QoS ARCHITECTURE FOR BROADBAND WIRELESS ACCESS BASED NEW PUBLIC NETWORK

ANJALI AGARWAL
Assistant Professor
Dept of Electrical and Computer Engineering
Concordia University
Montreal, Quebec, Canada

YOUSEF SHAYAN
Vice President, Engineering
BroadTel Canada
Saint Laurent, Quebec, Canada

ABSTRACT

This paper provides a description of the new public network architecture that is committed to replace the traditional IP network to include multimedia services for Broadband Wireless Access systems. Focus is on the different mechanisms and models available and the important aspect of end-to-end implementation of quality of service in the new public network domain. Quality of Service based on different service levels is considered in every side of the network – user, backbone network access based on fixed wireless link, and IP core network. The issue of an end-to-end implementation of network management system and security aspects is also considered.

KEY WORDS

Broadband Wireless Access, Quality of Service, Media Access Control, Voice over IP

1. INTRODUCTION

In recent years, the most active area in networking is – data, voice, and video integration. Business and residential users are beginning to combine real-time applications such as voice and video, which have a limited tolerance for network latency, with non-real time data traffic. In the wireless world, interests have also begun to provide point-to-multipoint broadband wireless access (BWA) system supporting high speed data and high quality voice services to enterprise and residential customers. BWA's architecture allows customers and service providers to enable their IP networks for telephony applications by deploying wireless access for voice, video and data applications over their existing IP/Data networks. Evolution of the current public switched telephone network to new public network is largely based on replacing much of the circuit-switched infrastructure with an IP-based packet-switched infrastructure.

Figure 1 presents a Voice-over-IP (VoIP) solution featuring IP-based BWA products interfaced to the IP network. There are basically three main building blocks: base station that serves as the central packet flow equipment linking backbone networks to access points; remote station that serves as the multi-service end-user access equipment; network management system that serves as the service provisioning and network operation management system. The base station communicates with the remote stations through the wireless link.

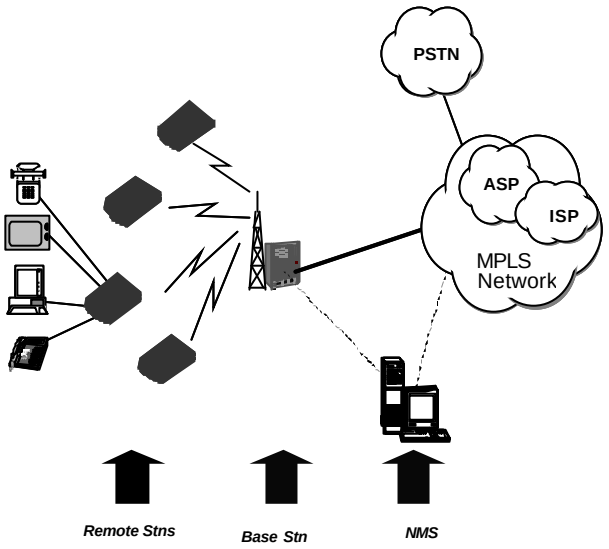

Figure 1: Broadband Wireless Access solution

2. QUALITY OF SERVICE

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies including Ethernet and 802.1 networks, Wireless networks, IP-routed networks, Asynchronous Transfer Mode (ATM), and Frame Relay that may use any or all of these underlying technologies. There are four factors that can profoundly impact the quality of service: delay, jitter (delay variability), packet loss and out of order packets, and bandwidth available. Service levels refer to the actual QoS capabilities,

meaning the ability of a network to deliver service needed by a specific network application from end-to-end. This can also include edge-to-edge, as in the case of a network that connects other networks rather than hosts or end systems, (the typical service provider network, for example), with some level of control over bandwidth, jitter, delay, and loss, provided by the network. Essentially, QoS can provide three levels of strictness from end-to-end or edge-to-edge: best effort, differentiated, and guaranteed.

Best-Effort Service: is basic connectivity with no priorities or guarantees. It provides basic queuing during congestion with first-in, first-out (FIFO) packet delivery on the link. Examples of this type of traffic include a wide range of networked applications such as low-priority e-mail and general file transfers.

Differentiated Service: treats some traffic better than the rest (faster handling, more bandwidth on average, lower loss rate on average), however, there is no hard and fast guarantee. With proper engineering, differentiated service can provide expedited handling appropriate for a wide class of applications, including lower delay for mission-critical interactive applications, packet voice applications, and so on. Typically, differentiated service is associated with a course level of Packet classification, which means that traffic gets grouped or aggregated into a small number of classes, with each class receiving a particular QoS in the network. The Differentiated Services (DiffServ) working group in the IETF is working on specific standards and definitions for services that fall under Differentiated QoS, largely focusing on the use of the ToS field in IPv4 header as a QoS mechanism.

Guaranteed Service: is an absolute reservation of network resources, typically bandwidth, which implies reservation of buffer space along with the appropriate queuing disciplines, and so on, to ensure that specific traffic gets a specific service level. This type of service is for delay-sensitive traffic, such as voice and video and is intended for applications requiring a fixed delay. The Integrated Services (IntServ) working group in the IETF has developed specific standards and definitions for services that fall under Guaranteed QoS. This effort attempted to specify flows in the Internet with varying requirements. RSVP was developed as a QoS signaling mechanism to provide these types of flow-based services.

2.1 End-to-End Implementation

There are three main components in an implementation of the end-to-end QoS in the new public network architecture (Figure 2). It requires that every element in the network path deliver its part of QoS:

1. QoS in the user-side network and remote station
2. QoS in the BWA network
3. QoS in the base station and the backbone core network

User-side Network and Remote Station

On the user side, a remote station may receive voice packets and/or data packets that are differentiated based on the ports on which they are received. For packets arriving at the voice port, its related service level is provided in the Layer 2 and/or Layer 3 header. For packets arriving at the data port, best effort service is provided if not specified in its Layer2/Layer3 header. If the same port is used for both voice and data packets, as in the case of PC and IPphone connected on the same network interface, differentiation is based on some fields of the Layer 2 header or Layer 3 header. The IEEE 802.1p prioritization field is added to the Ethernet packets by most of the terminal equipments such as IPphones providing voice traffic, to differentiate voice from data on the same port. If 802.1p field is not present, the packet is considered to be of lower priority on the same port. This prevents PCs transmitting data from obtaining higher priority relative to delay-sensitive applications.
802.1p establishes eight levels of priority similar to IP Precedence bits in the ToS byte, with 0 assigned as the lowest priority for Best-Effort traffic and typically 6 assigned for Interactive Voice traffic, enabling end-stations to request priority and network devices to enforce those priorities.

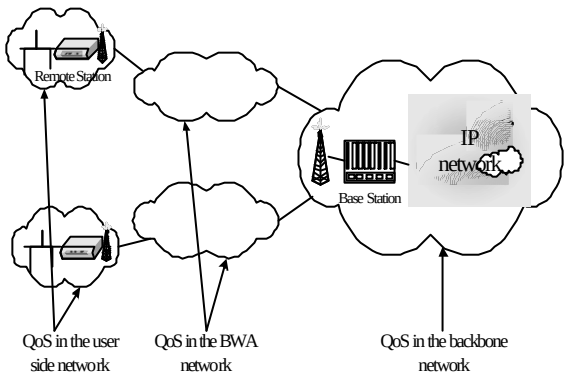

Figure 2: End-to-end QoS

Broadband Wireless Access Network - Remote Station/Base Station and Over the Air

Quality of Service is supported for both upstream and downstream traffic through the Remote station/Base station and over the air. The protocol mechanisms provide traffic shaping and policing, queuing based on the ToS byte, classification of the incoming packets to a specific QoS service flow, fragmentation, concatenation, and payload header suppression. Different levels of QoS are provided to different flows; from best-effort type flows that do not have any delay/jitter/minimum bandwidth requirements to flows that enable higher bandwidth efficiency for meeting delay requirements of very tight delay/jitter real-time traffic. Preferential treatment is

given to higher priority flows such as business database access compared to other best-effort flows such as FTP or Web browsing.

Real-time service flows that generate fixed-size data packets on a periodic basis and may become inactive for substantial portion of time, such as Voice over IP traffic are supported with silence suppression. When the flow corresponding to these services is inactive, non real-time service flows that require variable size data grants on a regular basis, such as high bandwidth FTP, are serviced. Figure 3 explains this for a simple BWA network with one remote station and a base station.

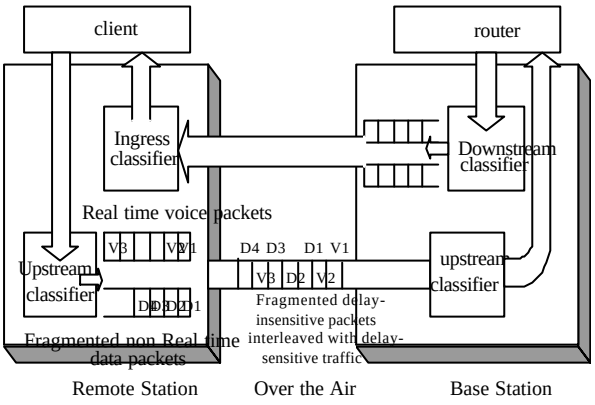

Figure 3: Mix of real-time and non real-time service flows

Using this approach multiple services are supported on a single channel over the air. Service Flow packets queued at the Base station in the downstream direction are also based on the 802.1p/ToS byte.

Base Station and the IP core network

The Base station maintains the service levels provided in the packet's Level2/Level3 header and forwards the packets in the upstream direction to the backbone network's router. In the downstream direction, the packets are forwarded from the router to the classifier where packet classification is done based on 802.1p/ToS byte.
Router switches that can forward packets and apply traffic conditioning at wire speeds are essential to provide QoS delivery in the IP backbone network. In fact, true end-to-end QoS within the IP network requires that every element in the network path – router, switch, firewall, etc. – deliver its part of QoS. The Service Providers who are providing Broadband Wireless Access to their customers should ensure that QoS elements are available throughout in the Intranet/Internet, or some other mechanisms such as reserving the bandwidth are available to support QoS in the network. The presence of legacy routers will potentially limit service offerings and the QoS level will default to the capability of the lowest performing router.

One of the possible solutions for the Service Provider would be to confine legacy routers to the best-effort traffic only and the QoS-sensitive traffic to send over ATM network. Following Figure 4 shows this. In addition to a large ATM cell header overhead, the disadvantage of using ATM networks would be the requirement to still use routers at the boundary of the network, and to maintain two sets of configurations: one for routers and the other for ATM switches.

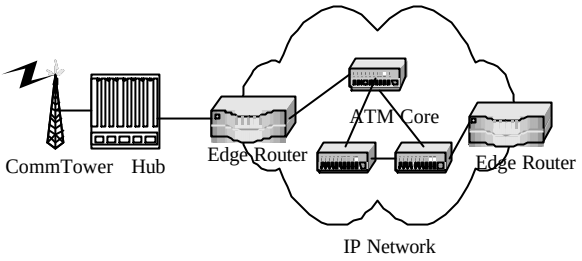

Figure 4: Delay-sensitive traffic channeled to ATM core

Another solution would be the use of Multi Protocol Label Switching (MPLS) with Differentiated Services (DS) where by router networks can also provide QoS and Traffic Engineering. The Service Provider must have a Service Level Agreement (SLA) with the BWA customers specifying the service levels supported. The BWA network marks the DS fields of individual packets to indicate the desired service and the ingress (edge) routers classify, police and possibly shape the incoming packets based on the service level agreements using the First-in First out Queuing, Weighted-Fair Queuing, Priority Queuing, or other queuing mechanisms. To support interactive traffic, the router should also be able to support fragmentation of large datagrams and interleaving of delay-sensitive packets with the resulting smaller packets. The BWA network should be made MPLS adaptive by providing the class of service fields to the MPLS based Service Provider network. The Remote Station does not need to implement MPLS since the BWA network has its mechanisms to provide QoS and traffic engineering at MAC layer itself.

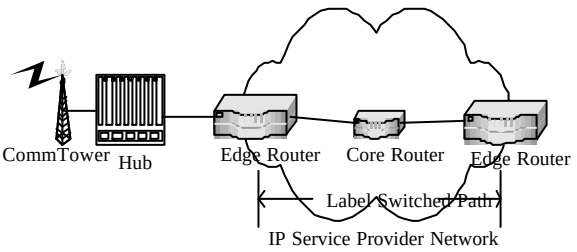

Figure 5: MPLS based Service Provider Network

3. NETWORK MANAGEMENT SYSTEM

Network management system (NMS) in a end-to-end network architecture consists of two major levels – management of the Broadband Wireless network Access products (Remote stations and Base stations), and management of the IP Core. Network access products are to be managed by web-based network management system while the IP core is to be managed by IP backbone Network Service Providers (NSPs). Network management system can be provided using a base platform that includes any SNMP compliant manager. The platform incorporates features to analyze alarms and presents the NMS personnel with the specific problem to investigate, along with complete information about the problem from data collected.

Network Access Management System

Network Access Management system remotely maintains the network access devices serving a given Broadband Network Access region. The primary functions of the access management system are:

- Configuration Management – to establish and provision service in accordance with customer service level agreements and change orders. This includes rapid configuration of remote stations and base stations for provisioning capacity to end-users
- Fault Management – consists of collecting, analyzing, and reacting to any alarms received from any device on the access network. This is performed on both a polling as well as a device-initiated basis. Alarms are analyzed on the basis of their severity, source, exceeding threshold values, and their mask criteria.
- Performance Management – to ensure that the access network operates as designed and delivers the service as contracted. Performance related data is collected and monitored for any unusual events. Based on the compilation of statistics reports are generated to document any conditions that might affect network performance and to document compliance with SLA parameters.

For all functions of the management system information can be transmitted using encrypted SNMP with both public and proprietary MIB blocks.

IP Core Management System

To manage bandwidth services for different service level agreements across the IP core network the old model of "best effort" delivery is no longer adequate. Extensive over-provisioning of the network to "guarantee" bandwidth is not a requirement anymore. Network Service Providers can use their network management systems to engineer guarantees into the IP core network. A customer can be provisioned with a minimum committed information rate (CIR) by adequate provisioning of the core network.

The primary functions supported by the IP core management system are similar to the access management system – configuration management, fault management, and performance management – except now these functions are related to the IP core instead of the access network. These functions include continuous testing and verification of network latency, and continuous monitoring of network traffic and network status.

Meeting QoS metrics based on configured SLAs is becoming a stringent requirement for service providers to meet their contractual obligations. Quality of Service and the measurement and assurance of QoS have taken a significant role in defining future network architecture requirements.

4. SECURITY

Security in the Access Network

Subscribers to the access network services must take precautions to secure their systems prior to attaching them to a public network. Users are provided with data privacy across the wireless network by encrypting traffic flows between the remote station and the base station located in the wireless network. Encryption of the MAC frame packets over the air follows the U.S. Data Encryption Standard (DES), and will be extended to support the new Advanced Encryption Standard (AES) once it is in place. An authenticated client/server key management protocol is employed in which the base station controls distribution of keying material to remote stations using X.509 digital certificates, RSA public key encryption and triple DES to secure key exchanges.

It should be noted that these security services apply only to the access network. Once traffic makes its way from the access network onto the Internet backbone, it will be subject to privacy threats common to all traffic traveling across the Internet, regardless of how it got onto the Internet.

Security in the IP Core Network

All IP messages will always be carried over secure Internet connections, as defined in the IP security architecture as defined in RFC 2401, using either the IP Authentication Header, defined in RFC 2402, or the IP Encapsulating Security Payload, defined in RFC 2406. All MGCP messages between Call Agents and access network are also carried over secure Internet.

5. CONCLUSIONS

With Internet usage doubling each year, more and more companies have started to develop products for Internet

Telephony and other real-time applications. In this work we provide a new public network architecture for Broadband Wireless Access systems that connects the user endpoints to the IP backbone network through wireless medium in order to provide real-time services such as voice and video, and non real-time data traffic. This paper proposes architecture to implement end-to-end quality of service for the same. Both access network and IP network should recognize and treat packets belonging to real-time traffic with priority. This involves marking such packets, classifying the packets based on the markings so that they are given differential treatment, and allowing the scheduling mechanisms to transmit the packets in a timely manner. The issues of end-to-end implementation of network management system and security are also considered for the new public network architecture.

6. REFERENCES

1. M. Arango et al., "Media Gateway Control Protocol, v1.0," RFC 2705, Oct 1999; http://www.ietf.org/rfc/rfc2705.txt
2. R. Braden, Ed. et al., "Resource ReSerVation Protocol (RSVP) --Version 1 Functional Specification," RFC 2205, Sep 1997; http://www.ietf.org/rfc/rfc2205.txt
3. Anjali Agarwal, "Quality of Service (QoS) in the New Public Network Architecture", IEEE Canadian Review, Fall 2000, No.36, pp 22-25.
4. M. Carlson et al., "An Architecture for Differentiated Services," RFC 2475, Dec 1998; http://www.ietf.org/rfc/rfc2475.txt
5. R. Braden, D. Clark, S. Shenker, "Integrated Services in the Internet Architecture: An Overview," RFC1633, June 1994; http://www.ietf.org/rfc/rfc1633.txt
6. J. Wroclawski, "The Use of RSVP with IETF Integrated Services," RFC 2210, Sept 1997; http://www.ietf.org/rfc/rfc2210.txt
7. S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, Nov 1998; http://www.ietf.org/rfc/rfc2401.txt