Quality of Service Enhancement of a Carrier Supporting Carrier Network using MQCQOS

P.Prabavathi[1], M.Ravindran[2], C.Gokila[3]

{pprabavathi@gmail.com[1,a],mravibsnl@gmail.com[2,b],gokiruby96@gmail.com[3]}

Department of ECE, PSG college of technology, Coimbatore, India[a] AGM, BSNL,Chennai,India[b]

Abstract. Quality of Service (QOS) is the major key element in research nowadays. The rapid development with internet and its associated technologies led the users to easily access the internet. Due to that, demand for network access has increased tremendously. On contrast, this development has increased the demands on ISP's. In order to meet the increasing demands, ISP's employ many technologies based on Service Level Agreements (SLA). Carrier Supporting Carrier (CSC) network based on MPLS VPN is one of the methods used to meet the ISP's requirements. MPLS backbone network will lend its bandwidth to send the customer ISP's traffic to its customers. This in turn increases the traffic load on MPLS networks. This work proposes a QOS enhancement of CSC network using Modular Quality of service Command Line Interface (MQC QOS). Traffic classes are defined and policy maps are employed to apply QOS policies to prioritize the traffic respectively. TELNET and ICMP protocols are considered to analyze the QOS policies and prioritization schemes. Bandwidth sharing will take place according to the priority value assigned to each traffic classes. In this work, highest priority of 30% is given to class (PING) whereas lowest of 10% priority is assigned to traffic class TELNET. According to that, traffic gets prioritized when both traffics are given.

Keywords: ISP's, CSC, MPLS VPN, MQC QOS.

1 Introduction

An ISP (Internet Service Provider) is an organizational network that renders its services to connect customers across the internet. A traditional ISP uses IP network (Internet Protocol) to route packets and establish communication within network boundaries **[D.Grayson.,2009]**. With respect to the IP address associated, IP packets are routed and forwarded from source to destination. Hop by hop routing is carried out with respect to the IP routing table. At each hop, the destination address of the packets are looked up in the IP routing table and then forwarded to the next hop. Increasing demands for network access cannot be satisfied by the traditional IP networks due to the factors such as IP routing table grows extensively in large networks due to look up and routing at each hops **[M.Hossain.,2010].** IP protocol is a connectionless protocol and so it will not support quality of service (QOS) **[Zhang.,2006].** Since number of users utilizing the network has increased rapidly, CSC network model is employed to meet the increasing demands of serving all the customers at the same time. CSC (Carrier Supporting Carrier) is the network model implemented to send one ISP's traffic over another ISP in order to connect geographically separated customer sites **[V.H.Shukla.,2015]**.

ICCAP 2021, December 07-08, Chennai, India

DOI 10.4108/eai.7-12-2021.2314700

When one ISP can't able to provide network access, connection is established through other ISP's network infrastructure. The ISP lending its own service to transport other ISP's traffic is called the backbone ISP or the core network as these ISP's have wholly established connection across the major area. ISP requesting service or access to send its traffic is called customer ISP. And due to that, it is not necessary for the small scale service providers or any customer ISP's to maintain their own backbone network.. In CSC model, interconnections between one ISP to another ISP's customer are established through VPN networks. A Virtual Private Network (VPN) is an encrypted connection method that is used to establish a private network between the authenticated user and the server or network resources securely. The difference with the normal networks and VPN network is that VPN uses virtual connections instead of dedicated physical lines **[Nasser.,2013].**

Extranet based site to site VPN is generally used to connect different autonomous system or individual networks **[Jian CHU.,2008]**. The backbone networks are nowadays an MPLS network. MPLS based VPN is one of the methods of implementing secured virtual private networks. Layer 3 VPN is mostly used to establish connections through MPLS backbones. It uses Virtual Routing and Forwarding (VRF) to route between customer sites and service provider networks **[C.Moberg.,2016]**. MPLS is the data forwarding mechanism with several advantages over traditional IP routing **[Yang.,2015]**. MPLS uses a 32-bit label field that is inserted between layer 2 and layer 3 headers **[S.Tomovic.,2019**].

In an MPLS network, only label swapping will take place instead of routing. The Label Switched Paths (LSP's) are defined by LDP's **[L.Huang.,2018].** All the routers within an MPLS network will forward labels only through LDP's. The experimental bits (3-bit) of the label field will represent the traffic condition per each hops (PHB). EXP bits are considered to implement Quality of Service (QoS) **[J.Andres.,2018]** and classify priority. QOS ensures the network to function at its maximum performance level **[W.Wendong.,2014]**. QOS models are the predefined set of mechanisms and technologies which are used as a solution to treat the network traffic problems **[Eva Ibarrola.,2010]**.

The best effort model was the first and default QOS model existed. This model will only ensure connectivity and check whether packets reached the destination and it is no way responsible to provide any better services. Integrated services model (IntServ) is the model defined next to the best effort model. This QOS model gives a set of guarantee to the network regarding its performance through certain mechanisms used. IntServ QOS model uses a protocol called Resource Reservation Protocol (RSVP) to manage network resources. Resource reservation is the major key parameter considered by this model to establish a good QOS **[S Liu.,2020]**.

MPLS uses differentiated services QOS model which provides many additional possibilities to enhance QOS. QOS across the network can be established according to our necessity based on requirement. It also supports MQC QOS which is one of the command line interface QOS establishment method. This paper is all about QOS enhancement of a CSC network through MQC QOS. Section I gives the basic concepts behind MPLS label forwarding mechanism and swapping. Section II discusses about differentiated services QOS model. Section III proposes the work that is to be implemented followed by results and discussion in section. Finally Section V gives the inference and conclusion followed by references.

MPLS BASIC FORWARDING MECHANISM MPLS is the data forwarding mechanism applied to the traditional IP networks as an enhancement and not as the replacement to IP networks. In IP networks, IP packets are forwarded based on the look up for destination address at each hops whereas in MPLS networks looking up will take place only at Provider Edge (PE) routers. Only two PE routers will be present in an MPLS network. The PE router present at the starting edge of the MPLS network is called Ingress PE router. The Ingress PE router will perform certain operations such as looking up for destination addresses of incoming IP packets, label generation, label mapping, label assignment to IP packets ,etc., Fig.1 shows the label swapping method in MPLS. The P-routers are the Provider routers which can only swap the labels towards the destination address. And the destination address is explicit to all P-routers with assigned labels. Here there is no need for look-up at each hop except at PE hops. The PE router at the end of the MPLS network is called Egress PE router. The egress PE router decodes the IP address from label and routing look up is done for further forwarding. So briefly, in an MPLS network, IP packets are not replaced but inaddition a label is added. Throughout the MPLS network, all further operations to forward the IP address will take place only with respect to labels.

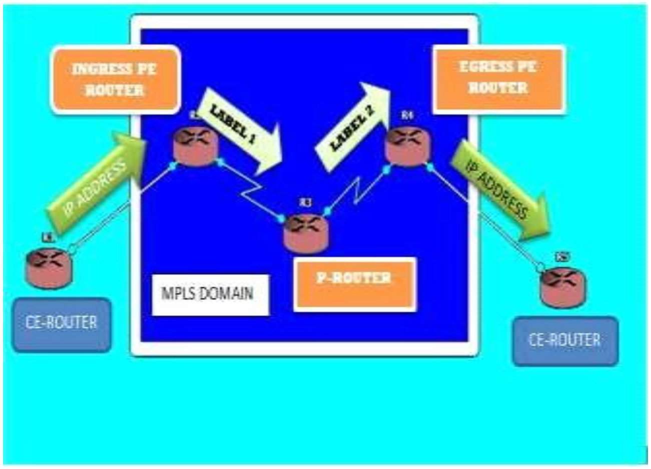


Fig.1. Basic Label swapping in MPLS

2 Differentiated Quality Of Service Model

Differential services QOS model provides different QOS solutions to different types of traffic problems met by the network. This QOS model is advantageous in such a way that it provides possibilities for the users to tailor the QOS according to their necessity. DiffServ QOS model has two major steps such as classifying and marking. DiffServ QOS model differs from other QOS models in such a way that it uses a Differential Services Field (DS Field). This DS field will contain a range of class selectors. Class selectors are defined by the 6-bit Differential Services Code Points (DSCP) value and 2-bit Explicit Congestion Notification (ECN) as the classifier or priority descriptor which would replace the Type of Service (TOS) field of the IP header. ECN mentions the amount of network congestion. Total of 64 DSCP values are available to classify the traffic. With respect to the DS field, Per Hop Behavior (PHB) is determined at each hops which define the traffic class and traffic level for each hops. Some of the most commonly used PHB traffic classes are default forwarding, expedited forwarding, assured forwarding and class selector PHB’s.

3 Proposed Work

QOS enhancement of a Carrier Supporting Carrier (CSC) network using Modular Quality of Service Command Line Interface (MQC QOS) is proposed in this paper. CSC network model is implemented using MPLS VPN. CSC network is implemented to support one ISP's traffic flow over another ISP's backbone. In order to improve the traffic flow across the network, QOS enhancement of the MPLS backbone is proposed using MQC QOS. Fig.2 gives the network topology.

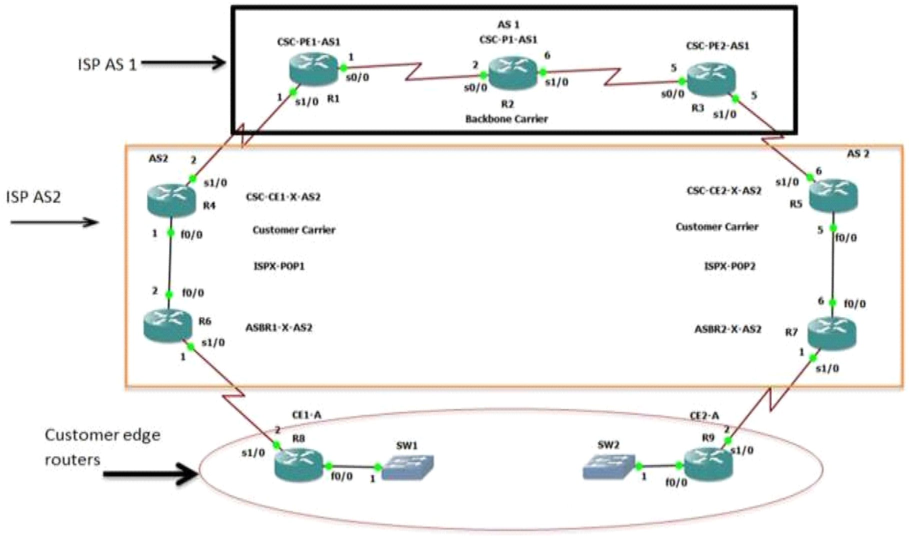


Fig.2. Network topology

4 CSC network using MPL VPN

A CSC network involves two ISP's. One ISP is the backbone network which allows other ISP's traffic to flow through. And this ISP would be the MPLS enabled backbone. Other ISP is the customer ISP which requests bandwidth from backbone ISP. First, the two ISP's are designed individually as an autonomous system. Then the ISP's are interconnected and customer routers are given access to connect across the MPLS backbone using VPN. A set of protocols are used to implement MPLS VPN networks. Any network must employ any of the routing protocols to route the information. Since ISP's have to be implemented, an IP routing protocol is used to route. So firstly, IP protocol is employed across the interfaces connecting the network. With respect to the topological design, network ID's are created and IP address for each routers are assigned respectively. Loopback ID's are also assigned. Next step after IP assignment and configuration is to build two individual autonomous system ISP's. And since both ISP's are based on MPLS, first MPLS configuration is done. Once if MPLS is configured, LDP will also get configured.

The third step is to use any Interior Gateway Protocol (IGP) for routing IP packets within the autonomous system. Open Shortest Path First (OSPF) protocol is used as IGP. The backbone ISP is the first autonomous system built using three routers. The second ISP has two pop sites. Hence, two differently located sites of a same ISP with two routers are implemented. Next in order to connect individual ISP's with each other, an Exterior Gateway protocol (EGP) is used. Border Gateway Protocol (BGP) is the EGP used. BGP is used to connect two autonomous ISP's and to route IP packets across the CSC network. The final step is to connect the customer edge routers to connect across the MPLS backbone through VPN creation. Since the design topology is of layer 3, a layer 3 MPLS VPN (VRF) is used.

4 QOS Enhancement Using MQC QOS

In a CSC model, there is a need for backbone ISP to transport other ISP's traffic additionally. In real time, there may be a chance for traffic problems such as congestion, and loss of packet due to collision. Hence, in order to ensure better traffic flow, QOS enhancement can be done.

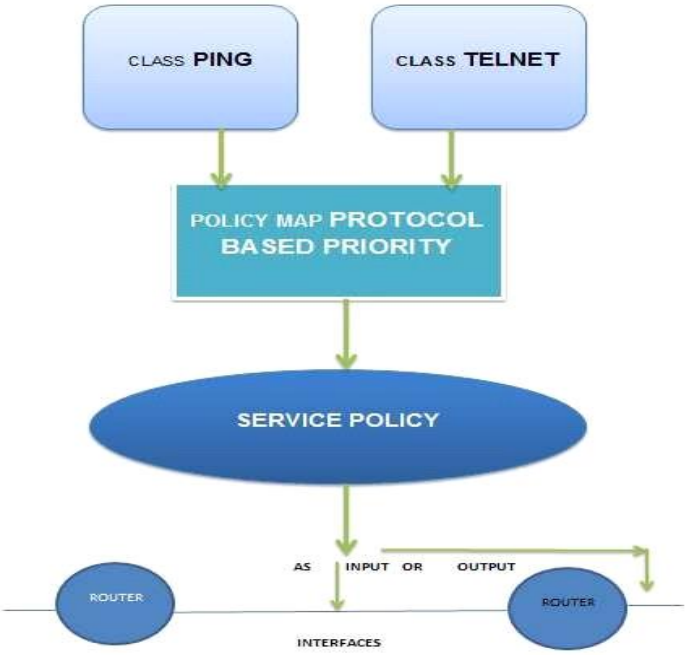


Fig. 3. MQC QOS Implementation steps

MPLS uses differentiated services QOS model and so further QOS enhancement is made possible through diffServ supported QOS model called, MQC QOS. MQC QOS provides the possibility for tailoring QOS according to the requirements. Priority based QOS is supported by MQC QOS. Many network parameters such as bandwidth, traffic type, etc., can be prioritized. MQC QOS is implemented in three steps:

- Class Map
- Policy Map
- Service Policy
- Class Map

Fig.3 gives the QOS configuring steps with class description. Class map is the first step in MQC QOS configuration. Class mapping is defined as the process of classifying and mapping the data traffic as per the QOS requirements. New class is defined and along with that, a set of matching parameters are defined. The traffic data that matches the parameters alone will group under the defined class. The two traffic classes defined here are PING and

TELNET. Matching parameter considered is protocol used and QOS group

- Policy Map

A policy map defines the set of policies that is to be applied to defined traffic classes. A policy map is responsible to apply all the operations and to process data traffic associated with each class respectively. Policy map PROTOCOL BASED PRIORITY is created. And this policy is used to assign different priorities to different traffics in order to allocate varied bandwidth.

- Service Policy

The service policy is used to apply all the policy maps at the interfaces of the required routers. Service policy enables the users to apply policy map as either input or output to the interfaces. Here service policy is applied across two routers which are the customer edge routers (R8, R9). Service policy is applied as input to R8 and as output to R9. It is because, the transition is between R8 and R9, where R8 relies on the whole network topology to transmit to R9.

5 Results And Discussion

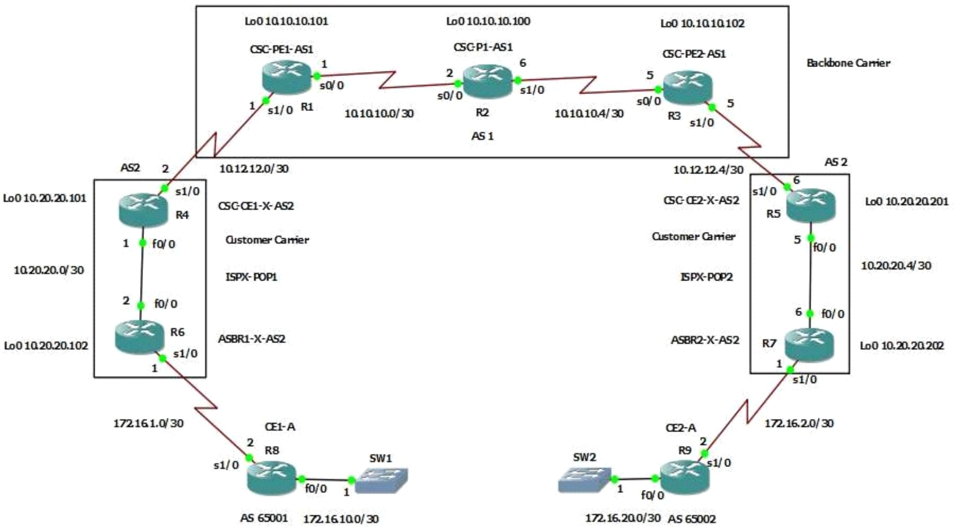
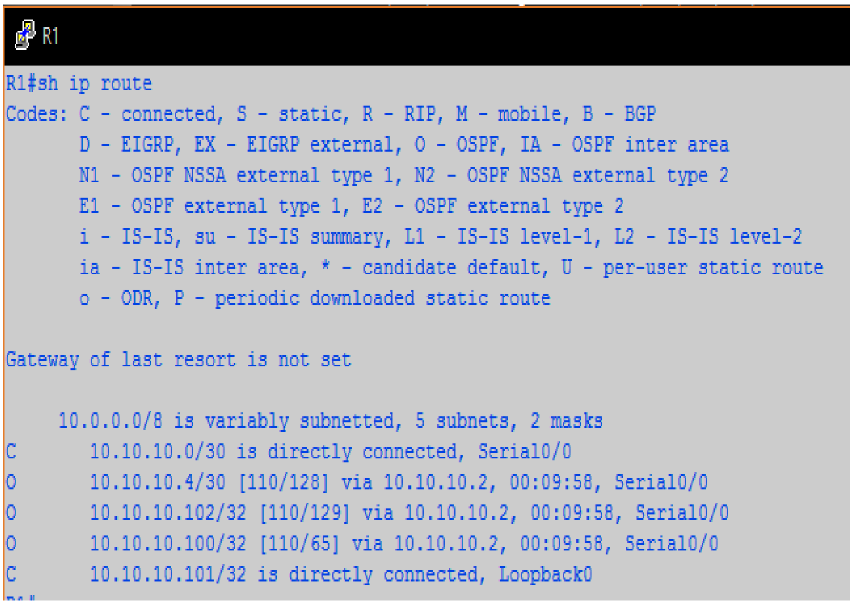


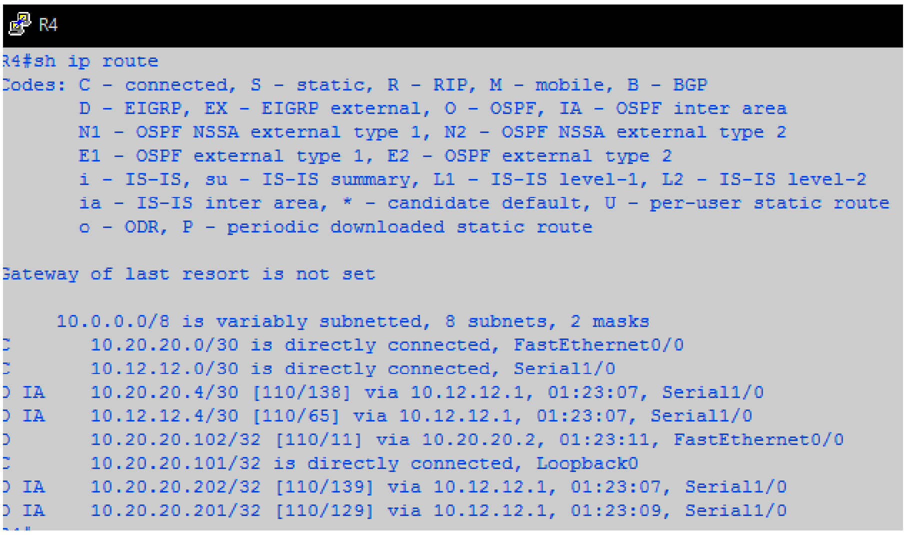
Fig.4. Implementation of CSC network using GNS3



```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.10.10.0/30 is directly connected, Serial0/0
O       10.10.10.4/30 [110/128] via 10.10.10.2, 00:09:58, Serial0/0
O       10.10.10.102/32 [110/129] via 10.10.10.2, 00:09:58, Serial0/0
O       10.10.10.100/32 [110/65] via 10.10.10.2, 00:09:58, Serial0/0
C       10.10.10.101/32 is directly connected, Loopback0
```

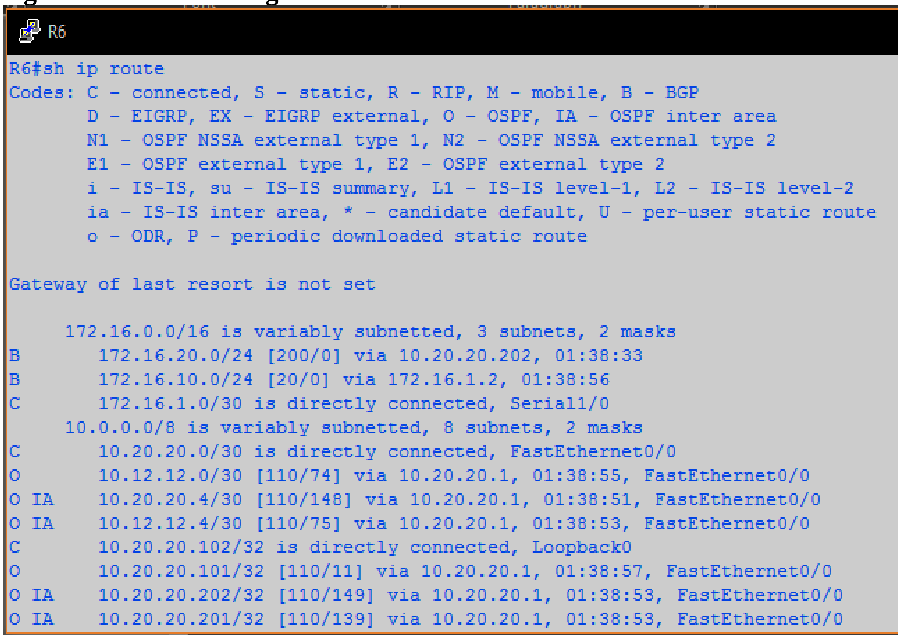
Fig.5. Routes connecting R1.

As per topology given by fig.1, a total of 9 routers are used. First ISP (Autonomous system 1) is designed using 3 routers. Second ISP (AS 2) is designed using 2 routers for each pop site. R1, R2, R3 belongs to one ISP, R4, R5, R6, R7 are routers of ISP 2 whereas R8 and R9 are customer edge routers. Next step after topological design is to assign IP address for each routers with respect to the network ID’s. Each ISP will have individual network ID’s. According to that, first, the interfaces are connected to the routers and then respective IP addresses are configured. Then MPLS is also configured on all routers except at customer routers. From fig.5, it is found that, the router R1 is connected to many routers through either directly or indirectly. The interface serial0/0 is connected directly to the router R1 and then IP configuration is done. The network id is 10.10.10.0/30. And then loopback id 10.10.10.101/32 is directly connected. All other networks are connected via directly connected interface serial0/0. Similarly all other routers are also directly connected by one or two networks and all other networks are indirectly connected via other network interfaces.



```
R4#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C       10.20.20.0/30 is directly connected, FastEthernet0/0
C       10.12.12.0/30 is directly connected, Serial1/0
O IA    10.20.20.4/30 [110/138] via 10.12.12.1, 01:23:07, Serial1/0
O IA    10.12.12.4/30 [110/65] via 10.12.12.1, 01:23:07, Serial1/0
O       10.20.20.102/32 [110/11] via 10.20.20.2, 01:23:11, FastEthernet0/0
C       10.20.20.101/32 is directly connected, Loopback0
O IA    10.20.20.202/32 [110/139] via 10.12.12.1, 01:23:07, Serial1/0
O IA    10.20.20.201/32 [110/129] via 10.12.12.1, 01:23:09, Serial1/0
```

Fig.6. Routes connecting R4

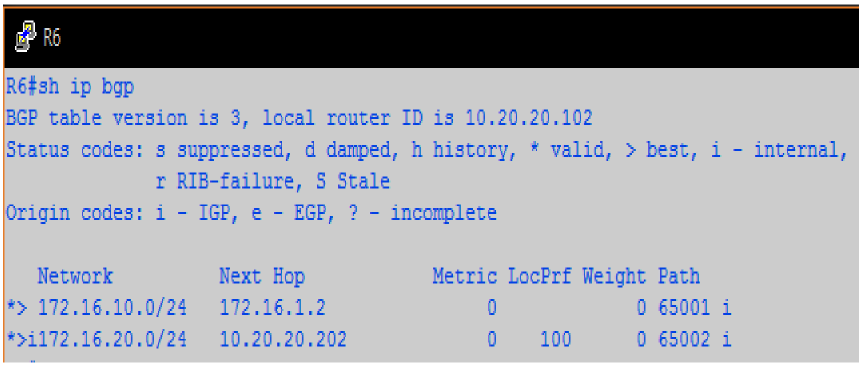


```
R6#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
B       172.16.20.0/24 [200/0] via 10.20.20.202, 01:38:33
B       172.16.10.0/24 [20/0] via 172.16.1.2, 01:38:56
C       172.16.1.0/30 is directly connected, Serial1/0
     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C       10.20.20.0/30 is directly connected, FastEthernet0/0
O       10.12.12.0/30 [110/74] via 10.20.20.1, 01:38:55, FastEthernet0/0
O IA    10.20.20.4/30 [110/148] via 10.20.20.1, 01:38:51, FastEthernet0/0
O IA    10.12.12.4/30 [110/75] via 10.20.20.1, 01:38:53, FastEthernet0/0
C       10.20.20.102/32 is directly connected, Loopback0
O       10.20.20.101/32 [110/11] via 10.20.20.1, 01:38:57, FastEthernet0/0
O IA    10.20.20.202/32 [110/149] via 10.20.20.1, 01:38:53, FastEthernet0/0
O IA    10.20.20.201/32 [110/139] via 10.20.20.1, 01:38:53, FastEthernet0/0
```

Fig.7. Routes connecting R7

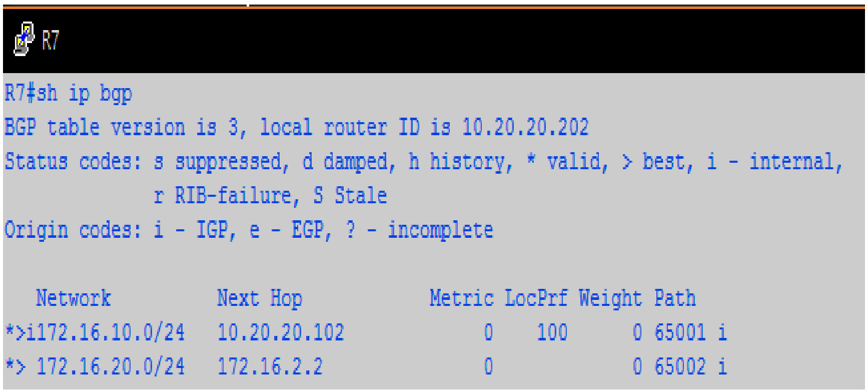
In ISP 1, numbers of sites are one and so routing within the ISP involves only IP protocol. But in ISP 2, there are two pop sites. Those two pop sites have to be connected to each other. But each one is located at different locations. Here, routing is between AS but different locations. Hence, an IGP called OSPF protocol is used to route within AS. From fig 6, other than IP connections, the interfaces are also connected through OSPF. The code IA denotes OSPF IA. The interfaces 10.20.20.102/32, 10.12.12.4/30 and loopback id's 10.20.20.202/32 and 10.20.20.201 are connected through OSPF. Similarly, fig.7 gives the OSPF connection at

R7. In order to route between one AS to other AS (ISP 1 to ISP 2), an exterior gateway protocol called, Border Gateway Protocol (BGP) is used. Fig.8 shows the BGP connections with R6 router. The network 172.16.20.0 is not directly connected to R6. ISP 2 has its pop sites at the other end. Since within ISP connections are already established through OSPF, R4 and R6 are interconnected via OSPF to R5 and R7 respectively. The intermediate routers R1, R2 and R3 are not connected since they belong to other ISP. Now BGP does it by interconnecting two ISP’s through exterior gateway routing ability. And only due to that, the whole connection across the topology is established. Similarly in fig 9, it is shown that, R7 is connected to the other ISP’s routers throughBGP.



```
R6
R6#sh ip bgp
BGP table version is 3, local router ID is 10.20.20.102
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.10.0/24   172.16.1.2               0             0 65001 i
*>i172.16.20.0/24   10.20.20.202             0    100      0 65002 i
```

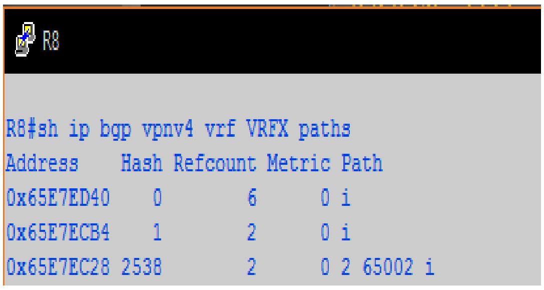
Fig. 8. BGP Connecting AS1 to AS2 (ISP to ISP)



```
R7
R7#sh ip bgp
BGP table version is 3, local router ID is 10.20.20.202
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i172.16.10.0/24   10.20.20.102             0    100      0 65001 i
*> 172.16.20.0/24   172.16.2.2               0             0 65002 i
```

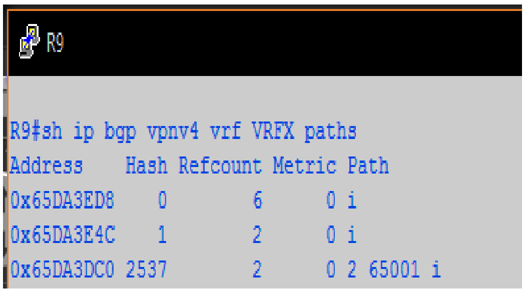
Fig.9. BGP Connecting AS1 to AS2 (ISP to ISP)

VPN is created in order to connect the customer edge routers to the backbone ISP. Layer 3 MPLS VPN is used. It uses virtual routing and forwarding. The vrf name is VRFX. VPN route checking at R1 router is done. At R1, the routes are incomplete. Yet, it connects all the networks except customer edge routers. In fig 10 and 11, VPN route checking at R8 and R9 (Customer routers) is done. It is found that, the VPN establishment is complete and it successfully connects the customer router to the other ISP internally. Similarly VPN path establishment at R9 is also done. The VPN path here connects customer routers 65002 and 65001 to the backbone ISP. Finally, the network topology is complete. And in order to check connectivity between the customer routers, pinging is done. Fig.12 shows that R8 pings with R9 successfully and so end to end connectivity is established throughoutly.



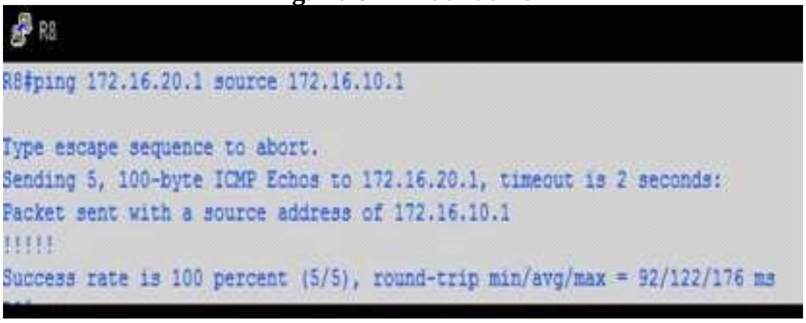
```
R8#sh ip bgp vpnv4 vrf VRFX paths
Address    Hash Refcount Metric Path
0x65E7ED40    0        6      0 i
0x65E7ECB4    1        2      0 i
0x65E7EC28 2538        2      0 2 65002 i
```

Fig.10 VPN Path at R8



```
R9#sh ip bgp vpnv4 vrf VRFX paths
Address    Hash Refcount Metric Path
0x65DA3ED8    0        6      0 i
0x65DA3E4C    1        2      0 i
0x65DA3DC0 2537        2      0 2 65001 i
```

Fig.11. VPN Path at R9

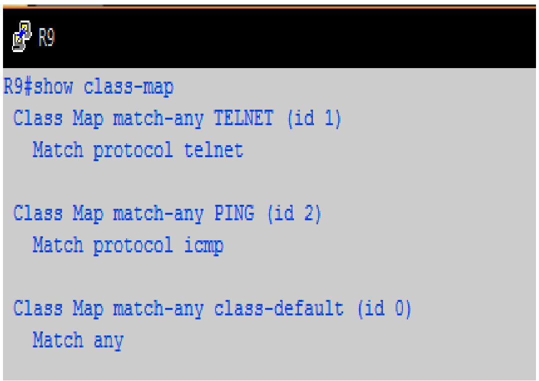


```
R8#ping 172.16.20.1 source 172.16.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.20.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/122/176 ms
```

Fig.12 Pinging two customer edge routers

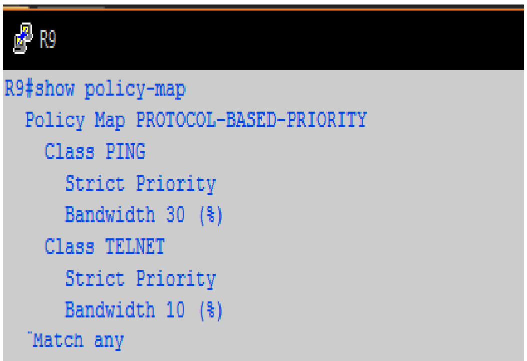
Next, QOS is established in three steps. The first step is to define class maps and matching parameters. Fig.13 shows that two class maps were defined such as TELNET and PING. Since hardware implementation is not done, only ping and telnet traffic alone is considered. Matching parameters considered here is protocol. Under class TELNET, only telnet traffic is grouped. Then under class PING, ICMP tarffic is grouped. Fig.14 gives the policy map configuration. Policy map called PROTOCOL BASED PRIORITY is defined and the policy is generated by giving prioritizing values. For telnet traffic priority is 10% whereas for ping it is 30%. The next step is to apply the policy map across the interfaces.

So for that, service policy is used. Since QOS establishment is to be done across the network, the service policy is to be applied across the starting and at the end of the network. Hence service policy is applied as the input to the interface connecting the R8 router. Then it is applied as output to R9 router interface. Fig 15 gives the service policy output after service policy mapping to the interface. And it is the output when no traffic input is given. (All the packets are zero). And fig.16 gives the service policy output when only ICMP traffic is given. Here the packets received at the TELNET class is 0 because no traffic matches the prescribed class. Any only PING class received packets.



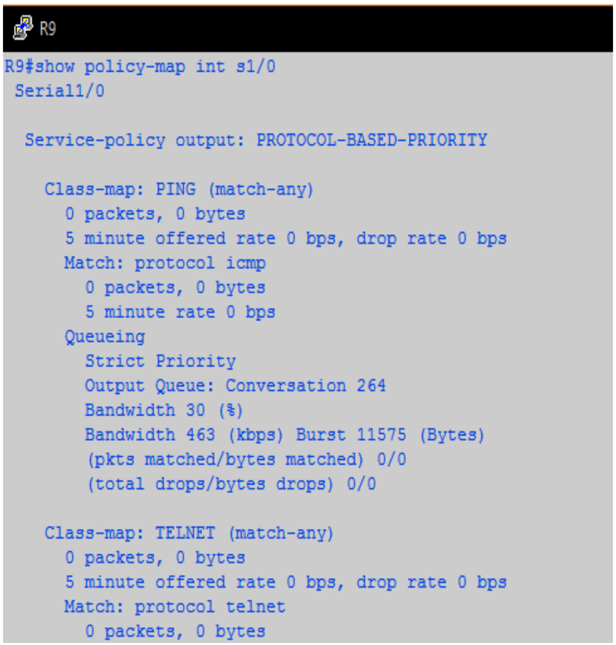
```
R9
R9#show class-map
 Class Map match-any TELNET (id 1)
   Match protocol telnet

 Class Map match-any PING (id 2)
   Match protocol icmp

 Class Map match-any class-default (id 0)
   Match any
```

Fig.13. Class Maps defined



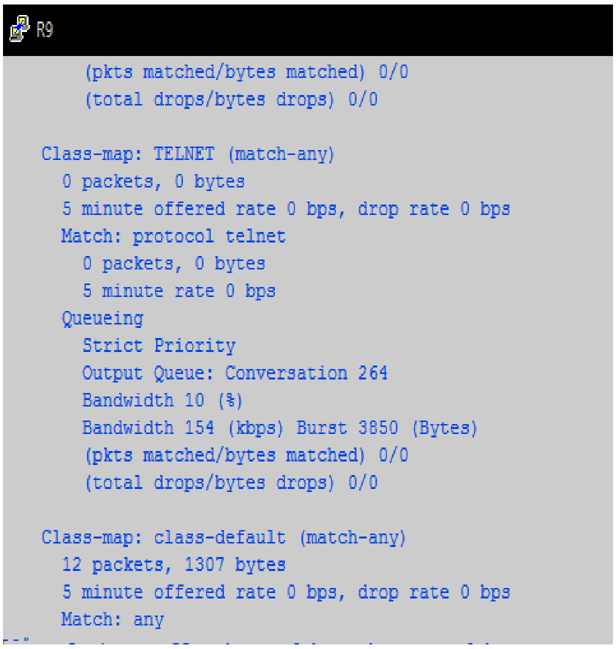
```
R9
R9#show policy-map
  Policy Map PROTOCOL-BASED-PRIORITY
    Class PING
      Strict Priority
      Bandwidth 30 (%)
    Class TELNET
      Strict Priority
      Bandwidth 10 (%)
   Match any
```

Fig.14. Policy Map defined



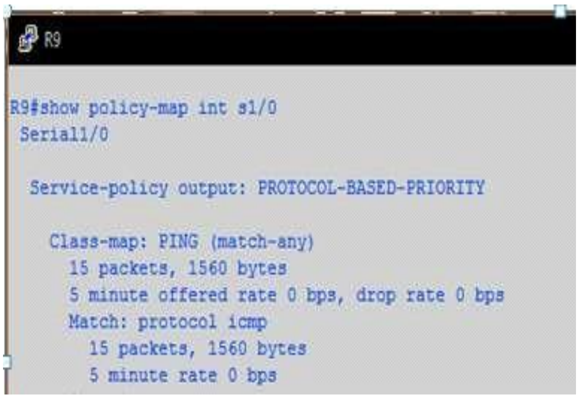
```
R9#show policy-map int s1/0
 Serial1/0

  Service-policy output: PROTOCOL-BASED-PRIORITY

    Class-map: PING (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol icmp
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 30 (%)
        Bandwidth 463 (kbps) Burst 11575 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0

    Class-map: TELNET (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol telnet
        0 packets, 0 bytes
```

Fig.15a. Service policy output when no traffic is given



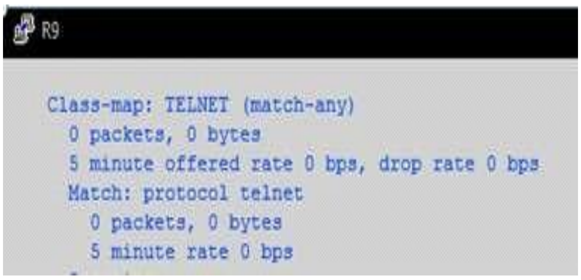
```
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0

    Class-map: TELNET (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol telnet
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 10 (%)
        Bandwidth 154 (kbps) Burst 3850 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0

    Class-map: class-default (match-any)
      12 packets, 1307 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Fig.15b. Service policy output when no traffic is given



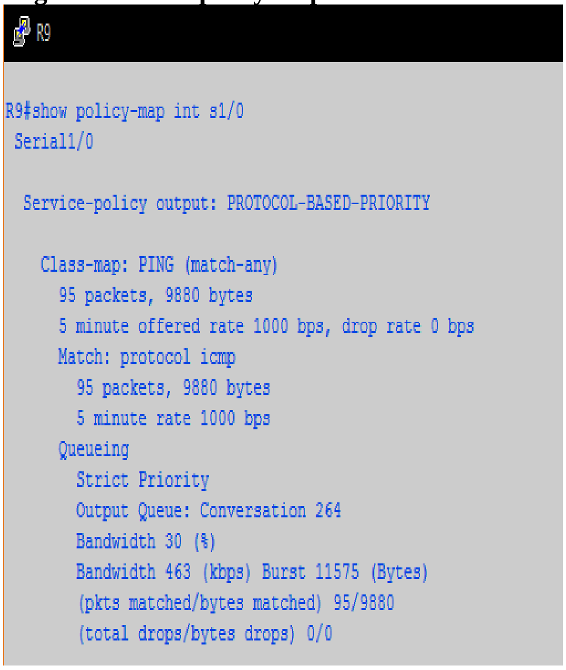
```
R9#show policy-map int s1/0
 Serial1/0

  Service-policy output: PROTOCOL-BASED-PRIORITY

    Class-map: PING (match-any)
      15 packets, 1560 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol icmp
        15 packets, 1560 bytes
        5 minute rate 0 bps
```

Fig.16a. Service policy output at class PING



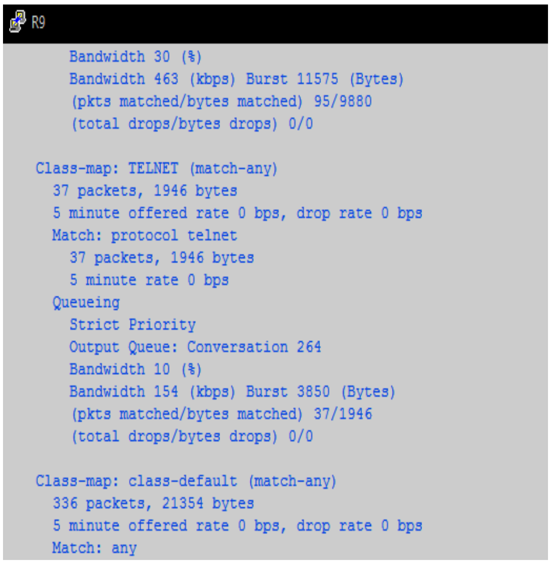
```
    Class-map: TELNET (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol telnet
        0 packets, 0 bytes
        5 minute rate 0 bps
```

Fig.16b. Service policy output at class TELNET



```
R9#show policy-map int s1/0
 Serial1/0

  Service-policy output: PROTOCOL-BASED-PRIORITY

    Class-map: PING (match-any)
      95 packets, 9880 bytes
      5 minute offered rate 1000 bps, drop rate 0 bps
      Match: protocol icmp
        95 packets, 9880 bytes
        5 minute rate 1000 bps
      Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 30 (%)
        Bandwidth 463 (kbps) Burst 11575 (Bytes)
        (pkts matched/bytes matched) 95/9880
        (total drops/bytes drops) 0/0
```

Fig.17a. Class PING after prioritizing



```
R9
        Bandwidth 30 (%)
        Bandwidth 463 (kbps) Burst 11575 (Bytes)
        (pkts matched/bytes matched) 95/9880
        (total drops/bytes drops) 0/0

    Class-map: TELNET (match-any)
      37 packets, 1946 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol telnet
        37 packets, 1946 bytes
        5 minute rate 0 bps
      Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 10 (%)
        Bandwidth 154 (kbps) Burst 3850 (Bytes)
        (pkts matched/bytes matched) 37/1946
        (total drops/bytes drops) 0/0

    Class-map: class-default (match-any)
      336 packets, 21354 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Fig.17b. Class TELNET after prioritizing

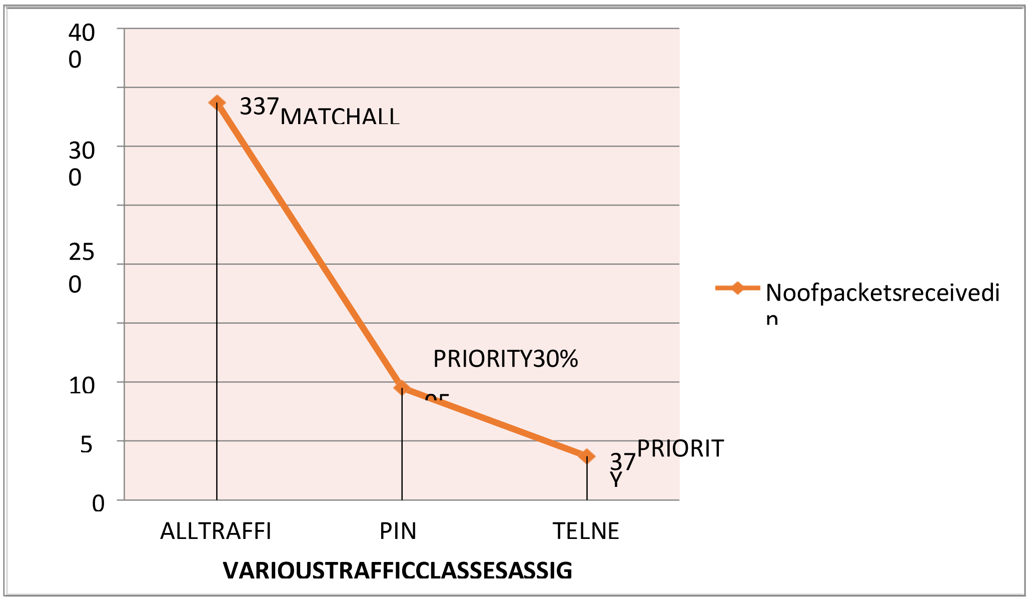


Fig.5.17. Comparison graph on class and priority assignments

Hence from fig.17, traffic got prioritized with respect to priority percent given. The highest priority was given to PING, hence highest no of packet are received in PING class. Total of 336 packets are transmitted and received at R9. The priority percent allocated to PING (ICMP) traffic is 30% and whereas for TELNET traffic 10% is given. Thus finally, QOS is achieved with the network topology implemented. Fig.18 gives the graph on comparison of traffic classes and its priorities. The graph gives the variation in packet flow and packets received amount with respect to priority assigned.

Conclusion

QOS enhancement of a CSC network using MQC QOS has been implemented and their results have been discussed through this work. A CSC network for supporting customer ISP through the backbone ISP is implemented. The backbone ISP and the customer ISP's are MPLS enabled. VPN network is used to connect the customer routers (R8 and R9) across the backbone ISP. Then Quality of Service enhancement was done through MQC QOS. And analysis on priority based traffic matching has been done through two traffic classes PING and TELNET. All these implementations are done through GNS3. Further proposed network topology can be implemented in hardware and in real time applications.

In real time, matching and priority mappings based on MQC QOS can be done to real time application protocols such as HTTP, DNS, FTP, SNMP, etc.,

References

[1] Denise Grayson, Daniel Guernsey, "Analysis of security threats to MPLS virtual private networks", Int. j. Critical Infrastructure Protection 2(2009)146- 153.

[2] MohammadHossein Bateni, Alexandre Gerber , "Multi-VPN Optimization for Scalable Routing via Relaying" , IEEE/ACM transactions on networking,

[3] Oct 2010, Vol. 18, no. 5

[4] Dongli Zhang, Dan Ionescu, "Measurement and Control of Packet Loss Probability for MPLS VPN Services" , IEEE transactions on instrumentation and measurement,oct 2006 vol. 55, no. 5.

[5] Vishal H. Shukla, Sanjay B. Deshmukh, "Implementing QOS Policy in MPLS Network" International Journal of Computer Applications, 2015 (0975 – 8887).

[6] Nasser-Eddine Rikli , Saad Almogari, "Efficient priority schemes for the provision ofend-to-end quality of service for multimedia traffic over MPLS VPN networks" , Journal of King Saud University – Computer and Information Sciences (2013) 25, 89– 98.

[7] Jian Chu , Chin-Tau Lea, "New Architecture and Algorithms for Fast Construction of Hose-Model VPNs" , IEEE/ACM TRANSACTIONS ON NETWORKING, June 2008, Vol. 16, NO. 3,

[8] Carl Moberg , Stefan Vallin "A Two-Layered Data Model Approach for Network Services" ,IEEE Communications Magazine, March 2016, Vol- 54,Issue:3,

[9] Yang, Student Member, Mingwei Xu, Member, "A Hop-by-hop Routing Mechanism for Green Internet", IEEE Transactions on Parallel and Distributed Systems, 2015, Vol 27,Issue:1

[10] Slavica Tomovic, Igor Radusinovic, Member, "Towards a scalable, robust and QoS-aware virtual-link provisioning in SDN-based ISP" , IEEE Transactions on Network and Service Management, 2019

[11] Julian Andres , Caicedo-Muñoz, "QoS-Classifier for VPN and Non-VPN traffic based on time-related features" , Computer Networks 144 (2018) 271– 279.

[12] Liaoruo Huang , Qingguo Shen , "Label Space Reduction based on LSP Multiplexing in MPLS Open flow Hybrid Network" , Computer Communications, Jan 2018,Vol 116, Pg.21-34..

[13] Wang Wendong, Qinglei, "Autonomic QoS Management Mechanism in Software Defined Network" , IEEE China Communications, 2014, Vol 11, Issue:7.

[14] Eva Ibarrola, Fidel Liberal, "Quality of Service Management for ISP : A Model and Implementation Methodology Based on the ITU-T Recommendation E.802 Framework" , IEEE Communications Magazine, Feb 2010.

[15] Shengxin Liu , Carlee Joe-Wong , "Economic Viability of a Virtual ISP" , IEEE/ACM transactions on networking, April 2020, vol. 28, no. 2,

[16] Hossein Lolaee, Mohammad Ali Akhaee, "Analytic model for network resourcemanagement between ISPs and users" , IET Netw., 2017, Vol. 6 Iss. 2, pp. 32-38.