A. Cross-Network Quality and Performance Measurement

Li-Chi Ku
Information System and Network Division
National Center for High-performance Computing
Hsinchu, Taiwan
lku@narlabs.org.tw

Hui-Lan Lee
Information System and Network Division
National Center for High-performance Computing
Hsinchu, Taiwan
gracelee@narlabs.org.tw

Min Chen
Information System and Network Division
National Center for High-performance Computing
Hsinchu, Taiwan
minchen@narlabs.org.tw

***Abstract*—In the era of 5G and future generation networks, cloud services take the dominant part of the network bandwidth usage. Therefore the quality and performance of the network between users and the cloud data centers dictate the perceived quality and responsiveness. Due to its distributed nature, the monitoring of the quality has to be made in a span-AS manner, into those networks we have almost no control. This paper introduces the way we developed to make long term measurement across different networks possible. (*Abstract*)**

Keywords—network measurement, cross network, performance (*key words****)***

II. INTRODUCTION

The usage pattern of the Internet has been shifting gradually from between peers to between client and cloud, and will become increasingly so in 5G and future generation networks. Due to this ongoing change, the user perceived network quality and responsiveness are increasingly more influenced by the cross-network transmission quality because the cloud services are usually hosted in the service provider owned facility and can only be reached by traversing multiple networks along the way.

In order to ensure the network quality and performance, active network measurements, such as the perfSONAR[1] are often introduced. By doing one way latency, one way packet loss, round trip latency and bandwidth test periodically in configurable intervals, network issues can be early detected and systematically analyzed. In this kind of measurement, however, the measurement software needs to be installed to and firewall settings adjusted with each measurement node for such measurement to be possible. This requirement makes it only ideal for environments where all measurement endpoints are in control.

In typical cases, the network traffic between users and cloud services needs to go through a client side network (often an ISP network), perhaps a trasitting network and finally the cloud service provider owned network. With the emergent of the hybrid cloud services, multiple clouds and networks may be involved, which makes the scenario even more complicated. Deploying measurement nodes onto these networks is only possible if virtual machines (VMs) are commercially available. Even so, the network environment of the VM is often strictly filtered which drives most network measurement tools unfunctional. Sometimes the endpoints are obtained without administrative privilege. In this case, only the operating system builtin software is accessible.

In this paper we presented our work in developing a cross network measurement tool and the results we have got among the Taiwan Advanced Research and Education Network (TWAREN)[2], the Taiwan Academic Network (TANET)[3], the Academia Sinica Network (ASNet)[4] and the Government Service Network (GSN)[5].

III. THE CHALLENGES AND SOLUTIONS

TWAREN and TANET are nation-wide research and education networks, which have abundant bandwidth and relatively open policies. Therefore there are a number of open websites capable of serving the measurement targets and it is even possible to install dedicated measurement servers. ASNet, on the other hand, is a research and education network dedicated to top notch scientific research related to Academia Sinica and has tight security control. GSN, as the name implied, serves the government and is highly protected. For the latter two networks, it is impossible to install measurement endpoints without their explicit consent. Due to strict security control mechanisms, it is also harder to collect the required measurement information.

The common problems can be categorized as follows:

1. ICMP blockage

Part of the ICMP[6] functionality is designed to detect network problems. But its exchange is often blocked to reduce unnecessary network information revelation. Among different ICMP messages, echo request, echo reply, TTL exceed, host unreachable and port unreachable are crucial to network measurement tools such as ping and traceroute.

2. Only accessible to certain TCP ports

Network access is often limited to port 80, 443 for HTTP traffic. All other ports are inaccessible from outside.

3. Limited exchange bandwidth

The exchange bandwidth between certain networks is rather limited and is often highly congested during day time. Thus the obtained measurement results differ significantly in different hours of a day.

4. Without administrative privilege

When setting up measurement endpoints is not allowed, an existing environment can only be borrowed. In such cases, it often goes without the administrator / root privilege thus it's impossible to install new software. The measurement must be done with only the builtin tools coming with the OS itself.

The network latency and the route traffic goes are often measured by using ping and traceroute. When the ICMP messages they depend on are blocked, httping serves as a nice alternative to measure latency because HTTP is rarely filtered. When with the -S flag, httping reports not only the HTTP response time but also the TCP connection establishment time, which is exactly the round trip latency we need.

The route can usually be measured by traceroute and mtr, with the former using UDP as the default probe and the latter using TCP. With the ICMP TTL exceed message blocked, there is no alternative able to discover the full path information. However netcat (nc) or socat can still be used in

978-1-6654-1951-2/21/$31.00 ©2021 IEEE

a special way to discover the hop count to the target. With the -M flag in nc and TTL=n argument in socat, the hop count can be found by iteratively searching for the smallest possible TTL value which can still reach the target. nc is almost provided in all Linux distributions as well as FreeBSD, but only the OpenBSD derived version supports -M flag. For those which don't, socat is a consistent choice across different OSes, though it is seldom natively provided. As a final measure, tcpdump, which is included by all Unix like systems, can display the TCP packets with SYN and SYN-ACK flag. The subtraction of the timestamp of these two kinds of packets yields the round trip latency to the target. The tcpdump arguments used in this case is as follows: tcpdump -npttl 'tcp[13] & 2 == 2' .

The transfer speed, which often reflects as website download speed, can be measured by using the system builtin curl to periodically download target files to /dev/null and report the download speed in the following way: curl -L -s -o /dev/null -w "%{speed_download} %{size_download}\n" <URL>. Eventually these stats will be written to influxDB and displayed by Grafana.

In summary, netcat, socat and tcpdump are used in case that ping and traceroute don't work. These OS builtin tools are combined in the form of shell scripts to maximize its compatibility to a wide range of Unix like systems, with the measurement results reported back to an influxDB in the backend.

IV. Cross Network Measurement Results

The round trip latencies between TWAREN measurement endpoints to several GSN targets are shown in Figure 1. While the latency remains nearly constant for most of the target sites, it fluctuates significantly for some of them.

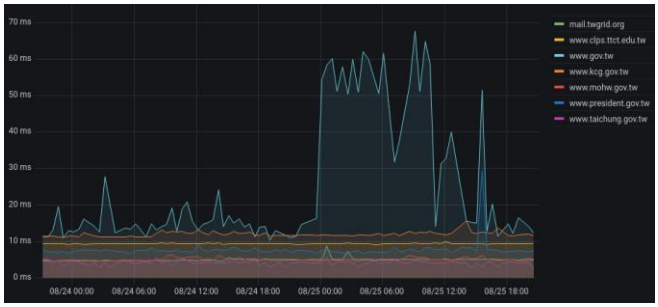

Fig. 1. TWAREN to GSN targets round trip latency

The download speeds from various GSN websites to TWAREN endpoint are shown in Figure 2. The download speed, which reflects the true user experience, varies across different websites. Thus a long term measurement is required to discover the trend of change along the time.

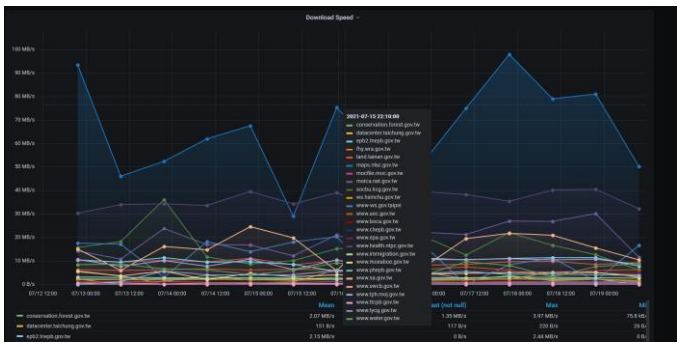

Fig. 2. Download speed of GSN websites to TWAREN endpoint

The aforementioned figures are dynamically generated by Grafana from a long term InfluxDB repository. By displaying the measurement results with different time ranges and target composition, the long term trend of network quality and performance can be clearly observed and any off normal readings can be quickly identified.

V. Conclusion

The network quality and performance, whether within a network or between networks, are constantly fluctuating. With a way to automatically collect those network performance stats from all adjacent networks in a long term period of time, the cross network quality and performance can be monitored and any issues quickly discovered. Future network services thrive when the underlying networks can be made reliable, in ways such as the example we suggested.

References

[1] The perfSONAR project, "performance Service-Oriented Network monitoring ARchitecture (perfSONAR)", perfsonar.net, March, 2020. [Online]. Available: https://www.perfsonar.net/. [Accessed: Aug. 24, 2021].

[2] National Center for High-performance Computing, "TWAREN", twaren.net, 2019. [Online]. Available: http://www.twaren.net/. [Accessed: Mar. 27, 2019].

[3] Ministry of Education, "TANET", tanet.edu.tw, 2019. [Online]. Available: https://noc.tanet.edu.tw/. [Accessed: Mar. 27, 2019].

[4] Academia Sinica Department of Information Technology Services (ITS), "Academia Sinica Network (ASNet)", its.sinica.edu.tw , 2021. [Online]. Available:https://its.sinica.edu.tw/. [Accessed: Aug. 25, 2019].

[5] National Development Council, "Government Service Network", gsn.nat.gov.tw, 2021. [Online]. Available:https://gsn.nat.gov.tw/. [Accessed: Aug. 24, 2021].

[6] Wikipedia, "Internet Control Message Protocol", wikipedia.org, Aug. 8, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol. [Accessed: Aug. 25, 2021].