File: iab-position-paper-observability
Published: 2 August 2021
Authors: J. Arkko *Ericsson*
M. Kühlewind *Ericsson*

Observability is needed to improve network quality

Abstract

A key problem regarding network quality is determining which parts of the network contribute to various performance aspects. In this paper we propose the inclusion of observability and built-in measurement capabilities in networks. This needs to be taken into account when designing protocols, and there is a need for a standardized way to request and exchange such measurements, securely and without exposing privacy-sensitive data.

This paper is a position paper submission to the IAB Measuring Network Quality for End-Users workshop.

Table of Contents

1. Problem Statement

Network quality measurements look at the performance and capabilities of a network, network monitoring reports on the health of the network, and troubleshooting comes into play when a problem is detected. All three depend heavily on the availability of good network measurements.

Often network monitoring largely relies on passive observations of traffic and changes in traffic behavior. In addition, active measurements can be used to enhance this information and probe for specific occurrences. However, active measurement is usually limited to the operator's own network, or for certain access networks may be extended to the end user, but usually does not cover the whole path. Network quality measurements on the other hand are far too often focused on momentary throughput measurements.

Because of these constraints, as also noted at the IAB workshop on COVID-19 network impacts, often neither users nor service providers have ability to understand where a particular problem arises or what is the limiting factor for better performance [I-D.iab-covid19-workshop]:

```
"It's clear that it's difficult for application providers an
operators to isolate problems.  Is a problem due to the local WiFi,
the access network, cloud network, etc.?  Metrics from access points
would help, but in general lack of observability into the network as
a whole is a real concern when it comes to debugging performance
issues."
```

Further, it's often the behaviour of the applications themselves that makes observability difficult. As noted in [I-D.iab-covid19-workshop]:

```
"These types of applications use surprising amounts of Forward Error
Correction (FEC).  Applications hide lots of loss to ensure a good
user experience.  This makes it harder to observe problems.  The
network can be behaving poorly, but experience can be good enough.
Resiliency measures can improve the user experience but hide severe
problems.  There may be a missing feedback loop between application
developers and operators."
```

2. Issues

2.1. Localizing Performance Problems

A key problem that many of us have struggled with is determining which parts of the network contribute to various performance aspects. For instance, a bad quality video conference may be due to issues in the server system, cloud farm that it runs on, somewhere along the path(s), in user's home network or WiFi, or in the user's equipment.

Some information relating to issues can be determined with commonly available tools such as traceroute, but in general, it is difficult to know where the issues are, in particular without collaboration from at least some parts of the associated network paths.

2.2. Observability

Problems with observability do not stop here, however. The ability of the network to support important features such as be able to carry specific transport protocols or use IPv6, exchange information with applications when congestion is detected, use secure DNS protocols, and so on is not always readily apparent. And certainly not something that is uncovered easily merely by performing a throughput measurement.

In addition, some things that can be visible to a host provide no indication of how something is treated in the network. For instance, the host may be able to determine that the first link in the network uses encryption, hiding the traffic from outsiders. However, this provides no indication of whether the user's information is secure beyond the first link. For instance, subsequent links can be unprotected.

2.3. Accessing and Sharing Measurement data

Collecting the right measurement data is a major challenge. Another challenge is also how to correctly interpret the data and provide the data to the right entities that can act on it, either for troubleshooting or improving future usage. To enable everybody to draw the right conclusion, it is especially important to correlate data from different sources, e.g. a network operators might not see increased loss if the endpoints adapt its rate accordingly, still network optimization could help certain traffic to utilize the available resources more efficiently.

Shared measurement data may relate to observations about a particular flow at different points along a path, but it may also be about aggregate information relating to the overall traffic situation (such as queue or congestion status), or the capabilities of the network nodes.

To exchange data, standardized definitions of measurements (e.g., [RFC7679]), communication protocols, as well as standardized formats are needed (e.g., QLOG [I-D.ietf-quic-qlog-main-schema]).

2.4. Capabilities

A high-quality network is capable of leveraging a number of features and connectivity options, such as:

- Support for broad range of protocols, including not just regular TCP traffic but also QUIC/UDP traffic, IPv6, and ICMP.
- Support protocols and suitable security mechanisms for interacting DNS, NATs, firewalls, and so on. For instance, for DNS resolution modern networks may offer services such as [RFC7858] [RFC8484] [I-D.ietf-dprive-dnsoquic].
- Provide mechanisms for network and applications to interact, e.g., via explicit congestion notifications [RFC3168].

For each of these categories, there may be additional parameters that are of interest as well, such as various timing parameters related to how long NAT or firewall entries are kept.

Discovering these capabilities can generally be accomplished in two ways: either by probing whether a given mechanism exists and what its characteristics are, or by asking the network. Some information may be available in router discovery packets and DHCP responses.

However, knowing in advance that a certain path supports a certain service, or not, is difficult, also because paths change dynamically. Built-in measurement capabilities that collect information on the flight, can help to detect capabilities or problems that require additional troubleshooting.

2.5. Security

Some aspects of security are readily visible to end hosts. The host knows what end-to-end protocols and security it runs, and it may have internal APIs to determine what type of connectivity security is being applied. For instance, both WiFi and mobile network stacks on the end host are aware of what security is being applied.

Some other aspects of security are something that may have to be discovered. For instance, the network may offer a DNS resolver address, but whether that resolver supports a secure protocol can be something that has to be discovered through a protocol mechanism such as [I-D.ietf-add-ddr].

But even when a particular network connectivity or support protocol is found to employ security, it provides no indication of how the user's is information treated by the server in question or by the rest of the network. For instance, the host may communicate securely with a DNS resolver that still leaks the user's browsing history to outsiders.

In some cases it may be possible for a network node to provide an attestation that it runs a particular software and does not leak information outside a trusted execution environment (see [I-D.arkko-dns-confidential]).

In general, endpoints would benefit from not only seeing claims about specific features or performance, but to actually get some assurances that the claims are valid. Similarly, endpoints need to be careful about exposing information related to the user to the network (see, e.g., the advice in [RFC8558]). This needs to be considered in protocol design.

3. What should we do from here?

To address this problem and improve visibility of network quality we need to consider observability and built-in measurement capabilities when designing protocols and networks. We need a standardized definitions and ways to request and exchange such measurement data, and this needs to happen securely and without exposing privacy-sensitive data.

4. Conclusions

The ability to observe the behaviour of the Internet connection extends far immediate or momentary speed measurements. Especially, localising a problem is challenging as multiple parties are involved. As such built-in measurement capabilities and ways to exchange measurement data securely are the basis for improved observability.

Some of the tools that may assist in better observability include

- Network assist for measurements
- Probing
- Capability discovery
- Indications about available security

5. Acknowledgments

The authors would like to thank the participants of the 2020 IAB COVID-19 Network Impacts Workshop on interesting discussions in this problem space.

6. References

[I-D.arkko-dns-confidential] Arkko, J. and J. Novotny, "Privacy Improvements for DNS Resolution with Confidential Computing", Work in Progress, Internet-Draft, draft-arkko-dns-confidential-02, 2 July 2021, <https://www.ietf.org/archive/id/draft-arkko-dns-confidential-02.txt>.

[I-D.iab-covid19-workshop] Arkko, J., Farrell, S., Kühlewind, M., and C. Perkins, "Report from the IAB COVID-19 Network Impacts Workshop 2020", Work in Progress, Internet-Draft, draft-iab-covid19-workshop-03, 5 May 2021, <https://www.ietf.org/archive/id/draft-iab-covid19-workshop-03.txt>.

[I-D.ietf-add-ddr] Pauly, T., Kinnear, E., Wood, C. A., McManus, P., and T. Jensen, "Discovery of Designated Resolvers", Work in Progress, Internet-Draft, draft-ietf-add-ddr-02, 8 July 2021, <https://www.ietf.org/archive/id/draft-ietf-add-ddr-02.txt>.

[I-D.ietf-dprive-dnsoquic] Huitema, C., Dickinson, S., and A. Mankin, "Specification of DNS over Dedicated QUIC Connections", Work in Progress, Internet-Draft, draft-ietf-dprive-dnsoquic-03, 12 July 2021, <https://www.ietf.org/archive/id/draft-ietf-dprive-dnsoquic-03.txt>.

[I-D.ietf-quic-qlog-main-schema] Marx, R., Niccolini, L., and M. Seemann, "Main logging schema for qlog", Work in Progress, Internet-Draft, draft-ietf-quic-qlog-main-schema-00, 10 June 2021, <https://www.ietf.org/archive/id/draft-ietf-quic-qlog-main-schema-00.txt>.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, DOI 10.17487/RFC3168, September 2001, <https://www.rfc-editor.org/info/rfc3168>.

[RFC7679] Almes, G., Kalidindi, S., Zekauskas, M., and A. Morton, Ed., "A One-Way Delay Metric for IP Performance Metrics (IPPM)", STD 81, RFC 7679, DOI 10.17487/RFC7679, January 2016, <https://www.rfc-editor.org/info/rfc7679>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8484]

Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC8558] Hardie, T., Ed., "Transport Protocol Path Signals", RFC 8558, DOI 10.17487/RFC8558, April 2019, <https://www.rfc-editor.org/info/rfc8558>.

Authors' Addresses

Jari Arkko
Ericsson
Email: jari.arkko@ericsson.com

Mirja Kühlewind
Ericsson
Email: mirja.kuhlewind@ericsson.com