Illuminating a small network: Perspective from within

StrangeBit

2025

Contents

Contents **3**

1. Introduction **5**

1.1 Questions 5

2. Background **7**

2.1 Basic network characteristics 7

2.2 Topologies 9

2.3 Tools 9

2.4 Network protocols to watch out for 9

2.4.1 Spanning trees 9

2.4.2 TCP, UDP and ICMP 9

2.4.3 DNS and DHCP 9

2.4.4 LDAP and other Windows services 9

2.4.5 What about timing: NTP 9

2.4.6 SSH, TLS and other security protocols 9

2.4.7 Watch out for anti-virus 9

3. Results **11**

3.1 Breakdown of the network protocols in small enterprise network 11

3.2 Watch out! We are plotting the network map 11

3.3 Performance, performance and once again performance: Stressing the outside world 11

3.4 Looking for the world: CGNs and TCP 11

4. Conclusions **13**

Bibliography **15**

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 while measuring 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 also 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 in the network. *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 of 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. But we are not going to cover

those in this report.

2.2 Topologies

2.3 Tools

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