Illuminating a small network: Perspective from within

StrangeBit

2025

Contents

1. Introduction

1.1 Questions

In this section we enumerate research questions that we would like to answer in this report. We foresee at least three important questions in this report. Namely those are: **(i) What to measure in the enterprise networks?** By answering this question we attempt to shed the light on most important characteristics in the network traffic analysis. Be it latency, throughput, goodput, error and loss rate, availability. **(ii) How to measure?** Here we would like to answer how to perform the network measurements. For example, how to select vantage point, how to minimize the dataset, but still be able to grasp the most important characteristics of the network. **(iii) When to measure?** This question is also important for a number of reasons. Selecting correct measurement period and correct duration of the measurements intervals will have the important impact on the quality of the research outcome.

By answering these questions properly one can illuminate the performance of the networking infrastructure. Note, in this work we are considering only small networks, comprising 10-100 devices. However, we believe that these questions are also applicable to larger networks and more complicated topologies.

2. Background

This section consists of several important parts: First, we discuss main network characteristics of the network; Second, we describe various types of network topologies and device orchestrations; Third, we present various tools which are useful in enterprise network measurements; Finally, we discuss most wide spread network protocols to watch out for in the enterprise network traffic.

2.1 Basic network characteristics

We believe that there are several key network characteristics: delay, jitter, throughput, goodput, error and loss rates. All these metrics can be used to measure the performance of the networked systems. In the paragraphs that follow we will describe these metrics and try to explain why they are so important.

Delay is the time it takes for the packet (on network layer) to reach the other communication side. Delay can be one way or two way, also called *round trip time*. The former one is hard to measure since the clocks on both sides need to be synchronized. Technically, of course we can use sophisticated algorithms and packet trains to measure one way delay (for example, the reader can look at the RFC 7679 []). But most of the time people rely on half of the RTT. This metric is less accurate since the packets can travel different paths and, hence, delays can be different. But yet this metric is quite common. For example, *ping* utility reports RTT as the measure of delay. We should note that delay impacts user experience greatly, and therefore, it is good to have links with low delays.

Jitter is yet another important metric and is wide spread across network engineers. Jitter is the variation of the delay, that is jitter shows how much the delay is varying throughout time. This metric is important

because it can affect how the protocol timers are calculated. For example, if the jitter is high, the calculated timers can be inaccurate and, hence, the performance of such protocols can be undermined. Thus, the lower the jitter the better, in authors opinion, the performance of the networked devices. One easy way to compute jitter is to build the histogram of the network delays and compute the variance.

Throughput is also important and it captures how much data (including protocol headers and user payload) can be delivered throughout network system in predefined time interval. Typically, the throughput is measured in Kb/s, Mb/s and Gb/s. Obviously, the larger is the throughput the better network operates. Networks with large throughput can service larger number of clients. *Goodput* is the same as throughput, but excludes the control data from the calculations. In other words, packet header is excluded from the calculations and only user's payload is considered.

Error rate describes how often the packets arrive at the receiver with the corrupted bits. Most of the protocols use notion of reliability (that is if the data is corrupted it is requested again) and, hence, high error rate can reduce the performance of such protocols considerably. It is therefore important for the network engineers to avoid highly unstable links. Different media and operational environments have different error rates. For example, wireless links are often have grater error rate than wired and optical links. Also, different applications have different tolerance to errors. For example, Voice over IP and Video over IP require error rates to be low. Mail systems, on the other side, can tolerate high error rates, because the system works in the background and corrupted packets can be requested again.

Loss rate is the final metrics that we will cover. Loss occurs, for example, when intermediary routers drop the packet because of congestion and corruption of the packet. Once again, similar to error rates, sensitive applications do not operate well in lossy environments. Hence, typically, network engineers design systems so that such applications will use links with little loss, while other traffic such as HTTP and SNMP protocols can use less expensive, but yet, lossy links. Typically, congested and wireless links with weak signals and obstructed with concrete, for example, have higher loss rates than fat wired and optical links.

There are also other characteristics that can be measured, for example, the reader can take a look at the congestion and some other. But we are not going to cover those in this report.

2.2 Topologies

There are several key topologies that are used in enterprises: mesh, star and hybrid. *Mesh* topology is such topology in which every network element is connected to every other network element. The links can be wired, wireless and pseudo links (if we are talking about overlays). Mesh can be full and partial. In full mesh, obviously, ever element is connected every other element in the network. Consider, for example, personal area network in which all nodes are connected using wireless medium. Wired meshes are expensive, though, and are rarely used in modern deployments. Meshes are crucial, however, when availability is a must. In mesh, some nodes can fail, yet, the network will remain alive and packets will be delivered, not to all, but some devices at least.

Star topologies are cheaper and less fault tolerant. In star-like topology some node becomes the root, while others connected to the root element and all the traffic flows through it. Oftentimes, redundant links are added to the topology to bring some level of tolerance to failures. A typical star topology is shown in Figure **??**.

Finally, there are also hybrid topologies, such as *hub-and-spoke* networks. In this type of networks spoke nodes are connected to hubs, while hubs form a full mesh between each other. Such networks are cheaper than full mesh, but more fault tolerant than star topologies. A typical network is shown in Figure **??**.

2.3 Tools

Network engineers use wide variety of tools for measuring the permanence of the networks and in debugging tasks. All tools can be categorized based on tasks they are meant to be used for such as measuring and troubleshooting.

Measurement tasks: to measure performance of the network a common set of tools includes ping utility, tcpping utility, traceroute utility, nc tool, speedtest and iperf, snmp statistics reports by agents and direct queries. In the following paragraph we will describe these tools.

Ping utility is the most common tool to measure reachability of a host and measure the round trip times. The tool is based on the ICMP protocol which we will describe later. This tool is widely available in Linux, Windows, BSD and Unix operating systems.

TCPing is another common network tool to measure the reachability of the TCP port in the network. But the tool can be also used to measure the time to establish a TCP connection. To our best knowledge this tool is widely available for Windows OS without any charges.

speedtest and iperf utilities were primarily designed for measuring the bandwidth between two systems. The later one has client and server implementations. This means that to measure the bandwidth (both UDP and TCP connections can be used) one needs to start first the server with the -s flag, and only then run the client with -c flag.

treceroute is used often to trace the path the packet takes from host A to host B. The tool uses ICMP under the hood. Not only it is used to trace the reachability of the intermediate routers but it also reports the RTTs.

netcat, or nc is the tool that is available in Linux distributions and commonly used to send the commands to the server over UDP sockets. It can be used to measure the bandwidth. For example, network administrators can send large enough binary package to the server and measure the time it takes for the transmission to happen.

And finally *SNMP* can be used to collect reports from agents about network performance. Such characteristics as bytes per second delivered by the network interface, ping RTT and many more can all be collected from network devices either with direct queries or with the help of agents.

Trouble shooting. A set of tools available in this category. nmap, tcpdump, Wireshark, nslookup, dig, iproute, and ifconfig. All these tools are indispensable in analyzing and troubleshooting the network problems. It is essential for any network engineer to be acquainted and actively apply these tools. In the paragraphs that follows we will describe what every tool means, but briefly.

nmap is a tool that allows network engineer to detect open network ports (both UDP and TCP). Essentially, the tool scans the remote system and reports which port is open. Network engineers and hackers actively use this tool to detect weak points in the network systems.

tcpdump and Wireshark. These tools are helpful in collecting and analyzing network protocols. tcpdump is typically used to collect the raw packets and frames from the network interface of interest, while Wireshark is more advanced it can analyze the network traffic and export it to XML and JSON file formats. We ourselves use these tools in our network traffic analysis tasks.

nslookup and dig are used to detect the problems with the DNS servers

and queries. These tools are often used by network engineers to detect the problems with DNS and get information about remote systems.

iproute is a tool that can be used for multiple purposes, but primarily this tools is useful in configuring the routes to remote systems. For example, network engineers can use the tool to check whether the routes to remote hosts exist. It can be also used to add static routes. But these are just few examples.

And finally, *ifconfig* tool can be used to configure the network interfaces. For example, network engineers can use this tool to set default gateway, IP address on the interface, and set the DNS server name, either manually or with help of DHCP server.

2.4 Network protocols to watch out for

2.4.1 Spanning trees

2.4.2 TCP, UDP and ICMP

2.4.3 DNS and DHCP

2.4.4 LDAP and other Windows services

2.4.5 What about timing: NTP

2.4.6 SSH, TLS and other security protocols

2.4.7 Watch out for anti-virus

3. Results

3.1 Breakdown of the network protocols in small enterprise network

3.2 Watch out! We are plotting the network map

3.3 Performance, performance and once again performance: Stressing the outside world

3.4 Looking for the world: CGNs and TCP

4. Conclusions

Bibliography