QoS Implementation Techniques

SEC-1

Video Tutorial - QoS Implementation Techniques

Click Play for an overview of classification, marking, trust boundaries, congestion avoidance, shaping and policing.

SEC-2

Avoiding Packet Loss

Now that you have learned about traffic characteristics, queuing algorithms, and QoS models, it is time to learn about QoS implementation techniques.

Let's start with packet loss. Packet loss is usually the result of congestion on an interface. Most applications that are delay-sensitive are also intolerant of packet loss. TCP automatically adjusts to network congestion. Unless TCP segments cause TCP sessions to resume their sessions later, frame applications do not use TCP and cannot recover from dropped packets.

The following approaches are common ways to remedy congestion:

- Increase the capacity to lease or unleash congestion.
- Implement congestion avoidance to monitor traffic loads to anticipate and avoid congestion at common points in a network.
- Implement congestion management tools to prioritize and accommodate bursts of traffic from Voice, Video, MPLS, VMWAREs, and CLOS can guarantee bandwidth and provide prioritized forwarding to voice packets, application.
- Drop lower priority packets before congestion occurs. Since ECN (QoS provides queuing mechanisms, such as weighted random early detection (WRED), that start dropping low priority packets before congestion occurs.

SEC-3

QoS Tools

There are three categories of QoS tools, as described in the table:

- Classification and marking tools
- Congestion avoidance tools
- Congestion management tools

Tools for Implementing QoS

QoS Tools	Description
Classification and marking tools	• Packets are analyzed to determine what traffic class they belong to. When the traffic class is determined, the packet is marked.
Congestion avoidance tools	• Traffic classes are allotted portions of network resources, as defined by the QoS model. • Congestion avoidance tools monitors how traffic is flowing within the network to anticipate congestion. Whenever, congestion is starting to assert congestion. • Congestion avoidance tools can then drop lower priority packets and start to send to impacts TCP sessions traffic to accommodate efficient network control and avoid congestion.
Congestion management tools	• When traffic exceeds available network resources, traffic is queued to await availability of resources. • Common Cisco IOS based congestion management tools include WRED and LLQ algorithms.

Refer to the figure to fully understand the sequence of how these tools are used when QoS is applied to packet flows.

QoS Sequence

As shown in the figure, frames (packets) (grey squares) are classified and then separated off inside the interface (colored squares). To which congestion, policers are then allocated resources based on arbitrary policies. Packets are then queued and scheduled out the egress interface based on their defined QoS shaping and policing policy.

Note: Classification and marking can be done on ingress or egress, whereas other QoS actions such queuing and shaping are usually done on egress.

SEC-4

Classification and Marking

Before a packet can have a QoS policy applied to it, the packet has to be classified. Classification and marking allows us to identify or "mark" types of packets, so that network devices can apply QoS policies to the packets. Classification and marking is the first step in a QoS implementation.

Cisco supports a variable sequence on the QoS implementation. Methods of marking traffic flows on Layer 2 (L2) include using 802.1Q, 802.1p, and Cisco Inter-Switch Traffic Link also the classification of Layer 3 (L3) using Network Based Application Recognition (NBAR).

Note: NBAR is a classification and protocol discovery feature of Cisco IOS software that works with QoS features. NBAR is not of scope for this course.

Marking means that we are setting a value in the packet header. Devices receiving the packet look at the marked field to see if it includes a defined policy. Marking packets allows us to maintain QoS settings throughout the network, as the packet traverses the network.

Cisco traffic is marked using classes of service. The table in the figure describes the Cisco traffic classes and defines bandwidth. The direction of whether to mark traffic at Layers 2 or 3 or both is not clear and should be made after consideration of the following points:

- Layer 2 marking is preferred if the frame does not leave the LAN.
- Layer 2 marking of frames only that QoS policies classifiers the packets that are sent "off subnet".
- Layer 3 marking will only be lost if/when packets are sent.

Traffic Marking for QoS

QoS Tools	Layer	Marking Field	Width in Bits
802.1Q (ISL)	2	User Priority (UP)	3
802.1 (ISL-ID)	2	ID of Traffic Identifier (TID)	3
MPLS	2	Experimental (EXP)	3
IPv4 and IPv6	3	IP Precedence (IPP)	3
IPv4 and IPv6	3	Differentiated Services Code Point (DSCP)	6

SEC-5

Marking at Layer 2

802.1Q is the IEEE standard that supports VLAN tagging on Layer 2 on Ethernet networks. When 802.1Q is implemented, two fields are added to the Ethernet Frame. As shown in the figure, these fields are inserted into the Ethernet frame after the source MAC address field.

Ethernet Class of Service (CoS) Values

The PRI (3 bitstream) are mapped into the packet header and are known as IEEE 802.1p. The 802.1p is standard, also the Ethernet data link the Tag Control Information (TCI) field. Known as the Priority (PRI) field, the 3 bit field identifies the Class of Service (CoS) bookings. These bits make a Layer 2 Ethernet frame can be marked with one of eight levels of priority (values 0-7) as displayed in the figure.

Ethernet Class of Service (CoS) Values

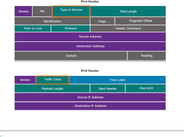
CoS Value	CoS Name	Description
0	BE	Best-Effort Data
1	BK	Network Priority Data
2	EX	Critical Priority Data
3	CR	Call Signaling
4	VI	Video Data
5	VO	Voice/Conferencing
6	IN	Voice Internal Control (traffic)
7	NC	Reserved
8	NC	Reserved

SEC-6

Marking at Layer 3

IPv4 and IPv6 specify an 8 bit field (octet) reserve in each packets. As shown in the figure, both IPv4 and IPv6 support an 8 bit field for marking, the "Type of Service" (ToS) field in IPv4 and "Traffic Class" in IPv6.

IPv4 and IPv6 Packet Headers



SEC-7

Type of Service and Traffic Class Field

The Type of Service (ToS) and Traffic Class (TfC) are the general header fields supported by the QoS classification tools. The field is then referred to by marking options which forward the packets based on the appropriate assigned QoS policy.

The figure displays the contents of the ToS field. In RFC 791, the original IP version specified the IP Precedence (IPP) field the ToS field. In RFC 2474 and 2475 (RFC 2475 updates RFC 1349), the IETF changed the ToS field to the DiffServ field.

RFC 2474 supersedes RFC 791 and redefines the ToS field by renaming and redefining the IPP field. The new field, as shown in the figure, now is fully attributed the QoS bytes the Differentiated Services Code Point (DSCP). Now, known as the DiffServ or Internet of Life protocol, consists of 64 bits. The remaining 2 bits IP Protocol 4 Congestion Notification (ECN) field. The ECN field is optional. The ECN field is used to inform routers of congestion. If the ECN settings inform congestion routers have to corresponds in the sender flow.

SEC-8

DSCP Values

The 64 DSCP values are organized into three categories:

- **Class Selector (CS):** This is the referred to as IP precedence. The DSCP which is 0. The pgc bop behavior is normal coding. When a node supplemental congestion, these packets are dropped. Class selector (CS) is 3 bits.
- **Assured Forwarding (AF):** RFC 2430 defines AF as the DSCP assured per hop. The AF class (1-4) is using the lower 3 bits of the DSCP. Each class is assigned a drop preference (low, medium, high) and is represented by the last 2 bits of the DSCP.
- **Expedited Forwarding (EF):** RFC 2598 defines EF as per hop. It is most significant DSCP bits. In binary causes zero drop preference. The definition of EF is illustrated in the Assured Forwarding table.

Assured Forwarding Values

	Assured Forwarding Values		
	Low Drop	Medium Drop	High Drop
Class 4	AF41 [34]	AF42 [36]	AF43 [38]
Class 3	AF31 [26]	AF32 [28]	AF33 [30]
Class 2	AF21 [18]	AF22 [20]	AF23 [22]
Class 1	AF11 [10]	AF12 [12]	AF13 [14]

Worst Queue

Best Queue

The AFxy formula is specified as follows:

- The first 3 bits significant bits are used to designate the class. Class 4 is the best service and Class 1 is the worst service.
- The next two bits are used to designate the drop preference.
- The last bit is reserved for a zero.

For example, AF31 belongs to class 3 (binary 011) and has a medium drop preference (binary 10). The full DSCP value is 26 because you include the 0011 (or binary 011 0100).

SEC-9

Class Selector Bits

Because the first 3 bits of significant bits of the DSCP field indicate the class, these bits are also called the Class Selector (CS) bits. These 3 bits map directly to the 3 bits of the ToS field and the IPP field in version compatibility with RFC 791, and RFC 791, as known in the figure.

Layer 2 CoS and Layer 3 ToS

The bits in the figure shows how the 3 bit values map to the Class Selectors and the corresponding DSCP in decimal. The table lists all 64 values in the Class Selectors.

Mapping CoS to Class Selectors in DSCP

CoS values, Class Selectors, and corresponding DSCP 6-bit value

CoS Value	CoS Binary Value	Class Selector (CS)	CS Binary	DSCP Decimal Value
0	000	CS0/DF	000 000	0
1	001	CS1	001 000	8
2	010	CS2	010 000	16
3	011	CS3	011 000	24
4	100	CS4	100 000	32
5	101	CS5	101 000	40
6	110	CS6	110 000	48
7	111	CS7	111 000	56

SEC-10

Trust Boundaries

Where should markings occur? Traffic should be classified and marked as close to its source as technically and administratively feasible. This attributes the trust boundary to the following devices:

- Trusted endpoints (hosts that accomplishes and intelligent to mark appropriate traffic values based on application or source IP/MAC address, Example of trusted endpoints include IP phones, wireless access points, videoconferencing gateways and systems, IP videoconferencing stations, and hosts.
- Switches, routers, and access servers.
- Traffic can also be marked at peer 2 networks / clients.

Be marking traffic, for example, on incoming QoS values 46 (Precedence) or DSCP (AF41, or typically necessary).

Various Trust Boundaries

SEC-11

Congestion Avoidance

Congestion management includes queuing and scheduling methods where network traffic is buffered or queued (and sometimes dropped) when it is held to wait on congestion to clear. Congestion avoidance is a QoS tool that is used to monitor network traffic flows to anticipate and avoid congestion at common points in a network. Congestion avoidance tools monitors congestion levels and start dropping packets. These tools are used to monitor traffic flows to anticipate congestion. When the queue is below the minimum threshold, packets are not drop. At the queue fill up to the maximum threshold, a small percentage of packets are dropped. When the maximum threshold is reached, all packets are dropped.

Congestion Avoidance Mechanisms

Some congestion avoidance techniques provide preferential treatment for certain priorities with QoS prospect. For example, Cisco IOS includes weighted random early detection (WRED) as a common congestion avoidance scheme. The WRED algorithm allows for congestion avoidance on interface interfaces by providing traffic management and early packet discard. This algorithm can selectively discard lower priority traffic when the interface begins to get congested and provide differentiated performance characteristics for different classes of service. Configuration options are provided to control how much traffic is dropped in each class of service. WRED can also be configured to differentiate traffic by IP precedence or DSCP values. Cisco IOS also supports DSCP-based WRED, which uses the DSCP value to determine packet drop probability.

SEC-12

Shaping and Policing

Traffic shaping and traffic policing are two mechanisms provided by Cisco IOS QoS software to prevent congestion.

Traffic shaping defines some boundary in queue and then schedules the traffic for later transmission (per bucketed) at time. The result of traffic shaping is a smoothed out traffic flow over time.

Shaping Traffic Example

Shaping creates the existence of a queue and of sufficient memory to buffer delayed packets, while policing does not.

Ensure that you choose efficient resource utilization. Shaping is a useful mechanism to optimize network resources (for sent transmission of any delayed packets). Then, scheduling function allows you for pugnacious the shaping queue has different queues. Examples of scheduling functions are CBWFQ and LLQ.

Policing can enforce on traffic properties using an interface or subinterface. Policing is also applied to packets ingress to interface traffic on an interface. When traffic exceeds a configured rate, the router can drop packets or change the IP precedence or DSCP value of the packet.

Policing is commonly implemented by service providers to enforce a contracted customer information rate (CIR). However, the service provider may also allow bursting over the CIR that is allowed in a network experiencing congestion.

Policing Traffic Example

SEC-13

QoS Policy Guidelines

Your QoS policy future updates the QoS plan focus second to destinations. If you discuss it the plan is using a different policy than desired, then the entire QoS policy is ineffective. Ensure that you have a well-defined QoS policy before implementing QoS. Ensure that you have a well-defined QoS plan before implementing QoS.

- Ensure that you have a well-defined QoS policy before implementing QoS.
- Ensure that you have a well-defined QoS plan before implementing QoS.
- Ensure that you have a well-defined QoS plan before implementing QoS.

SEC-14

Check Your Understanding – QoS Implementation Techniques

Check your understanding of assessing algorithms by choosing the BEST answer to the following questions.

1. Which criteria does traffic need to undergoing classmate can see drop excess traffic?
   - traffic policing
   - traffic shaping
   - traffic marking
2. Which classification and class of traffic assess or Tunnel belong to.
   - marking
   - classification
   - traffic shaping
3. Which voice is ideal for the packet header?
   - marking
   - classification
   - MQ-10
4. Which provides better management and allows TCP traffic to throttle back before buffers are overcrowded?
   - traffic policing
   - MQ-10
   - WRED
5. Which criteria should operators in a queue and then schedules the sources for later transmission and congestion?
   - WRED
   - traffic policing
   - traffic shaping

Check

Show Me

Reset