END-TO-END PACKET DELAY IN THE NETWORK

Vitali Aivazov, Roman Samkharadze
Georgian Technical University

Summary

In network performance evaluation and application quality assurance, delay is one of the fundamental parameters to consider. End-to-end delay provides the characteristics of application responsiveness and influences maximum achievable throughput. Measuring end-to-end delay is complex and several components can be distinguished. The information of one-way delay is also applied to available bandwidth estimation and topology changes during extensive periods of time. The main causes of delay are reviewed in this article, followed by a variety of tools that have been developed for delay measurements. The most widely used from them are evaluated in this work, along with evaluation of their advantages and limitations. An overall conclusion is made for applicability of these tools.

Keywords: delay. Latency. Packet delay variation. Jitter. PDV. RTT. ping. traceroute. pathchar. httping.

1. Introduction

The network delay represents an important design and performance characteristic of a computer network or telecommunications network. The delay of a network identifies a period of time a bit of data needs to be delivered across the network from a source node to the destination. It is typically measured in multiples or fractions of seconds. The delay is counted from the start of the packet being transmitted at the source to the end of that packet being received at the destination. A component of the delay which does not vary from packet to packet can be ignored, hence if the packet sizes are the same and packets always take the same time to be processed at the destination then the packet arrival time at the destination could be used instead of the time the end of the packet is received. A delay may differ slightly, depending on the location of the specific pair of communicating nodes. Although users are concerned about the total delay of a network, a precise measurement needs to be performed. Thus, usually both the maximum and average delays are measured. The causes of packet delay in the network can be divided into several parts, which are transmission delay, propagation delay, processing delay and queuing delay.

An overview of sources of delay and delay measurement tools like ping, traceroute, pathchar and httping are demonstrated and an impact of delay and Packet Delay Variation (PDV) on data and voice are analyzed.

2. Terminology

The sources of network delay can be divided into several parts and they are explained below [1].

A. Processing delay

The processing delay is the time needed to process a packet on each hop. In a network based on packet switching, processing delay is the time it takes routers to process the packet header. Processing delay is a key component in network delay. During processing of a packet, routers may check for bit-level errors in the packet that occurred during transmission as well as determining where the packet's next destination is. Processing delays on high-speed routers are typically in the order of microseconds or less. In the past, the processing delay was ignored as insignificant compared to the other forms of network delay. However, in some systems, the processing delay can be quite large, especially where routers are performing complex encryption algorithms and examining or modifying packet content. A deep packet inspection done by some networks examine packet content for security, legal, or other reasons, which can cause very large delay and

thus is only done at selected inspection points. Routers performing network address translation also have higher than normal processing delay because those routers need to examine and modify both incoming and outgoing packets. After this nodal processing, the router directs the packet to the queue where further delay can happen, which is called queuing delay.

B. Queuing delay

The queuing delay is the time needed to wait in a router queue before transmission. When packets arrive at a router, they have to be processed and transmitted. The queuing delay occurs on those network devices where packets from different ingress ports are destined to the same egress port concurrently. A router can only process one packet at a time from each egress port. The other packets must be queued for sequential transmission. If packets arrive faster than the router can process them, such as in a burst transmission, the router puts them into the queue which is also called the buffer, until it can transmit them. This interface contention is called head-of-line blocking and can lead to substantial latency and PDV. The maximum queuing delay is proportional to a buffer size. The longer the line of packets waiting to be transmitted, the longer the average waiting time is, and when the buffer fills, the router must drop packets.
Once packets are released from the queue, they are converted to bits and serialized into the physical line.

C. Transmission delay

The transmission delay is the time needed to convert data packets to or from optical/electrical signals on a physical link to values in a dedicated memory buffer. In other words, this is the delay caused by the data-rate of the link.

The transmission delay is a function of the packet's length and has nothing to do with the distance between the two nodes. This delay is proportional to the packet's length in bits,

$$D_T = \frac{N}{R},$$

where D_T is the transmission delay, N is the number of bits, and R is the rate of transmission.

Most packet switched networks use store-and-forward transmission at the input of the link. A switch using store-and-forward transmission will receive (save) the entire packet to the buffer and check it for CRC errors or other problems before sending the first bit of the packet into the outbound link. Thus store-and-forward packet switches introduce a store-and-forward delay at the input to each link along the packet's route.

D. Propagation delay

The propagation delay is the time needed for signals to travel through a medium such as Fiber optic, copper, or air. The properties of the medium, such as the reflective index of glass or the electron propagation through copper, impose a limit on propagation delay times. Propagation delay is equal to d/s where d is the distance and s is the wave propagation speed. In wireless communication, s=c, i.e. the speed of light. In copper wire, the speed s generally ranges from .59c to .77c.

E. Packet delay variation

Along with the end-to-end packet delay, network performance can be characterized with a packet delay variation or PDV. In computer networking, PDV is the difference in end-to-end one-way delay between selected packets in a flow with any lost packets being ignored [2,3]. The PDV is also referred to as a "jitter". This phenomenon is very critical for certain types of applications, especially for Voice over IP and interactive applications. Instantaneous packet delay variation is

the difference between successive packets. As an example, let us consider packets that are transmitted every 20 ms. If the 2nd packet is received 30 ms after the 1st packet, PDV = –10 ms. This is referred as dispersion. If the 2nd packet is received 10 ms after the 1st packet, IPDV = +10 ms. This is referred as clumping [2,3].

F. Round-trip time

Another term used in network delay evaluation is Round-trip time or RTT. It is also called a round-trip delay and represents the time required for a signal pulse or packet to travel from a specific source to a specific destination and back again. In this context, the source is a host initiating the signal and the destination is a remote system that receives the signal and retransmits it. In a network, particularly a WAN or the Internet, RTT is one of several factors affecting latency, which is the time between a request for data and the complete return or display of that data to the user. The RTT can range from a few milliseconds under ideal conditions between closely spaced points to several seconds under adverse conditions between points separated by a large distance. A theoretical minimum is imposed on the RTT because it can never be less than the total length of time the signals spend propagating in or through the transmitting media.

3. Tools to measure delay

Ping

Ping is probably the most widely used utility for delay measurement. It stands for "Packet Internet Groper" [4] and operates based on the Internet Control Message Protocol (ICMP) Echo function, described in RFC 792 [5] ICMP are certain type of IP control messages, with protocol number 1 [6] that are used to exchange network information between two hosts. Ping operates by sending ICMP echo-request packets to the destination host and waiting for an ICMP response. When a destination host receives an echo-request, it responds with an echo-reply packet, placing the original echo-request packet into the data field of the echo-reply.

The packet structure of an ICMP echo request/reply message is illustrated on the figure 1, and some of the fields are explained below. The Type field of the message identifies whether it is echo-request (type 8) or echo-reply (type 0) or any other type of ICMP message. This field is 8 bits long which is followed by a Code field that is applicable for only certain types of ICMP messages and stores the description of the message carried by the reply packet. The next field of the header is an Identifier, which is set in the request packet, and echoed back in the reply, to be able to keep different ping requests and replies together. A Sequence number field identifies the sequence number for each request. Generally, this starts at 1 and is incremented by 1 for each packet.

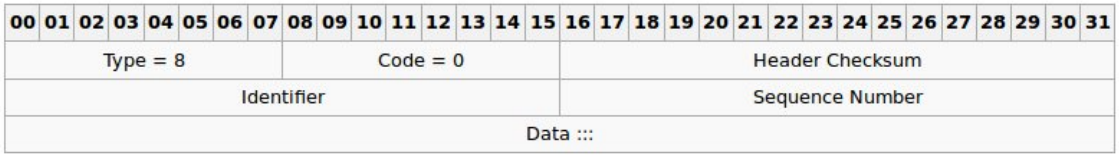

Fig.1. ICMP echo request/reply message header

On the Figure 2 there is displayed an output of ping utility on the lab PC running Linux. In this example, the host "lab" is pinging the official web server www.gtu.ge of the Georgian Technical University. The PC sends one ICMP echo-request packet every second to the web server.

```
user@lab:~$ ping www.gtu.ge
PING spider.gtu.ge (217.147.232.2) 56(84) bytes of data.
64 bytes from 217.147.232.2: icmp_req=1 ttl=44 time=74.2 ms
64 bytes from 217.147.232.2: icmp_req=2 ttl=44 time=76.6 ms
64 bytes from 217.147.232.2: icmp_req=3 ttl=44 time=74.8 ms
64 bytes from 217.147.232.2: icmp_req=4 ttl=44 time=73.7 ms
64 bytes from 217.147.232.2: icmp_req=5 ttl=44 time=76.1 ms
64 bytes from 217.147.232.2: icmp_req=6 ttl=44 time=73.3 ms
--- spider.gtu.ge ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 33422ms
rtt min/avg/max/mdev = 73.343/75.718/81.029/2.466 ms
```

Fig.2. The output of ping utility to www.gtu.ge web server

After receiving each echo-reply packets, ping utility prints out a line with IP address of the target. It can be accompanied by the hostname of the replying machine, followed by the sequence number of the echo-request that this reply belongs to and Time To Live value. Finally, in the end of the line there is a Round Trip Time value. The sequence number represents the unique identifier of each echo-request sent to the target and the reply back to it. This number starts from 1 and reflects which reply has been received back. The skipped sequence number can indicate that echo-reply packet related to that particular sequence number has been lost or dropped. This can be caused by lost echo-request or echo-reply never reached back the source. The reasons behind that can be various, for instance failing physical line, or over-utilized link or others. In general, with TCP/IP protocols, a packet loss below 0.1% can be tolerated. However, if this value is higher, then it can dramatically slow down the performance of an application or even make it unusable. The results of the test are printed in the form of a statistical summary of the reply packets received, including the minimum, maximum, round-trip-times, and the PDV. A tool Ping is straightforward in usage, which draws quite clear picture of the state of the network. It can be run continuously in the background. The ping command can be run with various special operational modes. For instance: by specifying the packet size used as the probe, automatic repeated operation for sending a specified count of probes and time stamping. There are certain extra software types to draw graphs based on the reports provided by ping utility.

Traceroute

Traceroute is a powerful network tool for tracing the path that a packet takes from the source to the destination. It sends a sequence of ICMP echo-request packets to a destination host determining the intermediate routers traversed by the packets. In order to achieve that, traceroute adjusts the time-to-live (TTL) value in the IP header. By default, for the Windows platform, any packet sent from the system has the default starting value of TTL set to 128. However, for Linux based systems it is 64.

Routers along the path decrement this value by 1 and discard a packet when the TTL value has reached zero. When the router decrements this value and it reaches 0, a returning ICMP error message is sent back to the source with ICMP Time Exceeded code. In a context of traceroute, to display the path a packet takes, it sets the value of TTL of the first probe packets to 1, ensuring that these packets will not be forwarded further by the first router along the path. While discovering each hop, traceroute sends 3 probe packets with the same TTL value which are compared to each other and statistics of min, max and average RTT are printed out in the line for that hop.

The next probe set has this value equal to 2, so that the first router will decrement them by one (TTL value becomes 1 at this point) and forwards them further to the second router, which in turn will decrement the TTL to 0 and send the error "Time Exceeded" reply message back to the source. This process continues until the destination host receives the packets. In order for traceroute to identify the destination hop, it sends User Datagram Protocol (UDP) datagrams with high destination port numbers ranged from 33434 to 33534 on Unix based operating systems. This makes it unlikely for the destination host to be using the same high range ports for any application [4]. When the destination host receives a UDP datagram with TTL 1, it doesn't discard it, because it does not need to be routed further, so it checks the UDP socket for that particular port, and generates ICMP "Port unreachable" message back to the source. This is an indication for traceroute that the packet has reached the destination. The traceroute utility usually has an option to specify whether to use ICMP echo-request (type 8) instead or not, as used by the Windows implementation.

This technique helps to identify each transit hop that a packet passes and provides some useful information back to the source. The Traceroute uses the returned ICMP messages to generate a list of network devices that the packets have traversed. The timestamp values returned for each hop along the path represent the IP address and possibly accompanied by DNS hostname of the hop, delay values, typically measured in milliseconds for each packet. A sample traceroute output is presented below on the figure 3, where the path to the web server of the Georgian Technical University is traced from a test machine located over the Internet.

```
user@lab:~$ traceroute www.gtu.ge
traceroute to www.gtu.ge (217.147.232.2), 30 hops max, 60 byte packets
1  192.168.1.1 (192.168.1.1)  6.125 ms  21.723 ms  22.831 ms
 2  * * *
 3  ip-86-49-52-129.net.upcbroadband.cz (86.49.52.129)  23.980 ms  24.979 ms  25.684 ms
4  84.116.220.237 (84.116.220.237)  39.868 ms  43.673 ms  44.004 ms
5  84.116.221.37 (84.116.221.37)  45.360 ms  49.171 ms  53.141 ms
6  cz-prg02a-ra1-ge-1-0-0.0.aorta.net (213.46.172.26)  53.442 ms 213.46.172.222 (213.46.172.222)
   31.931 ms *
7  cz-prg01a-ra1-ge-0-0-0-v50.aorta.net (213.46.172.18)  34.718 ms  40.163 ms  40.627 ms
8  prag-bb1-link.telia.net (213.155.131.62)  50.814 ms prag-bb1-link.telia.net (213.155.132.164)
   51.288 ms prag-bb1-link.telia.net (213.155.131.64)  59.871 ms
9  sfia-b2-link.telia.net (80.91.247.83)  90.358 ms  90.664 ms sfia-b2-link.telia.net (80.91.253.249)
   92.478 ms
10  ccsbulgaria-ic-153568-sfia-b2.c.telia.net (80.239.192.242)  124.232 ms  141.254 ms  141.622 ms
11  host-80-241-177-246.customer.co.ge (80.241.177.246)  137.021 ms  140.554 ms  76.819 ms
12  217.147.237.18 (217.147.237.18)  76.097 ms  75.658 ms  78.117 ms
13  217.147.237.173 (217.147.237.173)  88.551 ms  88.893 ms  89.904 ms
14  217.147.237.65 (217.147.237.65)  80.538 ms  80.842 ms  90.236 ms
15  217.147.237.102 (217.147.237.102)  90.531 ms  90.828 ms  91.500 ms
16  217.147.237.82 (217.147.237.82)  89.137 ms  89.482 ms  91.146 ms
17  217.147.232.130 (217.147.232.130)  92.778 ms  75.081 ms  73.941 ms
18  217.147.232.2 (217.147.232.2)  74.817 ms  72.805 ms  73.706 ms
```

Fig.3. The output of the traceroute tool to www.gtu.ge web server

On the second hop given in the figure 3, there are stars instead of numbered values. The reason behind it is that the originating host expects a reply within a specified number of seconds. If a packet is not acknowledged within the expected timeout, an asterisk is displayed. ICMP

packets on the routers are processed by CPU, which can be highly utilized, or simply ICMP error reporting may be disabled. However, this is not an obstacle for traceroute to continue tracing the path. After a timeout, the source generates another packet with increased value of TTL to reach the next hop behind the one that didn't reply. The hosts listed in the example may differ from the hosts used by other packets between the same pair of source and destination. The IP protocol does not require that packets between two hosts always take the same route. There may be a load balancing occurring somewhere in the network, or network has been re-converged.

Pathchar

Pathchar is another tool for assessing various characteristics of links along the Internet path. It estimates the bandwidth, the latency or the queuing delays characteristics of links along the path. For achieving that, Pathchar measures the round trip time (RTT) of the packets sent from a source host. The important difference between Pathchar and Traceroute is that Pathchar implements a packet train analysis technique. A packet train represents a series of probe packets sent along the path. The estimation of link characteristics as bandwidth value and RTT is performed by analysing the packets of different trains.

Similarly to Ping and Traceroute, Pathchar uses the TTL field in a packet's IP header, however, with variable packet sizes. The source address of the ICMP error message identifies the router, where the packet has expired. It sets the TTL to a value n, which in turn makes it possible to distinguish the address of the n-th router in the path. By measuring each probe sent, Pathchar estimates the RTT to each hop, which is the time until the error ICMP message has been received. It collects the results of analysis of these measurements and generates statistics of link's bandwidth, latency and queuing delay. By increasing the packet size, which in turn increases the RTT, Pathchar assumes that increment of RTT is caused by queuing delay, which can be estimated by considering the queuing delays of previous links.

Pathchar accurately reports characteristics of the bandwidth, latency and packet loss of each hop along the path and represents a powerful tool for latency and available bandwidth estimation [6].

Httping

Although measurement tools reviewed above are powerful instruments for measuring end-to-end delay, there are certain cases when it is problematic to use ICMP protocol. The reason behind it is that ICMP protocol can be blocked on the path or rate limited, which can lead to inaccurate reports or to complete fail. Another limitation of delay estimation on the layer 3 is that it doesn't estimate service response time that users are most sensitive to. Httping represents one of the tools for higher level of the end-to-end delay testing, essentially to measure a server's response time. This tool is similar to legacy ping. However, it is operating on a transport layer, setting up a connection to a web server on a specific port and measuring latency. This technique directly reflects the user's experience of accessing resources and represents a valuable tool for application performance monitoring.

4. Conclusion

The ability to measure metrics such as delay of the path, packet delay variation and transport layer latency are essential for achieving high performance of an application. In this work, we presented several of the most widely used tools and methodologies for such measurements and distinguished their advantages and limitations. They include Ping, Traceroute, Patchar, and httping. Ping is a simple in use utility that provides RTT and other useful statistics of the network. However, traceroute and pathchar provide vaster statistics, but require more complex analysis in terms of collecting and computing the data. Httping represents a tool for measuring transport layer

delay metrics, in other words to measure a latency the user is experiencing while accessing some web resources. Consequently, such tools can be integrated into the application based routing system and contribute in the application performance monitoring with a goal of choosing a path with best quality of service metrics.

References:

1. Hernandez A., Magana E. One-way Delay Measurement and Characterization. Universidad Publica de Navarra, Pamplona. Spain. IEEE. 2007, pp.114

2. Morton A., Claise B. Packet Delay Variation Applicability Statement. Cisco Systems, RFC5481, March 2009. pp.10-12

3. IP Packet Delay Variation Metric for IP Performance Metrics (IPPM). RFC3393 IETF, 2002. pp.2-6

4. W. Richard Stevens, TCP/IP Illustrated, Volume 1: The Protocols. Addison-Wesley, 1994, ISBN 0-201-63346-9. pp.85-109

5. J. Postel, Internet control message protocol, RFC792, ISI, 1981, pp.2-20

6. J. Reynolds, J. Postel, Assigned Internet Protocol Numbers. IANA, ISI, 1992, pp.7-23

7. Allen B. Downey, Using pathchar to estimate Internet link characteristics, Colby College, Waterville, ACM SIGGCOM, 1999, pp.241-250

კომპიუტერულ ქსელში კვანძთაშორის პაკეტების დაყოვნება

ვიტალი აივაზოვი, რომან სამხარაძე
საქართველოს ტექნიკური უნივერსიტეტი,

რეზიუმე

პაკეტების დაყოვნება არის ერთ-ერთი ფუნდამენტალური პარამეტრი ქსელის წარმადობის შეფასებისას და აპლიკაციების ხარისხის უზრუნველსაყოფად. კვანძთაშორის დაყოვნება წარმოადგენს აპლიკაციების რეაგირების მახასიათებელს და გავლენას ახდენს მაქსიმალურ მიღწევად გამტარუნარიანობაზე. კვანძთაშორის დაყოვნების გაზომვა საკმაოდ კომპლექსური ამოცანაა და ის შეიძლება იყოს დაყოფილი სხვა და სხვა კომპონენტებად. ერთი გზის დაყოვნების მონაცემები აგრეთვე გამოიყენება ხელმისაწვდომი გამტარუნარიანობის შეფასებისათვის და ტოპოლოგიის შეცვლისას დროის ვრცელ პერიოდში. ამ ამოცანის გადასაწყვეტად შემუშავებულია მრავალფეროვანი საზომი ინსტრუმენტები. სტატიაშია განხილულია მათ შორის ყველაზე ხშირად გამოყენებადი ინსტრუმენტები. განხილულია დაყოვნების ძირითადი მიზეზები, საზომი ინსტრუმენტები და აგრეთვე, მათი უპირატესობები და ნაკლი. გამოტანილია ზოგადი დასკვნები ამ ინსტრუმენტების გამოყენების შესაძლებლობაზე.

МЕЖ-УЗЛОВАЯ ЗАДЕРЖКА ПАКЕТОВ В КОМПЬЮТЕРНЫХ СЕТЯХ

Айвазов В.Ю., Самхарадзе Р.Ю.
Грузинский технический университет

Резюме

Задержка является одним из основных параметров оценки производительности сети и обеспечения качества обслуживания приложений. Меж-узловая задержка обеспечивает характеристики реакции приложений и влияет на максимально достижимую пропускную способность. Измерение меж-узловой задержки является комплексной задачей и может быть разделена на несколько компонентов. Информация односторонней задержки также применяется для оценки доступной пропускной способности и изменения топологии в течение обширных периодов времени. Для решения данной задачи, разработаны различные инструменты для измерения меж-узловой задержки. Самые широко используемые из них рассмотрены в данной работе. Разобраны основные причины задержки, а также рассмотрены преимущества и недостатки этих инструментов. В заключении рассматривается применяемость данных инструментов.