CHAPTER 4

WAN Infrastructure

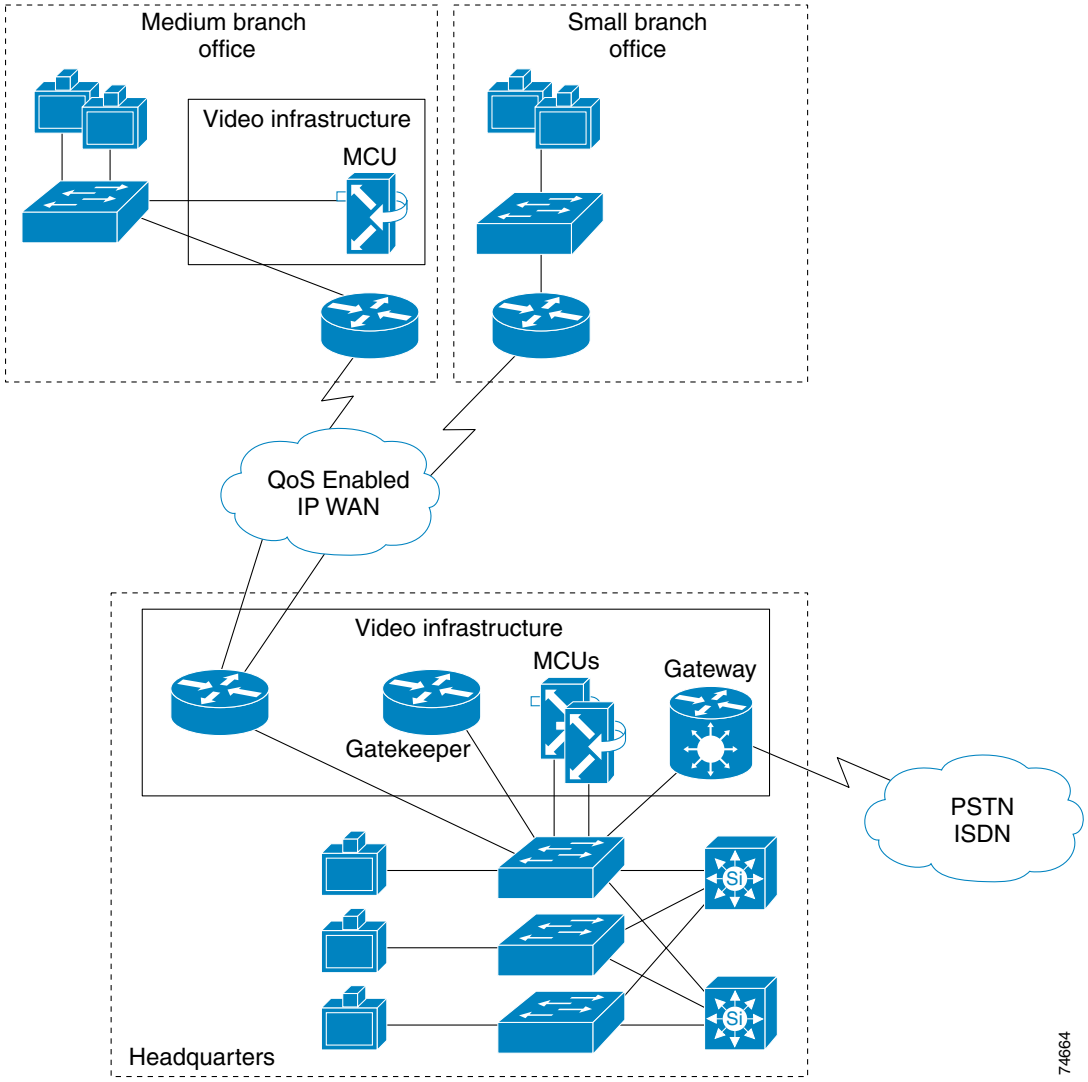
Last revised on: October 30, 2009

This chapter provides guidelines for deploying H.323 video across an IP WAN, and it describes IP WAN infrastructure design considerations for:

Single-Zone WAN

Figure 4-1 illustrates a single-zone WAN network.

Figure 4-1 Single-Zone WAN



A single-zone WAN model consists of the WAN environment and less than three videoconferencing terminals per remote site. (This limit is based on a T1 WAN link.) Cisco recommends that you configure a gatekeeper and a zone for a remote site with one or two video terminals, but this configuration is not strictly required.

Due to the limited number of endpoints and traffic classification options, you can achieve quality of service (QoS) and call admission control by following these basic rules:

- The total data rate of the video terminals plus 20% should not exceed 33% of the WAN link capacity.
- The priority queue must be provisioned for the maximum data rate of the video terminals plus 20%.

  For example, assume a site has a link capacity of 1.544 Mbps and contains two video terminals that support a maximum data rate of 256 kbps each. Therefore, the required queue size for the two video terminals is (256+256)x120% = 614 kbps. Provisioning the priority queue for 614 kbps allows both video terminals to be in a call across the WAN at the same time, without the possibility of overrunning the priority queue. If we add a third video terminal in this example, we would need to add a gatekeeper and create a zone to provide call admission control.

The key elements for successful deployment of videoconferencing in a single-zone WAN environment are:

- Traffic Classification, page 4-3
- Call Admission Control, page 4-4
- Provisioning, page 4-4
- Priority Queuing on the WAN, page 4-4
- Entrance Criteria, page 4-4

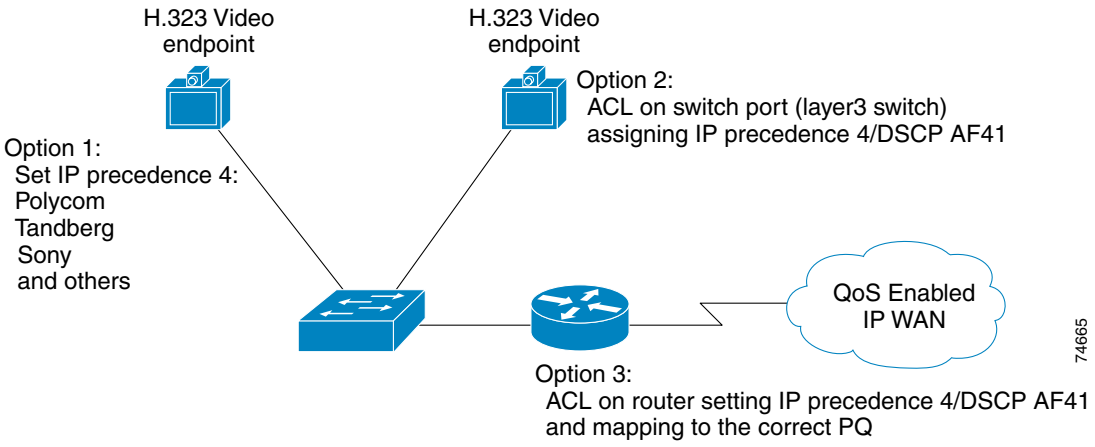
Traffic Classification

Classify traffic at one of the following places:

- Video endpoint (Polycom, Tandberg, Sony, and others); IP Precedence 4 or DSCP AF41
- Switch port (Layer 3 switch required); IP Precedence 4 or DSCP AF41 (recommended)
- Router (ACL entry); IP Precedence 4 or DSCP AF41

Figure 4-2 illustrates these three options for traffic classification.

Figure 4-2 Traffic Classification Options for Single-Zone WAN



Call Admission Control

For remote sites that do not have a gatekeeper to enforce call admission control, provision the priority queue and limit the number of video terminals at each site. The number of video terminals multiplied by the maximum call data rate, must not exceed the capacity of the priority queue. Cisco recommends that you use a gatekeeper and zones for remote sites with more than two video terminals. You can install a gatekeeper at each remote site with more than two video terminals, or you can install one gatekeeper at the central site and define a separate zone for each remote site.

Note This recommendation is based on a T1 WAN link.

Provisioning

Provision WAN queues according to the following equation:

Priority queue size = (Number of users) x (Maximum data rate of video terminals) x 120%

The priority queue must be provisioned to handle the maximum data rate used by any of the video terminals, otherwise the priority queue has the potential to become oversubscribed. Add 20% to the maximum data rate of the video terminals to allow for IP and transport overhead. The priority queue for the link should not exceed 33% of the link capacity. Refer to the WAN QoS chapter for more information.

Priority Queuing on the WAN

Configure multiple queues for the WAN ports on routers. Videoconferencing traffic goes into a priority queue (PQ) that services IP Precedence 4 or DSCP AF41. Class-based weighted fair queuing (CBWFQ) is *not* recommended for interactive video.

Entrance Criteria

In the single-zone WAN model, use access control lists (ACLs) to access configured priority queues at remote sites. ACLs ensure that only traffic from the video terminals has access to the configure PQ. The small number of video terminals at remote sites makes ACL entries a viable option.

Central sites that have either Layer 3 switches or video terminals capable of setting IP Precedence, should set the entrance criteria for the PQ to any packets with IP Precedence 4 or DSCP AF41. This method, however, is not as secure as the ACL option but works properly if the trust boundaries are configured correctly. This method can also be used at remote sites if ACLs are not acceptable.

Multi-Zone WAN

A multi-zone WAN model consists of the WAN environment and three or more videoconferencing terminals per remote site. (This model is based on a T1 WAN link.) Multi-zone WAN deployments are found in large enterprises and state-based distance-learning networks. Remote sites containing three or more video terminals are managed by either a centralized or local gatekeeper. The gatekeeper manages bandwidth within the local zone and across the WAN between zones.

The gatekeeper manages bandwidth only in a hub-and-spoke environment with bandwidth controls. An intermediate gatekeeper is not aware of a call passing through its zone. Only the originating zone gatekeeper and terminating zone gatekeeper are aware of the active call. Resource Reservation Protocol (RSVP) can be used in conjunction with Differentiated Services Code Point (DSCP) to scale larger than hub-and-spoke environments. For this configuration, you need to consider the impact of other applications such as IP telephony that monitor only the number of calls or bandwidth usage for call admission control. See the section on Interworking with Session Initiation Protocol (SIP), page A-1, for more information.

Figure 4-3 illustrates a multi-zone WAN network.

Figure 4-3 Multi-Zone WAN

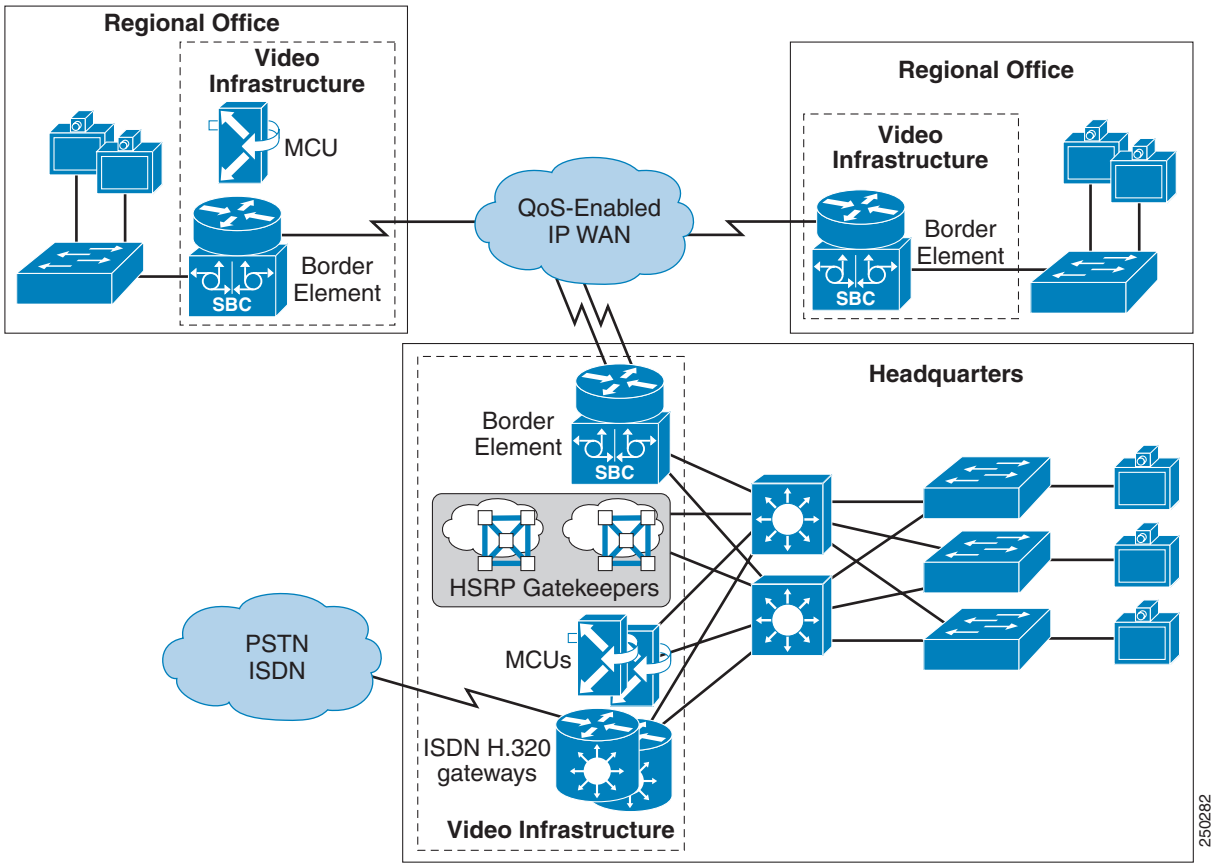


Figure 4-3 shows each remote site running the border element on the WAN router, and dedicated routers with Hot Standby Routing Protocol (HSRP) for the gatekeeper at the central site. You can deploy border elements with the gatekeeper enabled to support a large number of video endpoints and have flexibility of registration and call resolution in the event of a WAN failure.

The deployment guidelines for a multi-zone WAN environment are similar to those for a single-zone WAN. The biggest difference is the ability to control bandwidth in the multi-zone WAN through an added classification point (gatekeeper and zone). The key elements for successful deployment of videoconferencing in a multi-zone WAN environment are:

- Traffic Classification, page 4-6
- Bandwidth Control and Call Admission Control, page 4-6

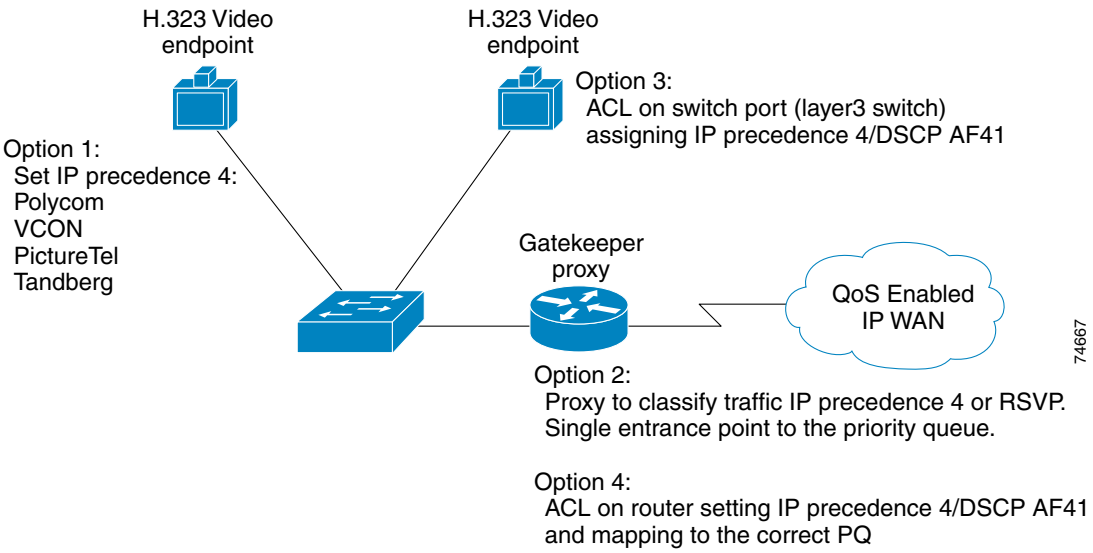
Traffic Classification

Classify traffic at one of the following places:

- Video endpoint (Polycom, Tandberg, Sony, and others); IP Precedence 4 or DSCP AF41
- Border Element classification; IP Precedence 4 or RSVP (recommended for traffic reclassification)
- Switch port (Layer 3 switch required); IP Precedence 4 or DSCP AF41 (recommended classification method for all video endpoints)
- Router (ACL entry); IP Precedence 4 or DSCP AF41 (Due to the larger number of video terminals at each site, this option is not typically used.)

Figure 4-4 illustrates classification options for a multi-zone WAN model.

Figure 4-4 Traffic Classification Options for Multi-Zone WAN



Bandwidth Control and Call Admission Control

Because each remote site in a multi-zone WAN has its own gatekeeper and zone, bandwidth control between zones is possible. By configuring the *remote* bandwidth in each remote gatekeeper, administrators can limit the amount of available bandwidth for calls to and from the WAN. Use the global **bandwidth remote** command at remote sites to control video calls across WAN links. For more information on the gatekeeper and bandwidth control, refer to the chapter on Cisco Video Infrastructure Components.

Provisioning

Provision WAN queues based on the bandwidth limits set in the gatekeeper, and do not provision more than 33% of the link capacity for voice and video applications. Cisco recommends that you provision the Priority Queue (voice and video traffic combined) to use no more than 33% of the link capacity.

Priority Queuing on the WAN

Configure multiple queues for WAN ports on routers. Videoconferencing traffic goes into a PQ that services the devices. If the border element is used, it can mark streams with IP Precedence 4 or DSCP AF41.

Entrance Criteria

Using the border element allows administrators to limit access to the priority queue by configuring an ACL on the WAN router. Only video calls authenticated by the gatekeeper go through the border element if configured appropriately. The ACL allows only packets received from the border element to access the configured priority queue. The ACL prevents unauthorized users from installing a video terminal on their desk, making video calls using IP addresses, and accessing the priority queue. By restricting access to the priority queue, the configured ACL ensures that unauthorized users cannot oversubscribe the priority queue. Rogue users are serviced out of the default queue, thus ensuring video quality for authorized video terminals.

If the border element is not used, the entrance criteria for the priority queue should be any packets with IP Precedence set to 4 or DSCP AF41. ACLs can be used if static addressing is deployed for the video endpoints. It is important to configure trust boundaries properly to prevent unauthorized traffic from accessing the priority queue.