Network Working Group A. Morton
Internet-Draft AT&T Labs
Intended status: Informational October 7, 2014
Expires: April 10, 2015

Rate Measurement Test Protocol Problem Statement
draft-ietf-ippm-rate-problem-07

Abstract

This memo presents an access rate-measurement problem statement for test protocols to measure IP Performance Metrics. The rate measurement scenario has wide-spread attention of Internet access subscribers and seemingly all industry players, including regulators. Key test protocol aspects require the ability to control packet size on the tested path and enable asymmetrical packet size testing in a controller-responder architecture.

Requirements Language

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 [RFC2119].

Table of Contents

1. Introduction

There are many possible rate measurement scenarios. This memo describes one rate measurement problem and presents a rate-measurement problem statement for test protocols to measure IP Performance Metrics (IPPM).

When selecting a form of access to the Internet, subscribers are interested in the performance characteristics of the various alternatives. Standardized measurements can be a basis for comparison between these alternatives. There is an underlying need to coordinate measurements that support such comparisons, and test control protocols to fulfill this need. The figure below depicts some typical measurement points of access networks.

```
User     ====== Fiber =======  Access Node \
Device   ----- Copper -------  Access Node -|--- Infrastructure --- GW
or Host ------ Radio -------  Access Node /
```

The access-rate scenario or use case has received wide-spread attention of Internet access subscribers and seemingly all Internet industry players, including regulators. This problem is being approached with many different measurement methods.

2. Purpose and Scope

The scope and purpose of this memo is to define the measurement problem statement for test protocols conducting access rate measurement on production networks. Relevant test protocols include [RFC4656] and [RFC5357], but the problem is stated in a general way so that it can be addressed by any existing test protocol, such as [RFC6812].

This memo discusses possibilities for methods of measurement, but does not specify exact methods which would normally be part of the solution, not the problem.

We are interested in access measurement scenarios with the following characteristics:

- The Access portion of the network is the focus of this problem statement. The user typically subscribes to a service with bi-directional access partly described by rates in bits per second. The rates may be expressed as raw capacity or restricted capacity as described in [RFC6703]. These are the quantities that must be measured according to one or more standard metrics, and for which measurement methods must also be agreed as a part of the solution.

- Referring to the reference path illustrated below and defined in [I-D.ietf-ippm-lmap-path], possible measurement points include a Subscriber's host, the access service demarcation point, Intra IP access where a globally routable address is present, or the gateway between the measured access network and other networks.

```
Subsc. -- Private -- Private -- Access -- Intra IP -- GRA -- Transit
device      Net #1      Net #2     Demarc.     Access      GW     GRA GW

            GRA = Globally Routable Address, GW = Gateway
```

- Rates at some links near the edge of the provider's network can often be several orders of magnitude less than link rates in the aggregation and core portions of the network.

o Asymmetrical access rates on ingress and egress are prevalent.

o In many scenarios of interest, extremely large scale of access services requires low complexity devices participating at the user end of the path.

This problem statement assumes that the most-likely bottleneck device or link is adjacent to the remote (user-end) measurement device, or

is within one or two router/switch hops of the remote measurement device.

Other use cases for rate measurement involve situations where the packet switching and transport facilities are leased by one operator from another and the link capacity available cannot be directly determined (e.g., from device interface utilization). These scenarios could include mobile backhaul, Ethernet Service access networks, and/or extensions of layer 2 or layer 3 networks. The results of rate measurements in such cases could be employed to select alternate routing, investigate whether capacity meets some previous agreement, and/or adapt the rate of traffic sources if a capacity bottleneck is found via the rate measurement. In the case of aggregated leased networks, available capacity may also be asymmetric. In these cases, the tester is assumed to have a sender and receiver location under their control. We refer to this scenario below as the aggregated leased network case.

Support of active measurement methods will be addressed here, consistent with the IPPM working group's traditional charter. Active measurements require synthetic traffic dedicated to testing, and do not make measurements on user traffic.

As noted in [RFC2330] the focus of access traffic management may influence the rate measurement results for some forms of access, as it may differ between user and test traffic if the test traffic has different characteristics, primarily in terms of the packets themselves (see section 13 of [RFC2330] for the considerations on packet type, or Type-P).

There are several aspects of Type-P where user traffic may be examined and selected for special treatment that may affect transmission rates. Without being exhaustive, the possibilities include:

- o Packet length

- o IP addresses

- o Transport protocol (e.g. where TCP packets may be routed differently from UDP)

- o Transport Protocol port numbers

This issue requires further discussion when specific solutions/ methods of measurement are proposed, but for this problem statement it is sufficient to identify the problem and indicate that the

solution may require an extremely close emulation of user traffic, in terms of one or more factors above.

Although the user may have multiple instances of network access available to them, the primary problem scope is to measure one form of access at a time. It is plausible that a solution for the single access problem will be applicable to simultaneous measurement of multiple access instances, but treatment of this scenario is beyond the current scope this document.

A key consideration is whether active measurements will be conducted with user traffic present (In-Service testing), or not present (Out-of-Service testing), such as during pre-service testing or maintenance that interrupts service temporarily. Out-of-Service testing includes activities described as "service commissioning", "service activation", and "planned maintenance". Opportunistic In-Service testing when there is no user traffic present (e.g., outside normal business hours) throughout the test interval is essentially equivalent to Out-of-Service testing. Both In-Service and Out-of-Service testing are within the scope of this problem.

It is a non-goal to solve the measurement protocol specification problem in this memo.

It is a non-goal to standardize methods of measurement in this memo. However, the problem statement will mandate support for one or more categories of rate measurement methods in the test protocol and adequate control features for the methods in the control protocol (assuming the control and test protocols are separate).

3. Active Rate Measurement

This section lists features of active measurement methods needed to measure access rates in production networks.

Coordination between source and destination devices through control messages and other basic capabilities described in the methods of IPPM RFCs [RFC2679][RFC2680], and assumed for test protocols such as [RFC5357] and [RFC4656], are taken as given.

Most forms of active testing intrude on user performance to some degree, especially In-Service testing. One key tenet of IPPM methods is to minimize test traffic effects on user traffic in the production network. Section 5 of [RFC2680] lists the problems with high measurement traffic rates, and the most relevant for rate measurement is the tendency for measurement traffic to skew the results, followed by the possibility of introducing congestion on the access link. In-Service testing MUST respect these traffic constraints. Obviously,

categories of rate measurement methods that use less active test traffic than others with similar accuracy are preferred for In-Service testing.

On the other hand, Out-of-Service tests where the test path shares no links with In-Service user traffic have none of the congestion or skew concerns, but these tests must address other practical matters such as conducting measurements within a reasonable time from the tester's point of view. Out-of-Service tests where some part of the test path is shared with In-Service traffic MUST respect the In-Service constraints.

The **intended metrics to be measured** have strong influence over the categories of measurement methods required. For example, using the terminology of [RFC5136], a it may be possible to measure a Path

Capacity Metric while In-Service if the level of background (user) traffic can be assessed and included in the reported result.

The measurement *architecture* MAY be either of one-way (e.g., [RFC4656]) or two-way (e.g., [RFC5357]), but the scale and complexity aspects of end-user or aggregated access measurement clearly favor two-way (with low-complexity user-end device and round-trip results collection, as found in [RFC5357]). However, the asymmetric rates of many access services mean that the measurement system MUST be able to evaluate performance in each direction of transmission. In the two-way architecture, it is expected that both end devices MUST include the ability to launch test streams and collect the results of measurements in both (one-way) directions of transmission (this requirement is consistent with previous protocol specifications, and it is not a unique problem for rate measurements).

The following paragraphs describe features for the roles of test packet SENDER, RECEIVER, and results REPORTER.

SENDER:

Generate streams of test packets with various characteristics as desired (see Section 4). The SENDER MAY be located at the user end of the access path or elsewhere in the production network, such as at one end of an aggregated leased network segment.

RECEIVER:

Collect streams of test packets with various characteristics (as described above), and make the measurements necessary to support rate measurement at the receiving end of an access or aggregated leased network segment.

REPORTER:

Use information from test packets and local processes to measure delivered packet rates, and prepare results in the required format (the REPORTER role may be combined with another role, most likely the SENDER).

4. Measurement Method Categories

A protocol that addresses the rate measurement problem MUST serve the test stream generation and measurement functions (SENDER and RECEIVER). The follow-up phase of analyzing the measurement results to produce a report is outside the scope of this problem and memo (REPORTER).

For the purposes of this problem statement, we categorize the many possibilities for rate measurement stream generation as follows;

1. Packet pairs, with fixed intra-pair packet spacing and fixed or random time intervals between pairs in a test stream.

2. Multiple streams of packet pairs, with a range of intra-pair spacing and inter-pair intervals.

3. One or more packet ensembles in a test stream, using a fixed ensemble size in packets and one or more fixed intra-ensemble packet spacings (including zero spacing, meaning that back-to-back burst ensembles and constant rate ensembles fall in this category).

4. One or more packet chirps, where intra-packet spacing typically decreases between adjacent packets in the same chirp and each pair of packets represents a rate for testing purposes.

The test protocol SHALL support test packet ensemble generation (category 3), as this appears to minimize the demands on measurement accuracy. Other stream generation categories are OPTIONAL.

For all categories, the test protocol MUST support:

a. Variable payload lengths among packet streams

b. Variable length (in packets) among packet streams or ensembles

c. Variable IP header markings among packet streams

d. Choice of UDP transport and variable port numbers, OR, choice of TCP transport and variable port numbers for two-way architectures

only, OR BOTH. See below for additional requirements on TCP transport generation.

e. Variable number of packets-pairs, ensembles, or streams used in a test session.

The items above are additional variables that the test protocol MUST be able to identify and control. The ability to revise these variables during an established test session is OPTIONAL, as multiple test sessions could serve the same purpose. Another OPTIONAL feature is the ability to generate streams with VLAN tags and other markings.

For measurement systems employing TCP as the transport protocol, the ability to generate specific stream characteristics requires a sender with the ability to establish and prime the connection such that the desired stream characteristics are allowed. See Mathis' work in progress for more background [I-D.ietf-ippm-model-based-metrics].

Beyond simple connection handshake and options establishment, an "open-loop" TCP sender requires the SENDER ability to:

- o generate TCP packets with well-formed headers (all fields valid), including Acknowledgement aspects.

- o produce packet streams at controlled rates and variable inter-packet spacings, including packet ensembles (back-to-back at server rate).

- o continue the configured sending stream characteristics despite all control indications except receive window exhaust.

The corresponding TCP RECEIVER performs normally, having some ability to configure the receive window sufficiently large so as to allow the SENDER to transmit at will (up to a configured target).

It may also be useful to provide a control for Bulk Transfer Capacity measurement with fully-specified (and congestion-controlled) TCP senders and receivers, as envisioned in [RFC3148], but this would be a brute-force assessment which does not follow the conservative tenets of IPPM measurement [RFC2330].

Measurements for each UDP test packet transferred between SENDER and RECEIVER MUST be compliant with the singleton measurement methods described in IPPM RFCs [RFC2679][RFC2680] (these could be listed later, if desired). The time-stamp information or loss/arrival status for each packet MUST be available for communication to the protocol entity that collects results.

5. Test Protocol Control & Generation Requirements

Essentially, the test protocol MUST support the measurement features described in the sections above. This requires:

1. Communicating all test variables to the SENDER and RECEIVER

2. Results collection in a one-way architecture

3. Remote device control for both one-way and two-way architectures

4. Asymmetric packet size and/or pseudo-one-way test capability in a two-way measurement architecture (along with symmetric packet size tests in common use)

The ability to control and generate asymmetric rates in a two-way architecture is REQUIRED. Two-way architectures are RECOMMENDED to include control and generation capability for both asymmetric and symmetric packet sizes, because packet size often matters in the scope of this problem and test systems SHOULD be equipped to detect directional size dependency through comparative measurements.

Asymmetric packet size control is indicated when the result of a measurement may depend on the size of the packets used in each direction, i.e. when any of the following conditions hold:

- there is a link in the path with asymmetrical capacity in opposite directions (in combination with one or more of the conditions below, but their presence or specific details may be unknown to the tester),

- there is a link in the path which aggregates (or divides) packets into link-level frames, and may have a capacity that depends on packet size, rate, or timing,

- there is a link in the path where transmission in one direction influences performance in the opposite direction,

- there is a device in the path where transmission capacity depends on packet header processing capacity (in other words, the capacity is sensitive to packet size),

- the target application stream is nominally MTU size packets in one direction vs. ACK stream in the other, (noting that there are a vanishing number of symmetrical-rate application streams for which rate measurement is wanted or interesting), o the distribution of packet losses is critical to rate assessment,

and possibly other circumstances revealed by measurements comparing streams with symmetrical size and asymmetrical size.

Implementations may support control and generation for only symmetric packet sizes when none of the above conditions hold.

The test protocol SHOULD enable measurement of the [RFC5136] Capacity metric, either Out-of-Service, In-Service, or both. Other [RFC5136] metrics are OPTIONAL.

6. Security Considerations

The security considerations that apply to any active measurement of live networks are relevant here as well. See [RFC4656] and [RFC5357].

There may be a serious issue if a proprietary Service Level Agreement involved with the access network segment provider were somehow leaked in the process of rate measurement. To address this, test protocols SHOULD NOT convey this information in a way that could be discovered by unauthorized parties.

7. IANA Considerations

This memo makes no requests of IANA.

8. Acknowledgements

Dave McDysan provided comments and text for the aggregated leased use case. Yaakov Stein suggested many considerations to address, including the In-Service vs. Out-of-Service distinction and its implication on test traffic limits and protocols. Bill Cerveny, Marcelo Bagnulo, and Kostas Pentikousis (a persistent reviewer) have contributed insightful, clarifying comments that made this a better draft. Barry Constantine also provided suggestions for clarification.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2330] Paxson, V., Almes, G., Mahdavi, J., and M. Mathis, "Framework for IP Performance Metrics", RFC 2330, May 1998.

[RFC2679] Almes, G., Kalidindi, S., and M. Zekauskas, "A One-way Delay Metric for IPPM", RFC 2679, September 1999.

[RFC2680] Almes, G., Kalidindi, S., and M. Zekauskas, "A One-way Packet Loss Metric for IPPM", RFC 2680, September 1999.

[RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", RFC 4656, September 2006.

[RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, October 2008.

[RFC6703] Morton, A., Ramachandran, G., and G. Maguluri, "Reporting IP Network Performance Metrics: Different Points of View", RFC 6703, August 2012.

9.2. Informative References

[I-D.ietf-ippm-lmap-path] Bagnulo, M., Burbridge, T., Crawford, S., Eardley, P., and A. Morton, "A Reference Path and Measurement Points for Large-Scale Measurement of Broadband Performance", draft-ietf-ippm-lmap-path-06 (work in progress), September 2014.

[I-D.ietf-ippm-model-based-metrics] Mathis, M. and A. Morton, "Model Based Bulk Performance Metrics", draft-ietf-ippm-model-based-metrics-03 (work in progress), July 2014.

[RFC3148] Mathis, M. and M. Allman, "A Framework for Defining

Empirical Bulk Transfer Capacity Metrics", RFC 3148, July 2001.

[RFC5136] Chimento, P. and J. Ishac, "Defining Network Capacity", RFC 5136, February 2008.

[RFC6812] Chiba, M., Clemm, A., Medley, S., Salowey, J., Thombare, S., and E. Yedavalli, "Cisco Service-Level Assurance Protocol", RFC 6812, January 2013.

Author's Address

Al Morton
AT&T Labs
200 Laurel Avenue South
Middletown,, NJ 07748
USA

Phone: +1 732 420 1571
Fax: +1 732 368 1192
Email: acmorton@att.com
URI: http://home.comcast.net/~acmacm/