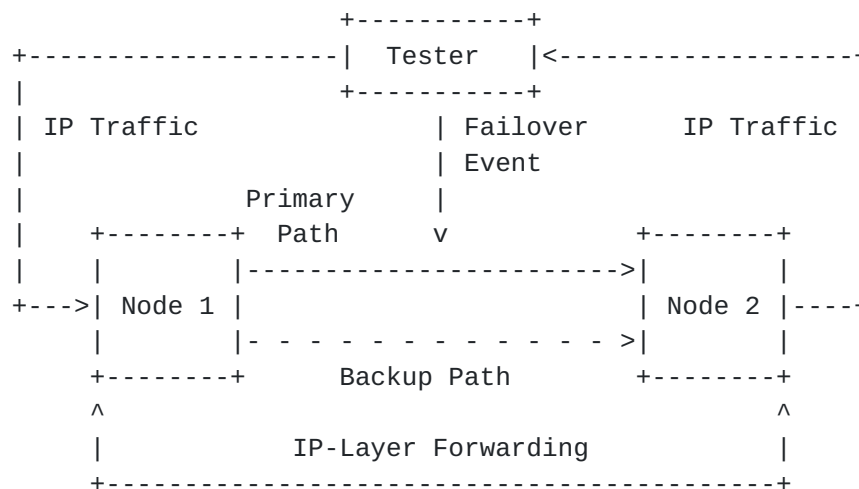


Figure 1. System Under Test (SUT) for Sub-IP Protection Mechanisms

## 2. Existing definitions

This document uses existing terminology defined in other BMWG work. Examples include, but are not limited to:

Latency	[Ref. <a href="#">[2]</a> , section 3.8]
Frame Loss Rate	[Ref. <a href="#">[2]</a> , section 3.6]
Throughput	[Ref. <a href="#">[2]</a> , section 3.17]
Device Under Test (DUT)	[Ref. <a href="#">[3]</a> , section 3.1.1]
System Under Test (SUT)	[Ref. <a href="#">[3]</a> , section 3.1.2]
Out-of-order Packet	[Ref. <a href="#">[4]</a> , section 3.3.2]
Duplicate Packet	[Ref. <a href="#">[4]</a> , section 3.3.3]
Forwarding Delay	[Ref. <a href="#">[4]</a> , section 3.2.4]
Jitter	[Ref. <a href="#">[4]</a> , section 3.2.5]
Packet Loss	[Ref. <a href="#">[7]</a> , Section 3.5]
Packet Reordering	[Ref. <a href="#">[10]</a> , section 3.3]

This document has the following frequently used acronyms:

DUT Device Under Test  
SUT System Under Test

This document adopts the definition format in [Section 2 of RFC 1242](#) [\[2\]](#).

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 [BCP 14](#), [RFC 2119](#) [\[5\]](#). [RFC 2119](#) defines the use of these key words to help make the intent of standards track documents as clear as possible. While this document uses these keywords, this document is not a standards track

document.

Poretsky, Papneja, Karthik, Vapiwala Expires May 2008 [Page 4]



### 3. Test Considerations

#### 3.1. Path

##### 3.1.1 Path

Definition:

A unidirectional sequence of nodes,  $\langle R1, \dots, Rn \rangle$ , and links  $\langle L12, \dots, L(n-1)n \rangle$  with the following properties:

- a.  $R1$  is the ingress node and forwards IP packets, which input into DUT/SUT, to  $R2$  as sub-IP frames over link  $L12$ .
- b.  $Ri$  is a node which forwards data frames to  $R[i+1]$  over Link  $Li[i+1]$  for all  $i$ ,  $1 < i < n$ , based on information in the sub-IP layer.
- c.  $Rn$  is the egress node and it outputs sub-IP frames from DUT/SUT as IP packets.

Discussion:

The path is defined in the sub-IP layer in this document, unlike an IP path in [RFC 2026](#) [1]. One path may be regarded as being equivalent to one IP link between two IP nodes, i.e.,  $R1$  and  $Rn$ . The two IP nodes may have multiple paths for protection. A packet will travel on only one path between the nodes. Packets belonging to a microflow [9] will traverse one or more paths. The path is unidirectional. Example paths are the SONET/SDH path and the label switched path for MPLS.

Measurement units:

n/a

Issues:

"A bidirectional path", which transmits traffic in both directions along the same nodes, consists of two unidirectional paths. Therefore, the two unidirectional paths belonging to "one bidirectional path" will be treated independently when benchmarking for "a bidirectional path".

See Also:



### 3.1.2. Working Path

Definition:

The path that the DUT/SUT is currently using to forward packets.

Discussion:

A Primary Path is the Working Path before occurrence of a Failover Event. A Backup Path becomes the Working Path after a Failover Event.

Measurement units:

n/a

Issues:

See Also:

Path  
Primary Path  
Backup Path

### 3.1.3. Primary Path

Definition:

The preferred path for forwarding traffic between two or more nodes.

Discussion:

Measurement units:

n/a

Issues:

None

See Also:

Path

### 3.1.4. Protected Primary Path

Definition:

A Primary Path that is protected with a Backup Path.

Discussion:

A Protected Primary Path MUST include at least one Protection Switching Node.

Measurement units:

n/a

Issues: None

See Also:

Path

Primary Path

### 3.1.5. Backup Path

Definition:

A path that exists to carry data traffic only if a Failover Event occurs on a Primary Path.

Discussion:

The Backup Path SHALL be the Working Path upon a Failover Event. A Path MAY have one or more Backup Paths. A Backup Path MAY protect one or more Primary Paths. There are various types of Backup Paths:

- a. dedicated recovery Backup Path (1+1), which has 100% redundancy for a specific ordinary path,
- b. shared Backup Path (1:N), which is dedicated to the protection for more than one specific Primary Path
- c. associated shared Backup Path (M:N) for which a specific set of Backup Paths protects a specific set of more than one Primary Path.

A Backup Path may be signaled or un signaled. The Backup Path MUST be created prior to the Failover Event. A new Path computed after the Failover Event is simply Convergence [\[7\]](#) to a new Primary Path.

Measurement units:

n/a

Issues:

See Also:

Path

Working Path

Primary Path



### 3.1.6. Standby Backup Path

Definition:

A Backup Path that is established prior to a Failover Event to protect a Primary Path.

Discussion:

Measurement units:

n/a

Issues:

See Also:

Path  
Working Path  
Primary Path  
Failover Event

### 3.1.7. Dynamic Backup Path

Definition:

A Backup Path that is established upon occurrence of a Failover Event.

Discussion:

Measurement units:

n/a

Issues:

See Also:

Path  
Working Path  
Primary Path  
Failover Event

### 3.1.8. Disjoint Paths

Definition:

A pair of paths is considered disjoint if they do not share a common link.

Discussions:

Paths that protect a segment of a path may merge beyond the segment being protected and are considered disjoint if they do not use a link from the set of links in the protected segment. A path is node disjoint if it does not share a

common node other than the ingress and egress.

Measurement units:

n/a

Issues:

See Also:

Path

Primary Path

SRLG

### 3.1.9. Shared Risk Link Group (SRLG)

Definition:

SRLG is a set of links which share a physical resource.

Discussion:

SRLG is considered the set of links to be avoided when the primary and secondary paths are considered disjoint. The SRLG will fail as a group if the shared resource fails.

Measurement units:

n/a

Issues: None

See Also:

Path

Primary Path

## 3.2. Protection

### 3.2.1. Protection Switching System

Definition:

A DUT/SUT that is capable of Failure Detection and Failover from a Primary Path to a Backup Path when a Failover Event occurs.

Discussion:

The Protection Switching System MUST have a Primary Path and a Backup Path. The Backup Path MAY be a Standby Backup Path or a dynamic Backup Path. The Protection Switching System includes the mechanisms for both Failure Detection and Failover.

Measurement units: n/a

Issues: None

See Also:



Primary Path  
Backup Path  
Failover

Poretsky, Papneja, Karthik, Vapiwala Expires May 2008 [Page 9]

### 3.2.2. Link Protection

Definition:

A Backup Path that is signaled to protect for failure of interfaces and links along a Primary Path.

Discussion:

Link Protection may or may not protect the entire Primary Path.

Measurement units: n/a

Issues: None

See Also:

Primary Path  
Backup Path

### 3.2.3. Node Protection

Definition:

A Backup Path that is signaled to protect for failure of interfaces, links and nodes along a Primary Path.

Discussion:

Node Protection may or may not protect the entire Primary Path. Node Protection also provides Link Protection.

Measurement units: n/a

Issues: None

See Also:

Link Protection

### 3.2.4. Path Protection

Definition:

A Backup Path that provides protection for the entire Primary Path.

Discussion:

Path Protection provides Node Protection and Link Protection for every node and link along the Primary Path. A Backup Path providing Path Protection MUST have the same ingress node as the Primary Path.

Measurement units: n/a

Issues: None

Poretsky, Papneja, Karthik, Vapiwala Expires May 2008 [Page 10]

See Also:

- Primary Path
- Backup Path
- Node Protection
- Link protection

#### 3.2.5. Backup Span

Definition:

The numbers of hop used by a Backup Path.

Discussion:

Measurement units: number of nodes

Issues: None

See Also:

- Primary Path
- Backup Path

#### 3.2.6 Protected Interface

Definition:

An interface along the Primary Path that is protected by a Backup Path

Discussion:

Measurement units: None

Issues: None

See Also:

- Primary Path
- Backup Path



### 3.3. Protection Switching

#### 3.3.1. Failover Event

Definition:

The occurrence of a planned or unplanned action in the network that results in a change in the Path that data traffic traverses.

Discussion:

Failover Events include, but are not limited to, link failure and router failure. Routing changes are considered Convergence Events [7] and are not Failover Events. This restricts Failover Events to sub-IP layers. Failover may be at the PLR or at the ingress. If the failover is at the ingress it is generally on a disjoint path from the ingress to egress.

Measurement units:

n/a

Issues:

See Also:

Path  
Failure Detection  
Disjoint Path

#### 3.3.2. Failure Detection

Definition:

The process to identify at a sub-IP layer a Failover Event along the Primary Path.

Discussion:

Failure Detection occurs at the ingress node of the Primary Path. Failure Detection occurs via a sub-IP mechanism such as detection of a link down event or timeout for receipt of a control packet. A failure may be completely isolated. A failure may affect a set of links which share a single SRLG (e.g. port with many sub-interfaces). A failure may affect multiple links that are not part of SRLG.

Measurement units: n/a

Issues:

See Also:

Primary Path



### 3.3.3. Failover

Definition:

The process to switch data traffic from the Protected Primary Path to the Backup Path upon Failure Detection of a Failover Event.

Discussion:

Failover to a Backup Path provides Link Protection, Node Protection, or Path Protection. Failover is complete when Packet Loss [7], Out-of-order Packets [4], and Duplicate Packets [4] are no longer observed. Forwarding Delay [4] may continue to be observed.

Measurement units:

n/a

Issues:

See Also:

- Primary Path
- Backup Path
- Failover Event

### 3.3.4. Restoration

Definition:

The act of failover recovery in which the Primary Path recovers from a Failover Event, but is not yet forwarding packets because the Backup Path remains the Working Path.

Discussion:

Restoration MUST occur while the Backup Path is the Working Path. The Backup Path is maintained as the Working Path during Restoration. Restoration produces a Primary Path that is recovered from failure, but is not yet forwarding traffic. Traffic is still being forwarded by the Backup Path functioning as the Working Path.

Measurement units:

n/a

Issues:

See Also:

- Primary Path
- Failover Event
- Failure Recovery



Working Path  
Backup Path

Poretsky, Papneja, Karthik, Vapiwala Expires May 2008 [Page 13]

### 3.3.5. Reversion

Definition:

The act of failover recovery in which the Primary Path becomes the Working Path so that it is forwarding packets.

Discussion:

Protection Switching Systems may or may not support Reversion. Reversion, if supported, MUST occur after Restoration. Packet forwarding on the Primary Path resulting from Reversion may occur either fully or partially over the Primary Path. A potential problem with Reversion is the discontinuity in end to end delay when the Forwarding Delays [\[4\]](#) along the Primary Path and Backup Path are different, possibly causing Out of Order Packets [\[4\]](#), Duplicate Packets [\[4\]](#), and increased Jitter [\[4\]](#).

Measurement units: n/a

Issues: None

See Also:

- Protection Switching System
- Working Path
- Primary Path

### 3.4. Nodes

#### 3.4.1. Protection-Switching Node

Definition:

A node that is capable to participate in a Protection Switching System.

Discussion:

The Protection Switching Node MAY be an ingress or egress for a Primary Path or Backup Path.

Measurement units:  
n/a

Issues:

See Also:

- Protection Switching System

#### 3.4.2. Non-Protection Switching Node

Definition:

A node that is not capable of participating in a Protection

Switching System, however it MAY exist along the Primary Path or Backup Path.

Discussion:

Measurement units:  
n/a

Issues:

See Also:  
Protection Switching System  
Primary Path  
Backup Path

#### 3.4.3. Failover Node

Definition:  
A node along the Primary Path that is capable of Failover.

Discussion:  
The Failover Node can be any node along the Primary Path except the egress node of the Primary Path. There can be multiple Failover Nodes along a Primary Path. The Failover Node MUST be the ingress to the Backup Path. The Failover Node MAY also be the ingress of the Primary Path.

Measurement units:  
n/a

Issues:

See Also:  
Primary Path  
Backup Path  
Failover

#### 3.4.4. Merge Node

Definition:  
A Node along the primary path where backup path terminates.

Discussion:  
The Merge Node can be any node along the Primary Path except the ingress node of the Primary Path. There can be multiple Merge Nodes along a Primary Path. A Merge Node can be the egress node for a single or multiple Backup Paths. The Merge Node MUST be the egress to the Backup Path. The Merge Node MAY also be the egress of the Primary Path or point of local repair (PLR).

Measurement units:

n/a

Poretsky, Papneja, Karthik, Vapiwala Expires May 2008 [Page 15]

Issues:

See Also:

- Primary Path
- Backup Path
- PLR
- Failover

#### 3.4.5. Point of Local Repair (PLR)

Definition:

A node along the Primary Path that uses a Backup Path to protect another node or link.

Discussion:

Based on the functionality of the PLR, its role is defined based on the type of method used. If the one-to-one backup method is used, the PLR is responsible for computing a separate Backup Path for each Primary Path. In the case the facility backup method is used, the PLR creates a single Backup Path that can be used to protect multiple Primary Paths.

Measurement units: n/a

Issues:

See Also:

- Primary Path
- Backup Path
- Failover

#### 3.4.6. Head-end Failover Node

Definition:

A node along the Primary Path that is capable of Failover.

Discussion:

The Head-end Failover Node is the ingress node to the Backup Path. The Head-end Failover Node is always a PLR

Measurement units: n/a

Issues:

See Also:

- Primary Path
- Point of Local Repair
- Failover



### 3.5. Benchmarks

#### 3.5.1. Failover Packet Loss

**Definition:**

The amount of packet loss produced by a Failover Event until Failover completes, where the measurement begins when the last unimpaired packet is received by the Tester on the Protected Primary Path and ends when the first unimpaired packet is received by the Tester on the Backup Path.

**Discussion:**

Packet loss can be observed as a reduction of forwarded traffic from the maximum forwarding rate. Failover Packet Loss includes packets that were lost, reordered, or delayed. Failover Packet Loss MAY reach 100% of the offered load.

**Measurement units:**

Number of Packets

Issues: None

**See Also:**

Failover Event  
Failover

#### 3.5.2. Reversion Packet Loss

**Definition:**

The amount of packet loss produced by Reversion, where the measurement begins when the last unimpaired packet is received by the Tester on the Backup Path and ends when the first unimpaired packet is received by the Tester on the Protected Primary Path .

**Discussion:**

Packet loss can be observed as a reduction of forwarded traffic from the maximum forwarding rate. Reversion Packet Loss includes packets that were lost, reordered, or delayed. Reversion Packet Loss MAY reach 100% of the offered load.

Measurement units: Number of Packets

Issues: None

**See Also:**

Reversion





### 3.5.3. Failover Time

Definition:

The amount of time it takes for Failover to successfully complete.

Discussion:

Failover Time can be calculated using the Time-Based Loss Method (TBLM), Packet-Loss Based Method (PLBM), or Timestamp-Based Method (TBM). It is RECOMMENDED that the TBM is used.

Measurement units:

milliseconds

Issues: None

See Also:

Failover  
Failover Time  
Time-Based Loss Method (TBLM)  
Packet-Loss Based Method (PLBM)  
Timestamp-Based Method (TBM)

### 3.5.4. Reversion Time

Definition:

The amount of time it takes for Reversion to complete so that the Primary Path is restored as the Working Path.

Discussion:

Reversion Time can be calculated using the Time-Based Loss Method (TBLM), Packet-Loss Based Method (PLBM), or Timestamp-Based Method (TBM). It is RECOMMENDED that the TBM is used.

Measurement units:

milliseconds

Issues: None

See Also:

Reversion  
Primary Path  
Working Path  
Reversion Packet Loss  
Time-Based Loss Method (TBLM)  
Packet-Loss Based Method (PLBM)



### 3.5.5. Additive Backup Delay

Definition:

The amount of increased Forwarding Delay [4] resulting from data traffic traversing the Backup Path instead of the Primary Path.

Discussion:

Additive Backup Delay is calculated using Equation 1 as shown below:

(Equation 1)

Additive Backup Delay =  
Forwarding Delay(Backup Path) -  
Forwarding Delay(Primary Path).

Measurement units:  
milliseconds

Issues:

Additive Backup Latency MAY be a negative result. This is theoretically possible, but could be indicative of a sub-optimum network configuration .

See Also:

Primary Path  
Backup Path  
Primary Path Latency  
Backup Path Latency

## 3.6 Failover Time Calculation Methods

### 3.6.1 Time-Based Loss Method (TBLM)

Definition:

The method to calculate Failover Time (or Reversion Time) using a time scale on the Tester to measure the interval of Failover Packet Loss.

Discussion:

The Tester MUST provide statistics which show the duration of failure on a time scale to granularity of milliseconds based on occurrence of packet loss on a time scale. This is indicated by the duration of non-zero packet loss. The TBLM includes failure detection time and time for data traffic to begin traversing the Backup Path. Failover Time and Reversion Time are calculated using the TBLM as shown in Equation 2:



(Equation 2)

(Equation 2a)

$$\text{TBLM Failover Time} = \text{Time(Failover)} - \text{Time(Failover Event)}$$

(Equation 2b)

$$\text{TBLM Reversion Time} = \text{Time(Reversion)} - \text{Time(Restoration)}$$

Measurement units:  
milliseconds

Issues:  
None

See Also:  
Failover  
Packet-Loss Based Method

### 3.6.2 Packet-Loss Based Method (PLBM)

Definition:

The method used to calculate Failover Time (or Reversion Time) from the amount of Failover Packet Loss.

Discussion:

PLBM includes failure detection time and time for data traffic to begin traversing the Backup Path. Failover Time can be calculated using PLBM from the amount Failover Packet Loss as shown below in Equation 3:

(Equation 3)

(Equation 3a)

$$\text{PLBM Failover Time} = \frac{\text{Number of packets lost}}{(\text{Offered Load rate} * 1000)}$$

(Equation 3b)

$$\text{PLBM Restoration Time} = \frac{\text{Number of packets lost}}{(\text{Offered Load rate} * 1000)}$$

Units are packets/(packets/second) = seconds

Measurement units:  
milliseconds

Issues:  
None

See Also:

Failover  
Time-Based Loss Method

Poretsky, Papneja, Karthik, Vapiwala Expires May 2008 [Page 20]

### 3.6.3 Timestamp-Based Method (TBM)

Definition:

The method to calculate Failover Time (or Reversion Time) using a time scale to quantify the interval between unimpaired packets arriving in the test stream.

Discussion:

The purpose of this method is to quantify the duration of failure or reversion on a time scale with granularity of milliseconds based on the observation of unimpaired packets, using Equation 2 with the difference being that the time values are obtained from the timestamp in the packet payload rather than from the Tester.

Unimpaired packets are normal packets that are not lost, reordered, or duplicated. A reordered packet is defined in [10, [section 3.3](#)]. A duplicate packet is defined in [4, [section 3.3.3](#)]. A lost packet is defined in [7, [Section 3.5](#)]. Unimpaired packets may be detected by checking a sequence number in the payload, where the sequence number equals the next expected number for an unimpaired packet. A sequence gap or sequence reversal indicates impaired packets.

For calculating Failover Time, the TBM includes failure detection time and time for data traffic to begin traversing the Backup Path. For calculating Reversion Time, the TBM includes Reversion Time and time for data traffic to begin traversing the Primary Path.

Measurement units:  
    milliseconds

Issues: None

See Also:

- Failover
- Failover Time
- Reversion
- Reversion Time





#### **4. Acknowledgements**

We would like thank the BMWG and particularly Al Morton and Curtis Villamizar for their reviews, comments, and contributions to this work.

#### **5. IANA Considerations**

This document requires no IANA considerations.

#### **6. Security Considerations**

This document only addresses terminology for the performance benchmarking of protection systems, and the information contained in this document has no effect on the security of the Internet.

#### **7. References**

##### **7.1. Normative References**

- [1] Bradner, S., "The Internet Standards Process -- Revision 3", [RFC 2026](#), October 1996.
- [2] Bradner, S., Editor, "Benchmarking Terminology for Network Interconnection Devices", [RFC 1242](#), July 1991.
- [3] Mandeville, R., "Benchmarking Terminology for LAN Switching Devices", [RFC 2285](#), February 1998.
- [4] Poretsky, S., et al., "Terminology for Benchmarking Network-layer Traffic Control Mechanisms", [RFC 4689](#), November 2006.
- [5] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), July 1997.
- [6] Paxson, V., et al., "Framework for IP Performance Metrics", [RFC 2330](#), May 1998.
- [7] Poretsky, S., Imhoff, B., "Benchmarking Terminology for IGP Convergence", [draft-ietf-bmwg-igp-dataplane-conv-term-13](#), work in progress, July 2007.
- [8] Pan., P. et al, "Fast Reroute Extensions to RSVP-TE for LSP Paths", [RFC 4090](#), May 2005.
- [9] Nichols, K., et al, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", [RFC 2474](#), December 1998.
- [10] Morton, A., et al, "Packet Reordering Metrics", [RFC 4737](#), November 2006.

##### **7.2. Informative References**

None

Poretsky, Papneja, Karthik, Vapiwala Expires May 2008 [Page 22]

**8. Author's Address**

Scott Poretsky  
Reef Point Systems  
8 New England Executive Park  
Burlington, MA 01803  
USA  
Phone: + 1 508 439 9008  
EMail: sporetsky@reefpoint.com

Rajiv Papneja  
Isocore  
12359 Sunrise Valley Drive  
Reston, VA 22102  
USA  
Phone: 1 703 860 9273  
Email: rpapneja@isocore.com

Jay Karthik  
Cisco Systems  
300 Beaver Brook Road  
Boxborough, MA 01719  
USA  
Phone: +1 978 936 0533  
Email: jkarthik@cisco.com

Samir Vapiwala  
Cisco System  
300 Beaver Brook Road  
Boxborough, MA 01719  
USA  
Phone: +1 978 936 1484  
Email: svapiwal@cisco.com

**Full Copyright Statement**

Copyright (C) The IETF Trust (2007).

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.

Poretsky, Papneja, Karthik, Vapiwala Expires May 2008 [Page 23]

## 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](mailto:ietf-ipr@ietf.org).

## Acknowledgement

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

