



Networkforyou

Subscribe to our
You Tube Channel



Networkforyou



**Welcome
To
Network for you
QOS**



Email us:
networkforyou4@gmail.com

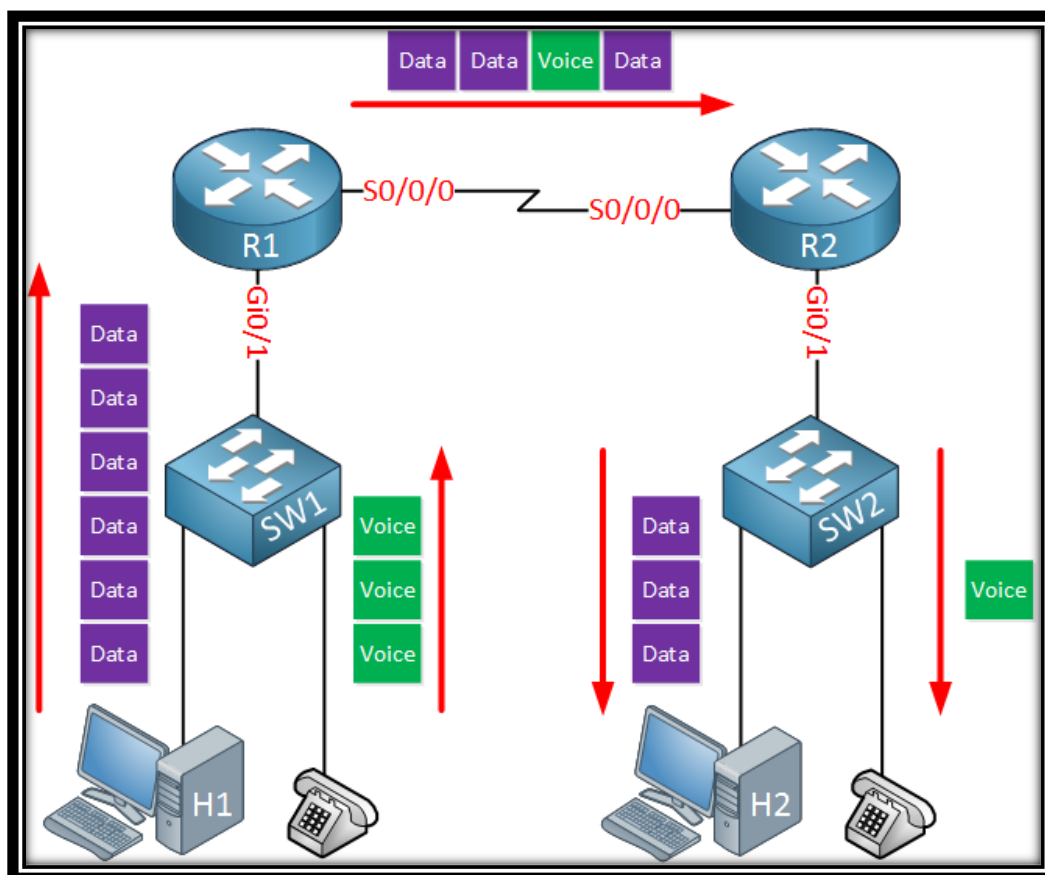
1 of 15

WhatsApp Us : +918143809578



QOS (Quality of Service):

- Quality of Service (QoS) is a feature of routers and switches which prioritizes traffic so that more important traffic can pass first.
- Quality of Service allows us to queue, limit, Filter and make reservations for our network traffic.
- Network devices don't really care about the type of traffic they have to forward.
- Example our switch receives an Ethernet frame, looks for the destination MAC address and forwards the frame towards the destination.
- And for Router also applies same thing like our router receives an IP packet, looks for the destination in the routing table and it forwards packet towards the destination.
- QoS is about using tools to change how the router or switch deals with the different packets.
- Quality of service (QoS) refers to any technology that manages data traffic to reduce packet loss, latency and jitter on the network.
- QoS controls and manages network resources by setting priorities for specific types of data on the network.



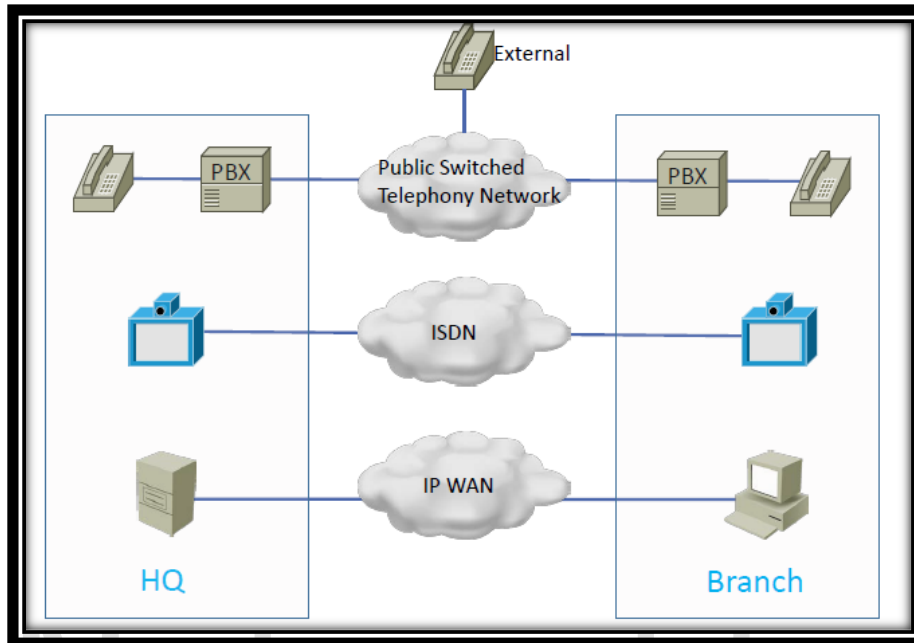
Email us:
networkforyou4@gmail.com

2 of 15

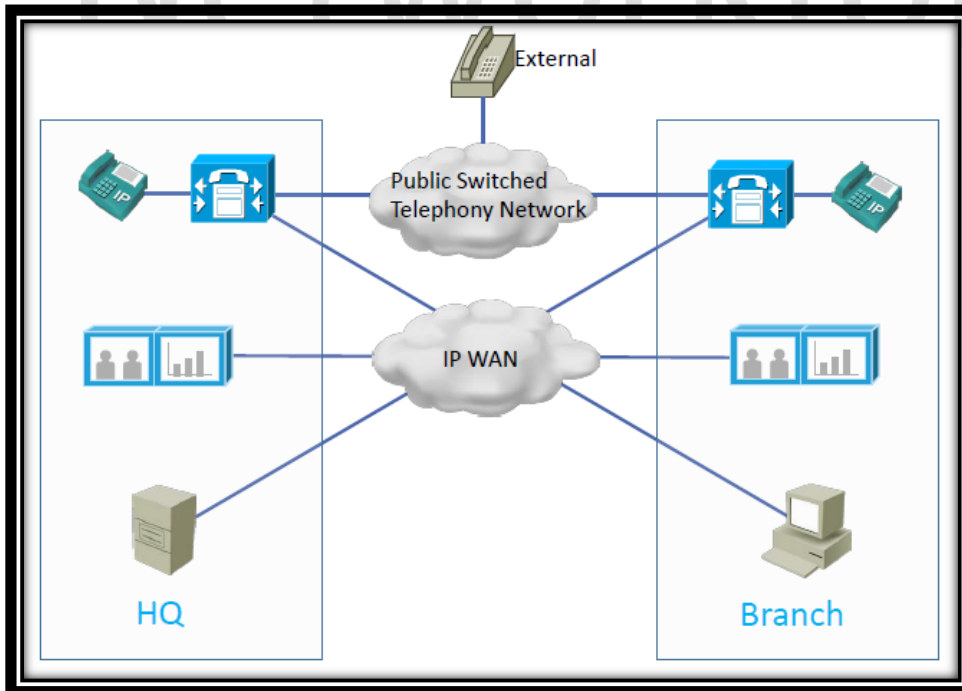
WhatsApp Us : +918143809578



Dedicated Voice, Video and Data Networks:



Converged Networks:



Email us:
networkforyou4@gmail.com

3 of 15

WhatsApp Us : +918143809578



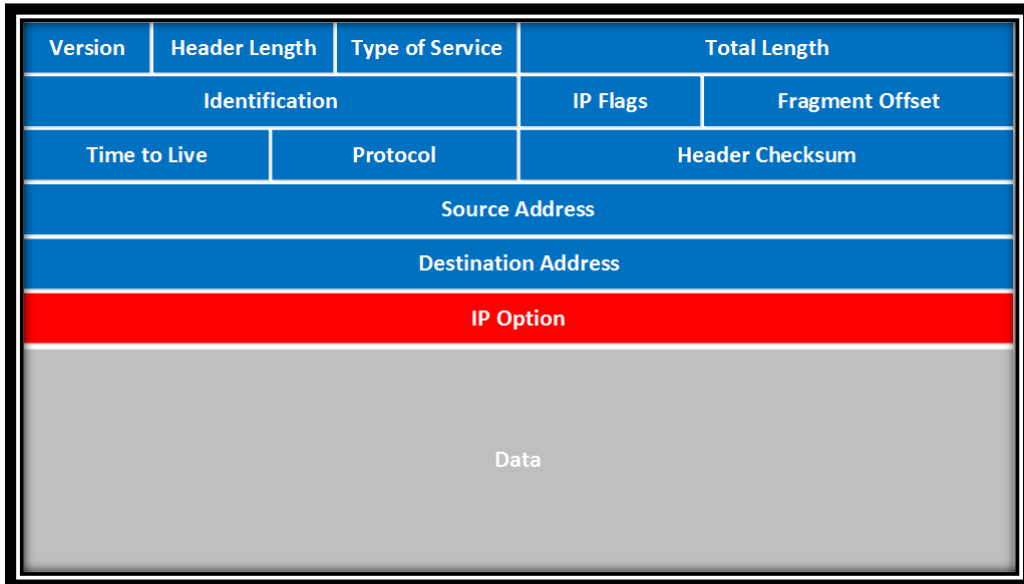
- On old traditional network , data, voice and video had their own separate network infrastructure and did not impact each other
- On modern networks, data, voice and video run over the same shared infrastructure.
- This enables cost savings and advanced features for voice and video.
- Data, voice and video are all fighting for all same shared bandwidth.
- FIFO (First in First Out) whenever congestion is experienced on router or switch, packets are sent out in a First in First out (FIFO) manner by default.
- Congestion can be experienced wherever it is possible for packets to come in quicker than they can be sent out.
- Example Traffic is going left to right from Head office to Branch office. The WAN edge router has a Fast Ethernet Interface on the inside LAN Interface and an E1 Interface on the outside WAN Interface.
- Packets are arriving faster than they can be sent out.
- Packets wait in the queue to go out. Packets are sent out FIFO in the order they were received.
- Congestion causes delay to packets as they wait in the queue.
- As the size of the queue changes it causes Jitter and there is a limit to the size of the queue. If packet arrives when the queue is full the router will drop it.
- Voice and Video calls and other applications will be unacceptable quality if they do not meet their delay, jitter and loss requirements.

How to Mitigate Congestion or How to Solve Congestion Problem?

- Add more bandwidth – this costs money.
- Use Quality of Service Techniques to give better service to the traffic which needs it.

Effects of Qos Queuing:

- QOS queuing can reduce latency, jitter and loss for particular traffic.
- The original driver for QoS was voice over IP but it can also be used to give better service to data applications.
- If we are giving one type of traffic better service on the same link we started with, the other traffic type must get worse service.
- The point is to give each type of traffic the service it requires.
- QoS queuing is designed to mitigate temporary periods of congestion. If a link is permanently congested the bandwidth should be increased.



Qos Terminologies:

Bandwidth:

- Network bandwidth refers to the speed of a link or interface, in bits per seconds.
- Think bandwidth as speed that mean capacity of the link
- Network bandwidth is measured in number of bits transmitted into bits per second

Congestion:

- Network congestions causes the delay or Latency
- Network congestions occur when interface experiences more traffic that it can handle

Delay:

- Delay or latency refers to time it takes for packet to travel from source to destination.
- In Quality of service there are two types of delays one is fixed delay and other is variable.

Jitter (Variation in delay):

- In QOS Jitter is defined as a variation in the delay of received packets. Or Difference between the delays of the IP Packets or we can say jitter is the irregular time delay in the sending of the data packet over network.

Email us:
networkforYou4@gmail.com

5 of 15

WhatsApp Us : +918143809578



Latency (Delay):

- Latency is the time required by a data packet to reach the destination from the source

Packet Loss:

- We have loss of packet when we have congestion and don't do QoS mechanisms or we can say when congestion occurs network devices such as router or switches can drop packets if we don't do QoS.

Voice:

- In the Network voice is very sensitive to delay and dropped packets. It make no sense and not possible to retransmit or re send the voice if packets are lost.
- So we need to take care for voice packets must receive a higher priority then other types of network traffic.

Videos:

- Videos also important without QoS significant amount of extra bandwidth capacity video quality degrades.

Data:

- Data applications that have no tolerance for data loss, such as email and web pages. And it use TCP to ensure that if the data packets are lost in the transit they will be resent.

Classification and Marking:

- For a router or switch to give a particular level of service to a type of traffic it has to recognize that traffic first.
- Common way to recognize the traffic are by **Class of Service (COS) for layer 2 marking** and **Differentiated service code point (DSCP) marking for L3** and **Access Control List or Network Based Application Recognition (NBAR)**.

Layer 2 Marking - Class of Service:

- There is a **3 bit** field in the **layer 2 802.1q frame header** which is used to carry the Cos QoS Marking.
- A value of 0 - 7 can be set. The default values are 0 which is designated as Best Effort traffic.
- Cos 6 and 7 are reserved for network use -- Like routing protocol and network control traffic.
- **Higher the number more important the traffic**
- IP Phones mark their **call signaling traffic as cos 3** and their voice payload (Spoking voice) **as cos 5**.
- **Spoking voice is most important then calls signaling.**

Email us:
networkforYou4@gmail.com

6 of 15

WhatsApp Us : +918143809578



Layer 3 Marking - DSCP (Differentiated Service Code Point):

- DSCP Qos marking carry in **Layer 3 IP Header**.
- In IP Header DSCP Qos marking **6 bits** are used which gives **64 possible values**. The default value is 0 which is designated **as Best effort traffic** here we can **mark DSCP zero** that mean that traffic not gets **any special services**.
- IP phones mark their call signaling traffic as **24 (CS3)** (**That is DSCP 24 is also known as CS3**) and their voice payload as 45 (EF) (**DSCP value 45 is also known as EF**)
- There are some standard markings for other traffic types such as 26 (AF31) for mission critical data and 34 (AF41) for SD video
- DSCP is the preferred classification and marking method because the router can very quickly gather the information from a single byte in the IP header.

Commonly Used DSCP Values:

DSCP Value	Decimal Value	Meaning	Drop Probability	Equivalent IP Precedence Value
101 110	46	High Priority Expedited Forwarding (EF)	N/A	101 - Critical
000 000	0	Best Effort	N/A	000 - Routine
001 010	10	AF11	Low	001 - Priority
001 100	12	AF12	Medium	001 - Priority
001 110	14	AF13	High	001 - Priority
010 010	18	AF21	Low	010 - Immediate
010 100	20	AF22	Medium	010 - Immediate
010 110	22	AF23	High	010 - Immediate
011 010	26	AF31	Low	011 - Flash
011 100	28	AF32	Medium	011 - Flash
011 110	30	AF33	High	011 - Flash
100 010	34	AF41	Low	100 - Flash Override
100 100	36	AF42	Medium	100 - Flash Override
100 110	38	AF43	High	100 - Flash Override
001 000	8	CS1		1
010 000	16	CS2		2

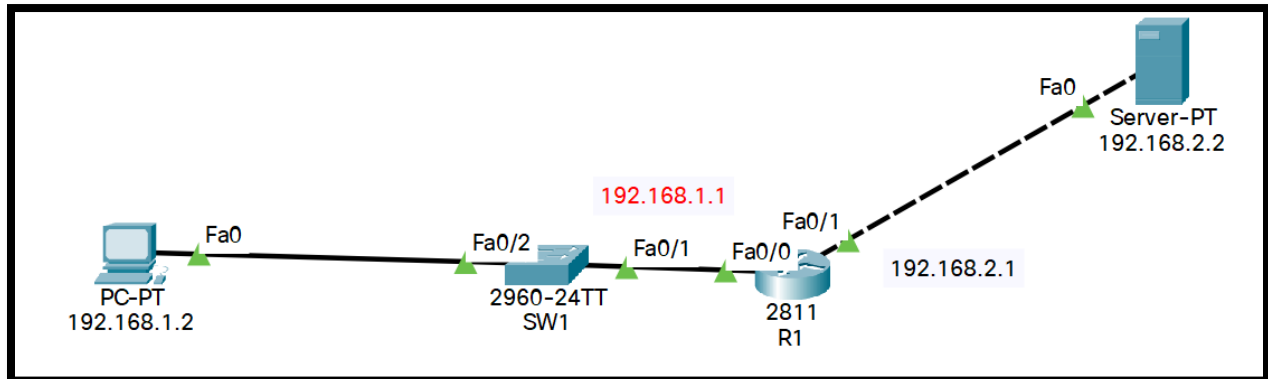
Email us:
networkforyou4@gmail.com

7 of 15

WhatsApp Us : +918143809578



Lab time QOS Lab(Match traffic and apply given value):



R1 Configuration:

```
En
Config t
Hostname R1
```

```
Int f0/0
Ip add 192.168.1.1 255.255.255.0
No sh
Int f0/1
Ip add 192.168.2.1 255.255.255.0
No sh
```

QOS:

Create Class Map to match traffic:
(Identify the traffic to apply special treatment):

```
class-map https_map
match protocol https
exit
class-map http_map
match protocol http
exit

class-map icmp_map
match protocol icmp
exit
```

Email us:
networkforyou4@gmail.com

8 of 15

WhatsApp Us : +918143809578



Create Policy Map to apply policy (What type of treatment we need to give to each kind of traffic):

```
policy-map f0/0_in  
class https_map  
set ip dscp AF31  
exit
```

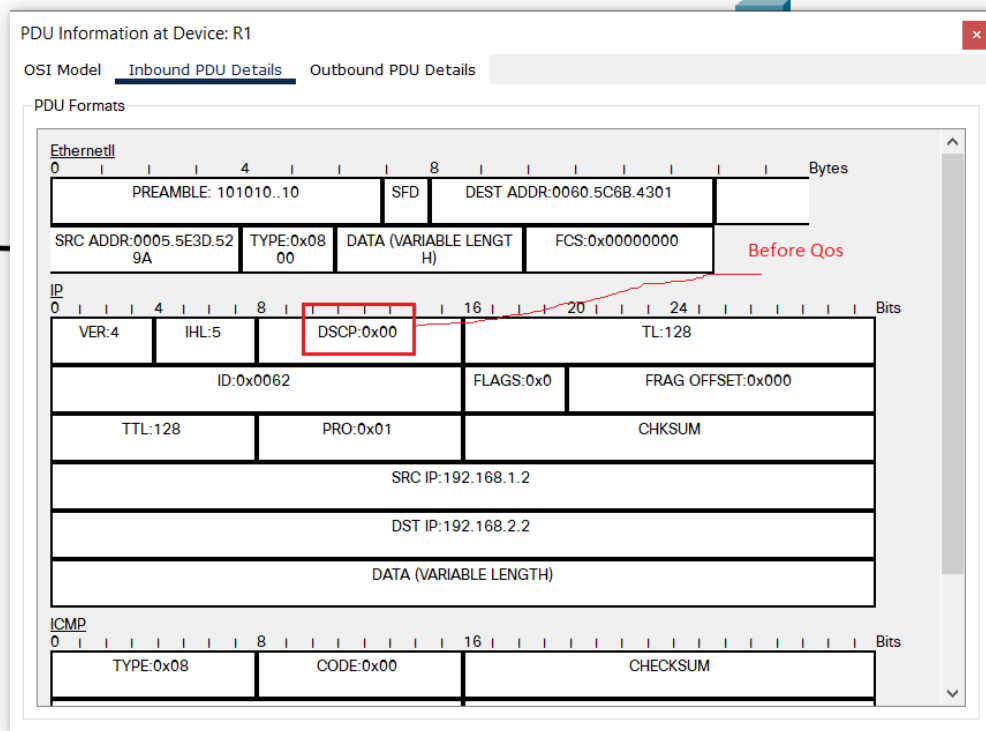
```
class http_map  
set ip dscp AF31  
exit
```

```
class icmp_map  
set ip dscp CS2  
exit
```

Apply Policy map by using Service policy:

```
int f0/0  
service-policy in f0/0_in
```

Without QOS



Email us:
networkforyou4@gmail.com

9 of 15

WhatsApp Us : +918143809578



With QOS

PDU Information at Device: R1

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

EthernetII

PREAMBLE: 101010..10		SFD	DEST ADDR:0005.5E9A.06A8	
SRC ADDR:0060.5C6B.4302	TYPE:0x0800	DATA (VARIABLE LENGTH)		FCS:0x00000000

After Qos

IP

VER:4	IHL:5	DSCP:0x10	TL:128	
ID:0x0062		FLAGS:0x0	FRAG OFFSET:0x000	
TTL:127	PRO:0x01	CHKSUM		
SRC IP:192.168.1.2				
DST IP:192.168.2.2				
DATA (VARIABLE LENGTH)				

ICMP

TYPE:0x08	CODE:0x00	CHECKSUM	
-----------	-----------	----------	--

DSCP = 0x10 (in Hexadecimal) that is in Decimal is 16 and that is dscp CS2 as we configure ICMP

Email us:
networkforyou4@gmail.com

10 of 15

WhatsApp Us : +918143809578

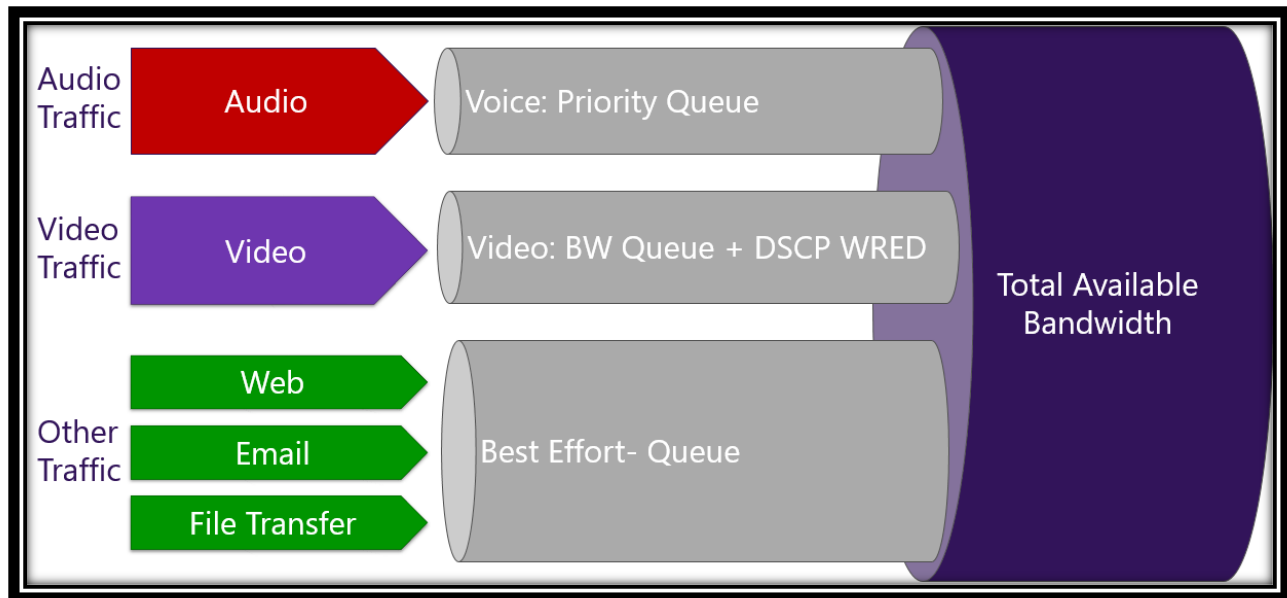


Recognizing Traffic with an ACL:

- An Access control list can be used to recognize traffic based on its layer 3 and layer 4 information.
- For example SSH traffic going to and from the router on TCP port number 22. Need to give good bandwidth etc.
- So we can configure ACL on router with referring port # etc.

Recognizing Traffic with NBAR (Network Based Application Recognition):

- NBR can be used to recognize traffic based on its layer 3 to layer 7 information.
- We can download signature from Cisco and loaded on your router which recognizes well known applications.



Congestion Management:

- So example in router or switch we are getting more traffic to send out with the outer interface bandwidth then we do queuing. Or in other words we can say Queuing can be used to manage congestion on routers and switches.

There are two type of Queuing policy commonly use

- CBWFQ (Class Based Weighted Fair Queuing) --- gives bandwidth guarantees to specified traffic types.
- LLQ (Low Latency Queuing) -- Priority queuing (Traffic into the priority queue is send before other traffic).

Email us:
networkforyou4@gmail.com

11 of 15

WhatsApp Us : +918143809578

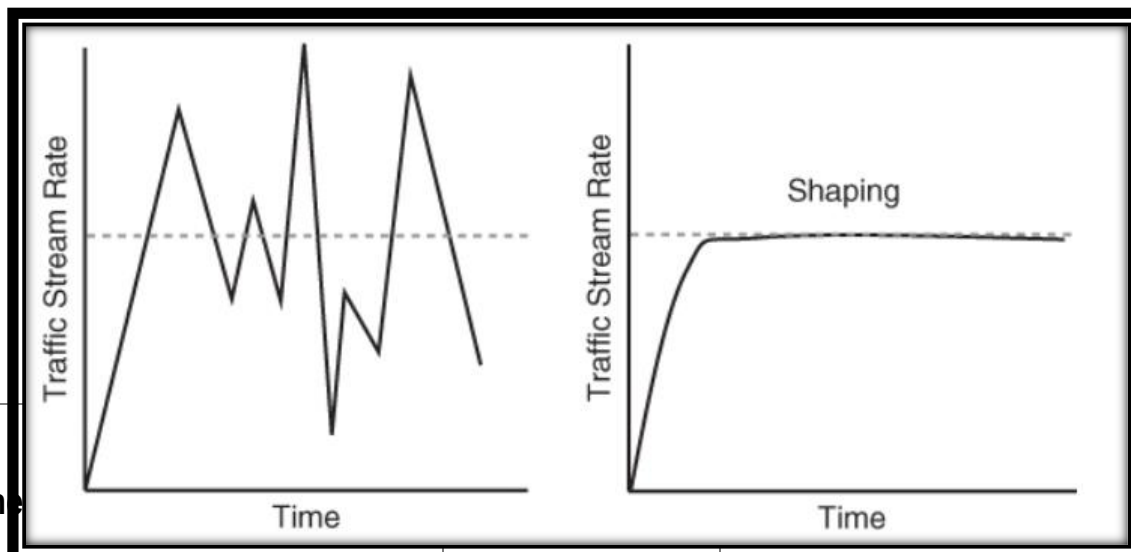
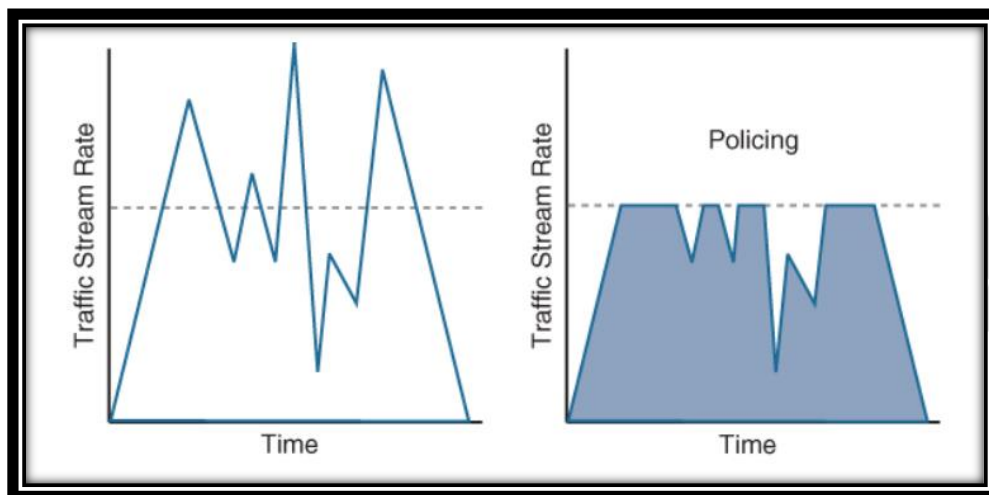


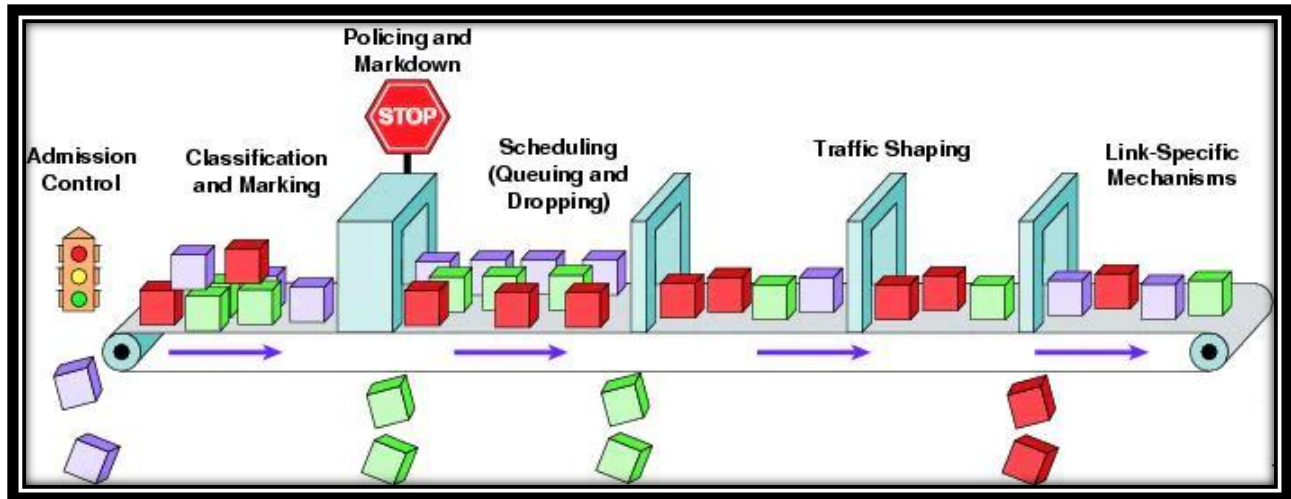
MQC (Modular Qos CLI):

- Cisco Qos Configuration uses the MQC modular Qos CLI
- It has 3 main sections
- **Class Maps** define the traffic to take an action on
- **Policy Maps** take the action on that traffic
- **Service Policies** apply the policy to an interface

Shaping and Policing:

- Traffic Shaping and Policing can be used to control traffic rate
- They both measure the rate of traffic through an interface and take an action if the rate is above a configured limit
- Traffic shaping buffers any excess traffic so the overall traffic stays within the desired rate limit.
- Traffic policing drops or remarks excess traffic to enforce the specified rate limit.

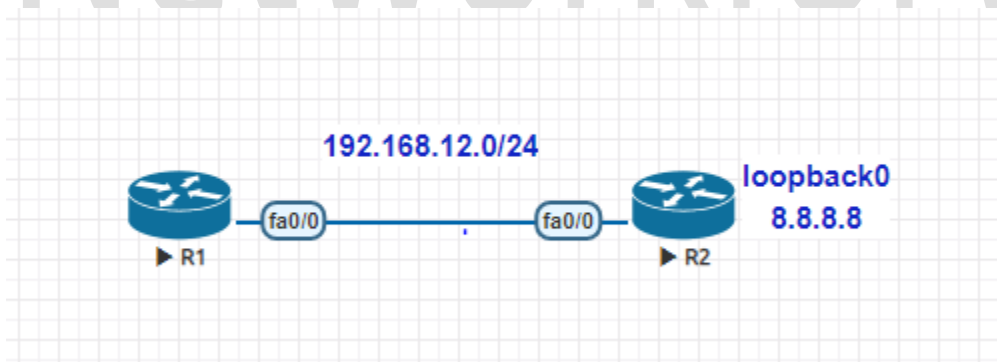




Networkforyou

QoS Lab:

Policing Lab:



R1 Configuration	R2 Configuration
En	En
Config t	Config t
Hostname R1	Hostname R2
Int f0/0	Int f0/0
Ip add 192.168.12.1 255.255.255.0	Ip add 192.168.12.2 255.255.255.0
No sh	No sh

Email us:
networkforyou4@gmail.com

WhatsApp Us : +918143809578



```
R2#sh policy-map interface f0/0
FastEthernet0/0

Service-policy input: pmap

Class-map: cmap (match-all)
 4771 packets, 543894 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: protocol icmp
police:
  cir 12500 bps, bc 1500 bytes
  conformed 4522 packets, 515508 bytes; actions:
  transmit
  exceeded 249 packets, 28386 bytes; actions:
  drop
  conformed 0 bps, exceed 0 bps

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

Email us:
networkforyou4@gmail.com

15 of 15

WhatsApp Us : +918143809578