iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VII **Month of publication:** July 2022

DOI: https://doi.org/10.22214/ijraset.2022.45220

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

Implementation of RSVP Subnetwork Bandwidth Manager Using GNS-3

E.V.S.S. Vyshnavi[1], Kalyani Jahnavi[2], Muniganti Rohini[3], J Mounika[4], Patibandla Kavya[5]
[1, 2, 3, 4, 5]*Department of Electronics and Communication Engineering, G. Narayanamma Institute of Technology and Science, Hyderabad, India*

Abstract: ***In order to obtain various quality of services (QoS) when using Internet applications, RSVP, a transport layer protocol, is used to reserve resources in a computer network. Resource reservations are started from the receiver's end and are carried out using Internet protocol (IP).The features of RSVP are, it is a receiver oriented signaling protocol. The receiver initiates and maintains resource reservation. It is used both for unicasting and multicasting. Unicasting is sending data from one source to one destination but multicasting is sending data simultaneously to a group of destination computers. RSVP supports dynamic automatic adaptation to changes in the network. It provides a number of reservation styles. Additionally, it offers assistance for the incorporation of upcoming fashions. RSVP will work fine once you have to make a reservation on the interface between two switches, but what on the off chance that you have got a shared fragment? An example could be a couple of routers that are connected to the same half-duplex Ethernet network. These switches will share the transfer speed so when different switches make an RSVP reservation it's conceivable that we oversubscribe. Subnet Transfer speed Director (SBM) is the QoS component that gives asset administration and arrangement based–admission control for QoS-aware applications utilizing shared media subnets (Ethernet, for case). The SBM is based on an IETF draft that characterizes SBM usefulness and its common execution. We are using GNS3 for this implementation. GNS-3 is Graphical Network Simulator3. It may be an arranged program emulator to begin with, discharged in 2008. It permits a combination of virtual and genuine gadgets, utilized to recreate complex systems.***
Keywords: OSPF-Open Shortest Path First, BGP-Border Gateway Protocol, RSVP SBM-Resource Resercation Protocol Subnetwork Bandwidth Manager, MPLS-TE-MultiProtocol Label Switching Traffic Engineering, QoS-Quality of Service

I. INTRODUCTION

In this project, firstly we implement the network connectivity between different autonomous systems. The network connection is done using routing protocols OSPF and BGP. OSPF is used to connect the interior routers within the autonomous system using commands given in the console. BGP is used to connect two autonomous systems externally. After the network is completely connected then RSVP is implemented. RSVP will work fine when you need to make a reservation on the link between two routers, but for a shared segment it could be a couple of routers that are connected to the same half-duplex Ethernet network. These switches will share the transmission capacity so when different switches make an RSVP reservation it's conceivable that we oversubscribe. The switches ought to know approximately all RSVP reservations that are made on this shared portion and that's precisely why we have the DSBM (Assigned Subnetwork Transmission capacity Manager). One of the switches on the shared fragment will be chosen as the DSBM and all other RSVP switches will intermediary their RSVP Way and RESV messages through the DSBM. This way we'll have centralized confirmation control and we won't chance oversubscribing the shared section. Other than being in charge of confirmation control, the DSBM can moreover disperse other data to RSVP switches, for example the sum of non-reservable activity that's permitted within the shared section or the average/peak rate and burst estimate for non-RSVP traffic.

A. Protocols

1) *OSPF:* OSPF is an Internal Gateway Protocol (IGP). It does this by disseminating routing information among routers in a single Autonomous System. SPF, or link-state technology, is the foundation of the OSPF protocol. This is a change from the norm. Traditional internet routing protocols employ the Bellman-Ford basis. The OSPF protocol was created by the Internet Engineering Task Force's OSPF working group. Each element of this database represents a specific router's local state (for example, the router's reachable neighbours and usable interfaces). Flooding is how the router spreads its local state throughout the Autonomous System OSPF enables the grouping of several networks. An area is a term used to describe a cluster like this. The rest of the Autonomous System is unaware of an area's topology. This data concealment allows for a large reduction in routing traffic. Furthermore, routing within the region is decided only by the topology of the area, protecting the area from incorrect routing data.

© IJRASET: All Rights are Reserved |

2) *BGP:* BGP is an exterior gateway protocol (EGP) that allows routers in various autonomous systems to share routing data (ASs). The entire route to each destination is included in the BGP routing information. In order to keep its database of network reachability data current, BGP shares routing information with other BGP systems. Each router has a routing table that determines how packets are routed. The BGP process on the router generates routing table information based on information received from other routers and information stored in the BGP routing information base (RIB), which is a data table kept on a server on the BGP router. The RIB stores information from both directly linked external and internal peers, and updates the routing table when changes occur, based on policies for which routes should be used and what information should be released. If one internet path goes down, BGP provides network stability by ensuring that routers can swiftly adapt to transmit messages through another link. BGP determines routing decisions based on network administrator-configured pathways, rules, and network regulations.
3) *RSVP-SBM:* RSVP is the first major industry-standard protocol for setting up end-to-end QoS across a heterogeneous network dynamically. RSVP allows an application to dynamically reserve network bandwidth over IP. Applications can use RSVP to request a certain degree of QoS for data flow across a network. RSVP does not execute its own routing; instead, it relies on underlying routing protocols to identify where reservation requests should be sent. Wherever reservations are in place, RSVP adapts its reservation to the new paths as routing changes paths to respond to topology changes. RSVP may still use different routing services because of its versatility. Because RSVP uses receiver-oriented reservation requests that merge as they advance up the multicast tree, it can scale to very large multicast groups. RSVP is primarily intended for multicast applications, but it can also establish unicast reservations. With a high number of unicast reservations, however, it does not scale as well. For QoS-aware applications using shared media subnets, the Subnetwork Bandwidth Manager (SBM) provides resource management and policy-based admission control (Ethernet, for example). Any WAN network that has real-time traffic (sometimes known as "sensitive traffic") that needs to be managed is increasingly going to need bandwidth management. Business processes must make judicious use of the constrained Internet resources because they increasingly rely on cloud-based apps. Although there are standalone bandwidth managers, it is more likely that you will have the bandwidth manager integrated into your firewall or multi-wan router because advanced QoS features, which are also a crucial component of bandwidth management, are made possible by having the bandwidth manager capabilities closer to the access side of the network.
4) *MPLS-TE:* In a conventional IP sending worldview, parcels are sent on a per-hop premise where a course lookup is performed on each switch from source to goal. As cited prior, the destination-based sending worldview leads to imperfect utilization of accessible transmission capacity between a match of switches within the benefit supplier arrange. Predominantly, the suboptimal paths are under-utilized in IP networks. To dodge parcel drops due to wasteful utilization of accessible transmission capacity and to supply superior execution, TE is utilized to direct a few of the activities predetermined to take after the ideal way to an imperfect way to empower superior transfer speed administration and usage between a match of switches. TE, hence, relieves transitory clog within the center of the arrangement on the essential or ideal fetched joins.

II. IMPLEMENTATION AND RESULTS

A. *Implementation*

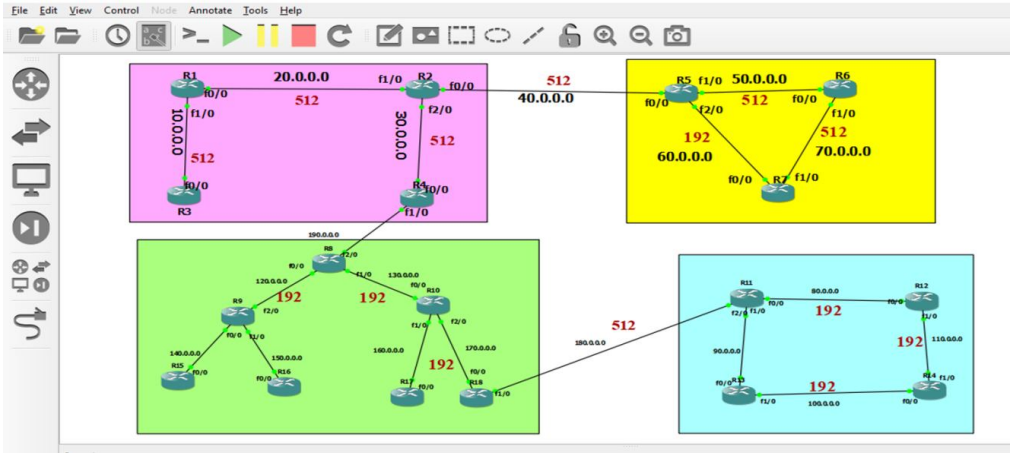


Fig. 1 Topology

1) *Step-1:* We have built a topology with 4 autonomous systems containing a different number of routers in each autonomous system.
2) *Step-2:* We have completely studied how the interface of GNS-3 will work and what are the various components and devices in the software.
3) *Step-3***:** We have first constructed the first autonomous system with 4 routers as shown in our topology and we have given the ip addresses to the routers.
4) *Step-4:* Then we have given connections to those routers using the wire in the GNS-3 software.
5) *Step-5:* Now we have used the Interior Routing Protocol to connect the routers inside the same autonomous system.
6) *Step-6:* The Interior Routing Protocol which we have used in our topology is OSPF that is Open Shortest Path First.
7) *Step-7:* Open Shortest Path First is the protocol which connects all the routers in an autonomous system.
8) *Step-8:* After implementing the interior routing protocol, our next work is to connect the routers in different autonomous systems.
9) *Step-9:* We used exterior routing protocol to connect the routers of different autonomous systems. There is only one exterior routing protocol in routing protocols.
10) *Step-10***:** We used Border Gateway Protocol to connect the routers in different autonomous systems.
11) *Step-11:* After implementing BGP, the complete topology is interconnected with all the routers in the topology.
12) *Step-12:* After this we have imported a firefox appliance into our topology for the real time working model
13) *Step-13:* We have also connected the firefox appliance to NAT. This made us to browse various websites using firefox appliances.
14) *Step-14:* After this we have chosen router 2 as RSVP subnetwork bandwidth manager and assigned the bandwidths to the links of the routers.
15) *Step-15***:** Now there are some benefits of RSVP subnetwork bandwidth manager which gives us extra information about the rate, burst and peak of the data descriptors.
16) *Step-16:* Using RSVP subnetwork bandwidth manager we have reserved some bandwidths to the links from R2 to R5 512 kbps and R5 to R6 512 kbps and so on.
17) *Step-16:* Using RSVP subnetwork bandwidth manager we have reserved some bandwidths to the links from R2 to R5 512 kbps and R5 to R6 512 kbps and so on.
18) *Step-18:* First we have performed static MPLS-TE using the tunnel formation by giving the source and destination addresses along with the next router or device address

B. Results

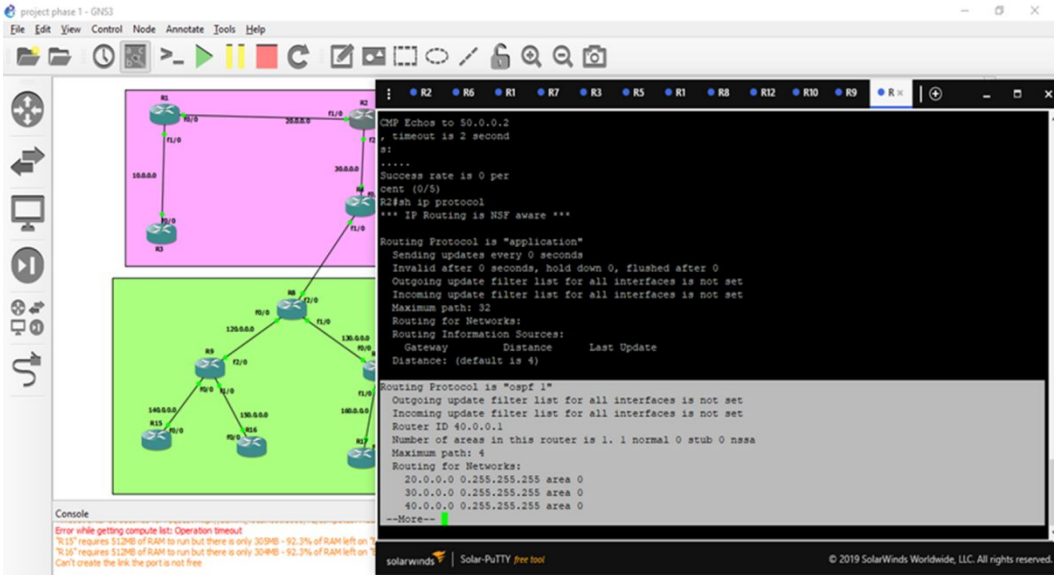


Fig.2 Result showing the protocol is OSPF for a router as the OSPF is implemented in that router

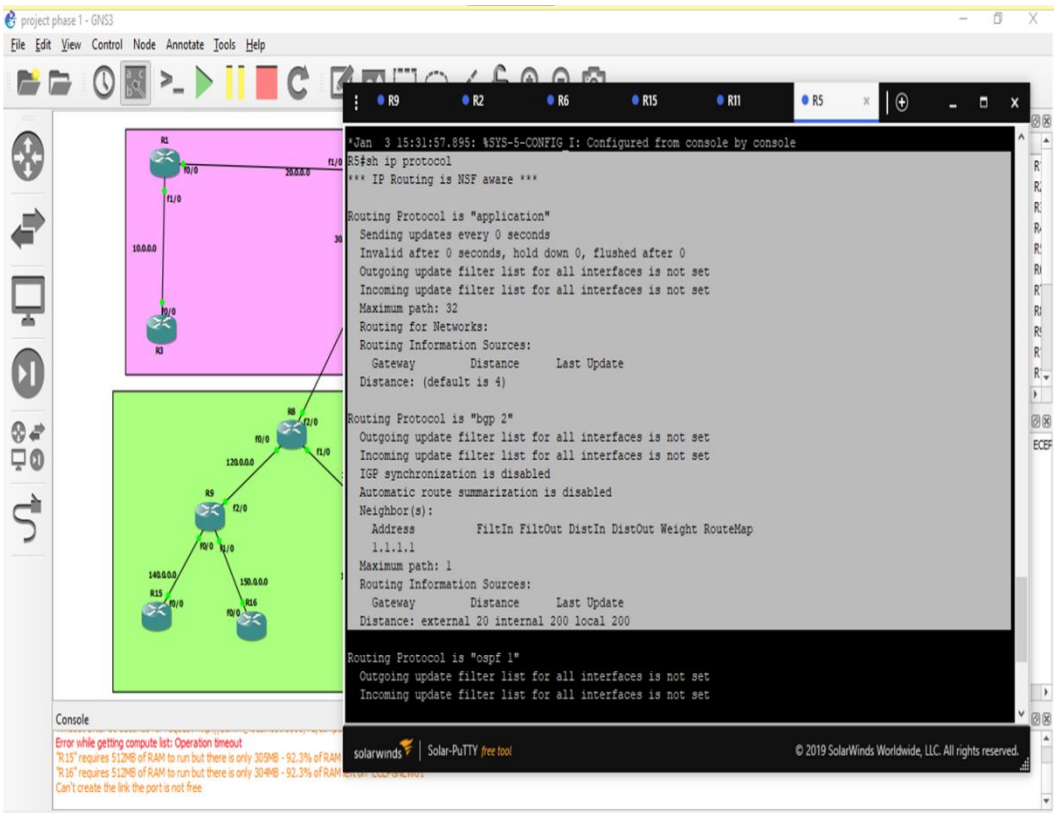


Fig.3 Result showing that the protocol is BGP as BGP is implanted between the two autonomous systems

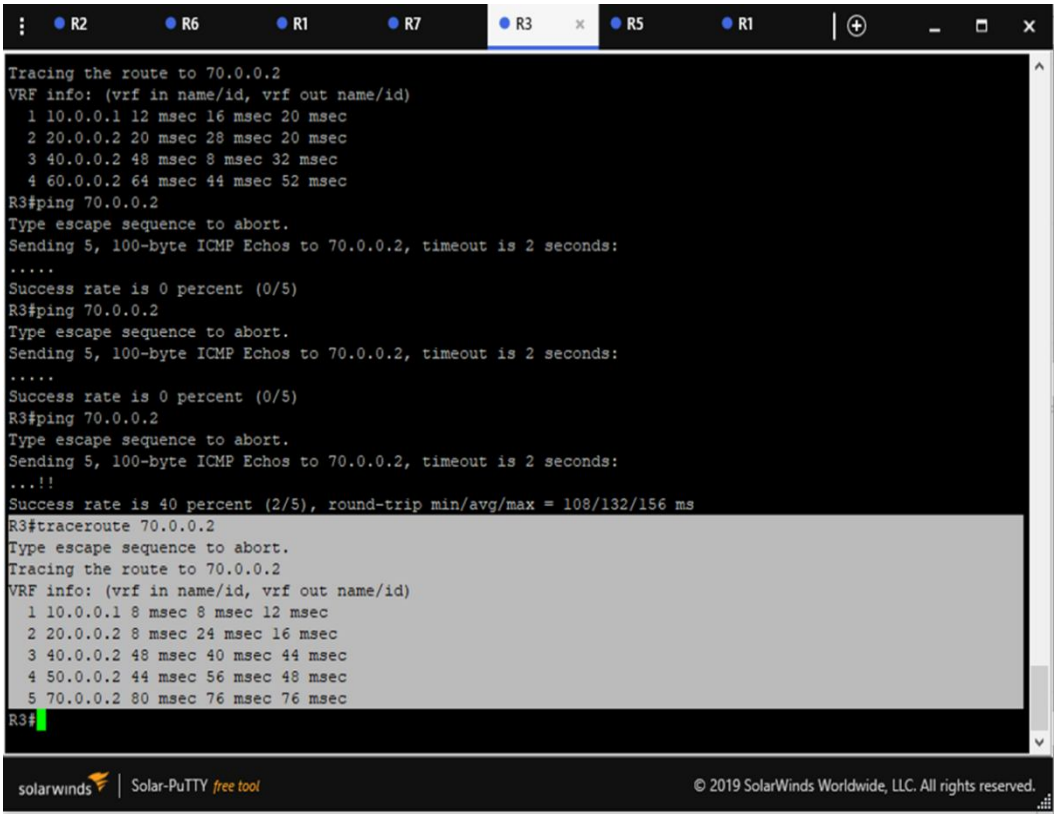


Fig.4 Result of BGP choosing the best path which is not busy when no path is busy

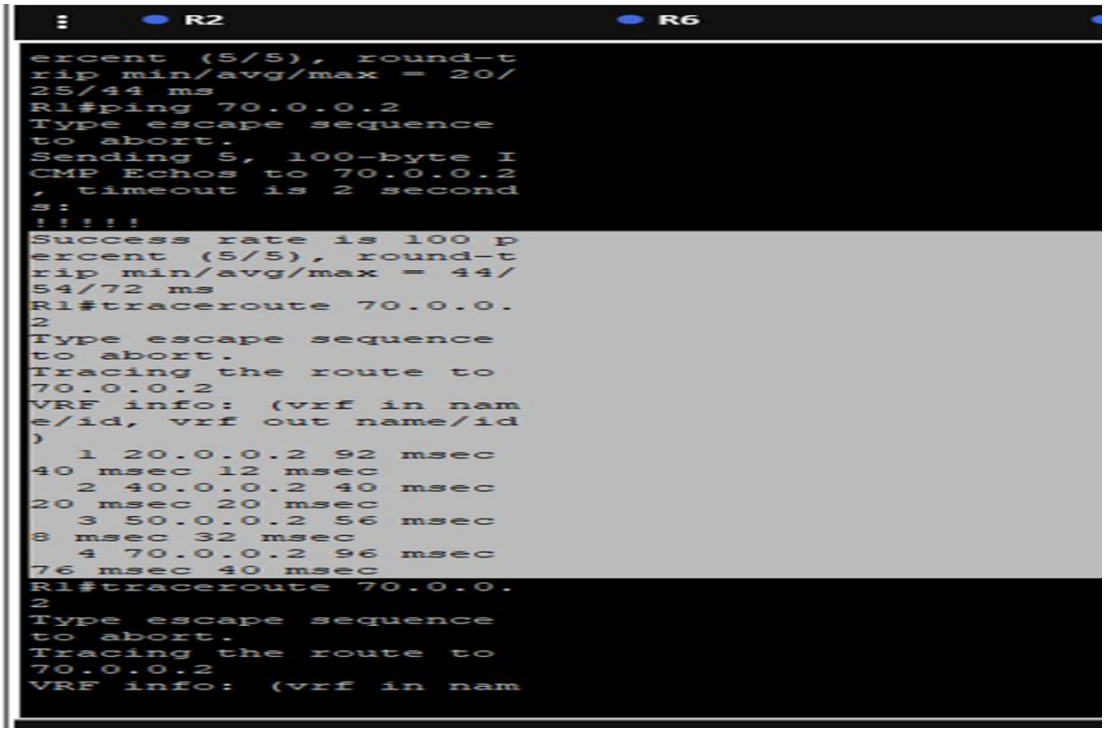


Fig.5 Result of the BGP choosing another path in another router when the path between R5 and R7 is busy

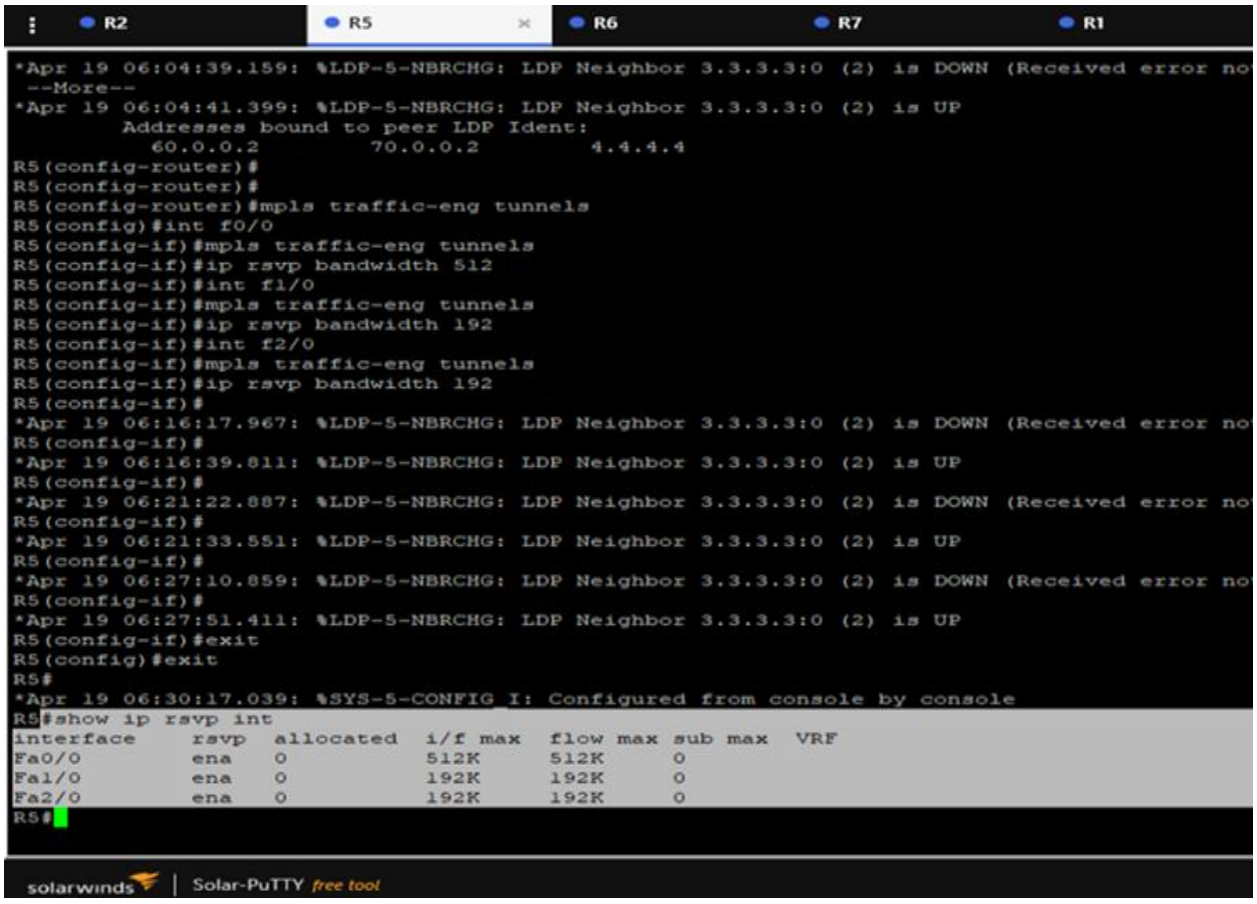


Fig. 6 Reservation of Bandwidth of the links between the routers using RSVP

© IJRASET: All Rights are Reserved |

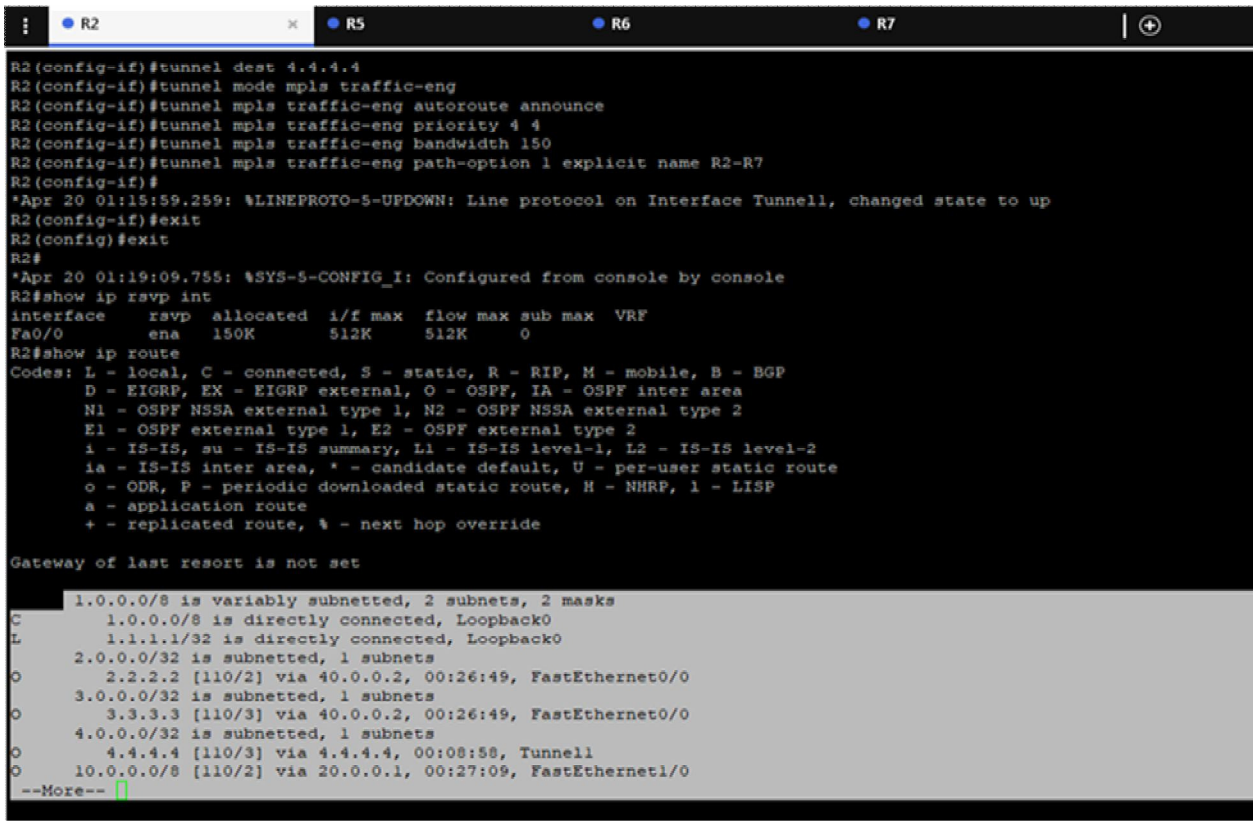


Fig. 7 Formation of tunnel in static MPLS-TE using the pre-determined path and given next device address

Fig. 8 Output depicting that the tunnels of MPLS-TE are unidirectional because they can only allocate bandwidth to those links which are in unidirectional

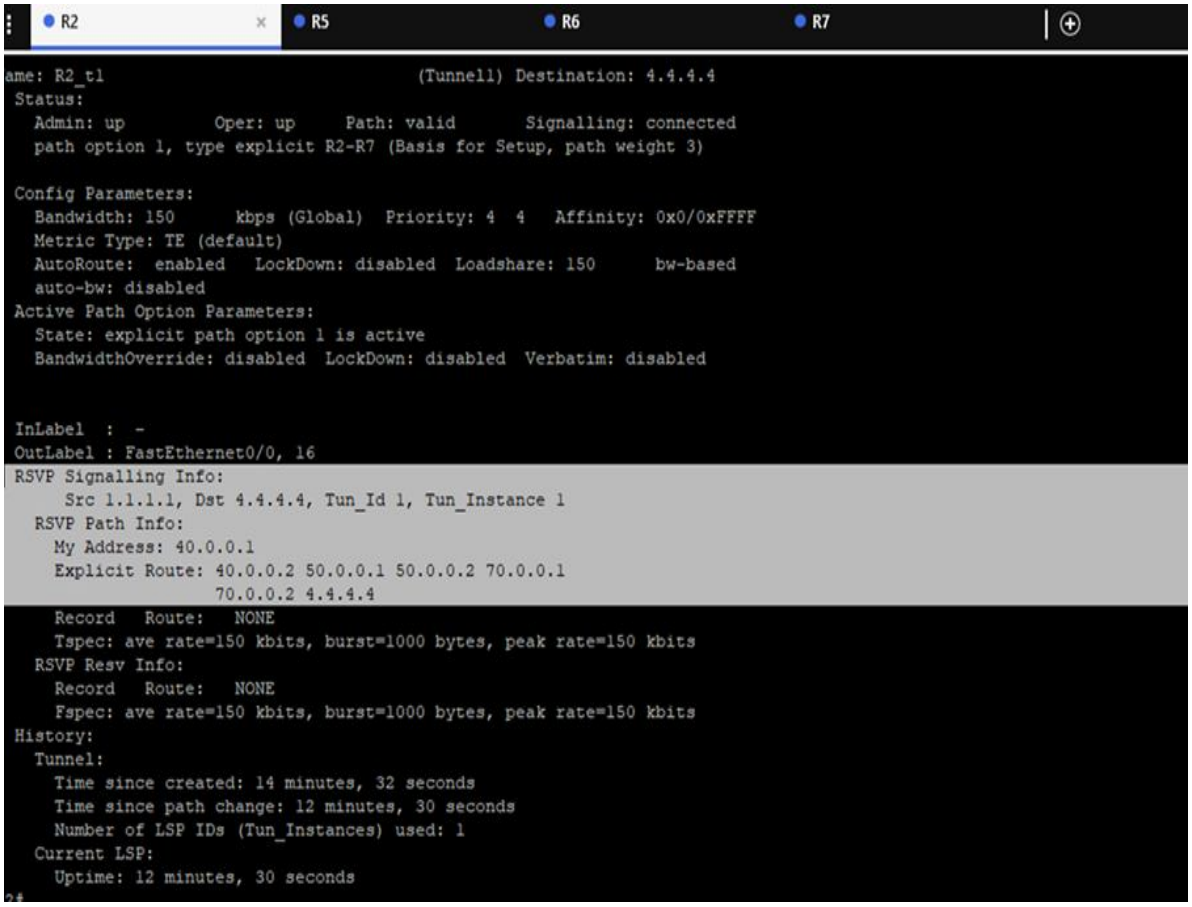


Fig. 9 The route consists of the router or devices address in static MPLS-TE which is a pre-determined path and does not have decision making.

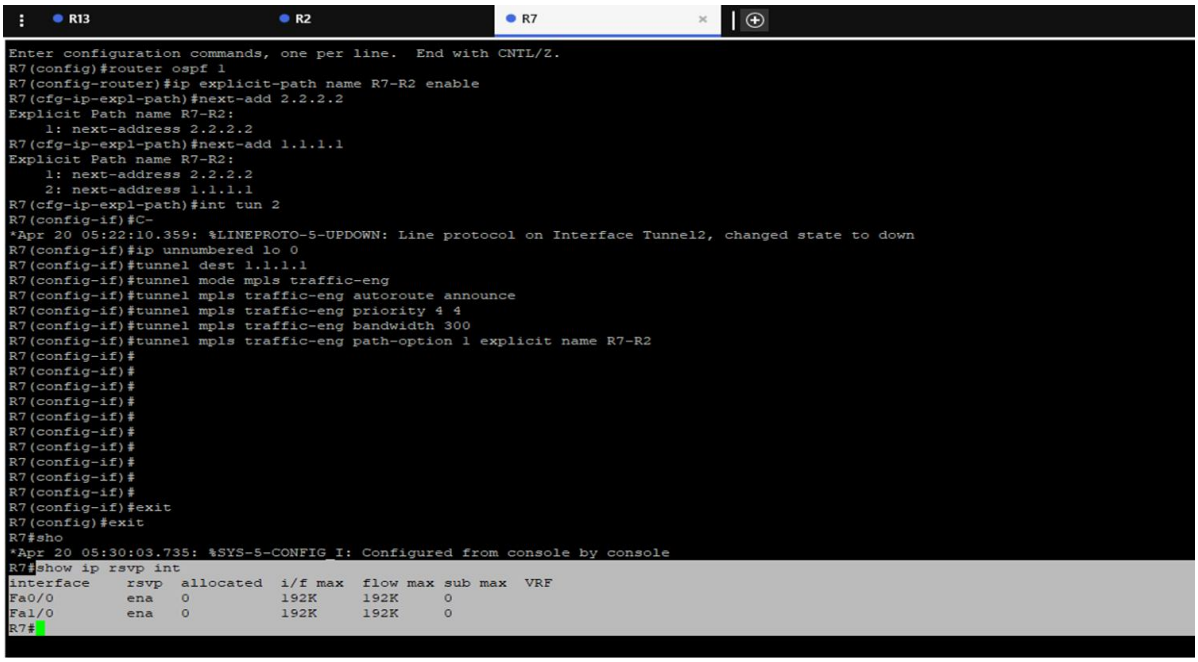
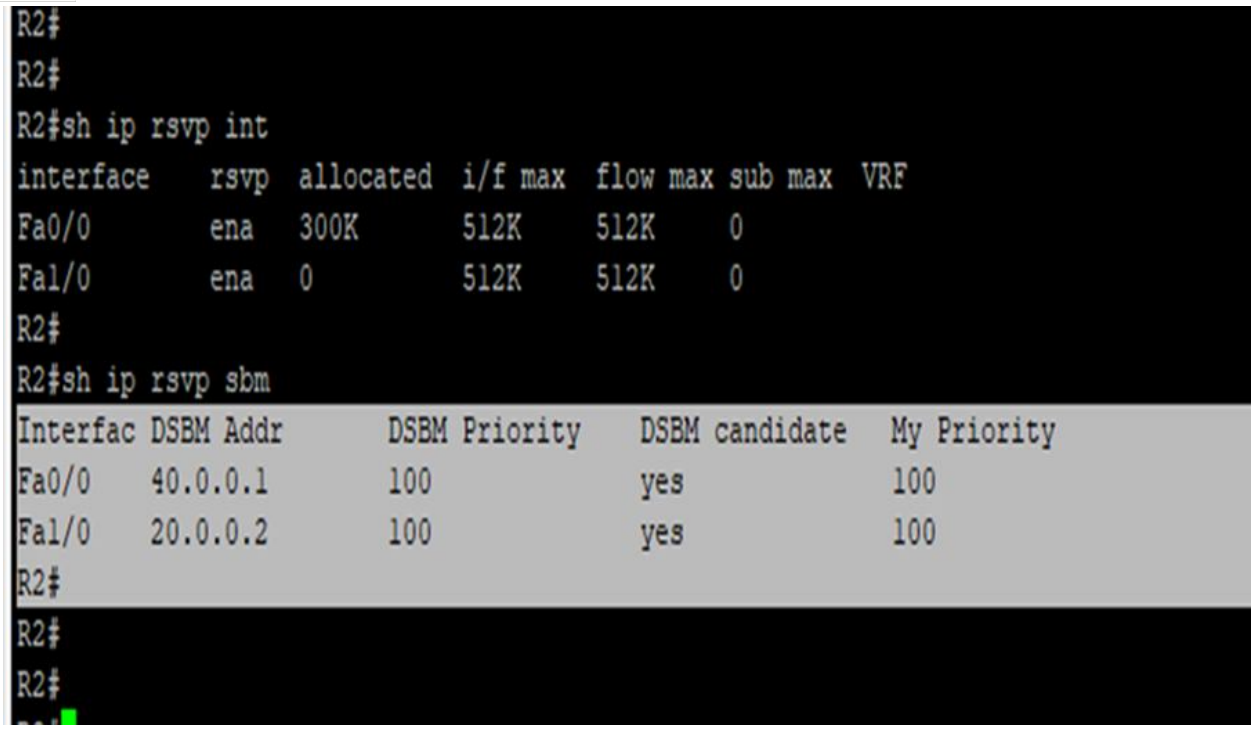
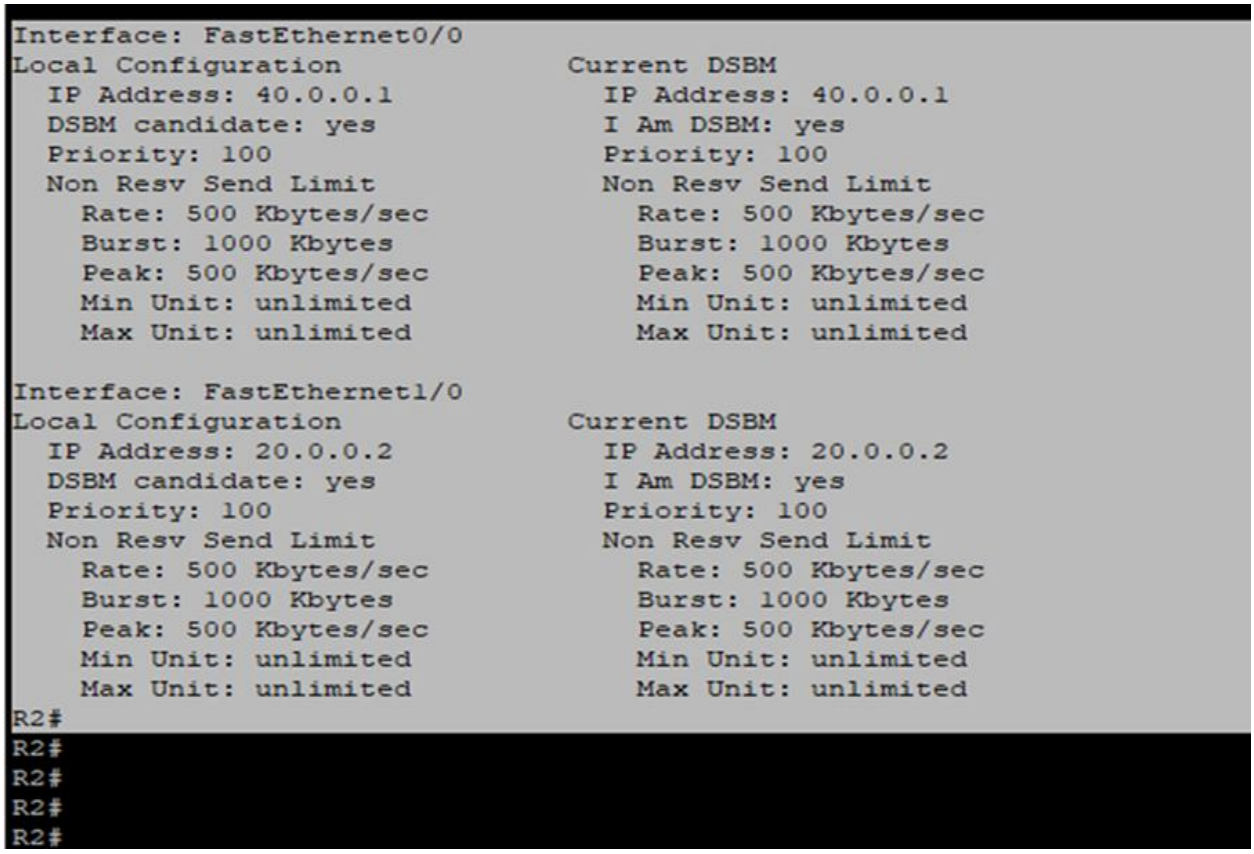


Fig. 10 The tunnel is not formed when the bandwidth exceeds the link bandwidth because the application bandwidth must be less than allocated bandwidth



```
R2#
R2#
R2#sh ip rsvp int
interface    rsvp  allocated  i/f max  flow max sub max  VRF
Fa0/0        ena   300K       512K     512K     0
Fa1/0        ena   0          512K     512K     0
R2#
R2#sh ip rsvp sbm
Interfac DSBM Addr       DSBM Priority    DSBM candidate   My Priority
Fa0/0    40.0.0.1        100              yes              100
Fa1/0    20.0.0.2        100              yes              100
R2#
R2#
R2#
```

Fig.11 Allocation of Bandwidth with subnetwork bandwidth manager and describing the priority for the designated subnetwork bandwidth manager candidate



```
Interface: FastEthernet0/0
Local Configuration                Current DSBM
  IP Address: 40.0.0.1               IP Address: 40.0.0.1
  DSBM candidate: yes                I Am DSBM: yes
  Priority: 100                      Priority: 100
  Non Resv Send Limit                Non Resv Send Limit
    Rate: 500 Kbytes/sec               Rate: 500 Kbytes/sec
    Burst: 1000 Kbytes                 Burst: 1000 Kbytes
    Peak: 500 Kbytes/sec               Peak: 500 Kbytes/sec
    Min Unit: unlimited                Min Unit: unlimited
    Max Unit: unlimited                Max Unit: unlimited

Interface: FastEthernet1/0
Local Configuration                Current DSBM
  IP Address: 20.0.0.2               IP Address: 20.0.0.2
  DSBM candidate: yes                I Am DSBM: yes
  Priority: 100                      Priority: 100
  Non Resv Send Limit                Non Resv Send Limit
    Rate: 500 Kbytes/sec               Rate: 500 Kbytes/sec
    Burst: 1000 Kbytes                 Burst: 1000 Kbytes
    Peak: 500 Kbytes/sec               Peak: 500 Kbytes/sec
    Min Unit: unlimited                Min Unit: unlimited
    Max Unit: unlimited                Max Unit: unlimited
R2#
R2#
R2#
R2#
R2#
```

Fig.12 Data descriptors like max, peak and burst which are giving the extra information regarding the subnetwork bandwidth manager

© IJRASET: All Rights are Reserved |

```
R2#
R2#
R2#
R2#
R2#
R2#
R2#ping 70.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 70.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/36/60 ms
R2#trace 70.0.0.2
Type escape sequence to abort.
Tracing the route to 70.0.0.2
VRF info: (vrf in name/id, vrf out name/id)
  1 40.0.0.2 [MPLS: Label 25 Exp 0] 12 msec 16 msec 24 msec
  2 60.0.0.2 36 msec 32 msec 32 msec
R2#
R2#
```

Fig.13 The route suggested by BGP and OSPF before dynamic MPLS-TE is the shortest path which does not include decision making

```
  InLabel  :  -
  OutLabel : FastEthernet0/0, 28
  RSVP Signalling Info:
       Src 1.1.1.1, Dst 4.4.4.4, Tun_Id 1, Tun_Instance 20
    RSVP Path Info:
      My Address: 40.0.0.1
      Explicit Route: 40.0.0.2 50.0.0.1 50.0.0.2 70.0.0.1
                      70.0.0.2 4.4.4.4
      Record   Route:   NONE
      Tspec: ave rate=300 kbits, burst=1000 bytes, peak rate=300 kbits
    RSVP Resv Info:
      Record   Route:   NONE
      Fspec: ave rate=300 kbits, burst=1000 bytes, peak rate=300 kbits
  History:
    Tunnel:
      Time since created: 6 minutes, 52 seconds
      Time since path change: 4 minutes, 9 seconds
      Number of LSP IDs (Tun_Instances) used: 20
    Current LSP:
      Uptime: 4 minutes, 9 seconds
R2(config)#
R2(config)#
```

Fig. 14 The route of the tunnel formed by dynamic MPLS-TE is formed by the own decision making of dynamic MPLS-TE.

© IJRASET: All Rights are Reserved |

C. Advantages And Disadvantages

1) Advantages

GNS-3 is a free software. It is an open-source software. It has no monthly or yearly license fees. It has no limitation on the number of devices supported (the only limitation is your hardware: CPU and memory). OSPF supports both IPv4 and IPv6 routed protocols. It provides unlimited hop counts. It provides trigger updates for fast convergence. It provides a loop-free topology using the SPF algorithm. It is run-on most routers. It is a Classless protocol. It transports and maintains traffic and policy control parameters that are opaque to RSVP. It is not a routing protocol but works with current and future routing protocols.It is highly efficient. BGP is implementable on a large scale.

2) Disadvantages

Cisco images need to be supplied by the user (download from Cisco.com, or purchase VIRL license, or copy from physical device). OSPF requires a very intensive processor. It maintains multiple copies of routing information,so the amount of memory needed increases. It can be logically segmented using areas. It is not easy to learn like some other protocols. Route selection and stability the shortest path may not have available resources,and the active path may go down. Setup time of an application cannot start transmitting until the reservation has been completed. BGP is not stable.

III. FUTURE SCOPE

This project is helpful for using the protocols in real-time applications. This helps to reduce the cost of routers and implementing the protocols in the real time. Because it helps to trial the different topologies and different combination of autonomous systems in the software. When the topology and the protocols are decided then we can intiate the real time project.

IV. CONCLUSIONS

Graphical Network Simulator-3 (shortened to GNS3) software is used for building the topology and for its implementation. After building the topology with a different number of routers and then the ip addresses have been assigned to each of them respectively. The interior routing protocol i.e, Open Shortest Path First (OSPF) is used to connect the routers within the same autonomous system. The exterior routing protocol i.e Border Gateway Protocol (BGP) is used to connect different autonomous Systems. OSPF is implemented and observed that routers in the same Autonomous System can communicate in OSPF and also implemented BGP and observed that two different Autonomous Systems can communicate with each other. Firefox appliances are imported to our topology and connected to the NAT. Our college website is opened using this. After getting the complete connectivity of the network, the RSVP subnetwork bandwidth is chosen to be router 2. Then using that router, the bandwidth is reserved to the links of the network. Then MPLS-TE is implemented using the RSVP subnetwork bandwidth manager. There are two types of MPLS-TE. They are static MPLS-TE and dynamic MPLS-TE. In static MPLS-TE, there are some disadvantages like a tunnel will not be formed if the allocated bandwidth is greater than the reserved bandwidth. The other point is that static MPLS-TE only follows the predetermined path. In dynamic MPLS-TE, there is a capability of decision making. Here the tunnel will be formed in that route only where the bandwidth is sufficient. We have analyzed that in dynamic MPLS-TE, the quality of service of the application will be improved as it makes its own decision in the formation of the tunnel.

V. ACKNOWLEDGMENT

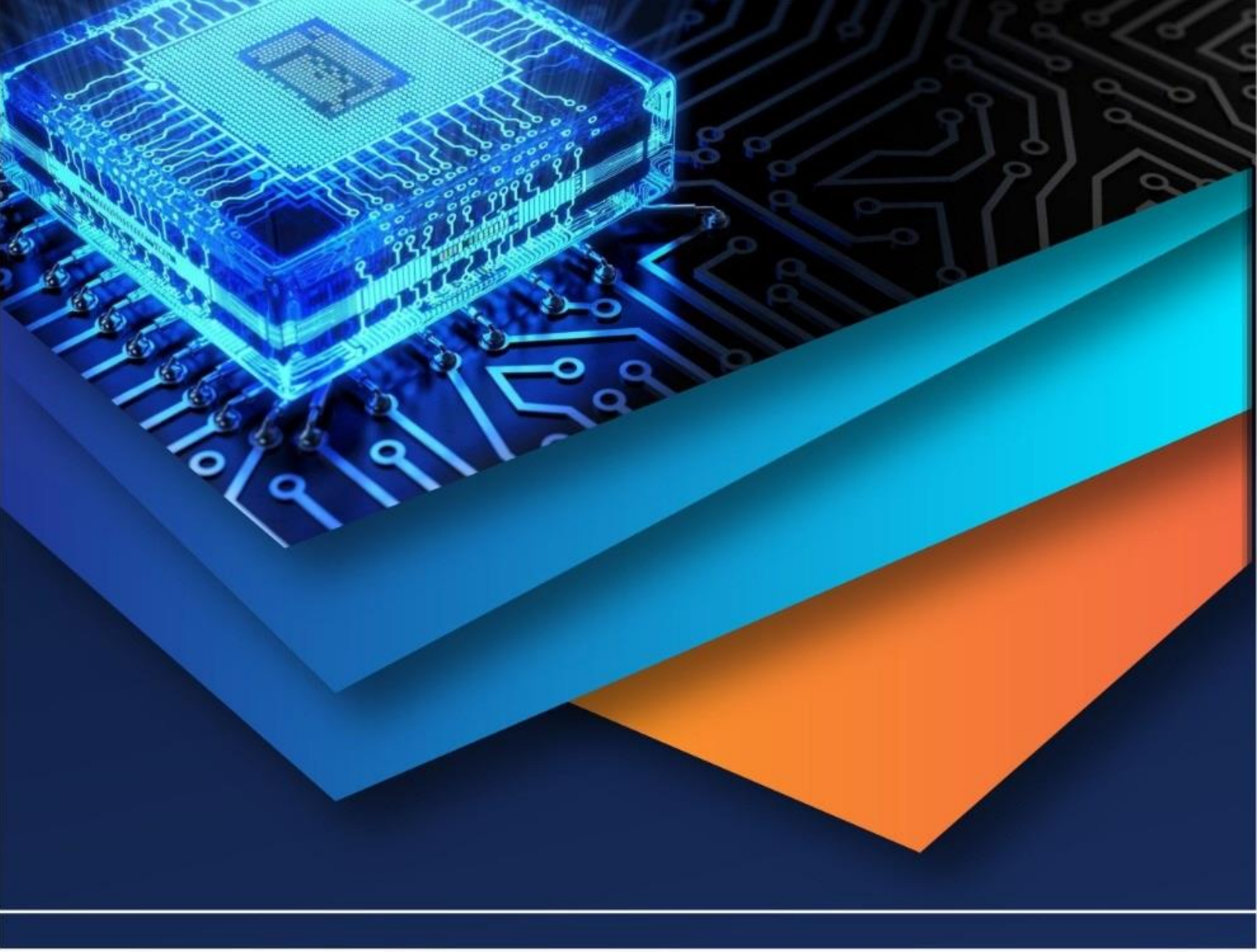
It is our proud privilege to release the feelings of our gratitude to several people who helped us directly or indirectly to complete this project work. We express our heartfelt indebtness and owe a deep sense of gratitude to our guide E.V.S.S. Vyshnavi, Asst.Professor, Department of Electronics and Communication Engineering for her sincere guidance in completing the project. Also, we extend our gratitude to our project coordinator N.Krishna Jyothi, Asst. Professor, Department of Electronics and Communication Engineering who has been very kind and patient while suggesting the outlines of this project and correcting the documents of the same with attention and care.We are extremely thankful to Dr.B.Venkateshulu, Head of Department of Electronics and Communication Engineering for providing us an opportunity to present our project on “Implementation of RSVP subnetwork bandwidth manager using GNS-3”.We would like to express our special thanks to Dr.K.Ramesh Reddy, Principal, G.Narayanamma Institute of Technology & Sciences, our teaching and non-teaching faculty without whom this project would have been a distant reality.Finally, we would also like to extend our thanks to our parents and all our friends who have contributed to the preparation of this project. We will be indebted to them.

© IJRASET: All Rights are Reserved |

REFERENCES

[1] https://www.javatpoint.com/border-gateway-protocol
[2] https://en.wikipedia.org/wiki/Open_Shortest_Path_First.
[3] https://www.techtarget.com/searchnetworking/definition/BGP-Border-Gateway-Protocol
[4] http://it-certification-network.blogspot.com/2008/12/disadvantages-of-using-rsvp.html
[5] https://argusrad.com/wp-content/uploads/formidable/6/bgp-protocol-advantages-and-disadvantages.pdf
[6] https://www.geeksforgeeks.org/border-gateway-protocol-bgp/
[7] https://en.wikipedia.org/wiki/Resource_Reservation_Protocol
[8] https://ipsit.bu.edu/sc546/sc441Spring2003/rsvp/RSVP.htm#:~:text=A%20second%20advantage%20to%20using,at%20a%20designated%20constant%20interval.
[9] https://www.juniper.net/documentation/us/en/software/junos/mpls/topics/topic-map/mpls-traffic-engineering-configuration.html
[10] https://www.mushroomnetworks.com/blog/look-bandwidth-managers/
[11] https://www.researchgate.net/publication/2490818_Bandwidth_Management_in_MPLS_Networks

© IJRASET: All Rights are Reserved |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)