Quality of Service – QoS Udemy Course Notes

Definition – providing a better quality to certain applications at the detriment of other applications.
Managed Unfairness
Priority to some sessions over other sessions
Voice and Video (Usually UDP) (Delay and Drop Sensitive) get priority over non delay sensitive applications

Three Traffic Types
- Data
- Voice
- Videos

Data
Bursty
Greedy – grabs as much bandwidth as is allocated
Drop-insensitive – if a packet is dropped, it is just resent
Delay-insensitive – latency is not a problem
TCP – most common for data applications, as there is guaranteed delivery

2 major types of Data applications
Interactive and Non-interactive
Telnet (interactive) - delay will hinder the experience
FTP (non-interactive) - delay will not be noticed, as files as being uploaded or downloaded

Voice
Smooth – uses a steady stream of bandwidth
Benign – opposite of greedy, they do not try to grab bandwidth from other applications
Drop-sensitive – if packets are dropped, the call quality degrades
Delay-sensitive – requires sub-150ms latency, otherwise the two ends of the calls are receiving the voice late
UDP – no ability to resend lost packets, best effort delivery

One-way requirements for Voice
Latency – <150ms
Jitter - <30ms
Loss <1%
Bandwidth (30-128kbps) (depends on codec)

Video
Bursty
Greedy
More movement requires more bandwidth
Delay-sensitive
Delay-sensitive

One-way requirements for Video
Latency – <150ms
Jitter - <30ms
Loss – 0.1 - 1.0%
Bandwidth (384kbps – 20+Mbps) (depends on resolution, color bitrate, fps, etc.)

Cisco Enterprise QoS Solution Reference Network Designs (SRND) Guide
This is a great resource

Loss - A relative measure of the number of packets that were not received compared to the total number of packets transmitted. Loss is typically a function of availability. If the network is Highly Available, then loss during periods of non-congestion would be essentially zero. During periods of congestion, however, QoS mechanisms can determine which packets are more suitable to be selectively dropped to alleviate the congestion.

Delay - The finite amount of time it takes a packet to reach the receiving endpoint after being transmitted from the sending endpoint. In the case of voice, this is the amount of time it takes for a sound to travel from the speaker's mouth to a listener's ear.

Delay variation (Jitter) - The difference in the end-to-end delay between packets. For example, if one packet requires 100 ms to traverse the network from the source endpoint to the destination endpoint and the following packet requires 125 ms to make the same trip, then the delay variation is 25 ms.

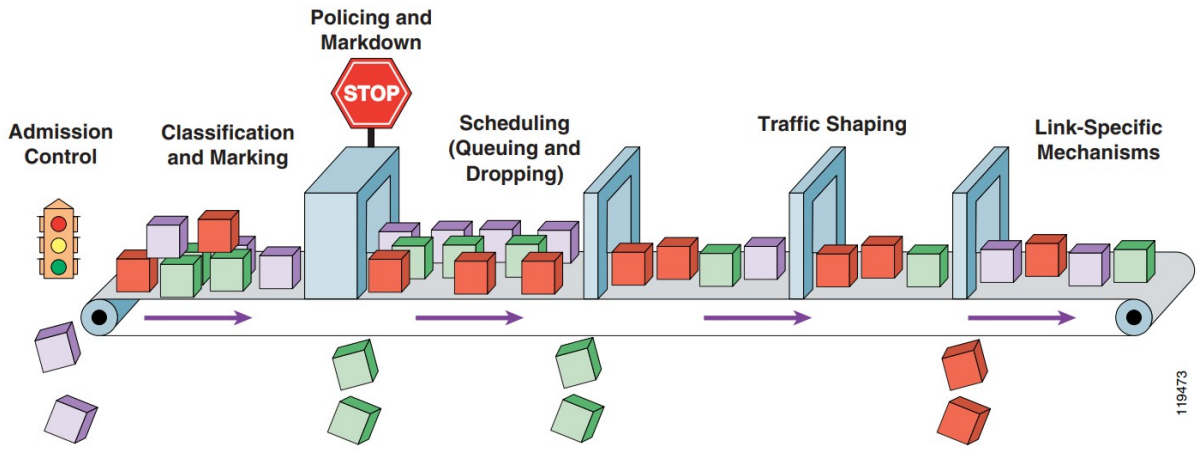
Keys QoS Concepts for the CCNA

- Marking
- Device Trust
- Prioritization
    - Voice
    - Video
    - Data
- Shaping
- Policing
- Congestion Management

Cisco QoS Toolset

- Classification and Marking tools
- Policing and Markdown tools
- Scheduling tools
- Link-specific tools
- AutoQoS tools
- Call Admission Control tools

Figure 1-1 The Cisco QoS Toolset



Classification and Marking
Label (a marking) applied to specific packets that tells each router and switch along the network path the priority level of the given packet.
Marking is done at Layer 2 or at Layer 3
When a marked packets arrive at a switch, the switch needs to decide what "class" the packets go into and the switch will then treat the packets per the class specifications.

Layer 2 Marking
EthII packet

Dest Add	Source Add	802.1Q | contains a 3bit priority header called COS – Class of Service	Voice Data

COS (Class of Service) – has 0 to 7 as possible value.
000 – 0
001 – 1
110 – 5 Used by Voice
111 – 7

Phone, switch, and router need to agree of COS parameters
The problem with Layer 2, 802.1Q, specifying the COS is the link between the Switch and the Router needs to be a 802.1q Trunk connection. Therefore, you may want to use a Layer 3 marking.

Layer 3 Marking
Marking would be done with an IPv4/IPv6 Header

ToS (Type of Service) Field:
Contains 8 binary values (0000 0000)
We used to only look at the most significant 3 bits (000x xxxx) – Values are 0 to 7 (voice is a 5)
The problem with this is there are only 8 options for ToS priority. The values were also not standardized
A value of 0 (000) would indicate best effort delivery
Often a value of 6 or 7 would be used for routing protocols
Adjusted to use 6 binary bits (0000 00xx) and is known as DSCP
DSCP (Differentiated Service Code Points) – same field in the IPv4 header, the interpretation of the bits is different, 6 bits are used instead of 3 bits (ToS) to determine how the packet is marked.
When 3 bits are used, it is known as IPP (IP Precedence)
When 6 bits are used, it is known as DSCP (Differentiated Service Code Points)
DSCP is backwards compatible to IP precedence.
The most significant 3 bits (IPP) are known as CS (Class Selector) Values
Voice data can be called IPP 5 (IP Precedence 5) or as CS 5 (Class Selector 5), it depends if they are using the old terminology or the new DSCP terms.

DSCP continued – (Note: in DSCP, Class Selector Values still exist) (Most significant bits are CS/IPP)
000 000 – when the 6 bits are set to 0, this denotes "best effort delivery"
001 000 – IPP 1 / CS 1

What are two field names corresponding to the IPv4 header field and the IPv6 header field that contain Differentiated Services Code Point (DSCP) markings? (Choose two.

The correct answers are **traffic class** and **type of service (ToS)**. In the original RFC definitions of the ToS field, IP precedence was a 3-bit sub-field.

Assured Forwarding Class

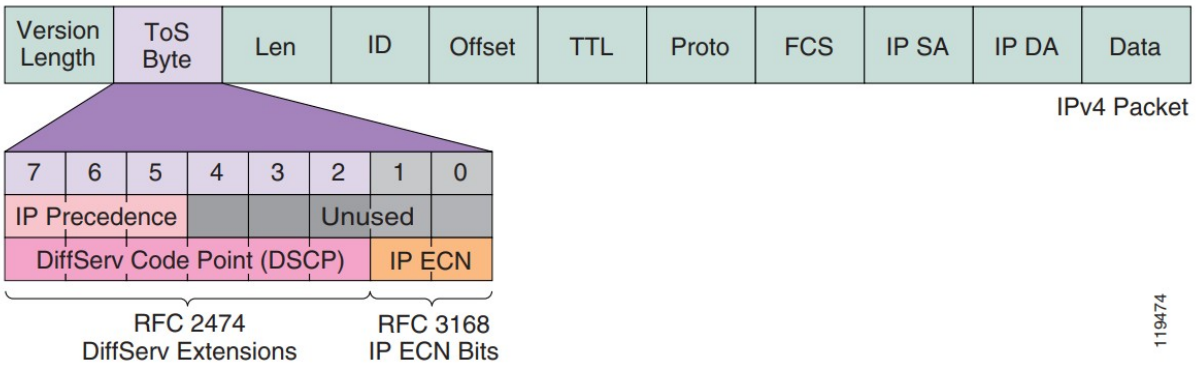
- 001 001 – AF 1 1 Assured Forwarding Class 1 - 1
- 001 010 – AF 1 2 Assured Forwarding Class 1 - 2
- 001 110 – AF 1 3 Assured Forwarding Class 1 - 3
- 001 100 – AF 1 4 Assured Forwarding Class 1 - 4

AF1 to AF4 (the digit refers to the binary value of the first 3 bits) (000 XXX) (0's represents AF Values)
The first 3 binary digits (000 XXX) represent how important the traffic is (AF 1 is more important than AF 4)
The second digit (AF 1 **1**) represents how likely it is packets will be dropped
(Higher Number = More likely to be dropped)

Assured Forwarding Values (1st 3 bits = AF Class) (Bits 4+5 = Drop Probability) (Last bit = DS0 is always 0)

Drop	Class 1	Class 2	Class 3	Class 4
Low	001010 AF11 DSCP 10	010010 AF21 DSCP 18	011010 AF31 DSCP 26	100010 AF41 DSCP 34
Medium	001100 AF12 DSCP 12	010100 AF 22 DSCP 20	011100 AF32 DSCP 28	100100 AF42 DSCP 36
High	001110 AF13 DSCP 14	010110 AF23 DSCP 22	011110 AF33 DSCP 30	100110 AF43 DSCP 38

Figure 1-2 The IP ToS Byte (DSCP and IP ECN)



ToS Byte

1	0	1	T2	T1	T0	CU2	CU0

DiffServ Field

1	0	1	0	0	0	ECN	ECN

The DiffServ standard utilizes the same precedence bits (the most significant bits–DS5, DS4 and DS3) for priority setting, but further clarifies the definitions, offering finer granularity through the use of the next three bits in the DSCP. DiffServ reorganizes and renames the precedence levels (still defined by the three most significant bits of the DSCP) into these categories (the levels are explained in greater detail in this document):

Precedence Level	Description
7	Stays the same (link layer and routing protocol keep alive)
6	Stays the same (used for IP routing protocols)
5	Express Forwarding (EF)
4	Class 4
3	Class 3
2	Class 2
1	Class 1
0	Best effort

With this system, a device prioritizes traffic by class first. Then it differentiates and prioritizes same-class traffic, taking the drop probability into account.

The DiffServ standard does not specify a precise definition of "low," "medium," and "high" drop probability. Not all devices recognize the DiffServ (DS2 and DS1) settings; and even when these settings are recognized, they do not necessarily trigger the same PHB forwarding action at each network node. Each node implements its own response based on how it is configured.

Within the ToS byte
The most significant 6 bits are used for DSCP (Differentiated Service Code Points) (aka DiffServ)
The least significant 2 buts are used for ECN (Explicit Congestion Notification) (ECN not in CCNA)
7 is the highest value for the most important network protocols (link layer and routing protocol keep alives)
Expediated Forwarding (EF)

RFC Definition (2598) – The EF PHB (per-hop behavior) can be used to build a low loss, low latency, low jitter, assured bandwidth, end-to-end service through DS (DiffServ) domains.
Such a service appears to the endpoints like a point-to-point connection or a 'virtual leased line.'
This service has also been described as *Premium Service*.
DSCP value of 101110 (binary value) is recommended for the EF PHB, which corresponds to a DSCP value 46.
Forwarding Per-Hop Behavior (PHB) is a mechanism used in Quality of Service (QoS) to control the behavior of packets as they traverse a network. The following are some of the key components of PHB:

- Classification: This is the process of categorizing network traffic into different groups based on specific criteria such as IP address, protocol, port, or application type.

- Marking: This is the process of setting a marking or tag on a packet, indicating its priority level or class. Marking is typically done at the edge of the network and is used by the network devices to make QoS decisions.

- Queuing: This is the process of holding packets in a queue and scheduling their transmission based on their priority. Queuing algorithms, such as Weighted Fair Queuing (WFQ), ensure that high-priority packets are transmitted before low-priority packets.

- Congestion: This occurs when the network becomes congested and there is not enough bandwidth to handle all the traffic. PHB includes mechanisms, such as Random Early Detection (RED), to help manage congestion by discarding low-priority packets before high-priority packets.

- Policing: This is the process of monitoring network traffic and enforcing specified traffic rate limits. If a packet exceeds the specified rate limit, it can be discarded or marked with a lower priority.

- Shaping: This is the process of controlling the rate at which packets are transmitted into the network. This helps to ensure that the network does not become congested and that all packets are transmitted in a timely manner.

The combination of these components in PHB helps to ensure that network traffic is managed in a way that meets the needs of the different applications and users, while also maintaining network performance and stability.

IOS DSCP Settings

```
Router1(config)# access-list 101 permit ip any any ?
dscp        Match packets with given dscp value
fragments   Check non-initial fragments
log         Log matches against this entry
log-input   Log matches against this entry, including input interface
precedence  Match packets with given precedence value
time-range  Specify a time-range
tos         Match packets with given TOS value
```

When you specify the *ip dscp* value in the **class map** command, you have these:

```
Router(config)# class-map match-all VOIP
 1751-uut1(config-cmap)# match ip dscp ?
   <0-63>   Differentiated services codepoint value
   af11     Match packets with AF11 dscp (001010)
   af12     Match packets with AF12 dscp (001100)
   af13     Match packets with AF13 dscp (001110)
   af21     Match packets with AF21 dscp (010010)
   af22     Match packets with AF22 dscp (010100)
   af23     Match packets with AF23 dscp (010110)
   af31     Match packets with AF31 dscp (011010)
   af32     Match packets with AF32 dscp (011100)
   af33     Match packets with AF33 dscp (011110)
   af41     Match packets with AF41 dscp (100010)
   af42     Match packets with AF42 dscp (100100)
   af43     Match packets with AF43 dscp (100110)
   cs1      Match packets with CS1(precedence 1) dscp (001000)
   cs2      Match packets with CS2(precedence 2) dscp (010000)
   cs3      Match packets with CS3(precedence 3) dscp (011000)
   cs4      Match packets with CS4(precedence 4) dscp (100000)
   cs5      Match packets with CS5(precedence 5) dscp (101000)
   cs6      Match packets with CS6(precedence 6) dscp (110000)
   cs7      Match packets with CS7(precedence 7) dscp (111000)
   default  Match packets with default dscp (000000)
   ef       Match packets with EF dscp (101110)
 Router1(config-cmap)# match ip dscp af31
```

Once you classified / matched on traffic, you need to do something with it; queue, prioritize, delay, drop, or rate-limit the classified/matched traffic.

Matching Criteria

CAR and class-based policing support different packet header values on which you can match to classify your traffic. Traffic matching defines the process of identifying traffic for rate limiting and/or packet marking.

Classification and Marking Tools

Classification and marking tools set this trust boundary by examining any of the following:

- Layer 2 parameters
  - 802.1Q Class of Service (CoS) bits,
  - Multiprotocol Label Switching Experimental Values (MPLS EXP)
- Layer 3 parameters
  - IP Precedence (IPP)
  - Differentiated Services Code Points (DSCP)
  - IP Explicit Congestion Notification (ECN)
  - Source/Destination IP address
- Layer 4 parameters
  - L4 protocol (TCP/UDP)
  - Source/Destination ports
- Layer 7 parameters
  - application signatures via Network Based Application Recognition (NBAR)

Trust Boundaries

The location in the network where packets are classified and marked.

Typically, a switch will not trust the ToS markings of a PC, but may trust the IP Phone with it ToS markings. An IP phone will tell a switch, by using a marking, that its traffic is very important. The switch needs to be configured to trust that marking from the phone.

Untrusted Domain: The part of the network that you are not managing (e.g., Printer or PC)
From a QoS point of view, you are not going to trust the markings sent by a PC

Trusted Domain: The part of the network that only administrators can manage (e.g., Routers, Switches, Phones)

In an enterprise network, the trust boundary is usually at the edge of the network
For an ISP, the trust boundary is usually located at the last device they manage (router/switch)

By default, Cisco routers will override any QoS markings they receive on an untrusted boundary.
So, voice and data traffic will be treated the same if you don't re-mark that traffic.

Traffic Classes

Before traffic policies can be applied to a packet, the packets need to be put into a class.
Classify and mark as close to the edge of the network as possible (best practice).
IP phones will mark their packets as they leave the IP phone.
For other traffic types you want to do your classification and marking on your edge switches.
Marking takes place on the edge, but every device along the path uses classification to determine what quality of service that traffic gets.

You can do your classification based on three criteria.

1. Marking – in a header (CoS or DSCP value)
2. IP Addressing – such as Destination/Source IP Subnet, Layer II Mac Address, Destination Port #, or domain address (cisco.com vs facebook.com)

3. Deep payload inspections using Application Signature - Network Based Application Recognition (NBAR)

Network Based Application Recognition (NBAR)
Uses Layers 4-7 and is more CPU intensive
Generally, only done at edge of network

2 Modes of Operation for NBAR
1. Passive Mode
    - Provides real-time statistics on application per protocol or interface and gives bidirectional statistics such as bit rate, packet, and byte counts.
2. Active Mode
    - Classifies application for traffic marking, so that QoS policies can be applied.

Policing and Shaping
Once traffic is identified it can be treated in a number of different ways, min bandwidth, max bandwidth, rate limit on bandwidth,
Policing and shaping limit the amount of traffic that you can transmit, aka they act as rate limiters.
Policers will drop excess traffic
Shapers will delay excess traffic

Policers – perform check for traffic violations against a configured rate.
You can configure a policer to send the traffic without modification, re-mark the traffic and still transmit (provided you are below the bandwidth threshold), or drop the traffic the traffic.
There can be two traffic thresholds.

Tri-Color implementation
Below the threshold – transmitted as normal
Exceeds the first threshold – re-marked to a lower class and still transmitted
Exceeds the second threshold – dropped

Shapers – Doesn't drop the traffic, rather it smooths the traffic out by delaying the traffic. So, that after a period of time, the traffic falls within a specified bitrate.
Are usually used to meet Service Level Agreements. When the traffic spikes above the contracted rate, the excess traffic is buffered and is delayed until it falls below the contracted rate.

Policers are much harsher than Shapers, as they will drop traffic rather than delay traffic.
Shapers will attempt to smooth traffic out by buffering excess traffic.

Where to use Policers and Shapers
Policers are generally used as "Ingress Tools". The traffic is dropped before it is processed (so you don't waste resources). If a packet is going to be dropped anyway, it best to drop it on the ingress interface (incoming interface), so you don't waste valuable bandwidth and CPU cycles.
Policers can be used on egress ports (exit interface) to control the traffic coming out of an interface,
Disadvantage of policers is that it is dropping packets which results in TCP resends. Doesn't introduce jitter or delay, as they simply drop the packet.
Disadvantage of shapers in that they introduce jitter and delay when they slow down / buffer packets.
Shapers result in fewer TCP retransmissions.

Queuing Mechanisms

Congestion Management

Queuing or Buffering – determines the ordering of packets and the output buffers. Determines how traffic leaves a router or switch interface.

Round Robin Queuing Mechanism – All traffic is treated the same way (Real Time Traffic)

Strict Queuing Mechanism – High priority traffic is handled first. This can lead to starvation of bandwidth to lower priority traffic as all the bandwidth is going to higher priority traffic.

There are both Ingress and Egress Queuing Mechanisms

Egress Queuing Mechanisms

Queuing is only required when there is congestion. When queues fill up packets are reordered, so higher priority packets will leave the interface first.

- Queuing – is the logic of ordering packets in output buffers
    i. Queuing is only activated when there is congestion on the link.
- Scheduling – is the process of deciding which packet should be sent out next.
    i. Scheduling occurs regardless of whether there is congestion on the link .

FIFO (First in First out)

A single queue with packets that are sent in the exact order that they arrived.
Problem with this mechanism is that voice packets can be delayed by large data packets
Legacy mechanism

PQ (Priority Queue)

Consists of four queue's (High, Medium, Normal, and Low) that are served in a strict priority order
The lower priority queues are served only when the high priority queues are empty.
Problem with this mechanism is it can lead to starvation in lower priority queues.

CQ (Custom Queuing)

Consists of 16 queues serviced in a round-robin fashion.
In order to prevent starvation, it provides traffic guarantees.
Problem with this mechanism is that it doesn't provide priority to real-time traffic and introduces delay
If you have important voice traffic arriving it will only be serviced in its round

WFQ (Weighted Fair Queuing)

Algorithm that divides the internet bandwidth by the number of flows.
Provides a good service for real-time traffic.
No bandwidth guarantees for particular flows.
Some flows can starve other flows.

WFQ Scheduling Algorithm

Incoming packets are classified by flows rather than classes.
Flows are classified by source/destination IP Address, the protocol, and a port number.
A "weight" is added to a "flow" based on certain criteria (IPP or RSVP - Resource Reservation Protocol)
Prioritizes smaller packets over larger packets.
More Fair queuing algorithm, in that it provides better QoS for small packets (which are generally used for interactive sessions) (example: voice packet may be 20 bytes in size, while an FTP packets may be 1500 bytes)
You can increase prioritization by adding a weight to smaller packets (based on IPP for example)
Uses a clever Scheduling Algorithm to prioritize smaller interactive packets, which you can make appear even smaller by increasing the IP Precedence (IPP) of the packet.
Problem with this mechanism is that it doesn't provide Bandwidth Guarantees.

CBWFQ (Class-based Weighted Fair Queuing)

- Guarantees bandwidth to specific classes and provides dynamic fairness of other flows.
- Allows you to create different classes where you can specify a min bandwidth
- Weighted Fair Queuing can be used on the "Best Effort Class" to ensure that traffic is handled fairly.
- Traffic gets fair bandwidth guarantees
- Minimum bandwidth to HTTP, FTP, Voice traffic, Video traffic, etc.
- No Latency guarantees (aka there is no priority queue. Thus, it suitable only for data networks.

LLQ (Low Latency Queuing)

- Basically, is Class-based WFQ with an added priority queue for real-time traffic.
- The priority queue has a minimum bandwidth guarantee, but is also policed (has a max bandwidth limit)
- Minimum bandwidth guarantee for voice and guarantees voice traffic won't starve by having a max bandwidth rate limit for other traffic types.

<u>Ways to Avoid Congestion</u>

Queues on routers and switches are finite, they can only hold or buffer a certain number of packets.
If there is a burst of traffic and the buffers are overrun (more packets are enqueued than dequeued), it will start to drop packets.
Tail Drop – when the queue fills up, all new packets will be dropped.

WRED (Weighted Random Early Detection)

Starts randomly dropping packets from multiple flows before the queue fills up to avoid congestion.
Better utilization of an interface's bandwidth, as some TCP flows are slowing down while others are speeding up simultaneously. Which in aggregate gives you a better utilization of the interface.

Below the threshold – transmitted as normal, no packets are dropped
Exceeds the minimum threshold – random drops of packets
Exceeds the maximum threshold – Full drops of a traffic class

The Weighted part of WRED has to do with our ability to apply a weight to certain types of traffic. E.g., drop FTP traffic before dropping HTTP traffic. Preselect which packets will get dropped.
Typically, you only want to drop TCP packets because TCP flows will retransmit.
Allows for buffer space to be left for voice packets.