Bachelor's Thesis (UAS)

Degree Program: Information Technology

Specialization: Data Communication & Networking

2011

Donald Egbenyon

Implementing QoS for VoIP in a Local Area Network (LAN)

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR’S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree Programme: Information Technology

November, 2011 | 54

Instructors: Harri Waltari, Ossi Väänänen

Quality of Service (QoS) is being deployed by most VoIP service providers today in order for such enterprises to efficiently use its bandwidth in an integrated network. These service providers expect their respective clients to implement QoS on their LAN in order to maximize the bandwidth resources at their disposal and ensure a flawless and high quality VoIP for its use. With the necessary equipment in the LAN, the network administrator with the required knowledge in QoS design and implementation can configure the various routers and switches to give priority to voice in the LAN.

This thesis focuses on the implementation of Quality of Service (QoS) in a LAN that extends over an IP/MPLS network. QoS was configured on all the switches in a particular network in order for priority to be given to the Voice packets going through this network. The aim is to show that although QoS is not so important in a LAN within a Region, it becomes important when that LAN extends to other Regions over an IP/MPLS network.

Keywords: VoIP, QoS, LAN, DiffServ

CONTENTS

FIGURES

TABLES

ACRONYMS, ABBREVIATIONS AND SYMBOLS

SNOM	SNOM Technology AG
SIP	Session Initiation Protocol
QoS	Quality Of Service
LAN	Local Area Network
VoIP	Voice Over internet protocol
IP	Internet Protocol
IntServ	Integrated Services
DiffServ	Differentiated Services
IETF	Internet Engineering Task Force
CoS	Class of Service
ToS	Type of Service
DSCP	Differentiated Service Code Point
PSTN	Public Switch Telephony Network
VoIP	Voice Over Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
RTP	Real-time Transport protocol
VIP	Sonera VIP softphone
HTTPS	Secured Hypertext Transport Protocol
STCP	Secured Transmission Control Protocol
PHB	Per Hop Behaviour
ACE	Access Control Entity

1. Introduction

A local area network (LAN) is a network covering a small geographical area. LAN is a high-speed data network that uses the Ethernet technology in connecting different devices together. Since the Ethernet technology offers simplicity, it is being deployed in WAN and used to connect LAN thus bringing simplicity to the Internet, as well. The Internet is a system of interconnected networks all over the world that connects millions of computers together.

The Internet network was designed to carry data on a best-effort delivery basis using either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), which are the two most common transport layer protocols of the Internet. It was designed with the notion of giving all traffic equal priority over the network. All packets have an equal chance to be delivered and an equal chance also to be dropped. This best-effort model of the Internet Protocol (IP) was completely suitable for most data packets carried over the network from one point to another until the advent of Voice over Internet Protocol (VoIP) or IP Telephony. Thus, the network should be able to carry voice, data, video and other traffic over a converged network instead of creating and maintaining separate networks.

A converged network allows the flow of the voice, video and data packets over it. This convergence reduces cost and complex network layers. When it is carefully designed and implemented, it has the ability to save bandwidth and the equipment used on such a network. The heart of the converged network is VoIP.

VoIP is the process of converting analogue audio signals to digital signals that can be transmitted over the Internet. It provides voice and telephony services over an IP network. The discovery of VoIP changed the paradigm of “IP over everything” to “everything over IP” [5]. This arrival of VoIP showed a flaw in the way IP carries packets. Voice packets will not wait to be delivered at the time the network chooses but it specifies a particular time of delivery which the network must abide to. This means that the best-effort delivery model of the IP network cannot be tolerated by voice packets. The network has to be configured to give more priority to some packets while giving less priority to other packets. This means that Quality of Service (QoS) has to be configured on a network in order for different priority to be given to traffic.

So because converged networks have taken a firm hold on the communication industry, most service providers of VoIP are encouraging the use of a converged network instead of separate VLANs for the voice, data and video packets. In order for these voice and data packets to be carried in the same VLAN, the network must be properly configured with the right priorities given to voice, data and video. If this is not done, it will eventually lead to chaos in the network as a result of congestion. This congestion is as a result of too many packets competing for the same bandwidth, thus all packets have an equal chance of being dropped by the switch or router. To avoid such scenario, Quality of Service (QoS) has to be configured on the switch in order for preferential treatment to be given to packets that are extremely important and require less delay. In this thesis, priority is given to voice packets in a particular network by configuring the switches to recognize voice packets. The goal is to implement QoS on the entire network.

The purpose of this thesis is to configure QoS in a converged local area network. It starts with giving an overview of QoS in Chapter 2. This chapter explains the reason QoS is needed for a network. Chapter 3 then gives details of how QoS can be beneficial to VoIP while Chapter 4 is used to explain the necessary materials required to configured QoS in a specific network. Chapter 5 then goes further to describe the way QoS configuration can be implemented in a network while Chapter 6 describes the results gathered and the conclusion of the work.

2. QoS Overview

Quality of Service (QoS) is the ability of a networking equipment to differentiate among different classes of traffic and to give each class different priority over the network when there is congestion in the network based on the traffic significance. QoS is not something that will be configured on a router or switch, rather it is a term that refers to a wide variety of mechanism used to influence traffic patterns on a network [21]. It gives network administrators the ability to give some traffic more priority over others.

2.1. Models of QoS

The purpose of QoS usage is to make sure that minimum bandwidth is guaranteed for identified traffic, jitter and latency is being controlled and packet loss is improved. This can be carried out using several means either QoS congestion management, congestion avoidance or policing and traffic shaping. The means chosen depends largely on the goal of the network administrator.

QoS can be divided into three different models.These models describes a set of end-to-end QoS capabilities [14]. In order to facilitate end-to-end QoS on an IP network, the Internet Engineering Task Force (IETF) defined two models: Integrated Services (IntServ) and Differentiated Services (DiffServ)[5]. A default model that comes with all networking devices is the Best Effort model. It does not require any QoS configuration. The IntServ model follows the end-to-end signalling process whereby the end-hosts tells the network their QoS needs in advance while DiffServ follows the provisioned-QoS model whereby the network elements set up multiple classes of traffic with different degrees of QoS needs.

IntServ provides high QoS for IP packets but it requires special QoS to be made available by the network for a period and that bandwidth should be reserved. This method uses a protocol to reserve bandwidth on a per flow basis. This protocol is called the Resource Reservation Protocol (RSVP). RSVP is a signalling mechanism that is used by IntServ architecture to carry out its function. Once the IntServ session is established it has to be maintained by the router along the path to that session. The IETF recommends that RSVP path and Reservation messages should be sent every 30 seconds periodically along the session path to prevent the soft state from timing out in the routers. A session will continue until it is torn down or there is no refresh messages received by the routers along the path and when this happens the soft state in the router times out. When such a measure is implemented, packet delivery is guaranteed but it limits the scalability of a network.

On the contrary, DiffServ provides the need for simple and coarse methods of putting traffic into classes, called Class of Service (COS). It does not specify that a specific protocol should be used for providing QoS but specifies an architectural framework for carrying out its function. DiffServ carries out its major function through a small, well-defined set of building blocks from which different aggregates of behaviours can be built [5] .The packet Type of Service (TOS) byte in the IP header is marked in order for the packets to be divided into different classes which forms the aggregate behaviours[5]. Differentiated Services Code Point (DSCP) is a 6-bit bit pattern in the IPv4 TOS Octet or the IPv6 traffic class Octet [5]. DSCP supports up to 64 aggregates or classes and all classification and QoS in the DiffServ model revolves around the DSCP.

Though classification is carried in the IP header, it can also be carried in the Layer 2 frame. These special bits in the Layer 2 frame or Layer 3 packet are described below.

A. Prioritization bits in Layer 2 frames: Layer 2 Inter-Switch Link (ISL) frame headers carries the IEEE 802.1p class of service(COS) in the 1-byte User field while the Layer 2 802.1Q frame headers carries the COS value in a 2-byte Tag Control Information field. The Tag Control Information (TAG) field carries the CoS value in the 3 most-important bits, which is normally called User Priority bits in a Layer 2 802.1Q header frame. Layer 2 CoS values range from 0 for low priority to 7 for high priority. The figure below shows the 2-byte TAG

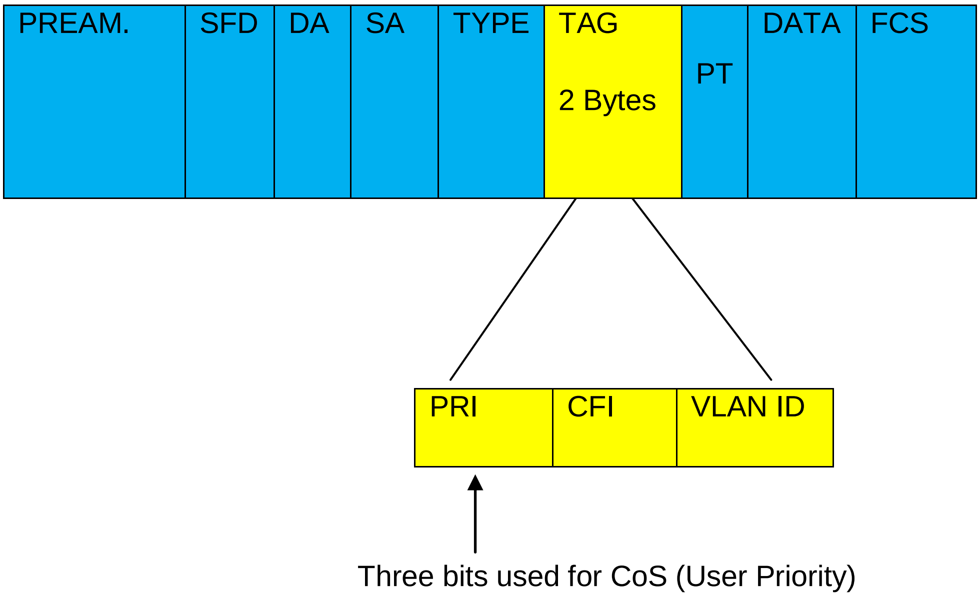


Figure 2.1. Overview of the TAG and User Priority in a Layer 2 802.1Q frame[26]

B. Prioritization bits in Layer 3 packets: Layer 3 IP packets can carry either Differentiated Services Code Point (DSCP) value or IP precedence value. This is possible because DSCP is backward compatible with IP precedence value. IP precedence values range from 0 to 7 while DSCP values range from 0 to 63. This can be seen in the table below.

Table 2.1. Comparing IP Precedence and DSCP values

IP Precedence and DiffServ		
Precedence	**DiffServ**	**DSCP**
7 111xxxxx	Class selector	CS7 111000xx 56
6 110xxxxx	Class selector 6 Expedited Forwarding	CS6 10000xx 48 EF 101110xx 46
5 101xxxxx	Class selector 5 Assured Forwarding 4	CS5 101000xx 40 AF4 100dd0xx 34, 36, 38
4 100xxxxx	Class selector 4 Assured Forwarding 3	CS4 100000xx 32 AF3 011dd0xx 26,28,30
3 011xxxxx	Class selector 3 Assured Forwarding 2	CS3 011000xx 24 AF2 010dd0xx 18,20,22
2 010xxxxx	Class selector 2 Assured Forwarding 1	CS2 010000x 16 AF1 001dd0xx 10,12,14
1 001xxxxx	Class selector 1	CS1 001000xx 8
0 000xxxxx	Best Effort	BE 000000xx 0

IP precedence 7 or DSCP 56 is reserved for network use. The DSCP values used in network configuration range from 0 to 48 while the IP precedence values used range from 0 to 7. Any of the DSCP values can be used to assign priority to a traffic flow.

3. QoS for Voice

Voice packets have minimal needs for delay. Voice packets are delay sensitive and a little delay in the transmitting of voice packets can cause so much discomfort to a user. For a long time, the Public Switched Telephone Network (PSTN) used to carry voice traffic from one user (caller) to another user (receiver). The PSTN uses a circuit-switched network. This means that when the caller decides to call the receiver, a circuit is open in the network between the caller and the receiver until the call is aborted. It guarantees that the caller can have a high quality call for as long as the call last. This circuit-switched network brings some difficulties because no other call can go through the already open circuit until it is closed. Also, it is expensive for the user since the user pays for the open circuit. In order to use a less expensive means of carrying voices over a network, the voice packet was designed to be carried as a packet over an Internet Protocol (IP). This gave birth to Voice over IP (VoIP). The major question in the minds of sceptics was if this new technology will be able to guarantee the same Quality of Service (QoS) that is required in voice communication. This is because the voice packet is not circuit-switched rather it is packet-switched over the network. Packet-switching entails the packet to be broken into fragments from the sender device and then reassembles before it gets to the receiver. Packet-switching technology is the ability to carry several voice communications at the same time without so many difficulties experienced in circuit-switch technology. In the case of VoIP, the major factors that will affect its quality are packet loss and packet delay.

Lost packets: Usually when data is being sent over an IP network some packets can be lost. Using TCP protocol, the lost packet can be resent but in the case of VoIP, it does use UDP. So any packet lost cannot be retransmitted. When a packet is lost, it brings about voice clipping and skips. There is a standard industry codec used to correct up to 30ms of lost voice in most Digital Signal Processor found on routers and switches.

Delay Packet (Latency): Packet delay is the time it takes a packet to reach the receiving end of an endpoint after it has been transmitted from the source. This is called end-to-end delay. It consists of two components: fixed network delay and variable delay. Packet delay can cause degradation of voice quality due to the end-to-end voice latency or packet loss if the delay is variable [6]. The end-to-end voice latency must not be longer than 250ms because it will make the conversation sound like two parties talking on a CB radio. If latency must be taken care of, then we have to know the main causes of latency. They are: codecs, queuing, waiting for packets being transmitted, serialization, jitter buffer and others.

Queuing, waiting for packets being transmitted and serialization are the main causes of delay and are the ones we can do something about while the other causes of delay, like jitter buffers, codecs, are causes we can do nothing about. This is where QoS can be used to prevent a voice packet from waiting on other packets before it is transmitted. QoS makes the voice to be sent out of queues faster than other packets in the queue and by giving more bandwidth to voice, it helps to mitigate against serialization delay.

In essence, QoS for the voice packets reduces latency, uses bandwidth well and delivers voice packets fast. Using Low Latency Queuing (LLQ) or Priority Queuing-Weighted Fair Queuing (PQ-WFQ) commands to give priority to voice is the preferred method of configuring QoS.

3.1. QoS tools for VoIP

The QoS tools for VoIP are a set of mechanisms used to increase the voice quality on a network by decreasing dropped voice packets during times of network congestion and by minimizing both the fixed and variable delays encountered in voice congestion[6]. The tools are divided into three categories: classification, queuing, and network provisioning.

3.1.1. Classification

Classification is the process of identifying traffic into classes and grouping the identified traffic into classes. It uses a traffic descriptor to categorize a packet within a specific group to define that packet [25]. These traffic descriptors are based upon incoming interfaces, IP precedence, DSCP, source or destination address and application.

Classification is the most fundamental QoS building block. Without it, all packets are treated the same. Usually, it should take place at the network edge maybe in the wiring closet or in the IP phones or in voice endpoints. The packets can be marked as important using Layer 2 Class of Service (CoS) setting on the User Priority bits of the 802.1p portion of the 802.1Q header or on the Differentiated Services Code

Point(DSCP)/ IP precedence bits in the Type of Service(ToS) byte of the IPv4 or IPv6 header as shown in Figure 3.1, 3.2, 3.3 and 3.4.

The diagram in Figure 3.1 shows the ToS field in IPv4 and IPv6 headers while the diagram in Figure 3.2 and Figure 3.3 shows the original IPv4 ToS field.

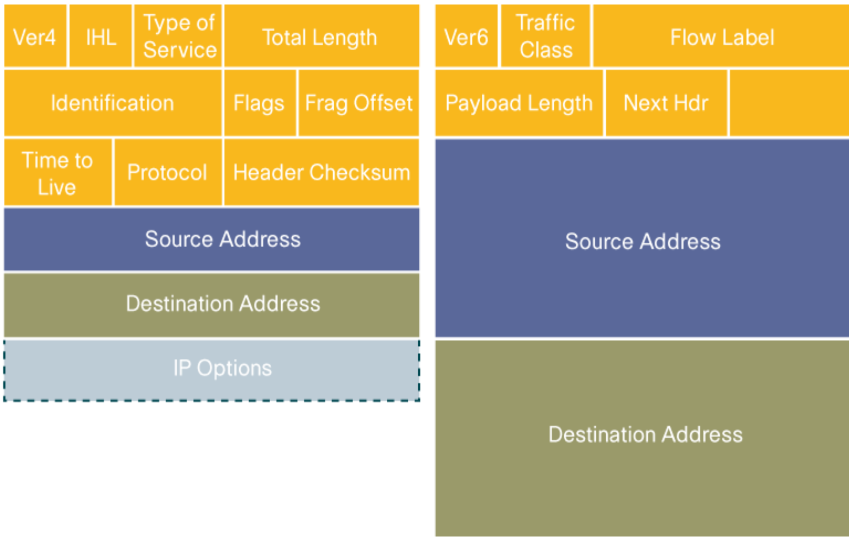


Figure 3.1. IPv4 and IPv6 headers [5]

This figure shows the ToS field before it was renamed to be the DS field.

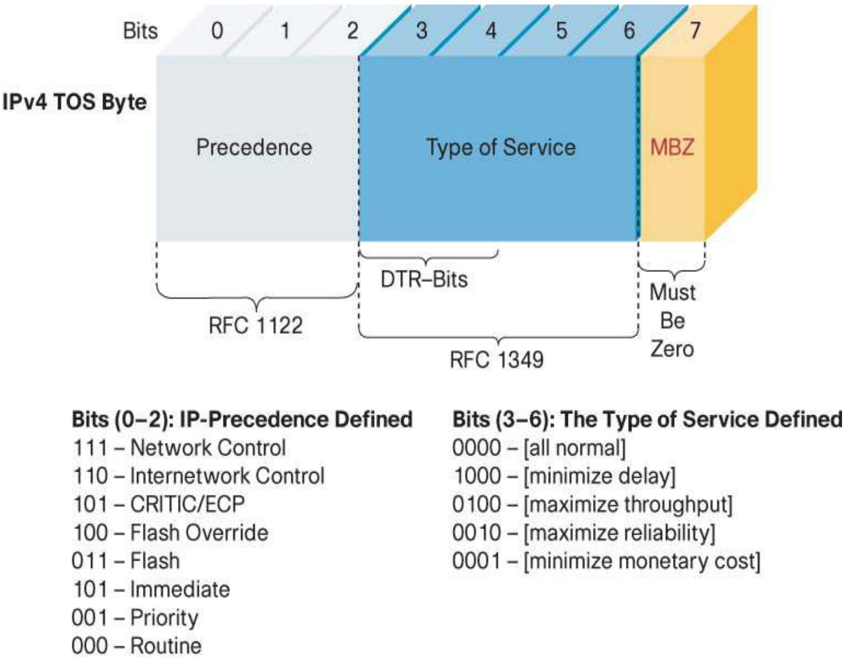


Figure 3.2. The original IPv4 ToS Byte [5]

This figure shows the DS field as is presently used today in the IPv4 header.

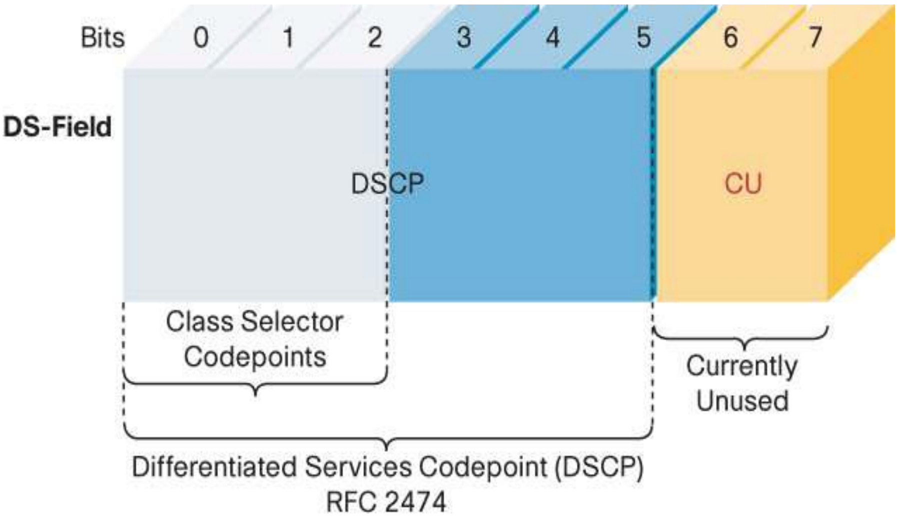
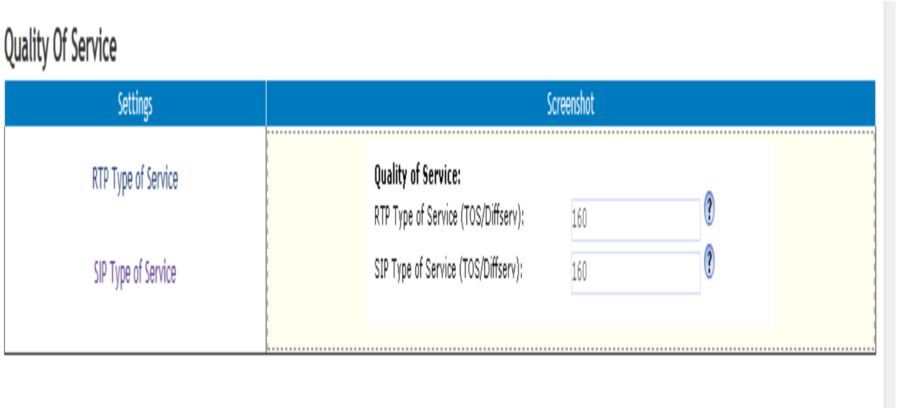

Bits
0
1
2
3
4
5
6
7
DS-Field
DSCP
CU
Class Selector Codepoints
Currently Unused
Differentiated Services Codepoint (DSCP)
RFC 2474

Figure 3.3. DiffServ CodePoint Field [5]

There is something worthy of note when it comes to classification. Some companies use the TOS marking to mark their DSCP settings. For example, most SNOM phones are marked with a TOS setting of 160. This can be seen in the figure below



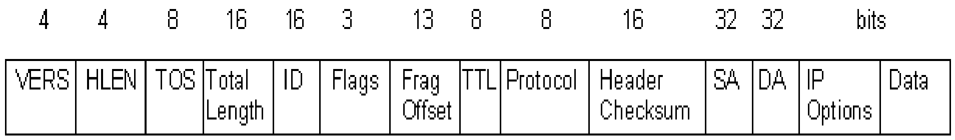
Quality Of Service

Settings	Screenshot
RTP Type of Service SIP Type of Service	Quality of Service: RTP Type of Service (TOS/Diffserv): 160 SIP Type of Service (TOS/Diffserv): 160

Figure 3.4. SNOM QoS setting [19]

Initially this looks confusing because it is not clearly started that this is IP precedence 5 until a close look is taken into ToS.

Type of Service (ToS) is an 8-bit field in the IP datagram header. It has been in the IP header from the beginning but was not used. It has two parts, the IP precedence value and ToS bits. Figure 3.5 below gives a clear picture of the location of this field in the IP header.



4	4	8	16	16	3	13	8	8	16	32	32	bits	
VERS	HLEN	TOS	Total Length	ID	Flags	Frag Offset	TTL	Protocol	Header Checksum	SA	DA	IP Options	Data

Figure 3.5. TOS 8-bits field [18]

The ToS field was renamed to the Differentiated Services field. 6-bits of the DS field is used as the code points for selecting the per-hop behaviour(PHB) while the last 2-bits are unused just like the original ToS field. Figure 3.6 gives a clear idea of what it looks like.

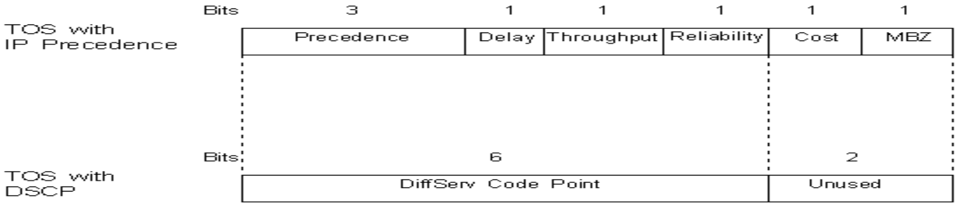


Figure 3.6. Comparing ToS to IP Precedence and DSCP [18]

Initially, it was established that the ToS field was not used by most manufacturers of networking devices and this is the reason why it was renamed to the DS field. Today, SNOM decides to use the ToS field in making the SNOM hard phone. According to SNOM hard phones manufacturers, the value 160 means IP precedence 5 or DSCP Class Selector 5(CS5) [16]. It is well explained in the table below.

Table 3.1. Comparing IP Precedence, DSCP and SNOM ToS Value [18]

IP Prec	IP Prec Bin	DSCP Class	DSCP Bin	DSCP Hex	DSCP Dec	ToS value(SNOM)
0	000	Best effort	000000	0x00	0	0
1	001	CS 1	001000	0x08	8	32
		AF11-Low	001010	0x0A	10	40
		AF12-Medium	001100	0x0C	12	48
		AF13-High	001110	0x0E	14	56
2	010	CS 2	010000	0x10	16	64
		AF21-Low	010010	0x12	18	72
		AF22-Medium	010100	0x14	20	80
		AF23-High	010110	0x16	22	88
3	011	CS 3	011000	0x18	24	96
		AF31-Low	011010	0x1A	26	104
		AF32-Medium	011100	0x1C	28	112
		AF33-High	011110	0x1E	30	120
4	100	CS 4	100000	0x20	32	128
		AF41-Low	100010	0x22	34	136
		AF42-Medium	100100	0x24	36	144
		AF43-High	100110	0x26	38	152
5	101	CS 5	101000	0x28	40	160
		EF	101110	0x2E	46	184

Presently, IP Precedence is still used by IP devices to mark packets. This is a transitional phase because most IP devices do not yet support DSCP. The ideal situation is that IP devices will use the DSCP value of Expedited Forwarding (EF) for RTP voice and VOIP Control traffic will have a DSCP value of Assured Forwarding 31 (AF31) in the future.

3.1.2. Queuing

Every packet that will be forwarded will have to be placed in a queue. Based on classification, queuing tools assign packets to several queues, for the required treatment in the network.

The voice, data, and video are placed in different queues on egress interfaces based on the classification. This will ensure that priority is given to the needed packets that need priority. This will be explained more with class-based queuing, priority queuing when QoS is implemented.

3.1.3. Network Provisioning

Network provisioning means making the network available for all the traffic that uses the network [15]. The network provisioning tools ensure that the needed bandwidth is accurately calculated for voice traffic, data traffic, video applications, and link management like routing protocols. It is worthy of note that the bandwidth used by the voice, data and other applications should not exceed 75% of the provisioned bandwidth. This will ensure that the remaining bandwidth of 25% is used for management purposes like routing protocols, VOIP bandwidth calculations and others.

4. Gathering Information

The right information is vital when a network needs to be configured for efficiency. A network engineer ought to know the required switches or routers that need configuration and which of these do not require configurations. Also, the engineer ought to know the ports to be configured and the interfaces to apply such configurations. In order for this to be done, network traffic analysis tools like Wireshark will be needed to gather the right information from the network.

In order for this work to proceed, there are some terms that need to be explained since it was noticed that different protocols are being used from the Wireshark data. What is a signal protocol? This will be answered by discussing Signal Protocol and some standard Signal protocols used today. They are:

a. VoIP Protocols

VoIP requires two types of protocols: a media protocol and a signalling protocol. The media protocol manages the transmission of voice packets over an IP networks. Examples are Real-time Transport Protocol (RTP), Real-time Transport Control Protocol (RTCP), and Secure Real-time Transport Protocol (SRTP). The signalling protocol manages call setup and call tear down. Examples of signalling protocols are H.323, SIP, MGCP, Skype etc. The signalling protocol uses Transmission Control Protocol (TCP) for its transmission while the Media protocol uses User Datagram Protocol (UDP) as its transmission.

b. Signal Protocol

A signal protocol is a type of protocol used to identify signalling encapsulation. It is used to identify the state of connections between telephones or VoIP [19]. VoIP has various standards that are being used for signalling. In the case of Sonera, they decided to use the SIP standard. In order for SIP to be appreciated, it will be better to have a good understanding of some other standard used as signal protocol such as H.323.

c. H.323

H.323 is an ITU recommended packet-based multimedia communication system that defines a distributed architecture for creating multimedia applications like VoIP. It is seen as an umbrella standard that covers other sub protocols like H.225 and H.245, connected to signalling and call setup. Its strength lies in its ability to serve in different roles like multimedia communication (voice, video and data conferencing) and inter working with PSTN applications [11]. It is the most widely used VoIP signalling and call-control protocol today.

It has four types of elements defined in this protocol: terminal, gateways, gatekeepers and Multipoint Control Units (MCU).

Every end-user device running the H.323 protocol is a terminal and gateways connect the H.323 network to other networks like PSTN. A gatekeepers provide services like addressing, authorization, and authentication for each terminal and gateway. It also manages the bandwidth utilization by all devices. The MCU allows multiparty audio or video conferences between several H.323 terminals.

d. SIP

Session Initiation Protocol (SIP) is an IETF defined protocol for VoIP, text and other multimedia sessions [16]. It is used for creating, modifying and terminating sessions between one or more participants. The major difference between SIP and other signalling protocols is that it is a text-based application-layer protocol and simpler than H.323. It does not require the use of Call agent when commencing and concluding between two clients. Since it works like HTTP in carrying out communication between clients, it became popular for companies that do not need complex VoIP setup. Since it is an application protocol, it can be carried out by UDP, TCP and STCP protocols. Its simplicity might have made companies like Sonera to choose it as its signalling protocol instead of H.323.

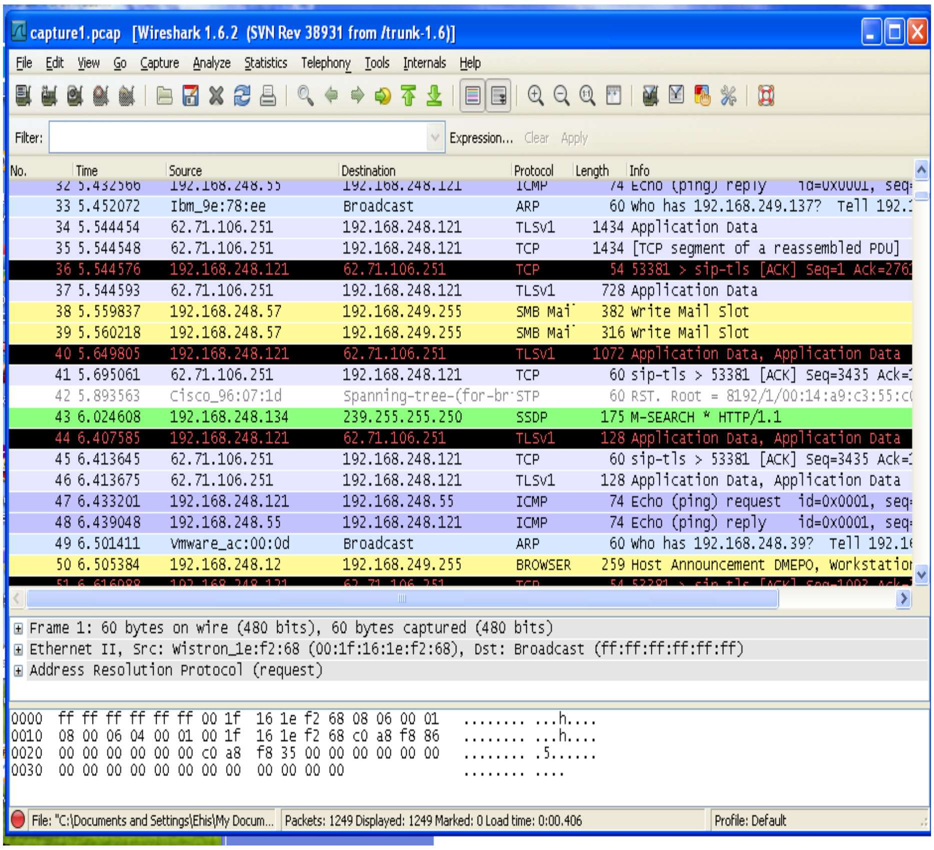
SIP has two kinds of ports: 5060 and 5061. Port 5060 is used for un-encrypted communication while port 5061 is used primarily for an encrypted communication over the Internet. The encrypted communication is carried over Transport Layer Security (TLS).

Transport Layer Security (TLS) is a cryptographic protocol that provides communication security over the Internet [20]. Its predecessor is Secure Socket Layer (SSL). It encrypts the segments of network connections above the Transport Layer using asymmetric cryptography, thus providing channel-oriented security. Therefore HTTPS is a combination of HTTP with SSL/TLS and this is what SIP uses to provide a secure connection.

Wireshark was used in this research to monitor the flow of traffic for some days in order to ascertain the ports used for communicating between the client computer or softphone and the server. In order for this to be done, a phone call was made from the VIP soft phone to different devices. The aim was to know if the port used by the VIP soft phone is static or a range of dynamic ports. This was carried out using several steps:

Step 1

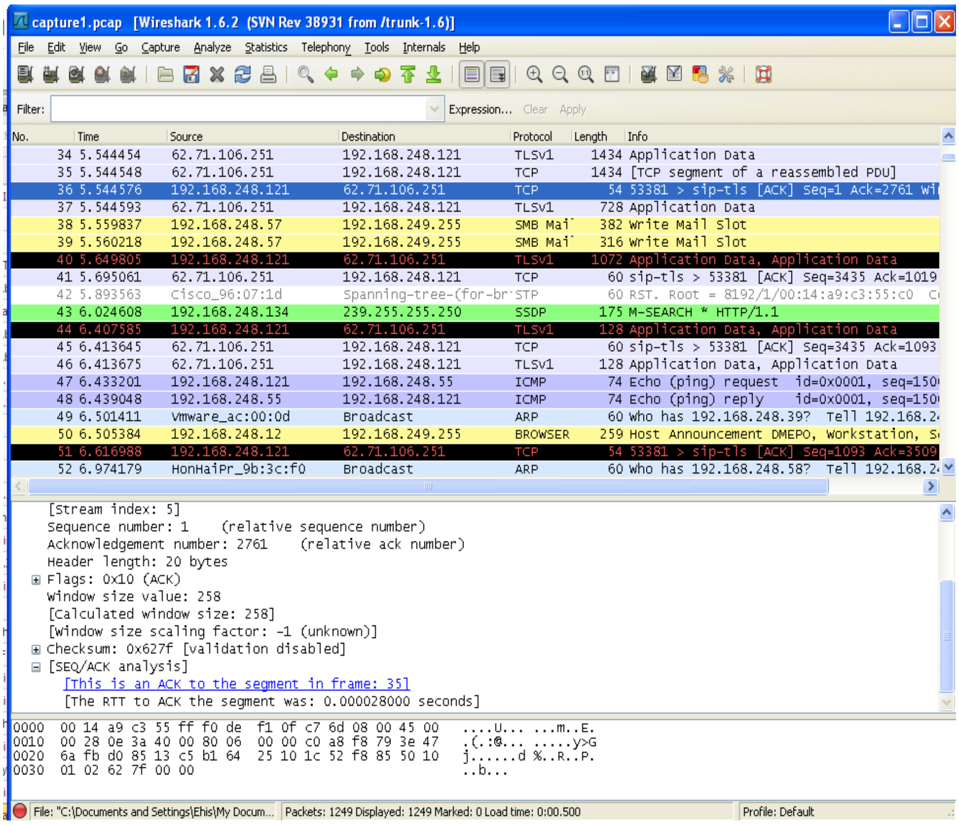
A phone call was made from the VIP soft phone on a laptop to a handset while monitoring the traffic with Wireshark. The captured traffic can be seen in the figure below.


capture1.pcap [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.  Time       Source             Destination          Protocol  Length Info
  32 5.432566   192.168.248.55     192.168.248.121      ICMP        74 Echo (ping) reply    id=0x0001, seq
  33 5.452072   Ibm_9e:78:ee       Broadcast            ARP         60 Who has 192.168.249.137?  Tell 192.1
  34 5.544454   62.71.106.251      192.168.248.121      TLSv1     1434 Application Data
  35 5.544548   62.71.106.251      192.168.248.121      TCP       1434 [TCP segment of a reassembled PDU]
  36 5.544576   192.168.248.121    62.71.106.251        TCP         54 53381 > sip-tls [ACK] Seq=1 Ack=276
  37 5.544593   62.71.106.251      192.168.248.121      TLSv1      728 Application Data
  38 5.559837   192.168.248.57     192.168.249.255      SMB Mai    382 Write Mail Slot
  39 5.560218   192.168.248.57     192.168.249.255      SMB Mai    316 Write Mail Slot
  40 5.649805   192.168.248.121    62.71.106.251        TLSv1     1072 Application Data, Application Data
  41 5.695061   62.71.106.251      192.168.248.121      TCP         60 sip-tls > 53381 [ACK] Seq=3435 Ack=
  42 5.893563   Cisco_96:07:1d     Spanning-tree-(for-br STP       60 RST. Root = 8192/1/00:14:a9:c3:55:c
  43 6.024608   192.168.248.134    239.255.255.250      SSDP       175 M-SEARCH * HTTP/1.1
  44 6.407585   192.168.248.121    62.71.106.251        TLSv1      128 Application Data, Application Data
  45 6.413645   62.71.106.251      192.168.248.121      TCP         60 sip-tls > 53381 [ACK] Seq=3435 Ack=
  46 6.413675   62.71.106.251      192.168.248.121      TLSv1      128 Application Data, Application Data
  47 6.433201   192.168.248.121    192.168.248.55       ICMP        74 Echo (ping) request  id=0x0001, seq
  48 6.439048   192.168.248.55     192.168.248.121      ICMP        74 Echo (ping) reply    id=0x0001, seq
  49 6.501411   Vmware_ac:00:0d    Broadcast            ARP         60 Who has 192.168.248.39?  Tell 192.1
  50 6.505384   192.168.248.12     192.168.249.255      BROWSER    259 Host Announcement DMEPO, Workstatio
  51 6.616088   192.168.248.121    62.71.106.251        TCP         54 53381 > sip-tls [ACK] Seq=1093 Ack=

⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: Wistron_1e:f2:68 (00:1f:16:1e:f2:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 1f  16 1e f2 68 08 06 00 01   ........ ...h....
0010  08 00 06 04 00 01 00 1f  16 1e f2 68 c0 a8 f8 86   ........ ...h....
0020  00 00 00 00 00 00 c0 a8  f8 35 00 00 00 00 00 00   ........ .5......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....

File: "C:\Documents and Settings\Ehis\My Docum...   Packets: 1249 Displayed: 1249 Marked: 0 Load time: 0:00.406   Profile: Default
```

Figure 4.1. Captured Phone call Traffic to Handset

From Figure 4.1, it can be seen that different protocols are being used for this single communication. The TCP, TLSv1 and UDP protocols are the protocols used for this particular communication from a VIP soft phone to the handset. In order for the communication to be really understood, a deeper analysis is required. This can be seen from the different figures below:


capture1.pcap [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.   Time      Source             Destination        Protocol Length Info
   34 5.544454  62.71.106.251      192.168.248.121    TLSv1     1434 Application Data
   35 5.544548  62.71.106.251      192.168.248.121    TCP       1434 [TCP segment of a reassembled PDU]
   36 5.544576  192.168.248.121    62.71.106.251      TCP         54 53381 > sip-tls [ACK] Seq=1 Ack=2761 Wi
   37 5.544593  62.71.106.251      192.168.248.121    TLSv1      728 Application Data
   38 5.559837  192.168.248.57     192.168.249.255    SMB Mai    382 Write Mail Slot
   39 5.560218  192.168.248.57     192.168.249.255    SMB Mai    316 Write Mail Slot
   40 5.649805  192.168.248.121    62.71.106.251      TLSv1     1072 Application Data, Application Data
   41 5.695061  62.71.106.251      192.168.248.121    TCP         60 sip-tls > 53381 [ACK] Seq=3435 Ack=1019
   42 5.893563  Cisco_96:07:1d     Spanning-tree-(for-br STP      60 RST. Root = 8192/1/00:14:a9:c3:55:c0  C
   43 6.024608  192.168.248.134    239.255.255.250    SSDP       175 M-SEARCH * HTTP/1.1
   44 6.407585  192.168.248.121    62.71.106.251      TLSv1      128 Application Data, Application Data
   45 6.413645  62.71.106.251      192.168.248.121    TCP         60 sip-tls > 53381 [ACK] Seq=3435 Ack=1093
   46 6.413675  62.71.106.251      192.168.248.121    TLSv1      128 Application Data, Application Data
   47 6.433201  192.168.248.121    192.168.248.55     ICMP        74 Echo (ping) request  id=0x0001, seq=150
   48 6.439048  192.168.248.55     192.168.248.121    ICMP        74 Echo (ping) reply    id=0x0001, seq=150
   49 6.501411  Vmware_ac:00:0d    Broadcast          ARP         60 Who has 192.168.248.39?  Tell 192.168.2
   50 6.505384  192.168.248.12     192.168.249.255    BROWSER    259 Host Announcement DMEPO, Workstation, S
   51 6.616988  192.168.248.121    62.71.106.251      TCP         54 53381 > sip-tls [ACK] Seq=1093 Ack=3509
   52 6.974179  HonHaiPr_9b:3c:f0  Broadcast          ARP         60 Who has 192.168.248.58?  Tell 192.168.2
```

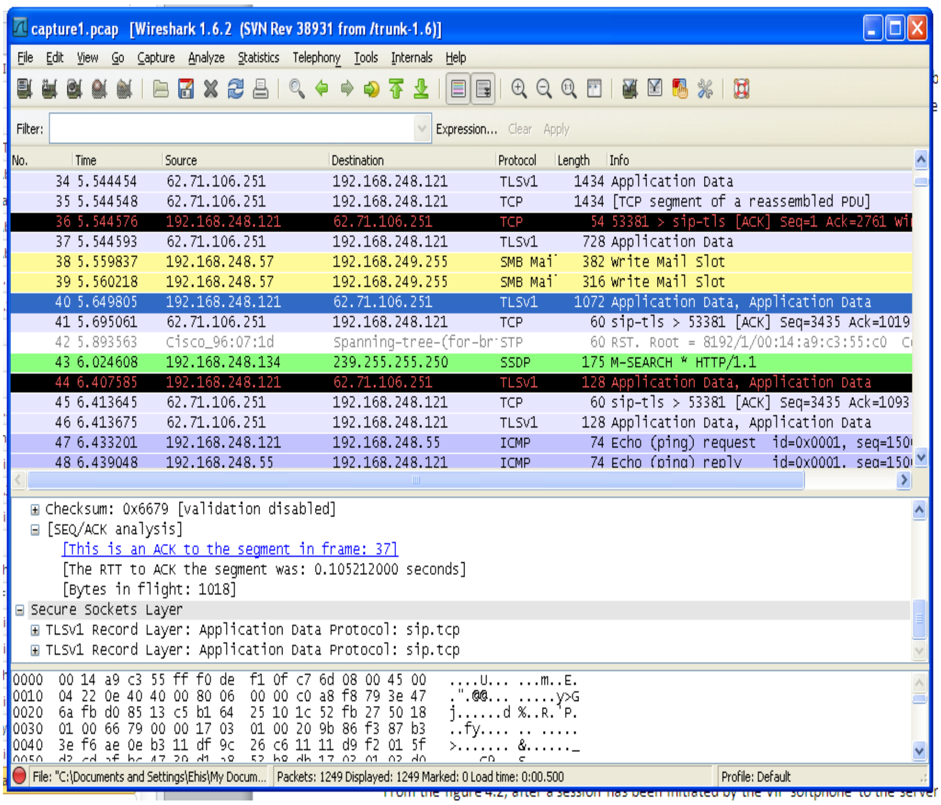
```
    [Stream index: 5]
    Sequence number: 1    (relative sequence number)
    Acknowledgement number: 2761    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x10 (ACK)
    Window size value: 258
    [Calculated window size: 258]
    [Window size scaling factor: -1 (unknown)]
  ⊞ Checksum: 0x627f [validation disabled]
  ⊟ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 35]
      [The RTT to ACK the segment was: 0.000028000 seconds]
```

```
0000  00 14 a9 c3 55 ff f0 de  f1 0f c7 6d 08 00 45 00   ....U... ...m..E.
0010  00 28 0e 3a 40 00 80 06  00 00 c0 a8 f8 79 3e 47   .(.:@... .....y>G
0020  6a fb d0 85 13 c5 b1 64  25 10 1c 52 f8 85 50 10   j......d %..R..P.
0030  01 02 62 7f 00 00                                  ..b...
```

File: "C:\Documents and Settings\Ehis\My Docum... Packets: 1249 Displayed: 1249 Marked: 0 Load time: 0:00.500 Profile: Default

Figure 4.2. TCP Communication

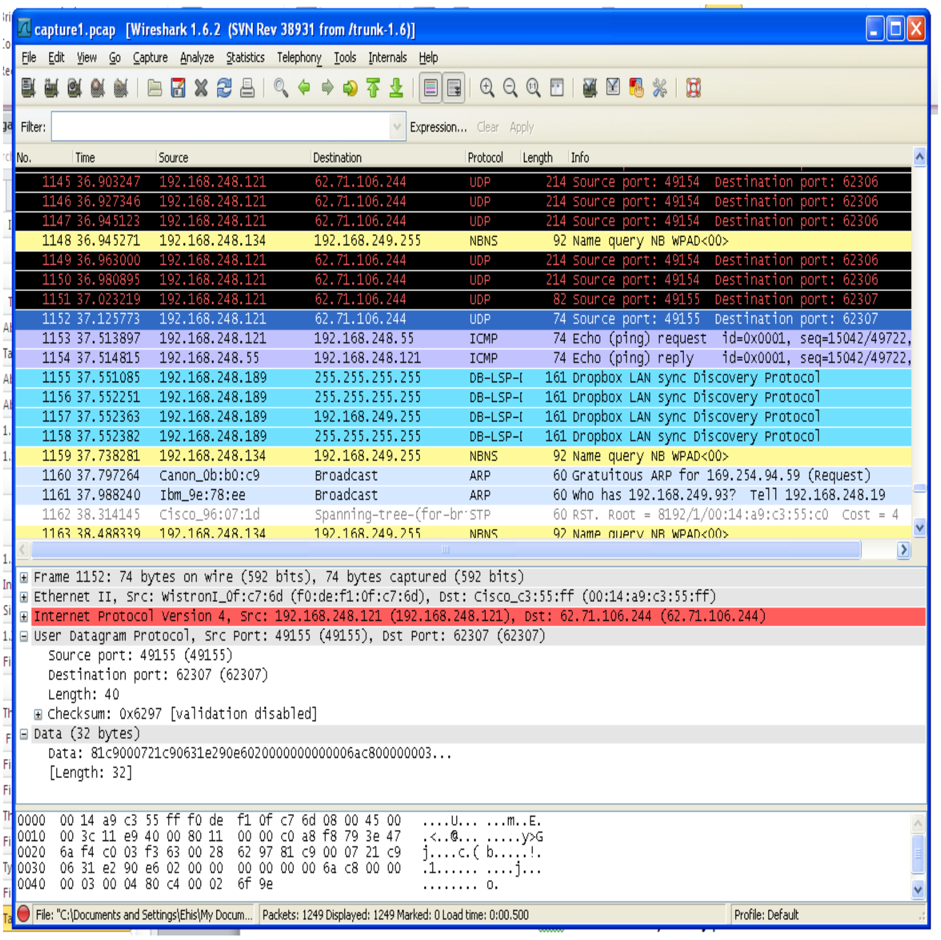
From Figure 4.2, analysing frame number 36 shows that after a session has been initiated by the VIP soft phone to the server (62.71.106.251), an acknowledgement is sent using TCP protocol from the client computer(192.168.248.121) to the server.


capture1.pcap [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.   Time      Source            Destination              Protocol Length Info
   34 5.544454  62.71.106.251     192.168.248.121          TLSv1    1434 Application Data
   35 5.544548  62.71.106.251     192.168.248.121          TCP      1434 [TCP segment of a reassembled PDU]
   36 5.544576  192.168.248.121   62.71.106.251            TCP        54 53381 > sip-tls [ACK] Seq=1 Ack=2761 Wi
   37 5.544593  62.71.106.251     192.168.248.121          TLSv1     728 Application Data
   38 5.559837  192.168.248.57    192.168.249.255          SMB Mai   382 Write Mail Slot
   39 5.560218  192.168.248.57    192.168.249.255          SMB Mai   316 Write Mail Slot
   40 5.649805  192.168.248.121   62.71.106.251            TLSv1    1072 Application Data, Application Data
   41 5.695061  62.71.106.251     192.168.248.121          TCP        60 sip-tls > 53381 [ACK] Seq=3435 Ack=1019
   42 5.893563  Cisco_96:07:1d    Spanning-tree-(for-br    STP        60 RST. Root = 8192/1/00:14:a9:c3:55:c0  C
   43 6.024608  192.168.248.134   239.255.255.250          SSDP      175 M-SEARCH * HTTP/1.1
   44 6.407585  192.168.248.121   62.71.106.251            TLSv1     128 Application Data, Application Data
   45 6.413645  62.71.106.251     192.168.248.121          TCP        60 sip-tls > 53381 [ACK] Seq=3435 Ack=1093
   46 6.413675  62.71.106.251     192.168.248.121          TLSv1     128 Application Data, Application Data
   47 6.433201  192.168.248.121   192.168.248.55           ICMP       74 Echo (ping) request  id=0x0001, seq=150
   48 6.439048  192.168.248.55    192.168.248.121          ICMP       74 Echo (ping) reply    id=0x0001, seq=150

  ⊞ Checksum: 0x6679 [validation disabled]
  ⊟ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 37]
      [The RTT to ACK the segment was: 0.105212000 seconds]
      [Bytes in flight: 1018]
⊟ Secure Sockets Layer
  ⊞ TLSv1 Record Layer: Application Data Protocol: sip.tcp
  ⊞ TLSv1 Record Layer: Application Data Protocol: sip.tcp

0000  00 14 a9 c3 55 ff f0 de  f1 0f c7 6d 08 00 45 00   ....U... ...m..E.
0010  04 22 0e 40 40 00 80 06  00 00 c0 a8 f8 79 3e 47   .".@@... .....y>G
0020  6a fb d0 85 13 c5 b1 64  25 10 1c 52 fb 27 50 18   j......d %..R.'P.
0030  01 00 66 79 00 00 17 03  01 00 20 9b 86 f3 87 b3   ..fy.... .. .....
0040  3e f6 ae 0e b3 11 df 9c  26 c6 11 11 d9 f2 01 5f   >....... &......_

File: "C:\Documents and Settings\Ehis\My Docum...   Packets: 1249 Displayed: 1249 Marked: 0 Load time: 0:00.500   Profile: Default
```

Figure 4.3. Analysing TLSv1 protocol

From Figure 4.3, when frame number 40 is also analysed it was noticed that the protocol used by the client to send an acknowledgment is the TLSv1 protocol. When there is communication between a TLS client and a TLS server, the hello request message is optional but in this case it was sent by the client to the server and the session had already been established. It can also be seen that the communication between the client and the server is a secured communication because Secure Socket Layer is being used for this communication since it is a TLSv1 protocol. When the session between the client VIP soft phone in the computer has been established to the other client VIP soft phone in the handset, the protocol was changed to a UDP. This is because VoIP communication cannot use a TCP protocol for communication. This can be seen in Figure 4.4 below:


capture1.pcap [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.  Time      Source           Destination            Protocol Length Info
1145 36.903247 192.168.248.121  62.71.106.244          UDP      214 Source port: 49154  Destination port: 62306
1146 36.927346 192.168.248.121  62.71.106.244          UDP      214 Source port: 49154  Destination port: 62306
1147 36.945123 192.168.248.121  62.71.106.244          UDP      214 Source port: 49154  Destination port: 62306
1148 36.945271 192.168.248.134  192.168.249.255        NBNS      92 Name query NB WPAD<00>
1149 36.963000 192.168.248.121  62.71.106.244          UDP      214 Source port: 49154  Destination port: 62306
1150 36.980895 192.168.248.121  62.71.106.244          UDP      214 Source port: 49154  Destination port: 62306
1151 37.023219 192.168.248.121  62.71.106.244          UDP       82 Source port: 49155  Destination port: 62307
1152 37.125773 192.168.248.121  62.71.106.244          UDP       74 Source port: 49155  Destination port: 62307
1153 37.513897 192.168.248.121  192.168.248.55         ICMP      74 Echo (ping) request  id=0x0001, seq=15042/49722,
1154 37.514815 192.168.248.55   192.168.248.121        ICMP      74 Echo (ping) reply    id=0x0001, seq=15042/49722,
1155 37.551085 192.168.248.189  255.255.255.255        DB-LSP-[ 161 Dropbox LAN sync Discovery Protocol
1156 37.552251 192.168.248.189  255.255.255.255        DB-LSP-[ 161 Dropbox LAN sync Discovery Protocol
1157 37.552363 192.168.248.189  192.168.249.255        DB-LSP-[ 161 Dropbox LAN sync Discovery Protocol
1158 37.552382 192.168.248.189  255.255.255.255        DB-LSP-[ 161 Dropbox LAN sync Discovery Protocol
1159 37.738281 192.168.248.134  192.168.249.255        NBNS      92 Name query NB WPAD<00>
1160 37.797264 Canon_0b:b0:c9   Broadcast              ARP       60 Gratuitous ARP for 169.254.94.59 (Request)
1161 37.988240 Ibm_9e:78:ee     Broadcast              ARP       60 Who has 192.168.249.93?  Tell 192.168.248.19
1162 38.314145 Cisco_96:07:1d   Spanning-tree-(for-br STP       60 RST. Root = 8192/1/00:14:a9:c3:55:c0  Cost = 4
1163 38.488339 192.168.248.134  192.168.249.255        NBNS      92 Name query NB WPAD<00>
```

```
⊞ Frame 1152: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: WistronI_0f:c7:6d (f0:de:f1:0f:c7:6d), Dst: Cisco_c3:55:ff (00:14:a9:c3:55:ff)
⊞ Internet Protocol Version 4, Src: 192.168.248.121 (192.168.248.121), Dst: 62.71.106.244 (62.71.106.244)
⊟ User Datagram Protocol, Src Port: 49155 (49155), Dst Port: 62307 (62307)
    Source port: 49155 (49155)
    Destination port: 62307 (62307)
    Length: 40
  ⊞ Checksum: 0x6297 [validation disabled]
⊟ Data (32 bytes)
    Data: 81c9000721c90631e290e6020000000000006ac800000003...
    [Length: 32]
```

```
0000  00 14 a9 c3 55 ff f0 de  f1 0f c7 6d 08 00 45 00   ....U... ...m..E.
0010  00 3c 11 e9 40 00 80 11  00 00 c0 a8 f8 79 3e 47   .<..@... .....y>G
0020  6a f4 c0 03 f3 63 00 28  62 97 81 c9 00 07 21 c9   j....c.( b.....!.
0030  06 31 e2 90 e6 02 00 00  00 00 00 00 6a c8 00 00   .1...... ....j...
0040  00 03 00 04 80 c4 00 02  6f 9e                     ........ o.
```

File: "C:\Documents and Settings\Ehis\My Docum... Packets: 1249 Displayed: 1249 Marked: 0 Load time: 0:00.500 Profile: Default

Figure 4.4. Using UDP for VoIP communication

Usually, SIP communication can both use UDP or TCP as the transport protocol for transfering data. Initially, UDP was the only protocol allowed in RFC2543 but in RFC3261, both TCP and UDP were given the permission to be used as the data transfer transport protocol. Today, UDP is still the most used in most SIP communications.

In this communication, as can be seen in the figure above, the UDP protocol was used until the call was ended by the users. The last UDP protocol used can be seen in frame 1110 and after the call was ended, a TCP protocol was used to eventually bring the session to an end.

After analysing the Wireshark captured results, it became obvious that a range of protocols and ports were used in the communication. The table below shows the ports used in the communication from the Wireshark data.

Table 4.1. Call Picked by VIP softphone on handset

Source IP address	Source Port			Dest. Port	Dest IP address
192.168.248.121	53381	→		5061	67.71.106.251
	53381	←		5061	
	53397	→		443	67.71.106.250
	53397	←		443	
	49154	→		62306	67.71.106.244
	53381	←		5061	62.71.106.251
	49154	←		62306	62.71.106.244
Ports Used				Ports Used	
53381				5061	
53397				443	
49154				62306	

Step 2

With the results gathered from the first call made from the laptop, it cannot be ascertained if these ports are static ports, or if the VIP soft phone uses a range of dynamic ports. Another call was made but this time it was picked by the soft phone on a laptop. After analysing the data captured with Wireshark, it was noticed that the ports changed slightly from the ports gathered from the previous result. The table below shows that fewer ports were used in this communication compared with the previous communication.

Table 4.2. Call picked by VIP softphone on Laptop

Source IP address	Source Port			Dest. Port	Dest IP address
192.168.248.121	49269	→		5061	67.71.106.250
	49269	←		5061	
	49154	→		56674	67.71.106.242
	49154	←		56674	
Ports Used				Ports Used	
49269				5061	
49154				56674	

From the table above, it was established that fewer ports are used for a SIP communication to a soft phone in a laptop compared with more ports that are used when the communication ends on a soft phone installed on a handset as can be seen in Table 4.1.

This process of making calls to the handset or laptop where the VIP soft phone is installed was repeated several times to know if the same ports used will be the same as the one earlier gathered or not. After studying different data captured by Wireshark, it became obvious that different ports are used whenever a call is made between users.

4.1. Deductions from analysed data

So from the data gathered using Wireshark, it became obvious that the range of RTP/UDP dynamic ports from 49152 – 65535 is being used by VIP soft phone to communicate with the server. These range ports are used for media requests sent from the client to the server. They are also used for inbound and outbound media transfer through the firewall.

From the data analysed, SIP uses signal port 5061 for communication and authentication between the client and the server. It is also used for outbound communication from the client to the server through the firewall.

In addition, it was observed that HTTPS/TCP port 443 is used by the client to send SIP traffic to the server. Most times, this port is also used by client connecting to the server for SIP communication outside an intranet.

Lastly, all communication for transferring important data uses TLSv1. This makes it difficult for hackers to hack the information in the server or intercept the communication between several users.

5. QoS Implementation

QoS implementation, as was earlier mentioned, can be a simple or complex task depending on several factors like the QoS features offered by the networking devices, the traffic types and pattern in the network and level of control that need to be exercised over incoming and outgoing traffic. The network engineer cannot even be able to exercise so much control over the network traffic beyond the QoS features in the networking devices.

5.1. QoS Model used

There are diverse models for implementing QoS on a network. As stated earlier, though IntServ, Best effort and DiffServ can be used to implement QoS, the best and most scalable model for implementing QoS in a network is the DiffServ model.

The DiffServ model allows network traffic to be broken down into small flows for appropriate marking. This small flow is called a class. Thus, the network recognises traffic as a class instead of the network receiving specific QoS request from an application. The devices along the path of the flow are able to recognise the flow because these flows are marked. So the marked flow is given appropriate treatment by the various devices on the network.

In the previous chapter, the DiffServ field was shown with some diagrams to clearly explain what it really looks like in IPv4 or IPv6. When the packet has been properly marked and identified by the router or switch, it is given special treatment called Per Hop Behaviour (PHB) by these devices. PHB identifies how the packets are treated at each hop. There are three standardized PHB currently in use:

a. Default PHB: This uses best-effort forwarding to forward packets

b. Expedited Forwarding (EF): It guarantees that each DiffServ node gives low-delay, low-jitter and low-loss to any packet marked with EF. It is used majorly for Real-time Transport Protocol (RTP) applications, like voice and video.

c. Assured Forwarding (AF): It gives lower level functions compared with EF. It is used mostly for mission-critical applications or any application that are not too sensitive to delay but want assurance that the packets will be delivered by the network.

There are several tools used in implementing QoS. These are some tools used in QoS implementation:

1. Congestion Management

Queuing is meant to accommodate temporary congestion on an interface of a network device by storing the excess packets until there is enough bandwidth to forward the packets. Sometimes some packets are dropped when the queue depth is full. Congestion management allows the administrator to control congestion by determining how and when the queue depth is full. There are several ways this can be done. These are some ways congestion management can be implemented:

a. Priority Queuing (PQ): This allows the administrator to give priority to certain traffic while allowing other to be dropped when the queue depths are full.

b. Custom Queuing (CQ): This allows the administrator to reserve queue space in the router or switch buffer for all traffic types.

c. Weighted Fair Queuing (WFQ): This allows the sharing of bandwidth with prioritization given to some traffic.

d. Class-based Weighted Fair Queuing (CBWFQ): This extends the functionality of WFQ to provide support for user-defined classed.

e. Low Latency Queuing (LLQ): This is a combination of CBWFQ and PQ. It is able to give traffic that requires low-delay the required bandwidth it needs while also giving data the needed bandwidth. It solves the starvation problem associated with PQ.

2. Traffic shaping and traffic Policing

Traffic shaping and policing are mechanisms used to control the rate of traffic. The main difference between them depends on the terms of implementation. While traffic policing drops excess traffic or remarks the traffic in order to control traffic flow within a specific rate limit without introducing any delay to traffic, traffic shaping retains excess traffic in a queue and then schedules such traffic for later transmission over an increment of time.

Since the traffic in this particular network was divided into two classes: the voice and others by the network administrator, it is important that LLQ and traffic policing is used to implement the various configurations in the different switches. How then is QoS implemented in a network? It starts with preparation.

5.1.1. Preparing to Implement the QoS model

a. Identifying types of traffic and their requirement.

Using Wireshark, the traffic required can be identified. In this scenario, Wireshark was used to confirm the range of ports that are to be configured. In addition, it is necessary to know the business importance of all traffic in a network.

b. Dividing traffics into classes.

The identified traffic is divided into two classes: Voice and Others. This is specified by the network administrator for the network. In this scenario, the traffic was divided into two classes: Voice and Others. The Voice class is given low latency while Others will be configured with guaranteed delivery.

c. Defining QoS policies for each class

Defining the QoS policy involves one or more of the following activities: setting a minimum bandwidth guarantee, setting a maximum bandwidth limit, assigning a priority to each class and using QoS technology to manage congestion.

5.1.2 Implementing the chosen QoS model

Since it has been established that the QoS model to be used is DiffServ, it is necessary for the network engineer to decide how this model will be implemented. This model can be implemented using Cisco AutoQoS or the Modular QoS CLI (MQC).

Cisco AutoQoS is a Cisco proprietary of implementing QoS on Cisco devices. It can only be used on Cisco router’s or switches but it is not supported by all switches. AutoQoS makes assumptions about the network design and generates a set of configurations suitable for the devices in the network. It is very easy to deploy and generates an efficient configuration suitable for the device and network. The major disadvantage of using AutoQoS in a heterogeneous network is that it recognises only Cisco devices.

Modular QoS CLI (MQC) is the most efficient way to implement QoS on any networking device like Cisco, HP etc. in a heterogeneous network. It is a common set of configuration commands used to configure most QoS features in a router or switch. The modularity is excellent and network administrators have complete control over the configuration to be used in the router or switch.

Since QoS is being implemented in a heterogeneous LAN, it will suffice if some of the steps are left to default and Modular QoS CLI is used to implement DiffServ in the network. The fact is that AutoQoS will not be able to recognise the range of ports to be configured and it will not be able to recognise the VIP soft phone or SNOM hard phone in the network since it recognises only Cisco devices. These are the steps used when using MQC to configure a network:

1. **Class Map**: Defining the class of traffic needed. Each class is defined using a **class-map** command.
2. **Policy Map**: The QoS policies for the classes are defined using policy-map command. This states what will be done to the traffic defined in the class map.
3. **Service Policy**: This attaches the configured policy to an interface using the **service-policy** command. Without attaching the policy, the class map and policy map configured will not be used by the device.

5.2. Lab test

Usually, in an enterprise network, it is wrong to test configurations in a real-time environment. It is important for the configurations to be fine-tuned in a lab environment before it is implemented in the network in order not to disrupt the network traffic. The MQC was tried initially in a lab environment before it was implemented gradually in the network. The lab topology can be seen below.

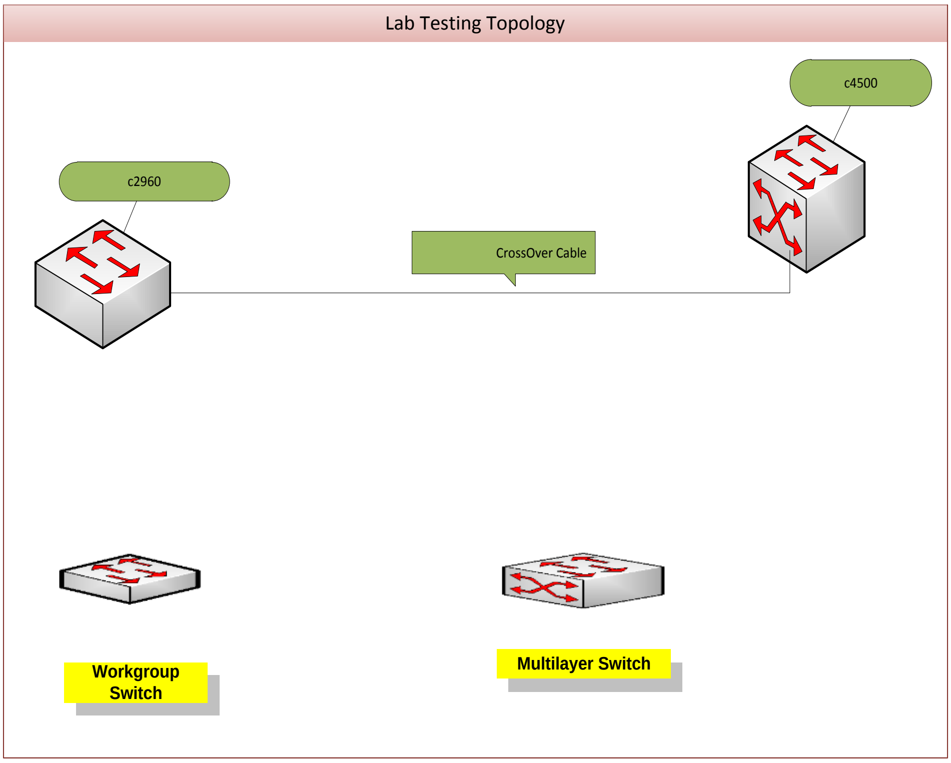


Figure 5.1. Lab Logical Topology

The lab network is made up of two switches, Cisco C2960 and a C4503 switch connected with a crossover cable. The configuration used was designed with an access-list that has a ping command attached. Part of the configuration can be seen below. This configuration shows just the access-list.

Voice RTP and Voice Control access list

```
ip access-list extended VOIP-RTP
permit udp any any range 49152 65535
permit ip any any precedence 5
permit ip any any dscp ef
permit ip any any dscp cs5
permit ip any any echo
permit ip any any echo-reply
ip access-list extended VOIP-CONTROL
```

```
permit tcp any any eq 5061

permit tcp any any eq 443
```

Echo and echo-reply was added to the access-list in order to determine if ping is given expedited forwarding or not. It was noticed from the results gathered from the lab work that there was a little difference in the ping result when QoS was implemented on one of the switches. This will be explained more clearly in the next chapter when QoS has been implemented in the network.

5.3. Configuration used

It will also be good to have an overview of what the logical network looks like in order to have a grasp of the network and the way packets flow from the different offices through the LAN. This is also necessary since QoS implementation will be complex or simple depending on the traffic patterns and types in the network. These switches and router make up the network topology. This can be seen in Figure 5.2 below.

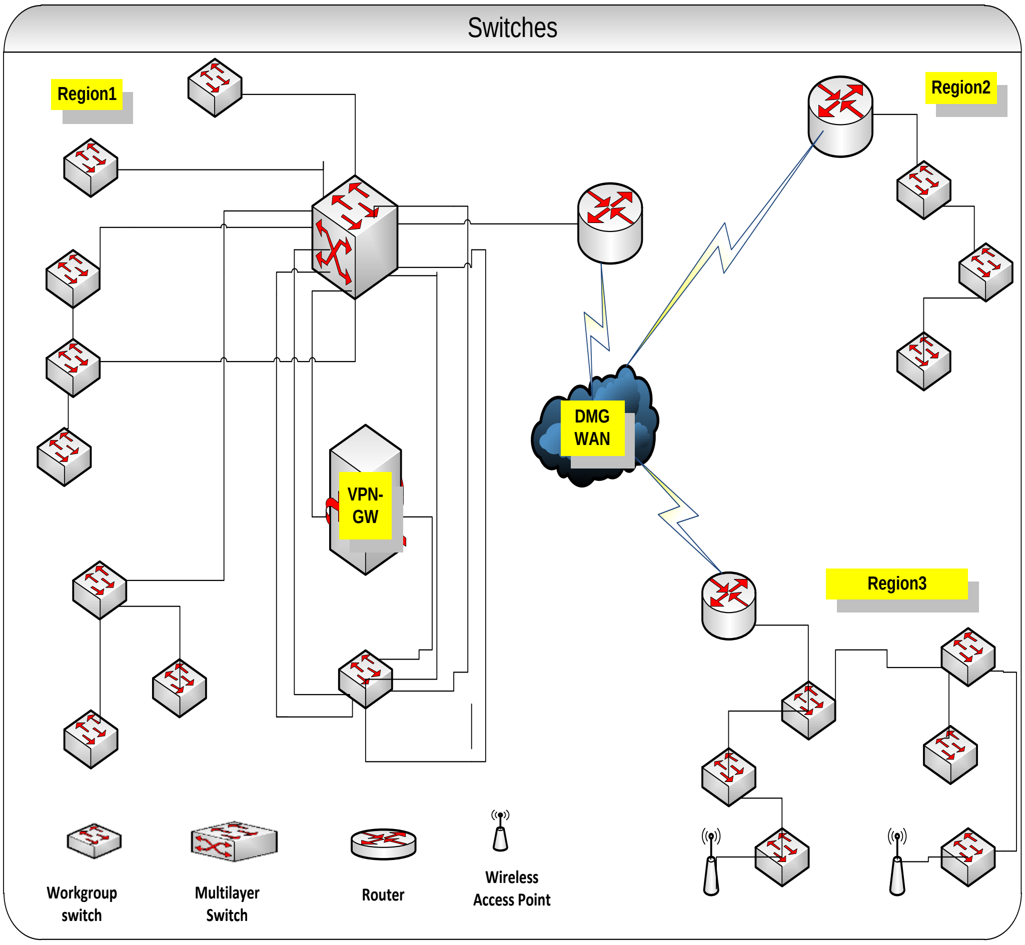


Figure 5.2. Logical LAN Network Topology

It is necessary to understand that there are three regions in this LAN topology. Region 1, region 2 and region 3. The LAN in region 1 is extended to region 2 and 3 using an IP/MPLS-based VPN from a service provider.

The network diagram above is made up of different devices with different IOS models and software versions and knowing this is important because implementing QoS in a network will be a simple task if the internetworking devices offer the right QoS features and it will be difficult if it does not.

Table 5.1. Devices in the network configured

Equipment	IOS Model	IOS Software Version
Cisco Catalyst 2950 switch	WS-C2950G-24-EI WS-C2950G-48-EI	12.1(22)EA4a 12.1(22)EA6
Cisco Catalyst 2960 switch	WS-C2960G-24TC-L WS-C2960G-48TC-L WS-C2960G-8TC-L	12.2(25)SEE2 12.2(35)SE5 12.2(44)SE6
Cisco Catalyst 3524 switch	WS-C3524XL	12.0(5)WC17
Cisco Catalyst 4500 series	Sup II+TS (WS-X4013+TS)	12.2(53)SG2
SNOM Hard phone	SNOM 320	
VIP Softphone		3.4

The switch in region 1 is made up of C2950, C2960, C3524 and C4500 while those in region 2 are made up of C2960 only. Region 3 is made up of both C2960 and C2950.

Since there are different Cisco switches in the network, it is paramount that different configurations need to be designed and loaded on these different switches. There are some cases where a particular configuration will fit into different switches. The Cisco IOS has different limitations on different Cisco platforms. Each configuration starts with a class map, a policy map, access list and then attaching the policy to an interface either a physical interface or a port-channel. Some sample configurations that were suitable for C2950 and C2960 can be seen in the Appendix.

The main reason different configuration will be needed is because every switch has different IOS models and these models are optimised for some specific purposes. Moreover, since technology is evolving the manufacturer of such device cannot integrate all features into one switch model since that will be difficult to do.

The switches were configured in this network but the routers were not configured since they are the property of the service provider installed in the company network. The routers have already been configured by the service provider since they are the provider’s edge (PE) device. It is worthy of note that this topology shows an MPLS Layer-2 VPNs which is a Layer-2 switched solution. This kind of approach allows for a separation of the customer network from the provider’s network, thus there is no route exchange between the customer devices and the provider’s devices. All that the provider devices do is to carry Layer-2 frames from one area like region 1 to another like region 2 in a manner transparent to the customer edge devices. So QoS should have been implemented in the PE router by the service provider.

5.4. Difficulties caused by Cisco IOS

Something of note is the various difficulties experienced as a result of the Cisco IOS limitation. Even with an upgraded software version, there are still so many restrictions in some of the switches used in this network.

In C2950 switches, there is a number of restrictions [2].

- All ACE in an ACL must have the same user-defined mask. Additionally, on a given interface, only one type of user-defined mask is allowed.
- Only four user-defined masks can be defined for the entire system. It can be used by either security or quality of service (QoS) but cannot be shared by QoS and Security. This is the most inconvenient restriction experienced when implementing the QoS configurations on these switches.

Table 5.2. Summary of ACL Restrictions

Restriction	**Number Permitted**
Number of User defined masks allowed in an ACL	1
Number of ACLs allowed on an interface	1
Total number of user-defined masks for security and QoS allowed on a switch	4

In C2960 switches and below there is a limitation on the use of show policy command [3].

Table 5.3. Syntax Description

policy *policy-map-name*	(Optional) Display the specified policy-map name
class *class-map-name*	(Optional) Display QoS policy actions for a individual class.
| **begin**	(Optional) Display begins with the line that matches the expression.
| **exclude**	(Optional) Display excludes lines that match the expression.
| **include**	(Optional) Display includes lines that match the specified expression.
expression	Expression in the output to use as a reference point.

Note: Though visible in the command-line help string, the **control-plane** and **interface** keywords are not supported, and the statistics shown in the display should be ignored.

One problem experienced in a C4506 switch is that the **bandwidth** command was able to be used when writing the configuration but generated several errors when the configuration was attached to an interface.

Why will a command be allowed that is not supported? This is a question only Cisco can answer. It might be purely for business purposes because even the updates released did not address these major limitations.

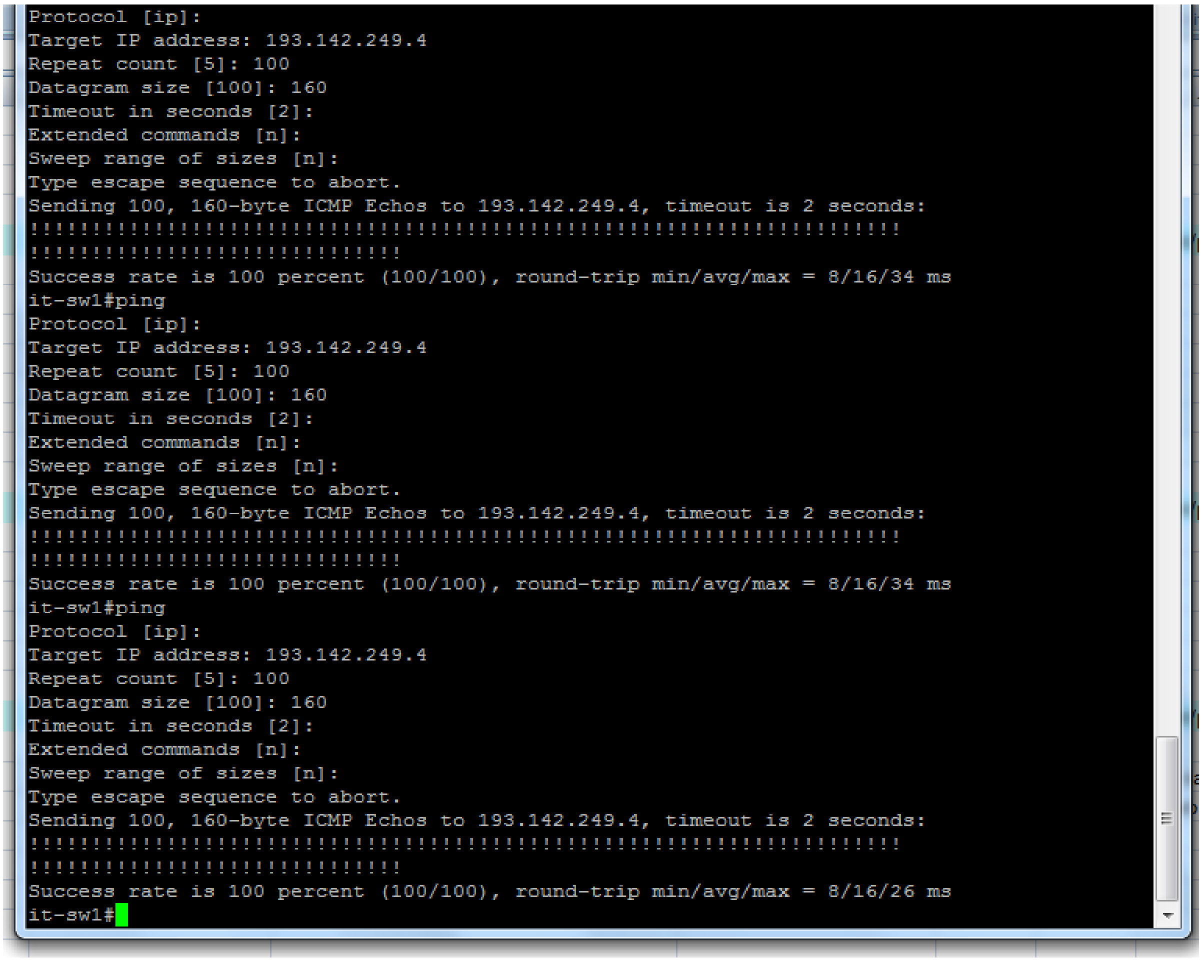
6. Results and Conclusion

6.1. QoS implementation

It is necessary to carry out a QoS baseline test in order to compare the results gathered before implementing QoS and after the implementation.

6.1.1. QoS Baseline

Before applying any QoS configurations, an extended ping from one of the switches (192.168.248.51) is sent to all the switches in the network in the three regions that make up the LAN 3 times for each switch. Below is a sample picture of the ping to one switch in region 2 office.



```
Protocol [ip]:
Target IP address: 193.142.249.4
Repeat count [5]: 100
Datagram size [100]: 160
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 160-byte ICMP Echos to 193.142.249.4, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 8/16/34 ms
it-sw1#ping
Protocol [ip]:
Target IP address: 193.142.249.4
Repeat count [5]: 100
Datagram size [100]: 160
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 160-byte ICMP Echos to 193.142.249.4, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 8/16/34 ms
it-sw1#ping
Protocol [ip]:
Target IP address: 193.142.249.4
Repeat count [5]: 100
Datagram size [100]: 160
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 160-byte ICMP Echos to 193.142.249.4, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 8/16/26 ms
it-sw1#
```

Figure 6.1. Region 2 switch

6.1.2 QoS Baseline Results

After configuring QoS, the extended ping test was repeated on all the switches again by adding echo and echo-reply to the access-list that permits Expedited Forwarding. Then a comparison was made between the ping before the QoS was configured on the network and after it was configured. The table below sums up the results. The results from four switches (two from the switches in Region 1 and two from those in Region 2) are used in this project only to explain the effects of QoS configuration.

Table 6.1. 192.168.248.51 to 192.168.248.235 QoS Baseline Ping results in Region 1

Packet Size	**WithOut QoS Policy**	**With QoS Policy**
160 bytes	**min/avg/max (ms)**	**min/avg/max (ms)**
Extended ping 1	1/3/9	1/2/9
Extended ping 2	1/3/25	1/3/17
Extended ping 3	1/2/9	1/3/17
	Success rate %	**Success rate %**
Extended ping 1	100%	100%
Extended ping 2	100%	100%
Extended ping 3	100%	100%

Table 6.2. 192.168.248.51 to 192.168.248.44 QoS Baseline Ping results in Region 1

Packet Size	**WithOut QoS Policy**	**With QoS Policy**
160 bytes	**min/avg/max (ms)**	**min/avg/max (ms)**
Extended ping 1	1/13/1007	1/4/34
Extended ping 2	1/3/25	1/3/17
Extended ping 3	1/3/16	1/3/16
	Success rate %	**Success rate %**
Extended ping 1	100%	100%
Extended ping 2	100%	100%
Extended ping 3	100%	100%

The results in Table 6.1 and 6.2 do not clearly show any proof that QoS will be beneficial when implemented in a LAN, since there is little difference between the min/avg/max time as this LAN does not extend over an MPLS.

Region 1 and Region 2 are on the same LAN but this LAN extends over an IP/MPLS as can be seen in the network topology in Figure 4.2. Since the LAN extends over an IP/MPLS, the extended ping before QoS is implemented and after the implementation, the effect of QoS implementation is clearly shown.

Table 6.3. 192.168.248.51 to 193.142.250.3 QoS Baseline Ping results from Region 1 to Region 2

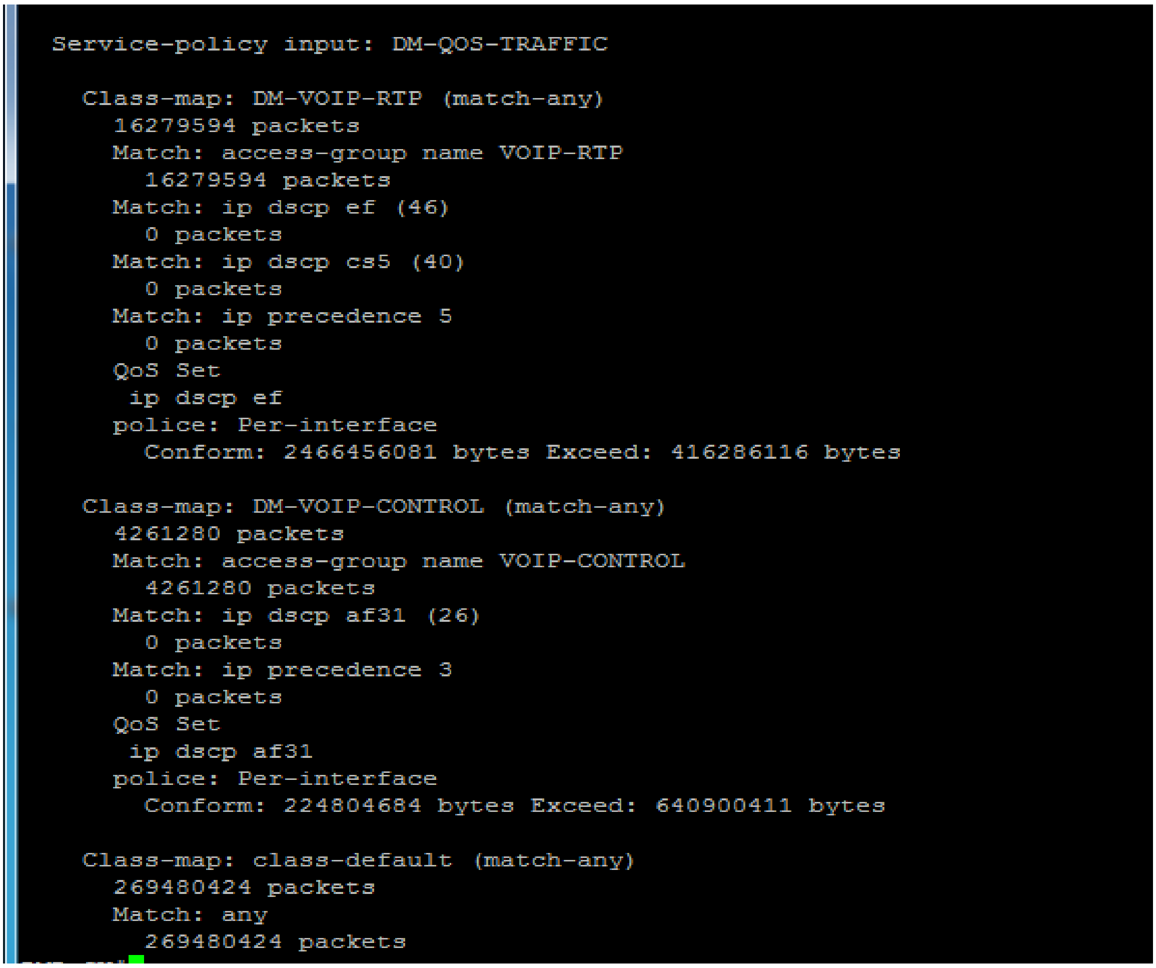
Packet Size	WithOut QoS Policy	With QoS Policy
160 bytes	**min/avg/max (ms)**	**min/avg/max (ms)**
Extended ping 1	8/16/26	1/8/17
Extended ping 2	8/16/26	1/8/17
Extended ping 3	8/16/33	1/8/25
	Success rate %	**Success rate %**
Extended ping 1	100%	100%
Extended ping 2	100%	100%
Extended ping 3	100%	100%

Table 6.4. 192.168.248.51 to 193.142.250.8 QoS Baseline Ping results for Region 1 to Region 2

Packet Size	WithOut QoS Policy	With QoS Policy
160 bytes	**min/avg/max (ms)**	**min/avg/max (ms)**
Extended ping 1	8/15/25	1/7/25
Extended ping 2	8/15/25	1/7/17
Extended ping 3	8/15/42	1/8/17
	Success rate %	**Success rate %**
Extended ping 1	100%	100%
Extended ping 2	100%	100%
Extended ping 3	100%	100%

While the results for the Pings to the switches in Region 1 may not clearly show the effect of the QoS configuration on a LAN, the result of the ping to the switches in the region 2 shows that because the Ping was moved to the expedited forwarding class with the VOIP traffic, the minimum average and the maximum response time were shorter before the QoS setting was implemented.

So it can be clearly seen that the VoIP traffic in this network is being given expedited forwarding therefore QoS configuration is beneficial to this network traffic from region 1 to region 2. Below is an output from one of the switches to show the packets that matched the different access lists and are being given expedited forwarding to further buttress the fact that the voice packets are given expedited forwarding. It can be seen from the output below that the access-list extended VOIP-RTP and VOIP-CONTROL has some packets that match it. Moreover, from the output below it can be seen that the policy map is being matched by the VoIP packets.



```
Service-policy input: DM-QOS-TRAFFIC

  Class-map: DM-VOIP-RTP (match-any)
    16279594 packets
    Match: access-group name VOIP-RTP
      16279594 packets
    Match: ip dscp ef (46)
      0 packets
    Match: ip dscp cs5 (40)
      0 packets
    Match: ip precedence 5
      0 packets
    QoS Set
     ip dscp ef
    police: Per-interface
      Conform: 2466456081 bytes Exceed: 416286116 bytes

  Class-map: DM-VOIP-CONTROL (match-any)
    4261280 packets
    Match: access-group name VOIP-CONTROL
      4261280 packets
    Match: ip dscp af31 (26)
      0 packets
    Match: ip precedence 3
      0 packets
    QoS Set
     ip dscp af31
    police: Per-interface
      Conform: 224804684 bytes Exceed: 640900411 bytes

  Class-map: class-default (match-any)
    269480424 packets
    Match: any
      269480424 packets
```

Figure 6.2. Policy for an interface

From the previous tables and the output captured in Figure 6.4, it has been established that the required packet that needs priority is being given priority in the network. Since this is the case then when QoS is configured in a LAN, it is of utmost importance to VoIP traffic or any traffic that needs expedited forwarding. All that is required in such a scenario is for a set bandwidth to be allocated to the VoIP traffic or other important traffic and for the other traffic that do not require priority, should be given a fair share of the bandwidth.

Additionally, networking devices usually drop packets that exceed the configured bandwidths so for voice packets to always be sent, it is required that after the initial bandwidth is given to the VoIP class, the network should be monitored for some time in order for the network engineer to ascertain if the bandwidth will have to be increased or not and if the configurations in such devices will be modified to prevent the dropping of VoIP packets. This will help the network to deliver all traffic regardless of it being voice traffic or not. All traffic is given the required attention by the networking devices and delivered to the required destination.

6.2. Conclusion

Since implementing QoS on a LAN might have minimal effects on the network when such a LAN is within the same region, it is obvious that if that LAN extends over a WAN, then implementing QoS in a network will be of paramount importance since the network can give preferential treatment to set traffic like VoIP. The QoS configuration on such a converged network brings low latency, low jitter and high availability to VoIP traffic on such a network. Moreover, it can be seen clearly that in a network with diverse switches or routers, different QoS configurations have to be designed and implemented on such a network. Furthermore, DiffServ model of QoS is the most scalable and better model for implementing QoS on a network since it allows the use of Modular QoS CLI to be used on different networking devices.

REFERENCES

[1.] Alvarez, S., & Cisco Systems, I. (2006). *QoS for IP*. Indianapolis: Cisco Press.

[2.] Cisco Systems, Inc. (2001). Cisco IP telephony QoS design guide. (pp. 92-106). San Jose, CA: Cisco Systems, Inc.

[3.] Cisco Systems, Inc. (2005). Configuring QoS. *Catalyst 2960 series switch cisco IOS software configuration guide* (12.2(25)FX ed., pp. 487-573). San Jose, CA: Cisco Systems, Inc.

[4.] Cisco Systems, Inc. (2005). Configuring quality of service. *Catalyst 4500 series switch cisco IOS software configuration guide* (12.2(25)SG ed., pp. 406-458). San Jose, California: Cisco Systems, Inc.

[5.] Cisco Systems, Inc. (2005). *DiffServ -- the scalable end-to-end QoS model* No. 19). San Jose,CA: Cisco Systems, Inc.

[6.] Cisco Systems, Inc. (2006). Configuring QoS. *Catalyst 3750 switch software configuration guide* (12.2(25)SEE ed., pp. 703-781). San Jose, CA: Cisco Systems, Inc.

[7.] Cisco Systems, Inc. (2008). Configuring QoS. *Catalyst 2950 and catalyst 2955 switch software configuration guide* (12.1(22)EA11 ed., pp. 529-567). San Jose,CA: Cisco Systems, Inc.

[8.] Cisco Systems, Inc. (2010). *Legacy QoS CLI commands deprecation.* Retrieved August 10, 2011, from http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6558/product_bulletin_c25-580832.html

[9.] Flannagan, M. E., Durand, B., Sommerville, J., Buchmann, M., & Fuller, R. (2001). *Administering cisco QoS in IP networks*. Rockland, MA: Syngress Publishing, Inc.

[10.] Gallon, C. (2003). *Quality of service for next generation voice over IP networks* No. 17). California: Multiservice Switching Forum.

[11.] Gonia, K. (2004). *Latency and QoS for voice over IP* No. 21) SANs Institute.

[12.] JHT2. (2011). *H.323.* Retrieved July 27, 2011, from http://www.voip-info.org/wiki/view/H.323

[13.] Park, P. (2009). *Voice over IP security*. Indianapolis, Ind.: Cisco Press.

[14.] Persky, D. (2007). *VoIP security vulnerabilities* No. 127)SANS Institute.

[15.] Provisioning*.* (2000). Retrieved July 19, 2011, from http://searchsoa.techtarget.com/definition/provisioning

[16.] Session initiation protocol*.* (2010). Retrieved July 20, 2011, from http://en.wikipedia.org/wiki/Session_Initiation_Protocol

[17.] Snom Technology, A. (2005). *Snom 320 user manual* (1.00th ed.). Berlin, Germany: [17.] Snom Technology, A.

[18.] Snom Technology, A. (2009). *FAQ/What does the TOS values 160 mean.* Retrieved July 27, 2011, from http://wiki.snom.com/FAQ/What_does_the_TOS_value_160_mean

[19.] Snom Technology, A. (2009). *Web Interface/V8/Advanced.* Retrieved July 14, 2011, from http://wiki.snom.com/Web_Interface/V8/Advanced

[20.] *Transport layer protocol.* (2010). Retrieved July 20, 2011, from http://en.wikipedia.org/wiki/Transport_Layer_Security

[21.] Tucker, G. S. (2004). *Voice over internet protocol (VoIP) and security* No. 16)SANS Institute.

[22.] Wallace, K., CCNP. (2005). *Voice over IP first-step*. Indianapolis, Ind.: Cisco.

[23.] Wallace, K., CCNP. (2009). *Authorized self-study guide: Cisco voice over IP (CVOICE)* (3rd ed.). Indianapolis, IN: Cisco Press.

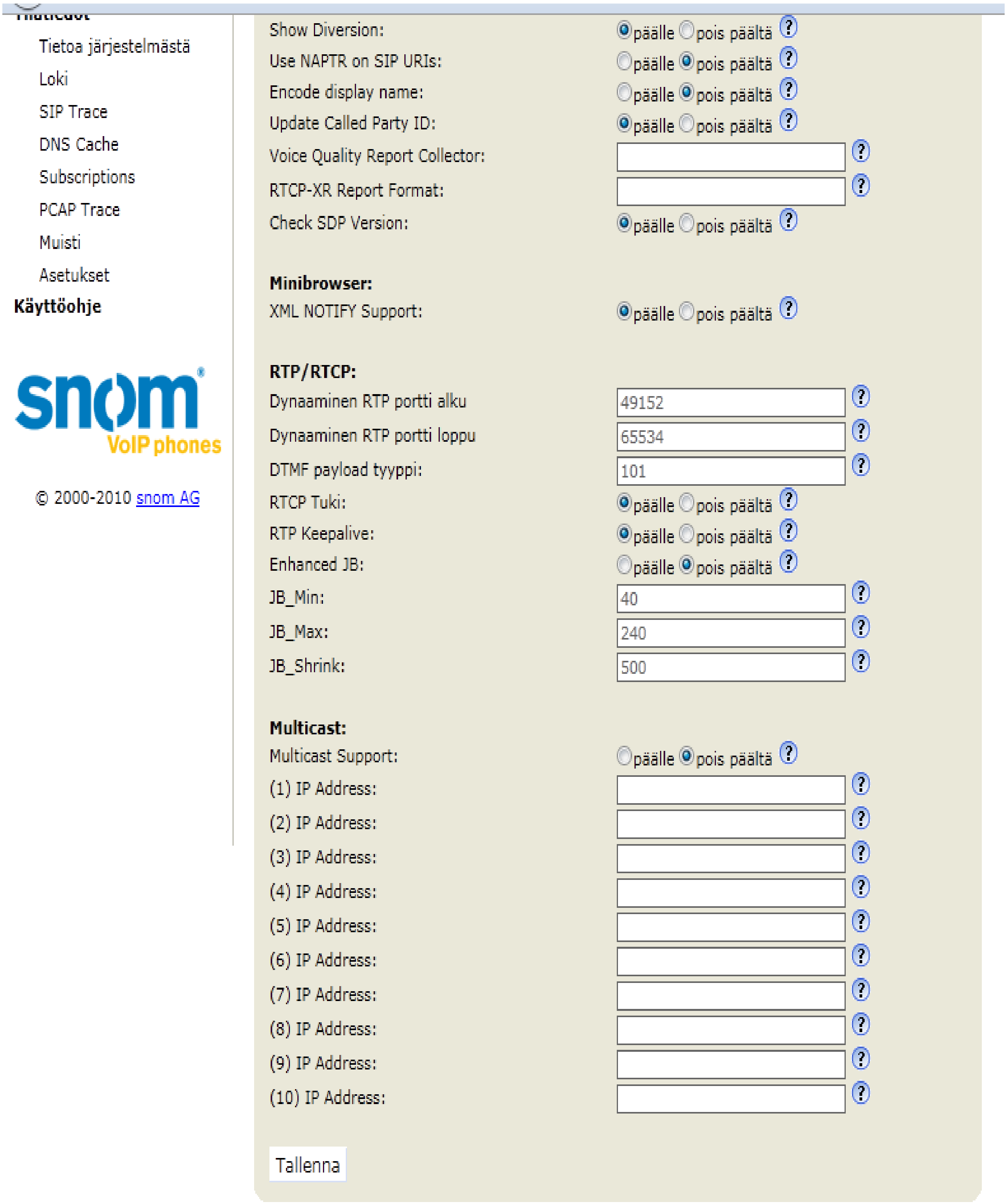
[24.] Wallace, K., CCNP. (2011). In Wallace K.,CCNP.Authorized self-study guide (Ed.), *Implementing cisco unified communications voice over IP and QoS (cvoice) foundation learning guide* (4th ed.). Indianapolis, Ind.; London: Cisco; Pearson Education distributor.

[25.] A sample configuration of AutoQoS for VoIP*.* (2003). Retrieved July, 2011, from http://www.avaya.com/uk/emea/en-us/resource/assets/applicationnotes/autoqos.pdf

[26.] Cisco Systems, Inc. (2003). *Cisco AutoQoS whitepaper.* Retrieved July, 2011, from http://www.cisco.com/en/US/tech/tk543/tk759/technologies_white_paper09186a00801348bc.shtml;

Appendix

SIP/RTP



Tietoa järjestelmästä
Loki
SIP Trace
DNS Cache
Subscriptions
PCAP Trace
Muisti
Asetukset

Käyttöohje

© 2000-2010 snom AG

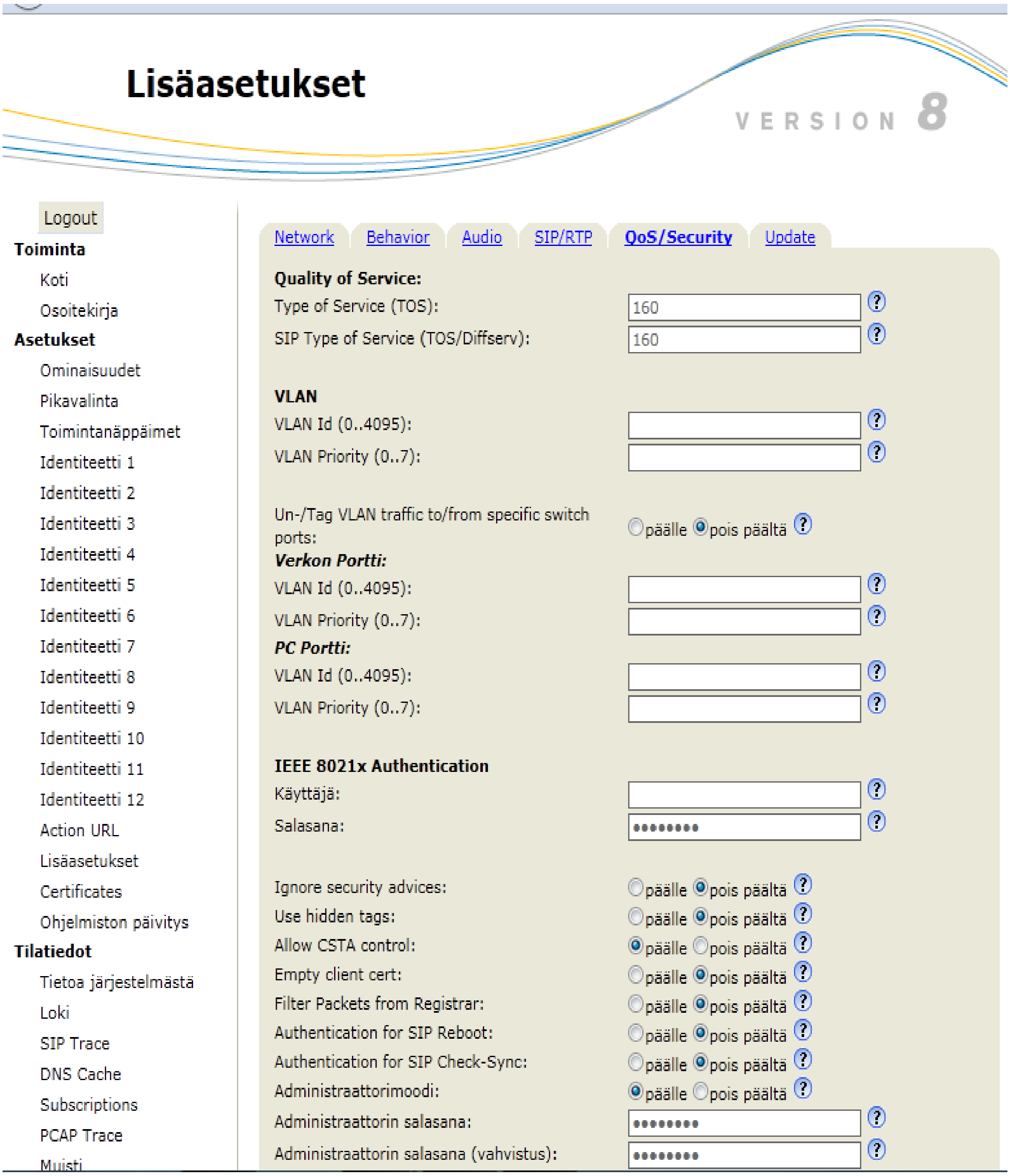
Show Diversion: ● päälle ○ pois päältä
Use NAPTR on SIP URIs: ○ päälle ● pois päältä
Encode display name: ○ päälle ● pois päältä
Update Called Party ID: ● päälle ○ pois päältä
Voice Quality Report Collector:
RTCP-XR Report Format:
Check SDP Version: ● päälle ○ pois päältä

Minibrowser:
XML NOTIFY Support: ● päälle ○ pois päältä

RTP/RTCP:
Dynaaminen RTP portti alku: 49152
Dynaaminen RTP portti loppu: 65534
DTMF payload tyyppi: 101
RTCP Tuki: ● päälle ○ pois päältä
RTP Keepalive: ● päälle ○ pois päältä
Enhanced JB: ○ päälle ● pois päältä
JB_Min: 40
JB_Max: 240
JB_Shrink: 500

Multicast:
Multicast Support: ○ päälle ● pois päältä
(1) IP Address:
(2) IP Address:
(3) IP Address:
(4) IP Address:
(5) IP Address:
(6) IP Address:
(7) IP Address:
(8) IP Address:
(9) IP Address:
(10) IP Address:

ToS bit used in SNOM



Lisäasetukset

Quality of Service:

Type of Service (TOS): 160

SIP Type of Service (TOS/Diffserv): 160

VLAN

VLAN Id (0..4095):

VLAN Priority (0..7):

Un-/Tag VLAN traffic to/from specific switch ports: ○päälle ●pois päältä

Verkon Portti:

VLAN Id (0..4095):

VLAN Priority (0..7):

PC Portti:

VLAN Id (0..4095):

VLAN Priority (0..7):

IEEE 8021x Authentication

Käyttäjä:

Salasana: ••••••••

Ignore security advices: ○päälle ●pois päältä

Use hidden tags: ○päälle ●pois päältä

Allow CSTA control: ●päälle ○pois päältä

Empty client cert: ○päälle ●pois päältä

Filter Packets from Registrar: ○päälle ●pois päältä

Authentication for SIP Reboot: ○päälle ●pois päältä

Authentication for SIP Check-Sync: ○päälle ●pois päältä

Administraattorimoodi: ●päälle ○pois päältä

Administraattorin salasana: ••••••••

Administraattorin salasana (vahvistus): ••••••••

Configuration for Catalyst switch 2950

Class Maps

```
class-map match-all DOM-VOIP-RTP
description ****** DOM-VOIP-RTP-TRAFFIC ******
match access-group name VOIP-RTP
```

Policy Map

```
policy-map DOM-QOS-TRAFFIC
description ****** DOM-QOS-TRAFFIC-POLICY ******
class DOM-VOIP-RTP
set ip dscp ef
```

COS setting

```
mls qos map cos-dscp 0 8 16 26 34 46 48 56
```

Attaching Policy to an interface

```
int gi0/1
service-policy input DOM-QOS-TRAFFIC
```

Voice RTP access list

```
 ip access-list extended VOIP-RTP
permit ip any any dscp ef
permit ip any any dscp cs5
```

Configuration for Catalyst switch 2960

Class Maps

```
class-map match-all DOM-VOIP-RTP
description ****** DOM-VOIP-RTP-TRAFFIC ******
match access-group name VOIP-RTP
class-map match-all DOM-VOIP-CONTROL
description ****** DOM-VOIP-CONTROL-TRAFFIC ******
match access-group name VOIP-CONTROL
```

Policy Map

```
policy-map DOM-QOS-TRAFFIC
description ****** DOM-QOS-TRAFFIC-POLICY ******
class DOM-VOIP-RTP
set ip dscp ef
police 1000000 65536 exceed-action policed-dscp-transmit
class DOM-VOIP-CONTROL
set ip dscp af31
police 1000000 16000 exceed-action policed-dscp-transmit
```

Turning QoS on

```
mls qos
```

COS setting

```
mls qos map cos-dscp 0 8 16 26 34 46 48 56
```

Attaching to an interface

```
int gi0/48
service-policy input DOM-QOS-TRAFFIC
```

Voice RTP and Voice Control access list

```
ip access-list extended VOIP-RTP
permit udp any any range 49152 65535
permit ip any any precedence 5
permit ip any any dscp ef
permit ip any any dscp cs5

ip access-list extended VOIP-CONTROL
permit tcp any any eq 5061
permit tcp any any eq 443
```

.