Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 14, 2014

L. Zheng
Huawei Technologies
N. Elkins
Inside Products
L. Deng
China Mobile
M. Ackermann
BCBS Michigan
G. Mirsky
Ericsson

June 12, 2014

Framework for IP Passive Performance Measurements
draft-zheng-ippm-framework-passive-00

Abstract

This document describes the framework for passive measurement. In particular, the differences between passive and active measurements are analyzed, general considerations for both metric definition and measurement methodology are discussed, and requirements for various entities performing a given passive measurement task are described according to a reference model.

Table of Contents

1 Introduction

This document describes the framework for passive measurement. In particular, the differences between passive and active measurements are analyzed, general considerations for both metric definition and measurement methodology are discussed, and requirements for various entities performing a given passive measurement task are described according to a reference model.

The IETF IP Performance Metrics (IPPM) working group first created a framework for metric development in [RFC2330], which enabled development of many fundamental metrics. [RFC2330] has been updated once by [RFC5835], which describes a detailed framework for composing and aggregating metrics originally defined in [RFC2330].

The first task of this document will be to define active and passive measurement methods.

Active Measurement Method: The process of measuring some performance or reliability parameter associated with the transfer of traffic by generating and/or receiving packets injected into the network.

In contrast, passive measurement is defined as:

Passive Measurement Method: The process of measuring some performance or reliability parameter associated with the existing traffic (packets) on the network.

[Note: There are definitions for both active and passive measurement methods in [I-D.manyfolks-ippm-metric-registry]. Further discussion and coordination may be needed.]

The de facto focus of RFC2330 is on active measurement. Although many of the concepts discussed in RFC2330, metrics, measurement methodology, errors with time apply to both passive and active methods of measurement techniques, there are considerable differences in terms of metric definition and measurement methodology for passive measurement.

It should be noted that there can be different ways of how one conducts a "passive" measurement task (without injecting packets) as well as pure observation.

Examples include:

1. adding a dedicated packet header[draft-PDM]

2. changes to an existing header for marking[draft-coloring]

Terminology used in the above examples will be defined in Section 2: Terminology.

Passive measurements may be used in scenarios where active measurement alone is not enough or applicable. Since no extra in-band traffic which may alter service and performance behavior is introduced, passive measurement may be done during peak traffic.

Passive measurement is not without cost. In the best scenario, the passive measurement point is external to the devices participating in the network traffic. For example, a passive network TAP may be placed at a switch to capture traffic. This would create very little, if any, interference with in-band traffic. Alternatively, care must be taken if a passive measurement technique creates load on a participant in the network. For example, a packet trace taken at one of the end host points may add load to the device thus potentially changing the environment which it is measuring. The benefits of this method for measurement and diagnostics must be weighed with the costs.

For networks who charge for the amount of data sent, passive measurement may be the first choice for end-to-end measurement, as it does not introduce any extra expense to the subscriber. In terms of Quality of Experience (QoE) measurement, passive measurement is expected to be more accurate and helpful in troubleshooting as it reflects the status of real application traffic.

2 Terminology

In this sections, we will define some terms and acronyms which will be referred to in this document.

Coloring : A scheme for modifying a field in the IP header for purposes of measurement. A description of this scheme for IPv4 may be found at [draft-coloring].

PDM : Performance and Diagnostic Metrics (PDM) header. An IP header which is appended to packets for the purposes of measurement. A description of the IPv6 version of this header may be found at [draft-PDM].

3 Passive Metric Definition

In RFC2330, singleton, sample, and statistics are defined as follows:

"By a 'singleton' metric, we refer to metrics that are, in a sense, atomic. For example, a single instance of "bulk throughput capacity"

from one host to another might be defined as a singleton metric, even though the instance involves measuring the timing of a number of Internet packets.

By a 'sample' metric, we refer to metrics derived from a given singleton metric by taking a number of distinct instances together. For example, we might define a sample metric of one-way delays from one host to another as an hour's worth of measurements, each made at Poisson intervals with a mean spacing of one second.

By a 'statistical' metric, we refer to metrics derived from a given sample metric by computing some statistic of the values defined by the singleton metric on the sample. For example, the mean of all the one-way delay values on the sample given above might be defined as a statistical metric."

For passive measurement, the concepts of singleton, sample and statistical also apply. However, there are some differences. The singleton, sample, and statistical measurements are those taken within the boundaries of captured traffic.

In passive measurement, the most important aspects have to do with the portion of reality which is actually measured at any point in time. So, it may be useful to define some terms for passive measurement. These are as follows:

1. Capture content: this is the type(s) of packet or metric found.

2. Capture distribution: this is the actual pattern of data in the collected packets. The pattern or distribution may be poisson but it may also be bimodal, uniform, or skewed. For example, one might see an FTP transfer as a relatively uniform distribution, a TCP connection with a windowing issue may display a skewed distribution, etc.

3. Capture limits: this is the way the set of packets or metrics are selected. For example, one may decide to take a trace that consists of 1,000 packets. Alternatively, one might take a packet capture for 5 minutes with no regard to how many packets are found.

4. Capture methodology: this is the area in which passive differs most greatly from active methods. For example, [RFC2679], section 3.6. Methodologies discusses the various techniques of injecting test packets into the network. This is not applicable to passive measurement. Passive measurement simply collects that which exists.

5. Unruly Nature of Capture: With reality, there are no guarantees. That is, if one imagines a passive sample to be a packet trace taken

at a host. If the metric one is looking for is IP-TCP- connectivity measured by a TCP three way handshake, then in active measurement, one can be guaranteed to find that metric because one has injected packets of that type into the stream. In passive measurement, the capture may contain anywhere from zero occurrences of the desired metric to many instances of the desired metric.

6. Capture Selection: With active measurement, one may create 500 packets of a certain type and pick according to the sampling distribution desired.

For example, [RFC2330] in the discussion of generating poisson distributions (11.1.3), discusses a method:

Method 1 is to proceed as follows:

1. Generate E1 and wait that long.
2. Perform a measurement.
3. Generate E2 and wait that long.
4. Perform a measurement.
5. Generate E3 and wait that long.
6. Perform a measurement ...

With passive measurement, one has no way of knowing if a particular desired packet or packet sequence exists at all in the set of packets captured.

Having said that, if there do exist many such packets, one may use a random (or another) sampling method to pick the instances desired. That is, if one has 100,000 instances of TCP three-way handshakes, one may decide to randomly choose 50 to examine more closely.

7. Inherent Inequality of Active and Passive Measurements: due to the nature of data traffic, depending on what metric is measured, it is unlikely that it will have a random or poisson distribution. Hence, metrics created using Active methods and those generated using Passive methods are likely to differ. It is not known at this point whether that difference is significant or not.

[TBD: More discussion here on distributions and inequality]

8. Point of View: In passive measurement, it matters greatly where the measurement is being done. Point of view is critical. Passive measurement only knows what it sees from its own perspective.

In troubleshooting problems using passive measurement, it is often necessary to get multiple points of view. Let us take a simple case of diagnosing packet loss from an end user perspective. If one takes

a packet trace at the client host, one sees that certain packets are not being received. If one takes two packet traces at the same time at the server and client, one sees that the server sends these packets yet the client does not receive them. Hence, the problem must be at a middle box. So, then, one must start taking traces at client, server, and a trace point after the first middle box, etc.

The measurement techniques for passive measurement must accommodate and facilitate such tasks.

Active measurement techniques know clearly the measurement point and path because that is a part of the definition of the Active measurement task.

4 Reference Model

This section describes the main functional components of the passive measurement system, and the interactions between the components. Some new terms are defined in this document and some are borrowed from the LMAP Framework [I-D.ietf-lmap-framework] (indicated by brackets).

```
     +---------------+                 +---------------+
     |  Measurement  |  Coordination   | Measurement   |
     |   Agent A     |<--------------->|  Agent B      |
     +---------------+                 +---------------+
               ^  |                       ^    |
      Control  |  | Report        Control |    | Report
               |  |     +-----------------+    |
               |  +-----|-------------------+  |
               |        |                   |  |
               v        v                   v  v
             +------------+          +------------+
             | Controller |<-------->|  Collector |
             +------------+          +------------+
```

Although there are considerable similarities between the proposed reference model and the LMAP framework [I-D.ietf-lmap-framework], it should be noted that the above architecture is provided as a more general outline of an integral collection of functional components collaborating in performing a specific instance of passive measurement method. Various functions from LMAP framework in performing a passive measurement task represent a specific way of realizing the general model.

Controller: A entity that exchanges the Control of the Measurement Task with the Measurement Entity, receives the Report from the

Collector and conducts the value calculation/derivation for the metrics measured of the Measurement Task. When multiple Measurement Entities are involved for a certain Measurement Task, Controller may only have Control exchanged with one or some of the Measurement Entities.

Collector: A entity that receives a Report from a Measurement Entity and provides the Report to the Controller for metric calculation / derivation.

Measurement Agent: An entity that exchanges the Control of the Measurement Task with the Controller, performs Measurement Tasks and sends the Report to Collector. When multiple Measurement Agents are involved for a certain Measurement Task, Coordination may be required between Measurement Entities.

Control: The collective description of information exchanged between Controller and Measurement Agent, i.e. configurations, instructions, states,etc. for a Measurement Agent to perform and Report Measurement Tasks.

Coordination: [TBD. Discuss coordination with MAs and Controller]

Report: The set of Measurement Results and other associated information as defined by the Control.

[Measurement Task]: The act that consists of the single operation of the Measurement Method at a particular time and with all its Input Parameters set to specific values.

[Measurement Result]: The output of a single Measurement Task (the value obtained for the parameter of interest or Metric).

[Note: further discussion and clarifications regarding these borrowed terms from LMAP framework are to be expected, with coordination with [I-D.ietf-lmap-framework].]

5 Methodology

For a given set of well-defined metrics, a number of distinct measurement methodologies may exist. Let us take One-way Packet Loss as example. Packet loss over a path is the difference between the number of packets transmitted at the starting interface of the path and received at the ending interface of this path. In order to perform packet loss measurements on a live traffic flow, different methodologies exist. A partial list includes:

1.Observation, e.g. Sequence Number, pros and cons

2.inserting a delimiting packet: Y.1731, RFC6374, pros and cons

3.altering the packet: Coloring/PDM

Note: This list is by no means exhaustive. The purpose is to point out the variety of measurement techniques.

Note: A methodology for a metric should have the property that it is repeatable: if the methodology is used multiple times under identical conditions, it should result in consistent measurements. A methodology for a metric should be scalable, robust and secured.

6 Methodology Design Considerations

This section gives the functional requirements and design considerations of any passive measurement methodology.

6.1 Discussion of Errors / Unintended Consequences

As discussed in Section 6.3 Measurements, Uncertainties and Errors of RFC2330, the measurement technique itself can introduce errors.

"consider the timing error due to measurement overheads within the computer making the measurement, as opposed to delays due to the Internet component being measured. The former is a measurement error, while the latter reflects the metric of interest. Note that one technique that can help avoid this overhead is the use of a packet filter/sniffer, running on a separate computer that records network packets and timestamps them accurately."

With some types of passive measurement, changing the packet may create extra load on the network, change the characteristics of network traffic, or change the nature of the problem itself. Obviously, the benefits of the measurement must be such as to offset the potential unintended consequences.

6.2 Control Protocol

As depicted by the reference model, there are different functional components residing along an end-to-end path or within an ISP's domain that cooperate to perform a specific passive measurement task. This section describes the high level function requirements for the control protocol between these collaborating components.

Note: LMAP is developing the control protocol between MA and controller, here will be the discussion for control protocol between measurement parties, i.e. MA to MA or MA to MP.

6.3 Measurement Session Management

A measurement session refers to the period of time in which measurement for certain performance metrics is enabled over a forwarding path. A measurement session may be started either proactively or on demand. The methodology must indicate how the measurement session is to be started.

6.4 Measurement Configuration

A measurement session can be configured statically or dynamically. The methods must be discussed.

6.5 Scalability and Robustness

7 Security Considerations

This document does not bring new security issues to IPPM.

8 IANA Considerations

This document has no actions for IANA.

9 Acknowledgements

The authors would like to thank Al Morton, Brian Trammell and Robert Hamilton for their valuable comments.

10 References

10.1 Normative References

[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.

[RFC5835] Morton, A. and S. Van den Berghe, "Framework for Metric Composition", RFC 5835, April 2010.

10.2 Informative References

[draft-PDM] Elkins, N., et al, "IPPM Considerations for the IPv6 PDM Extension Header", draft-elkins-ippm-pdm-metrics-04 (work in progress), April 2014

[I-D.manyfolks-ippm-metric-registry] Bagnulo, M., Claise, B., Eardley, P., and A. Morton, "Registry for Performance Metrics", draft-manyfolks-ippm-metric-registry-00 (work in progress), February 2014.

[draft-coloring] Chen, M, et al, "Coloring based IP Flow Performance Measurement Framework", draft-chen-ippm-coloring-based-ipfpm-framework-01 (work in progress), November, 2013.

[I-D.ietf-lmap-framework] Eardley, P., Morton, A., Bagnulo, M., Burbridge, T., Aitken, P., and A. Akhter, "A framework for large-scale measurement platforms (LMAP)", draft-ietf-lmap-framework-05 (work in progress), May 2014.

Authors' Addresses

Lianshu Zheng
Huawei Technologies
China

Email: vero.zheng@huawei.com

Nalini Elkins
Inside Products, Inc.
USA

Email: nalini.elkins@insidethestack.com

Lingli Deng
China Mobile
China

Email: denglingli@chinamobile.com

Michael Ackermann
Blue Cross Blue Shield of Michigan
USA

Email: mike.ackermann@bcbsmi.com

Greg Mirsky

Ericsson
USA

Email: gregory.mirsky@ericsson.com