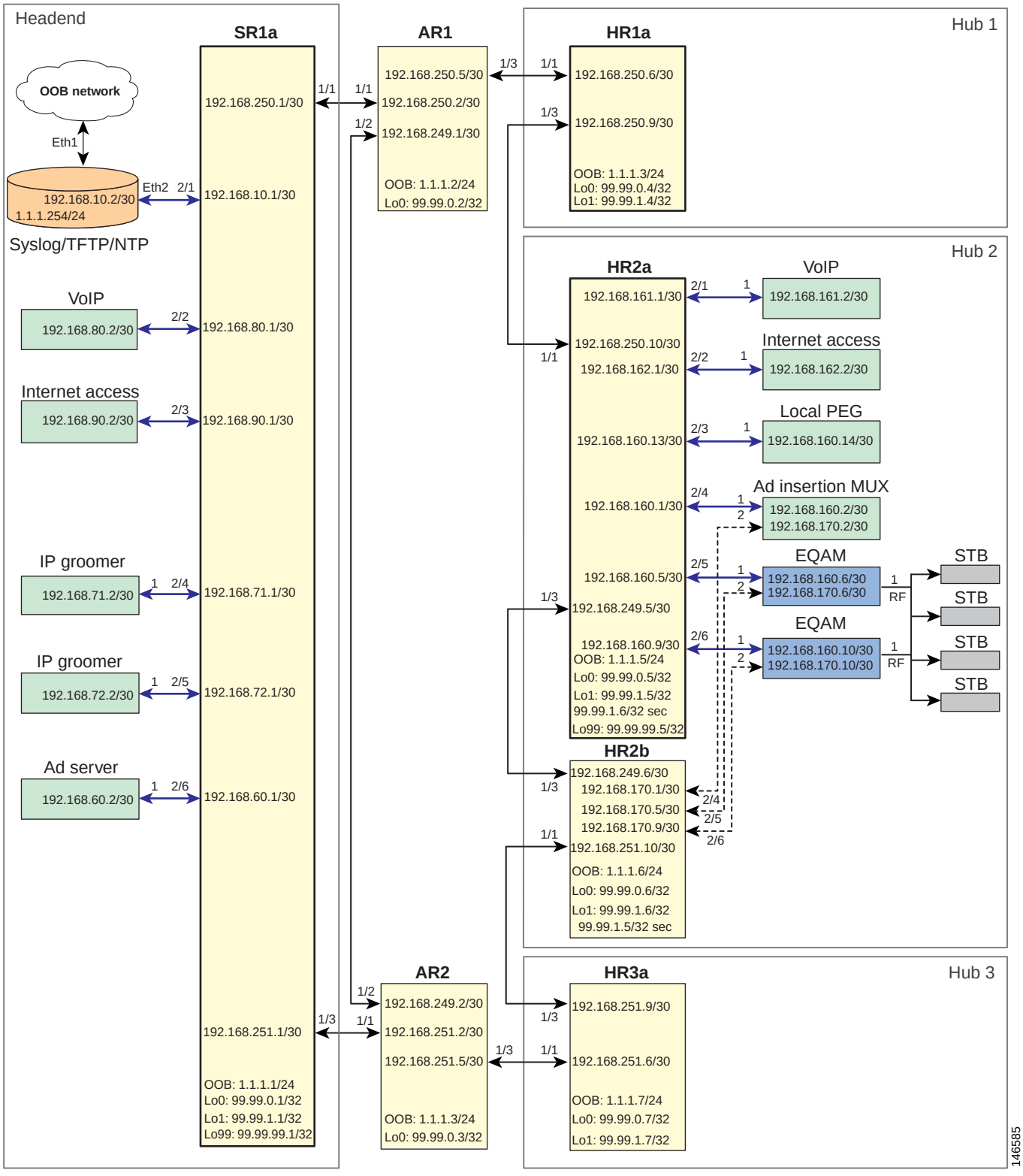
Implementing the Solution

This chapter presents the following major topics:

Network Topology

Figure 3-1 on page 3-2 illustrates the network topology that was tested. (See Hub and IP Architecture, page 2-1.)

Figure 3-1 Network Topology



Basic Configuration: Configuring Global and Interface Attributes

The following tasks are presented:

- Configuring Routing
- Configuring Multicast

Configuring Routing

End-to-end network connectivity is accomplished by using multiple dynamic protocols and processes. OSPF is used to advertise the transport links, interswitch links, and loopbacks, while internal BGP (iBGP) is used to advertise subnets for the edge devices.

Note See IP Architecture, page 2-2.

OSPF is configured into two domains, one for the RAN and one for the hub. The RAN OSPF process enables connectivity and shortest path through the network; the hub OSPF process enables connectivity within the hub. The two domains simplify the routing tables on the RAN and hub routers, because a hub does not have routes for the interhub links of the other hubs. Routing table stability is also improved, because network changes in a hub are not advertised out of the hub.

The iBGP uses route reflectors and route reflector clients to advertise the subnets for the edge devices throughout the network. The SR and HR routers advertise their hub OSPF and directly connected subnets up to the AR routers, which aggregate all the received routes and advertise the aggregate back to the SR and HR routers.

To configure routing, perform the following tasks:

- Configuring the RAN OSPF Process
- Configuring the Hub OSPF Process
- Configuring the iBGP Process

Configuring the RAN OSPF Process

The RAN OSPF routing configurations on SR, AR, and HR routers are similar. To configure HR2a, do the following.

Step 1 Create the OSPF process and configure a router ID.

```
router ospf 100
 router-id 99.99.0.5
```

Step 2 The following default commands are added to the process configuration automatically. The first sends Syslog messages when adjacent neighbors' states change. The second is the maximum number of equal-cost paths that can be used.

```
log-adjacency-changes detail

maximum-paths 6
```

Step 3 Configure which subnets and interfaces will advertise in this process. All loopback interfaces (99.99.*xxx.xxx*) and all 10-GE interswitch links in the RAN (192.168.2*xx.xxx*) are advertised to the neighboring routers.

```
passive-interface default
no passive-interface TenGigabitEthernet1/1
no passive-interface TenGigabitEthernet1/3
network 99.99.0.0 0.0.255.255 area 0
network 192.168.249.0 0.0.0.255 area 0
network 192.168.250.0 0.0.0.255 area 0
```

Step 4 Modify the SPF algorithm to converge more quickly.

```
timers throttle spf 400 400 4000
```

- The first value is the initial SPF schedule delay in milliseconds (1–600000 msec).
- The second value is the minimum hold time between two consecutive SPF calculations (1–600000 msec).
- The last value is the maximum wait time between two consecutive SPF calculations (1–600000 msec).

Step 5 To ensure that routes from this process are not used in routing decisions until the routing process converges, advertise the maximum metric until the iBGP converges or the default timer has expired (600 sec).

```
max-metric router-lsa on-startup wait-for-bgp
```

Configuring the Hub OSPF Process

In the testing of this solution, no devices in the hubs other than the HR routers participated in OSPF, so the configurations do not contain a configuration for this process. However, it is described here for completeness.

Step 1 The hub OSPF process includes Steps 1 through Step 5 of the RAN OSPF process (see Configuring the RAN OSPF Process, page 3-3), where the interfaces from Step 3 would include the point-to-point between the hub routers, subnets for the CMTSes, QAMs with routing capabilities, and so on. instead of the RAN interfaces. These networks would be configured in a second OSPF area (area 1), and any routes learned from this process would have a high metric, because it would not be the preferred route.

Configure the hub OSPF process, noting the variables in `<angle brackets>`.

```
router ospf 200
 router-id 99.99.1.5
 log-adjacency-changes
 maximum-paths 6
 passive-interface default
 no passive-interface GigabitEthernet2/48
 network <hub point-to-point link> 0.0.0.3 area 1
 network <IP address of attached routing device> <wildcard mask> area 1
 timers throttle spf 400 400 4000
 max-metric router-lsa on-startup wait-for-bgp
 distance ospf external 175
```

Step 2 In global configuration mode, define a prefix list and route map to set the metric and next hop of the routes redistributed from the hub OSPF process into iBGP.

a. Define a prefix list.

```
ip prefix-list hub-ospf-to-bgp-pfx seq 100 permit <hub point-to-point link>/30 le 32
ip prefix-list hub-ospf-to-bgp-pfx seq 200 permit <IP address of attached routing
  device>/<subnet mask> le <bitmask>
```

b. Define a route map.

```
route-map hub-ospf-to-bgp permit 100
 match ip address prefix-list hub-ospf-to-bgp-pfx
 set metric 100
 set ip next-hop <hub loopback1 primary address>
```

Note The above enables hub connectivity. However, the routes from the hub OSPF process must be redistributed into BGP to ensure the network connectivity of devices using routes defined in Step 2b, above. See Step 8 of Configuring the iBGP Process, page 3-5.

Configuring the iBGP Process

The iBGP routing configuration on the SR and HR routers is similar. To configure HR2a, do the following.

Step 1 Create the BGP process and configure a router ID.

```
router bgp 100
 bgp router-id 99.99.0.5
```

Step 2 The following default commands are added to the process configuration automatically. The first allows the router to advertise a network route without waiting for OSPF. The second disables auto summary, so subnet prefixes are not summarized when they are advertised.

```
no synchronization

no auto-summary
```

Step 3 Enable the logging of BGP neighbor changes.

```
bgp log-neighbor-changes
```

Step 4 Configure the router to display BGP communities in the AA:NN format to conform with RFC 1997. This command only affects the format in which BGP communities are displayed; it does not affect the community or community exchange.

```
ip bgp-community new-format
```

Note For more information, see “RFC 1997—BGP Communities Attributes,” at the following URL:

http://www.faqs.org/rfcs/rfc1997.html

Step 5 Define a peer group (here arbitrarily named “rr-server”) for the route reflectors AR1 and AR2. Neighbors configured for this group share all of the following information.

```
neighbor rr-server peer-group
neighbor rr-server remote-as 100
neighbor rr-server update-source Loopback0
neighbor rr-server version 4
neighbor rr-server send-community
```

Step 6 Define AR1 and AR2 as neighbors and associate them with the peer group defined in Step 5.

```
neighbor 99.99.0.2 peer-group rr-server
neighbor 99.99.0.2 description AR1

neighbor 99.99.0.3 peer-group rr-server
neighbor 99.99.0.3 description AR2
```

Step 7 Configure the BGP process to redistribute the directly connected subnets according to a defined route map. (The route map is defined in Step 9b, below.)

```
redistribute connected route-map rmap_Connected-to-BGP
```

Step 8 Configure the BGP process to redistribute the hub OSPF process defined in Step 1 of Configuring the Hub OSPF Process, page 3-4.

```
redistribute ospf 200 route-map hub-ospf-to-bgp
```

Step 9 Define a prefix list and route map to set the metric and next hop of the directly connected subnets redistributed into iBGP.

a. Define the prefix list.

```
ip prefix-list pl_Connected-to-BGP seq 5 permit 192.168.160.0/24 le 32
```

b. Define the route map.

```
route-map rmap_Connected-to-BGP permit 100
 match ip address prefix-list pl_Connected-to-BGP
 set metric 100
 set ip next-hop 99.99.0.5
```

The BGP configuration on the AR routers is similar. To configure AR1, do the following.

Step 1 Create the BGP process and configure a router ID.

```
router bgp 100
 bgp router-id 99.99.0.2
```

Step 2 The following default commands are added to the process configuration automatically:

- The first allows the router to advertise a network route without waiting for OSPF.
- The second disables auto summary, so subnet prefixes are not summarized when they are advertised.

```
no synchronization
no auto-summary
```

Step 3 Enable the logging of BGP neighbor changes.

```
bgp log-neighbor-changes
```

Step 4 Configure the router to display BGP communities in the AA:NN format to conform with RFC-1997. This command only affects the format in which BGP communities are displayed; it does not affect the community or community exchange.

```
ip bgp-community new-format
```

Step 5 Define a peer group for the route reflector clients SR1a and the HRs. Neighbors configured for this group share all of the following information.

```
neighbor rr-client peer-group
neighbor rr-client remote-as 100
```

```
neighbor rr-client update-source Loopback0
neighbor rr-client version 4
neighbor rr-client route-reflector-client
neighbor rr-client send-community
```

Step 6 Define SR1a and the HRs as neighbors and associate them with the peer group defined in Step 5, above.

```
neighbor 99.99.0.1 peer-group rr-client
neighbor 99.99.0.1 description SR1a
neighbor 99.99.0.4 peer-group rr-client
neighbor 99.99.0.4 description HR1a
neighbor 99.99.0.5 peer-group rr-client
neighbor 99.99.0.5 description HR2a
neighbor 99.99.0.6 peer-group rr-client
neighbor 99.99.0.6 description HR2b
neighbor 99.99.0.7 peer-group rr-client
neighbor 99.99.0.7 description HR3a
```

Step 7 Define a peer group (here arbitrarily called “ibgp”) for the two route reflectors AR1 and AR2. Neighbors configured for this group share all of the following information.

```
neighbor ibgp peer-group
neighbor ibgp remote-as 100
neighbor ibgp update-source Loopback0
neighbor ibgp version 4
neighbor ibgp send-community
```

Step 8 Define AR1 as a neighbor and associate it with the peer group defined in Step 7, above.

```
neighbor 99.99.0.3 peer-group ibgp
neighbor 99.99.0.3 description AR2
```

Step 9 Define the networks to be advertised.

```
network 192.168.10.0 route-map rmap_Network-Management
network 192.168.60.0 route-map rmap_Ad-Insertion
network 192.168.71.0 route-map rmap_IPmc-DS-Source
network 192.168.72.0 route-map rmap_IPmc-DB-Source
network 192.168.80.0 route-map rmap_Voice
network 192.168.90.0 route-map rmap_Internet-Access
network 192.168.150.0 route-map rmap_Hub1
network 192.168.160.0 route-map rmap_Hub2
network 192.168.170.0 route-map rmap_Hub2
network 192.168.180.0 route-map rmap_Hub3
```

Step 10 Use route maps to set the metric for each route.

```
route-map rmap_Network-Management permit 100
  set metric 100

 route-map rmap_Ad-Insertion permit 100
  set metric 100

 route-map rmap_IPmc-DS-Source permit 100
  set metric 100

 route-map rmap_IPmc-DB-Source permit 100
  set metric 100

 route-map rmap_Voice permit 100
  set metric 100

 route-map rmap_Internet-Access permit 100
  set metric 100
```

```
route-map rmap_Hub1 permit 100
 set metric 100

route-map rmap_Hub2 permit 100
 set metric 100

route-map rmap_Hub3 permit 100
 set metric 100
```

Configuring Multicast

Video equipment currently supports IGMPv2 and is starting to support IGMPv3. Cisco has a transitional solution to help customers implement SSM with IGMPv2 instead of waiting for multicast clients to support IGMPv3. IGMPv2 Membership Reports are converted to IGMPv3 on the Cisco router, which uses static mappings or a DNS server to resolve the source address of the multicast group. The static mappings and DNS server implementations both have pros and cons, which the user needs to weigh before implementing either approach.

Note For an overview of how multicast is used in the solution, see Understanding and Optimizing Video Flows, page 2-4.

In this solution, static SSM mappings are used. This requires the user to map all multicast groups to the appropriate source addresses for SSM multicast to operate properly. The following SSM configuration is implemented on all switches in the network.

Note If the network is currently on an ASM model and the MSO wants to mic\grate to an SSM model, see Upgrading the Network: Migrating from ASM to SSM, page 2-38.

The following tasks are presented below:

- Configuring SSM
- Configuring IGMP

Configuring SSM

To configure SSM, do the following.

Step 1 Enable multicast routing.

```
ip multicast routing
```

Step 2 Enable SSM mapping.

```
ip igmp ssm-map enable
```

Note Although the document “Source Specific Multicast (SSM) Mapping,” referenced above, states that the **ip igmp ssm-map enable** command needs to be configured only on switches that are connected to IGMP clients, it was found that this led to inconsistent recovery times during solution network failure and recovery tests. A majority of the time, recovery was fast, but occasionally recovery times were poor. It

was found that when this command was configured on the headend switch, recovery times were more consistent, although slightly slower than the best recovery times when SSM mapping was not configured on the headend switch.

Step 3 By default, DNS queries are used to resolve the source address of IGMPv2 Membership Reports. Because the solution uses static SSM mapping, disable the DNS method of resolution buy using the following command.

```
no ip igmp ssm-map query dns
```

Step 4 Define a nondefault multicast IP address range for SSM. (By default, the IP address range for SSM is 232.0.0.0/8, but it can be defined manually.) In this solution, the 239.0.0.0/8 range is used for SSM.

a. Create an access list with a permit statement that defines the range.

```
ip access-list standard acl_SSM-IPmc-range
 permit 239.0.0.0 0.255.255.255
```

b. Define the SSM range of IP multicast [Protocol Independent Multicast (PIM)] addresses.

```
ip pim ssm range acl_SSM-IPmc-range
```

Tip To use the default SSM range, omit Step 4a and Step 4b above, and use the **ip pim ssm default** command.

Step 5 Define the static SSM mappings for the multicast groups in the network. To accomplish this, define access lists for each range of multicast groups and associate them with a source IP address.

```
ip access-list standard acl_SSM-map-DB
 remark SSM mapping for DB blue/red
 permit 239.16.0.0 0.0.0.255

ip access-list standard acl_SSM-map-DS
 remark SSM mapping for DS blue/red
 permit 239.20.0.0 0.0.255.255

ip access-list standard acl_SSM-map-DS-post-splice
 remark SSM mapping for post splice DS blue/red
 permit 239.28.0.0 0.0.255.255

ip igmp ssm-map static acl_SSM-map-DB 192.168.71.2
ip igmp ssm-map static acl_SSM-map-DS 192.168.72.2
ip igmp ssm-map static acl_SSM-map-DS-post-splice 192.168.160.2
```

Step 6 Verify the SSM configuration, using the following commands.

```
HR2a# show ip igmp ssm-mapping

SSM Mapping  : Enabled
DNS Lookup   : Disabled
Mcast domain : in-addr.arpa
Name servers : 255.255.255.255
```

```
HR2a# show ip igmp ssm-mapping 239.16.0.1

Group address: 239.16.0.1
Database     : Static
Source list  : 192.168.71.2
```

Note For the details and an extended discussion of SSM mapping, see "Source Specific Multicast (SSM) Mapping" at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtssmma.htm

Configuring IGMP

The configuration of IGMP depends on the version of IGMP that is configured for the attached IGMP clients. The two options are discussed below.

- All Clients Support IGMPv2 Only
- All Clients Support and Are Configured for IGMPv3

Note See Upgrading the Network: Migrating from ASM to SSM, page 2-38.

All Clients Support IGMPv2 Only

If *any* clients support *only* IGMPv2, then you should configure the router interfaces connected to the IGMP client for IGMPv2, which is the default. (To restore the default, use the **ip igmp version 2** command in global configuration mode.)

If the router receives an IGMPv2 Membership Report (MR) for a multicast group in the SSM range, the MR is accepted and converted to IGMPv3 if SSM static or DNS mapping is configured on the router. Otherwise, the IGMPv2 MR is ignored. If the router receives an IGMPv2 MR for a multicast group outside of the SSM range, then the MR is accepted and processed as Any Source Multicast (ASM). Consequently, if the router receives an IGMPv3 MR, the MR is ignored. The router later sends an IGMPv2 Membership Query, and the client should see this lower version and start using IGMPv2 MRs. The router then behaves as previously described.

All Clients Support and Are Configured for IGMPv3

If *all* of the clients support and are configured for IGMPv3, then you should configure the router interface for IGMPv3. To enable this, use the **ip igmp version 3** command in global configuration mode.

In this case, if the router receives an IGMPv2 MR, the router ignores the MR. If the router receives an IGMPv3 MR for a multicast group in the SSM range, the MR is accepted and processed as IGMPv3. If the router receives an IGMPv3 MR for a multicast group outside the SSM range, the MR is accepted and processed as ASM.

Configuring Quality of Service

In this solution, Quality of Service (QoS) is based on Differentiated Services (DiffServ). (See QoS Fundamentals, page 2-35.) Traffic is marked at the ingress ports of the network, and each router in the network independently provides varying levels of quality by means of queueing and scheduling.

The traffic types in Table 2-5 on page 2-36 have different QoS requirements. For example, VoIP traffic requires minimum loss and minimum jitter; video traffic requires no loss and low jitter; and, at the lower end, suspect traffic can suffer loss and high jitter.

The following tasks are presented below:

- Configuring Marking and Classification
- Configuring DSCP-to-CoS Mapping
- Configuring CoS-to-Queue Mapping

Configuring Marking and Classification

The first step in providing quality of service is to classify and mark traffic according to Table 2-5 on page 2-36. Traffic is classified and marked at the edges, and the transports trust the DSCP value on incoming packets. To configure marking and classification, do the following.

Step 1 Enable QoS in global configuration mode.

```
mls qos
```

Step 2 Create an access list to identify each type of service in the network.

Caution The following examples are for illustration only. To avoid undesired access, use the most restrictive addresses and wildcard masks possible.

```
ip access-list extended acl_voice
 remark Identify voice traffic
 permit ip any 192.168.161.0 0.0.0.255

ip access-list extended acl_broadcast-video
 remark Identify broadcast video traffic (multicast on 239.x.x.x)
 permit ip any 239.0.0.0 0.255.255.255

ip access-list extended acl_ad-server
 remark Identify ad server traffic
 permit ip 192.168.60.0 0.0.0.255 any

ip access-list extended acl_video-signaling
 remark Identify video signaling
 permit ip any 192.168.61.0 0.0.0.255

ip access-list extended acl_net-mgmt
 remark Identify net management traffic (TFTP, Syslog, NTP, etc)
 permit ip 192.168.10.0 0.0.0.255 any
 permit ip any 192.168.10.0 0.0.0.255

ip access-list extended acl_internet-access
 remark Identify Internet access traffic
 permit ip 192.168.90.0 0.0.0.255 any
```

```
ip access-list extended acl_permit-any
 permit ip any any
```

Step 3 Create a class map for each of the access lists created in Step 2, above.

```
class-map match-all class_voice
  match access-group name acl_voice

class-map match-all class_broadcast-video
  match access-group name acl_broadcast-video

class-map match-all class_ad-server
  match access-group name acl_ad-server

class-map match-all class_video-signaling
  match access-group name acl_video-signaling

class-map match-all class_net-mgmt
  match access-group name acl_net-mgmt

class-map match-all class_internet-access
  match access-group name acl_internet-access

class-map match-all class_suspect
  match access-group name acl_permit-any
```

Step 4 Create a policy map for each type of ingress port in the network. Each policy map should have classes for each service type expected on the port, and should end with a suspect class. The DSCP values of each server are set to the values shown in Table 2-5 on page 2-36.

```
policy-map pmap_voice-port
  class class_voice
   trust dscp
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default

policy-map pmap_broadcast-video-port
  class class_broadcast-video
   set dscp af41
  class class_video-signaling
   set dscp cs3
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default

policy-map pmap_ad-server-port
  class class_ad-server
   set dscp af41
  class class_video-signaling
   set dscp cs3
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default

policy-map pmap_net-mgmt-port
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
```

```
policy-map pmap_internet-access-port
  class class_internet-access
   set dscp 8
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
```

Step 5 Apply the policy maps to the ingress ports. The following interface configurations are from SR1a.

```
interface GigabitEthernet2/1
 description Syslog/TFTP/NTP on PC0a (Eth2) dual-homed to 1.1.1.0/24
 ip address 192.168.10.1 255.255.255.252
 <---snip--->
 service-policy input pmap_net-mgmt-port

interface GigabitEthernet2/2
 description Voice over IP
 ip address 192.168.80.1 255.255.255.252
<---snip--->
 service-policy input pmap_voice-port

interface GigabitEthernet2/3
 description Internet Access
 ip address 192.168.90.1 255.255.255.252
<---snip--->
 service-policy input pmap_internet-access-port

interface GigabitEthernet2/4
 description CherryPicker DM0a (Port 1) - DB
 ip address 192.168.71.1 255.255.255.252
<---snip--->
 service-policy input pmap_broadcast-video-port

interface GigabitEthernet2/5
 description CherryPicker DM0b (Port 1) - DS
 ip address 192.168.72.1 255.255.255.252
<---snip--->
 service-policy input pmap_broadcast-video-port

interface GigabitEthernet2/6
 description Ad Server Ad0a
 ip address 192.168.60.1 255.255.255.252
<---snip--->
 service-policy input pmap_ad-server-port
```

Step 6 Configure the noningress ports to trust the DSCP value set at the ingress ports. The following configuration is from the 10-GE transport link on SR1a.

```
interface TenGigabitEthernet1/1
 description Transport between AR1 (TenGig1/1)
 ip address 192.168.250.1 255.255.255.252
<---snip--->
mls qos trust dscp
```

Configuring DSCP-to-CoS Mapping

The DSCP values are used to carry the QoS value between the switches. Once the packet is in the switch, the Class of Service (CoS) value is used to queue the packet in the transmit queues. There are 64 possible DSCP values and only 8 CoS values, so multiple services need to be mapped to a single CoS value.

To configure DSCP-to-CoS mapping, do the following:

Step 1 View the default DSCP-to-CoS mapping by using the following command.

```
SR1a# show mls qos maps dscp-cos

   Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 03 03
      3 :    03 03 04 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
```

Step 2 Configure the DSCP-to-CoS mappings by using the following commands.

```
mls qos map dscp-cos 34 36 38 to 6
mls qos map dscp-cos 46 48 to 5
mls qos map dscp-cos 26 28 30 to 4
mls qos map dscp-cos 16 18 20 to 3
mls qos map dscp-cos 40 42 44 to 2
mls qos map dscp-cos 8 10 to 1
mls qos map dscp-cos 0 2 to 0
```

Note Several of the mappings are the same as the default mappings, so they will not show up in the running configuration once the above is configured, as shown below.

```
SR1a# show running-config | include mls qos map
mls qos map dscp-cos 16 18 20 to 3
mls qos map dscp-cos 26 28 30 to 4
mls qos map dscp-cos 34 36 38 to 6
mls qos map dscp-cos 40 42 44 to 2
mls qos map dscp-cos 48 to 5
```

Step 3 View the modified DSCP-to-CoS mapping by using the following command.

```
SR1a# show mls qos maps dscp-cos

   Dscp-cos map:                                     (dscp= d1d2)
     d1 : d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 03 02 03 02
      2 :    03 02 02 02 03 03 04 03 04 03
      3 :    04 03 04 04 06 04 06 04 06 04
      4 :    02 05 02 05 02 05 05 05 05 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
```

Configuring CoS-to-Queue Mapping

The Sup720 PFC performs the QoS classification and marking, but the line cards perform the queueing and congestion management. The following table shows the QoS characteristics of the line cards used in this solution. The 10-GE line cards are used in the transport and are most susceptible to congestion. The 1-GE line cards are used at the edges and are usually configured for a specific role, so the amount of traffic being transmitted out the switch interface should be provisioned appropriately. (Ingress queues are rarely congested and were not examined during testing.)

Table 3-1 lists the characteristics of the line cards used in solution testing.

Table 3-1 Line Card Characteristics

Line Card	Description	Buffer size			Port type		Queue size	
		Total	Rx	Tx	Rx	Tx	Rx	Tx
WS-X6704-10GE	4-port 10-GE dual-fabric with XENPAK receivers	16 MB	2 MB	14 MB	8q8t (w/ DFC3)	1p7q8t	Q8: 400 KB	—
							Q7: 0 KB	Q7: 0 KB
							Q6: 0 KB	Q6: 0 KB
							Q5: 0 KB	Q5: 0 KB
							Q4: 0 KB	Q4: 0 KB
							Q3: 0 KB	Q3: 2.2 MB
							Q2: 0 KB	Q2: 2.9 MB
							Q1: 1.6 MB	Q1: 7.2 MB
							SP: 2.2 MB	—
WS-X6748-GE-TX	48-port 10/100/1000T dual-fabric with RJ-45 connectors	1.3 MB	166 KB	1.2 MB	2q8t (w/ DFC3)	1p368t	—	Q3: 175 KB
							Q2: 33 KB	Q2: 233 KB
							Q1: 133 KB (w/ DFC3)	Q1: 583 KB
							—	SP: 175 KB
WS-X6724-SFP	24-port 1000BASE-X single-fabric with SFP	1.3 MB	166 KB	1.2 MB	2q8t (w/ DFC3)	1p368t	—	Q3: 175 KB
							Q2: 33 KB	Q2: 233 KB
							Q1: 133 KB (w/ DFC3)	Q1: 583 KB
							—	SP: 175 KB

To configure CoS-to-Queue mapping, do the following.

Step 1 Verify the default CoS-to-queue mapping, by using the following command.

```
SR1a# show queueing interface TenGigabitEthernet 1/1
```

Note To save space, the following output shows only the differences resulting from the mapping.

```
queue thresh cos-map
---------------------------------------
1     1      0
1     2      1
<---snip--->
2     1      2
2     2      3 4
<---snip--->
3     1      6 7
<---snip--->
8     1      5
<---snip--->
```

Step 2 Modify the CoS-to-queue mapping by using the following commands.

```
wrr-queue cos-map 1 3 2
wrr-queue cos-map 2 1 3
wrr-queue cos-map 2 2 4
```

This maps COS 2 to TxQueue1, threshold 2; COS 3 to TxQueue2, threshold 1; and COS 4 to TxQueue2, threshold 2.

Step 3 Verify the modified CoS-to-queue mapping by using the following command.

```
SR1a# show queueing interface TenGigabitEthernet 1/1
```

Note To save space, the following output shows only the differences resulting from the mapping.

```
queue thresh cos-map
---------------------
1     1      0
1     2      1
1     3      2
<---snip--->
2     1      3
2     2      4
<---snip--->
3     1      6 7
<---snip--->
8     1      5
<---snip--->
```

Note Although the CoS-to-queue and threshold mappings are modified, the transmit queue lengths, thresholds, and queue management are left at default values. The decision to use default values is based on the expected traffic profile, and may differ from network to network.

Figure 2-7 on page 2-37 shows transmit queues graphically. Table 3-2 on page 3-17 summarizes the results of the preceding mapping task on the traffic tested, as depicted in that figure. (The names of some traffic types vary.)

Table 3-2 Traffic Types Tested and Graphical Representation in Figure 2-7

Traffic Type Tested	Graphical Representation in Figure 2-7
Suspect	Suspect
Internet Access	HSD
Gaming	Gaming
SIP bearer	SIP bearer
Network management	Network management
VoIP control	VoIP control
DTV control	DTV control
Broadcast video	Broadcast video
VoIP bearer	VoIP bearer
IP routing	IGP & EGP

Configuring Network Enhancements

This section presents the following major topics:

- Configuring New Features
- Configuring Hardware Rate Limiters

Configuring New Features

Three new features that enhance the solution are available with Cisco IOS Release 12.2(18)SXF and later:

- EtherChannel Min-Links Feature
- Multicast Replication Mode Feature
- Local Egress Replication Feature

The following sections provide a brief summary, with links to more information and command syntax.

EtherChannel Min-Links Feature

This feature on Link Aggregation Control Protocol (LACP) EtherChannels allows you to do the following:

- Configure the minimum number of member ports that must be in the link-up state and bundled in the EtherChannel for the port channel interface to transition to the link-up state.
- Prevent low-bandwidth LACP EtherChannels from becoming active.
- Cause LACP EtherChannels to become inactive if they have too few active member ports to supply your required minimum bandwidth.

Note For more information, as well as command syntax and examples, see Configuring the EtherChannel Min-Links Feature at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/channel.htm#wp1047602

Multicast Replication Mode Feature

This feature (called "Multicast Enhancement - Replication Mode Detection" in the release notes and Feature Navigator) supports the **egress** keyword, to provide the functionality described below.

By default, a Supervisor Engine 720 automatically detects the replication mode based on the module types installed in the system. If all modules are capable of egress replication, the system uses egress-replication mode. If the supervisor engine detects modules that are not capable of egress replication, the replication mode automatically changes to ingress replication. You can override this action by entering the **mls ip multicast replication-mode egress** command, so that the system continues to work in egress-replication mode even if there are fabric-enabled modules installed that do not support egress replication (for example, OSMs). You can also configure the system to operate only in ingress-replication mode.

Note For more information, as well as command syntax and examples, see Configuring the Replication Mode at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/mcastv4.htm#wp1076728

Local Egress Replication Feature

This feature (called "Multicast Enhancement—Egress Replication Performance Improvement" in the release notes and Feature Navigator) allows you to enable local egress replication unconditionally. You can prevent the redundant replication of multicast packets across the switch-fabric connection by entering a command that instructs the two replication engines on these modules to forward packets only to local interfaces; these interfaces are associated with the switch-fabric connection that the replication engine supports.

Note For more information, as well as command syntax and examples, see Enabling Local Egress Replication at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/mcastv4.htm#wp1093310

Configuring Hardware Rate Limiters

For background and examples, see Hardware Rate Limiters, page 2-13, and the configurations in Appendix A, "Sample Configurations."

For troubleshooting information, see Viewing HWRL Counters, page 4-6.

Configuring Non-Solution-Specific Features

The previous implementation sections included configuration recommendations for features that are specific to the video solution, but did not address other important features that are non-solution specific. Use the following resources to configure features not addressed in this document.

- *Catalyst 6500 Series Cisco IOS Command Reference, 12.2SX*

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/index.htm

- *Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.2SX*

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/index.htm

- Best Practices for Catalyst 6500/6000 Series and Catalyst 4500/4000 Series Switches Running Cisco IOS Software

  http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products_white_paper09186a00801b49a4.shtml

- IOS Command Lookup Tool

  http://www.cisco.com/cgi-bin/Support/Cmdlookup/home.pl