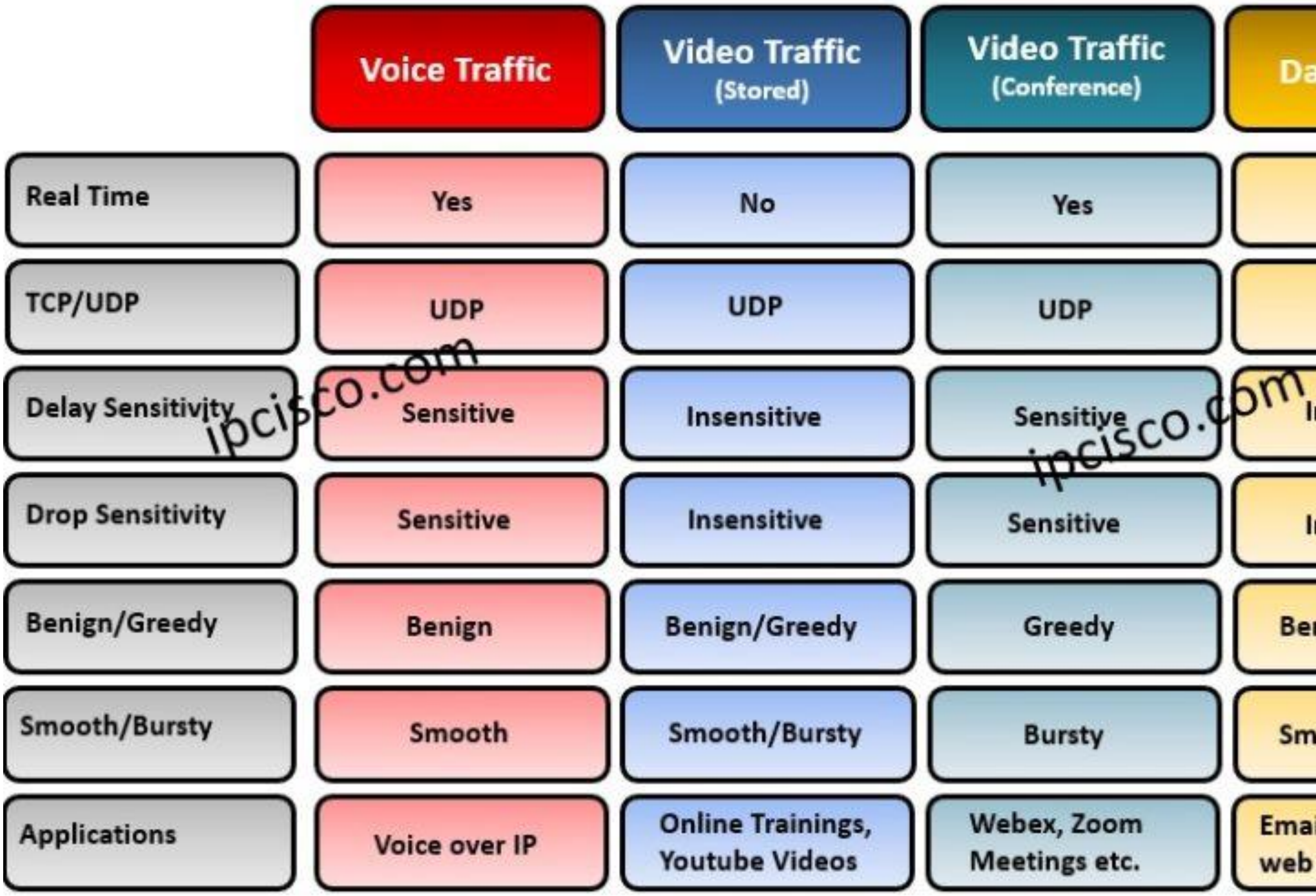
Network Traffic Types



	Voice Traffic	Video Traffic (Stored)	Video Traffic (Conference)	Da
Real Time	Yes	No	Yes	
TCP/UDP	UDP	UDP	UDP	
Delay Sensitivity	Sensitive	Insensitive	Sensitive	I
Drop Sensitivity	Sensitive	Insensitive	Sensitive	I
Benign/Greedy	Benign	Benign/Greedy	Greedy	Ber
Smooth/Bursty	Smooth	Smooth/Bursty	Bursty	Sm
Applications	Voice over IP	Online Trainings, Youtube Videos	Webex, Zoom Meetings etc.	Emai web

There are different **network traffic types** in a network. These traffic types have different characteristics and requirements. So, in a network there are different behavior according to the traffic types. We achieve this with **Quality of Service (QoS)** configurations. So, what are these network traffic types? These are basically three types of traffic: voice, video and data traffic.

Now, let’s focus on each of these traffic types and learn what they need or what are the best behavior for these types of traffics.

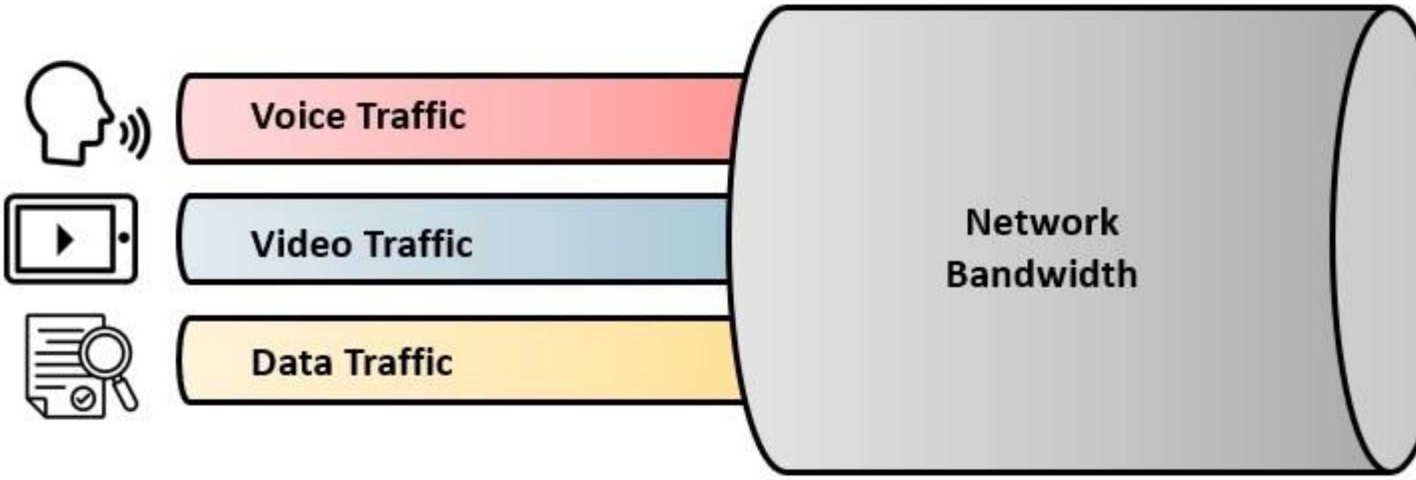


Table of Contents

Voice Traffic

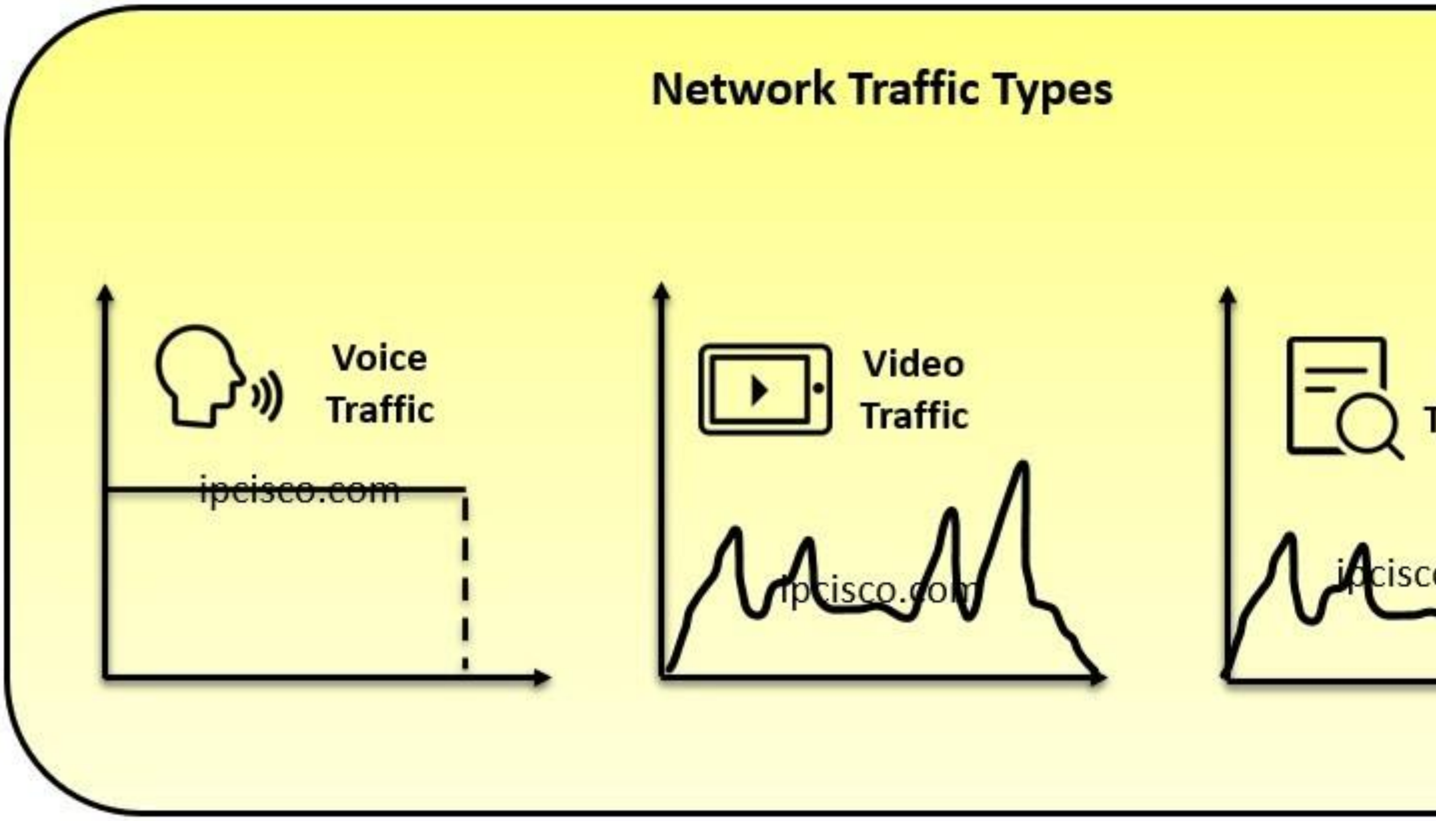
Voice traffic is a **real time** and **sensitive** traffic type. The voice packets must be delivered at the same time or with a very low delay. Because, if the voice packets arrive in different types to the destination, we can not understand what they are saying. So, **delay time** is very important for such a traffic.

Beside variable delays cause **jitter** and jitter is a wellknown problem for voice traffics. To have a clear voice at the other end, jitter must be avoided.

The last important problem is **packet loss** for voice traffic. We can tolerate some loss but this must not be a high value that will make the communication incomprehensible.

To avoid delay, jitter and packet loss we use Quality of Service (QoS) configuration on routers. With these configurations, we avoid any problem on voice packets and we prioritize this type of traffic. Voice packets needs higher priorities over other network traffic types. Because, this type of traffic is the most sensitive traffic.

In voice traffic, generally **UDP** is used because of its fast behavior.



Video Traffic

Video traffic is one of the most used traffic types in today’s world. With the increase of the youtube watching times, online training and similar traffics, video became very important as a traffic type. Video traffic is a **high volume** traffic that is not as sensitive as voice traffic. Because video traffic is not real time generally. It can tolerate packet loss and delays. And delay on the packets do not cause any misunderstanding. It causes only a little extra time. Beside any loss can be tolerated because it is a very high volume traffic and if we loss small amount of this traffic, the video can be still understandable and clear.

There is also another video type that is used in real time. **Videoconferencing** traffic can be an example of this type of traffic. In this type of traffic, delays became more important because we are in the real time and we do not have too much extra time for a face to face conference call. A person is talking and waiting other person's talking. This type of communication can not be achieved with higher delays.

Because of its volume, video traffic can be **bursty** and can consume many resources of your network. So, for such traffic, your network and bandwidth must be ready.

For video traffic **UDP** is used again because this type of traffic is also delay sensitive traffic.

Data Traffic

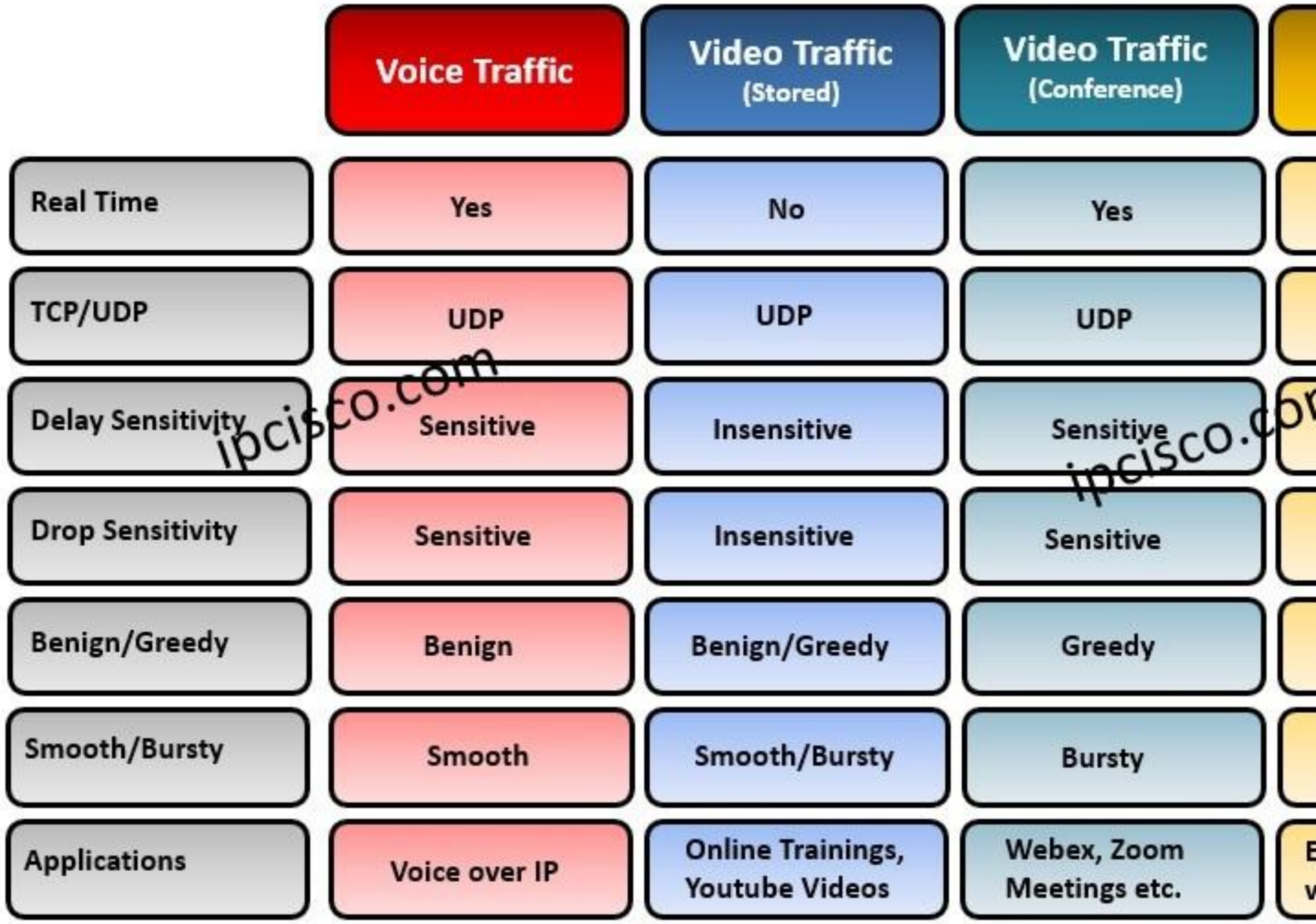
Data traffic is the other important traffic type. This type of network traffic is insensitive traffic to packet loss if we compare with voice and video traffic. It uses retransmission mechanism if any packet loss occurs.

This type of traffic is used in emails, file transfers, web pages etc.
So, **guarantee** is an important term for such a network traffic. To provide secure and guaranteed transfer, **TCP** is used with data traffic.
The **restransmission** mechanism of TCP gives this guarantee and data traffic is sent with a minimum loss.

Again, delay is not too important for this type of traffic. For example, if any delay occurs, you receive an email a little lately that we can measure it with seconds.

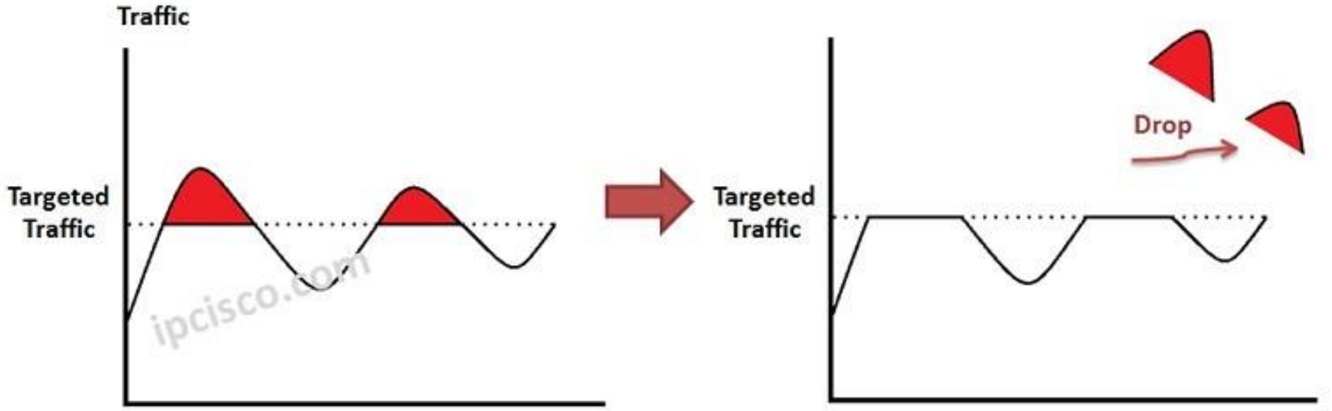
Voice versus Video versus Data Traffic

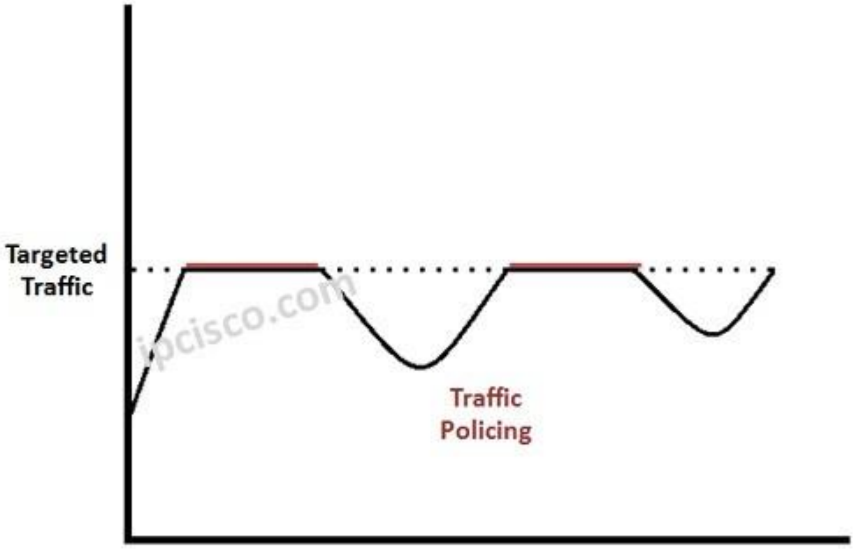
We have talked about these traffic detailly above. Below, you can find comparison table for voice traffic, video traffic and data traffic.



	Voice Traffic	Video Traffic (Stored)	Video Traffic (Conference)
Real Time	Yes	No	Yes
TCP/UDP	UDP	UDP	UDP
Delay Sensitivity	Sensitive	Insensitive	Sensitive
Drop Sensitivity	Sensitive	Insensitive	Sensitive
Benign/Greedy	Benign	Benign/Greedy	Greedy
Smooth/Bursty	Smooth	Smooth/Bursty	Bursty
Applications	Voice over IP	Online Trainings, Youtube Videos	Webex, Zoom Meetings etc.

Policing and Shaping in QoS





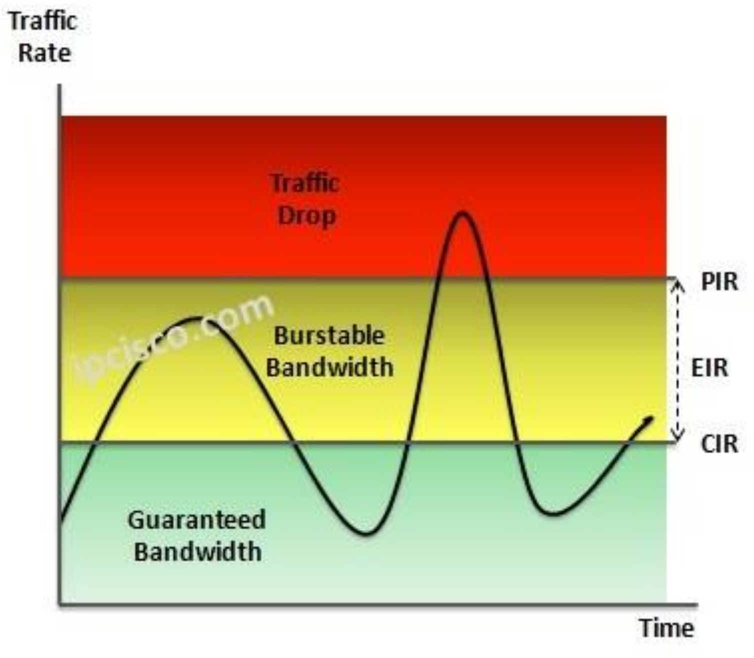
In networks, the traffic increses for a variety of reasons. Some **Quality of Service Adjustments** are done to handle this increases. During these increases, if the capacity of the link is exceeded, then the traffic on this link is dropped. Without any arrangement, this drop can cause unexpected and undesired important data drops. To avoid such problems, **QoS Traffic Policing and Shaping** mechanisms are used. This mechanisms are another important mechanisms beside **QoS Classification and QoS Marking**.

Basically, **Traffic Policing** is using a predefined **Traffic Policy** to manage the network traffic. With these configured Traffic Policies, during a bandwidth exceed, the required and desired actions are ordered according to the traffic variety. With this policies, traffics are remarked or they are dropped with a predefined actions.

On the other hand, **Traffic Shaping** is not as strict as Traffic Policing. With Traffic Shaping, the traffic is controlled and if the traffic close to the traffic exceed, it uses queues and made some of the traffic wait (buffered the traffic) without any drop action.

There are also some important terms used with Traffic Policing and Traffic ShapingThese terms are given below:

CIR : Committed Information Rate
EIR : Exceed Information Rate
PIR : Peak Information Rate



Traffic is controlled according to these values. Now, let’s briefly check what are these value. You can also reach the detailed explanation of these values in another article.

CIR (Committed Information Rate) is the traffic rate that is guaranteed by the provider. The traffic rate under this value is delivered certainly. After this value, to the PIR value, the traffic is delivered but not guaranteed. During busy times, these traffic can be dropped.

Beside, **PIR (Peak Information Rate)** is the top traffic rate that the traffic will delivered in the normal traffic flows. Any traffic that exceed this value, certainly policied or shaped.

EIR (Exceed Information Rate) is the value, between CIR and PIR. This is the amouth of unguaranteed but delivered traffic.

Now, let’s talk about **QoS Traffic Policing** and **QoS Traffic Shaping** detailly.

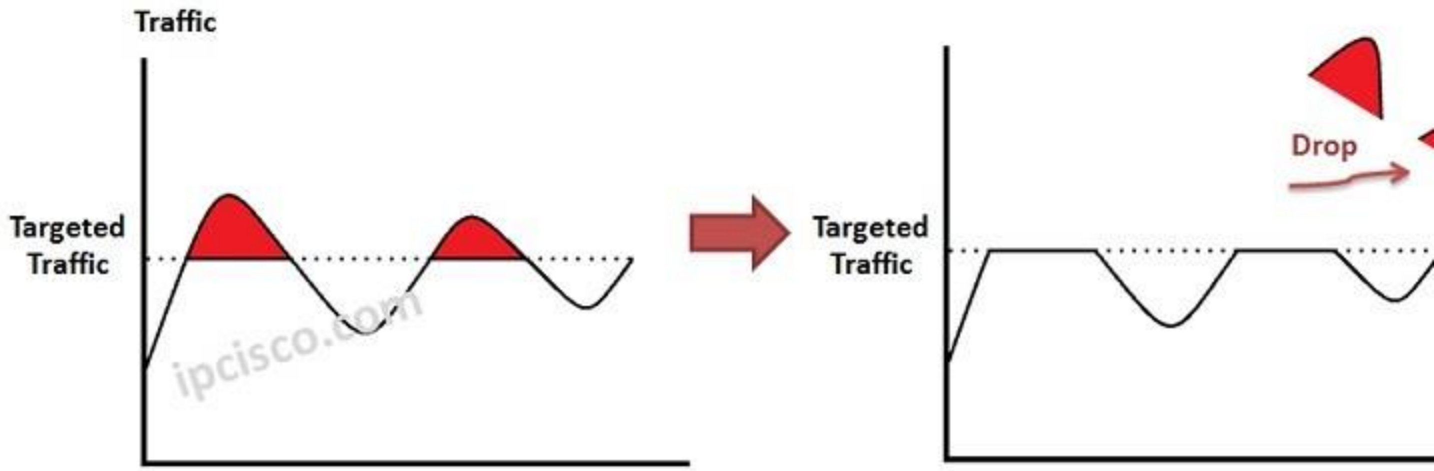
Table of Contents

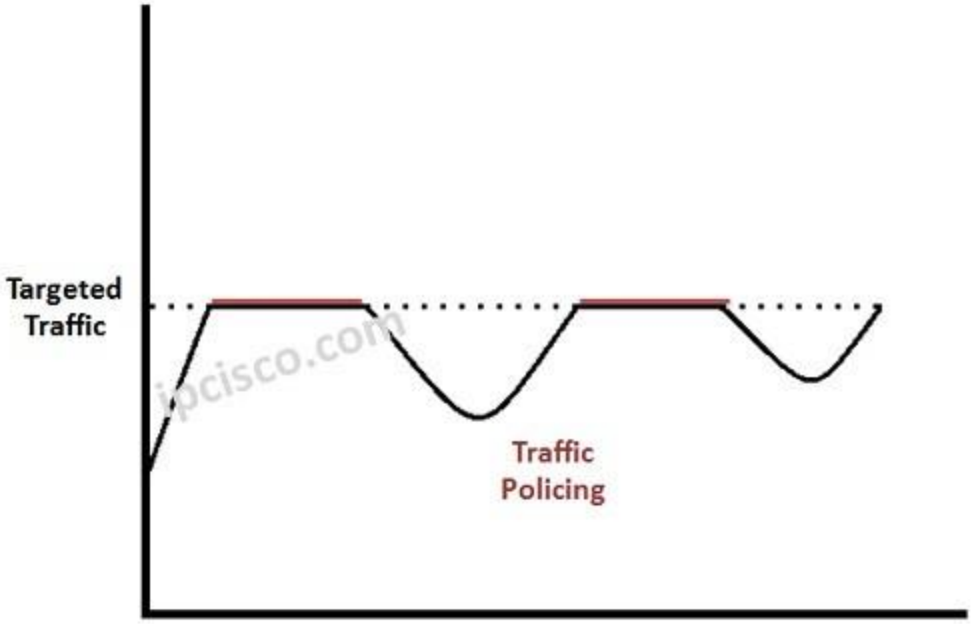
□

Traffic Policing

Traffic Policing is the strict method of controlling bandwidth exceed according to high traffic. For Quality of Service, some predefined actions are determined by the network administrators. This predefined actions build a Traffic Policy. With Traffic Policy, network knows what to do even if a traffic violation occurs.

For example, in the **Traffic Policy**, if a bandwidth exceed occurs, you can define to drop a video streaming traffic. At that moment, users can not watch videos because of the limitation of Traffic Policy. This Traffic limitation provides extra bandwidth in the network and network bandwith exceed is overcomed. This limitation is also done with remarking the traffic.





Here, we can say that there are two key techniques used in **Traffic Policing**. These techniques are:

- **Dropper**
- **Marker**

Dropper is the mechanims that drops the traffic if a traffic violation occurs as its name implies.
Marker is the mechsnism that remarks the traffic, with a new priority.

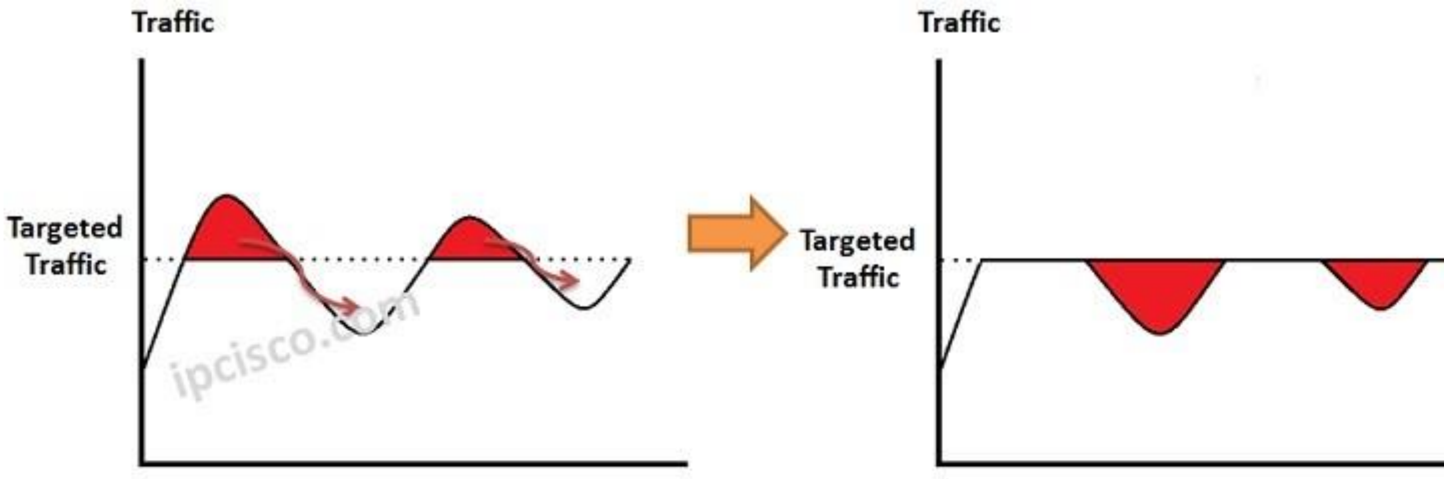
Traffic Policies are configured and can be used both inbound and outbound directions. So, both in coming and outgoing traffic can be controlled with Traffic Policies.

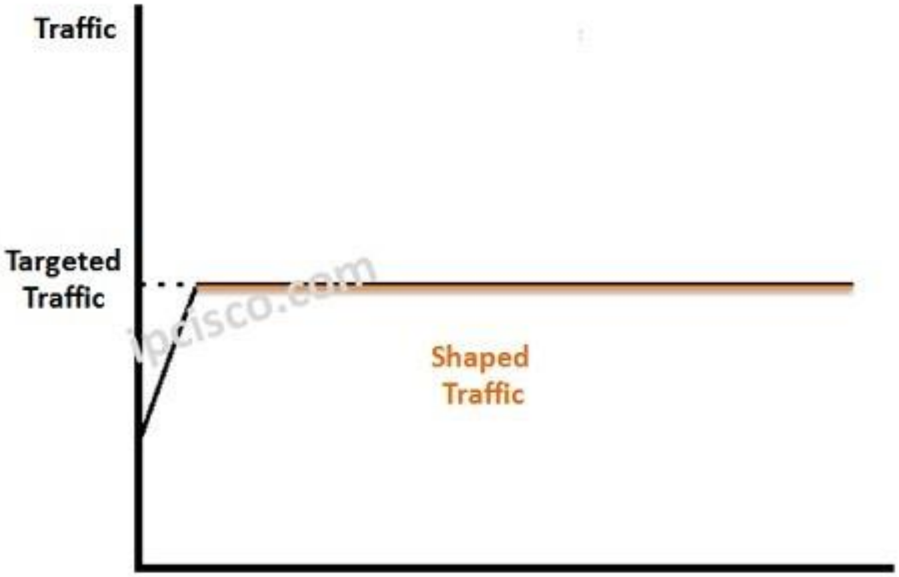
Generally **Traffic Policing** causes more TCP retransmissions. This provide more resource utilization.

Traffic Shaping

QoS Traffic Shaping is the mechanism that is used during a **Traffic Exceed**. The Exceed Traffic is **buffered** and with a little delay, it is sent again. With this buffer and queue mechanism, **Traffic Shaping** is a soft medhod if we compare with Traffic Policing.

There can be **Traffic Exceeds (traffic bursts)** in the network. With **Traffic Shaping**, this burst become smooth. Think about this graphic. The top of the graphic seems as it is cut with a pair of scissors. The traffic continue to be at top border, but the exceed traffic buffered.

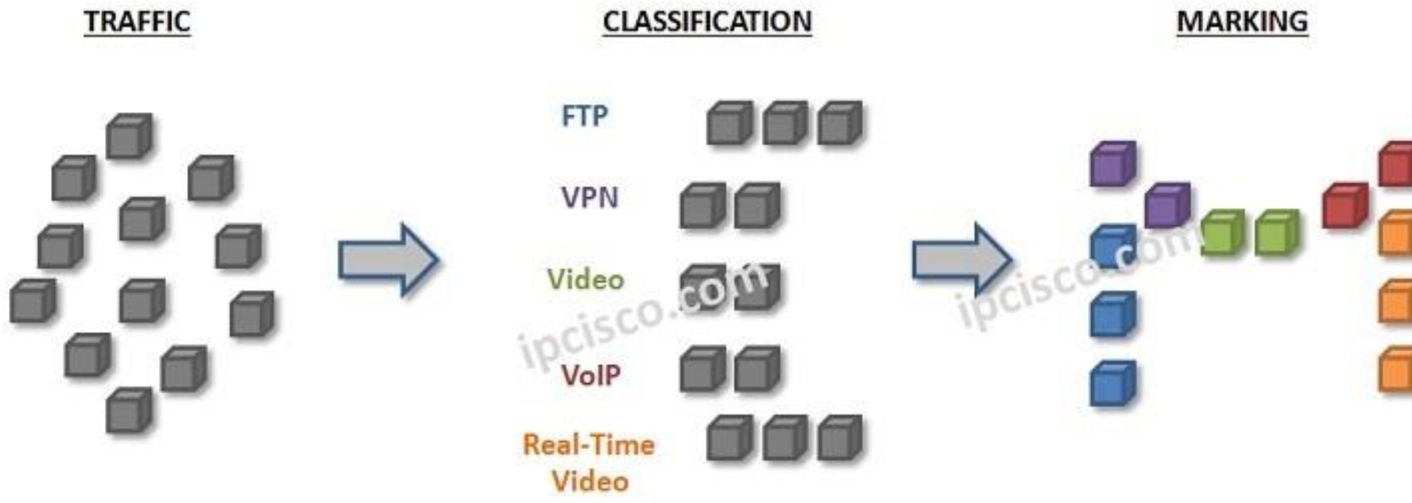




QoS Traffic Shaping do not support Marking or Remarking again. This is done only with Traffic Policing. **QoS Traffic Shaping** is applied only through outgoing interfaces. The buffer mechanims used by **Traffic Shaping** minimize TCP retransmissions. This provide less resource utilization.

In **Cisco CCNA Exam** and **CCNP ENCOR Certification Exams**, you can see questions about Traffic Shaping and Policing.

lassification and Marking in QoS



To use **Quality of Service** for a traffic, firstly traffic need to be identified. With this identification, traffic types are classified and then they are marked with an understandable way by the network. This process is basically called "**QoS Classification and Marking**". Another important mechanisms are Qos **Traffic Policing and QoS Traffic Shaping**. We will talk about this in the next lesson.

The identification mechanism used by **QoS** can be divide into **two** important process. These process are :

- **Classification**
- **Marking**

Now, let's go a little deeply on **QoS Classification and Marking**, and talk about these two important QoS Process more.

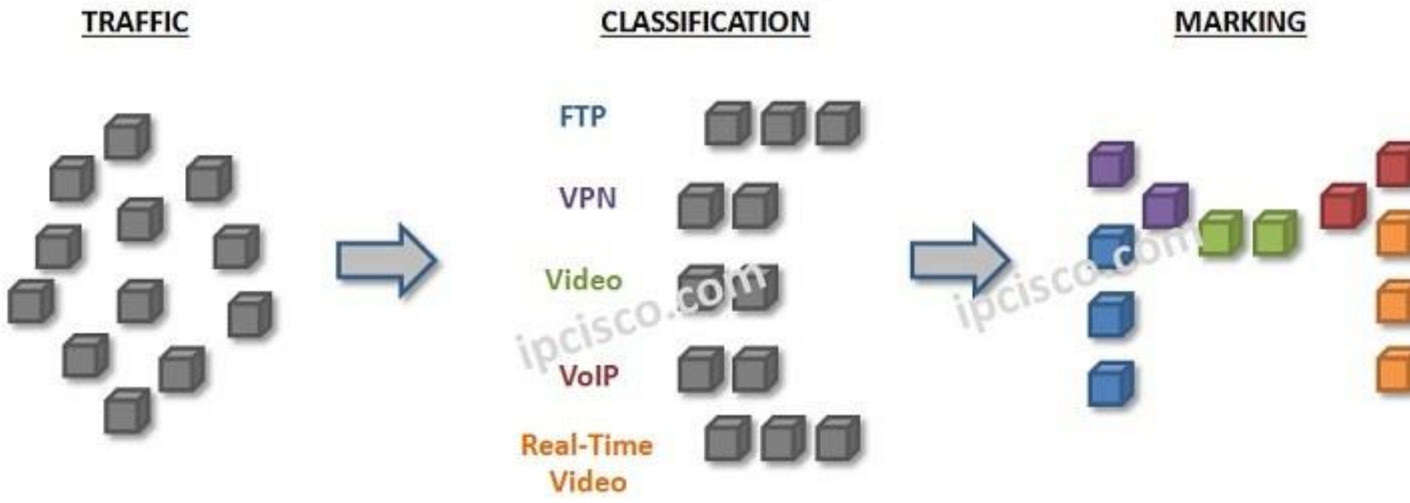


Table of Contents

□

QoS Classification

There are carious of traffic types in a network. These traffic types can be **data, voice, video streaming** etc. **Without QoS**, all these traffic types are behaved **similarly**. But behaving similarly to all the traffic types is not a proper way. Because, different traffic types need different threatments.

For example, voice traffic must be **fast** but security is in the second plane for voice traffic. Beside, pure data, ftp can be slower than a voice traffic.

Because of the fact that different types of traffics need different threatments, first of all we need to categorize the type of our traffic. Identifying and categorizing the type of the traffic is called "**Classification**". After this process, we know that, we have a voice traffic, or video, or what else.

QoS Classification Process can be done by checking the different fileds of a packet. There are fields that shows the traffic types in a packet like IP Precedence,DSCP. Beside, incoming interfaces, source and destination addresses can also be used for Classification.

QoS Classification is done **close to the source**. This is because, early determination of the type and threat as required through the network.

QoS Marking

After classification, traffic type determination must be showed also in the packet. To do this, a field in a packet header is changed. This changes explains that, the packet is belong to a specific type of traffic. The name of this process is called "**Marking**". It is also called "**Coloring**".

QoS Classification Process is a must before **Marking Process**. Because, you can not mark something about its characteristic without knowing what is it.

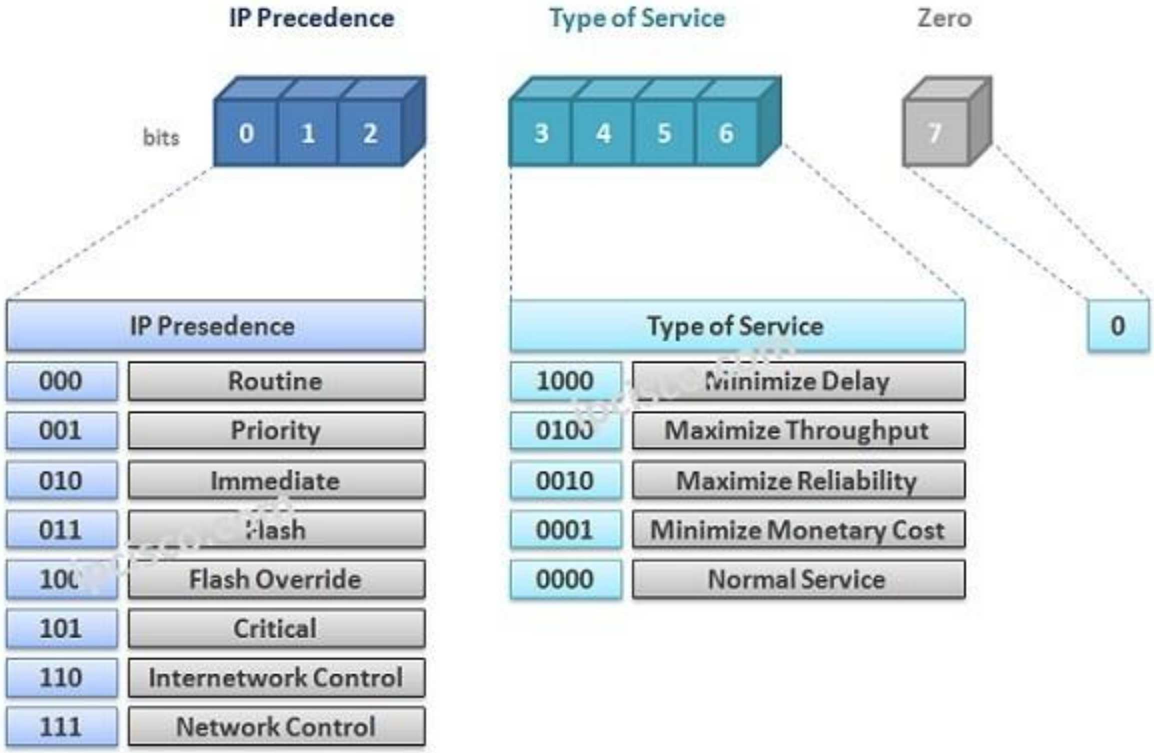
Marking can be done in different levels with different field changes. With this changes, the traffic is quickly recognized anywhere in the network.

In **Layer 2**, in Ethernet Header, Class of Service field is used for Marking.

In **Layer 2.5**, in MPLS Header, Type of Service (Experimental) field is used for Marking.

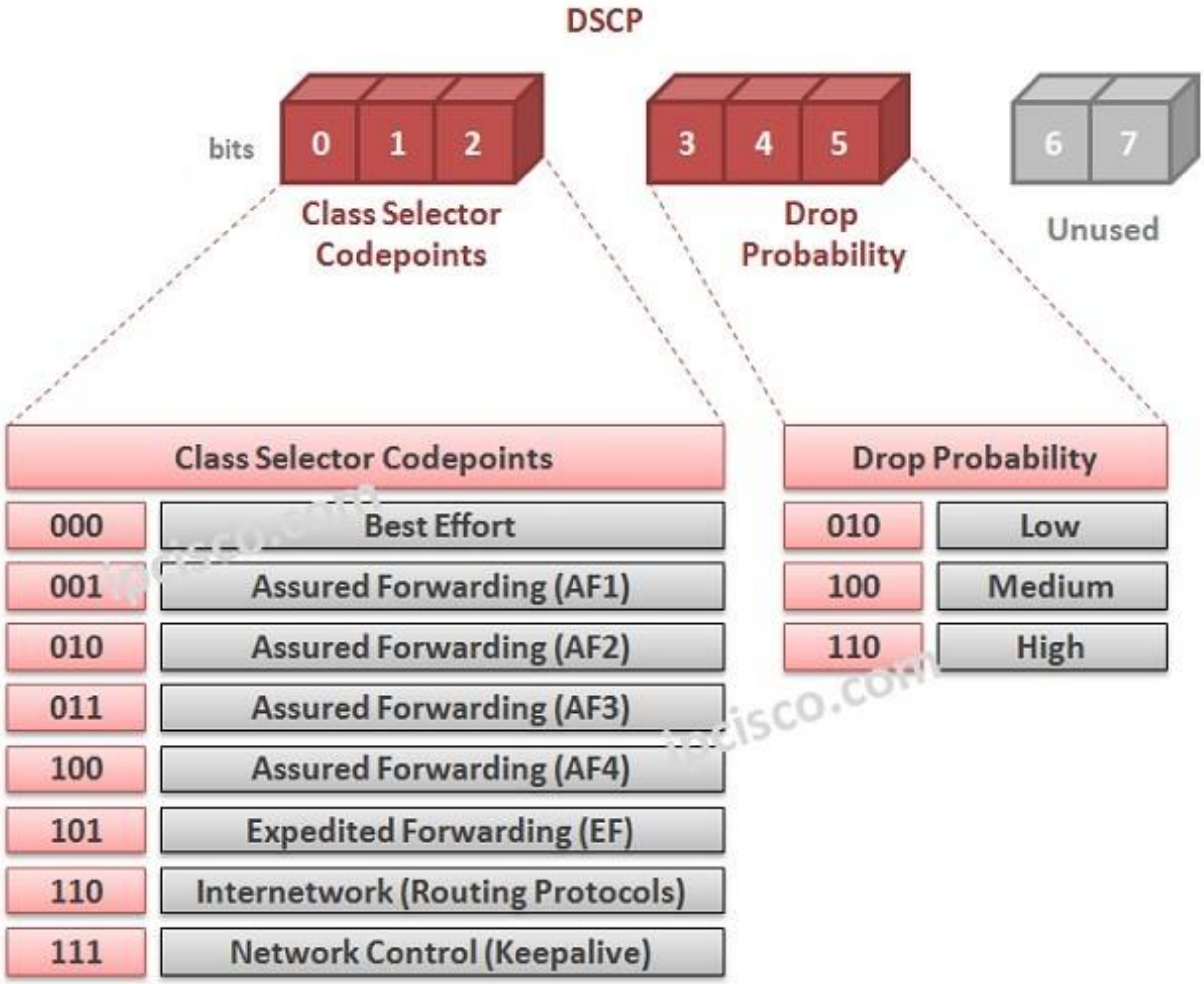
In **Layer 3**, in IP Header, Type of Service IP Precedence and DSCP fields are used for Marking.

In **Upper Layers**, NBAR and Deep Packet Inspection are used for Marking.



IP Presedence	
000	Routine
001	Priority
010	Immediate
011	Flash
100	Flash Override
101	Critical
110	Internetwork Control
111	Network Control

Type of Service	
1000	Minimize Delay
0100	Maximize Throughput
0010	Maximize Reliability
0001	Minimize Monetary Cost
0000	Normal Service



Class Selector Codepoints	
000	Best Effort
001	Assured Forwarding (AF1)
010	Assured Forwarding (AF2)
011	Assured Forwarding (AF3)
100	Assured Forwarding (AF4)
101	Expedited Forwarding (EF)
110	Internetwork (Routing Protocols)
111	Network Control (Keepalive)

Drop Probability	
010	Low
100	Medium
110	High

In **Cisco CCNA** and **CCNP ENCOR Certification Courses**, Traffic Classification and MArking is an important QoS Lesson.

Quality of Service Overview

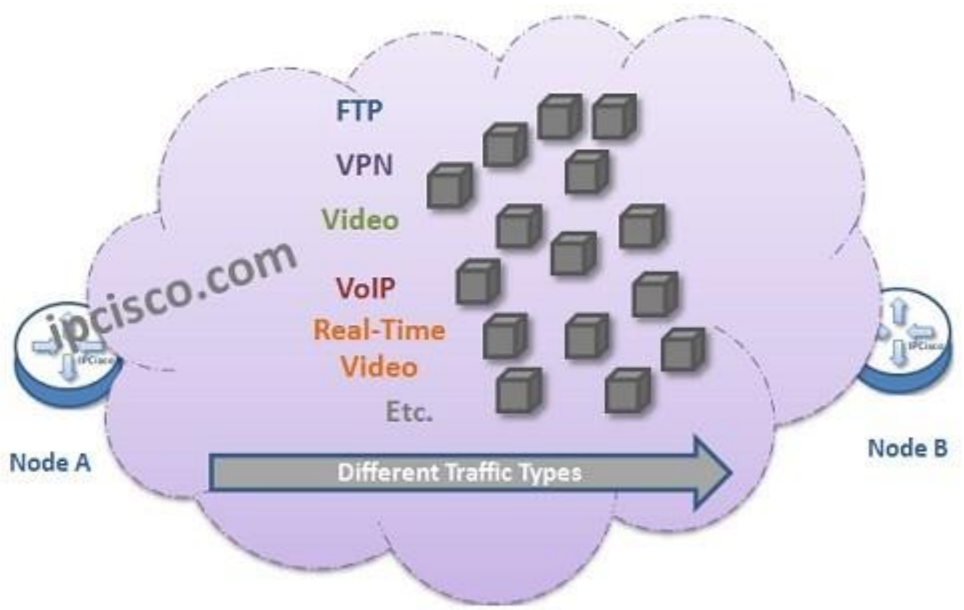


Table of Contents

□

What Does QoS Stand For?

This is the most ask questions by Network Engineers, especially the Newbies, **What Does QoS Stand** For? It is also an important lessons of **CCNA** and **CCNP Trainings**. **QoS (Quality of Service)** is the general name of a concept , which is used to optimize networks with different priority levels to different applications and provide improved services for these appliations on these networks. From the view point of customer, with **QoS**, users get a better performance without drops, packet loss, unaccepted delays etc. From the view point of your Service Provider company, with **QoS**, you can use your networks more efficient. With optimized network bandwidh and with a best performance.

You can also view the QoS related lessons:

- **Network Traffic Types**
- **Traffic Classification & Marking**

- **Traffic Policing & Traffic Shaping**

After answering what ooes qoS stand for question, now let’s focus on some terms, **QoS Enemies** in QoS. **QoS (Quality of Service)** adjusts some important **QoS Enemies** for the traffic mainly. With this adjustments, networks become more efficient.

These important **QoS** enemies are given below:

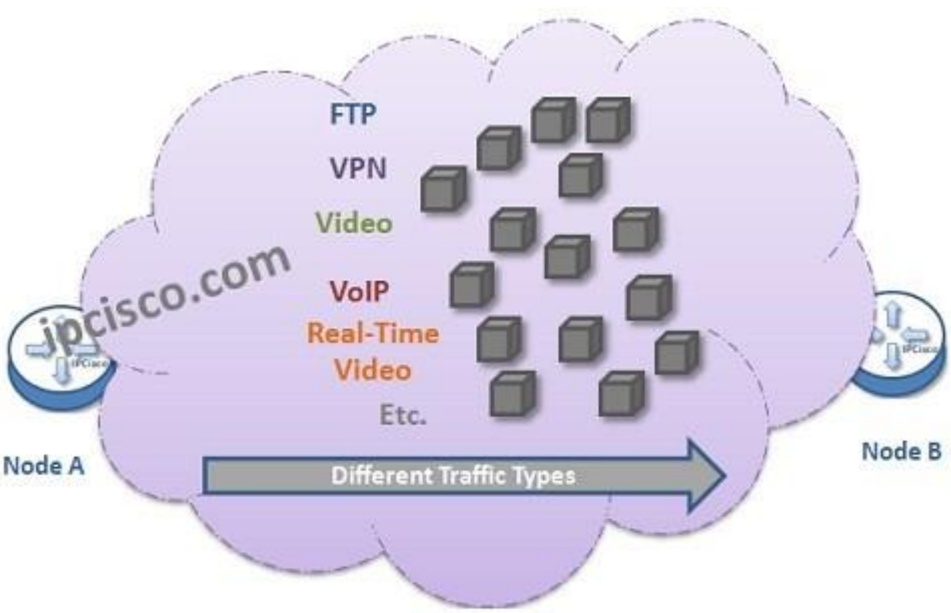
- **Packet Loss**
- **Jitter**
- **Delay**

You can test your knowledg eon **All Network Questions Page**!

So, what are these terms?

Packet Loss : Losing the packets along the path.
Delay : The time taken from one point to the other along the path.
Jitter : Variable Delay in packet transfer.

There are various types of traffics like **real-time voice, data, streaming video** etc. All of these traffic types need different QoS adjustments. Some of these traffics are very **senstive to delay**, some of them are not. Another is **senstive to packet loss**, for the other, packet loss is not too important.



Let’s give some examples for these different types of traffic to understand better.

As you know, **voice** is a **real-time** traffic. When you talk with another people, the vioce data is created at that time **interactively** by you and this traffic needs to reach to the other end in a very short time. If this is not achieved, then it is not possible to communicate with the person at the other end. So, voice traffic is **senstive for delays**. Beside, your voice data must not have a variable delays, jitter. Because, this also makes the communication worst. Lastly, for a good communication, your sentences need to be clear without any loss. All your talking need to be heared at the other end. This makes voice traffic also **packet loss senstive**.

QoS Service Models

QoS (Quality of Service) can be implemented with different Service Models. There are three main QoS Service Models. These QoS Service Models are given below:

- **Best Effort**
- **Integrated Services**
- **Differentiated Services**

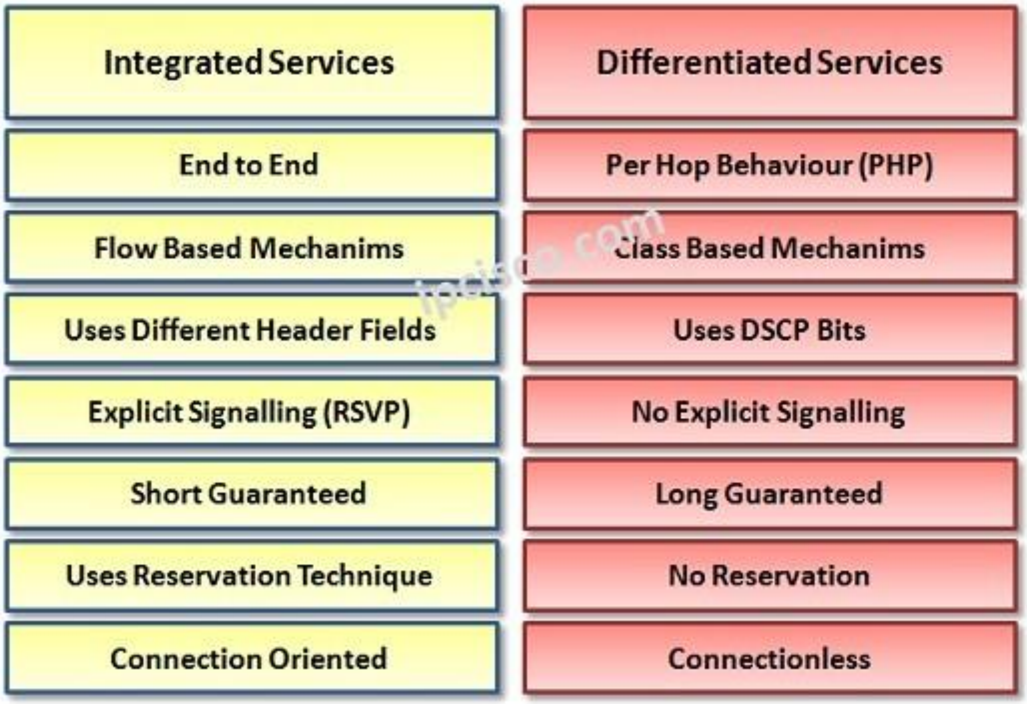
Best Effort is the simplest Service Model. It is also known as a model without QoS. In other words, thi sis the model that there is no QoS Adjustments.

In this model, all the traffic are seem similar. So, all the behaviours are same to all types of traffics. The only parameter is the time. In **Best Effort** traffic, always the first come packets, are sent firstly.

Integrated Services is the second QoS Model in which, applications requests QoS from the network's control plane. With an explicit signalling, Integrated Services QoS instruct the network that it need QoS. In other words, it requests a reservation. For this explicit signalling, **RSVP (Resource Reservation Protocol)** is used. After this request, it gets specific QoS parameters associated to that traffic and after the confirmation, the data is sent.

Differentiated Services is the third QoS Model. In this model, there is no prior reservation technique. In Differentiated Services Model, the network classifies the different types of traffic into groups. After that it marks these groups with **DSCP** values. All the groups are behaved with different QoS values. There is no explicit signalling before the data sent in Differentiated Services. And Differentiated Services is implemented **per hop**. **Differentiated Services** uses **DS Feilds** in **ToS (Type of Service)** field.

As a summary, you can find the below comparison of **Integrated Services** and **Differentiated Services**.



Integrated Services	Differentiated Services
End to End	Per Hop Behaviour (PHP)
Flow Based Mechanims	Class Based Mechanims
Uses Different Header Fields	Uses DSCP Bits
Explicit Signalling (RSVP)	No Explicit Signalling
Short Guaranteed	Long Guaranteed
Uses Reservation Technique	No Reservation
Connection Oriented	Connectionless