Packet Pair Gap Metric
draft-cheng-ippm-packet-pair-gap-00.txt

Abstract

This document describes a metric for network performance. This metric is based on the time difference of a continuous packet pair which are sent back-to-back from the source IP address to the destination IP address. The basic packet pair probing can be used to measure the capacity of an end-to-end path.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and 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 is at http://datatracker.ietf.org/drafts/current/.

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

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

This Internet-Draft will expire on December 22, 2011.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect
Table of Contents

1. Introduction ...................................................... 4
2. Terminology ...................................................... 5
3. A singleton definition of pgap .................................... 5
   3.1. Metric Parameters ........................................... 5
   3.2. Metric Unit .................................................. 6
   3.3. Definition .................................................. 6
   3.4. Discussion .................................................. 6
4. Definition of pgap variation ...................................... 7
   4.1. Metric name .................................................. 7
   4.2. Metric parameters .......................................... 7
   4.3. Metric Unit .................................................. 8
   4.4. Definition .................................................. 8
   4.5. Discussion .................................................. 9
5. Security Considerations ........................................... 9
   5.1. Denial-of-Service Attacks .................................. 9
   5.2. Privacy/Confidentiality .................................... 9
   5.3. Integrity ................................................... 9
References ...................................................................... 10
Acknowledgments ....................................................... 10
Author’s Addresses .................................................... 10
1. Introduction

This memo defines a metric for time difference between 'back-to-back' IP Packet Pair on end-to-end network paths. It builds on the notions and conventions introduced in the IP Performance Metric (IPPM) framework [RFC2330].

Active end-to-end probing techniques, where probe packets are injected into network, are widely used in network measurement system. There are two primary classes: the one-packet methods and the packet pair family. The one-packet methods are based on the assumption that the transmission delay is proportional to the probe packet size. This idea was first introduced by V. Jacobson in his tool "pathchar". The packet pair family is based on the fact that the minimum inter-departure time of consecutive packets is attained when they are back-to-back. The basic packet pair probing can be used to measure the capacity of a end-to-end network path, i.e. the bottleneck bandwidth. First of all, there is no background traffic at the link. The source sends multiple packet pairs to the receiver. Each packet pair consists of two packets of the same size and is sent back to back. The receiver can obtain the dispersion of a packet pair by calculating the time distance between the last bit of each packet. With this dispersion, the path capacity can be obtained. When there is background traffic, the available bandwidth and the path capacity can still be measured using packet pair method. To decrease the influence of the background traffic, the packet train technique, which is based on packet pair technique, is used. The source sends multiple back-to-back probe packets to the receiver. The dispersion of this packet train is the time distance between the first packet and the last one. There are still several improved methods of packet pair probing technique, such as packet quartets which combines two packet pairs and so on. With the capability of estimating the path capacity and available bandwidth as referred above, they can also be used to observe the changes of network stated in order to control the flow rate properly, to measure the network loss, to avoid network congestion, to estimate the network delay, even to measure the link quality in wireless networks and so on. In this draft, we simply define the basic packet pair model.

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 [RFC2119].
2. Terminology

Terms used in this document that are defined in the Terminology section of the IPPM Protocol [RFC2330] document are to be interpreted as defined there.

IP packet One-way-delay and IP packet delay variation are defined in RFC2679 and RFC3393. Metric here originates from a more special send method from the source addresses, and it was used in RFC2544 to describe the frames used to do equipment test.

Here we use back-to-back packet in IP level, and define IP type-P back-to-back packet group similarly in the following: IP Type-P packets presented at a rate such that there is the minimum legal separation for a given medium between type-P packets over a short to medium period of time, starting from an idle state.

In addition, this document defines the following terms

IP Type-P back-to-back packet pair: An IP type-P back-to-back packet group has 2 packets as its members.

Pgap: The time difference of arrival times of two packets which are sent back-to-back from the same source at the measurement point.

3. A singleton definition of pgap

In this section, we specify definitions for IP type P back-to-back packet pair gap (pgap). It is the time difference of arrival times of two packets which are sent back-to-back from the same source at the measurement point.

3.1. Metric Parameters

+ Src, the IP address of a host
+ Dst, the IP address of a host
+ MP, the measure point
+ T1, a time
+ T2, a time
+ L, a packet length in bits. The packets of a Type P packet pair MUST be of the same length.
+ P, the specification of the packet type, over and above the source and destination addresses.
3.2. Metric Unit

The value of a IP Type-P back to back packet pair gap time is either a real number of seconds (positive, zero, negative) or an undefined number of seconds.

3.3. Definition

We are given a Type P packet pair, and they are sent from the Src in back-to-back way. T1 is the wire-time at which the measure point or Dst received the first packet of the Type P packet pair. T2 is the wire-time at which measure point or Dst received the latter packet of the Type P packet pair. Therefore the time difference between T1 and T2 is value of our metric. So \( P_{gap} = T_2 - T_1 \).

The Type P \( P_{gap} \) from Src to Dst is "undefined" means that Src sent Type P packet pair in back-to-back way and that Dst did not receive one or both packets.

3.4. Discussion

There are some practical issues to be considered.

+ This metric is less sensitive to clock synchronization problems.

The metric definition depends on the IP Type P back-to-back packet pair that has been measured. They SHOULD be consecutive packets with no time interval from one source and heading for the same destination.

Being a differential measurement and use the same clock at the MP or Dst, this metric is has barely nothing to do with clock synchronization problem.

In [RFC2330], "skew" is defined as derivative of the offset of a clock with respect to "true time" and "drift" as the second derivative of the offset of a clock with respect to "true time".

Since in this metric, only one clock is used here, and discussion of "relative skew" and "relative drift" between two clocks is needless.

NOTE: The drift of a clock, as it is above defined over a long period must have an average value that trends to zero while the period becomes large since the frequency of the clock has a finite (and small) range. In order to underline the order of magnitude of this effect, it is considered that the maximum range of drift for commercial crystals is about 50 part per million (ppm). Since it is mainly connected with variations in operating temperature (from 0 to...
70 degrees Celsius), it is expected that a host will have nearly constant temperature during its operation period, and variations in temperature, even if quick, could be less than one Celsius per second, and range in the order of a few degrees. The total range of the drift is usually related to variations from 0 to 70 Celsius. There are important points for evaluation of precisions of our measurement.

+ A methodology will have to include a way to determine whether a delay value is infinite or whether it is merely very large (and the packet is yet to arrive at Dst). As noted by Mahdavi and Paxson, simple upper bounds (such as the 255 seconds theoretical upper bound on the lifetimes of IP packets [Postel: RFC 791]) could be used, but good engineering, including an understanding of packet lifetimes, will be needed in practice.

Comment: Note that, for many applications of these metrics, the harm in treating a large delay as infinite might be zero or very small. A TCP data packet, for example, that arrives only after several multiples of the RTT may as well have been lost.

+ As with other ‘Type-P’ metrics, the value of the metric may depend on such properties of packet as protocol, (UDP or TCP) port number, size, and arrangements for special treatment (as with IP precedence or with RSVP).

+ If the packet is duplicated along the path (or paths) so that multiple no-corrupt copies arrive at the destination, then the packet is counted as received, and the first copy to arrive determines the packets’ pgap.

+ If the packet is fragmented and if, for whatever reason, reassembly does not occur, and then the packet will be deemed lost.

4. Definition of pgap variation

4.1. Metric name

In this section, we specify definitions of IP type P back-to-back packet pair gap variation (pgapv).

4.2. Metric parameters

+ Src, the IP address of a host
+ Dst, the IP address of a host
+ MP, the measure point
+ T1, T2, T3, T4, times
+ L, a packet length in bits. The packets of a Type P packet pair MUST be of the same length.
+ P, the specification of the packet type, over and above the source and destination addresses.
+ F, a selection function defining unambiguously the two back-to-back packet pairs from the packet pair stream selected for the metric.
+ I1, I2, times which mark that beginning and ending of the interval in which the packet pair stream from which the singleton measurement is taken occurs.

4.3. Metric Unit

The value of a Type-P pgapv is either a real number of seconds (positive, zero or negative) or an undefined number of seconds.

4.4. Definition

Given a Type P back-to-back packet stream and I1 and I2 such that the first Type P packet pair to pass measurement point MP1 after I1 is give index 0 and the last Type P packet to pass measurement point MP1 before I2 is given the highest index number.

Type-P back-to-back IP packet pair gap variation is defined for two packet pairs from Src to Dst selected by the selection function F, as the difference between the value of the Type-P back-to-back IP packet pair gap from Src to Dst and the value of the Type-P back-to-back IP packet pair gap from Src to Dst. T1 and T2 are the wire-time of first packet and last packet in first Type-P packet pair. T3 and T4 are the wire-time of first packet and last packet in the second Type-P packet pair.

Therefore, for a real number dT "the Type-P back-to-back IP packet pair gap variation from Src to Dst at T1, T2, T3, T4 is dT" means that Src send two packet pairs, the first packet in first packet pair was received at wire-time T1 (first bit), and second at wire-time T2 (first bit) and the first packet in second packet pair was received at wire-time T3(first bit) and the second at wire-time T4 (first bit), and that dT=(T4-T3)-(T2-T1).

"The Type-P back-to-back packet pair gap variation from Src to Des at T1, T2, T3, T4 is undefined" means that Src sent the two IP packet pairs but the Dst did not receive all packets.
4.5. Discussion

The metric definition depends on a stream of Type-P back-to-back IP packet pairs that have been measured. In general this can be a stream of two or more back-to-back IP packet pairs, delimited by the interval endpoints I1 and I2. There must be a stream of at least two packet pairs in order for a singleton pgapv to take place. The purpose of the selection function is to specify exactly which two packet pairs from the stream are to be used for the singleton measurement.

In this document it is assumed that the Type-P packet pair stream is generated according to the Poisson sampling methodology described in [RFC2330].

The reason for Poisson sampling is that it ensures an unbiased and uniformly distributed sampling of times between I1 and I2. However, alternate sampling methodologies are possible.

5. Security Considerations

This metric has the same security properties as the one-way-delay metric [RFC2679], and thus they inherit the consideration of that document. The reader should consult [RFC2679] for a more detailed treatment of security considerations. Nevertheless, there are a few things to highlight.

5.1. Denial-of-Service Attacks

It is still possible that there could be an attempt at a denial of service attack by sending many measurement packets into the network. In general, legitimate measurement must have their parameters carefully selected in order to avoid interfering with normal traffic.

5.2. Privacy/Confidentiality

The packets contain no user information, and so privacy of user data is not a concern.

5.3. Integrity

There could also be attempts to disrupt measurements by diverting packets or corrupting them. To ensure that test packets are valid and have not been altered during transit, packet authentication and integrity checks may be used.
References


Acknowledgments

This work is materially supported by the National Key Technology Program of China under Grant No.2008BAH37B04, the National Grand Fundamental Research 973 program of China under Grant No. 2009CB320505, the National Nature Science Foundation of China under Grant No. 60973123.

Author’s Addresses

Guang Cheng  
School of Computer Science and Engineering  
Southeast University  
Sipailou No.2, Nanjing, P.R.China  
Phone: +86 25 83794000  
Email: gcheng@njnet.edu.cn

Jian Gong  
School of Computer Science and Engineering  
Southeast University  
Sipailou No.2, Nanjing, P.R.China  
Phone: +86 25 83794000  
Email: jgong@njnet.edu.cn

Haiting Zhu  
School of Computer Science and Engineering  
Southeast University  
Sipailou No.2, Nanjing, P.R.China  
Phone: +86 25 83794000  
Email: htzhu@njnet.edu.cn

Hua Wu  
School of Computer Science and Engineering  
Southeast University
