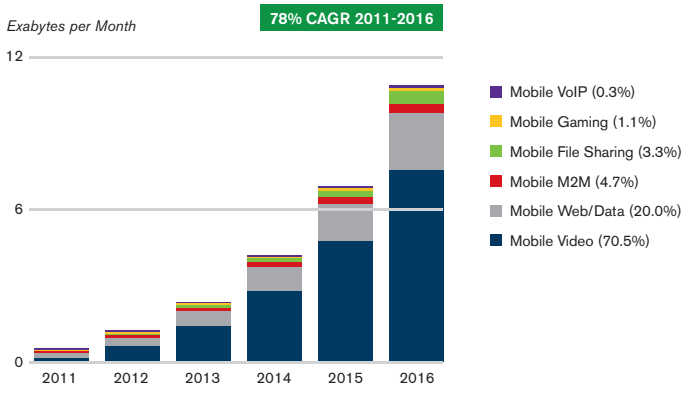
W²CM Smart Replay

Nisar Sanadi, Product Manager, EXFO

INTRODUCTION

Along with the phenomenal growth in volume of data on the mobile Internet, there has been an increase in the different types of data flowing through wireless networks. In addition to traditional types of data, such as file transfer protocol (FTP), hypertext transfer protocol (HTTP), voice-over-Internet protocol (VoIP), e-mail and video streaming, there has been a constantly increasing list of over-the-top (OTT) smartphone applications generating new types of data, including peer-to-peer (P2P) data from applications such as BitTorrent and Kazaa. In an effort to differentiate themselves, operators have also been offering their subscribers their own unique applications, which in turn contribute to the variety of data on wireless networks.



Figures in legend refer to traffic share in 2016.
Source: Cisco VNI Mobile, 2012

Figure 1. The explosive growth in mobile data.

This vast amount and variety of data has created a need for it to be managed effectively. There are several motivating factors to do so, chief among them being:

- Honoring service-level agreements (SLAs) and delivering committed quality of service (QoS) to customers
- Efficiently managing network resources
- Generating revenue as opposed to being just a "dumb pipe" for data
- Securing the network

Let's look at each one of these aspects in a little more detail.

HONORING SLAS

Operators have SLAs with their customers to guarantee a certain minimum performance from their networks. To be able to meet these commitments, the network elements have to be able to ensure that the required amount of resources is made available when needed. A recent study has shown that 5% of users consume 60% of bandwidth. This type of usage pattern can endanger an operator's ability to meet its SLA commitments to the rest of its subscribers. Operators have a strong incentive to manage the data usage of such heavy data users (e.g., by throttling the throughput rates available to such users).

Figure 2. Mobile network operators (MNOs) need to proactively manage network usage.

Honoring SLAs may also mean being able to identify data associated with key customers and giving it preferential treatment in the network. There are strict guidelines in the LTE specifications about the handling of data with different levels of QoS. Gateways in the network have to correctly implement these techniques to ensure that committed QoS is delivered.

EFFICIENT MANAGEMENT OF NETWORK RESOURCES

Another motivation for operators is to manage their CAPEX. Operators are making huge investments in building out their networks to keep up with the growth in data consumption. Unmanaged data usage coupled with the need to deliver on SLAs would result in operators having to deploy more equipment to handle the load. A better alternative is to manage the data usage. The LTE 3GPP specifications introduced the concept of maximum bit rates (MBR). The idea is to limit the maximum throughput used by a subscriber. This is a very critical technique for operators in order to prevent abuse of network resources by a few "bad" subscribers.

REVENUE GENERATION

With an explosion in over-the-top (OTT) applications on the Internet, operators risk becoming mere "dumb" pipes carrying user data back and forth. This is not an enviable situation for operators, considering the enormous investments in infrastructure required to keep up with growth in data usage. Operators want to find ways to generate revenue from the data flowing through their pipes. They can do this by providing the same services as the OTT players, for instance voice-over LTE (VoLTE), but with significantly better and more predictable quality. Operators may want data associated with their own applications to be given preferential treatment as compared to equivalent OTT applications. Additionally, they can add value to the data already flowing through their network (e.g., by signing revenue-sharing deals with service providers in exchange for prioritizing their data, or through targeted advertising based on the content of user data, similar to what Google does with Gmail).

NETWORK SECURITY

LTE marks the full transition of wireless networks to all-IP. IP networks are inherently more open in nature, and hence more prone to security vulnerabilities, primarily in the form of denial-of-service (DoS) attacks. This clearly poses a major threat to the operators, who absolutely must have ways to mitigate this risk. It is imperative that these DoS attacks are detected and dealt with immediately before they have the potential to bring down significant portions of the network for an extended period of time. A catastrophic event of this type could do irreparable damage to a company's reputation.

LTE GATEWAYS

Elements in the wireless networks, primarily the gateways, have mechanisms to address all of the above. They use a technique called deep packet inspection (DPI) to achieve this. DPI is the technology that enables the gateways to "peek" inside the data that is flowing through the network and take action depending on the characteristics of the data. This could include the source/destination of the data, the type of data, the duration of the data session, and so forth. The gateways could take actions such as throttling the throughput, terminating the session, or raising or lowering the priority of the data.

REAL WORLD TESTING

Clearly, the DPI functionality in the gateways is key to the efficient and secure functioning of wireless networks. Since the primary function of DPI is to identify characteristics of user-plane data, it is important to extensively test this aspect of DPI in the lab by subjecting it to traffic patterns seen in live networks. This includes not just the high-throughput levels, but also the wide variety of data types. Such data types include thousands of different OTT smartphone applications, each generating its own unique type of data, as well as operators' proprietary applications aimed at differentiating their offerings. It should be mentioned that operators want their customers to have a better experience using their applications than they would with OTT applications. In addition, P2P and file sharing applications are on the rise. Of course, the threat of security attacks must also be taken into consideration. It is critical to simulate such attacks in a lab environment to ensure that they can be properly detected and dealt with should they occur in a live network.

The sheer number of different types of data presents a serious challenge to simulating realistic traffic patterns in the lab. New applications are constantly being introduced, and at a rapid rate. Waiting on test-tool vendors to support these applications directly on their tools is not feasible due to turnaround times. What is needed is a quick way to replicate data from these applications to ensure that gateways can handle them appropriately.

W²CM

The first and foremost consideration is a module that is capable of user-plane data generation and analysis at high throughput over 10G ports. EXFO introduced its W²CM module specifically to address this need.

- Purpose-built for wireless testing
- Two 10 Gigabit Ethernet and eight 1G ports
- Line-rate generation and analysis of real-world application data (best in the industry)
- Native support for standard data types, such as FTP, HTTP and VoIP
- SmartReplay feature for rapid introduction of new data types into the traffic mix

Figure 3. EXFO's best-in-class W²CM user-plane blade.

SMARTREPLAY

The SmartReplay feature on the W²CM module provides the framework for end users to quickly generate the desired traffic themselves. W²CM natively supports generation of traffic for standard and popular types of applications, including FTP, HTTP, VoIP and RTSP. However, it would be practically impossible for a test-tool vendor to keep up with the rapidly growing list of applications. A much better approach would be to provide the end user with the capability to generate any type of data from the test tool.

The SmartReplay feature does just that. All users need to do is provide a Wireshark trace of the desired data. The system will present various options to filter the required flows from the trace file, from which a SmartReplay profile is generated. These profiles could be of the client/server type or the peer-to-peer type.

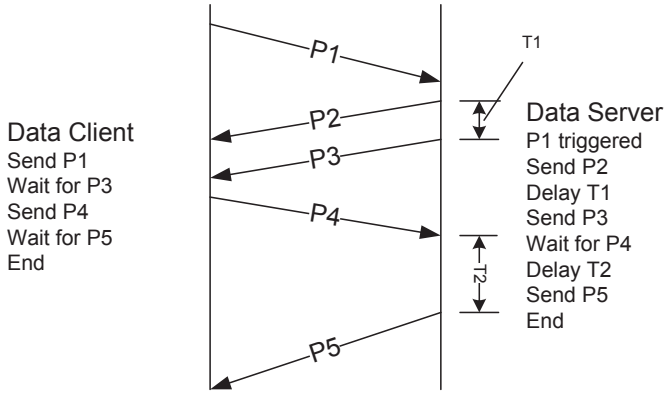


Figure 4. A conceptual representation of a profile.

An editor allows users to view and customize the profile, as shown in the snapshot below. The editor may be used to manipulate delays between messages or even the content of messages, and more. This same editor could also be used to manually create data profiles from scratch.

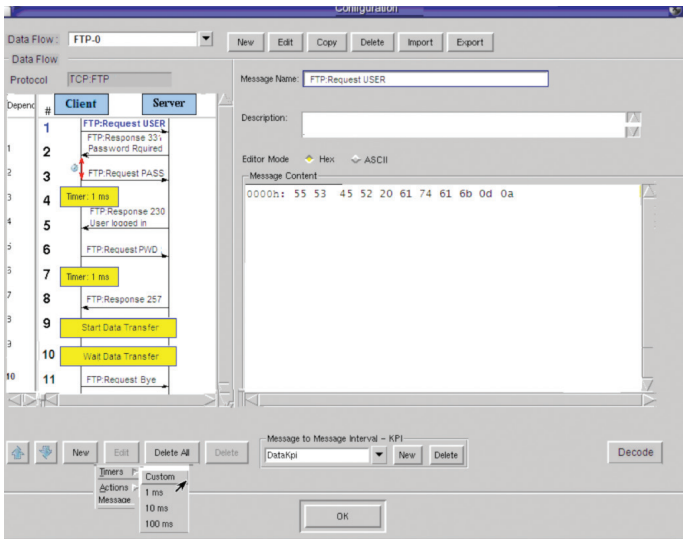


Figure 5. Call Flow Editor.

Once a data profile is created, the SmartReplay feature will replay these flows with the lower-layer address being replaced with the targeted emulation (L4 – L2). The user can provide the parameters for this replay, e.g., the number of endpoints to simulate and the range of IP addresses. Both IPv4 and IPv6 are supported over Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). UDP and TCP statistics are reported indicating the performance of the system under test (SUT) for that particular type of data.

Data generated by SmartReplay is based on a set of specific session captures. These sessions may represent only a subset of the flows possible for that particular type of data. From the perspective of testing the DPI functionality of the gateways, these representative flows would be sufficient. However, it is necessary to have both the client and server sides or the two peers simulated by the W²CM module. It is not possible to emulate just the client or the server side based on the SmartReplay feature.

EXFO Headquarters > Tel.: +1 418 683-0211 | Toll-free: +1 800 663-3936 (USA and Canada) | Fax: +1 418 683-2170 | info@EXFO.com | www.EXFO.com

EXFO serves over 2000 customers in more than 100 countries. To find your local office contact details, please go to www.EXFO.com/contact.