8/11/2010

HARISHVADADA.WORDPRESS.COM

LTE & WiMAX Blog

Net neutrality and 4G | hvadada

The media is on fire talking about how Google has surrendered the net-neutrality pledge and gone with the carriers, but there are technical reasons how it is the carrier-way or the highway. FCC last year set forth three rules - Providers can't favor their own content, Providers need to explain variable speeds and Providers cannot limit access to lawful content, which Comcast had it overturned in court. Though FCC might posses the power to make rules on net-neutrality, albeit it is the technologies that control the flow of traffic which will decide how much of content delivery is neutral after all!

So what's at stake here? Let's start by following the money trail.

According to a recent report by the Sunlight Foundation, forces opposing Net neutrality (big broadband providers like Comcast, AT&T, and Verizon, as well as telecom-centric trade groups and unions like the NCTA and the CWA) outspent pro-Net neutrality forces (Google, Yahoo, Amazon, and so on) by a margin of four to one. The opposers of the bill spent nearly $20 million on lobbyists in the first quarter of 2010, and the supporters spent roughly $5 million.

All bits are not really created equal. The quality-of-service requirements for Web pages and email are not the same as for voice and video. ISPs are unlikely to invest in the technology required to prioritize certain types of bits unless they can recoup their investment -- again and again and again. Without that, the Internet will never truly become the end-all, be-all delivery system for phone, television, data, and so on.

So how can a Wireless ISP or a Mobile Network Operator (MNO) control the traffic – as we know not all packets are created equal and not all applications will get the priority? So how would 4G networks in future shape the traffic and provide quality of service (QOS). Let us peel the onion and peer into the technical details:

QOS classifiers - LTE & WiMAX

Traffic shaping with QOS mechanisms will play a big role in how services are delivered in the evolved LTE and WIMAX systems, with IP as a backbone to their deliverability and will be done via Deep Packet Inspection (DPI) mechanisms that will exist at the control nodes of the network. QoS refers to the ability (or probability) of the network to provide a desired level of service for selected traffic on the network.

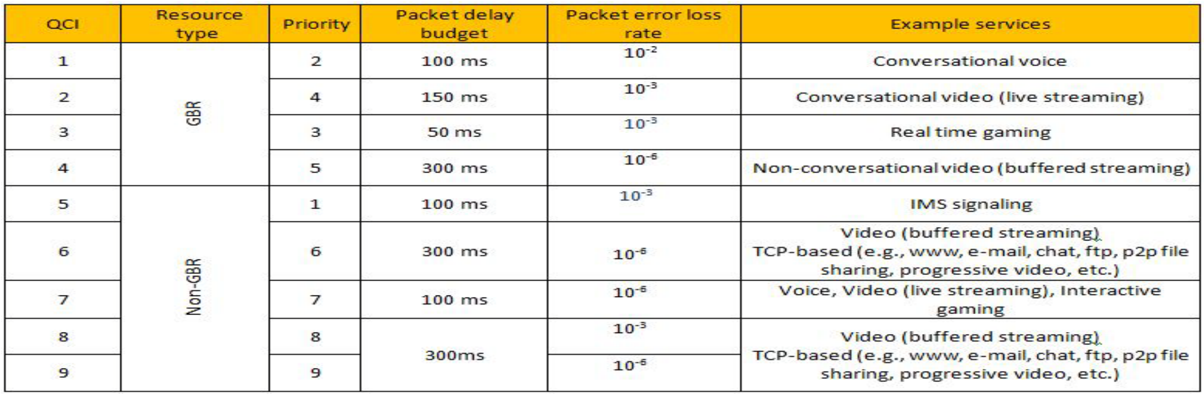
- Service levels are specified in terms of **throughput**, **latency** (delay), **jitter** (delay variation) and **packet errors or loss**.
- Different service levels are specified for different types or streams of traffic.
- To provide QoS, the network identifies or “classifies” different types or streams of traffic and processes these traffic classes differently to achieve (or attempt to achieve) the desired service level for each traffic class.
- The effectiveness of any QoS scheme can be measured based on its ability to achieve the desired service levels for a typical combination of traffic classes (“traffic profile”).

LTE bearers:

- **Guaranteed bit rate (GBR)**: Dedicated network resources related to a GBR value associated with the bearer are permanently allocated when a bearer becomes established or modified.

- **Non-guaranteed bit rate (non-GBR):** A non-GBR bearer is referred to as the default bearer, which is also used to establish IP connectivity, similar to the initial Service Flow in WiMAX.

LTE specifies a number of standardized QCI values with standardized characteristics, which are preconfigured for the network elements. This ensures multivendor deployments and roaming.



QCI	Resource type	Priority	Packet delay budget	Packet error loss rate	Example services
1	GBR	2	100 ms	10^{-2}	Conversational voice
2		4	150 ms	10^{-3}	Conversational video (live streaming)
3		3	50 ms	10^{-3}	Real time gaming
4		5	300 ms	10^{-6}	Non-conversational video (buffered streaming)
5	Non-GBR	1	100 ms	10^{-3}	IMS signaling
6		6	300 ms	10^{-6}	Video (buffered streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7		7	100 ms	10^{-6}	Voice, Video (live streaming), Interactive gaming
8		8	300ms	10^{-3}	Video (buffered streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9		9		10^{-6}	

WIMAX Service Flows:

WiMAX employs flow-based QoS - traffic can be classified to different service flows with different QoS parameters. The ASN (Access Service Network) supports admission control & resource scheduling to manage (nonguaranteed) QoS per service flow. The WiMAX ASN also marks traffic to enable other networks/elements (e.g. backhaul network) to provide QoS consistent with the air interface. WiMAX provides QoS by classifying traffic to service flows with different QoS. A service flow (SF) is a unidirectional MAC-layer transport connection with particular QoS parameters.

- **Unsolicited grant service (UGS):** Supports real-time traffic with fixed-size data packets on a periodic basis
- **Real-time polling service (rtPS):** Supports real-time traffic with variable-size data packets on a periodic basis
- **Extended rtPS (ertPS):** Supports real-time traffic that generates variable-size data packets on a periodic basis with a sequence of active and silence intervals
- **Non-real-time polling service (nrtPS):** Supports delay-tolerant traffic that requires a minimum reserved rate
- **Best effort (BE) service:** Supports regular data services

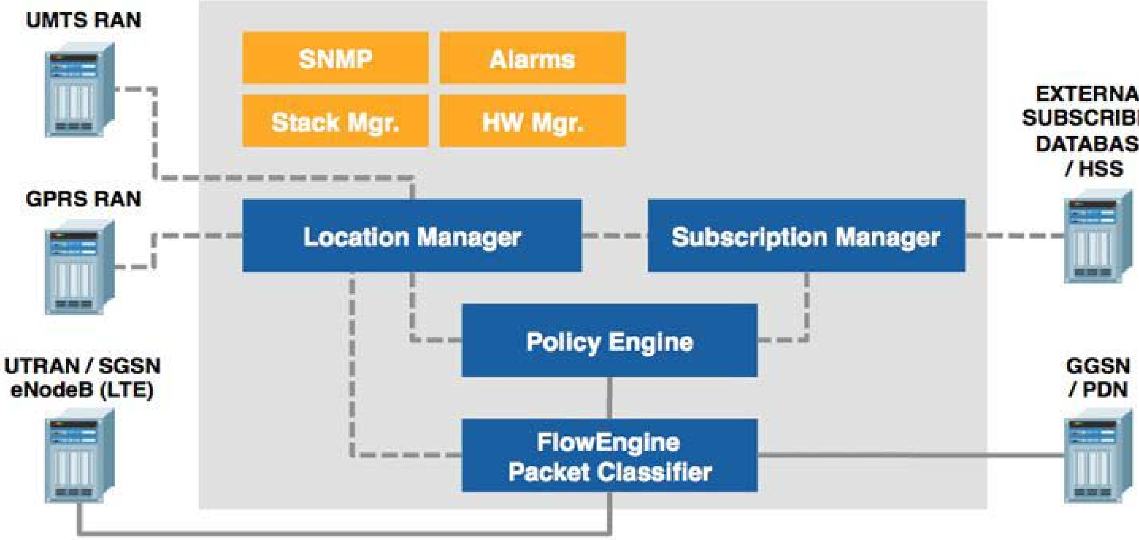
Traffic engineering has always ensured QOS assurance to wireless voice and data traffic, but with these enhanced features in 4G, an operator will be able to fine tune the delivery of content based on the profile of the user stored in the AAA for WiMAX and HSS for LTE.

Deep Packet Inspection

Deep Packet Inspection (DPI) is currently one of the hottest issues for ISPs and carriers. Constantly seeking new sources of revenue and to reduce churn, they are deploying or forming projects for the deployment of triple play, new services and applications. There are several levels of deep packet inspection (DPI), ranging from a relatively shallow approach, which simply looks for TCP and UDP port numbers and patterns in packet headers, to a more sophisticated approach, which actively parses packets, peeling away each layer of encapsulation until it reaches the data contained within. This approach can:

- identify applications independently of which port numbers they might use;
- detect when tunneling protocols are being used, and parse through them in order to find the information that they encapsulate;
- Group application data into their respective flows, and use the signaling information to group correlated flows into sessions;
- Extract application metadata; and
- Extract application content.

It is a deeper form of DPI, similar to an Information Extraction DPI, or ixDPI.



Why DPI?

We need DPI technologies to -

- To analyze their current network situations and their readiness to receive rich, demanding, consuming and real time traffic.
- To analyze their subscribers' behavior, such as traffic patterns generated per hour/day/week and measure the over-the-top services being used by subscribers.
- To set up global application control policies - such as the total quantity of P2P or VoIP/Skype traffic - at the various peering points where they purchase bandwidth from upstream providers.
- To set up per subscriber SLAs/policies, in order to enforce smarter services, volume/duration-based billing, be more competitive, provide better QoE, and increase ARPU.
- Monetization and target advertising above all!

Vendors that have DPI capabilities built into their PDN gateways are – Cisco (Starent), Ericsson, Huawei, NSN(Flexi ISN), as well as specialist DPI solutions providers like Sandvine, Allot, Bivio, Cloudshield to name a few are set to grow by more than four times.

Peering

Internet consists of over 25,000 Autonomous Systems (AS). An Autonomous System can independently decide who to exchange traffic with on the 'Net', and it isn't dependent upon a third party for access. Networks of ISPs, hosting providers, telecommunications monopolists, multinationals, schools, hospitals and even individuals can be Autonomous Systems; all you need is a single 'AS number' and a block of provider independent IP-numbers. These can be had from a regional Internet registry (like RIPE, ARIN, APNIC, LACNIC and AFRINIC). Most organizations and individuals do not interconnect autonomously to other networks, but connect via an ISP. One could say that an end-user is 'buying transit' from his ISP.

In order to get traffic from one end-user to another end-user, these networks need to have an interconnection mechanism. These interconnections can be either direct between two networks or indirect via one or more other networks that agree to transport the traffic. These inter-ISP sharing arrangements are known as peering or transit, and they are the two mechanisms that underlie the interconnection of networks that form the Internet. The economic arrangements that allow networks to interconnect directly and indirectly are called peering and transit:

Peering: when two or more autonomous networks interconnect directly with each other to exchange traffic. This is often done without charging for the interconnection or the traffic.
Transit: when one autonomous network agrees to carry the traffic that flows between another autonomous network and all other networks. Since no network connects directly to all other networks, a network that provides transit will deliver some of the traffic indirectly via one or more other transit networks. A transit provider's routers will announce to other networks that they can carry traffic to the network that has bought transit. The transit provider receives a "transit fee" for the service.

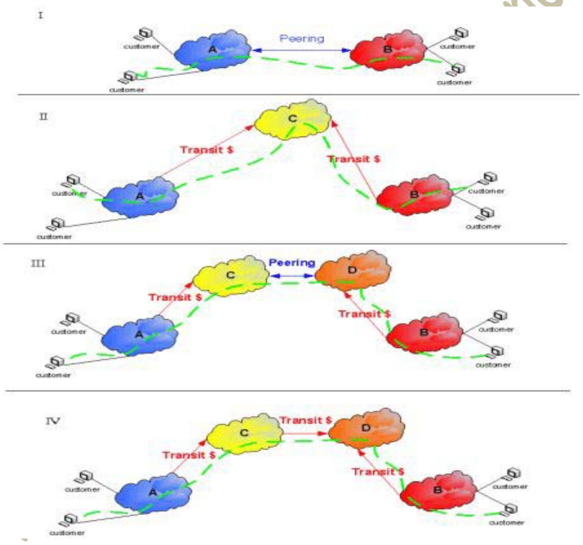


Diagram I shows peering between two networks. Diagram II shows transit over two networks. Diagram III shows transit over three networks where there is a peering agreement between networks C and D, and A and B both pay for transit. Diagram IV shows how A pays to C, and B and C pay to D for transit.

Peering is exactly what must have happened between Google and Verizon, an agreement that will route traffic directly from the Verizon core to the Google servers and have a class of service that bypasses the Internet exchange latencies. But is this unethical, I would not think so as ISP-level traffic shaping has been around for a long time, but tinkering with the QOS classification based on the observations from DPI, and routing traffic based on this would definitely be a grey area that FCC and other ISPs need to hash out. We would still need Telcos to watch out for CALEA (Communications Assistance for Law Enforcement Act) and Copyright Infringement.