Video Tutorial – QoS Implementation Techniques (9 min)

We can categorize QoS implementation tools into three broad categories: classification and marking tools, congestion avoidance tools, and congestion management tools. Under classification and marking tools, session traffic is classified into different priority groupings, and packets are marked. Under congestion avoidance tools, traffic classes are allotted network resources. Some traffic may be selectively dropped, delayed, or remarked to avoid congestion. Weighted random early detection regulates TCP data traffic in a bandwidth efficient manner before tail drops caused by queue overflows basically congestion occurs.

Under congestion management tools, when traffic exceeds available network resources, or we have congestion, then traffic is queued to await the availability of those resources. Common Cisco IOS based congestion management tools include class based weighted fair queuing, and low latency queuing, or the CBWF queue and LL queue algorithms. If we look at this diagram you can see the three sets of tools being used in sequence. From the Ingress interface on a router, to the Egress, or exit interface of the router you can see that traffic is first classified and then marked.

Notice in the graphic how the packets before being classified are all seen here as gray. As they're classified into different classes, they're marked in the IP headed indicated here with the colorization of the different packets. Congestion avoidance is where traffic is policed and selectively dropped. This is where network resources are allotted into different priorities. Packets are put into different queues based on different weights, or sizes. The main congestion avoidance tool that's used in Cisco devices is weighted random early detection, or W-RED. If queue buffers fill up, packets may be dropped proactively as to avoid congestion. Lastly we have the congestion management section where packets are put into their queues, and are scheduled and shaped based on the network priorities, or policies that have been applied.

If we look a little closer at QoS traffic marking, we can see that traffic marking happens at both layer two and layer three. At layer two we have class of service, or COS, which happens using the 802.1Q V-LAN tagging, and 802.1P, quality of service protocols. Traffic marking at layer two happens on the local area network, and is limited to the LAN using layer two switches. Under WiFi traffic marking happens with the WiFi traffic identifier field, or TID. With MPLS you have the experimental or EXP field, also at layer two. At layer three with IPv4 and IPv6, we use the TOS and traffic class fields. Using IP precedence, or IPP, and DSCP, the differentiated services code point. With layer three traffic marking the marking can go from router to router, and therefore the QoS marking can be carried end to end across the network.

In this slide you can see how QoS marking happens at layer two. We have an Ethernet frame, and the 801.1Q protocol can be inserted between the source address and the type length field. You can see the two fields inserted into the Ethernet frame, the TPID field and the TCI field, or tag control information field, which contains a three bit PRI priority field which identifies the class of service, or CoS marking. The class of service markings have six different values, best effort, medium priority data, high priority data, call signaling, video conferencing, and voice bearer for voice traffic. Bit six and seven are reserved for network control information.

At layer three QoS is implemented in the IPv4 and IPv6 packet headers in the type of service field, and the traffic class field. In the older implementation, class of service at layer three was implemented using IPP and ToS. The IP precedence is three bits, and the type of service is five bits. You can see them there in the eight bits. The classifications have eight levels, which map to the layer two class of service. You can see there, routine, priority, immediate flash, flash override, and critical. Once again, value six and seven are reserved for network control information.

The current implementation of QoS uses the differentiated services code point and explicit congestion notification fields, or DSCP and ECN. DSCP and ECN map directly over the eight bits of the IPP and ToS fields. The DSCP field is backwards compatible with the IPP field. You can see in this example that an IPP classification of five involves the one here, and the one here, if you have IPP and you have three bits, then this would be a four and a one, which would be a five. Which would signal a critical flow. Under the DSCP specification, you have six bits. One, two, three, four, five, six. This is a 32, and this is an eight. 32 plus eight is 40, so you can see how it would map a five under IPP using three bits, or a 40 using DSCP using six bits. Since DSCP uses six bits there are 64 possible classifications of traffic.

QoS marking happens at trust boundaries. Marking should happen as close to the source as possible. End points like voiceover IP phones, wireless access points, and video conferencing gateways have the ability to mark QoS packets, as indicated in number one. Traffic can also be marked using layer two switches, as in number two, or at layer three using layer three switches and routers. As packets travel across the network, the remarking of the traffic can be necessary. The remarking of class of service values, or IP precedent values, or DSCP values.

The main mechanism of congestion avoidance in QoS on Cisco routers and switches is weighted random early detection, or W-RED. With weighted random early detection, a percentage of the packets are dropped once we've gone over in a queue the minimum threshold. If the queue has gone over the maximum threshold, then packets are automatically dropped. In this image you can see the difference between traffic policing, and traffic shaping. In traffic policing when the traffic rate reaches the configured maximum rate, excess traffic is dropped. The result is an output rate that appears as a sawtooth with crest and troughs, as shown in the graph at the top. With traffic shaping, excess packets are retained in a queue, and then rescheduled for later transmission over increments of time. The result of traffic shaping is a smooth packet output rate, as shown in the bottom graph.

