

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: May 15, 2008

Y. Kikuchi  
Kochi University of Technology  
S. Matsushima  
Softbank Telecom Corp.  
K. Nagami  
Intec Netcore Inc.  
S. Uda  
Japan Advanced Institute of  
Science and Technology  
Nov 12, 2007

Quality Measurement Requirements for Tunneling Protocols  
draft-kikuchi-tunnel-measure-req-02.txt

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."

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>.

This Internet-Draft will expire on May 15, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Internet-Draft [draft-kikuchi-tunnel-measure-req-02.txt](#)

Nov 2007

## Abstract

This draft describes the necessary requirements to passively measure the quality of end-to-end tunnels and to monitor them via applicable ways. This feature is crucial for Service Providers (SPs), especially who provide transports to users using tunnels.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">1.1.</a>	Requirements notation . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Service Model . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Motivations . . . . .	<a href="#">6</a>
<a href="#">4.</a>	Requirements . . . . .	<a href="#">7</a>
<a href="#">4.1.</a>	Active vs. Passive . . . . .	<a href="#">7</a>
<a href="#">4.2.</a>	Quality Evaluation . . . . .	<a href="#">7</a>
<a href="#">4.3.</a>	Getting Quality Information . . . . .	<a href="#">8</a>
<a href="#">4.4.</a>	Overhead Consideration . . . . .	<a href="#">8</a>
<a href="#">4.5.</a>	Header Information . . . . .	<a href="#">8</a>
<a href="#">4.5.1.</a>	Sequence Numbering . . . . .	<a href="#">9</a>
<a href="#">4.5.2.</a>	Time Stamping . . . . .	<a href="#">9</a>
<a href="#">5.</a>	Security Considerations . . . . .	<a href="#">10</a>
<a href="#">Appendix A.</a>	Acknowledgements . . . . .	<a href="#">11</a>
<a href="#">6.</a>	References . . . . .	<a href="#">12</a>
<a href="#">6.1.</a>	Normative References . . . . .	<a href="#">12</a>
<a href="#">6.2.</a>	Informative References . . . . .	<a href="#">12</a>
	Authors' Addresses . . . . .	<a href="#">13</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">14</a>

## [1.](#) Introduction

This draft describes the necessary requirements to passively measure the quality of end-to-end tunnels passively and to monitor them via some applicable ways.

In this document, ``tunnel'' refers to the various technologies used to provide networks or datalinks virtually over real networks. Examples of tunneling are GRE [\[2\]](#), IP Encapsulation within IP (IPIP) [\[3\]](#), and Pseudo Wire Emulation Edge-to-Edge (PWE3) [\[4\]](#).

Measuring end-to-end quality of tunnels is necessary for Transport Service Providers (TSPs) who provide transport to users using tunnels. However, the standards do not define the measurement and monitoring of a network, which is helpful when TSPs want to know the quality of their traffic through tunnels. Therefore, measurement and monitoring standards need to be defined.

### [1.1.](#) Requirements notation

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 [\[1\]](#).

## 2. Service Model

Figure 1 shows that TSP X provides a transport between user A and user B using a tunnel. The users construct an application over the transport. The TSP may apply two or more tunnels to provide one transport.

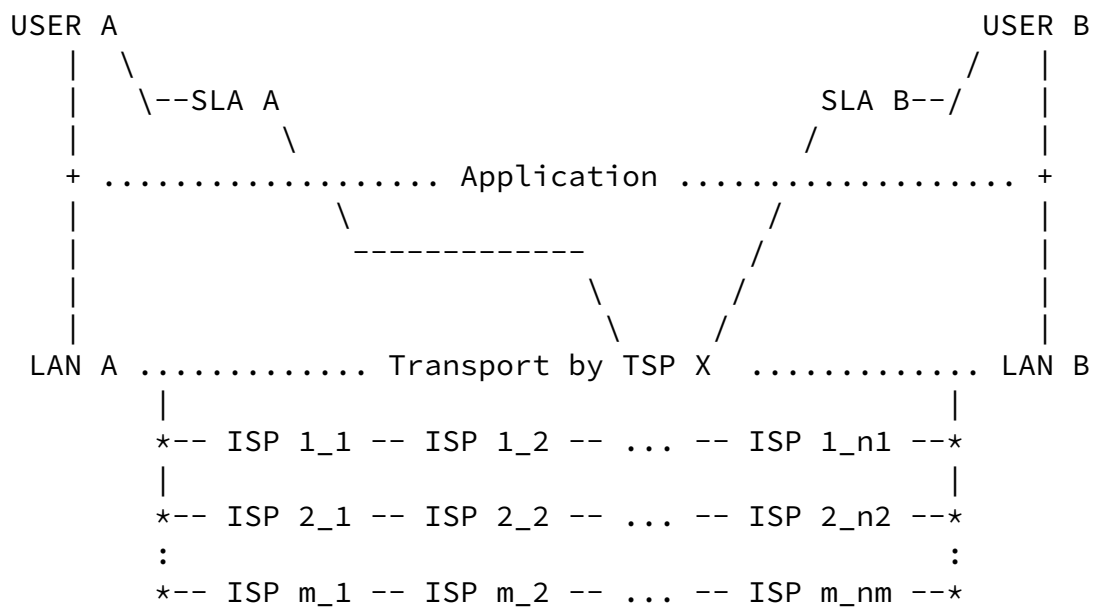


Figure 1: A Service Model of TSP

TSPs provide a reachability of IP datagrams or layer 2 frames to users. Typically, users are not able to identify the path details

under the transport, which is the sequence of transit ISPs, because the tunnel eliminates the path information so that the users must recognize that both ends of the transport as a neighbor.

TSPs provide simplified and virtual transports by hiding the underlying layers from the users. The users are able to reduce the cost of operation and management because they need not maintain the underlying layers. The reachability maintenance and the quality management are served as TSPs' communication services.

There must be a Service Level Agreement (SLA) in the contract between a TSP and its user. The SLA specifies the level that the TSP must maintain, which is a set of measurable characteristics such as the total unavailable time in a month, maximum out-of-sequence rates and some qualities for real time applications.

In addition, TSPs may be able to provide better transports when the TSPs have several tunnels via different paths. Furthermore, TSPs may be able to provide protocols needed by the users even if there are no

such protocols served by the ISPs.

### 3. Motivations

TSPs need to know the quality of their tunnels in order to know whether the tunnels are in a normal state or not. The measured quality could be important information to trace down the cause of the trouble when an application is not working properly. Without the necessary information, it is difficult for TSPs to determine whether problems come from the user, the TSP itself, or the ISPs.

The tunnel quality measurement is specially needed by TSPs because they have SLAs to their customers. They must be aware of the status of underlying tunnels well and must report it as an evidence of quality to the users.

TSPs also need to know the tunnels' quality when they have multiple

tunnels to serve transports. TSPs may be able to serve appropriate transports to users by selecting better quality tunnels. In addition, the TSPs may be able to distribute the load of a transport to different path tunnels.

#### 4. Requirements

This section describes each requirement necessary to measure end-to-end tunnel quality for TSPs.

The quality should be measured for tunnel traffic in operation because the measured quality is used to maintain the tunnel, to report regarding to the SLA and to select the best tunnel. The

measurement would be used not only for testing and benchmarking but also for the daily operational tool. Therefore, the requirements are from operational points of view.

#### [4.1.](#) Active vs. Passive

There are two ways to measure the quality of a tunnel, one is active and the other is passive. Active measurement uses additional probing packets to determine the quality of the channel. Passive measurement uses the traffic packets to measure quality.

From the TSPs point of view, passive measurement should be supported. Because SLAs should refer to the users' packets, the measurement should be determined passively rather than actively.

On the other hand, it is not necessary to let the protocol have a quality measurement function with active measurement. TSPs can construct the active measurement method independently from the target protocol. A typical example is PING, which uses Internet Control Message Protocol (ICMP) [\[5\]](#).

#### [4.2.](#) Quality Evaluation

The standard that define a passive measurement of a tunneling protocol must contain two items, one is 'WHAT' type of quality the protocol measure, or 'metrics', and the other is 'HOW' the protocol evaluate the quality.

The most basic metric is to detect whether the packets in a tunnel are in-sequence or out-of-sequence. Measurements of out-of-sequence packets are also basic metrics, such as loss, duplication and reordering. Additionally, it may support to measure delay and/or jitter when the packets are in-sequence.

It is required to disable the measurement function for avoiding the measurement overhead in case when TSPs need not to measure the tunnel quality. See also the discussion in the [Section 4.4](#).

Note that the tunnel quality discussed in this document shall not refer any specific application, so that the metrics must be

independent from the payload information. See also the discussion in



the [Section 4.5](#).

#### [4.3](#). Getting Quality Information

Tunneling protocols must support monitoring when the protocols have quality measurement functions. The protocol must define how to monitor the result of the quality measurement of tunnels, such as SNMP [\[6\]](#).

The parameters used in the measurement mechanisms might be modified by TSPs' operators. Moreover, it may notify exceptional situations and illegal operations to the operators.

#### [4.4](#). Overhead Consideration

Protocol designers should take into account the computing and space costs of the implementations where the standard defines the measurement and monitoring. This includes overhead of traffic transmission, which may reflect the cost of equipment introductions and operational expenses. The designers should not adopt non-scalable mechanisms and should pay particular attention to resource consumption sensitive protocols such as mobile protocols.

The types of overheads are as follows.

- o the space of additional information in protocol header,
- o the time of sending and receiving the information above, and
- o the computing resources for quality measurement implemented in routers.

We should adopt a simplified determination in some cases when both a precise complex determination and a simpler one exist. Sometimes it is sufficient for operators to show an approximate degree different from the normal operation rather than a precise state.

#### [4.5](#). Header Information

The target tunneling protocol must provide information to measure the quality. This means that the protocol header has enough information because the measurement must be passive and must not refer to the payload, according to the [Section 4.1](#) and the [Section 4.2](#).

For example, in an extreme case, IPIP [\[3\]](#) does not have any extra field in the outer header on encapsulation, so that it is difficult to define passive metrics for IPIP. However many tunneling protocols

have some information in their headers, which allows to detect some quality passively.

#### [4.5.1.](#) Sequence Numbering

If a protocol has a sequence number field, it is easy for egress router to determine the tunnel is in-sequence or not. Moreover, it can recognize how the irregular is, such as loss, duplication and reordering.

The original GRE [2] does not have much information but the extended GRE [7] has a sequence number field, therefore it can detect out-of-sequence and how irregular.

#### [4.5.2.](#) Time Stamping

If there is a timestamp in the header of a tunneling protocol, even the timestamps might be synchronized to a reference clock, it can measure delay and jitter. Such kinds of metrics provide the tunnel quality when the packets are in-sequence rather than out-of-sequence.

## [5.](#) Security Considerations

Fraud header information, such as sequence numbers and time stamps, causes the measurement process to become disorganized. This discussion boils down to the issues of the header protection.

#### [Appendix A](#). Acknowledgements

The authors would like to thank for helpful discussions in TERECo 2.0 research project sponsored in part by the ministry of internal affairs and communications Japan (SCOPE 072309007).

---

Internet-Draft [draft-kikuchi-tunnel-measure-req-02.txt](#)

Nov 2007

## [6.](#) References

### [6.1.](#) Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

### [6.2.](#) Informative References

- [2] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", [RFC 2784](#), March 2000.
- [3] Perkins, C., "IP Encapsulation within IP", [RFC 2003](#), October 1996.
- [4] Bryant, S. and P. Pate, "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture", [RFC 3985](#), March 2005.
- [5] Postel, J., "Internet Control Message Protocol", STD 5, [RFC 792](#), September 1981.
- [6] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, [RFC 3411](#), December 2002.

- [7] Dommety, G., "Key and Sequence Number Extensions to GRE",  
[RFC 2890](#), September 2000.

Kikuchi, et al.

Expires May 15, 2008

[Page 12]

---

Internet-Draft [draft-kikuchi-tunnel-measure-req-02.txt](#)

Nov 2007

#### Authors' Addresses

Yutaka Kikuchi  
Kochi University of Technology  
306B Research Collaboration Center  
185 Miyanokuchi, Tosayamada-cho  
Kami-shi, Kochi 782-0003  
JP

Phone: +81-887-57-2068  
Email: [yu@kikuken.org](mailto:yu@kikuken.org)

Satoru Matsushima  
Softbank Telecom Corp.  
1-9-1 Higashi-Shinbashi  
Minato-ku, Tokyo  
JP

Email: satoru@ft.solteria.net

Ken-ichi Nagami  
Intec Netcore Inc.  
1-3-3 Shin-suna  
Koto-ku, Tokyo  
JP

Phone: +81-3-5565-5069  
Email: nagami@inetcore.com

Satoshi Uda  
Japan Advanced Institute of Science and Technology  
1-1 Asahi-dai  
Nomi-shi, Ishikawa-ken 923-1292  
JP

Email: zin@jaist.ac.jp

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

## Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).