**DEPARTMENT OF COMPUTER SCIENCES**

**PROJECT FOR**

**NETWORK MANAGEMENT SYSTEM** **(CS590)**

(KIM YEONGKWUN)

PROJECT REPORT

ON

**DIFFERENT TRAFFIC MANAGEMENT TECHNIQUES FOR MOBILE BROADBAND NETWORKS**

By Group: 05

Vanga Alekhya

When we see the current situation in the mobile broadband network the service providers have manage the traffic created by the networks. Because every year mobile traffic is growing very fast. To control this we need some techniques to solve these problems. The broadband industry has provides have some business models and techniques.

These models have some policy control mechanisms like, bandwidth management, good quality of service and service level agreements. These policies will apply to desired end-user to experience the quality of the service. When users need good quality of service then how is it possible in terms of provide more data in peers network and keep maintain the good quality service to users in the wireless network in very busy network. To fulfill this what kind of actions are necessary to handle efficiency. Because we are handling mobile traffic using multiple wireless networks.

Some technical solutions for the traffic management issues in the mobile broadband network

**1. Service/user differentiation for congestion management**

Every link and the router in the different networks the internet has its own capacity to handle the data. The capacity of the each router and the link is measured by equipment installed by the entity that runs each network that will optimize the cost and performance. When congestion occurs in the network it will typically effects queuing delay, packet loss or the blocking of the new connections. If the capacity is lower than the expected demand then the broadband internet is bursty. When the demand exceeds the capacity on the network it causes congestion that will degrade the performance. The network providers typically take months to estimate the demand. Depending upon the demand they can work on the upgrade and increase the demand. But it takes months to upgrade the new scale.

If the congestion is short user will not notice degradation in performance. It is problem when its duration is long enough to be descriptive to applications. We need some practice for the congestion management. Also to decide which practice is good to keep impact upon users and applications. Network operators apply some practices to the traffic of subnet of specific users to subset of types of applications.

There are some other reasons to cause the congestion, like unexpected changes in the routing that can increase the congestion, unexpected natural disasters like earthquake and dramatic weather change also be the reason for the congestion, the network failures and the accidents like hardware failure or the router fail can also cause the congestion and the network attacks like Denial of Service (DoS) attacks also be the problem to create congestion in the network.

**Location of congestion**

As we know congestion can occur on any link or router within the internet. The potential congestion in the ISP networks are as follows.

a. Wireless broadband access links and routers

b. Wi-Fi wireless broadband access link and routers

c. Wireline access links and routers

d. Core network links and routers

e. Network interconnection routers

**Congestion Management Techniques**

Many congestion management techniques at or above the network layer are standardized by the Internet Engineering Task Force (IETF), and many at the physical and data link layers are standardized by the Institute of Electrical and Electronics Engineers(IEEE).

**Packet Classification**

In this technique, it is based on the particular user or application component, packet must be classified using criteria that identifies the particular user or application traffic. In this network providers have to know the source and destination. This is agreements between users and network operators. In other way it has one challenge to packet classification is the ease or difficulty in accurately identifying particular application traffic. It also has one challenge like resource may be reserved only in portion of a single operator network in which network provider has to control flow which are granted to which user.

**Admission Control & Resource Reservation**

Resource reservation is thus a congestion management technique appropriate for such applications. Reservation of an appropriate level of resources can ensure that congestion does not negatively impact the flows using the reserved resources.

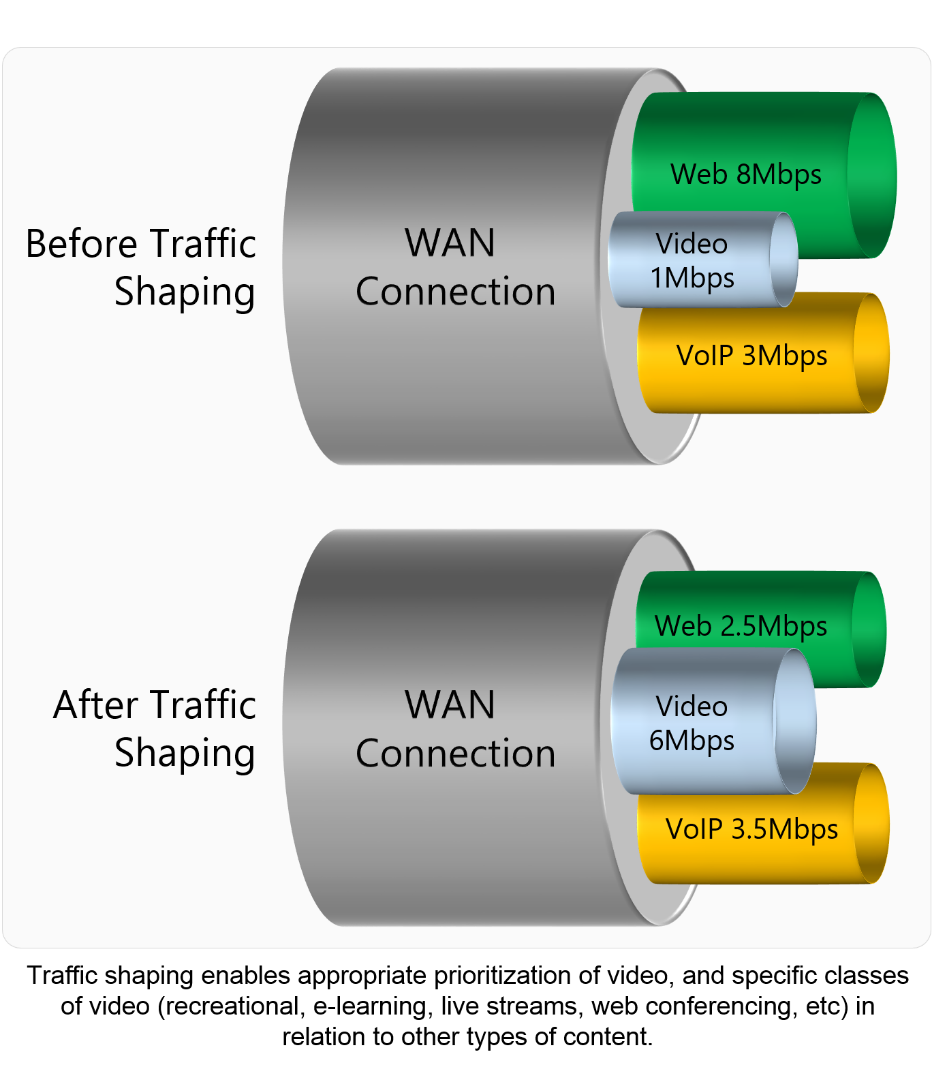
**Caching**

Caching is typically implemented by directing a request from a user for a particular piece of content to the closest cache that has the content or to the most lightly loaded cache. If the closest cache is selected, this lessens traffic between the ASP and the user

**Rate Control and Traffic Shaping**

Rate control by applications and operating systems is implemented at the source and destination. It may be based on the requirements of the application.

Traffic shaping by network operators is implemented at routers between the source and destination, most commonly at the edge of an operator’s network.



**Routing and traffic Engineering**

An alternative approach to determining routes solely on the basis of the destination IP address is to route certain traffic to the destination based on the type of contract or the desired QoS characteristics

**Packet dropping**

Each queue has a buffer of a certain size in which to store packets, and thus occasionally an arriving packet will find that the buffer is full. Routers thus must occasionally drop packets.

**Packet scheduling**

In this, simplest queuing technique places arriving packets in queues in the order in which they arrive, and the simplest packet scheduling technique transmits the packet at the head of the queue. This technique is FIFO and it transmits packets in the order in which they were received, independent of user application.

**2. Strategies for mobile data traffic offloading**

In this concept of data offloading is not new. Generic Access Network (GAN), it is also known by its commercial name Unlicensed Mobile Access (UMA), is a 3GPP standard released in 2005 and designed to enable access to GSM and GPRS mobile services over unlicensed spectrum, including Bluetooth and Wi-Fi. This technology chosen by many industries to offload the data. It is an alternate method to offload the data thorough WiFi. Globally 33% of the total mobile and tablets data traffic was offload onto the fixed network through dual mode WiFi. This is shows good impact already. Given that much of the total mobile data traffic is generated at users' homes, Wi-Fi. However, the strength of Wi-Fi is that it is already widely available so the possibility of using the existing capacity makes it a better option from a deployment cost point of view. Mobile data offloading will keep growing and it is also predicted that it could become a new industry segment. A technology that was originally hold as a temporary solution to deal with the growth of data traffic while wait for position of new generation networks.

**3. IP flow mobility for future wireless networks**

In the IP flow mobility there are two approaches namely client-based and network based IP flow mobility. The client-based is based on Mobile IPV6, extending its basic functionality to also support dual stack IPv4/IPv6 scenario. In order to enable flow mobility in a client-based mobile IP context, the IETF has standardized the basic components that are required.

The components are:

•Multiple CoA (care of address) registration support

• Flow bindings support

• Traffic selector’s definition

The basic MIPv6 protocol provides the tools to bind a HoA to single CoA. The flow mobility requires the ability to receive traffic plan to the same HoA via different CoA. MIPv6 needed to be extended to support the registration of several CoAs with the same HoA. This is the purpose of the Multiple Care-of Addresses Registration extensions, standardized in RFC 5648. Multiple CoAs for a HoA and create multiple binding cache entries. In order to do so, the binding update (BU) message defined by MIPv6 is extended with a new mobility option used to carry a CoA and a number to uniquely identify the binding entry, called the binding identification (BID) number.

Network –based IP mobility locate the solutions at the terminal of the network. In this way terminal is not required to perform any kind of signaling to react to changes of its point of attachment to the network. As these changes are transparent to the mobile terminal IP protocol stack. Proxy MIPv6 (PMIPv6) is the protocol standardized by the IETF to provide network-based IP mobility support. Although this protocol provides basic multi-interface functionality, in its current state it is not able to provide full flow mobility granularity. Hence, extensions to support it are required and are being standardized in the IETF NETEXT Working Group (WG).

**4. Virtualization techniques for efficient network sharing**

This technique is require to for growing the need for an enhanced infrastructure with a high degree of flexibility and adaptability to service requirements. In this virtualization techniques represent a best solution for providing good quality of service, service isolation and real time adaptation to service requirements. Network virtualization technology has evolved from virtual local area networks, VPN, active programmable networks and overly networks. Based on the virtualization technology and network virtualization concept, traffic load and communication operations could be easily controlled and managed to better support big data applications and parallel processing systems, online gaming, High Definition Television (HDTV), and bandwidth on-demand, such as MapReduce.

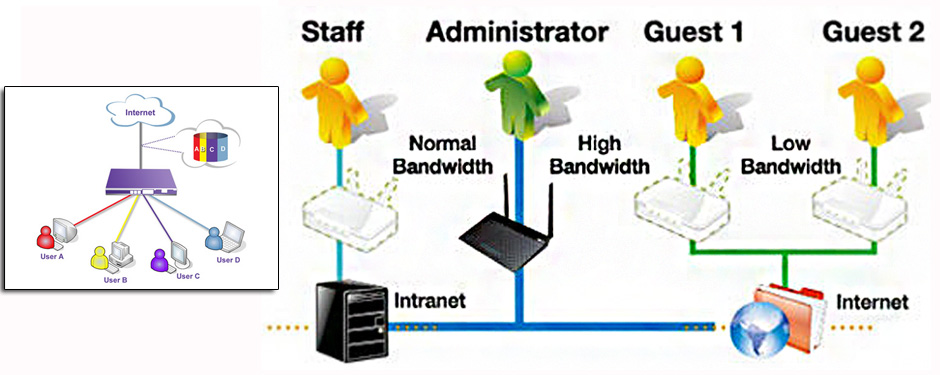
Two virtual nodes from the same virtual network are mapped to different physical nodes, although two virtual nodes from different virtual networks can be mapped to the same physical node. The main resources used by virtual nodes and virtual links are CPU and bandwidth, respectively. Under the term link virtualization, multiple separate traffic flows are transferred over a shared link (physical or emulated), in such a way that each traffic flow appears to be using a dedicated link referred to as virtual link. The guarantee is achieved by reserving some resources over an entire communication path using the resource reservation protocol. In modern packet-switched networks, traffic classification combined with packet scheduling algorithms is used to differentiate QoS levels.

A virtual network device is any networking device that does not exist in a pure physical form, but acts like an analogous physical equivalent. A virtual network device can be broadly classified as follows: (i) device aggregation that enables multiple networking devices to act as a single logical entity; (ii) device emulation represented by software emulating a physical device, where emulation can be applied to selected parts or the whole device.

There are different virtualization approaches that can support network topology virtualization, such as the following: (i) VLANs; (ii) VPNs; and (iii) active and programmable networks.

**5. Bandwidth Management Issues**

Now that broadband services are present and bandwidth is widely available, for dealing with bandwidth congestion, the telecom service providers need to find above-board solutions by adopting traffic management ideas that provide users with clear options and mitigate bandwidth congestion caused by applications like peer-to-peer computing. The transition to widely available broadband Internet has changed a lot in the present days in their behavior of some end users who consume inordinate amounts of bandwidth. The unexpected rise in demand from these users invalidated residential Internet business models and forced service providers to introduce network congestion and traffic management practices, the most controversial thing in bandwidth management is [deep packet inspection](http://searchcloudprovider.techtarget.com/tip/Deep-packet-inspection-Controversial-but-valuable-traffic-management-tool) (DPI).

****

There is war between a small percentage of bandwidth users and service providers has escalated into a full-scale conflict in terms of how much bandwidth users are paying for and what constitutes abusing the network. Bandwidth management issues that have come to the surface include cable operators trying to stop third parties from delivering video over their infrastructure, regulatory actions to oversee traffic management policies, and Congressional hearings on broadband services. Add users who have bandwidth and carriers that perform covert traffic management actions to that explosive mix the most infamous.

The whole traffic management issue would be an exciting thing if it didn't affect the performance of the Internet.

* **Bandwidth usage**:

Before broadband Internet technologies (cable, DSL and fiber) were introduced, almost all residential Internet services were based on dial-up access, which contains an implicit usage model: the longer you are connected, the larger your phone charges. Even when ISPs offered flat-rate services and there were no hidden charges, access speeds were so low that average line utilization closely matched maximum line speed.

The dial-up access model also provided clear separation between individual users, so their traffic mixed only on backhaul and transit links. The limited number of dial-in ports at each point of presence (POP) represented another bottleneck that limited core network congestion.

Fast-forward a few years to the broadband explosion, where the landscape has changed dramatically.

* Numerous service providers offer broadband access that uses shared media (cable). The bandwidth of the access link is shared by many users, and a single misbehaving user can affect the whole segment.
* The average bandwidth consumption has not grown in proportion to increased access-line speeds. It's hard to stress a 10 Mbit connection when you're reading email, chatting on IM, commenting on friends' Facebook photos or even watching YouTube videos.
* Users are online all the time, and the dial-up port barrier has been busted because of the use of a lot of bandwidth.

Furthermore, ruthless competition among providers has eroded most of the profit margin, and they are forced to utilize large access-to-backhaul and even larger access-to-transit oversubscription ratios.

* **Realistic service definitions and acceptable-use policies**:

All this wouldn't be so bad if service providers were transparent and truthful in their service offerings. In most cases, their marketing departments committed the original sin by launching fuzzy "service definitions" along the lines of "20 Mbps Amazingly Fast Internet Connections." The actual speed (beyond the local office) or user behavior expectations were never specified, apart from vague acceptable-use policies.

* **Technical problems in the residential broadband market:**

The problems in this are

1. Users who don’t conform to expectations.

The average usage of a typical residential user is a small percentage of the access speed. Service providers rely on this behavior and use high oversubscription ratios in their calculations, otherwise they could never achieve the financial break-even point with current low prices. A small percentage of "abnormal" users that saturate access links for prolonged periods, sometimes days or weeks, can adversely affect a large user population**.**

1. Peer-to-peer applications

One of the fundamental design assumptions of the Internet is that each application session gets its fair share of bandwidth. The [TCP](http://searchnetworking.techtarget.com/definition/TCP) protocol and existing queuing mechanisms in routers and switches are fine-tuned to achieving this goal, resulting in fair service delivery across a large user base, as long as each customer uses approximately the same number of TCP sessions. Peer-to-peer applications typically open a large number of constantly active TCP sessions.

1. Video streaming affects other applications

Some video applications use TCP to download the content (YouTube or Netflix, for example). Others, particularly the streaming applications, use the UDP. Since UDP doesn't respond to congestion and packet loss as well as TCP, users receiving UDP video streams could squeeze out TCP users (Web browsing, email, etc.) in addition to using large amounts of bandwidth for a long time.

1. Undesired applications tend to be obfuscated and encrypted

The moment a noticeable percentage of users started to use bandwidth-hogging applications, service providers engaged in a lose-lose game of trying to identify the offending applications and slow or block them. The developers of these applications responded by obfuscating them (using random TCP or UDP port numbers or pretending to be Web requests) and encrypting the content to prevent packet inspection looking for application-specific signatures.

**6. NEUTRAL MANAGEMENT WITH LTE TECHNOLOGY:**

This technique provides an approach that would serve to:

1. Provides application a prioritization in situations of moderate congestion, with the wireless carrier prioritizing users seeking a premium service and
2. this enable like applications to be treated in a like way for purposes of QoS during periods of severe congestion, with the wireless carrier determining the mechanics of prioritization for a given class of applications as defined by standards bodies or the FCC.

This approach and others can be implemented within the framework of the LTE standard and within the capabilities of LTE technology. Indeed, it would be counterproductive to create an environment that diverges unnecessarily from other industry efforts or creates minimum levels of service based on wireline service norms. Therefore, the proposed framework described below draws on current practices, the LTE standards, work currently underway to create QoS for mission-critical FirstNet applications, and the development of QoS technologies and standards that can include independent edge providers as well as wireless carrier.

* Application-Agnostic prioritization in moderate congestion:

The wireless carriers are prioritizing users when they “throttle” capacity for users who have exceeded capacity limits. This type of prioritization is already commonly implemented and widely understood. Application agnostic prioritization can also be implemented in a more affirmative, user-directed fashion, such as by offering subscribers the option to pay a premium for prioritization at times of congestion, as noted in the previous section.

* Prioritization of like applications with like prioritization in severe congestion:

In severe congestion, latency-sensitive applications become impaired or stop working. We outline below a technical approach for like prioritization of like application under those conditions. Wireless carriers have begun to use application-specific QoS profiles and will use them more frequently as the utilization of networks increase, as congestion increases, as latency-sensitive and bandwidth-rich applications grow in popularity, and as wireless carriers develop partnerships with select edge providers.

* Once the wireless carrier began to offer QoS for applications in those categories, the carrier would also be required to offer the same QoS treatment to all like applications in those categories, including over-the-top applications and small edge providers unaffiliated with the wireless carrier. Implementation of our proposed approach by a carrier includes the following steps:

1. The wireless carrier establishes a set of QoS profiles, with each profile supporting a class of applications that may require like QoS treatment (e.g., streaming, interactive video, toll-quality voice, and so on).
2. An edge provider identifies itself to the wireless network as an operator of an application that should be placed in one of the profiles and receive QoS.
3. A user device activates the application, identifies itself to the wireless network and the edge provider through the default bearer connection, and asks to operate the application through the network.
4. The edge provider authenticates the user device to use the application (if required by the edge provider).
5. The wireless carrier sets up QoS between the user device and the Internet according to the QoS characteristics of the profile.

**Conclusion:-**

* The LTE technology is capable of managing congestion through prioritization protocols.
* When with severe congestion, prioritize latency-sensitive while avoiding discrimination among applications, content or services.

**References:**

1. <https://www.bitag.org/report-congestion-management.php>
2. <http://www.strategies.nzl.com/wpapers/2012013.htm>
3. <https://www.researchgate.net/publication/220144705_IP_flow_mobility_Smart_traffic_offload_for_future_wireless_networks>
4. <http://searchtelecom.techtarget.com/tip/Broadband-traffic-management-Finding-rational-solutions-to-ease-congestion>
5. <https://static.newamerica.org/attachments/188-mobile-broadband-networks-can-manage-congestion-while-abiding-by-open-internet-principles/OTI_CTC_Wireless_Network_Neutrality_Engineering_Study_FINAL_111314.pdf>
6. http://searchtelecom.techtarget.com/tip/Offering-realistic-broadband-service-definitions-and-acceptable-use-policies