Technical report, IDE1048, May 2010

QoS management in DSL services of an ISP in Iran

Master’s Thesis in Computer System Engineering

Seyed Rashidaldin Hassani
QoS Management in DSL services of an ISP in Iran

Master Thesis in Computer System Engineering

School of Information Science, Computer and Electrical Engineering
Halmstad University
Box 823, S-301 18 Halmstad, Sweden

May 2010
Introduction

Preface

This thesis is submitted as the requirement for a Swedish Master's Degree in Computer System Engineering for the author. It contains work done from October 2009 to May 2010. The supervisor on the project has been professor Tonny Larsson, the Halmstad University. The thesis has been made solely by the author; most of the text, however, is based on the research and experiments of others, and the author has done his best to provide references to these sources.

Writing this thesis has been hard but in the process of writing I have learned a lot and my initial conceptions of engineering the quality of service in a large network systems have certainly changed. I have dealt with a lot of subjects, in an attempt to give this thesis a broad perspective on QoS engineering in large systems, thus combining many aspects of IP network and Computer System Engineering.

I would like to thank my supervisor, professor Tony Larsson, for lots of great inspirations and help. Thanks also Network Engineering Team in PardisOnline for their endless support and for letting me stay there for two weeks, conducting some tests in their well-equipped laboratory.

I wish to express my sincere gratitude to people and government of Sweden who so generously awarded this opportunity for me to learn and gain educational experience here in this beautiful country.

Finally come my parents, family and my friends who encouraged me and supported me at all times.

Seyed Rashidaldin Hassani
Halmstad University, May 2010
QoS Management for DSL users of an ISP in Iran
Introduction

Abstract

Quality of Service is a set of mechanisms created for differentiating users and data flows. Provisioning the QoS in service provider networks is always interesting for their business departments for they can offer and sell diverse services and to make more money. This thesis work focuses on implementing QoS for DSL subscribers of Pardis Online - the private ISP in Iran. The size of the network, the certain network connectivity limitations the ISP has in addition to the complexity of the services it provides, necessitate a comprehensive study to elucidate the different service types and requirements and then choosing a specific implementation of QoS in order to meet the ISP’s need. The internet bandwidth in the region that ISP operates is very expensive and the users suffer from the lack of bandwidth so the limited internet links are usually congested in the network. This document concludes with proposing a layered QoS that guarantees that the total bandwidth of an area in congested times is distributed to the users in that area proportionate to the subscribed bandwidth. The resulting proposals are tested in the Lab and their performance under the simulated traffic is monitored and analyzed.
QoS Management for DSL users of an ISP in Iran
Introduction

Contents

PREFACE ................................................................................................................................. 1

ABSTRACT ............................................................................................................................... 3

CONTENTS ............................................................................................................................... 5

1 INTRODUCTION ..................................................................................................................... 8

1.1 APPLICATION AREA AND MOTIVATION ................................................................. 8

1.2 PROBLEM STUDIED ...................................................................................................... 8

1.3 APPROACH CHOSEN TO SOLVE THE PROBLEM......................................................... 9

1.4 THESIS GOALS AND EXPECTED RESULTS ............................................................... 9

2 BACKGROUND ..................................................................................................................... 11

2.1 TX AND LX .................................................................................................................... 11

2.2 DCI ............................................................................................................................... 12

2.3 PPoE .............................................................................................................................. 12

2.4 DSLAM .......................................................................................................................... 12

2.5 BRAS ROUTER ............................................................................................................ 12

2.6 VPDN ............................................................................................................................. 13

2.7 AToM (MPLS XCONNECT) .......................................................................................... 13

2.8 NETWORK MANAGEMENT SERVICES ....................................................................... 13

3 SOLUTION IDEA TO BE INVESTIGATED ............................................................................ 15

3.1 SCENARIO 1 – QoS FOR MANAGEMENT TRAFFIC IN BACKBONE ........................... 15

3.1.1 Overview .................................................................................................................. 15

3.1.2 Scenario .................................................................................................................... 15

3.2 SCENARIO 2: QoS FOR MANAGEMENT TRAFFIC IN PROVINCE NETWORKS ................ 16

3.2.1 Overview .................................................................................................................. 16

3.2.2 Scenario .................................................................................................................... 16

3.3 SCENARIO 3: QoS TO HOME ...................................................................................... 19

4 DETAILED DESCRIPTION OF THE INVESTIGATED SOLUTION ........................................ 22

4.1 SCENARIO 1: QoS FOR MANAGEMENT TRAFFIC IN BACKBONE ........................... 22

4.1.1 Hardware Requirements ......................................................................................... 22

4.1.2 Software Requirements ......................................................................................... 22

4.1.3 Procedure ................................................................................................................. 22

4.2 SCENARIO 2: QoS FOR MANAGEMENT TRAFFIC IN PROVINCE NETWORKS ................ 24
QoS Management for DSL users of an ISP in Iran

4.2.1 Test Case Description ........................................................................................................... 25
4.2.2 Hardware Requirements ....................................................................................................... 25
4.2.3 Software Requirements ........................................................................................................ 25
4.2.4 Procedure ............................................................................................................................. 26

4.3 SCENARIO 3: QoS TO HOME ................................................................................................. 27
4.3.1 Hardware Requirements ....................................................................................................... 27
4.3.2 Procedure ............................................................................................................................. 27

5 TEST RESULTS ........................................................................................................................... 33
5.1 QoS FOR MANAGEMENT TRAFFIC IN BACKBONE .............................................................. 33
5.2 QoS FOR MANAGEMENT TRAFFIC IN PROVINCE NETWORKS ........................................... 36
5.3 QoS TO HOME ....................................................................................................................... 39
  5.3.1 Without QoS ....................................................................................................................... 39
  5.3.2 With QoS ............................................................................................................................ 40

6 CONCLUSIONS .......................................................................................................................... 42

7 REFERENCES ............................................................................................................................... 45

APPENDIX- I: DEVICE CONFIGURATION FILES (SCENARIO 2) ..................................................... 46
APPENDIX- II: DETAILED TOPOLOGY DIAGRAM FOR THE TEST (SCENARIO 2) ......................... 57
Introduction
1 Introduction

1.1 Application Area and Motivation

This thesis work aims to increase customer satisfaction and facilitate network maintenance and provisioning by applying QoS on the network. QoS is a technique to better utilize the bandwidth and resources. It doesn’t increase the bandwidth capacities, but through QoS, network administrators could prioritise the traffic in a way that if the link is congested so that the traffic is likely to be dropped in some extents, they could decide on intentionally drop lower priority traffics for keeping the higher priority traffics to be steadily served. Therefore it doesn’t help avoiding from the drops in the traffic, but help to guarantee serving sensitive traffics continually in routers and switches.

On the basis of our primary investigations on the ISP network and the company’s requirements, the critical traffic is identified that includes the management traffic for remote accessing and controlling the network devices in addition to voice traffic. These traffics are important to be treated as a high priority traffic so that the devices become accessible all the time either their uplinks are congested or not. It helps recovering the incidents fast and reliable. On the other hand, the traffic of customers should be differentiated in the way that they feel more quality in their services. On account of fact that the network topology varies in different areas, our attempts to manage QoS in the ISP’s network are focused in three independent phases. First, to giving high priority for some identified traffic (namely management traffic) in the backbone network where the solutions deal with high speed links that connects the resources together. Second, to apply QoS on the province distribution network where the solution mostly deals with layer-2 traffic and transportation technologies to carry layer-2 traffic over layer-3 links. Third, to provide a QoS on individual user’s services that deals with prioritizing user’s different traffics such as http, ftp, smtp and such like.

1.2 Problem Studied

In overall, this thesis work aims to provide solutions for two main problems. First, increasing user satisfaction by providing QoS for user’s traffic, and second, prioritising the overall traffic flows to ISP nodes in order to facilitate remote management and control of the devices in the network. The resulting solution must fit with the hardware capabilities of the devices employed in the network.

On the other hand, the best way to enable QoS on POL network should be determined first. Accordingly, the expected levels of service for some application specific traffic need to be provided. Some of the key things that needed to be considered in this work were:

1. Where should traffic initially be marked, or classified, and which devices would do the marking?

2. Different network devices have different traffic management capabilities; a way was required to implement a common packet marking strategy to overcome these differences.

3. It must be decided about how to map markings between OSI Layer 2 (Data Link) and Layer 3 (Network) levels, when traffic is handed off between the LAN and the WAN.
Introduction

1.3 Approach Chosen to Solve the Problem

The approach to solve the problem is to define some scenarios in order to simulate the problem first and then to test them in the lab. Marking/trusting mechanisms in QoS are standard methods to apply QoS in a network but the design of the QoS solution is depending on the network design and applications.

1.4 Thesis Goals and Expected Results

The project goal is to increase customer satisfaction and facilitate network management in the ISP by provisioning QoS in the network. The thesis will conclude with the following result:

1. Measure and test the most three successful scenarios and ideas in the LAB.
2. Evaluate and analyse the results.
3. Implement a prototype of the QoS provisioned network and a template configuration for helping to set up the solution in the entire network.
QoS Management for DSL users of an ISP in Iran
2 Background

There are some terminologies and technical concepts that are related to this work or locally known in the company. These concepts are regularly used in the proceeding chapters. This chapter addresses these terminologies.

2.1 TX and LX

Transit Exchange and Local Exchange are the terminologies used in Public Switching Telephone Network in Iran. Each city in Provinces has one TX and some LXs. The network topology of POL\(^1\) has been influenced from and is very dependent on this system for the major backbone links are provided by the Iran Telecommunication Organization that runs the Telephone Networks. The voice and data traffic of all LXs in the cities are aggregated in the TX centre through where they are crossed the city boarders and transported to other Cities (such as Tehran). Each LX covers a specific area in the city and to provide DSL service in that area, POL installs its DSL equipments such as DSLAM and router (LAC) in the LXs. Consequently, POL installs some equipment in the TX such as BRAS router to handle the aggregated data traffic of all LXs and route it to its core network in Tehran or to internet.

Figure 1 shows the topology of POL network in the provinces.

---

\(^1\) PardisOnline Company
QoS Management for DSL users of an ISP in Iran

2.2 DCI

Data Communication Company of Iran (DCI) is the governmental company that provides the backbone links to the private ISPs such as POL. These Links are more provided within a shared infrastructure such as layer 3 intranet links, or through dedicated point to point (layer 2) links such as E1 links. These links are connecting LXs in the cities to the related TX and, TXs of different cities to POL’s main POP site in Tehran [1].

Figure 2 illustrates the DCI’s intranet service.

![Figure 2. DCI intranet cloud](image)

2.3 PPPoE

The Point-to-Point Protocol over Ethernet (PPPoE) is an encapsulation protocol that encapsulates layer-2 PPP frames inside Ethernet frames. It is widely used in DSL networks by which the users are directly connected to a router called BRAS [2]. In this document, PPPoE traffic is sometimes referred as user’s layer 2 traffic for the PPPoE frames are handled between layer 2 and 3 so that network IP protocol is not applied on transporting PPPoE traffic from user to BRAS, because there is no need for routing in a point to point link. But from BRAS over, the traffic should be routed (E.g to internet cloud) so the PPPoE traffic will be turned into layer 3 (IP) traffic.

2.4 DSLAM

A Digital Subscriber Line Access Multiplexer in the telephone exchange centre (CO) aggregates multiple user DSL lines and converts the DSL signalling to Ethernet frames [3]. It is installed in LX and TX offices by the POL.

2.5 BRAS Router

A Broadband Remote Access Server (BRAS) is used in DSL topologies to terminate user PPP sessions over Ethernet (PPPoE) or ATM (PPPoA). This router is usually aggregates the output
Background

of one or several DSLAMs. Users usually establish a point to point PPPoE session and send all their outgoing traffic over this session. After the layer-2 PPPoE sessions are terminated in BRAS, resulting layer-3 traffic is routed toward the internet. The alternative terminology for BRAS is LNS\(^1\) for when Layer 2 Tunnelling Protocol or VPDN protocol is used to transport PPPoE traffic from a router (LAC\(^2\)) in an LX to a LNS (acts as BRAS) in the TX [3].

2.6 VPDN

Virtual Private Dial Network is protocol to transport layer-2 traffic (such as PPPoE traffic) over an IP (Layer 3) network from LAC router to LNS router. To give an example, Users in POL establish PPPoE sessions that enable a layer 2 point-to-point link with the BRAS. On account of the fact that the links between BRASes and the LXs -where DSLAMs are located- are provided from shared infrastructures such as Intranet clouds, the layer 2 traffic of the users should be somehow transported over the shared IP cloud to reach to the BRAS [5]. In such cases, the VPDN (or L2TP) is one of the several solutions that are being used in PardisOnline.

2.7 AToM (MPLS XConnect)

Like VPDN, the AToM\(^3\) (so called MPLS Xconnect or MPLS pseudowire) is a transport technology that aims to transport all types of traffic over MPLS enabled cloud. Comparing to VPDN, AToM is a modern technology and provides many features and capabilities on its virtual circuits. A virtual circuit (VC) in the AToM is a virtual point to point link that connects two peers over any network infrastructure as if the two peers are connected through a physical wire [4]. In POL, AToM technology is used besides VPDN to transport layer 2 PPPoE traffic from LXs to the TX. But some of the solutions proposed in this document conclude with this fact that providing an efficient QoS that enables bandwidth differentiation between different LXs is only possible in the cases that utilize AToM rather than VPDN for their layer 2 transportation protocol.

2.8 Network Management Services

A part of this thesis work is on providing QoS on network management traffics. Therefore, the network management traffics should be identified first. Each device in the network such as routers, switches and DSLAMs has possibilities of remote access to enable control, management and configurations remotely. Some of these operations such as daily backup of the configuration or monitoring could be scheduled and performed automatically through some specific network management software, or could be done manually using telnet protocol and such like. These communications form the management traffic. Solarwinds, Cacti and Radius are some examples of the network management tools used in POL.

---

\(^1\) L2TP Network Server

\(^2\) L2TP Access Concentrator

\(^3\) Any Transport over MPLS
QoS Management for DSL users of an ISP in Iran
3 Solution Idea to be Investigated

Many solutions have been supposed and investigated in this work in order to apply the appropriate QoS on the network. Among them, three solutions that could better satisfy the needs are chosen to be presented here. Others scenarios are either failed in experiments or inconsistent in the current topology of the company’s network. The ending chapters of this paper briefly address these failed experiments and compare them with the investigated scenarios.

3.1 Scenario 1 – QoS for Management Traffic in Backbone

3.1.1 Overview

The default service offering associated with POL network is best effort service. For some kinds of traffic like web, best effort is usually good enough. If packets get lost somewhere in the path, the end hosts will retransmit the missing packets. However, certain applications like management traffic require better performance for we want to make the highest possible priority to these traffics.

In deploying the chosen QoS mechanism, the proposed scenario has been inspired from the RFC 4594 Configuration Guidelines for DiffServ Service Classes [6].

This thesis work addresses the experiments carried out in the LAB to examine the QoS effectiveness and functionality in the POL Backbone with the purpose of giving priority to some POL NMS applications such as Cacti, Solarwinds, CSI and Radius.

3.1.2 Scenario

In order to ensure the QoS for the management traffic, a QoS mechanism is implemented in the scenario that is explained in the procedure section. Hereafter in this report, this mechanism will be called marking/trusting in the backbone.

The scenario simulates POL core network and different pipes are assigned to the connecting links. The management traffic originated from/destined to some particular management applications is marked as ‘DSCP CS2’ (second precedence) at the first hop and a minimum bandwidth is guaranteed for this traffic on all the other hops (routers and switches) in the path so that once a link became congested the minimum bandwidth over the whole path is preserved.

The management traffic could be destined to any device in the POL network and its reply is originated in the target device so the returning traffic should be marked at the same device once accessed by the management applications. The following diagram shows the network topology proposed for this scenario.

As could be seen from the diagram in Figure 3, the links have different pipes and some bottlenecks are made on the core links to examine the QoS efficiency on the congested links. This topology tends to deploy different types of devices used in POL core such as Juniper/Cisco routers and switches to make sure service consistency.

The Management Server on the left generates some traffic in special ports such as port 23 for telnet and the traffic should be marked at the first router and the mark is spread out by the traffic and reaches to the destination device. If the minimum bandwidth is guaranteed for the management traffic, the management server could be easily able to communicate with all
QoS Management for DSL users of an ISP in Iran

devices in the network regardless it is congested or not. Without this QoS, this communication is slow and undergoes some difficulties once a link in the path becomes congested.

The traffic generator on the management server is installed to produce dummy traffic of IP/ICMP/TCP/UDP types to stress the QoS test on management traffic and congesting the links.

![Network diagram for scenario 1](image)

**Figure 3. Network diagram for scenario 1**

### 3.2 Scenario 2: QoS for Management Traffic in Province Networks

#### 3.2.1 Overview

In continuance of the efforts to establish QoS for certain NMS applications in POL, this scenario addresses the QoS application in the province networks. The QoS in POL core is explained and tested in solution 1 but the province topologies are not conforming to the core network model. As tested in the other LAB activities, for the TX and LX pairs where the intranet link is provided, the bandwidth differentiation for the LX is not feasible with the current topology. Therefore, this document proposes a new solution (including a slight change in topology and configuration of TX router) to enable QoS on such TXs with the purpose of giving priority to some POL NMS applications, namely Cacti, Solarwinds, CSI and Radius.

#### 3.2.2 Scenario

With the purpose of applying QoS on the DCI1 intranet link in per LX basis, the traffic of each LX should be differentiated in the TX. For this, the former VPDN tunnels could be replaced by AToM (Any Transport over MPLS) circuits to transfer PPPoE traffic of the LX to TX and vice versa over the DCI intranet. The goal of putting all these technologies and techniques together is to provide a way to transfer all the traffic of one LX over one link, that in this scenario this interface is GRE Tunnel interface. The reason of this method is in that if

---

1 Data Communication company of Iran
Solution Idea to be Investigated

the traffic should be dynamically differentiated by QoS, all the traffic should pass through a single pipe. Therefore a QoS mechanism can be provisioned on the GRE Tunnel interface. It should be noted that, in the traditional topology in this ISP that the VPDN tunnels are used, PPPoE traffic is being transferred over a distinct VPDN tunnel whereas the other traffic for the same LX passes through the GRE Tunnel, so provisioning QoS in one interface was not feasible. Figure 4 shows the former topology diagram.

We have to determine the best way to enable QoS on the Cisco BRAS. The scenario simulates TX networks but instead of establishing VPDN tunnels for relaying PPPoE traffic to LNS (TX), AToM circuits are used. For this, a GRE tunnel is established first and LX routers form an LDP neighbourhood with the TX over the GRE tunnel. Afterwards, the AToM link is configured on a separate sub-interface on the router which is cross connected to another interface. Therefore, the traffic of each LX is terminated on a designated sub-interface related to that LX so that a distinct sub interface is configured on the cross-connected interfaces on BRAS for each LX.

The topology diagram is shown on Figure 5. The PPPoE traffic leaves the PC and passes through a switch to be tagged by relative dot1q value so that it could enter to the appropriate sub-interface on the router. At this sub-interface, the PPPoE traffic is encapsulated in AToM tunnel by the xconnect command configured on ingress sub-interface. In order to travel to the BRAS router, the packets are re-encapsulated by GRE tunnel to be carried over the GRE tunnel. Leaving the packet from tunnel egress interface, an MPLS label is pushed on the
QoS Management for DSL users of an ISP in Iran

packets to enable MPLS switching. At this point, the packet mtu\(^1\) reaches to 1400 bytes so it won’t make any mtu problem. Figure 6 illustrates the layer-2 encapsulations done on the user’s data.

On the other end, in Cisco BRAS (TX) router, the GRE tunnel ends up on the FastEthernet interface that in real cases, this is connected to DCI intranet. The MPLS label is stripped out and the GRE packets are decapsulated. The AToM traffic is entered to the router and directed to an egress sub-interface where the AToM is decapsulated to the original PPPoE traffic. The PPPoE traffic leaves the sub-interface and carried to other ingress sub-interface through a physical cable cross-connected to the other interface on the router where it is terminated.

The xconnect between LX1 and BRAS is configured on the gig0/1.401 of router LX and fa1/0.401 of BRAS router. For LX2, the xconnected interfaces are gig0/1.402 and fa1/0.402 in LX2 and BRAS respectively. To enable PPPoE session termination on BRAS, RADIUS server is used to push the required AVPs.

Therefore, the traffics generated in the PCs pass through the AToM link and reaches to the related sub-interface in BRAS and carried to the other interface on the same router where PPPoE traffics are being terminated.

The following key points should be considered in this scenario:
1. What policy-map should be configured on the router?
2. Which interface/sub-interface the service-policy should be applied on?
3. Checking the router stability while QoS is applied on the GRE tunnel besides per session QoS and shaping.

These questions are addressed in details in the next chapter.

---

\(^1\) Maximum Transmission Unit
3.3 Scenario 3: QoS to Home

According to our preliminary investigations from the DSL services in the Pars Online ISP, an ADSL user consumes his/her internet bandwidth by any applications and various purposes such as browsing web pages, playing online video or music, text chatting or voice chat, downloading files and etc. If the user is asked about quality of these internet services that is provided to him, in most cases he/she may reply “Sometimes I feel that the download speed has been decreased or voice and video quality is bad or, I no longer can send my emails concurrently with downloading”. There are many factors that may cause these issues for one or all users. Imagine 100 users are connected to a same PoP¹ site at the same time but only one user encounters the mentioned problems. In this case the most plausible reason is that the user is utilizing all his contracted bandwidth through different applications installed on his computer so that his web requests are no longer responded as quick as usual and yet the user expects to surf the web pages as fast as always. Among technical persons, this issue is called “Line Congestion”. It means that for instance, the specified user has subscribed to a 128kbps BW² limitation but he requests more than 128kbps, so some applications are starved and user may encounter poor voice quality but his download manager may still work well in the same time. This congestion may be even taken place when the uplink of that PoP site (the provided bandwidth to that PoP site) is fully utilized and reached to its limits. In this case all 100 connected users will be affected. It is not possible to tell it exactly that which user application (which type of traffic) is affected in this condition because it is depending on clients, servers and the number of sessions and so on. Therefore in normal conditions nobody can say that the voice quality is always good or always bad. The normal condition that is mentioned in the previous sentence means that the applications and their related traffic are not prioritized. Application prioritization means that ISP does congestion management on its uplinks or even on the single user’s link. For instance, in congestion time, the ISP can decide that voice and video requests are served before all other requests such as download requests. The ISP usually faces with multiple choices to prioritize the user’s traffic and requests. It was the most common problem of almost every ISP in Iran.

The other major problem of ISPs is their slow uplinks that are usually being congested at peak times and this affects the whole users connected to the congested PoP sites. In order to more efficiently utilize these limited bandwidths, this project is defined to apply some QoS on POL³ ADSL backbone (uplinks) and even on the user’s link to the PoP sites. This project is called “QoS to Home” in the company and this thesis work aims to attain this project’s goals. According to the identified requirements of the company, Voice, Video, DNS, POP3, SMTP and ICMP traffic must be supplied by higher and strict priorities to enable forwarding these traffics on the links even when the links are congested by other traffic types. After these traffics, HTTP and HTTPS traffic will take the remaining capacity through the second strict priority queue. The other traffic not mentioned in the above group will be served as the lowest priority and only if there is a free bandwidth yet remains on the link. Strict priority in first queue means that all applications which are classified as highest priority can consume whole the line rate in anytime. Second queue is still using strict priority feature so HTTP and HTTPS traffics will use whole remained bandwidth after the first queue. If the first queue is empty,

¹ Point of Presence
² Bandwidth
³ PardisOnline
QoS Management for DSL users of an ISP in Iran

then the second queue can be served by the whole remaining bandwidth. Last queue can use any other remained capacity from upper queues if there are still any.
Solution Idea to be Investigated
4 Detailed Description of the Investigated Solution

4.1 Scenario 1: QoS for Management Traffic in Backbone

4.1.1 Hardware Requirements

The hardware employed in order to demonstrate and test this scenario are listed as the followings:

- Cisco 7200VXR with one IO-2FE and as core router (IOS: c7200-a3jk91s-mz.122-31.SB13).
- Two Cisco 2821 series routers with GigabitEthernet interfaces as access routers (IOS: c2800nm-adventerprisek9-mz.124-24.7).
- Juniper M10 Router as core router
- Cisco 3550 Switch with a common IOS
- Laptops as management server and traffic generator client/server.

4.1.2 Software Requirements

The software and network tools used to run this test is listed as the followings:

- The Network Traffic Generator

4.1.3 Procedure

The routers form an OSPF neighbourhood like in the POL core. According to the diagram shown in Fig 2.1, different pipes are created over the connectivity links using output shaping on the routers. An access-list is configured in the router (POP1-2821-K1) at the first Hop to select the management traffic in order to apply the QoS on it. This selection is performed only once at the first hop. The following exhibition shows how this ACL should look like in the real implementation:

<table>
<thead>
<tr>
<th>Access-list to select Management Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list extended Management_QoS_out</td>
</tr>
<tr>
<td>permit tcp host 91.98.99.150 any eq telnet</td>
</tr>
<tr>
<td>permit tcp host 213.217.60.146 any eq telnet</td>
</tr>
<tr>
<td>permit tcp host 91.99.96.76 any eq 161</td>
</tr>
<tr>
<td>permit tcp host 91.98.29.131 any eq 161</td>
</tr>
<tr>
<td>permit tcp host 213.217.40.189 any eq 161</td>
</tr>
<tr>
<td>permit tcp host 91.98.28.10 any eq 161</td>
</tr>
<tr>
<td>permit ip 82.99.218.130 0.0.0.3 any</td>
</tr>
<tr>
<td>permit udp host 192.168.32.10 any eq 1645</td>
</tr>
<tr>
<td>permit udp host 192.168.32.10 any eq 1646</td>
</tr>
<tr>
<td>permit udp host 192.168.32.27 any eq 1645</td>
</tr>
<tr>
<td>permit udp host 192.168.32.27 any eq 1646</td>
</tr>
<tr>
<td>permit udp host 192.168.32.62 any eq 1645</td>
</tr>
<tr>
<td>permit udp host 192.168.32.62 any eq 1646</td>
</tr>
<tr>
<td>permit udp host 10.234.8.99 any eq 1812</td>
</tr>
<tr>
<td>permit udp host 10.234.8.99 any eq 1813</td>
</tr>
</tbody>
</table>

For simplicity, the following access-list is configured on the POP1 router to represent the above access-list:
Detailed Description of the Investigated Solution

<table>
<thead>
<tr>
<th>Access-list for test</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list extended Management_QoS_out</td>
</tr>
<tr>
<td>ip access-list extended MGM_QoS_ACL</td>
</tr>
<tr>
<td>permit tcp host 192.168.208.252 any eq telnet</td>
</tr>
<tr>
<td>permit tcp host 100.100.100.1 eq telnet host 192.168.208.252</td>
</tr>
<tr>
<td>permit icmp any any</td>
</tr>
</tbody>
</table>

Where, the management server IP is ‘192.168.208.252’. The first line selects the traffics originated by the management server and the second line selects the returning traffic related to the same router (POP1-2832-K1) for the case that the management applications communicate with this router itself. To enable to make a better judgment on the QoS effect after and before applying it to the traffics, the ping diagram is used and monitored to clarify the result. So the third line is configured to select the ICMP traffic.

The following class/policy-map together define the QoS function to be applied on the selected traffic.

<table>
<thead>
<tr>
<th>Marking the selected traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map match-all MARK_MGM</td>
</tr>
<tr>
<td>match access-group name MGM_QoS_ACL !</td>
</tr>
<tr>
<td>policy-map MGM_OUT</td>
</tr>
<tr>
<td>class MATCH_MGM</td>
</tr>
<tr>
<td>bandwidth 20</td>
</tr>
<tr>
<td>set dscp CS2</td>
</tr>
</tbody>
</table>

As can be seen from the configuration, a minimum bandwidth of 20kbps is preserved for this class on (this router) and then the traffic is marked as DSCP CS2.

The other class is configured supposing that the management traffic is generated and already tagged by DSCP CS2 in elsewhere not close to this router and passes through this router as a middle hop so that the required QoS function should be applied on it. The class is used at the same policy-map:

<table>
<thead>
<tr>
<th>Policy-Map</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map match-any MATCH_MGM</td>
</tr>
<tr>
<td>match dscp CS2 !</td>
</tr>
<tr>
<td>policy-map MGM_OUT</td>
</tr>
<tr>
<td>class MATCH_MGM</td>
</tr>
<tr>
<td>bandwidth 20</td>
</tr>
<tr>
<td>class MARK_MGM</td>
</tr>
<tr>
<td>bandwidth 20</td>
</tr>
<tr>
<td>set dscp CS2</td>
</tr>
<tr>
<td>class class-default</td>
</tr>
<tr>
<td>shape average 90000000</td>
</tr>
</tbody>
</table>

As shown in the exhibition, a default class is applied to shape the rest of the traffic and to define the pipe for the router’s egress port. It is supposed that the slight 20kbps bandwidth is extracted out of the total pipe capacity.
Finally, the policy map is applied on the egress interface of the router as output service policy:

<table>
<thead>
<tr>
<th>Service-policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface GigabitEthernet0/1</td>
</tr>
<tr>
<td>description connected to SW (toward 7200_core)</td>
</tr>
<tr>
<td>service-policy output MGM_OUT</td>
</tr>
</tbody>
</table>

The configuration is very similar in the other routers.

On the switch, the configuration undergoes a slight difference. The switch should trust the DSCP values on some certain interfaces connected to the core network; otherwise it resets the DSCP values by default:

<table>
<thead>
<tr>
<th>Switch configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>mls qos</td>
</tr>
<tr>
<td>!</td>
</tr>
<tr>
<td>class-map match-all MARK_MGM</td>
</tr>
<tr>
<td>match access-group name MGM_QoS_ACL</td>
</tr>
<tr>
<td>class-map match-all MATCH_MGM</td>
</tr>
<tr>
<td>match ip dscp 32</td>
</tr>
<tr>
<td>!</td>
</tr>
<tr>
<td>policy-map MGM_OUT</td>
</tr>
<tr>
<td>class MATCH_MGM</td>
</tr>
<tr>
<td>bandwidth 20</td>
</tr>
<tr>
<td>class MARK_MGM</td>
</tr>
<tr>
<td>bandwidth 20</td>
</tr>
<tr>
<td>set ip dscp CS2</td>
</tr>
<tr>
<td>!</td>
</tr>
<tr>
<td>interface FastEthernet0/13</td>
</tr>
<tr>
<td>mls qos trust dscp</td>
</tr>
<tr>
<td>service-policy output MGM_OUT</td>
</tr>
<tr>
<td>!</td>
</tr>
<tr>
<td>interface FastEthernet0/20</td>
</tr>
<tr>
<td>mls qos trust dscp</td>
</tr>
<tr>
<td>service-policy output MGM_OUT</td>
</tr>
<tr>
<td>!</td>
</tr>
<tr>
<td>ip access-list extended MGM_QoS_ACL</td>
</tr>
<tr>
<td>permit tcp host 100.10.10.2 host 192.168.208.252 eq telnet</td>
</tr>
</tbody>
</table>

The traffic generator client installed on the Management Server starts to generate dummy traffic (TCP protocol) to congest the connectivity links. Meanwhile, the end-to-end ping result is monitored on the computers to examine the QoS effect on the selected/marked traffic.

### 4.2 Scenario 2: QoS for Management Traffic in Province Networks

On account of the fact that this scenario requires some changes in the current topology on the POL in the provinces, several cases have been tested focusing on the different technologies to transport layer-2 traffic over layer-3 traffic. Among all these cases, one case has been chosen.
Detailed Description of the Investigated Solution

on the basis of its performance and consistency with the devices employed in the POL. Therefore, this specific case is explained in the followings.

4.2.1 Test Case Description

<table>
<thead>
<tr>
<th>Preserving QoS on point-to-point connectivity over intranet links in provinces using MPLS AToM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Test Case Name</strong></td>
</tr>
<tr>
<td><strong>Requirement Description</strong></td>
</tr>
<tr>
<td><strong>Test Object</strong></td>
</tr>
<tr>
<td><strong>Test Procedure</strong></td>
</tr>
<tr>
<td><strong>Units</strong></td>
</tr>
<tr>
<td><strong>Results</strong></td>
</tr>
<tr>
<td><strong>Remarks</strong></td>
</tr>
</tbody>
</table>

4.2.2 Hardware Requirements

The hardware employed in order to demonstrate and test this scenario are listed as the followings:

- Cisco 7200VXR (IOS: c7200-a3jk91s-mz.122-31.S813).
- Cisco 3550 Catalyst Switch.
- Four Laptops (two laptops for establishing PPPoE and to laptops to generate dummy traffic and stress the connections).

4.2.3 Software Requirements

The software and network tools used to run this test is listed as the followings:

- The Network Traffic Generator
4.2.4 Procedure

Each LX-TX pair forms an EIGRP neighborhood and a GRE tunnel is established between the two routers. Then the targeted MPLS LDP adjacency is established over the GRE tunnel. An AToM virtual-circuit is established between the customer side sub-interface on the LX and a sub-interface on the TX using xconnect command. In TX, a bba-group is applied on the other end of the cross-connected interfaces so that the PPPoE traffic could be terminated.

Regardless the LXs, the QoS could be applied in different places in TX. One could configure it on the PPPoE enabled sub-interface to shape the whole PPPoE traffic related to a single LX so that the LX intranet link will never be congested. The other way is to configure it on the ingress interface which is cross-connected to the PPPoE enabled interface. The advantage of QoS on this interface is that we have no other QoS mechanisms applied on the same interface like what is applied on the PPPoE enabled interface for per PPPoE session QoS.

The third solution which is preferred in this scenario is to apply QoS on the tunnel interface for all traffic containing both PPPoE and management traffic passes through the same interface so that the QoS could be applied to the whole LX pipe.

The policy-maps and class-maps are shown in the following exhibition.

<table>
<thead>
<tr>
<th>QoS Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map match-any MGM</td>
</tr>
<tr>
<td>match dscp cs2</td>
</tr>
<tr>
<td>match access-group name MGM</td>
</tr>
</tbody>
</table>

-------------- POLICY-MAPS

<table>
<thead>
<tr>
<th>policy-map LX_MGM</th>
</tr>
</thead>
<tbody>
<tr>
<td>class MGM</td>
</tr>
<tr>
<td>bandwidth 20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>policy-map LX1</th>
</tr>
</thead>
<tbody>
<tr>
<td>class class-default</td>
</tr>
<tr>
<td>shape average 2000000</td>
</tr>
<tr>
<td>service-policy LX_MGM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>policy-map LX2</th>
</tr>
</thead>
<tbody>
<tr>
<td>class class-default</td>
</tr>
<tr>
<td>shape average 1800000</td>
</tr>
<tr>
<td>service-policy LX_MGM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>policy-map 128s</th>
</tr>
</thead>
<tbody>
<tr>
<td>class class-default</td>
</tr>
<tr>
<td>police cir 1700000 bc 320000</td>
</tr>
<tr>
<td>conform-action transmit</td>
</tr>
<tr>
<td>exceed-action drop</td>
</tr>
</tbody>
</table>

---------------- ACLs

<table>
<thead>
<tr>
<th>ip access-list extended MGM</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit icmp any any</td>
</tr>
</tbody>
</table>

Shaping can be applied in different ways on the tunnel interface either by using explicit traffic shaping command or using service-policy which is preferred in this scenario:

<table>
<thead>
<tr>
<th>Service Policy on tunnel interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface Tunnel3</td>
</tr>
<tr>
<td>description to LX1</td>
</tr>
<tr>
<td>bandwidth 2000</td>
</tr>
<tr>
<td>service-policy output LX1</td>
</tr>
</tbody>
</table>
Detailed Description of the Investigated Solution

```
interface Tunnel2
  description to LX2
  bandwidth 1800
  service-policy output LX2
```

4.3 Scenario 3: QoS to Home

4.3.1 Hardware Requirements

The hardware employed in order to demonstrate and test this scenario are listed as the followings:

- Cisco 7200VXR (IOS: c7200-a3jk91s-mz.122-31.SB13).
- RedBack SmartEdge 100 (SmartEdge OS Version SEOS-5.0.7.7-Release)
- Cisco 7204VXR (IOS: c7200-a3jk91s-mz.122-31.SB13)
- Cisco 2821 (IOS: c2800nm-adventprisek9-mz.124-24.T)
- Alcatel ISAM 7330 DSLAM (OS version 3.6).
- Alcatel ISAM 7302FD DSLAM (OS version 3.6).
- 3COM switch.
- SY604 ADSL CPE.
- RADIUS Server
  - Debian version 5
  - FreeRadius 1.3

4.3.2 Procedure

Currently there are 3 major topologies in POL DSL network that can be found in table 1.

<table>
<thead>
<tr>
<th>NO</th>
<th>BRAS</th>
<th>Connectivity between LX &amp; TX</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Redback</td>
<td>802.1q</td>
</tr>
<tr>
<td>2</td>
<td>Redback / Cisco 7200</td>
<td>L2TP</td>
</tr>
<tr>
<td>3</td>
<td>Redback</td>
<td>AToM</td>
</tr>
</tbody>
</table>

In all topologies, two brands of DSLAMs are used in POL network: Alcatel ISAM and Corecess. Corecess platforms don’t support QoS in any layers. But ISAM supports QoS but their features differ according to the models of NT line cards. ISAM 7302FD and 7330FD are more flexible than POL older ISAM 7302XD. According to POL ADSL network design, the PPPoE session that is established between user and BRAS is layer-2 traffic. According to best practices of QoS, it’s better to enable QoS as close as possible to the source. Therefore, in this project we put our focus more on BRAS rather than DSLAM though all possible QoS features of ISAM DSLAMs are enabled as well and this will help us in some situations that will be discussed later in this document. Here two levels hierarchical QoS features are provided by SEOS (OS of Redback): per Session & per Pipe.

3.3.2.1 Per Session Queuing

- PWFQ:
A session is created between BRAS and each user who establishes a PPPoE connection. According to username and password of the user, an asymmetric minimum and maximum BW is being allocated as user’s uplink and downlink rates. Amount of real allocated BW is varied each time according to BRAS uplink congestion. In per session QoS, BRAS observes the amount of data rate for each session and compares it to allocated BW so if these two values are equal then BRAS assumes that the congestion is occurred in that specific session. After that, four different queues per each session start to serve traffic efficiently to the user according to PWFQ algorithm. For better understanding of this queuing, it’s better to take a look at the related commands first:

```
queue 0 priority 0 weight 100
queue 1 priority 1 weight 100
queue 2 priority 2 weight 50
queue 3 priority 2 weight 50
```

These commands define four queues for a session. Queue 0 has highest priority and is a strict priority queue so that in congestion time, the traffics in queue 0 will be served before other types of traffic. Queue 1 is also a strict priority queue and will use all the BW after queue 0 gets empty. Finally queue 2 and 3 with same priority number will get BW according to the specified weight (WRR schema). Here, one packet will be forwarded from queue 2 and one from queue 3 because the weight of both queues is equal.

Redback has a default table and puts the packets to a specific queue according to classification [7]:

<table>
<thead>
<tr>
<th>Priority Group</th>
<th>DSCP Value</th>
<th>IP Precedence</th>
<th>MPLS EXP</th>
<th>802.1p</th>
<th>4 Queues</th>
<th>2 Queues</th>
<th>1 Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Network Control</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>Queue 0</td>
<td>Queue 0</td>
<td>Queue 0</td>
</tr>
<tr>
<td>1</td>
<td>Reserved</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>Queue 1</td>
<td>Queue 1</td>
<td>Queue 0</td>
</tr>
<tr>
<td>2</td>
<td>Expedited Forwarding (EF)</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>Queue 2</td>
<td>Queue 1</td>
<td>Queue 0</td>
</tr>
<tr>
<td>3</td>
<td>Assured Forwarding (AF) Level 4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>Queue 3</td>
<td>Queue 2</td>
<td>Queue 0</td>
</tr>
<tr>
<td>4</td>
<td>AF Level 3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>Queue 4</td>
<td>Queue 1</td>
<td>Queue 0</td>
</tr>
<tr>
<td>5</td>
<td>AF Level 2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>Queue 5</td>
<td>Queue 2</td>
<td>Queue 0</td>
</tr>
<tr>
<td>6</td>
<td>AF Level 1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Queue 6</td>
<td>Queue 2</td>
<td>Queue 1</td>
</tr>
<tr>
<td>7</td>
<td>Default Forwarding (DF)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Queue 7</td>
<td>Queue 3</td>
<td>Queue 0</td>
</tr>
</tbody>
</table>

As shown in above table, packets are placed on each queue according to DSCP, IP Precedence, MPLS Experimental bits or 802.1p values. In this scenario, we are using 4-queues basis as the orange column that indicates mapping parameters used in this project.

BRAS does a pre-classification of the traffic enters to a specific session before executing other policies. Pre-classification is performed by a QoS policy and this policy uses a policy access-list to match desired packets and put them on correct classes. The related commands are as the followings:

```
policy access-list MARK
  seq 10 permit tcp any eq www any class HTTP (HTTP)
  seq 11 permit tcp any eq 443 any class HTTP (HTTPS)
  seq 20 permit udp any gt 1024 any class VOICE (VoIP, Video)
```
Detailed Description of the Investigated Solution

seq 30 permit tcp any eq 5060 any class VOICE (SIP)
seq 40 permit udp any eq domain any class DNS (DNS)
seq 50 permit icmp host 213.217.40.190 any class class-default (Exclude for ADSL Support)
seq 60 permit icmp host 82.99.193.2 any class class-default (Exclude for ADSL Support)
seq 70 permit icmp any any class ICMP (ICMP)
seq 80 permit tcp any eq pop3 any class POP3 (eMail)
seq 81 permit tcp any eq smtp any class SMTP (eMail)
seq 100 permit ip any any class class-default (other traffics)

qos policy MARK metering
access-group MARK local
   class VOICE
      mark dscp 63
class DNS
      mark dscp 63
class SMTP
      mark dscp 63
class POP3
      mark dscp 63
class ICMP
      mark dscp 62
class HTTP
      mark dscp ef
class class-default
      mark dscp df

Policy access-list MARK selects the traffic on the basis of its conditions and then put them on specified class. For example in sequence 10, traffic with source port 80 is forwarded to HTTP class. Sequence numbers 50 and 60 are for specific sources of ICMP for ADSL support team or NOC\(^1\) must feel the congestion during troubleshooting. So the generated ICMP traffics from LAN public IPs of NOC are excluded from prioritization.

QoS policy MARK metering, Marks DSCP values on each IP packet which will be matched by access-list to be used in next steps.

Now this QoS policy must be applied for each PPPoE session during its first establishment. There are two ways to perform that: First is the common solution in POL to push policies by Radius server and second is to apply it for all the sessions connected to BRAS:

subscriber default
qos policy queuing MARK

---

\(^1\) Network Operation Center
Applying this policy by default for all the subscribers eliminates the needs to add new attributes in Radius (AAA) server.

So far this section discussed about number and types of queues, types of traffics inside each queue, classification method and doing pre classification per session. The next discussion explains how to enable queuing per session.

At the current POL DSL network, each BRAS applies two policies for every session according to received attributes from AAA server and AAA chooses correct attributes according to authentication information of each user. These two policies tell BRAS about how much BW must be allocated for that user. One policy is for downlink and the other is for uplink of the user. In this project, QoS is applied for downlink of user so queuing configurations will be added to downlink service policy. Below one of these service policies in old and new format can be seen:

<table>
<thead>
<tr>
<th>OLD</th>
<th>NEW</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos policy 128SharedUserRx pwfq</td>
<td>qos policy 128SharedUserRx pwfq</td>
</tr>
<tr>
<td>rate maximum 1152</td>
<td>rate maximum 1152</td>
</tr>
<tr>
<td>rate minimum 128</td>
<td>rate minimum 128</td>
</tr>
<tr>
<td>num-queues 1</td>
<td>num-queues 4</td>
</tr>
<tr>
<td>queue 0 priority 0 weight 100</td>
<td>congestion-map CONGEST queue 0 priority 0 weight 100</td>
</tr>
<tr>
<td></td>
<td>queue 1 priority 1 weight 100</td>
</tr>
<tr>
<td></td>
<td>queue 2 priority 2 weight 50</td>
</tr>
<tr>
<td></td>
<td>queue 3 priority 2 weight 50</td>
</tr>
</tbody>
</table>

- **Congestion Avoidance:**

As you can be seen in the above table, the number of queues and configuration of queues weight and priority have been changed in the new format. Queuing concept discussed before in this scenario.

*congestion-map CONGEST* is the only difference between old and new syntaxes that is needed to be discussed here. By default, the SmartEdge OS drops packets at the end of the queue when the number of packets exceeds the configured maximum depth of the queue. A congestion avoidance map attached to a PWFQ scheduling policy, provides congestion management for each queue defined by the policy. Congestion avoidance is used in every queue to drop lower priority packets when the queue is going to be congested. For example in queue 0, ICMP traffic is forwarded beside real time traffics. In normal condition when queue 0 is not congested, then both ICMP and RTP are forwarded without being dropped at all. But whenever the used queue capacity reaches to a minim threshold of each flow, then BRAS starts to drop the packets randomly to avoid congestion in that queue. It is better that syntaxes be reviewed before further explanations.

```plaintext
qos congestion-avoidance-map CONGEST pwfq
  queue 0 red profile-1 dscp 63 min-threshold 1000 max-threshold 4000 probability 10
  queue 0 red profile-2 dscp 62 min-threshold 500 max-threshold 3000 probability 5
  queue 1 red profile-1 dscp ef min-threshold 1000 max-threshold 4000 probability 10
```
Detailed Description of the Investigated Solution

queue 1 red profile-2 dscp 45 min-threshold 500 max-threshold 2000 probability 5
queue 2 red profile-1 dscp df min-threshold 100 max-threshold 500 probability 1
queue 3 red profile-1 dscp df min-threshold 1000 max-threshold 4000 probability 5

For instance, second and third lines are for queue 0. Packets marked by DSCP 63 will be dropped before 62, because defined minimum threshold of them is less than the packets with 63 DSCP value. **Probability** defines the probability of a packet being dropped as the average queue occupancy approaches the maximum threshold value. The value of the Probability argument is the inverse of the probability of a packet being dropped. The higher value of the probability argument is the lower the probability of a packet to be dropped.

3.3.2.2 *Per Pipe Queueing*

- PWFQ

RedBack is able to do PWFQ per pipe. Pipe is dedicated uplink of special site (LX, CO, POP Site) to BRAS. By enabling this feature if that pipe be congested then BRAS will start to forward the packets to that site according to its PWFQ settings. Per pipe queuing can be applied just on layer 2 logical pipes like layer 2 MPLS, 802.1q. Over layer 3 connections like L2TP it’s not possible to enable per pipe queuing because in that situation an interface is shared to more than one pipe and BRAS cannot determine congestion to enable queuing.

Let’s continue explanation after reviewing syntaxes:

```
qos policy PIPE-Name-QOS pwfq
rate maximum 512
rate minimum 511
num-queues 4
congestion-map CONGEST
queue 0 priority 0 weight 100
queue 1 priority 1 weight 100
queue 2 priority 2 weight 50
queue 3 priority 2 weight 50
!
port ethernet 2/3
mtu 1400
no shutdown
encapsulation dot1q
dot1q pvc 100 profile MARK-COS encapsulation pppoe
qos rate maximum 512
qos policy queuing PIPE-QOS
bind authentication pap context local maximum 8000
```

*qos policy PIPE-QOS pwfq* is almost like the QoS policy of per-session queuing but it differs in maximum and minimum rates. The max and min rate in this policy should be equal to actual maximum rate of that pipe which now configures under PVC configuration of BRAS physical port. This policy map must be created per pipe and to apply it on special pipe QoS policy queuing, PIPE-QOS must be set under PVC configuration as can be seen in above syntaxes.
QoS Management for DSL users of an ISP in Iran
5 Test Results

Three scenarios for tests has been designed and explained in the previous section. The result of each test could demonstrate how effective the solution is. Therefore, the results of the tests are addressed in detail in this section.

5.1 QoS for Management Traffic in Backbone

In order to facilitate the test, the ICMP packets obtained higher priorities. The ping times are monitored before and after applying the QoS on the routers. The following exhibit demonstrates the long ping times over the congested link.

![Without QoS](image)

**Figure 7. Without QoS**

The ping is performed in the computer (management server) with the target of POP2-2821-Ay router. As can be seen from the Figure 7, the average ping time never falls from a considerable high level (approximately 350ms) and it sometimes undergoes ‘request timeout’.

The window at the right is the traffic generator software that produces as much TCP traffic as possible to the traffic generator server in the other end.

The next exhibit shows the result after applying the QoS on the selected traffic. As can be seen from Figure 8, the ping diagram becomes much optimized so that the ping time significantly drops from 350ms to roughly 5ms.

The other test was performed to examine the telnet operation. Before applying the QoS on the congested link, the telnet from the management server to the routers (especially to POP2-2821-ay) worked difficultly and very slow. After applying the QoS, the telnet operations seemed very natural and fluent.

The link between the C7200 router and the Juniper is the only 2mbps and accounts as the bottleneck so that the majority of the drops happen in 7200 router while the traffic flows from traffic management client to the traffic management server (left to right).
QoS Management for DSL users of an ISP in Iran

Figure 8. After Applying QoS

The following exhibit shows the policy map applied to the interface pos3/0 in C7200 (connected to Juniper):

```
7200_core (bottleneck)

7200_core#sh policy-map int pos3/0
POS3/0

Service-policy output: MGM_OUT_2

Class-map: MATCH_MGM (match-any)
3016 packets, 190219 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: dscp CS2 (32)
3016 packets, 190219 bytes
5 minute rate 0 bps
Queueing
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkt output/bytes output) 3016/190219
bandwidth 20 kbps

Class-map: MARK_MGM (match-all)
416 packets, 21756 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name MGM_QoS_ACL
Queueing
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkt output/bytes output) 416/21756
```
Test Results

<table>
<thead>
<tr>
<th>QoS Set</th>
<th>dscp CS2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets marked 416</td>
<td></td>
</tr>
<tr>
<td>bandwidth 20 kbps</td>
<td></td>
</tr>
</tbody>
</table>

Class-map: class-default (match-any)
720974 packets, 1066072260 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: any
720974 packets, 1066072260 bytes
5 minute rate 0 bps
Queueing
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/29815/0
(pkt output/bytes output) 691159/1022198300
shape (average) cir 2000000, bc 8000, be 8000
target shape rate 2000000

The number of packets marked in the POP1-2821-K1 that is the first hop for the management server is significantly high since the main telnet and ICMP traffic is generated here to different destinations:

<table>
<thead>
<tr>
<th>POP1_2821_K1</th>
</tr>
</thead>
</table>
| POP1_2821_K1#sh policy-map int gig0/1
GigabitEthernet0/1 |
| Service-policy output: MGM_OUT |

Class-map: MATCH_MGM (match-any)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: dscp CS2 (32)
0 packets, 0 bytes
5 minute rate 0 bps
Queueing
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkt output/bytes output) 0/0
bandwidth 20 kbps

Class-map: MARK_MGM (match-all)
3560 packets, 271592 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name MGM_QoS_ACL
Queueing
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkt output/bytes output) 3560/271592
bandwidth 20 kbps
QoS Set
dscp CS2
5.2 QoS for Management Traffic in Province Networks

To test the QoS performance and its functionality, the QoS is applied on ICMP protocol and mutual pings are performed on two computers, one is connected to LX1 and the other is connected to TX router. To simulate the real environment and examine QoS functionality in conjunction with per session QoS, a PPPoE connection is established in the test as well and generates dummy traffic up to the maximum allowed rate for the subscriber. Moreover, to examine the behavior of the router when applying QoS over heavy traffics, the pipes of each LX are selected in large extents such as 10 mbps or so and this leaded to some considerations in the testing methods.

Figure 9. Pipe Assignment in Scenario2
Test Results

To give an example, first we experienced a very high CPU load so that the router was not able to truly apply the QoS since a good deal of various types of traffics had been flooded to the router. This problem was solved by enabling interrupt switching on ingress interface and those which were burden with traffic.

Figure 9 shows the test bed and the traffic flows between each node. Moreover, the pipe capacities are indicated on the figure. PC3 and PC4 are PPPoE users and they exchange some dummy traffic (like ftp) by each other. On the other hand, PC1 and PC2 are directly connected to TX Bras and LX1 router respectively and their traffic are distinct from PPPoE traffic. First, they start to exchange a good deal of traffic using a TCP/UDP traffic generator by making several simultaneous connections. Moreover, some ftp sessions are established between two PCs for stressing the link even further. Afterwards, PC1 and PC2 start to exchange large ICMP packets with each other.

The scenario is designed in a way so that the ping traffic besides the PPPoE traffic pass through the tunnel interface in addition to all other traffics such as management, EIGRP protocol and so on that are destined to the same LX.

Approximately 80 kbps ping traffic is generated on both computers. Figure 10 shows the ping result before and after applying QoS on the tunnel interface.

As can be seen from the exhibition, while a 100 kbps bandwidth is guaranteed for the ping traffic (representing the management traffic in the test) the ping diagram remains stable without any drops along the time and its delay average time is about 400 ms. The reason for such long delay is that the link from LX1 to TX is entirely congested and on the other hand,
the 100 kbps bandwidth is not really enough for the largely selected ping datagram so they are queued on the interfaces. Once the minimum guaranteed bandwidth for ping traffic is removed, the ping replies started to be dropped continuously though the delays seemed to be declined by 30%.

As could be expected, increasing the guaranteed bandwidth for the MGM class resulted in reducing the ICMP delays. Figure 11 compares the delay times corresponding to the bandwidths of 20 kbps and 100 kbps for MGM class.

The LLQ configuration is also tested in the lab. The LLQ makes the delay time quite short but it makes a maximum rate on the traffic so that the exceeding traffic will be dropped, that is indeed undesirable for MGM traffic. Figure 12 compares the ping performance for three different QoS configuration: LLQ, bandwidth and no Qos. The minimum LLQ priority rate is 220 kbps in this test to allow MGM traffic (here ping traffic) passes through the link. Any lesser rates cause dropping the large ping datagram entirely, so LLQ is not recommended to be used for MGM QoS unless a lesser latency was desired so a bigger number for LLQ priority rate should be assigned.
Test Results

5.3 QoS to Home

According to the diagram, the test has been accomplished and BRAS queuing was monitored as the followings:

User Package = 128/128 Kb/s
Burst = No
ADSL Physical Line Rate = 1024 Kb/s
POL Cache = Bypassed
User Connection = PPPoE

5.3.1 Without QoS

FTP Download Rate (KB/s): 15 to 16 stable (the PPPoE session was congested)
Time takes to open yahoo.com: 1:40

Ping results:

Reply from 4.2.2.4: bytes=32 time=3886ms TTL=237
Reply from 4.2.2.4: bytes=32 time=3914ms TTL=237
Request timed out.
QoS Management for DSL users of an ISP in Iran

Request timed out.
Request timed out.
Request timed out.
Reply from 4.2.2.4: bytes=32 time=3994ms TTL=237
Reply from 4.2.2.4: bytes=32 time=3690ms TTL=237
Request timed out.
Reply from 4.2.2.4: bytes=32 time=3941ms TTL=237
Request timed out.

Ping statistics for 4.2.2.4:
   Packets: Sent = 42, Received = 24, Lost = 18 (42% loss),
   Approximate round trip times in milliseconds:
      Minimum = 594ms, Maximum = 4317ms, Average = 3820ms

5.3.2 With QoS

FTP Download Rate (KB/s): 15 to 16 (decreased when higher priority traffic requested by user)

Time takes to open yahoo.com: 23

Ping results:
Reply from 4.2.2.4: bytes=32 time=240ms TTL=237
Reply from 4.2.2.4: bytes=32 time=240ms TTL=237
Reply from 4.2.2.4: bytes=32 time=229ms TTL=237
Reply from 4.2.2.4: bytes=32 time=240ms TTL=237
Reply from 4.2.2.4: bytes=32 time=240ms TTL=237
Reply from 4.2.2.4: bytes=32 time=230ms TTL=237
Reply from 4.2.2.4: bytes=32 time=240ms TTL=237
Reply from 4.2.2.4: bytes=32 time=240ms TTL=237
Reply from 4.2.2.4: bytes=32 time=240ms TTL=237
Reply from 4.2.2.4: bytes=32 time=240ms TTL=237
Reply from 4.2.2.4: bytes=32 time=240ms TTL=237
Reply from 4.2.2.4: bytes=32 time=230ms TTL=237
Reply from 4.2.2.4: bytes=32 time=240ms TTL=237
Reply from 4.2.2.4: bytes=32 time=230ms TTL=237
Reply from 4.2.2.4: bytes=32 time=230ms TTL=237
Reply from 4.2.2.4: bytes=32 time=240ms TTL=237
Reply from 4.2.2.4: bytes=32 time=240ms TTL=237
Reply from 4.2.2.4: bytes=32 time=230ms TTL=237
Reply from 4.2.2.4: bytes=32 time=250ms TTL=237
Reply from 4.2.2.4: bytes=32 time=239ms TTL=237
Reply from 4.2.2.4: bytes=32 time=240ms TTL=237

Ping statistics for 4.2.2.4:
   Packets: Sent = 610, Received = 610, Lost = 0 (0% loss),
   Approximate round trip times in milliseconds:
      Minimum = 219ms, Maximum = 321ms, Average = 251ms

In order to check real time streaming traffic, youtube.com was tested. When the player started to play the video, the FTP connection speed reached to 2 KB/s or even FTP was being disconnected because the queue was congested.
Test Results
6 Conclusions

The test scenarios was able to demonstrate the efficiency of the chosen QoS mechanisms in POL backbone and access networks. As long as the DSCP field remains unchanged during the path, this QoS mechanism could be applied on any devices in the network including Juniper and Cisco routers as well as layer-3 switches. On some Layer-2 switches, since the DSCP and CoS fields are unrecognizable by these switches and QoS is poorly implemented or not implemented at all on these devices, all QoS mechanisms will fail at these nodes. In POL, C3524 switches that are used in a few numbers in the POL Core and in large extents in the provinces raise these difficulties.

There are a few other methods for applying QoS in the backbone for management such as matching the L-3 traffic against the IP access-lists on all hops individually and independently applying QoS on them and this leads to decline the performance comparing to the marking and trusting method. The other option was to assign a reserved and fixed bandwidth to the management traffic (like LLQ in Cisco) but it would be considerably costly to throw more bandwidth at the problem.

To conclude with, we understood that a better way to deal with QoS is to setup a framework that allows for categorizing the traffic and guaranteeing that service levels are met by monitoring the traffic. As part of the QoS project, we decided to use marking/trusting methods on the specific management applications. The RFC 4594 “Configuration Guidelines for DiffServ Service Classes” was used as our guideline to set the DSCP (differentiated service code point) bits in the IP packet. DSCP defines the relative priority and drop precedence for IP packets in a network.

To ensuring the marking of IP packets when the traffic transported from the POL network to DCI intranet cloud, it is important to ensure that the DSCP setting are copied from the packet header to the GRE tunnel header so that the QoS could be applied on the outgoing interface of the equipment (at the provinces edge). When the GRE packet passes through the DCI switch, its DSCP bits are reset by default. At the tunnel destination, when the packets are decapsulated the original DSCP bits remains unchanged. Using QoS over GRE tunnels is tested in the scenario 2 and Figure 13 shows the integration of the first and second scenario connecting the management traffic sources in Tehran to the province networks.

When the traffic moves from the POL core network toward the province TXs, it either passes through a layer-2 link such as E1 link or through GRE tunnel over the DCI intranet. In the first case, the DSCP settings remains unchanged and reaches to the TX router. The second case is also discussed and examined in the LAB.

We developed standard configuration templates to minimize implementation risks. Finally, step-by-step plan enables us to implement and test the configurations before applying changes to entire backbone, and eventually across the entire POL network.
Conclusions

Figure 13. QoS from Tehran to Province Backbone
QoS Management for DSL users of an ISP in Iran
Conclusions

7 References


Appendix- I: Device Configuration Files (Scenario 2)

Since the configuration implemented on the Scenario 2 (for QoS on Province Networks) are complicated, the complete snapshot of configuration files are enclosed by the following tables. The detailed topology diagram is shown in Appendix II.

<table>
<thead>
<tr>
<th>LX1</th>
</tr>
</thead>
<tbody>
<tr>
<td>version 12.4</td>
</tr>
<tr>
<td>service timestamps debug datetime msec</td>
</tr>
<tr>
<td>service timestamps log datetime msec</td>
</tr>
<tr>
<td>no service password-encryption</td>
</tr>
<tr>
<td>hostname LX_1</td>
</tr>
<tr>
<td>boot-start-marker</td>
</tr>
<tr>
<td>boot-end-marker</td>
</tr>
<tr>
<td>logging message-counter syslog</td>
</tr>
<tr>
<td>enable secret 5 $1$fK5x$nOg1Pp9iOYgA5TjiWuKr/</td>
</tr>
<tr>
<td>no aaa new-model</td>
</tr>
<tr>
<td>dot11 syslog</td>
</tr>
<tr>
<td>ip source-route</td>
</tr>
<tr>
<td>ip cef</td>
</tr>
<tr>
<td>no ip domain lookup</td>
</tr>
<tr>
<td>no ipv6 cef</td>
</tr>
<tr>
<td>mpls ldp neighbor 100.100.100.1 targeted</td>
</tr>
<tr>
<td>mpls label protocol ldp</td>
</tr>
<tr>
<td>voice-card 0</td>
</tr>
<tr>
<td>username cisco password 0 cisco</td>
</tr>
<tr>
<td>archive log config</td>
</tr>
</tbody>
</table>
Conclusions

```
hidekeys
!
!
class-map match-any MGM
  match access-group name MGM
  match dscp cs2
!
!
policy-map LX_MGM
  class MGM
    bandwidth 100
  class class-default
    random-detect
policy-map LX1
  class class-default
    shape average 1800000
    service-policy LX_MGM
!
!
interface Loopback1
  ip address 100.100.100.2 255.255.255.255
!
interface Tunnel1
  description GRE Tunnel to TX over Intranet
  ip address 30.30.30.2 255.255.255.252
  mpls ip
  tunnel source GigabitEthernet0/1.401
  tunnel destination 10.10.10.1
!
interface Tunnel3
  description new Tun to TX
  bandwidth 2000
  ip address 60.60.60.2 255.255.255.252
  load-interval 30
  mpls ip
  tunnel source GigabitEthernet0/1.401
  tunnel destination 10.10.10.1
  service-policy output LX1
!
interface GigabitEthernet0/0
  no ip address
  duplex auto
  speed auto
!
interface GigabitEthernet0/0.302
  encapsulation dot1Q 302
  ip address 192.168.2.1 255.255.255.0
!```
interface GigabitEthernet0/0.401
capsulation dot1Q 401
xconnect 100.100.100.1 200 encapsulation mpls
!
interface GigabitEthernet0/1
no ip address
duplex full
speed 100
!
interface GigabitEthernet0/1.401
encapsulation dot1Q 401
ip address 10.10.10.2 255.255.255.0
!
router eigrp 100
   network 60.60.60.0 0.0.0.3
   network 100.100.100.2 0.0.0.0
   network 192.168.2.0
   no auto-summary
!
ip forward-protocol nd
ip route 11.11.11.0 255.255.255.0 10.10.10.1 name TX_tunnel
no ip http server
no ip http secure-server
!
!
!
ip access-list extended MGM
   permit icmp any any
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
Conclusions

```
line con 0
line aux 0
line vty 0 4
    login local
line vty 5 15
    login local
!
scheduler allocate 20000 1000
end

LX2

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname LX2
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$M8fP$wAbPjTtZKq9P96NCf5Tv4/
!
no aaa new-model
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
no ip domain lookup
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
mpls label protocol ldp
vpdn enable
vpdn source-ip 20.20.20.2
!
vpdn-group Relay
    request-dialin
        protocol l2tp
    initiate-to ip 10.10.10.2
```
local name LX-ROUTER
no l2tp tunnel authentication

voice-card 0

username cisco password 0 cisco
archive
log config
hidekeys

bba-group pppoe Intranet
virtual-template 1
service profile Relay
sessions per-mac limit 1
sessions per-vlan limit 10000
sessions per-mac throttle 10 20 30
sessions auto cleanup

class-map match-any MGM
match access-group name MGM
match dscp cs2

policy-map LX_MGM
class MGM
  bandwidth 100
class class-default
  random-detect

policy-map LX2
class class-default
  shape average 1300000
  service-policy LX_MGM

interface Loopback1
ip address 100.100.100.2 255.255.255.255

interface Tunnel1
ip address 30.30.30.2 255.255.255.252
mpls ip
go pre-classify
tunnel source GigabitEthernet0/1
tunnel destination 10.10.10.2
service-policy output LX2
!
interface GigabitEthernet0/0
description PPPoE-LX
no ip address
duplex auto
speed auto
pppoe enable group Intranet
!
interface GigabitEthernet0/1
description Connected to TX
ip address 20.20.20.2 255.255.255.252
duplex auto
speed auto
!
interface Virtual-Template1
ip unnumbered GigabitEthernet0/1
no ip redirects
ip mtu 1460
ip tcp adjust-mss 1420
load-interval 30
no snmp trap link-status
ppp authentication pap
!
router eigrp 100
passive-interface default
no passive-interface Tunnel1
network 30.30.30.0 0.0.0.3
network 100.100.100.2 0.0.0.0
no auto-summary
!
ip forward-protocol nd
ip route 0.0.0.0 20.20.20.1 200
ip route 192.168.0.0 255.255.255.0 20.20.20.1 200
no ip http server
no ip http secure-server
!
!
ip access-list extended MGM
permit tcp any host 192.168.208.252 eq telnet
permit icmp any any
!
!
ip access-list extended MGM
permit tcp any host 192.168.208.252 eq telnet
!
!
mpls ldp router-id Loopback1 force
!
control-plane
QoS Management for DSL users of an ISP in Iran

<table>
<thead>
<tr>
<th>TX</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>version 12.2</strong></td>
</tr>
<tr>
<td>service timestamps debug uptime</td>
</tr>
<tr>
<td>service timestamps log uptime</td>
</tr>
<tr>
<td>no service password-encryption</td>
</tr>
<tr>
<td>!</td>
</tr>
<tr>
<td>hostname TX-Router</td>
</tr>
<tr>
<td>!</td>
</tr>
<tr>
<td>boot-start-marker</td>
</tr>
<tr>
<td>boot-end-marker</td>
</tr>
<tr>
<td>!</td>
</tr>
<tr>
<td>enable secret 5 $1$vF8K$6tlK1YR1PiPvY4Zw1p10.</td>
</tr>
<tr>
<td>!</td>
</tr>
<tr>
<td>aaa new-model</td>
</tr>
<tr>
<td>!</td>
</tr>
<tr>
<td>aaa authentication login default local</td>
</tr>
<tr>
<td>aaa authentication ppp default group radius</td>
</tr>
<tr>
<td>aaa authorization network default group radius</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>version 12.1</strong></td>
</tr>
<tr>
<td>no service pad</td>
</tr>
<tr>
<td>service timestamps debug uptime</td>
</tr>
<tr>
<td>service timestamps log uptime</td>
</tr>
<tr>
<td>no service password-encryption</td>
</tr>
<tr>
<td>!</td>
</tr>
</tbody>
</table>
hostname C3550
!
enable secret 5 $1$PKsd$9B1d/xgZ8oNY.j8NLE.j1
!
ip subnet-zero
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!policy-map LX2_SW
   class class-default
       police 1500000 320000 exceed-action drop
policy-map LX1_SW
   class class-default
       police 2000000 320000 exceed-action drop
!
interface FastEthernet0/1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 75
  switchport mode trunk
!
interface FastEthernet0/2
  switchport access vlan 301
  switchport mode access
!
interface FastEthernet0/3
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 401
  switchport mode trunk
  switchport protected
duplex full
spanning-tree portfast
service-policy input LX1_SW
service-policy output LX1_SW
!
interface FastEthernet0/4
  switchport access vlan 402
  switchport mode access
  switchport protected
duplex full
spanning-tree portfast
service-policy input LX2_SW
service-policy output LX2_SW
!
interface FastEthernet0/5
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 401,402
  switchport mode trunk
duplex full
interface FastEthernet0/6
    switchport access vlan 150
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan 150,301
    switchport mode trunk

interface FastEthernet0/7
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan 302,401
    switchport mode trunk

interface FastEthernet0/8
    switchport access vlan 301
    switchport mode access
    spanning-tree portfast

interface FastEthernet0/9
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan 402
    switchport mode trunk

interface FastEthernet0/10
    switchport access vlan 402
    switchport mode access
    spanning-tree portfast

interface FastEthernet0/11
    switchport access vlan 302
    switchport mode access

interface FastEthernet0/12
    switchport access vlan 150
    switchport mode access
    duplex full

interface FastEthernet0/13
    switchport access vlan 100
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan 250
    switchport mode access
    duplex full

interface FastEthernet0/14
    switchport access vlan 100
    switchport mode access
    duplex full

interface FastEthernet0/15
    switchport mode dynamic desirable

interface FastEthernet0/16
    switchport mode dynamic desirable
Conclusions

! interface FastEthernet0/17
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 15
  switchport mode trunk
duplex full
!
interface FastEthernet0/18
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 15,250
  switchport mode trunk
!
interface FastEthernet0/19
  switchport mode dynamic desirable
!
interface FastEthernet0/20
  switchport access vlan 100
  switchport mode access
!
interface FastEthernet0/21
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 15,250
  switchport mode trunk
!
interface FastEthernet0/22
  switchport access vlan 150
  switchport mode access
duplex full
!
interface FastEthernet0/23
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 250
  switchport mode trunk
!
interface FastEthernet0/24
  switchport access vlan 250
  switchport mode access
carrier-delay msec 0
duplex full
!
interface GigabitEthernet0/1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 75
  switchport mode trunk
!
interface GigabitEthernet0/2
  switchport mode dynamic desirable
!
interface Vlan1
  no ip address
  shutdown
!
ip classless
ip http server
!
!
line con 0
line vty 0 4
  password cisco
  login
line vty 5 15
  login
!
!
End
Appendix- II: Detailed Topology Diagram for the Test (Scenario 2)