PingPlotter - How it really works

Overview

Just like with every great invention, a lot of people want to know what makes PingPlotter tick - which is exactly what we aim to illustrate in this article!

We"ll start by defining some network terms, followed by a brief explanation of their concepts. Finally, these things will all come together in the last section which will not only describe how PingPlotter works but hopefully, will enhance your understanding of network troubleshooting.

Definitions

Packet
A packet is a small amount of data sent over a network, such as a LAN or the Internet. Similar to a real-life package, each packet includes a source and destination as well as the content (or data) being transferred. When the packets reach their destination, they are reassembled into a single file or other contiguous blocks of data.

Packet Loss
When one or more of these packets fails to reach their intended destination

Network Latency
Describes a delay that takes place during communication over a network (including the Internet) - usually measured in milliseconds. Higher Latency = Longer Delay.

Ping
A ping is a signal sent to a host that requests a response. It serves two primary purposes: 1) to check if the host is available and 2) to measure how long the response takes. The ping command sends an ICMP Echo Request consisting of a single packet of data (often 32 or 56 bytes), and the host device should reply with an ICMP Echo Reply.

Sometimes, a company's network security policy requires ping (ICMP Echo Reply) to be disabled on all devices to make them more difficult to be discovered by unauthorized persons.

Traceroute
Traceroute, also called tracepath or tracert, is a TCP/IP network utility used to determine the path packets take from one IP address to another. It also measures the amount of time it took the data to get from one device to the next. This is possible through the use of the TTL (Time-To-Live) field.

Hop (hop count)
A hop count of X equates to having X gateways between the source host and destination host. For instance, your home router is typically hop #1, whereas the gateway to your ISP is often hop #2 (this can vary depending on how your network and your ISP"s network are configured).

Router

A networking device that routes or forwards data packets from one computer network to another.

Server
A computer that provides data to other computers. It may serve data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet.

Local Area Network (LAN)
A network of devices connected within a single, limited area. This could be confined to a house, apartment, or office floor but could very well apply to an entire building.

Wide Area Network (WAN)
A large network that is not limited to a single location (the Internet is one such example). A wide area network connects many different local area networks (LANs) and even other WANs. Access can be granted via different links, such as virtual private networks (VPNs), wireless networks, cellular networks, or Internet access.

The Internet
The internet is a global WAN meaning that it can connect with other wide area networks as well as local area networks. It includes many high-bandwidth data lines that comprise the Internet "backbone" (backbones interconnect various pieces of WANs).

These lines are connected to major hubs that distribute data to other locations, such as web servers and ISPs (Internet Service Providers). It is a global network of connections from millions of devices that facilitates the exchange of information (not to be confused with the World Wide Web).

How other things work

Traceroute

This network utility helps to determine the path that packets take (your data) through various networks to the destination by exploiting a field in the IP Packet Header called TTL (Time-To-Live), which is normally used to prevent routing loops (using Layer 3 of the OSI model).

The TTL field is usually initialized to a value of 64, which means that it can be passed along or transmitted up to 64 times by various devices en route before timing-out (expiring). Each time the packet reaches a router/hop, the value of the TTL field is decremented by 1.

Traceroute exploits this field by purposefully setting the TTL value so that it expires or times-out when it â€œhitsâ€• a router. The router will then return information about itself to the client using an ICMP Time-Exceeded message (type 11). Traceroute then sends out another packet using a higher TTL value that becomes forwarded to a router further down the network path.

Traceroute repeats this process until the packet reaches the destination, effectively mapping the path your packets take on their journey.

All information sent back to the client is provided by a network router"s ICMP Time Exceeded messages.

Ping

This network tool works by using your router to send some packets to an IP address you"ve specified in one way or another (such as a command-line ping), then waiting for the response. It uses an ICMP

Echo Request, or type 8 packet. If it"s configured to, the server or device at the destination will respond with an ICMP Echo Reply, or type 0 packet. The round-trip-time is then calculated and presented on your screen.

How PingPlotter works

With traceroute

By utilizing the traceroute utility, PingPlotter has the ability to collect information about each Layer 3 device in a data packet"s route to the destination. Using our fancy software and some skilled graphing, PingPlotter then translates that data into graphs and data tables within the user interface. Both ping and traceroute operate on Layer 3 of the OSI model

PingPlotter can even customize the packet parameters before they"re sent (and is slightly customized for the user by default). This allows the user to manipulate some properties of the packet to allow for a wider range of network investigative powers.

To get the most accurate reading of the destination, however, PingPlotter needs to additionally use a packet type that does not have a decrementing TTL value, such as ***ping (see below).***

With ping

Just before traceroute is initiated, PingPlotter uses an ICMP Echo Request, or ping, to â€œplaceâ€• the destination. This is helpful because, without it, the destination may prefer to reject or block the packet sent with traceroute (some routers/servers reject a packet with a TTL value), meaning the destination would appear offline or unavailable.

Using a ping request means that PingPlotter will always receive an appropriate response from the destination.

Interpreting Results

Combining traceroute with ping means that PingPlotter can both receive a response from the destination and gather important data from each Layer 3 device in the packet"s route.

As PingPlotter rapidly collects and presents this data in a colorful user interface, it"s up to the user to discern what it all means. Time to level-up your skill in Network Interpretation!

Because of the nature of traceroute, it"s necessary to work backward when interpreting your results. After all, you"re looking for where the network problem starts.

Correlation is everything when analyzing data trends. If there"s a pattern of poor latency and packet loss at the destination, then compare the patterns with the ones from other hops en" route. The pattern that is **most similar and furthest from the destination** is usually the offender.

This also means that packet loss and increased latency values are only relevant to the connection quality when they show up in the results of the following hop. So feel free to discard that pesky 50% packet loss at hop #1 that is not carrying through to other downstream hops (this explained further below!).

On that note, you may ask â€œWhy would a hop show 50% packet loss or increased latency, but the next

one is totally fine?â€•. To answer this question, we need to revisit how traceroute works its magic.

Using traceroute, PingPlotter collects data from ICMP Time Exceeded messages sent back by the routers leading up to the destination.

In this situation, a hop may block or set a low priority for sending Time Exceeded messages back to the client. PingPlotter â€œseesâ€• *that these messages aren"t being returned and, naturally, logs them as lost packets. Though a router may not send back ICMP Time Exceeded messages, it could still* ***forward packets with a higher TTL value to the next router.***