Characteristics of Traffic Type Changes and Their Architectural Implications

Jari Arkko, Ericsson Research
(jari.arkko@piuha.net)

Göran Eriksson, Ericsson Research
(goran.ap.eriksson@ericsson.com)

Abstract: *This paper summarizes the reasons for the recent evolution in Internet traffic patterns, focusing on the increased encrypted content and the evolution of the web protocols in particular. These changes and factors enabling them have some interesting characteristics that can perhaps help us understand these and the upcoming changes better. The paper highlights some of the implications, and suggests some potential directions for work that seem fruitful for dealing with the traffic evolution.*

Introduction

This paper summarizes the reasons for the recent evolution in Internet traffic patterns, focusing on the increased encrypted content and the evolution of the web protocols in particular. These changes and factors enabling them have some interesting characteristics that can perhaps help us understand these and the upcoming changes better.

The paper highlights some of the implications of the characteristics for Internet architecture, and suggests some directions for work that seem fruitful for dealing with the traffic evolution.

Characteristics

One characteristic is that there are both long-term and faster-paced changes in Internet evolution. When long-term evolution brings fundamental new capabilities, sudden changes in actual traffic patterns become possible.

One example of this is the availability of secure web communications in browsers, servers, and other systems. This underlying capability can develop but be in limited use, until a service provider finds a reason for employing this capability. Given some highly popular Internet services, even a single service provider may have a big impact on the global traffic patterns, if they find such a reason. If such reasons appear on the global scale for many providers, they together will have an even more pronounced effect.

In the case of secure web communications, the capabilities for doing this have been broadly available in browsers for a long time, and a growing number of server farms have been set up to provide that capability as well. The use of these capabilities is now growing relatively rapidly, and has for the last several years. The reasons for the use of these capabilities are varied, ranging from basic need to protect end-user accounts in open networks, privacy protection in a broad sense, to securing control of the service delivery or other business reasons.

This phenomenon has also been seen with IPv6 deployment, where the development of IPv6-capable devices and content services has created a latent capability. When IPv6 connectivity becomes available through an operator’s network, the swing to using IPv6 in those content services can be quick. The home country of one of the authors, Finland, recently experienced this as IPv6 take-up rate increased from 0.5% to 8% in a matter of weeks, merely because one large access provider turned their IPv6 networking on. Latent capabilities in the rest of the ecosystem – devices and content providers, enabled that change to lead to quick changes in traffic patterns.

There is also one fundamental latent capability that can drive other capability improvements: automatic software updates. While there are of course many systems (such as small IOT devices) that unfortunately do not update themselves automatically, many other systems today do.

Analysis

The evolution in secure web communications and IPv6 are just examples of the kinds of effects that we may see. It is very likely that further evolution in web and transport protocols will follow similar paths.

Also, the mobile device markets and associated content and application services are a relatively consolidated market. This implies that there are cases where some large entities find it easy to evolve both ends of the communication, such as the browser and content service including origin servers and deep network caches. This makes evolution faster than if a broad change within the overall Internet community would be needed first.

Implications

These swings in traffic can have impacts on the operators carrying the traffic. This is not merely a question of managing traffic, but can go to the core questions of the amount of traffic, the direction of traffic flows, and who the communicating parties are.

When we look at the increased encryption, we should not prepare ourselves to merely deal with its effects. We need to prepare for a period of increasingly fast evolution in the Internet traffic patterns and technology. Such evolution may include new transport solutions, HTTP version 3 and beyond, the introduction of new parties (such as caching, CDN, or P2P entities), new types of security (such as content-based security), and other things that we cannot foresee at this point. Indeed, many of these changes are already being discussed, prototyped, or even deployed.

There are several architectural implications of this. Traffic management tools dealing with pure IP transport and traffic patterns continue to have significance. Perhaps even more than they have had for a while – “back to basics”. But without the ability to peek into what the applications are doing, there may be some opportunities for end-points, such as user devices, to provide more information to the network regarding the traffic characteristics.

Application-level operations (such as deep packet inspection) in the network become difficult or need to evolve into different types of practices. One potential aspect of such evolution is that current network management tasks are often done standalone by an operator. End-to-end security will likely increase co-operative management operations, such as contracted CDN operations. These operations are less easy to deploy due to the need for the agreements, and may not be setup in all networks.

Finally, if the evolution is about fundamentally increased flexibility rather than the specific issue of encryption, networks need to deal with that flexibility. The ability to evolve network services on a fast-paced timeline will be crucial, be it about reacting to traffic pattern changes or building those co-operative network components that were mentioned above. Many of the current trends in networking are largely about addressing this need: automation, software-defined networking, virtualization of network functions, and cloud services, for instance.

But at the same time it is important to understand the distinction between pure networking services and application-level operations. Even with highly flexible tools, the latter operations will likely need to operate in co-operative fashion, because access to application-level information may not be available otherwise.

The ability of networking services to make decisions with limited information can be improved by opening APIs where some information can be exposed, without compromising the user's privacy or other reasons behind the use of end-to-end security.

The difficulty in doing this lies mostly in our ability to provide interfaces that actually get deployed both in networks that offer the interfaces and applications that use the interfaces. Some of the potential interface developments have issues with deployment incentives or with the incentives for the parties to not lie or misrepresent themselves through those interface. For instance, it is necessary to prevent a situation where everyone will claim all traffic as high priority, to get better treatment in the network.

The development of such interfaces may also lead to potentially complex processes in operating them, by both network operators and service providers. This is a problem that should be considered when designing collaborative interfaces. Here careful, minimalistic designs as well as standardized technologies, such as data models, and allowing for semi-automation seem fruitful to consider. The designs should also be such that they respond to broad, general needs rather than specific issues with current technology, to be useful in a quickly changing environment.

Conclusions

All access network management techniques need to be thought in light of quickly changing environment, where not all information may be accessible, and the protocol mechanisms carrying the information can change rapidly.

Pure IP transport based management techniques, co-operative management techniques, and new network interfaces are some of the tools to deal with this situation.

Acknowledgements

The author would like to thank Natasha Rooney, John Mattsson, Iuniana Oprescu, Salvatore Loreto, Gonzalo Camarillo, Joel Halpern, Stephen Farrell, Kathleen Moriarty, and members of the IAB for interesting discussions in this problem space.