



CHAPTER 7

Network Control Technologies

Different applications have different networking requirements. For example, real-time interactive voice requires a low latency network path, but does not require high bandwidth. Quality of Service (QoS) deterministically degrades network service quality to protect the user experience. In the case of voice, queuing delays can occur when there is congestion in a network path. Classifying voice, and placing it in a special queue that is serviced more often, enables the creation of a virtual path having lower latency. However, other traffic now must wait longer to be sent out a network interface. Such deterministic degradation is the fundamental aspect of control optimization. No additional bandwidth is created. Instead, a class of traffic is given special treatment based on its requirements and relative importance, as determined by the network operator.

7.1 QoS Requirements and Placement

As shown in [Figure 7-1](#), the best place to apply QoS policy is on the branch WAN edge, which is usually the branch router WAN-facing interface. This interface has the following characteristics:

- Aggregation point for traffic
 - The WAN interface is often the first location at which many different streams are placed on the same wire. Merging this traffic- can cause contention between different traffic types. These different streams can come from many different paths: multiple interfaces on the branch edge device, optimized traffic from WAAS, and so on.
- Interface speed mismatches
 - The WAN edge interface can be the first point at which traffic must face congestion. In [Figure 7-1](#), for example, the LAN interface might be 100MB, but the WAN facing interface could very well be a T1 (1.5Mb/s). This drastic difference in speed forces congestion and causes some traffic to be dropped.
- Features specific to access technologies
 - Some access technologies, such as Frame Relay, with forward explicit congestion notification/backward explicit congestion notification (FECN/BECN), and cable-modems, with nondeterministic bandwidth) present unique challenges that only QoS awareness at branch edge router can address.

An operator can make relative judgments about how to treat specific traffic classes and apply QoS at the WAN edge router. This requires an awareness of all the traffic exiting a site toward the WAN link.

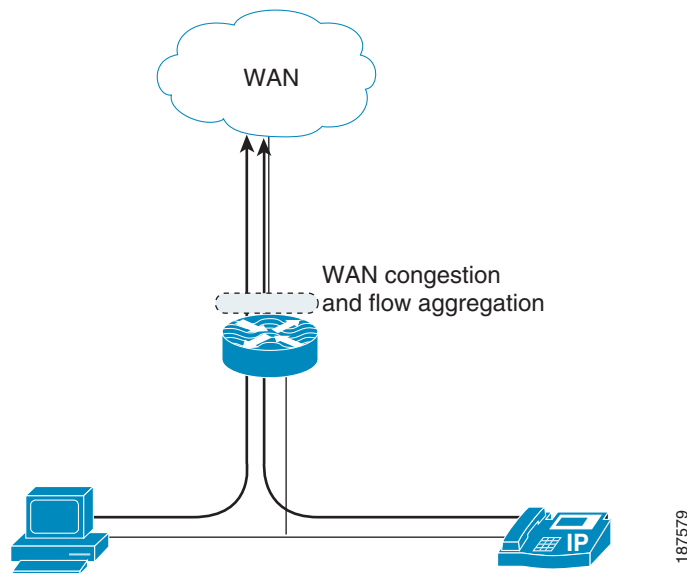
QoS features available in the WAN aggregation router, and WAAS network transparency, correctly identify and separate individual flows to support more granular optimization of application delivery and more effective differentiated services. QoS classifies different WAN flows by IP precedence bits, or by

port levels present in their packet headers. QoS can make efficient use of WAN resources required by mission critical applications. QoS can ensure that the bandwidth and latency requirements for voice and multimedia applications are met, and that excess capacity is shared equally among lower priority applications.

Cisco routers provide an infrastructure for QoS features, including hardware based packet low latency queuing elements, shapers, and policers. For more information, refer to *Enterprise QoS Solution Reference Network Design Guide*:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html

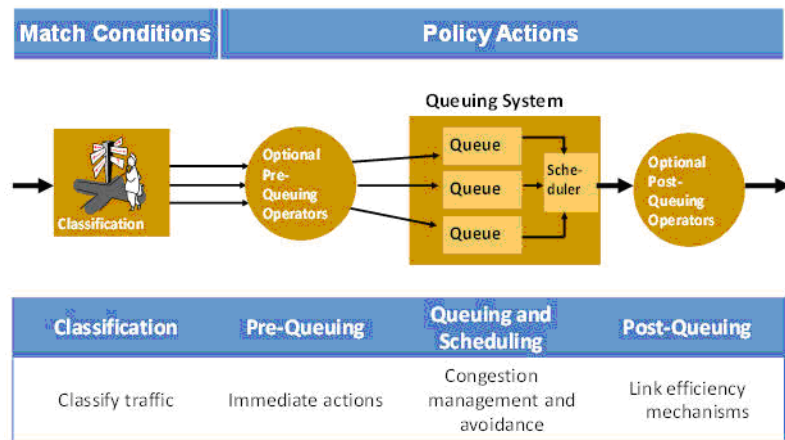
Figure 7-1 Applying QoS Policy at a WAN Congestion Point



7.2 Cisco IOS QoS Model

QoS on IOS routers supports extremely granular management of valuable network and path services. QoS control functions follow the model shown in [Figure 7-2](#).

Figure 7-2 Cisco IOS QoS Model



QoS can be thought of as a collection of classification tools and actions on the classified traffic flows.

7.2.1 Classification

Classification has already been covered in chapter 4 XREF TBD. The basic concept with classification in the context of QoS is to allow for selection of kinds of traffic for the purpose of further actions. As shown in Table 7-1 different kinds of applications ranging from interactive voice and email have radically different needs and requirements from the network. These requirements need to be well understood as well as their relationship with other network attributes. For example in the case of interactive transactional traffic loss of packets can add more delay due to retransmission. A classification system needs to be able to identify these different traffic classes by either explicit application identification or by keying off an agreed upon control point (such as DSCP) that has been previously set.

7.2.2 Prequeuing

After classification has been performed, there is an opportunity to filter specific traffic that has been identified as superfluous or unauthorized on the network. For explicit removal, this could be as simple as an access-list or a bit more complicated such as discarding specific traffic only when exceeding a rate of transmission. In rate based removal, a QoS traffic policer could be configured. Additionally, a Denial of Service (DoS) attack can be constrained by placing drop access-lists towards the source, or if the exact match criteria have not been explicitly discovered or identified, the traffic can be rate-limited.

Table 7-1 Different Applications Have Different Needs

Application Examples	Sensitivity		
	Delay	Jitter	Packet Loss
Interactive voice and video	Y	Y	Y
Streaming video	N	Y	Y
Transactional/interactive	Y	N	Y
Bulk data	N	N	N

Application Examples	Sensitivity		
	Delay	Jitter	Packet Loss
Email	N	N	N
File transfer	N	N	N

7.2.3 Queuing and Scheduling

The queuing and scheduling portion of QoS is often the most powerful with the ability to shape (shaping), prioritize (low-latency queuing), provide a level of session fairness (fair-queuing) among many other features. Given elastic and inelastic traffic types, the queuing and scheduling technologies can create artificial bandwidth limitations (shaping) as well as signal the end host (for example, dropping the packet or Explicit Congestion Notification (ECN)) such that it reduces the rate of transmission.

7.2.4 Postqueuing

As the packet is scheduled to exit the router, there is an opportunity to do a few last actions on it. The other items in the model refrain from modifying the actual packet. They either drop or delay the packet, but do not modify the payload or the frame itself. These last bits of post-queuing functions act on the packet. For example, for RTP packets, header compression can be performed that can reduce a significant percentage of the bandwidth space that the packet was using. Large packets on slow links can cause excessive jitter as sending a large packet takes up a solid chunk of time that prevents other real-time traffic streams from being transmitted.

Post-queuing features such as multilink ppp link fragment interleave (MLPPP-LFI) and IMA (inverse multiplex for ATM) break the large packets into smaller packets, and interleave smaller packets requiring low-latency from other traffic streams in between. In addition, post-queuing allows “bandwidth fairness” to be applied on a per-user or even at the level of per-application-per-user level of traffic management.

7.2.5 Congestion Management and Avoidance

When no congestion exists, packets are sent out the WAN interface as soon as they arrive. However, when packets are arriving at a faster rate than the router can forward them-- congestion occurs. The Congestion Management QoS features can be enabled to address congestion conditions.

Queuing algorithms are used to sort and prioritize traffic overflow before packets are transmitted onto the network. Packets are scheduled for transmission according to their assigned priority and queuing mechanism applied to the WAN interface. There are different types of queuing mechanisms such as First-In-First-Out (FIFO), Priority Queuing (PQ), and Weighted-Fair-Queuing (WFQ). Traffic flows classified as expedite forwarding will be placed in the high priority queue and transmitted first. Traffic flows requiring a certain amount of bandwidth will be sorted and placed on different queues before being transmitted. In times of congestion, some of these queues will overflow and excess traffic will be dropped.

Selective packet drop can be implemented with Weighted Random Early Detection (WRED). By assigning a drop probability to a traffic class, the operator can select which traffic class will drop packets at the time of congestion. In general, a higher drop probability is given to traffic classes considered to be of lower priority. WRED is one of the algorithms used by the Congestion Avoidance feature in IOS.

WRED also supports the Explicit Congestion Notification (ECN) bits of the IP header of packets as defined in RFC3168. The ECN bits indicate whether the endpoints of a traffic flow support the feature. If they do, WRED can mark the packet via ECN and forward the packet instead of dropping. The ECN bits will indicate to the sender that a congestion condition is present and that they should reduce their windows—effectively reducing the data transmission rate. If the endpoints do not support ECN, the packets will be processed by the WRED algorithm and depending on traffic conditions, the packets may be dropped. Traffic optimized by the WAAS TFO feature automatically supports ECN.

7.2.6 Integrated Services and RSVP

In addition to marking packets and generalized queues, that traffic can be scheduled in there is a more strict system for reserving and enforcing bandwidth available in Cisco IOS. Known as IntServ, the RSVP protocol is used to reserve resources in the network for streams of traffic by applications to allow for guaranteed QoS.

RSVP reservations can be especially effective for inelastic traffic types, such as many types of video, or, more generally, UDP based applications, which do not respond to congestion in the network path. In the previous section, ECN was mentioned as a mechanism for relaying to the end host the need reduce the traffic rate. Packet drops and ECN do not apply to inelastic traffic, and an explicit reservation of bandwidth is used to protect the quality of the traffic. If multiple applications try to reserve bandwidth for a specific queue type and the reservation cannot be met, the network denies the reservation, which prevents a subpar application experience and protects existing reservations from degradation.

7.2.7 Modular QoS CLI

The QoS tools described in this chapter can be applied in IOS platforms using Modular QoS CLI (MQC). MQC provides a standard set of CLI commands and QoS semantics that supports a simple, straightforward way to configure QoS features. MQC uses definitions of class-maps, policy-maps, and service policies to apply QoS controls to traffic going through a router. MQC policies share a common language across IOS platforms, and are easily understood and rapidly deployed to ensure consistent behavior across a network.

A class-map defines the criteria for a traffic class. Traffic matching specific criteria is grouped into a traffic class, and is processed according to the traffic policy defined in the policy-map. The traffic policy is attached to an interface so that all traffic going through the interface in a particular direction is subject to the policy.

7.3 References

1. *Enterprise QoS Solution Reference Network Design Guide*:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html
2. **IOS QoS**:
<http://www.cisco.com/go/qos>
3. **Modular QoS CLI (MQC)**:
http://www.cisco.com/en/US/technologies/tk543/tk545/technologies_white_paper09186a0080123415.html

4. DiffServ Scalable End-to-End QoS Model:

http://www.cisco.com/en/US/technologies/tk543/tk766/technologies_white_paper09186a00800a3e2f_ps6610_Products_White_Paper.html

5. QoS RSVP:

<http://www.cisco.com/en/US/docs/internetworking/technology/handbook/RSVP.html>

6. RFC 2508, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*, Stephen L. Casner and Van Jacobson, 1999.**7. RFC 3168, *The Addition of Explicit Congestion Notification (ECN) to IP*, K. Ramakrishnan, S. Floyd, and D. Black, 2001.**