Implementing and Configuring the Solution

This chapter begins with tasks common to the 10-GE symmetric and 1-GE asymmetric topologies used in the Cisco GOVoBB solution:

- Common Tasks: Configuring SSM Mapping with DNS Lookup, page 4-1

It then presents the details of configuring each topology:

- Configuring the 10-GE Symmetric Topology, page 4-4
- Configuring the 1-GE Asymmetric Topology, page 4-53

Note For command references and best practices for the switches used, see the following:

— Cisco Catalyst 6500 Series Switches:

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

— Cisco 7600 Series Router:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/index.htm

—Cisco Catalyst 4500 Series Switches:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/

Common Tasks: Configuring SSM Mapping with DNS Lookup

As discussed in Multicast, page 3-16, Source Specific Multicast (SSM) is used simplify the configuration of a multicast network, and is common to both topologies. The solution uses edge devices that do not support IGMPv3. The switches accept IGMPv2 messages and convert these to IGMPv3 by resolving the source IP address of the multicast group by means of either a static mapping or a DNS resource record. This solution uses a DNS lookup method.

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

The following tasks are presented:

- Configuring DNS Servers
- Configuring SSM Mapping on All Switches
- Configuring the Edge Switches for DNS Queries

Configuring DNS Servers

The following steps are general. Refer to your DNS server documentation for details.

Step 1 For background, refer to “DNS-Based SSM Mapping” in “Source Specific Multicast (SSM) Mapping,” referenced above.

Step 2 Configure the following parameters, as appropriate:

a. Resource records for the first multicast IP address associated with a source

b. All other multicast IP addresses from the same source

c. The multicast domain

d. The timeout (optional)

)

Configuring SSM Mapping on All Switches

Configure the following on all switches (the DER and the ARs) in both topologies.

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 configuring this command 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 Enable SSM on the edge switches. The default IP address range for SSM is 232.0.0.0 to 232.255.255.255.

Note The above command also enables the **ip igmp ssm-map query dns** command. By default, IGMPv2 is configured on the Layer 3 interfaces, so no commands are required to enable SSM mapping with DNS query on the interfaces connected to the device that receives multicast. Also, no special commands are required to enable SSM mapping with DNS query on the Cisco 7609 interfaces that connect to the DNS servers.

Configuring the Edge Switches for DNS Queries

On the edge switches that perform the DNS queries, you must configure the domain and IP addresses of the domain name servers. The domain for the multicast video in the following example is coronado.net. (Domain names will vary.) The switches send queries to the first DNS listed in the running configuration. If the first query fails, the next query is sent to the second DNS.

Step 1 Configure the domain for multicast video.

```
ip domain multicast coronado.net
```

Step 2 Configure the IP address of the first DNS.

```
ip name-server 192.168.10.101
```

Step 3 Configure the IP address of the second DNS.

```
ip name-server 192.168.11.101
```

Configuring the 10-GE Symmetric Topology

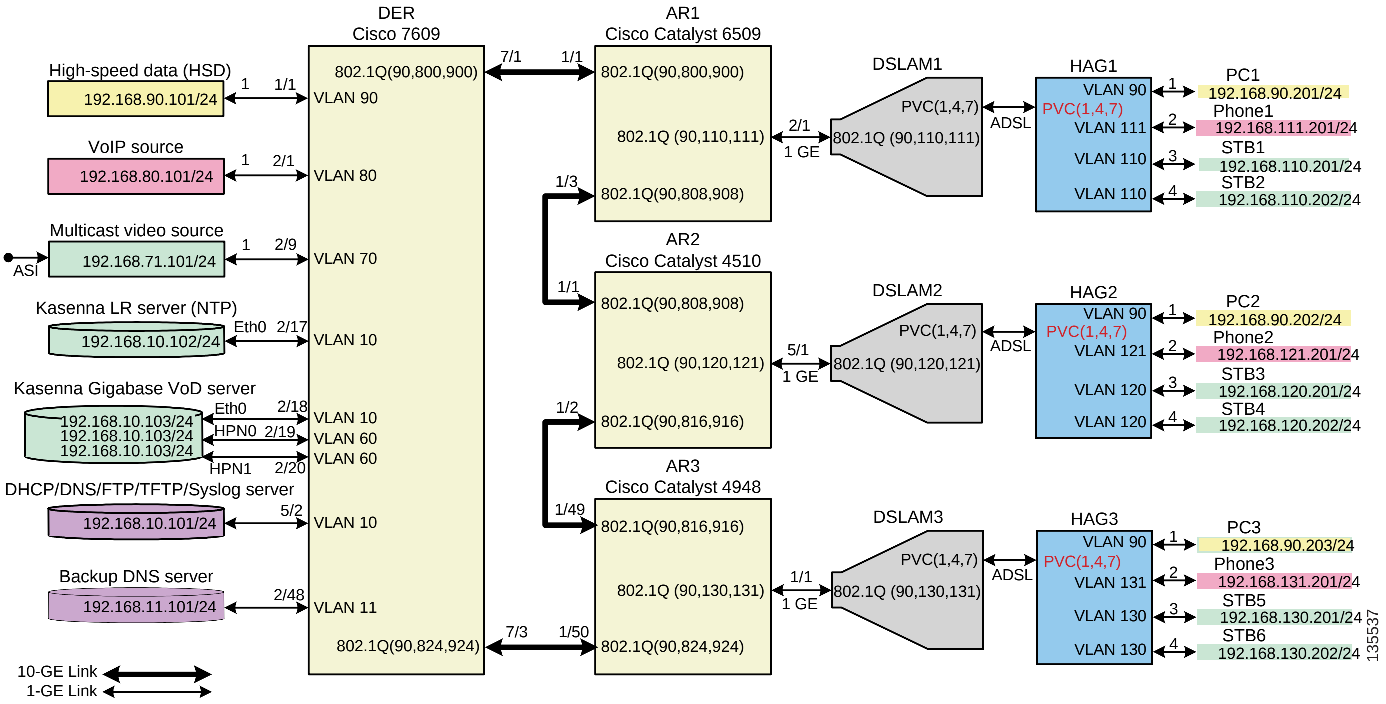
This section presents the following major topics:

- Introduction, page 4-4
- Configuring DER, page 4-7
- Configuring AR1, page 4-21
- Configuring AR2, page 4-31
- Configuring AR3, page 4-42

Introduction

Figure 4-1 illustrates the 10-GE symmetric topology used in the solution. (See Configuration 1: 10-GE Layer 3 Symmetric Ring, page 3-33.) All video traffic sources are on DER. Policy maps are applied to the ingress ports on DER in order to mark the DSCP values of the different service types. Traffic is routed through 10-GE bidirectional links, configured as IEEE 802.1q trunks that carry three VLANs: one for video, one for VoIP, and one for high-speed data (HSD). Two OSPF processes are used for the routing protocol. The first advertises routes for the video-related interfaces, and second advertises routes for the VoIP-related interfaces. HSD is carried around the ring on Layer 2. The HAG used in the test bed used service separation based on physical ports, as described in Traffic Separation Based on Physical Ports, page 3-43.

Figure 4-1 10-GE Symmetric Topology



The switches in Figure 4-1 use the line cards, hardware versions, and IOS versions listed in Table 4-1 on page 4-5.

Table 4-1 Hardware and IOS Versions for the 10-GE Symmetric Topology

Switch	Module	Line Card	Hardware Version	IOS Release	Submodule	Hardware Version
DER	1	WS-X6816-GBIC	1.7	12.2(18)SXE1	WS-F6K-DFC3BXL	2.2
	2	WS-X6748-GE-TX	1.4		WS-F6700-DFC3BXL	4.0
	5	WS-SUP720-BASE	3.1		WS-F6K-PFC3BXL	1.2
					WS-SUP720 (MFSC)	2.1
	7	WS-X6704-10-GE	1.2		WS-F6700-DFC3BXL	3.0
AR1	1	WS-X6704-10GE	1.2		WS-F6700-DFC3BXL	4.0
	2	WS-X6816-GBIC	1.7		WS-F6K-DFC3BXL	2.2
	5	WS-SUP720-BASE	3.1		WS-F6K-PFC3BXL	1.2
AR2	1	WS-X4516-10GE	2.0	12.2(25)EWA	—	—
	5	WS-X4448-GB-RJ45	1.1			
AR3	1	WS-C4948-10GE	1.0			

Table 4-2 lists VLANs, their descriptions (service types), and IP addresses, for the DER and ARs in Figure 4-1 on page 4-4.

Table 4-2 VLANs, Descriptions, and IP Addresses for the 10-GE Symmetric Topology

Node	VLAN	Description	IP Address
DER	10	Management (VoD signaling, DHCP, DNS, FTP, TFTP, Syslog servers)	192.168.10.1/24
	11	Management (backup DNS server)	192.168.11.1/24
	60	Unicast video aggregation	192.168.60.1/24
	70	Multicast video aggregation	192.168.70.1/24
	80	VoIP	192.168.80.1/24
	90	HSD	Layer 2
	800	VoIP to/from AR1	192.168.252.1/30
	824	VoIP to/from AR1	192.168.252.25/30
	900	Video transport to/from AR1	192.168.254.1/30
	924	Video transport to/from AR3	192.168.254.25/30
AR1	90	HSD	Layer 2
	110	Video edge	192.168.110.1/24
	111	VoIP edge	192.168.111.1/24
	800	VoIP to/from DER	192.168.252.2/30
	808	VoIP to/from AR2	192.168.252.9/30
	900	Video transport to/from DER	192.168.254.2/30
	908	Video transport to/from AR2	192.168.254.9/30

Table 4-2 VLANs, Descriptions, and IP Addresses for the 10-GE Symmetric Topology (continued)

Node	VLAN	Description	IP Address
AR2	90	HSD	Layer 2
	120	Video edge	192.168.120.1/24
	121	VoIP edge	192.168.121.1/24
	808	VoIP to/from AR1	192.168.254.10/30
	816	VoIP to/from AR3	192.168.254.17/30
	908	Video transport to/from AR2	192.168.254.10/30
	916	Video transport to/from AR3	192.168.254.17/30
AR3	90	HSD	Layer 2
	130	Video edge	192.168.130.1/24
	131	VoIP edge	192.168.131.1/24
	816	VoIP to/from AR2	192.168.254.18/30
	824	VoIP to/from DER	192.168.254.26/30
	916	Video transport to/from AR2	192.168.254.18/30
	924	Video transport to/from DER	192.168.254.26/30

Table 4-3 on page 4-6 lists the parameters used to configure the home access gateway (HAG).

Note See HAG Functions, page 3-42, and Appendix D, "Configuring DSL Equipment."

Table 4-3 HAG Configuration Parameters

Traffic	VLAN	HAG Ports	PVC[1]	VPI[2]	VCI[3]	Encapsulation	Service Class	PCR[4]	SCR[5]	MBS[6]
HSD	90	0	1	8	35	LLC	UBR	—	—	—
VoIP	1*x*0[7]	1	4	0	51		CBR	—	300	—
Video	1*x*1	2, 3	7	8	59		VBR-RT	1200	600	10

[1] Permanent virtual connection

[2] Virtual path identifier

[3] Virtual connection identifier

[4] Peak cell rate

[5] Sustained cell rate

[6] Maximum burst size

[7] The *x* corresponds to the AR number 1, 2, or 3 in the corresponding VLAN

Configuring DER

This section addresses the configuration required on the switch labeled DER in Figure 4-1 on page 4-4, to route multiple services from that switch to the ARs.

See Configuring DNS Servers, page 4-2.

Note A Cisco Catalyst 6509 can also be used, as it uses the same supervisor engine, line cards, and Cisco IOS code as the Cisco 7609 router.

This section addresses the following:

- Configuring QoS on DER
- Establishing and Configuring Interfaces on DER
- Configuring OSPF Routing for Video and Voice Traffic on DER
- Configuring Spanning Tree on DER

Note For a complete configuration example, see Appendix A, "Sample DER and AR Switch Configurations for the 10-GE Symmetric Topology."

Configuring QoS on DER

This section presents the following topics:

- Overview of QoS on a Cisco 7600 Series and Cisco Catalyst 6500 Series
- Configuring Marking and Classification on DER
- Configuring Mapping on DER

Note For more information specific to QoS as applied to the solution, see Appendix C, "Understanding QoS as Implemented in the Solution."

Overview of QoS on a Cisco 7600 Series and Cisco Catalyst 6500 Series

This section addresses the configuration of quality of service (QoS) on the DER, through marking, classification, mapping, and queueing, to provide different degrees of quality of service for the different types of services supported by the solution architecture. For example, it is important to ensure the expeditious delivery of video and VoIP traffic, while providing only best-effort delivery for high-speed data (HSD).

By default, the Cisco 7600 series router and Cisco Catalyst 6500 series switch do not trust the incoming QoS markings, and therefore rewrite these bits with zeros. In this solution, packets at the network ingress ports are identified, classified, and marked according to type of traffic. The packets are marked with one of 64 possible Differentiated Services Code Point (DSCP) values at the ingress ports. These in turn are internally mapped to one of eight possible Class of Service (CoS) values, because CoS is used to determine the appropriate transmit queue for each packet. Queueing is configured on the individual 10-GE interfaces.

Note For more information on class of service, see “White Paper: Cisco IOS Software Features for Differentiated Class of Service for Internetworks,” at the following URL:

http://www.cisco.com/warp/public/cc/pd/iosw/iore/tech/osfea_wp.htm

Configuring Marking and Classification on DER

Do the following to enable marking and classification on DER.

Step 1 Enable QoS in global configuration mode.

```
mls qos
```

Step 2 Create access lists to identify the different service types in the network.

```
ip access-list extended acl_HSD
 remark Identify HSD traffic
 permit ip 192.168.90.0 0.0.0.255 any
ip access-list extended acl_VoD_signaling
 remark Identify VoD signaling traffic
 permit ip host 192.168.10.102 any
 permit ip host 192.168.10.103 any
ip access-list extended acl_VoIP
 remark Identify VoIP traffic
 permit ip 192.168.80.0 0.0.0.255 any
ip access-list extended acl_video_VoD_high
 remark Identify high priority VoD traffic
 permit udp 192.168.60.0 0.0.0.255 192.168.110.0 0.0.0.255 range 5000 9000
 permit udp 192.168.60.0 0.0.0.255 192.168.120.0 0.0.0.255 range 5000 9000
 permit udp 192.168.60.0 0.0.0.255 192.168.130.0 0.0.0.255 range 5000 9000
ip access-list extended acl_video_VoD_low
 remark Identify low priority VoD traffic
 permit udp 192.168.60.0 0.0.0.255 192.168.110.0 0.0.0.255 range 1000 4999
 permit udp 192.168.60.0 0.0.0.255 192.168.120.0 0.0.0.255 range 1000 4999
 permit udp 192.168.60.0 0.0.0.255 192.168.130.0 0.0.0.255 range 1000 4999
ip access-list extended acl_video_broadcast
 remark Identify broadcast video traffic (multicast)
 permit ip 192.168.70.0 0.0.0.255 232.0.0.0 0.255.255.255
```

Step 3 Create class maps for the access lists created in Step 2.

```
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_video_VoD_high
  match access-group name acl_video_VoD_high
class-map match-all class_video_VoD_low
  match access-group name acl_video_VoD_low
class-map match-all class_video_broadcast
  match access-group name acl_video_broadcast
class-map match-all class_VoD_signaling
  match access-group name acl_VoD_signaling
class-map match-all class_HSD
  match access-group name acl_HSD
```

Step 4 Create a policy map to set the DSCP values of the different classes created in Step 3.

```
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoIP
   set dscp ef
```

```
class class_HSD
 set dscp default
class class_VoD_signaling
 set dscp cs3
class class_video_broadcast
 set dscp af41
class class_video_VoD_high
 set dscp af42
class class_video_VoD_low
 set dscp af43
```

Step 5 Apply the policy map from Step 4 to the ingress interfaces using the following command.

```
service-policy input setDSCP
```

Note Specific interface examples of this and other interface commands are shown in the interface provisioning sections.

Step 6 To maintain the DSCP marking applied at the network ingress interface, configure all noningress transport interfaces to trust the incoming DSCP markings.

```
mls qos trust dscp
```

Configuring Mapping on DER

Do the following to configure mapping on DER.

Step 1 View the Cisco 7600 and Cisco Catalyst 6500 default DSCP-to-CoS mapping for the different services. Use the **show mls qos maps dscp-cos** command.

Note At the beginning of this section, we mentioned that there are 64 possible DSCP values and only 8 CoS values. This means that there could be more than one DSCP value for one CoS value. The following command shows the default DSCP-to-CoS mapping on the Cisco 7600 and Catalyst 6500.

Note In the map, d1 corresponds to the *y*-axis value of the table, and d2 to the *x*-axis value.

```
DER# 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
```

This table shows the following mappings:

Service Type	DSCP	CoS
HSD	0	0
VoD low priority	34	4
VoD high priority	36	4
VoD OOB	24	3
Broadcast video	38	4
VoIP	46	5

Step 2 Change the Cisco 7600 and Cisco Catalyst 6500 DSCP-to-CoS mapping for the different services to match the specifications of the solution.

The solution specifies the following DSCP-to CoS-mappings:

Service Type	DSCP	CoS
HSD	0	0
VoD low priority	38	1
VoD high priority	36	2
VoD OOB	24	3
Broadcast video	34	4
VoIP	46	5

a. Execute the following command on the Cisco 7600 and Cisco Catalyst 6500 to modify the DSCP-to-CoS mapping.

```
mls qos map dscp-cos 36 to 2
mls qos map dscp-cos 38 to 1
```

b. Verify the changes to the DSCP-to-CoS mappings.

```
DER# show mls qos maps dscp-cos
DSCP-CoS Mapping Table (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 02 04 01 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
```

Establishing and Configuring Interfaces on DER

Refer to Figure 4-1 on page 4-4.

This section addresses the following:

- Establishing VLANs for Services on DER
- Establishing 1-GE Interfaces for Servers, HSD, and Management on DER
- Establishing 10-GE Interfaces for Transport on DER

Establishing VLANs for Services on DER

Before 1-GE interfaces and 10-GE trunks can be configured, VLANs for the various services must be created. With the exception of VLAN 90 (high-speed data), these are all Layer 3 VLANs. (Refer to Table 4-2 on page 4-5.)

The following is configured on DER.

Tip For convenience in establishing these VLANs and others, you can establish all VLANs in global configuration mode first, then configure all the interfaces in interface configuration mode.

Step 1 Establish VLANs and VLAN interfaces for management (including VoD signaling, connectivity with DHCP, DNS, FTP, TFTP, and Syslog servers.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 10
name VLAN_10_Management
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan10
 description Management VLAN (VoD signaling, DNS, DHCP, etc)
 ip address 192.168.10.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

c. Change the load interval from the default of 300.

```
 load-interval 30
```

d. Repeat Step 1a through Step 1c, as appropriate, for the remaining management and video aggregation VLANs and interfaces. The abbreviated configurations are shown below.

Backup DNS server

```
vlan 11
name VLAN_11_Management


interface Vlan11
 description Management VLAN (Backup DNS)
 ip address 192.168.11.1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

Unicast video aggregation

```
vlan 60
name VLAN_60_Unicast_Video


interface Vlan60
 description VoD server VLAN (Unicast Video)
 ip address 192.168.60.1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

VoIP

```
vlan 80
name VLAN_80_VoIP


interface Vlan80
 description VoIP gateway VLAN
 ip address 192.168.80.1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

Step 2 Establish a VLAN for multicast video aggregation.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 70
name VLAN_70_Multicast_Video
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan70
 description Broadcast video source VLAN (Multicast Video)
 ip address 192.168.70.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

c. Enable PIM sparse mode. This is the ingress port for broadcast video traffic, which is multicast addressed.

```
 ip pim sparse-mode
```

d. Change the load interval from the default of 300.

```
 load-interval 30
```

Step 3 In global configuration mode, establish a Layer 2 VLAN for high-speed data (HSD). (No Layer 3 interface is required.)

```
vlan 90
name VLAN_90_HSD
```

Step 4 Establish VLANs for VoIP transport. The first is for transport to and from AR1.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 800
name VLAN_800_VoIP_to/from_AR1
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan800
 description VoIP transport to/from AR1
 ip address 192.168.252.1 255.255.255.252
```

c. Configure Open Shortest Path First (OSPF) on the transport VLAN interface.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

Note To avoid the election of the designated router (DR) and backup designated router (BDR), and prevent the origination of an unnecessary network link state advertisement (LSA), configure the transport VLAN as a point-to-point network. In addition, reduce the interval between OSPF hello messages from 10 seconds to 1 second. This improves reconvergence in the event of failure in the transport or in a neighboring switch.

d. Change the load interval from the default of 300.

```
 load-interval 30
```

e. Repeat Step 4a through Step 4d for VoIP transport to and from AR3.

```
vlan 824
name VoIP transport to/from AR3


interface Vlan824
 description VoIP transport to/from AR3
 ip address 192.168.252.25 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Step 5 Establish VLANs for video transport. The first is for transport to and from AR1.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 900
name VLAN_900_Video_to/from_AR1
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan900
 description Video transport VLAN to/from AR1
 ip address 192.168.254.1 255.255.255.252
```

c. Enable PIM sparse mode. This is the ingress port for broadcast video traffic, which is multicast addressed.

```
 ip pim sparse-mode
```

d. Configure OSPF on the transport VLAN interface.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

e. Change the load interval from the default of 300.

```
 load-interval 30
```

f. Repeat Step 5a through Step 5e to establish a VLAN for video transport to and from AR3.

```
vlan 924
name VLAN_924_Video_to/from_AR3

interface Vlan924
 description Video transport VLAN to/from AR3
 ip address 192.168.254.25 255.255.255.252
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Establishing 1-GE Interfaces for Servers, HSD, and Management on DER

VoD servers, high-speed data sources, and management resources connect to Layer 2 interfaces on DER, and their traffic is aggregated into the appropriate service VLANs.

The following is configured on DER.

Step 1 Establish an interface.

a. Establish an interface for high-speed data.

```
interface GigabitEthernet1/1
 description High speed data ingress/egress port
 no ip address
```

b. Configure the interface as a Layer 2 access port and assign it to VLAN 90.

```
 switchport
 switchport access vlan 90
 switchport mode access
```

c. Change the load interval from the default of 300.

```
load-interval 30
```

d. Disable Cisco Discovery Protocol (CDP) on the interface.

```
no cdp enable
```

e. Enable PortFast on the interface to bypass the listening and learning states in Spanning Tree Protocol (STP). This allows the interface to move immediately from the blocking state to the forwarding state, rather than waiting for STP to converge.

```
spanning-tree portfast
```

f. Configure the switch to disable any interface that is configured for PortFast and receives a Bridge Protocol Data Unit (BPDU).

```
spanning-tree bpduguard enable
```

Note This guards against a user accidentally connecting a switch to a switchport that is intended for a VoD server or other host. The switchport is disabled and the user must investigate why the port is down. If this command is not used and such an accidental connection were to happen, STP could reconverge and block other connections in the switch.

g. Apply the “setDSCP” service policy to mark DSCP values in the inbound IP packets.

```
service-policy input setDSCP
```

Step 2 Repeat Step 1a through Step 1g for the remaining server, HSD, and management 1-GE interfaces and their associated VLANs, changing the value in **switchport access vlan** *xxx* as appropriate. Those configurations are shown abbreviated below.

VoIP traffic

```
interface GigabitEthernet2/1
 description VoIP traffic ingress/egress

 switchport access vlan 80
```

Ingress multicast broadcast video

```
interface GigabitEthernet2/9
 description Broadcast video source (multicast 232.1.1.1 - 232.1.1.10)

 switchport access vlan 70
```

Management for the Kasenna LR server

```
interface GigabitEthernet2/17
 description Management port from Kasenna LR Server (Eth0)

 switchport access vlan 10
```

Management for the Kasenna VoD pump

```
interface GigabitEthernet2/18
 description Kasenna VoD Pump Management

 switchport access vlan 10
```

Ingress unicast video from the Kasenna VoD pump (1)

```
interface GigabitEthernet2/19
 description Unicast video from Kasenna VoD Pump (HPN0)

 switchport access vlan 60
```

Note In Kasenna’s terminology, HPN0 stands for High-Performance Network interface 0.

Ingress unicast video from the Kasenna VoD pump (2)

```
interface GigabitEthernet2/20
 description Unicast video from Kasenna VoD Pump (HPN1)

 switchport access vlan 60
```

Backup DNS server

```
interface GigabitEthernet2/48
 description Backup DNS server

 switchport access vlan 11
```

Primary DNS, DHCP, NTP, TFTP, and Syslog servers

```
interface GigabitEthernet5/2
 description Primary DNS/DHCP/NTP/TFTP/Syslog servers

 switchport access vlan 10
```

Note In this case, specify the physical connection on a Gigabit Ethernet interface as RJ-45.

```
media-type rj45
```

Establishing 10-GE Interfaces for Transport on DER

The 10-GE trunk interfaces create the ring topology from the DER through the ARs and back to the DER.

The following is configured on DER.

Step 1 Establish an interface to and from AR1.

a. Establish the interface.

```
interface TenGigabitEthernet7/1
 description Transport to/from AR1 (TenGig1/1)
 switchport

 switchport mode trunk
 dampening
 no ip address

 carrier-delay msec 0
```

b. Configure the trunk for 802.1q encapsulation.

```
 switchport trunk encapsulation dot1q
```

c. Assign the trunk to VLANs 90, 800, and 900. (See Table 4-2 on page 4-5.)

```
 switchport trunk allowed vlan 90,800,900
```

d. Change the load interval from the default of 300.

```
 load-interval 30
```

Step 2 Configure QoS on the interface.

Note The 10-GE transport links from the DER to the ARs require modifications to the transmit queues. There are eight transmit queues, but this solution uses only three.

a. View the default CoS to Tx-Queue mapping. The following information was extracted from the **show queueing interface** command.

TxQueue	CoS
1	0, 1
2	2, 3, 4
3	6, 7
4	—
5	—
6	—
7	—
8	5

b. Configure the CoS-to TxQueue mapping on the 10-GE transport interfaces. HSD (CoS = 0) remains in TxQueue1 and VoIP (CoS = 5) remains in TxQueue8. The other six CoS values are associated with TxQueue2.

```
wrr-queue cos-map 2 1 1
wrr-queue cos-map 2 2 2
wrr-queue cos-map 2 3 3 4 6 7
```

Note TxQueue1 and TxQueue8 use the default mappings. TxQueue2 has three thresholds: Threshold 1 = CoS 1, Threshold 2 = CoS 2, and Threshold 3 = CoS 3, 4, 6, and 7. For details, see Appendix C, “Understanding QoS as Implemented in the Solution.”

c. Verify the modified CoS-to-Tx-Queue mapping. The following information was extracted from the **show queueing interface** command.

TxQueue	CoS
1	0
2	1, 2, 3, 4, 6, 7
3	6, 7
4	—
5	—
6	—
7	—
8	5

d. Configure the TxQueue thresholds.

TxQueue1 uses Weighted Random Early Drop (WRED) for queue-congestion management. Only HSD is queued in this queue, and when the amount of HSD in the queue reaches 75%, random packets are dropped in an attempt to keep the queue from reaching 100% utilization.

```
wrr-queue threshold 1 100 100 100 100 100 100 100 100
wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
```

TxQueue2 uses tail drop for queue congestion management. Low-priority VoD is assigned to the first threshold and is dropped once the queue reaches 45% utilization. High-priority VoD is assigned to the second threshold and is dropped once the queue reaches 85% utilization. VoD signaling, network signaling, and broadcast video are assigned to the third threshold and are dropped once the queue reaches 100% utilization.

```
wrr-queue threshold 2 45 85 100 100 100 100 100 100
no wrr-queue random-detect 2
```

e. Configure the bandwidth of the weighted queues.

The weighted queues need to be modified to handle our modified TxQueue mappings. The ratio between TxQueue2 and TxQueue1 is 255/64 = 4, so TxQueue2 needs four times as much bandwidth as TxQueue1. Therefore, TxQueue1 is allocated 20% of the bandwidth on the interface, and TxQueue2 is allocated 80% of the bandwidth.

```
wrr-queue bandwidth 64 255 0 0 0 0 0
```

f. Configure the size of the weighted queues.

Each line card has a limited amount of buffer for the transmit queues. For this interface, 40% of the buffer is allocated for TxQueue1, and 50% of the buffer is allocated for TxQueue2.

```
wrr-queue queue-limit 40 50 0 0 0 0 0
```

g. Configure this interface (and all noningress transport interfaces) to trust the incoming DSCP markings. (This maintains the DSCP marking applied at the network ingress interface.)

```
mls qos trust dscp
```

Step 3 Establish an interface to and from AR3.

a. Establish the interface, configure the trunk for 802.1q encapsulation, and assign it to VLANs 90, 800, and 900. (See Table 4-2 on page 4-5.)

```
interface TenGigabitEthernet7/1
 description Transport to/from AR1 (TenGig1/1)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,800,900
 switchport mode trunk
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
```

b. Proceed as in Step 1b through Step 2 of this task.

Configuring OSPF Routing for Video and Voice Traffic on DER

Two OSPF routing processes must be established:

- One to route the video traffic over the transport VLANs for video
- One to route VoIP traffic over the transport VLANs for VoIP

The first OSPF process (100) associates the management VLANs, the VoD VLAN, and the broadcast VLAN with the two transport VLANs that carry video. The second OSPF process (101) associates the VoIP VLAN with the two transport VLANs that carry VoIP. Routing advertisements are enabled on the transport VLANs, but are turned off on the aggregation VLANs by means of the **passive-interface** command.

The following is configured on DER.

Step 1 Define an OSPF routing process to route video traffic.

```
router ospf 100
 router-id 1.1.1.1
 log-adjacency-changes
```

a. The OSPF timers are modified to provide fast convergence. The following command enables OSPF SPF throttling: **timers throttle spf** *spf-start spf-hold spf-max-wait*

```
 timers throttle spf 10 100 1000
```

b. The following command sets the rate-limiting values for OSPF link-state advertisement (LSA) generation: **timers throttle lsa all** *start-interval hold-interval max-interval*

```
timers throttle lsa all 1 10 1000
```

c. The following command controls the minimum interval for accepting the same LSA: **timers lsa arrival** *milliseconds*

```
timers lsa arrival 100
```

If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped.

d. Apply the **passive-interface** statements to the aggregation VLANs.

```
 passive-interface Vlan10
 passive-interface Vlan11
 passive-interface Vlan60
 passive-interface Vlan70
```

e. Advertise the networks in the first OSPF routing process.

```
 network 192.168.10.0 0.0.1.255 area 0
 network 192.168.60.0 0.0.0.255 area 0
 network 192.168.70.0 0.0.0.255 area 0
 network 192.168.254.1 0.0.0.0 area 0
 network 192.168.254.25 0.0.0.0 area 0
```

Step 2 Define a second OSPF process to route voice traffic. For details, refer to Step 1.

```
router ospf 101
 router-id 1.1.1.2
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan80
 network 192.168.80.0 0.0.0.255 area 0
 network 192.168.252.1 0.0.0.0 area 0
 network 192.168.252.25 0.0.0.0 area 0
```

Configuring Spanning Tree on DER

Because VLAN 90 is at Layer 2 around the 1-GE ring, Spanning Tree Protocol (STP) is needed to guard against loops. To improve convergence time, the four switches are configured for IEEE 802.1w Rapid Spanning Tree Protocol (RTSP), with the root at DER.

Do the following in global configuration mode to configure spanning tree parameters on DER.

Step 1 Configure DER as the root node of the spanning tree for VLAN 90. There are two ways to do this.

a. Use the **root primary** option.

```
spanning-tree vlan 90 root primary
```

or

b. Set the priority to 24576.

```
spanning-tree vlan 90 priority 24576
```

Step 2 Configure RTSP.

```
spanning-tree mode rapid-pvst
```

Step 3 Because the transport VLANs in the 10-GE ring are point-to-point networks, there is no risk of Layer 2 loops, so STP can be disabled on these VLANs.

```
no spanning-tree vlan 800, 808, 900, 908
```

Configuring AR1

This section addresses the configuration required on the switch labeled AR1 in Figure 4-1 on page 4-4, to route multiple services from AR1 to DER and AR2.

See Configuring DNS Servers, page 4-2.

Note A Cisco Catalyst 6509 can also be used, as it uses the same supervisor engine, line cards, and Cisco IOS code as the Cisco 7609 router.

This section addresses the following:

- Configuring QoS on AR1
- Establishing and Configuring Interfaces on AR1
- Configuring OSPF Routing for Video and Voice Traffic on AR1
- Configuring Spanning Tree on AR1

Note For a complete configuration example, see Appendix A, "Sample DER and AR Switch Configurations for the 10-GE Symmetric Topology."

Configuring QoS on AR1

See Overview of QoS on a Cisco 7600 Series and Cisco Catalyst 6500 Series, page 4-7.

This section presents the following topics:

- Configuring Marking and Classification on AR1
- Configuring Mapping on AR1

Note For more information specific to QoS as applied to the solution, see Appendix C, "Understanding QoS as Implemented in the Solution."

Configuring Marking and Classification on AR1

Do the following to enable marking and classification on AR1.

Step 1 Enable QoS in global configuration mode.

```
mls qos
```

Step 2 Create access lists to identify the different service types in the network.

```
ip access-list extended acl_HSD
 remark Identify HSD traffic
 permit ip 192.168.90.0 0.0.0.255 any
ip access-list extended acl_VoD_signaling
 remark Identify VoD signaling traffic
 permit ip 192.168.110.0 0.0.0.255 192.168.10.102
 permit ip 192.168.110.0 0.0.0.255 192.168.10.103
ip access-list extended acl_VoIP
 remark Identify VoIP traffic
 permit ip 192.168.111.0 0.0.0.255 any
```

Step 3 Create class maps for the access lists created in Step 2.

```
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_VoD_signaling
  match access-group name acl_VoD_signaling
class-map match-all class_HSD
  match access-group name acl_HSD
```

Step 4 Create a policy map to set the DSCP values of the different classes created in Step 3.

```
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoIP
   set dscp ef
  class class_HSD
   set dscp default
  class class_VoD_signaling
   set dscp cs3
```

Step 5 Apply the policy map from Step 4 to the ingress interfaces using the following command.

```
service-policy input setDSCP
```

Note Specific interface examples of this and other interface commands are shown in the interface provisioning sections.

Step 6 To maintain the DSCP marking applied at the network ingress interface, configure all noningress transport interfaces to trust the incoming DSCP markings.

```
mls qos trust dscp
```

Configuring Mapping on AR1

Do the following to configure mapping on AR1.

Step 1 View the Cisco 7600 and Cisco Catalyst 6500 default DSCP-to-CoS mapping for the different services. Use the **show mls qos maps dscp-cos** command.

Note At the beginning of this section, we mentioned that there are 64 possible DSCP values and only 8 CoS values. This means that there could be more than one DSCP value for one CoS value. The following command shows the default DSCP-to-CoS mapping on the Cisco 7600 and Cisco Catalyst 6500.

Note In the map, d1 corresponds to the *y*-axis value of the table, and d2 to the *x*-axis value.

```
AR1# 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
```

This table shows the following mappings:

Service Type	DSCP	CoS
HSD	0	0
VoD low priority	34	4
VoD high priority	36	4
VoD OOB	24	3
Broadcast video	38	4
VoIP	46	5

Step 2 Change the Cisco 7600 and Cisco Catalyst 6500 DSCP-to-CoS mapping for the different services to match the specifications of the solution.

The solution specifies the following DSCP-to CoS-mappings:

Service Type	DSCP	CoS
HSD	0	0
VoD low priority	38	1
VoD high priority	36	2
VoD OOB	24	3
Broadcast video	34	4
VoIP	46	5

a. Execute the following command on the Cisco 7600 and Cisco Catalyst 6500 to modify the DSCP-to-CoS mapping.

```
mls qos map dscp-cos 36 to 2
mls qos map dscp-cos 38 to 1
```

b. Verify the changes to the DSCP-to-CoS mappings.

```
AR1# show mls qos maps dscp-cos
DSCP-CoS Mapping Table (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 02 04 01 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
```

Establishing and Configuring Interfaces on AR1

Refer to Figure 4-1 on page 4-4.

This section addresses the following:

- Establishing VLANs for Services on AR1
- Establishing 10-GE Interfaces for Transport on AR1
- Establishing 1-GE Interfaces to a DSLAM on AR1

Establishing VLANs for Services on AR1

Before 1-GE interfaces and 10-GE trunks can be configured, VLANs for the various services must be created. With the exception of VLAN 90 (high-speed data), these are all Layer 3 VLANs. (Refer to Table 4-2 on page 4-5.)

Note For additional details, see Establishing VLANs for Services on DER, page 4-11.

The following is configured on AR1.

Step 1 In global configuration mode, establish a Layer 2 VLAN for high-speed data (HSD). (No Layer 3 interface is required.)

```
vlan 90
name VLAN_90_HSD
```

Step 2 Establish a VLAN for video at the edge.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 110
name VLAN_110_Video
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan110
 description Video edge VLAN
 ip address 192.168.110.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

c. Enable PIM sparse mode. This is the aggregation VLAN for video traffic to the DSLAMs. Broadcast video is multicast addressed.

```
 ip pim sparse-mode
```

d. To ensure consistently fast PIM convergence times, statically join the aggregation VLAN for video at the AR to the multicast groups.

```
 ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
```

e. Change the load interval from the default of 300.

```
 load-interval 30
```

f. Change the ARP timeout from the default.

```
 arp timeout 250
```

Note The default timeout for an entry in the ARP cache is 4 hours. The default timeout for an entry in the MAC address table is only 5 minutes. Because video traffic is mostly unidirectional, the MAC address table may not be refreshed within the 5-minute timeout. This causes video traffic to be flooded until the destination MAC address is found. To prevent this, reduce the ARP cache timeout to 250 seconds. This forces the switch to re-ARP for the entries in the ARP cache before the entries in the MAC address table time out, avoiding the disruptive behavior.

Step 3 Establish a VLAN for VoIP at the edge.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 111
name VLAN_111_VoIP
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan111
 description VoIP edge VLAN
 ip address 192.168.111.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

c. Change the load interval from the default of 300.

```
 load-interval 30
```

Step 4 Establish VLANs for VoIP transport. The first is to and from DER.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 800
name VLAN_800_VoIP_to/from_DER
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan800
 description VoIP transport VLAN to/from DER
 ip address 192.168.252.2 255.255.255.252
```

c. Configure OSPF on the transport VLAN interface.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

d. Change the load interval from the default of 300.

```
 load-interval 30
```

e. Repeat Step 4a through Step 4d, as appropriate, to establish a VLAN for VoIP transport to and from AR2.

```
vlan 808
name VLAN_808_VoIP_to/from_DER


interface Vlan808
 description VoIP transport VLAN to/from AR2
 ip address 192.168.252.9 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Step 5 Establish VLANs for video transport. The first is to and from DER.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 900
name VLAN_900_Video_to/from_DER
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan900
 description Video transport VLAN to/from DER
 ip address 192.168.254.2 255.255.255.252
```

c. Enable Protocol Independent Multicast (PIM) sparse mode. Broadcast video is multicast addressed.

```
 ip pim sparse-mode
```

d. Configure OSPF on the transport VLAN interface.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

e. Change the load interval from the default of 300.

```
 load-interval 30
```

f. Repeat Step 5a through Step 5e, as appropriate, to establish a VLAN for video transport to and from AR2.

```
vlan 908
name VLAN_908_Video_to/from_AR2


interface Vlan908
 description Video transport VLAN to/from AR2
 ip address 192.168.254.9 255.255.255.252
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Establishing 10-GE Interfaces for Transport on AR1

The 10-GE trunk interfaces provide the transport between AR1 and DER and AR2.

Note For additional details, see Establishing 10-GE Interfaces for Transport on DER, page 4-16.

The following is configured on AR1.

Step 1 Establish an interface. The first is to and from DER.

a. Establish the interface to and from DER, configure the trunk for 802.1q encapsulation, and assign it to VLANs 90, 800, and 900. (See Table 4-2 on page 4-5.)

```
interface TenGigabitEthernet1/1
 description Transport to/from DER (TenGig7/1)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,800,900
 switchport mode trunk
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
```

b. Proceed as in Step 2 of Establishing 10-GE Interfaces for Transport on DER, page 4-16.

```
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 1 100 100 100 100 100 100 100 100
 wrr-queue threshold 2 85 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 2 1 1
 wrr-queue cos-map 2 2 2
 wrr-queue cos-map 2 3 3 4 6 7
 mls qos trust dscp
```

Step 2 Repeat Step 1, as appropriate, to establish an interface to and from AR3 and assign it to VLANs 90, 824, and 924.

```
interface TenGigabitEthernet1/3
 description Transport to/from AR2 (TenGig1/1)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,808,908
 switchport mode trunk
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 1 100 100 100 100 100 100 100 100
 wrr-queue threshold 2 45 85 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 2 1 1
 wrr-queue cos-map 2 2 2
 wrr-queue cos-map 2 3 3 4 6 7
 mls qos trust dscp
```

Establishing 1-GE Interfaces to a DSLAM on AR1

The only 1-GE interface is to and from DSLAM1.

The following is configured on AR1.

Step 1 Establish an interface to DSLAM1.

a. Establish the interface and assign it to VLANs 90, 110, and 111.

```
interface GigabitEthernet2/1
 description GigE trunk to/from DSLAM uplink GigE
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,110,111
 switchport mode trunk

 no ip address
```

b. Prevent unknown unicast traffic from being flooded to the port.

```
 switchport block unicast
```

Note Occasionally, unknown unicast or multicast traffic is flooded to a switch port because a MAC address has timed out or has not been learned by the switch. (This condition is especially undesirable for a private VLAN isolated port.) To guarantee that no unicast or multicast traffic is flooded to the port, use the **switchport block unicast** or **switchport block multicast** commands.

c. Apply the “setDSCP” service policy to mark DSCP values in the inbound IP packets.

```
 service-policy input setDSCP
```

d. Change the load interval from the default of 300.

```
load-interval 30
```

e. Proceed as in Step 2 of Establishing 10-GE Interfaces for Transport on DER, page 4-16.

```
wrr-queue bandwidth 64 255
wrr-queue queue-limit 40 50
wrr-queue random-detect min-threshold 1 75 100
wrr-queue random-detect min-threshold 2 50 100
wrr-queue random-detect max-threshold 1 100 100
wrr-queue random-detect max-threshold 2 50 100
wrr-queue cos-map 1 1 0
wrr-queue cos-map 2 1 1
wrr-queue cos-map 2 2 2 3 4 6 7
```

Note The cos-map value 1 1 0 is a default setting on 1-GE interfaces.

f. Disable Cisco Discovery Protocol (CDP) on the interface.

```
no cdp enable
```

g. Enable PortFast on the interface to bypass the listening and learning states in Spanning Tree Protocol (STP). This allows the interface to move immediately from the blocking state to the forwarding state, rather than waiting for STP to converge.

```
spanning-tree portfast
```

h. Configure the switch to disable any interface that is configured for PortFast and receives a Bridge Protocol Data Unit (BPDU).

```
spanning-tree bpduguard enable
```

Note This guards against a user accidentally connecting a switch to a switchport that is intended for a VoD server or other host. The switchport is disabled and the user must investigate why the port is down. If this command is not used and such an accidental connection were to happen, STP could reconverge and block other connections in the switch.

i. Apply the “setDSCP” service policy to mark DSCP values in the inbound IP packets.

```
service-policy input setDSCP
```

Configuring OSPF Routing for Video and Voice Traffic on AR1

For background and details, refer to Configuring OSPF Routing for Video and Voice Traffic on DER, page 4-19.

The following is configured on AR1.

Step 1 Define an OSPF routing process to route video traffic. This process associates the transport VLANs for video with the video aggregation VLAN for the for DSLAM1 and other DSLAMs to be served by AR1 (VLAN 110).

```
router ospf 100
 router-id 2.2.2.1
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan110
 network 192.168.110.0 0.0.0.255 area 0
 network 192.168.254.2 0.0.0.0 area 0
 network 192.168.254.9 0.0.0.0 area 0
```

Step 2 Define an OSPF process to route voice traffic. This process associates the transport VLANs for VoIP with the VoIP aggregation VLAN for the for DSLAM1 and other DSLAMs to be served by AR1 (VLAN 111).

```
router ospf 101
 router-id 2.2.2.2
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan111
 network 192.168.111.0 0.0.0.255 area 0
 network 192.168.252.2 0.0.0.0 area 0
 network 192.168.252.9 0.0.0.0 area 0
```

Configuring Spanning Tree on AR1

Note See Configuring Spanning Tree on DER, page 4-20.

The following is configured on AR1.

Step 1 Configure RTSP.

```
spanning-tree mode rapid-pvst
```

Step 2 Because the transport VLANs in the 10-GE ring are point-to-point networks, there is no risk of Layer 2 loops, so STP can be disabled on these VLANs.

```
no spanning-tree vlan 800, 808, 900, 908
```

Configuring AR2

This section addresses the configuration required on the switch labeled AR2 in Figure 4-1 on page 4-4, to route multiple services from AR2 to DER, AR1, and AR3.

See Configuring DNS Servers, page 4-2.

This section addresses the following:

- Configuring QoS on AR2
- Establishing and Configuring Interfaces on AR2
- Configuring OSPF Routing for Video and Voice Traffic on AR2
- Configuring Spanning Tree on AR2

Note For a complete configuration example, see Appendix A, "Sample DER and AR Switch Configurations for the 10-GE Symmetric Topology."

Configuring QoS on AR2

This section presents the following topics:

- Overview of QoS on a Cisco Catalyst 4500 Series
- Configuring Marking and Classification on AR2
- Configuring Mapping on AR2
- Configuring Queueing on AR2

Note For more information specific to QoS as applied to the solution, see Appendix C, "Understanding QoS as Implemented in the Solution."

Overview of QoS on a Cisco Catalyst 4500 Series

This section addresses the configuration of quality of service (QoS) on AR2, through marking, classification, mapping, and queueing, to provide different degrees of quality of service for the different types of services supported by the solution architecture. For example, it is important to ensure the expeditious delivery of video and VoIP traffic, while providing only best-effort delivery for high-speed data (HSD).

By default, the Cisco Catalyst 4500 series switches (including the Cisco Catalyst 4948-10GE) do not trust the incoming QoS markings, and therefore rewrite these bits with zeros. In this solution, packets at the network ingress ports are identified, classified, and marked according to type of traffic. The packets are marked with one of 64 possible Differentiated Services Code Point (DSCP) values at the ingress ports. These in turn are internally mapped to one of eight possible Class of Service (CoS) values. The DSCP values are used to determine the appropriate transmit queue for each packet.

Configuring Marking and Classification on AR2

Do the following to enable marking and classification on AR2.

Step 1 Enable QoS in global configuration mode.

```
qos
```

Step 2 Create access lists to identify the different service types in the network.

```
ip access-list extended acl_HSD
 remark Identify HSD traffic
 permit ip 192.168.90.0 0.0.0.255 any
ip access-list extended acl_VoD_signaling
 remark Identify VoD signaling traffic
 permit ip 192.168.120.0 0.0.0.255 192.168.10.102
 permit ip 192.168.120.0 0.0.0.255 192.168.10.103
ip access-list extended acl_VoIP
 remark Identify VoIP traffic
 permit ip 192.168.121.0 0.0.0.255 any
```

Step 3 Create class maps for the access lists created in Step 2.

```
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_VoD_signaling
  match access-group name acl_VoD_signaling
class-map match-all class_HSD
  match access-group name acl_HSD
```

Step 4 Create a policy map to set the DSCP values of the different classes created in Step 3.

```
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoIP
   set dscp ef
  class class_HSD
   set dscp default
  class class_VoD_signaling
   set dscp cs3
```

Step 5 Apply the policy map from Step 4 to the ingress interfaces using the following command.

```
service-policy input setDSCP
```

Note Specific interface examples of this and other interface commands are shown in the interface provisioning sections.

Step 6 To maintain the DSCP marking applied at the network ingress interface, configure all noningress transport interfaces to trust the incoming DSCP markings.

```
qos trust dscp
```

Configuring Mapping on AR2

Do the following to configure mapping on AR2.

Step 1 View the Cisco Catalyst 4500 series default DSCP-to-CoS mapping for the different services. Use the **show qos maps dscp-cos** command.

Note At the beginning of this section, we mentioned that there are 64 possible DSCP values and only 8 CoS values. This means that there could be more than one DSCP value for one CoS value. The following command shows the default DSCP-to-CoS mapping on the Cisco Catalyst 4500 series.

Note In the map, d1 corresponds to the *y*-axis value of the table, and d2 to the *x*-axis value.

```
AR2# show qos maps dscp

DSCP-CoS Mapping Table (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
```

This table shows the following mappings:

Service Type	DSCP	CoS
HSD	0	0
VoD low priority	34	4
VoD high priority	36	4
VoD OOB	24	3
Broadcast video	38	4
VoIP	46	5

Step 2 Change the Cisco Catalyst 4500 series DSCP-to-CoS mapping for the different services to match the specifications of the solution.

The solution specifies the following DSCP-to CoS-mappings:

Service Type	DSCP	CoS
HSD	0	0
VoD low priority	38	1
VoD high priority	36	2
VoD OOB	24	3
Broadcast video	34	4
VoIP	46	5

a. Execute the following command on the Cisco Catalyst 4500 series to modify the DSCP-to-CoS mapping.

```
qos map dscp 38 to cos 1
qos map dscp 36 to cos 2
```

b. Verify the changes to the DSCP-to-CoS mappings.

```
AR2# show qos maps dscp

DSCP-CoS Mapping Table (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 02 04 01 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
```

Configuring Queueing on AR2

Unlike the Cisco 7600 series and Cisco Catalyst 6500 series, the Cisco Catalyst 4500 series uses the same queueing on all interfaces. Queueing is configured globally.

Do the following to change the DSCP-to-TxQueue mappings on AR2.

Step 1 View the default DSCP-to-Tx-Queue mapping. The following information was extracted from the **show qos maps dscp** command.

```
DSCP-TxQueue Mapping Table (dscp = d1d2)
d1 : d2  0  1  2  3  4  5  6  7  8  9
-------------------------------------
 0 :    01 01 01 01 01 01 01 01 01 01
 1 :    01 01 01 01 01 01 02 02 02 02
 2 :    02 02 02 02 02 02 02 02 02 02
 3 :    02 02 03 03 03 03 03 03 03 03
 4 :    03 03 03 03 03 03 03 03 04 04
 5 :    04 04 04 04 04 04 04 04 04 04
 6 :    04 04 04 04
```

Step 2 Configure the DSCP-to TxQueue mapping by moving DSCP 34 and 36 to TxQueue2. Additionally, move all DSCPs that are in TxQueue4 to TxQueue2, because TxQueue4 is not used.

```
qos map dscp 34 36 38 48 49 50 51 52 to tx-queue 2
qos map dscp 53 54 55 56 57 58 59 60 to tx-queue 2
qos map dscp 61 62 63 to tx-queue 2
```

Step 3 Verify the modified DSCP-to-Tx-Queue mapping. The following information was extracted from the **show queueing interface** command.

```
DSCP-TxQueue Mapping Table (dscp = d1d2)
d1 : d2  0  1  2  3  4  5  6  7  8  9
-------------------------------------
 0 :    01 01 01 01 01 01 01 01 01 01
 1 :    01 01 01 01 01 01 02 02 02 02
 2 :    02 02 02 02 02 02 02 02 02 02
 3 :    02 02 03 03 02 03 02 03 02 03
 4 :    03 03 03 03 03 03 03 03 02 02
 5 :    02 02 02 02 02 02 02 02 02 02
 6 :    02 02 02 02
```

Step 4 Configure the TxQueue thresholds.

TxQueue1 uses Weighted Random Early Drop (WRED) for queue-congestion management. Only HSD is queued in this queue, and when the amount of HSD in the queue reaches 75%, random packets are dropped in an attempt to keep the queue from reaching 100% utilization.

```
wrr-queue threshold 1 100 100 100 100 100 100 100 100
wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
```

TxQueue2 uses tail drop for queue congestion management. Low-priority VoD is assigned to the first threshold and is dropped once the queue reaches 45% utilization. High-priority VoD is assigned to the second threshold and is dropped once the queue reaches 85% utilization. VoD signaling, network signaling, and broadcast video are assigned to the third threshold and is dropped once the queue reaches 100% utilization.

```
wrr-queue threshold 2 45 85 100 100 100 100 100 100
no wrr-queue random-detect 2
```

Step 5 Configure the bandwidth of the weighted queues.

The weighted queues need to be modified to handle our modified TxQueue mappings. The ratio between TxQueue2 and TxQueue1 is 255/64 = 4, so TxQueue2 needs four times as much bandwidth as TxQueue1. Therefore, TxQueue1 is allocated 20% of the bandwidth on the interface, and TxQueue2 is allocated 80% of the bandwidth.

```
wrr-queue bandwidth 64 255 0 0 0 0 0
```

Step 6 Configure the size of the weighted queues.

Each line card has a limited amount of buffer for the transmit queues. For this interface, 40% of the buffer is allocated for TxQueue1, and 50% of the buffer is allocated for TxQueue2.

```
wrr-queue queue-limit 40 50 0 0 0 0 0
```

Establishing and Configuring Interfaces on AR2

Refer to Figure 4-1 on page 4-4.

This section addresses the following:

- Establishing VLANs for Services on AR2
- Establishing 10-GE Interfaces for Transport on AR2
- Establishing 1-GE Interfaces to a DSLAM on AR2

Establishing VLANs for Services on AR2

Before 1-GE interfaces and 10-GE trunks can be configured, VLANs for the various services must be created. With the exception of VLAN 90 (high-speed data), these are all Layer 3 VLANs. (Refer to Table 4-2 on page 4-5.)

Note For additional details, see Establishing VLANs for Services on DER, page 4-11, and Establishing VLANs for Services on AR1, page 4-24.

The following is configured on AR2.

Step 1 In global configuration mode, establish a Layer 2 VLAN for high-speed data (HSD). (No Layer 3 interface is required.)

```
vlan 90
name VLAN_90_HSD
```

Step 2 Establish a VLAN for video at the edge.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 120
name VLAN_120_Video
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan120
 description Video edge VLAN
 ip address 192.168.120.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

c. Enable PIM sparse mode.

```
ip pim sparse-mode
```

d. To ensure consistently fast PIM convergence times, statically join the aggregation VLAN for video at the AR to the multicast groups.

```
ip igmp static-group 232.1.1.1 source ssm-map
ip igmp static-group 232.1.1.2 source ssm-map
ip igmp static-group 232.1.1.3 source ssm-map
ip igmp static-group 232.1.1.4 source ssm-map
ip igmp static-group 232.1.1.5 source ssm-map
ip igmp static-group 232.1.1.6 source ssm-map
ip igmp static-group 232.1.1.7 source ssm-map
ip igmp static-group 232.1.1.8 source ssm-map
ip igmp static-group 232.1.1.9 source ssm-map
ip igmp static-group 232.1.1.10 source ssm-map
```

e. Change the load interval from the default of 300.

```
 load-interval 30
```

f. Change the ARP timeout from the default.

```
 arp timeout 250
```

Step 3 Establish a VLAN for VoIP at the edge.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 121
name VLAN_121_VoIP
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan121
 description VoIP edge VLAN
 ip address 192.168.121.1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

Step 4 Establish VLANs for VoIP transport. The first is to and from AR1.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 808
name VLAN_808_VoIP_to/from_AR1
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan808
 description VoIP transport VLAN to/from AR1
 ip address 192.168.252.10 255.255.255.252
```

c. Configure OSPF on the transport VLAN interface.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

d. Change the load interval from the default of 300.

```
 load-interval 30
```

e. Repeat Step 4a through Step 4d, as appropriate, to establish a VLAN for VoIP transport to and from AR3.

```
vlan 816
name VLAN_816_VoIP_to/from_AR3


interface Vlan816
 description VoIP transport VLAN to/from AR3
 ip address 192.168.252.17 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Step 5 Establish VLANs for video transport. The first is to and from AR1.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 908
name VLAN_908_Video_to/from_AR1
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan908
 description Video transport VLAN to/from AR1
 ip address 192.168.254.10 255.255.255.252
```

c. Enable PIM sparse mode.

```
 ip pim sparse-mode
```

d. Configure OSPF.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

e. Change the load interval from the default of 300.

```
 load-interval 30
```

f. Repeat Step 5a through Step 5e, as appropriate, to establish a VLAN for video transport to and from AR3.

```
vlan 916
name VLAN_916_Video_to/from_AR3


interface Vlan916
 description Video transport VLAN to/from AR3
 ip address 192.168.254.17 255.255.255.252
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Establishing 10-GE Interfaces for Transport on AR2

The 10-GE trunk interfaces provide the transport between AR2 and AR1 and AR3.

The following is configured on AR2.

Note For additional details, see Establishing 10-GE Interfaces for Transport on DER, page 4-16.

Step 1 Establish an interface. The first is to and from AR1.

a. Establish the interface, configure the trunk for 802.1q encapsulation, and assign it to VLANs 90, 808, and 908. (See Table 4-2 on page 4-5.)

```
interface TenGigabitEthernet1/1
 description Transport to/from AR1 (TenGig1/3)
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,808,908
 switchport mode trunk
 dampening
 load-interval 30
 carrier-delay msec 0
```

b. Configure this interface (and all noningress transport interfaces) to trust the incoming DSCP markings. (This maintains the DSCP marking applied at the network ingress interface.)

```
 qos trust dscp
```

c. Set transmit-queue bandwidth thresholds and priority.

```
tx-queue 1
  bandwidth percent 19
tx-queue 2
  bandwidth percent 80
tx-queue 3
  priority high
tx-queue 4
  bandwidth percent 1
```

Note See Appendix C, "Understanding QoS as Implemented in the Solution."

Step 2 Repeat Step 1, as appropriate, to establish an interface to and from AR3 and assign it to VLANs 90, 816, and 916.

```
interface TenGigabitEthernet1/2
 description Transport to/from AR3 (TenGig1/49)
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,816,916
 switchport mode trunk
 dampening
 load-interval 30
 carrier-delay msec 0
 qos trust dscp
 tx-queue 1
   bandwidth percent 19
 tx-queue 2
   bandwidth percent 80
 tx-queue 3
   priority high
 tx-queue 4
   bandwidth percent 1
 spanning-tree cost 10 <---See Note below
```

Note Note that the spanning-tree cost is set to 10 on AR2. This breaks the loop for VLAN 90 (Layer 2) between AR2 and AR3, rather than somewhere else.

Establishing 1-GE Interfaces to a DSLAM on AR2

The only 1-GE interface is a trunk to and from DSLAM2.

The following is configured on AR2.

Step 1 Establish an interface to DSLAM2.

a. Establish the interface and assign it to VLANs 90, 120, and 121.

```
interface GigabitEthernet5/1
 description GigE trunk to/from DSLAM uplink GigE
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,120,121
 switchport mode trunk
```

b. Prevent unknown unicast traffic from being flooded to the port.

```
 switchport block unicast
```

Note Occasionally, unknown unicast or multicast traffic is flooded to a switch port because a MAC address has timed out or has not been learned by the switch. (This condition is especially undesirable for a private VLAN isolated port.) To guarantee that no unicast or multicast traffic is flooded to the port, use the **switchport block unicast** or **switchport block multicast** commands.

c. Change the load interval from the default of 300.

```
load-interval 30
```

d. Set transmit-queue bandwidth thresholds and priority.

```
tx-queue 1
  bandwidth percent 19
tx-queue 2
  bandwidth percent 80
tx-queue 3
  priority high
tx-queue 4
```

e. Disable Cisco Discovery Protocol (CDP) on the interface.

```
no cdp enable
```

f. Enable PortFast on the interface to bypass the listening and learning states in Spanning Tree Protocol (STP). This allows the interface to move immediately from the blocking state to the forwarding state, rather than waiting for STP to converge.

```
spanning-tree portfast trunk
```

g. Configure the switch to disable any interface that is configured for PortFast and receives a Bridge Protocol Data Unit (BPDU).

```
spanning-tree bpduguard enable
```

Note This guards against a user accidentally connecting a switch to a switchport that is intended for a VoD server or other host. The switchport is disabled and the user must investigate why the port is down. If this command is not used and such an accidental connection were to happen, STP could reconverge and block other connections in the switch.

h. Apply the “setDSCP” service policy to mark DSCP values in the inbound IP packets.

```
service-policy input setDSCP
```

Configuring OSPF Routing for Video and Voice Traffic on AR2

Note For background and details, see Configuring OSPF Routing for Video and Voice Traffic on DER, page 4-19.

The following is configured on AR2.

Step 1 Define an OSPF routing process to route video traffic. This process associates the transport VLANs for video with the video aggregation VLAN for the DSLAM (VLAN 120).

```
router ospf 100
 router-id 3.3.3.1
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan120
 network 192.168.120.0 0.0.0.255 area 0
 network 192.168.254.10 0.0.0.0 area 0
 network 192.168.254.17 0.0.0.0 area 0
```

Step 2 Define an OSPF process to route voice traffic. This process associates the transport VLANs for VoIP with the VoIP aggregation VLAN for the DSLAM (VLAN 121).

```
router ospf 101
 router-id 3.3.3.2
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan121
 network 192.168.121.0 0.0.0.255 area 0
 network 192.168.252.10 0.0.0.0 area 0
 network 192.168.252.17 0.0.0.0 area 0
```

Configuring Spanning Tree on AR2

Note See Configuring Spanning Tree on DER, page 4-20.

The following is configured on AR2.

Step 1 Configure RTSP.

```
spanning-tree mode rapid-pvst
```

Step 2 Because the transport VLANs in the 10-GE ring are point-to-point networks, there is no risk of Layer 2 loops, so STP can be disabled on these VLANs.

```
no spanning-tree vlan 800, 816, 908, 916
```

Configuring AR3

This section addresses the configuration required on the switch labeled AR3 in Figure 4-1 on page 4-4, to route multiple services from AR3 to AR2 and DER.

See Configuring DNS Servers, page 4-2.

This section addresses the following:

- Configuring QoS on AR3
- Establishing and Configuring Interfaces on AR3
- Configuring OSPF Routing for Video and Voice Traffic on AR3
- Configuring Spanning Tree on AR3

Note For a complete configuration example, see Appendix A, "Sample DER and AR Switch Configurations for the 10-GE Symmetric Topology."

Configuring QoS on AR3

See Overview of QoS on a Cisco Catalyst 4500 Series, page 4-31.

This section presents the following topics:

- Configuring Marking and Classification on AR3
- Configuring Mapping on AR3
- Configuring Queueing on AR3

Note For more information specific to QoS as applied to the solution, see Appendix C, "Understanding QoS as Implemented in the Solution."

Configuring Marking and Classification on AR3

Do the following to enable marking and classification on AR3.

Step 1 Enable QoS in global configuration mode.

```
qos
```

Step 2 Create access lists to identify the different service types in the network.

```
ip access-list extended acl_HSD
 remark Identify HSD traffic
 permit ip 192.168.90.0 0.0.0.255 any
ip access-list extended acl_VoD_signaling
 remark Identify VoD signaling traffic
 permit ip 192.168.130.0 0.0.0.255 192.168.10.102
 permit ip 192.168.130.0 0.0.0.255 192.168.10.103
ip access-list extended acl_VoIP
 remark Identify VoIP traffic
 permit ip 192.168.131.0 0.0.0.255 any
```

Step 3 Create class maps for the access lists created in Step 2.

```
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_VoD_signaling
  match access-group name acl_VoD_signaling
class-map match-all class_HSD
  match access-group name acl_HSD
```

Step 4 Create a policy map to set the DSCP values of the different classes created in Step 3.

```
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoIP
   set dscp ef
  class class_HSD
   set dscp default
  class class_VoD_signaling
   set dscp cs3
```

Step 5 Apply the policy map from Step 4 to the ingress interfaces using the following command.

```
service-policy input setDSCP
```

Note Specific interface examples of this and other interface commands are shown in the interface provisioning sections.

Step 6 To maintain the DSCP marking applied at the network ingress interface, configure all noningress transport interfaces to trust the incoming DSCP markings.

```
qos trust dscp
```

Configuring Mapping on AR3

Do the following to configure mapping on AR3.

Step 1 View the Cisco Catalyst 4500 series default DSCP-to-CoS mapping for the different services. Use the **show qos maps dscp-cos** command.

Note At the beginning of this section, we mentioned that there are 64 possible DSCP values and only 8 CoS values. This means that there could be more than one DSCP value for one CoS value. The following command shows the default DSCP-to-CoS mapping on the Cisco Catalyst 4500 series.

Note In the map, d1 corresponds to the *y*-axis value of the table, and d2 to the *x*-axis value.

```
AR3# show qos maps dscp

DSCP-CoS Mapping Table (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
```

This table shows the following mappings:

Service Type	DSCP	CoS
HSD	0	0
VoD low priority	34	4
VoD high priority	36	4
VoD OOB	24	3
Broadcast video	38	4
VoIP	46	5

Step 2 Change the Cisco Catalyst 4500 series DSCP-to-CoS mapping for the different services to match the specifications of the solution.

The solution specifies the following DSCP-to CoS-mappings:

Service Type	DSCP	CoS
HSD	0	0
VoD low priority	38	1
VoD high priority	36	2
VoD OOB	24	3
Broadcast video	34	4
VoIP	46	5

a. Execute the following command on the Cisco Catalyst 4500 series to modify the DSCP-to-CoS mapping.

```
qos map dscp 38 to cos 1
qos map dscp 36 to cos 2
```

b. Verify the changes to the DSCP-to-CoS mappings.

```
AR3# show qos maps dscp

DSCP-CoS Mapping Table (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 02 04 01 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
```

Configuring Queueing on AR3

Unlike the Cisco 7600 series and Cisco Catalyst 6500 series, the Cisco Catalyst 4500 series uses the same queueing on all interfaces. Queueing is configured globally.

Do the following to change the DSCP-to-TxQueue mappings on AR3.

Step 1 View the default DSCP-to-Tx-Queue mapping. The following information was extracted from the **show qos maps dscp** command.

```
DSCP-TxQueue Mapping Table (dscp = d1d2)
d1 : d2  0  1  2  3  4  5  6  7  8  9
-------------------------------------
 0 :    01 01 01 01 01 01 01 01 01 01
 1 :    01 01 01 01 01 01 02 02 02 02
 2 :    02 02 02 02 02 02 02 02 02 02
 3 :    02 02 03 03 03 03 03 03 03 03
 4 :    03 03 03 03 03 03 03 03 04 04
 5 :    04 04 04 04 04 04 04 04 04 04
 6 :    04 04 04 04
```

Step 2 Configure the DSCP-to TxQueue mapping by moving DSCP 34, 36, and 38 to TxQueue2. Additionally, move all DSCPs that are in TxQueue4 to TxQueue2, because TxQueue4 is not used.

```
qos map dscp 34 36 38 48 49 50 51 52 to tx-queue 2
qos map dscp 53 54 55 56 57 58 59 60 to tx-queue 2
qos map dscp 61 62 63 to tx-queue 2
```

Step 3 Verify the modified DSCP-to-TxQueue mapping. The following information was extracted from the **show queueing interface** command.

```
DSCP-TxQueue Mapping Table (dscp = d1d2)
d1 : d2  0  1  2  3  4  5  6  7  8  9
-------------------------------------
 0 :    01 01 01 01 01 01 01 01 01 01
 1 :    01 01 01 01 01 01 02 02 02 02
 2 :    02 02 02 02 02 02 02 02 02 02
 3 :    02 02 03 03 02 03 02 03 02 03
 4 :    03 03 03 03 03 03 03 03 02 02
 5 :    02 02 02 02 02 02 02 02 02 02
 6 :    02 02 02 02
```

Step 4 Configure the TxQueue thresholds.

TxQueue1 uses Weighted Random Early Drop (WRED) for queue-congestion management. Only HSD is queued in this queue, and when the amount of HSD in the queue reaches 75%, random packets are dropped in an attempt to keep the queue from reaching 100% utilization.

```
wrr-queue threshold 1 100 100 100 100 100 100 100 100
wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
```

TxQueue2 uses tail drop for queue congestion management. Low-priority VoD is assigned to the first threshold and is dropped once the queue reaches 45% utilization. High-priority VoD is assigned to the second threshold and is dropped once the queue reaches 85% utilization. VoD signaling, network signaling, and broadcast video are assigned to the third threshold and is dropped once the queue reaches 100% utilization.

```
wrr-queue threshold 2 45 85 100 100 100 100 100 100
no wrr-queue random-detect 2
```

Step 5 Configure the bandwidth of the weighted queues.

The weighted queues need to be modified to handle our modified TxQueue mappings. The ratio between TxQueue2 and TxQueue1 is 255/64 = 4, so TxQueue2 needs four times as much bandwidth as TxQueue1. Therefore, TxQueue1 is allocated 20% of the bandwidth on the interface, and TxQueue2 is allocated 80% of the bandwidth.

```
wrr-queue bandwidth 64 255 0 0 0 0 0
```

Step 6 Configure the size of the weighted queues.

Each line card has a limited amount of buffer for the transmit queues. For this interface, 40% of the buffer is allocated for TxQueue1, and 50% of the buffer is allocated for TxQueue2.

```
wrr-queue queue-limit 40 50 0 0 0 0 0
```

Establishing and Configuring Interfaces on AR3

Refer to Figure 4-1 on page 4-4.

This section addresses the following:

- Establishing VLANs for Services on AR3
- Establishing 10-GE Interfaces for Transport on AR3
- Establishing 1-GE Interfaces to a DSLAM on AR3

Establishing VLANs for Services on AR3

Before 1-GE interfaces and 10-GE trunks can be configured, VLANs for the various services must be created. With the exception of VLAN 90 (high-speed data), these are all Layer 3 VLANs. (Refer to Table 4-2 on page 4-5.)

Note For additional details, see Establishing VLANs for Services on DER, page 4-11, and Establishing VLANs for Services on AR1, page 4-24.

The following is configured on AR3.

Step 1 In global configuration mode, establish a Layer 2 VLAN for high-speed data (HSD). (No Layer 3 interface is required.)

```
vlan 90
name VLAN_90_HSD
```

Step 2 Establish a VLAN for video at the edge.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 130
name VLAN_130_Video
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan130
 description Video edge VLAN
 ip address 192.168.130.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

c. Enable PIM sparse mode

```
 ip pim sparse-mode
```

d. To ensure consistently fast PIM convergence times, statically join the aggregation VLAN for video at the AR to the multicast groups.

```
ip igmp static-group 232.1.1.1 source ssm-map
ip igmp static-group 232.1.1.2 source ssm-map
ip igmp static-group 232.1.1.3 source ssm-map
ip igmp static-group 232.1.1.4 source ssm-map
ip igmp static-group 232.1.1.5 source ssm-map
ip igmp static-group 232.1.1.6 source ssm-map
ip igmp static-group 232.1.1.7 source ssm-map
ip igmp static-group 232.1.1.8 source ssm-map
ip igmp static-group 232.1.1.9 source ssm-map
ip igmp static-group 232.1.1.10 source ssm-map
```

e. Change the load interval from the default of 300.

```
 load-interval 30
```

f. Change the ARP timeout from the default.

```
 arp timeout 250
```

Step 3 Establish a VLAN for VoIP at the edge.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 131
name VLAN_131_VoIP
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan131
 description VoIP edge VLAN
 ip address 192.168.131.1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

Step 4 Establish VLANs for VoIP transport. The first is to and from AR2.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 816
name VLAN_816_VoIP_to/from_AR2
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan816
 description VoIP transport VLAN to/from AR2
 ip address 192.168.252.18 255.255.255.252
```

c. Configure OSPF on the transport VLAN interface.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

d. Change the load interval from the default of 300.

```
 load-interval 30
```

e. Repeat Step 4a through Step 4d to establish a VLAN for VoIP transport to and from DER.

```
vlan 824
name VLAN_824_VoIP_to/from_DER

interface Vlan824
 description VoIP transport VLAN to/from DER
 ip address 192.168.252.26 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Step 5 Establish VLANs for video transport. The first is to and from AR2.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 916
name VLAN_916_Video_to/from_AR2
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan916
 description Video transport VLAN to/from AR2
 ip address 192.168.254.18 255.255.255.252
```

c. Enable PIM sparse mode.

```
 ip pim sparse-mode
```

d. Configure OSPF.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

e. Change the load interval from the default of 300.

```
 load-interval 30
```

f. Repeat Step 5a through Step 5e to establish a VLAN for video transport to and from DER.

```
vlan 924
name VLAN_924_Video_to/from_DER

interface Vlan924
 description Video transport VLAN to/from DER
 ip address 192.168.254.26 255.255.255.252 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Establishing 10-GE Interfaces for Transport on AR3

The 10-GE trunk interfaces provide the transport between AR3 and AR2 and DER.

The following is configured on AR3.

Step 1 Establish an interface. The first is to and from AR2.

a. Establish the interface, configure the trunk for 802.1q encapsulation, and assign it to VLANs 90, 816, and 916. (See Table 4-2 on page 4-5.)

```
interface TenGigabitEthernet1/49
 description Transport to/from AR2 (TenGig1/2)
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,816,916
 switchport mode trunk
 dampening
 load-interval 30
 carrier-delay msec 0
```

b. Configure this interface (and all noningress transport interfaces) to trust the incoming DSCP markings. (This maintains the DSCP marking applied at the network ingress interface.)

```
qos trust dscp
```

c. Set transmit-queue bandwidth thresholds and priority.

```
 tx-queue 1
   bandwidth percent 19
 tx-queue 2
   bandwidth percent 80
 tx-queue 3
   priority high
 tx-queue 4
   bandwidth percent 1
```

Step 2 Repeat Step 1 to establish an interface to and from DER assign it to VLANs 90, 824, and 924.

```
interface TenGigabitEthernet1/50
 description Transport to/from DER (TenGig7/3)
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,824,924
 switchport mode trunk
 dampening
 load-interval 30
 carrier-delay msec 0
```

Establishing 1-GE Interfaces to a DSLAM on AR3

The only 1-GE interface is a trunk to and from DSLAM3.

The following is configured on AR3.

Note For additional details, see Establishing 10-GE Interfaces for Transport on DER, page 4-16.

Step 1 Establish an interface to DSLAM1.

a. Establish the interface and assign it to VLANs 90, 130, and 131.

```
interface GigabitEthernet1/1
 description GigE trunk to/from DSLAM uplink GigE
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,130,131
 switchport mode trunk

 service-policy input setDSCP
 load-interval 30
```

b. Set transmit-queue bandwidth thresholds and priority.

```
 tx-queue 1
   bandwidth percent 19
 tx-queue 2
   bandwidth percent 80
 tx-queue 3
   priority high
 tx-queue 4
   bandwidth percent 1
```

c. Prevent unknown unicast traffic from being flooded to the port.

```
 switchport block unicast
```

Note Occasionally, unknown unicast or multicast traffic is flooded to a switch port because a MAC address has timed out or has not been learned by the switch. (This condition is especially undesirable for a private VLAN isolated port.) To guarantee that no unicast or multicast traffic is flooded to the port, use the **switchport block unicast** or **switchport block multicast** commands.

d. Disable Cisco Discovery Protocol (CDP) on the interface.

```
no cdp enable
```

e. Enable PortFast on the trunk interface to bypass the listening and learning states in Spanning Tree Protocol (STP). This allows the interface to move immediately from the blocking state to the forwarding state, rather than waiting for STP to converge.

```
spanning-tree portfast trunk
```

f. Configure the switch to disable any interface that is configured for PortFast and receives a Bridge Protocol Data Unit (BPDU).

```
spanning-tree bpduguard enable
```

Note This guards against a user accidentally connecting a switch to a switchport that is intended for a VoD server or other host. The switchport is disabled and the user must investigate why the port is down. If this command is not used and such an accidental connection were to happen, STP could reconverge and block other connections in the switch.

g. Apply the "setDSCP" service policy to mark DSCP values in the inbound IP packets.

```
service-policy input setDSCP
```

Configuring OSPF Routing for Video and Voice Traffic on AR3

For background and details, see Configuring OSPF Routing for Video and Voice Traffic on DER, page 4-19.

The following is configured on AR3.

Step 1 Define an OSPF routing process to route video traffic. This process associates the transport VLANs for video with the video aggregation VLAN for the DSLAM (VLAN 130).

```
router ospf 100
 router-id 4.4.4.1
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan130
 network 192.168.130.0 0.0.0.255 area 0
 network 192.168.254.18 0.0.0.0 area 0
 network 192.168.254.26 0.0.0.0 area 0
```

Step 2 Define an OSPF process to route voice traffic. This process associates the transport VLANs for VoIP with the VoIP aggregation VLAN for the DSLAM (VLAN 131).

```
router ospf 101
 router-id 4.4.4.2
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan131
 network 192.168.131.0 0.0.0.255 area 0
 network 192.168.252.18 0.0.0.0 area 0
 network 192.168.252.26 0.0.0.0 area 0
```

Configuring Spanning Tree on AR3

Note See Configuring Spanning Tree on DER, page 4-20.

The following is configured on AR3.

Step 1 Configure RTSP.

```
spanning-tree mode rapid-pvst
```

Step 2 Because the transport VLANs in the 10-GE ring are point-to-point networks, there is no risk of Layer 2 loops, so STP can be disabled on these VLANs.

```
no spanning-tree vlan 816, 824, 916, 924
```

Configuring the 1-GE Asymmetric Topology

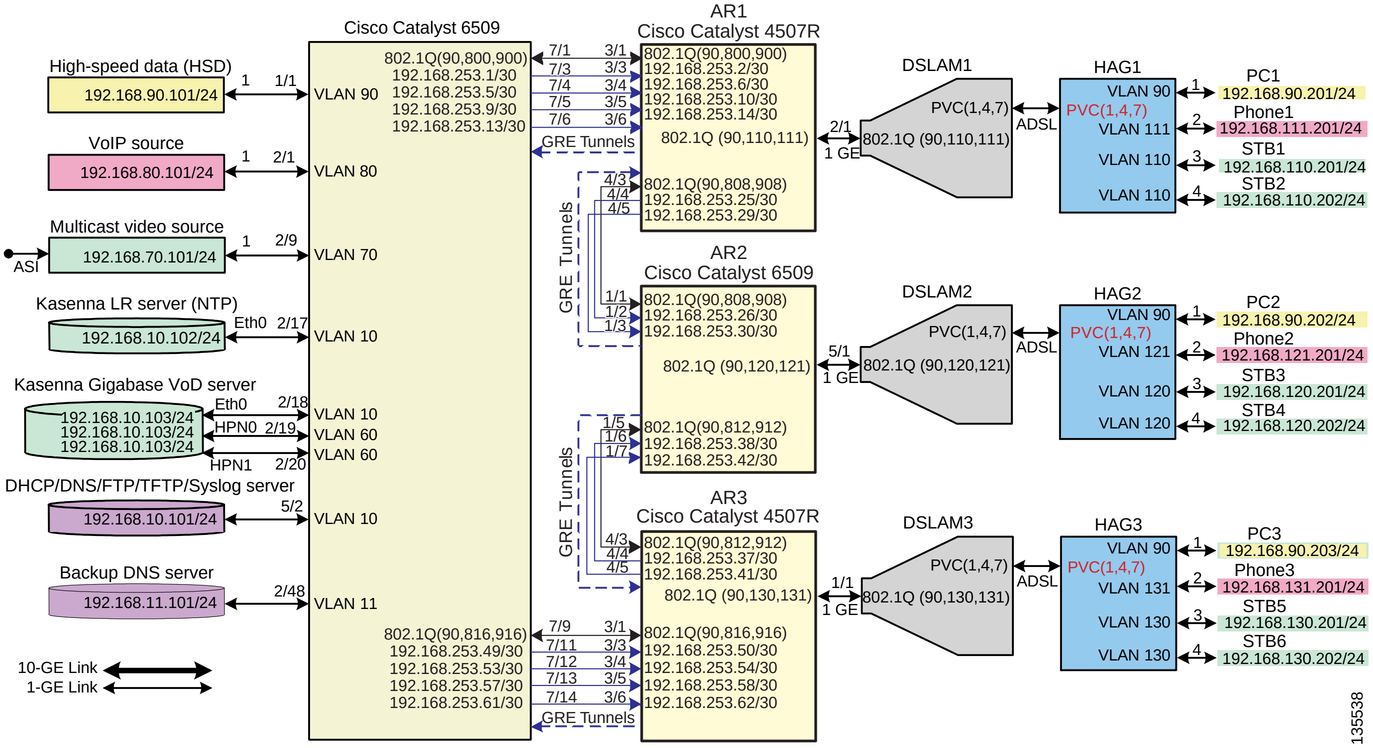
This section presents the following major topics:

- Introduction, page 4-53
- Configuring DER, page 4-57
- Configuring AR1, page 4-74
- Configuring AR2, page 4-89
- Configuring AR3, page 4-100

Introduction

Figure 4-2 illustrates the 1-GE symmetric topology used in the solution. (See Configuration 2: N x 1-GE Asymmetric Ring, page 3-34.) All video traffic sources are on DER. Policy maps are applied to the ingress ports on DER in order to mark the DSCP values of the different service types. Traffic is routed through 1-GE bidirectional links, configured as IEEE 802.1q trunks that carry three VLANs: one for video, one for VoIP, and one for high-speed data (HSD). VoD traffic is also routed through 1-GE unidirectional links that use GRE tunnels for bidirectional connectivity. Multiple OSPF processes are used for the routing protocol. One or two processes advertise routes for the video-related interfaces, and second advertises routes for the VoIP-related interfaces. HSD is carried around the ring on Layer 2.

Figure 4-2 1-GE Asymmetric Topology



The switches in Figure 4-2 use the line cards, hardware versions, and IOS versions listed in Table 4-1 on page 4-5.

Table 4-4 Hardware and IOS Versions for the 1-GE Asymmetric Topology

Switch	Module	Line Card	Hardware Version	IOS Release	Submodule	Hardware Version
DER	1	WS-X6724-SFP	2.0	12.2(18)SXE1	WS-F6700-DFC3BXL	4.0
	2	WS-X6748-GE-TX	1.4			
	5	WS-SUP720-BASE	3.0		WS-F6K-PFC3BXL	1.2
	7	WS-X6816-GBIC	1.7		WS-SUP720 (MFSC)	2.0
					WS-F6K-DFC3BXL	S2.2
AR1	1	WS-X4515	3.1	12.2(25)EWA	—	—
	2	WS-X4306-GB	2.2			
	3					
	5					
AR2	1	WS-X6816-GBIC	1.7	12.2(18)SXE1	WS-F6K-DFC3BXL	2.2
	2	WS-X6724-SFP	1.3		WS-F6700-DFC3BXL	4.0
	5	WS-SUP720-BASE	3.1		WS-F6K-PFC3BXL	1.2
					WS-SUP720 (MSFC)	2.1
AR3	1	WS-X4515	1.2	12.2(25)EWA	—	—
	3	WS-X4306-GB	2.2			
	4					
	5					

Table 4-5 lists VLANs, their descriptions (service types), and IP addresses, for the DER and ARs in Figure 4-1.

Table 4-6 on page 4-55 lists loopback addresses and endpoints for the topology, and describes the associated tunnels.

Table 4-5 VLANs, Descriptions, and IP Addresses for the 1-GE Asymmetric Topology

Node	VLAN	Description	IP Address
DER	10	Management (VoD signaling, DHCP, DNS, FTP, TFTP, Syslog servers)	192.168.10.1/24
	11	Management (backup DNS server)	192.168.11.1/24
	60	VoD server (unicast video aggregation)	192.168.60.1/24
	70	Broadcast video ingress (multicast video aggregation)	192.168.70.1/24
	80	VoIP ingress/egress	192.168.80.1/24
	90	HSD	Layer 2
	800	VoIP transport to/from AR1	192.168.252.1/30
	816	VoIP transport to/from AR3	192.168.252.17/30
	900	Video transport to/from AR1	192.168.254.1/30
	916	Video transport to/from AR3	192.168.254.17/30

Table 4-5 VLANs, Descriptions, and IP Addresses for the 1-GE Asymmetric Topology (continued)

Node	VLAN	Description	IP Address
AR1	90	HSD	Layer 2
	110	Video edge	192.168.110.1/24
	111	VoIP edge	192.168.111.1/24
	800	VoIP transport to/from DER	192.168.252.2/30
	808	VoIP transport to/from AR2	192.168.252.9/30
	900	Video transport to/from DER	192.168.254.2/30
	908	Video transport to/from AR2	192.168.254.9/30
AR2	90	HSD	Layer 2
	120	Video edge	192.168.120.1/24
	121	VoIP edge	192.168.121.1/24
	808	VoIP transport to/from AR1	192.168.252.10/30
	812	VoIP transport to/from AR3	192.168.252.13/30
	908	Video transport to/from AR1	192.168.254.10/30
	912	Video transport to/from AR3	192.168.254.13/30
AR3	90	HSD	Layer 2
	130	Video edge	192.168.130.1/24
	131	VoIP edge	192.168.131.1/24
	812	VoIP transport to/from AR2	192.168.252.14/30
	816	VoIP transport to/from DER	192.168.252.18/30
	912	Video transport to/from AR2	192.168.254.14/30
	916	Video transport to/from DER	192.168.254.18/30

Table 4-6 Loopback and Tunnel Descriptions and IP Addresses for the 1-GE Asymmetric Topology

Node	Loopback	Endpoint for Tunnel No.	Description	IP Address
DER	0	0	Rx side of Tx-only GigabitEthernet7/3	10.10.10.1/32
	4	4	Rx side of Tx-only GigabitEthernet7/4	10.10.10.5/32
	8	8	Rx side of Tx-only GigabitEthernet7/5	10.10.10.9/32
	12	12	Rx side of Tx-only GigabitEthernet7/6	10.10.10.13/32
	48	48	Rx side of Tx-only GigabitEthernet7/11	10.10.10.49/32
	52	52	Rx side of Tx-only GigabitEthernet7/12	10.10.10.53/32
	56	56	Rx side of Tx-only GigabitEthernet7/3	10.10.10.57/32
	60	60	Rx side of Tx-only GigabitEthernet7/14	10.10.10.61/32

Table 4-6 Loopback and Tunnel Descriptions and IP Addresses for the 1-GE Asymmetric Topology (continued)

Node	Loopback	Endpoint for Tunnel No.	Description	IP Address
AR1	0	0	Tx side of Rx-only GigabitEthernet3/3	10.10.10.2/32
	4	4	Tx side of Rx-only GigabitEthernet3/4	10.10.10.6/32
	8	8	Tx side of Rx-only GigabitEthernet3/5	10.10.10.10/32
	12	12	Tx side of Rx-only GigabitEthernet3/6	10.10.10.14/32
	24	24	Tx side of Rx-only GigabitEthernet4/4	10.10.10.25/32
	28	28	Tx side of Rx-only GigabitEthernet4/5	10.10.10.29/32
AR2	24	24	Tx side of Rx-only GigabitEthernet1/2	10.10.10.26/32
	28	28	Tx side of Rx-only GigabitEthernet1/3	10.10.10.30/32
	36	36	Tx side of Rx-only GigabitEthernet1/6	10.10.10.38/32
	40	40	Tx side of Rx-only GigabitEthernet1/7	10.10.10.42/32
AR3	36	36	Tx side of Rx-only GigabitEthernet4/4	10.10.10.37/32
	40	40	Tx side of Rx-only GigabitEthernet4/5	10.10.10.41/32
	48	48	Tx side of Rx-only GigabitEthernet3/3	10.10.10.45/32
	52	52	Tx side of Rx-only GigabitEthernet3/4	10.10.10.54/32
	56	56	Tx side of Rx-only GigabitEthernet3/5	10.10.10.58/32
	60	60	Tx side of Rx-only GigabitEthernet3/6	10.10.10.62/32

Table 4-3 on page 4-6 lists the parameters used to configure the home access gateway (HAG). They are the same as those for the 10-GE symmetric topology.

Note See HAG Functions, page 3-42.

Configuring DER

This section addresses the configuration required on the switch labeled DER in Figure 4-2 on page 4-53, to route multiple services from that switch to the ARs.

See Configuring DNS Servers, page 4-2.

Note A Cisco Catalyst 6509 can also be used, as it uses the same supervisor engine, line cards, and Cisco IOS code as the Cisco 7609 router.

This section addresses the following:

- Configuring QoS on DER
- Establishing and Configuring Interfaces on DER
- Configuring OSPF Routing for Video and Voice Traffic on DER
- Configuring Spanning Tree on DER

Note For a complete configuration example, see Appendix B, "Sample DER and AR Switch Configurations for the 1-GE Asymmetric Topology."

Configuring QoS on DER

This section presents the following topics:

- Overview of QoS on a Cisco 7600 Series and Cisco Catalyst 6500 Series
- Configuring Marking and Classification on DER
- Configuring Mapping on DER

Note For more information specific to QoS as applied to the solution, see Appendix C, "Understanding QoS as Implemented in the Solution."

Overview of QoS on a Cisco 7600 Series and Cisco Catalyst 6500 Series

This section addresses the configuration of quality of service (QoS) on the DER, through marking, classification, mapping, and queueing, to provide different degrees of quality of service for the different types of services supported by the solution architecture. For example, it is important to ensure the expeditious delivery of video and VoIP traffic, while providing only best-effort delivery for high-speed data (HSD).

By default, the Cisco 7600 series router and Cisco Catalyst 6500 series switch do not trust the incoming QoS markings, and therefore rewrite these bits with zeros. In this solution, packets at the network ingress ports are identified, classified, and marked according to type of traffic. The packets are marked with one of 64 possible Differentiated Services Code Point (DSCP) values at the ingress ports. These in turn are internally mapped to one of eight possible Class of Service (CoS) values, because CoS is used to determine the appropriate transmit queue for each packet. Queueing is configured on the individual 1-GE interfaces.

Note For more information on class of service, see “White Paper: Cisco IOS Software Features for Differentiated Class of Service for Internetworks,” at the following URL:

http://www.cisco.com/warp/public/cc/pd/iosw/iore/tech/osfea_wp.htm

Configuring Marking and Classification on DER

Do the following to enable marking and classification on DER.

Step 1 Enable QoS in global configuration mode.

```
mls qos
```

Step 2 Create access lists to identify the different service types in the network.

```
ip access-list extended acl_HSD
 permit ip 192.168.90.0 0.0.0.255 any
ip access-list extended acl_VoD_signaling
 remark Identify VoD signaling traffic
 permit ip host 192.168.10.102 any
 permit ip host 192.168.10.103 any
ip access-list extended acl_VoIP
 remark Identify VoIP traffic
 permit ip 192.168.80.0 0.0.0.255 any
ip access-list extended acl_video_VoD_high
 remark Identify high priority VoD traffic
 permit udp 192.168.60.0 0.0.0.255 192.168.110.0 0.0.0.255 range 5000 9000
 permit udp 192.168.60.0 0.0.0.255 192.168.120.0 0.0.0.255 range 5000 9000
 permit udp 192.168.60.0 0.0.0.255 192.168.130.0 0.0.0.255 range 5000 9000
ip access-list extended acl_video_VoD_low
 remark Identify low priority VoD traffic
 permit udp 192.168.60.0 0.0.0.255 192.168.110.0 0.0.0.255 range 1000 4999
 permit udp 192.168.60.0 0.0.0.255 192.168.120.0 0.0.0.255 range 1000 4999
 permit udp 192.168.60.0 0.0.0.255 192.168.130.0 0.0.0.255 range 1000 4999
ip access-list extended acl_video_broadcast
 remark Identify broadcast video traffic (multicast)
 permit ip 192.168.70.0 0.0.0.255 232.0.0.0 0.255.255.255
```

Step 3 Create class maps for the access lists created in Step 2.

```
class-map match-all class_VoIP
match access-group name acl_VoIP
class-map match-all class_video_VoD_high
match access-group name acl_video_VoD_high
class-map match-all class_video_VoD_low
match access-group name acl_video_VoD_low
class-map match-all class_video_broadcast
match access-group name acl_video_broadcast
class-map match-all class_VoD_signaling
match access-group name acl_VoD_signaling
class-map match-all class_HSD
match access-group name acl_HSD
```

Step 4 Create a policy map to set the DSCP values of the different classes created in Step 3.

```
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoIP
   set dscp ef
  class class_HSD
   set dscp default
  class class_VoD_signaling
   set dscp cs3
  class class_video_broadcast
   set dscp af41
  class class_video_VoD_high
   set dscp af42
  class class_video_VoD_low
   set dscp af43
```

Step 5 Apply the policy map from Step 4 to the ingress interfaces using the following command.

```
service-policy input setDSCP
```

Note Specific interface examples of this and other interface commands are shown in the interface provisioning sections.

Step 6 To maintain the DSCP marking applied at the network ingress interface, configure all noningress transport interfaces to trust the incoming DSCP markings.

```
mls qos trust dscp
```

Configuring Mapping on DER

Do the following to configure mapping on DER.

Step 1 View the Cisco 7600/Catalyst 6500 default DSCP-to-CoS mapping for the different services. Use the **show mls qos maps dscp-cos** command.

Note At the beginning of this section, we mentioned that there are 64 possible DSCP values and only 8 CoS values. This means that there could be more than one DSCP value for one CoS value. The following command shows the default DSCP-to-CoS mapping on the Cisco 7600 and Catalyst 6500.

Note In the map, d1 corresponds to the *y*-axis value of the table, and d2 to the *x*-axis value.

```
DER# 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
```

This table shows the following mappings:

Service Type	DSCP	CoS
HSD	0	0
VoD low priority	34	4
VoD high priority	36	4
VoD OOB	24	3
Broadcast video	38	4
VoIP	46	5

Step 2 Change the Cisco 7600/Catalyst 6500 DSCP-to-CoS mapping for the different services to match the specifications of the solution.

The solution specifies the following DSCP-to CoS-mappings:

Service Type	DSCP	CoS
HSD	0	0
VoD low priority	38	1
VoD high priority	36	2
VoD OOB	24	3
Broadcast video	34	4
VoIP	46	5

a. Execute the following command on the Cisco 7600 and Cisco Catalyst 6500 to modify the DSCP-to-CoS mapping.

```
mls qos map dscp-cos 36 to 2
mls qos map dscp-cos 38 to 1
```

b. Verify the changes to the DSCP-to-CoS mappings.

```
DER# show mls qos maps dscp-cos
DSCP-CoS Mapping Table (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 02 04 01 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
```

Establishing and Configuring Interfaces on DER

Refer to Figure 4-2 on page 4-53.

This section addresses the following:

- Establishing VLANs for Services on DER
- Establishing Interfaces for Servers, HSD, and Management on DER
- Establishing Bidirectional and Unidirectional Interfaces for Transport on DER
- Establishing Tunnels on DER

Establishing VLANs for Services on DER

Before the 1-GE interfaces can be configured, VLANs for the various services must be created. With the exception of VLAN 90 (high-speed data), these are all Layer 3 VLANs. (Refer to Table 4-5 on page 4-54.)

The following is configured on DER.

Tip For convenience in establish these VLANs and others, you can establish all VLANs in global configuration mode first, then configure all the interfaces in interface configuration mode.

Step 1 Establish a VLAN and VLAN interface for management (including VoD signaling, connectivity with DHCP, DNS, FTP, TFTP, and Syslog servers.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 10
name VLAN_10_Management
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan10
 description Management VLAN (VoD signaling, DNS, DHCP, etc)
 ip address 192.168.10.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

c. Change the load interval from the default of 300.

```
 load-interval 30
```

d. Repeat Step 1a through Step 1c, as appropriate, for the remaining management, unicast video, and and VoIP VLANs. Abbreviated configurations are shown below.

Backup DNS server

```
vlan 11
name VLAN_11_Management


interface Vlan11
 description Management VLAN (Backup DNS)
 ip address 192.168.11.1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

Unicast video aggregation

```
vlan 60
name VLAN_60_Unicast_Video


interface Vlan60
 description VoD server VLAN (Unicast Video)
 ip address 192.168.60.1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

VoIP

```
vlan 80
name VLAN_80_VoIP


interface Vlan80
 description VoIP ingress/egress VLAN
 ip address 192.168.80.1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

Step 2 Establish a VLAN for multicast video aggregation.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 70
name VLAN_70_Multicast_Video
```

b. In interface configuration mode, create and configure the VLAN interfaces.

```
interface Vlan70
 description Broadcast video source VLAN (Multicast Video)
 ip address 192.168.70.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

c. Enable PIM sparse mode. This is the ingress port for broadcast video traffic, which is multicast addressed.

```
 ip pim sparse-mode
```

d. Change the load interval from the default of 300.

```
 load-interval 30
```

Step 3 In global configuration mode, establish a Layer 2 VLAN for high-speed data (HSD). (No Layer 3 interface is required.)

```
vlan 90
name VLAN_90_HSD
```

Step 4 Establish VLANs for VoIP transport. The first is for transport to and from AR1.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 800
name VLAN_800_VoIP_to/from_AR1
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan800
 description VoIP transport to/from AR1
 ip address 192.168.252.1 255.255.255.252
```

c. Configure OSPF on the transport VLAN interface.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

Note To avoid the election of the (designated router (DR) and backup designated router (BDR), and prevent the origination of an unnecessary network link state advertisement (LSA), configure the transport VLAN as a point-to-point network. In addition, reduce the interval between OSPF hello messages from 10 seconds to 1 second. This improves reconvergence in the event of failure in the transport or in a neighboring switch.

d. Change the load interval from the default of 300.

```
 load-interval 30
```

e. Repeat Step 4a through Step 4d for VoIP transport to and from AR3.

```
vlan 816
name VoIP transport to/from AR3


interface Vlan816
 description VoIP transport to/from AR3
 ip address 192.168.252.17 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Step 5 Establish VLANs for video transport. The first is for transport to and from AR1.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 900
name VLAN_900_Video_to/from_AR1
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan900
 description Video transport VLAN to/from AR1
 ip address 192.168.254.1 255.255.255.252
```

c. Enable PIM sparse mode. This is the ingress port for broadcast video traffic, which is multicast addressed.

```
 ip pim sparse-mode
```

d. Configure OSPF on the transport VLAN interface.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

e. Change the load interval from the default of 300.

```
 load-interval 30
```

f. Repeat Step 5a through Step 5b to establish a VLAN for video transport to and from AR3.

```
vlan 916
name Video_transport_to/from_AR3


interface Vlan916
 description Video transport VLAN to/from AR3
 ip address 192.168.254.17 255.255.255.252
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Establishing Interfaces for Servers, HSD, and Management on DER

VoD servers, high-speed data sources, and management resources connect to Layer 2 interfaces on DER, and their traffic is aggregated into the appropriate service VLANs.

The following is configured on DER.

Step 1 Establish an interface.

a. Establish an interface for high-speed data and assign it to VLAN 90.

```
interface GigabitEthernet1/1
 description High speed data ingress/egress port
 no ip address
```

b. Configure the interface as a Layer 2 access port.

```
 switchport
 switchport access vlan 90
 switchport mode access
```

c. Change the load interval from the default of 300.

```
load-interval 30
```

d. Disable Cisco Discovery Protocol (CDP) on the interface.

```
no cdp enable
```

e. Enable PortFast on the interface to bypass the listening and learning states in Spanning Tree Protocol (STP). This allows the interface to move immediately from the blocking state to the forwarding state, rather than waiting for STP to converge.

```
spanning-tree portfast
```

f. Configure the switch to disable any interface that is configured for PortFast and receives a Bridge Protocol Data Unit (BPDU).

```
spanning-tree bpduguard enable
```

Note This guards against a user accidentally connecting a switch to a switchport that is intended for a VoD server or other host. The switchport is disabled and the user must investigate why the port is down. If this command is not used and such an accidental connection were to happen, STP could reconverge and block other connections in the switch.

g. Apply the “setDSCP” service policy to mark DSCP values in the inbound IP packets.

```
service-policy input setDSCP
```

Step 2 Repeat Step 1a through Step 1g for the remaining server, HSD, and management interfaces and their associated VLANs, changing the value in **switchport access vlan** *xxx* as appropriate. The abbreviated configurations are shown below.

VoIP traffic

```
interface GigabitEthernet2/1
 description VoIP traffic ingress/egress port

 switchport access vlan 80
```

Ingress multicast broadcast video

```
interface GigabitEthernet2/9
 description Broadcast video source (multicast 232.1.1.1 - 232.1.1.10)

 switchport access vlan 70
```

Management for the Kasenna LR server

```
interface GigabitEthernet2/17
 description Management port from Kasenna LR Server (Eth0)

 switchport access vlan 10
```

Management for the Kasenna VoD pump

```
interface GigabitEthernet2/18
 description Kasenna VoD Pump Management

 switchport access vlan 10
```

Ingress unicast video from the Kasenna VoD pump (1)

```
interface GigabitEthernet2/19
 description Unicast video from Kasenna VoD Pump (HPN0)

 switchport access vlan 60
```

Note In Kasenna’s terminology, HPN0 stands for High-Performance Network interface 0.

Ingress unicast video from the Kasenna VoD pump (2)

```
interface GigabitEthernet2/20
 description Unicast video from Kasenna VoD Pump (HPN1)

 switchport access vlan 60
```

Backup DNS server

```
interface GigabitEthernet2/48
 description Backup DNS server

 switchport access vlan 11
```

Primary DNS, DHCP, NTP, TFTP, and Syslog servers

```
interface GigabitEthernet5/2
 description Primary DNS/DHCP/NTP/TFTP/Syslog servers

 switchport access vlan 10
```

Note In this case, specify the physical connection on a Gigabit Ethernet interface as RJ-45.

```
media-type rj45
```

Establishing Bidirectional and Unidirectional Interfaces for Transport on DER

The 1-GE interfaces create the ring topology from the DER through the ARs and back to the DER. Both bidirectional and unidirectional trunking interfaces and VoD unidirectional transport are established.

The following is configured on DER.

Step 1 Establish bidirectional transport interfaces.

a. Establish a bidirectional transport interface to and from AR1.

```
interface GigabitEthernet7/1
 description Transport to/from AR1 (Gig3/1)
 switchport

 switchport mode trunk
 dampening
 no ip address

 carrier-delay msec 0
```

b. Configure the trunk for 802.1q encapsulation.

```
 switchport trunk encapsulation dot1q
```

c. Assign the trunk to VLANs 90, 800, and 900. (See Table 4-5 on page 4-54.)

```
 switchport trunk allowed vlan 90,800,900
```

d. Change the load interval from the default of 300.

```
 load-interval 30
```

Step 2 Configure QoS on the interface.

Note The 1-GE transport links from the DER to the ARs require modifications to the transmit queues. There are eight transmit queues, but this solution uses only three.

a. View the default CoS to Tx-Queue mapping. The following information was extracted from the **show queueing interface** command.

TxQueue	CoS
1	0, 1
2	2, 3, 4
3	6, 7
4	—
5	—
6	—
7	—
8	5

b. Configure the CoS-to TxQueue mapping on the transport interfaces. HSD (CoS = 0) remains in TxQueue1 and VoIP (CoS = 5) remains in TxQueue8. The other six CoS values are associated with TxQueue2.

```
wrr-queue cos-map 1 1 0
wrr-queue cos-map 2 1 1
wrr-queue cos-map 2 2 2 3 4 6 7
```

Note TxQueue1 and TxQueue8 use the default mappings. TxQueue2 has three thresholds: Threshold 1 = CoS 1, Threshold 2 = CoS 2, and Threshold 3 = CoS 3, 4, 6, and 7. For details, see Appendix C, “Understanding QoS as Implemented in the Solution.”

c. Verify the modified CoS-to-Tx-Queue mapping. The following information was extracted from the **show queueing interface** command.

TxQueue	CoS
1	0
2	1, 2, 3, 4, 6, 7
3	—
4	—
5	—
6	—
7	—
8	5

d. Configure the TxQueue thresholds.

TxQueue1 uses Weighted Random Early Drop (WRED) for queue-congestion management. Only HSD is queued in this queue, and when the amount of HSD in the queue reaches 75%, random packets are dropped in an attempt to keep the queue from reaching 100% utilization.

```
wrr-queue random-detect min-threshold 1 75 100
wrr-queue random-detect max-threshold 1 100 100
```

TxQueue2 uses tail drop for queue congestion management. Low-priority VoD is assigned to the first threshold and is dropped once the queue reaches 50% utilization. High-priority VoD is assigned to the second threshold and is dropped once the queue reaches 85% utilization. VoD signaling, network signaling, and broadcast video are assigned to the third threshold and is dropped once the queue reaches 100% utilization.

```
wrr-queue random-detect min-threshold 2 50 100
wrr-queue random-detect max-threshold 2 50 100
```

e. Configure the bandwidth of the weighted queues.

The weighted queues need to be modified to handle our modified TxQueue mappings. The ratio between TxQueue2 and TxQueue1 is 255/64 = 4, so TxQueue2 needs four times as much bandwidth as TxQueue1. Therefore, TxQueue1 is allocated 20% of the bandwidth on the interface, and TxQueue2 is allocated 80% of the bandwidth.

```
wrr-queue bandwidth 64 255
```

f. Configure the size of the weighted queues.

Each line card has a limited amount of buffer for the transmit queues. For this interface, 40% of the buffer is allocated for TxQueue1, and 50% of the buffer is allocated for TxQueue2.

```
wrr-queue queue-limit 40 50
```

g. Configure this interface (and all noningress transport interfaces) to trust the incoming DSCP markings. (This maintains the DSCP marking applied at the network ingress interface.)

```
mls qos trust dscp
```

Step 3 Repeat Step 1 and Step 2, as appropriate, for the bidirectional transport to and from AR3.

```
interface GigabitEthernet7/9
 description Transport to/from AR3 (Gig3/1)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,816,916
 switchport mode trunk
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255
 wrr-queue queue-limit 40 50
 wrr-queue random-detect min-threshold 1 75 100
 wrr-queue random-detect min-threshold 2 50 100
 wrr-queue random-detect max-threshold 1 100 100
 wrr-queue random-detect max-threshold 2 50 100
 wrr-queue cos-map 1 1 0
 wrr-queue cos-map 2 1 1
 wrr-queue cos-map 2 2 2 3 4 6 7
 mls qos trust dscp
```

Step 4 Establish unidirectional VoD transport interfaces.

a. Establish the unidirectional VoD transport interface to AR1 and assign the IP address.

```
interface GigabitEthernet7/3
 description VoD transport to AR1 (Gig3/3)
 dampening
 ip address 192.168.253.1 255.255.255.252
```

b. Configure OSPF on the transport VLAN interface.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

c. Change the load interval from the default of 300.

```
 load-interval 30
```

d. Disable the link-negotiation protocol on the port.

```
 speed nonegotiate
```

e. Mark the interface as send only.

```
 unidirectional send-only
```

f. Repeat Step 4a through Step 4e, as appropriate, for the remaining unidirectional VoD transport interfaces. Abbreviated interface configurations are shown below.

Second VoD transport interface to AR1

```
interface GigabitEthernet7/4
 description VoD transport to AR1 (Gig3/4)

 ip address 192.168.253.5 255.255.255.252
```

Third VoD transport interface to AR1

```
interface GigabitEthernet7/5
 description VoD transport to AR1 (Gig3/5)

 ip address 192.168.253.9 255.255.255.252
```

Fourth VoD interface to AR1

```
interface GigabitEthernet7/6
 description VoD transport to AR1 (Gig3/6)

 ip address 192.168.253.13 255.255.255.252
```

First VoD interface to AR3

```
interface GigabitEthernet7/11
 description VoD transport to AR1 (Gig3/3)

 ip address 192.168.253.49 255.255.255.252
```

Second VoD interface to AR3

```
interface GigabitEthernet7/12
 description VoD transport to AR1 (Gig3/4)

 ip address 192.168.253.53 255.255.255.252
```

Third VoD interface to AR3

```
interface GigabitEthernet7/13
 description VoD transport to AR1 (Gig3/5)

 ip address 192.168.253.57 255.255.255.252
```

Fourth VoD interface to AR3

```
interface GigabitEthernet7/14
 description VoD transport to AR1 (Gig3/6)

 ip address 192.168.253.61 255.255.255.252
```

Establishing Tunnels on DER

The following is configured on DER.

Step 1 Create a loopback interface to serve as the tunnel endpoint for the first tunnel and assign an IP address.

```
interface Loopback0
 description Endpoint for Tunnel0
 ip address 10.10.10.1 255.255.255.255
```

Step 2 Create the interface for the corresponding tunnel. No IP address is required for the tunnel itself.

```
interface Tunnel0
 description Rx-side of Tx-only Gig7/3
 no ip address
```

Step 3 Configure the source and destination endpoints of the tunnel and assign IP addresses.

```
 tunnel source 10.10.10.1
 tunnel destination 10.10.10.2
```

Step 4 Configure UDLR for the tunnel and mark it as receive only.

```
 tunnel udlr receive-only GigabitEthernet7/3
```

Step 5 Refer to Table 4-7 and repeat Steps 1 through Step 4 for the remaining tunnels on DER, making modifications as appropriate.

Table 4-7 Additional Corresponding Loopback and Tunnel Interfaces for DER

Loopback Interface	Tunnel Interface
interface Loopback4 description Endpoint for Tunnel4 ip address 10.10.10.5 255.255.255.255	interface Tunnel4 description Rx-side of Tx-only Gig7/4 no ip address tunnel source 10.10.10.5 tunnel destination 10.10.10.6 tunnel udlr receive-only GigabitEthernet7/4
interface Loopback8 description Endpoint for Tunnel8 ip address 10.10.10.9 255.255.255.255	interface Tunnel8 description Rx-side of Tx-only Gig7/5 no ip address tunnel source 10.10.10.9 tunnel destination 10.10.10.10 tunnel udlr receive-only GigabitEthernet7/5
interface Loopback12 description Endpoint for Tunnel12 ip address 10.10.10.13 255.255.255.255	interface Tunnel12 description Rx-side of Tx-only Gig7/6 no ip address tunnel source 10.10.10.13 tunnel destination 10.10.10.14 tunnel udlr receive-only GigabitEthernet7/6

Table 4-7 Additional Corresponding Loopback and Tunnel Interfaces for DER (continued)

Loopback Interface	Tunnel Interface
interface Loopback48 description Endpoint for Tunnel48 ip address 10.10.10.49 255.255.255.255	interface Tunnel48 description Rx-side of Tx-only Gig7/11 no ip address tunnel source 10.10.10.49 tunnel destination 10.10.10.50 tunnel udlr receive-only GigabitEthernet7/11
interface Loopback52 description Endpoint for Tunnel52 ip address 10.10.10.53 255.255.255.255	interface Tunnel52 description Rx-side of Tx-only Gig7/12 no ip address tunnel source 10.10.10.53 tunnel destination 10.10.10.54 tunnel udlr receive-only GigabitEthernet7/12
interface Loopback56 description Endpoint for Tunnel56 ip address 10.10.10.57 255.255.255.255	interface Tunnel56 description Rx-side of Tx-only Gig7/13 no ip address tunnel source 10.10.10.57 tunnel destination 10.10.10.58 tunnel udlr receive-only GigabitEthernet7/13
interface Loopback60 description Endpoint for Tunnel60 ip address 10.10.10.61 255.255.255.255	interface Tunnel60 description Rx-side of Tx-only Gig7/14 no ip address tunnel source 10.10.10.61 tunnel destination 10.10.10.62 tunnel udlr receive-only GigabitEthernet7/14

Configuring OSPF Routing for Video and Voice Traffic on DER

There are a number of ways to configure the routing of the multiple services across the 1-GE asymmetric topology. HSD, VoIP, broadcast video, and VoD signaling can be routed across the bidirectional links, while VoD traffic can be routed across both the bidirectional and unidirectional links, or just across the unidirectional links.

In this example, HSD, VoIP, broadcast video, and VoD signaling are routed across the bidirectional links. To accomplish this, the bidirectional link is a trunk that carries three VLANs (90, 8*xx*, and 9*xx*). Because VLAN 90 is at Layer 2 around the network, there is no OSPF configuration for HSD. VoIP-related interfaces are advertised across the 8*xx* VLANs. Broadcast video is multicast, so the path is built from the receiver to the source. Because the DER does not need to know how to route to the destination for broadcast video, we only need to advertise the broadcast video sources across the 9*xx* VLANs, so that the receivers can build the reverse path back to the broadcast video source. VoD signaling is lower-bitrate, bidirectional traffic, but we still want this traffic to travel across the bidirectional transport links, rather than through the GRE tunnels associated with the unidirectional transport links. To accomplish this, we advertise the VoD server-related interfaces across the 9*xx* VLANs. In addition, the loopback interfaces that serve as the endpoints of the GRE tunnels for the unidirectional links are also advertised on the 9*xx* VLANs.

Finally, in this example the VoD traffic is routed across the unidirectional transport links only. VoD traffic is routed from the source to the receivers, so the DER must know how to route to the receivers. To accomplish this, no interfaces need to be advertised from the DER, but the DER needs a routing process associated with the unidirectional transport links to receive routing advertisements for the video aggregation VLANs on the ARs.

Three Open Shortest Path First (OSPF) routing processes must be established:

- OSPF 100—to route the management, broadcast video, and loopbacks over the transport VLANs for video
- OSPF 101—to route VoIP traffic over the transport VLANs for VoIP
- OSPF 102—to route VoD traffic over the unidirectional Layer 3 transport network for VoD

Routing advertisements are enabled on the transport VoD network, but are turned off on the aggregation VLANs by means of the **passive-interface** command.

The following is configured on DER.

Step 1 Define an OSPF routing process to route video traffic.

```
router ospf 100
 router-id 1.1.1.1
 log-adjacency-changes
```

a. The OSPF timers are modified to provide fast convergence. The following command enables OSPF SPF throttling: **timers throttle spf** *spf-start spf-hold spf-max-wait*

```
timers throttle spf 10 100 1000
```

b. The following command sets the rate-limiting values for OSPF link-state advertisement (LSA) generation: **timers throttle lsa all** *start-interval hold-interval max-interval*

```
timers throttle lsa all 1 10 1000
```

c. The following command controls the minimum interval for accepting the same LSA: **timers lsa arrival** *milliseconds*

```
timers lsa arrival 100
```

If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped.

d. Apply the **passive-interface** command to the aggregation VLANs.

```
passive-interface Vlan10
passive-interface Vlan11
passive-interface Vlan60
passive-interface Vlan70
```

e. Advertise the networks in the first OSPF routing process.

```
network 10.10.10.0 0.0.0.255 area 0
network 192.168.10.0 0.0.1.255 area 0
network 192.168.60.0 0.0.0.255 area 0
network 192.168.70.0 0.0.0.255 area 0
network 192.168.254.0 0.0.0.255 area 0
```

Step 2 Repeat Step 1, as appropriate, to define a second OSPF process to route VoIP traffic.

```
router ospf 101
 router-id 1.1.1.2
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan80
 network 192.168.80.0 0.0.0.255 area 0
 network 192.168.252.0 0.0.0.255 area 0
 maximum-paths 8
```

Step 3 Define a third OSPF process to route VoD transport traffic.

```
router ospf 102
 router-id 1.1.1.3
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 network 192.168.253.0 0.0.0.255 area 0
 maximum-paths 8
```

Configuring Spanning Tree on DER

Because VLAN 90 is at Layer 2 around the 1-GE ring, Spanning Tree Protocol (STP) is needed to guard against loops. To improve convergence time, the four switches are configured for IEEE 802.1w Rapid Spanning Tree Protocol (RTSP), with the root at DER.

Do the following in global configuration mode to configure spanning tree parameters on DER.

Step 1 Configure DER as the root node of the spanning tree for VLAN 90. There are two ways to do this.

a. Use the **root primary** option.

```
spanning-tree vlan 90 root primary
```

or

b. Set the priority to 24576.

```
spanning-tree vlan 90 priority 24576
```

Step 2 Configure RTSP.

```
spanning-tree mode rapid-pvst
```

Step 3 Because the transport VLANs in the ring are point-to-point networks, there is no risk of Layer 2 loops, so STP can be disabled on these VLANs.

```
no spanning-tree vlan 800, 816, 900, 916
```

Configuring AR1

This section addresses the configuration required on the switch labeled AR1 in Figure 4-2 on page 4-53, to route multiple services from AR1 to DER and AR2.

See Configuring DNS Servers, page 4-2.

This section addresses the following:

- Configuring QoS on AR1
- Establishing and Configuring Interfaces on AR1
- Configuring OSPF Routing for Video and Voice Traffic on AR1
- Configuring Spanning Tree on AR1

Note For a complete configuration example, see Appendix B, "Sample DER and AR Switch Configurations for the 1-GE Asymmetric Topology."

Configuring QoS on AR1

See Overview of QoS on a Cisco 7600 Series and Cisco Catalyst 6500 Series, page 4-57.

This section presents the following topics:

- Overview of QoS on a Cisco Catalyst 4500 Series, page 4-74
- Configuring Marking and Classification on AR1
- Configuring Mapping on AR1
- Configuring Queueing on AR1

Note For more information specific to QoS as applied to the solution, see Appendix C, "Understanding QoS as Implemented in the Solution."

Overview of QoS on a Cisco Catalyst 4500 Series

This section addresses the configuration of quality of service (QoS) on AR2, through marking, classification, mapping, and queueing, to provide different degrees of quality of service for the different types of services supported by the solution architecture. For example, it is important to ensure the expeditious delivery of video and VoIP traffic, while providing only best-effort delivery for high-speed data (HSD).

By default, the Cisco Catalyst 4500 series switches (including the Cisco Catalyst 4948-10GE) do not trust the incoming QoS markings, and therefore rewrite these bits with zeros. In this solution, packets at the network ingress ports are identified, classified, and marked according to type of traffic. The packets are marked with one of 64 possible Differentiated Services Code Point (DSCP) values at the ingress ports. These in turn are internally mapped to one of eight possible Class of Service (CoS) values. The DSCP values are used to determine the appropriate transmit queue for each packet.

Configuring Marking and Classification on AR1

Do the following to enable marking and classification on AR1.

Step 1 Enable QoS in global configuration mode.

```
qos
```

Step 2 Create access lists to identify the different service types in the network.

```
ip access-list extended acl_HSD
 remark Identify HSD traffic
 permit ip 192.168.90.0 0.0.0.255 any
ip access-list extended acl_VoD_signaling
 remark Identify VoD signaling traffic
 permit ip 192.168.110.0 0.0.0.255 192.168.10.102
 permit ip 192.168.110.0 0.0.0.255 192.168.10.103
ip access-list extended acl_VoIP
 remark Identify VoIP traffic
 permit ip 192.168.111.0 0.0.0.255 any
```

Step 3 Create class maps for the access lists created in Step 2.

```
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_VoD_signaling
  match access-group name acl_VoD_signaling
class-map match-all class_HSD
  match access-group name acl_HSD
```

Step 4 Create a policy map to set the DSCP values of the different classes created in Step 3.

```
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoIP
   set dscp ef
  class class_HSD
   set dscp default
  class class_VoD_signaling
   set dscp cs3
```

Step 5 Apply the policy map from Step 4 to the ingress interfaces using the following command.

```
service-policy input setDSCP
```

Note Specific interface examples of this and other interface commands are shown in the interface provisioning sections.

Step 6 To maintain the DSCP marking applied at the network ingress interface, configure all noningress transport interfaces to trust the incoming DSCP markings.

```
qos trust dscp
```

Configuring Mapping on AR1

Do the following to configure mapping on AR1.

Step 1 View the Cisco Catalyst 4500 series default DSCP-to-CoS mapping for the different services. Use the **show qos maps dscp-cos** command.

Note At the beginning of this section, we mentioned that there are 64 possible DSCP values and only 8 CoS values. This means that there could be more than one DSCP value for one CoS value. The following command shows the default DSCP-to-CoS mapping on the Cisco Catalyst 4500 series.

Note In the map, d1 corresponds to the *y*-axis value of the table, and d2 to the *x*-axis value.

```
AR2# show qos maps dscp

DSCP-CoS Mapping Table (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
```

This table shows the following mappings:

Service Type	DSCP	CoS
HSD	0	0
VoD low priority	34	4
VoD high priority	36	4
VoD OOB	24	3
Broadcast video	38	4
VoIP	46	5

Step 2 Change the Cisco Catalyst 4500 series DSCP-to-CoS mapping for the different services to match the specifications of the solution.

The solution specifies the following DSCP-to CoS-mappings:

Service Type	DSCP	CoS
HSD	0	0
VoD low priority	38	1
VoD high priority	36	2
VoD OOB	24	3
Broadcast video	34	4
VoIP	46	5

a. Execute the following command on the Cisco Catalyst 4500 series to modify the DSCP-to-CoS mapping.

```
qos map dscp 38 to cos 1
qos map dscp 36 to cos 2
```

b. Verify the changes to the DSCP-to-CoS mappings.

```
AR2# show qos maps dscp

DSCP-CoS Mapping Table (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 02 04 01 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
```

Configuring Queueing on AR1

Unlike the Cisco 7600 series and Cisco Catalyst 6500 series, the Cisco Catalyst 4500 series uses the same queueing on all interfaces. Queueing is configured globally.

Do the following to change the DSCP-to-TxQueue mappings on AR1.

Step 1 View the default DSCP-to-Tx-Queue mapping. The following information was extracted from the **show qos maps dscp** command.

```
DSCP-TxQueue Mapping Table (dscp = d1d2)
d1 : d2  0  1  2  3  4  5  6  7  8  9
-------------------------------------
 0 :    01 01 01 01 01 01 01 01 01 01
 1 :    01 01 01 01 01 01 02 02 02 02
 2 :    02 02 02 02 02 02 02 02 02 02
 3 :    02 02 03 03 03 03 03 03 03 03
 4 :    03 03 03 03 03 03 03 03 04 04
 5 :    04 04 04 04 04 04 04 04 04 04
 6 :    04 04 04 04
```

Step 2 Configure the DSCP-to-TxQueue mapping by moving DSCP 34, 36, and 38 to TxQueue2. Additionally, move all DSCPs that are in TxQueue4 to TxQueue2, because TxQueue4 is not used.

```
qos map dscp 34 36 38 48 49 50 51 52 to tx-queue 2
qos map dscp 53 54 55 56 57 58 59 60 to tx-queue 2
qos map dscp 61 62 63 to tx-queue 2
```

Step 3 Verify the modified DSCP-to-Tx-Queue mapping. The following information was extracted from the **show queueing interface** command.

```
DSCP-TxQueue Mapping Table (dscp = d1d2)
d1 : d2  0  1  2  3  4  5  6  7  8  9
-------------------------------------
 0 :    01 01 01 01 01 01 01 01 01 01
 1 :    01 01 01 01 01 01 02 02 02 02
 2 :    02 02 02 02 02 02 02 02 02 02
 3 :    02 02 03 03 02 03 02 03 02 03
 4 :    03 03 03 03 03 03 03 03 02 02
 5 :    02 02 02 02 02 02 02 02 02 02
 6 :    02 02 02 02
```

Step 4 Configure the TxQueue thresholds.

TxQueue1 uses Weighted Random Early Drop (WRED) for queue-congestion management. Only HSD is queued in this queue, and when the amount of HSD in the queue reaches 75%, random packets are dropped in an attempt to keep the queue from reaching 100% utilization.

```
wrr-queue threshold 1 100 100 100 100 100 100 100 100
wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
```

TxQueue2 uses tail drop for queue congestion management. Low-priority VoD is assigned to the first threshold and is dropped once the queue reaches 45% utilization. High-priority VoD is assigned to the second threshold and is dropped once the queue reaches 85% utilization. VoD signaling, network signaling, and broadcast video are assigned to the third threshold and is dropped once the queue reaches 100% utilization.

```
wrr-queue threshold 2 45 85 100 100 100 100 100 100
no wrr-queue random-detect 2
```

Step 5 Configure the bandwidth of the weighted queues.

The weighted queues need to be modified to handle our modified TxQueue mappings. The ratio between TxQueue2 and TxQueue1 is 255/64 = 4, so TxQueue2 needs four times as much bandwidth as TxQueue1. Therefore, TxQueue1 is allocated 20% of the bandwidth on the interface, and TxQueue2 is allocated 80% of the bandwidth.

```
wrr-queue bandwidth 64 255 0 0 0 0 0
```

Step 6 Configure the size of the weighted queues.

Each line card has a limited amount of buffer for the transmit queues. For this interface, 40% of the buffer is allocated for TxQueue1, and 50% of the buffer is allocated for TxQueue2.

```
wrr-queue queue-limit 40 50 0 0 0 0 0
```

Establishing and Configuring Interfaces on AR1

Refer to Figure 4-2 on page 4-53.

This section addresses the following:

- Establishing VLANs for Services on AR1
- Establishing Bidirectional and Unidirectional Transport Interfaces on AR1
- Establishing Tunnels on AR1
- Establishing an Interface to a DSLAM on AR1

Establishing VLANs for Services on AR1

Before bidirectional and unidirectional transport interfaces can be configured, VLANs for the various services must be created. With the exception of VLAN 90 (high-speed data), these are all Layer 3 VLANs. (Refer to Table 4-2 on page 4-5.)

The following is configured on AR1.

Note For additional details, see Establishing VLANs for Services on DER, page 4-61.

Step 1 In global configuration mode, establish a Layer 2 VLAN for high-speed data (HSD). (No Layer 3 interface is required.)

```
vlan 90
name VLAN_90_HSD
```

Step 2 Establish a VLAN for video at the edge.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 110
name VLAN_110_Video
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan110
 description Video edge VLAN
 ip address 192.168.110.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

c. Enable PIM sparse mode. This is the aggregation VLAN for video traffic to the DSLAMs. Broadcast video is multicast addressed.

```
 ip pim sparse-mode
```

d. To ensure consistently fast PIM convergence times, statically join the aggregation VLAN for video at the AR to the multicast groups.

```
 ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
```

e. Change the load interval from the default of 300.

```
 load-interval 30
```

f. Change the ARP timeout from the default.

```
arp timeout 250
```

Note The default timeout for an entry in the ARP cache is 4 hours. The default timeout for an entry in the MAC address table is only 5 minutes. Because video traffic is mostly unidirectional, the MAC address table may not be refreshed within the 5-minute timeout. This causes video traffic to be flooded until the destination MAC address is found. To prevent this, reduce the ARP cache timeout to 250 seconds. This forces the switch to re-ARP for the entries in the ARP cache before the entries in the MAC address table time out, avoiding the disruptive behavior.

Step 3 Establish a VLAN for VoIP at the edge.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 111
name VLAN_111_VoIP
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan111
 description VoIP edge VLAN
 ip address 192.168.111.1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

Step 4 Establish a VLAN for VoIP transport to and from DER.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 800
name VLAN_800_VoIP_to/from_DER
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan800
 description VoIP transport VLAN to/from DER
 ip address 192.168.252.2 255.255.255.252
```

c. Configure OSPF on the transport VLAN interface.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

d. Change the load interval from the default of 300.

```
load-interval 30
```

Step 5 Repeat Step 4, as appropriate, to establish a VLAN for VoIP transport to and from AR2.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 808
 name VLAN_808_VoIP_to/from_AR2
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan808
 description VoIP transport to/from AR2
 ip address 192.168.252.9 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Step 6 Establish a VLAN for video transport to and from DER.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 900
name VLAN_900_Video_to/from_DER
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan900
 description Video transport VLAN to/from DER
 ip address 192.168.254.2 255.255.255.252
```

c. Enable PIM sparse mode.

```
 ip pim sparse-mode
```

d. Configure OSPF on the transport VLAN interface.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

e. Change the load interval from the default of 300.

```
 load-interval 30
```

Step 7 Repeat Step 6, as appropriate, to establish a VLAN for video transport to and from AR2.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 908
name VLAN_908_Video_to/from_AR2
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan908
 description Video transport VLAN to/from AR2
 ip address 192.168.254.9 255.255.255.252
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Establishing Bidirectional and Unidirectional Transport Interfaces on AR1

Bidirectional and unidirectional transport interfaces must be established between AR1 and DER and AR2.

The following is configured on AR1.

Note For additional details, see Establishing Bidirectional and Unidirectional Interfaces for Transport on DER, page 4-66.

Step 1 Establish bidirectional transport interfaces.

a. Establish a bidirectional interface to and from DER.

```
interface GigabitEthernet3/1
 description Transport to/from DER (Gig7/1)
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,800,900
 switchport mode trunk
 dampening
 load-interval 30
 carrier-delay msec 0
```

b. Configure this interface (and all noningress transport interfaces) to trust the incoming DSCP markings. (This maintains the DSCP marking applied at the network ingress interface.)

```
 qos trust dscp
```

c. Set transmit-queue bandwidth thresholds and priority.

```
 tx-queue 1
   bandwidth percent 19
 tx-queue 2
   bandwidth percent 80
 tx-queue 3
   priority high
 tx-queue 4
   bandwidth percent 1
```

d. Repeat Step 1a through Step 1c, as appropriate, to establish the bidirectional transport interface to AR2.

```
interface GigabitEthernet4/3
 description Transport to/from AR2 (Gig1/1)
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,808,908
 switchport mode trunk
 dampening
 load-interval 30
 carrier-delay msec 0
 qos trust dscp
 tx-queue 1
   bandwidth percent 19
 tx-queue 2
   bandwidth percent 80
 tx-queue 3
   priority high
 tx-queue 4
   bandwidth percent 1
```

Step 2 Establish unidirectional receive-only transport interfaces.

a. Establish a unidirectional receive-only transport interface to DER. With the exceptions noted, the following is as in Step 1.

```
interface GigabitEthernet3/3
 description Transport from DER (Gig7/3)
 no switchport
 dampening
 ip address 192.168.253.2 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0

 qos trust dscp
```

b. Disable the link-negotiation protocol on the port.

```
 speed nonegotiate
```

c. Mark the interface as receive only.

```
 unidirectional receive-only
```

Note Transmit-queue bandwidth thresholds and priority do not need to be applied to a receive-only interface.

d. Repeat Step 2a through Step 2c, as appropriate, for the remaining unidirectional receive-only transport interfaces. Interface configurations are shown below.

Second unidirectional transport from DER

```
interface GigabitEthernet3/4
 description Transport from DER (Gig7/4)
 no switchport
 dampening
 ip address 192.168.253.6 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 speed nonegotiate
 qos trust dscp
 unidirectional receive-only
```

Third unidirectional transport from DER

```
interface GigabitEthernet3/5
 description Transport from DER (Gig7/5)
 no switchport
 dampening
 ip address 192.168.253.10 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 speed nonegotiate
 qos trust dscp
 unidirectional receive-only
```

Fourth unidirectional transport from DER

```
description Transport from DER (Gig7/6)
 no switchport
 dampening
 ip address 192.168.253.14 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 speed nonegotiate
 qos trust dscp
 unidirectional receive-only
```

Step 3 Establish unidirectional send-only interfaces.

a. Establish a unidirectional send-only transport interface to AR2. The following is as in Step 1.

```
interface GigabitEthernet4/4
 description Transport to AR2 (Gig1/2)
 no switchport
 dampening
 ip address 192.168.253.25 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 speed nonegotiate
 qos trust dscp
 tx-queue 1
   bandwidth percent 19
 tx-queue 2
   bandwidth percent 80
 tx-queue 3
   priority high
 tx-queue 4
   bandwidth percent 1
```

b. Mark the interface as send only.

```
 unidirectional send-only
```

c. Repeat Step 3a and Step 3b, as appropriate, for the second unidirectional send-only interface to AR2.

```
interface GigabitEthernet4/5
 description Transport to AR2 (Gig1/3)
 no switchport
 dampening
 ip address 192.168.253.29 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 speed nonegotiate
 qos trust dscp
 tx-queue 1
   bandwidth percent 19
 tx-queue 2
   bandwidth percent 80
 tx-queue 3
   priority high
 tx-queue 4
   bandwidth percent 1
 unidirectional send-only
```

Establishing Tunnels on AR1

See Establishing Tunnels on DER, page 4-70.

Table 4-8 on page 4-85 lists the loopback interfaces and corresponding tunnel interfaces configured on AR1.

Table 4-8 Corresponding Loopback and Tunnel Interfaces for AR1

Loopback Interface	Tunnel Interface
interface Loopback0 description Endpoint for Tunnel0 ip address 10.10.10.2 255.255.255.255	interface Tunnel0 description Tx-side of Rx-only Gig3/3 no ip address tunnel source 10.10.10.2 tunnel destination 10.10.10.1 tunnel udlr send-only GigabitEthernet3/3 tunnel udlr address-resolution
interface Loopback4 description Endpoint for Tunnel4 ip address 10.10.10.6 255.255.255.255	interface Tunnel4 description Tx-side of Rx-only Gig3/4 no ip address tunnel source 10.10.10.6 tunnel destination 10.10.10.5 tunnel udlr send-only GigabitEthernet3/4 tunnel udlr address-resolution
interface Loopback8 description Endpoint for Tunnel8 ip address 10.10.10.10 255.255.255.255	interface Tunnel8 description Tx-side of Rx-only Gig3/5 no ip address tunnel source 10.10.10.10 tunnel destination 10.10.10.9 tunnel udlr send-only GigabitEthernet3/5 tunnel udlr address-resolution

Table 4-8 Corresponding Loopback and Tunnel Interfaces for AR1 (continued)

Loopback Interface	Tunnel Interface
interface Loopback12 description Endpoint for Tunnel12 ip address 10.10.10.14 255.255.255.255	interface Tunnel12 description Tx-side of Rx-only Gig3/6 no ip address tunnel source 10.10.10.14 tunnel destination 10.10.10.13 tunnel udlr send-only GigabitEthernet3/6 tunnel udlr address-resolution
interface Loopback24 description Endpoint for Tunnel24 ip address 10.10.10.25 255.255.255.255	interface Tunnel24 description Rx-side of Tx-only Gig4/4 no ip address tunnel source 10.10.10.25 tunnel destination 10.10.10.26 tunnel udlr receive-only GigabitEthernet4/4
interface Loopback28 description Endpoint for Tunnel28 ip address 10.10.10.29 255.255.255.255	interface Tunnel28 description Rx-side of Tx-only Gig4/5 no ip address tunnel source 10.10.10.29 tunnel destination 10.10.10.30 tunnel udlr receive-only GigabitEthernet4/5

Establishing an Interface to a DSLAM on AR1

Do the following to establish an interface to DSLAM1.

The following is configured on AR1.

Step 1 Establish a 1-GE trunk to and from the uplink 1-GE port on the DSLAM.

a. Configure the trunk for 802.1q encapsulation, and assign the trunk to VLANs 90, 110, and 111.

```
interface GigabitEthernet5/1
 description GigE trunk to/from DSLAM uplink GigE
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,110,111

 switchport mode trunk
```

b. Prevent unknown unicast traffic from being flooded to the port.

```
 switchport block unicast
```

Note Occasionally, unknown unicast or multicast traffic is flooded to a switch port because a MAC address has timed out or has not been learned by the switch. (This condition is especially undesirable for a private VLAN isolated port.) To guarantee that no unicast or multicast traffic is flooded to the port, use the **switchport block unicast** or **switchport block multicast** commands.

c. Apply the “setDSCP” service policy to mark DSCP values in the inbound IP packets.

```
 service-policy input setDSCP
```

d. Change the load interval from the default of 300.

```
 load-interval 30
```

e. Set transmit-queue bandwidth thresholds and priority.

```
tx-queue 1
  bandwidth percent 19
tx-queue 2
  bandwidth percent 80
tx-queue 3
  priority high
tx-queue 4
  bandwidth percent 1
```

f. Disable Cisco Discovery Protocol (CDP) on the interface.

```
no cdp enable
```

g. Enable PortFast on the interface to bypass the listening and learning states in Spanning Tree Protocol (STP). This allows the interface to move immediately from the blocking state to the forwarding state, rather than waiting for STP to converge.

```
spanning-tree portfast trunk
```

Step 2 Repeat Step 1 for all additional GE DSLAMs served by the switch.

Configuring OSPF Routing for Video and Voice Traffic on AR1

Refer to Configuring OSPF Routing for Video and Voice Traffic on DER, page 4-71.

The following is configured on AR1.

Step 1 Define an OSPF routing process to route video traffic.

```
router ospf 100
 router-id 2.2.2.1
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 network 10.10.10.0 0.0.0.255 area 0
 network 192.168.254.0 0.0.0.255 area 0
 maximum-paths 8
```

Step 2 Define a second OSPF process to route VoIP traffic.

```
router ospf 101
 router-id 2.2.2.2
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan111
 network 192.168.111.0 0.0.0.255 area 0
 network 192.168.252.0 0.0.0.255 area 0
 maximum-paths 8
```

Step 3 Define a third OSPF process to route VoD transport traffic.

```
router ospf 102
 router-id 2.2.2.3
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan110
 network 192.168.110.0 0.0.0.255 area 0
 network 192.168.253.0 0.0.0.255 area 0
 maximum-paths 8
```

Configuring Spanning Tree on AR1

See Configuring Spanning Tree on DER, page 4-73.

The following is configured on AR1.

Step 1 Configure RTSP.

```
spanning-tree mode rapid-pvst
```

Step 2 Because the transport VLANs in the 10-GE ring are point-to-point networks, there is no risk of Layer 2 loops, so STP can be disabled on these VLANs.

```
no spanning-tree vlan 800, 808, 900, 908
```

Configuring AR2

This section addresses the configuration required on the switch labeled AR2 in Figure 4-2 on page 4-53, to route multiple services from AR2 to DER, AR1, and AR3.

See Configuring DNS Servers, page 4-2.

Note A Cisco Catalyst 6509 can also be used, as it uses the same supervisor engine, line cards, and Cisco IOS code as the Cisco 7609 router.

This section addresses the following:

- Configuring QoS on AR2
- Establishing and Configuring Interfaces on AR2
- Configuring OSPF Routing for Video and Voice Traffic on AR2
- Configuring Spanning Tree on AR2

Note For a complete configuration example, see Appendix B, “Sample DER and AR Switch Configurations for the 1-GE Asymmetric Topology.”

Configuring QoS on AR2

See Overview of QoS on a Cisco 7600 Series and Cisco Catalyst 6500 Series, page 4-57.

This section presents the following topics:

- Configuring Marking and Classification on AR2
- Configuring Mapping on AR2

Note For more information specific to QoS as applied to the solution, see Appendix C, “Understanding QoS as Implemented in the Solution.”

Configuring Marking and Classification on AR2

Do the following to enable marking and classification on AR2.

Step 1 Enable QoS in global configuration mode.

```
mls qos
```

Step 2 Create access lists to identify the different service types in the network.

```
ip access-list extended acl_HSD
 remark Identify HSD traffic
 permit ip 192.168.90.0 0.0.0.255 any
ip access-list extended acl_VoD_signaling
 remark Identify VoD signaling traffic
 permit ip 192.168.120.0 0.0.0.255 192.168.10.102
 permit ip 192.168.120.0 0.0.0.255 192.168.10.103
ip access-list extended acl_VoIP
 remark Identify VoIP traffic
 permit ip 192.168.121.0 0.0.0.255 any
```

Step 3 Create class maps for the access lists created in Step 2.

```
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_VoD_signaling
  match access-group name acl_VoD_signaling
class-map match-all class_HSD
  match access-group name acl_HSD
```

Step 4 Create a policy map to set the DSCP values of the different classes created in Step 3.

```
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoIP
   set dscp ef
  class class_HSD
   set dscp default
  class class_VoD_signaling
   set dscp cs3
```

Step 5 Apply the policy map from Step 4 to the ingress interfaces using the following command.

```
service-policy input setDSCP
```

Note Specific interface examples of this and other interface commands are shown in the interface provisioning sections.

Step 6 To maintain the DSCP marking applied at the network ingress interface, configure all noningress transport interfaces to trust the incoming DSCP markings.

```
mls qos trust dscp
```

Configuring Mapping on AR2

To configure mapping on AR2, refer to Configuring Mapping on DER, page 4-59.

Establishing and Configuring Interfaces on AR2

Refer to Figure 4-2 on page 4-53.

This section addresses the following:

- Establishing VLANs for Services on AR2
- Establishing Bidirectional and Unidirectional Transport Interfaces on AR2
- Establishing Tunnels on AR2
- Establishing an Interface to a DSLAM on AR2

Establishing VLANs for Services on AR2

Before bidirectional and unidirectional transport interfaces can be configured, VLANs for the various services must be created. With the exception of VLAN 90 (high-speed data), these are all Layer 3 VLANs. (Refer to Table 4-2 on page 4-5.)

The following is configured on AR2.

Note For additional details, see Establishing VLANs for Services on DER, page 4-61.

Step 1 In global configuration mode, establish a Layer 2 VLAN for high-speed data (HSD). (No Layer 3 interface is required.)

```
vlan 90
name VLAN_90_HSD
```

Step 2 Establish a VLAN for video at the edge.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 120
name VLAN_120_Video
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan120
 description Video edge VLAN
 ip address 192.168.120.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

c. Enable PIM sparse mode. This is the aggregation VLAN for video traffic to the DSLAMs. Broadcast video is multicast addressed.

```
 ip pim sparse-mode
```

d. To ensure consistently fast PIM convergence times, statically join the aggregation VLAN for video at the AR to the multicast groups.

```
 ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
```

e. Change the load interval from the default of 300.

```
 load-interval 30
```

f. Change the ARP timeout from the default.

```
arp timeout 250
```

Note The default timeout for an entry in the ARP cache is 4 hours. The default timeout for an entry in the MAC address table is only 5 minutes. Because video traffic is mostly unidirectional, the MAC address table may not be refreshed within the 5-minute timeout. This causes video traffic to be flooded until the destination MAC address is found. To prevent this, reduce the ARP cache timeout to 250 seconds. This forces the switch to re-ARP for the entries in the ARP cache before the entries in the MAC address table time out, avoiding the disruptive behavior.

Step 3 Establish a VLAN for VoIP at the edge.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 121
name VLAN_121_VoIP
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan121
 description VoIP edge VLAN
 ip address 192.168.121.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

c. Change the load interval from the default of 300.

```
 load-interval 30
```

Step 4 Establish a VLAN for VoIP transport to and from AR1.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 808
name VLAN_808_VoIP_to/from_AR1
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan808
 description VoIP transport VLAN to/from AR1
 ip address 192.168.252.10 255.255.255.252
```

c. Change the load interval from the default of 300.

```
 load-interval 30
```

d. Configure OSPF on the transport VLAN interface.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

Step 5 Repeat Step 4, as appropriate, to establish a VLAN for VoIP transport to and from AR3.

```
vlan 812
name VLAN_812_VoIP_to/from_AR3


interface Vlan812
 description VoIP transport VLAN to/from AR3
 ip address 192.168.252.14 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Step 6 Establish a VLAN for video transport to and from AR1.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 908
name VLAN_912_Video_to/from_DER
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan908
 description Video transport VLAN to/from AR1
 ip address 192.168.254.10 255.255.255.252
```

c. Enable PIM sparse mode.

```
 ip pim sparse-mode
```

d. Change the load interval from the default of 300.

```
 load-interval 30
```

e. Configure OSPF on the transport VLAN interface.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

Step 7 Repeat Step 6, as appropriate, to establish a VLAN for video transport to and from AR3.

```
vlan 912
name VLAN_908_Video_to/from_AR3


interface Vlan912
 description Video transport VLAN to/from AR3
 ip address 192.168.254.14 255.255.255.252
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Establishing Bidirectional and Unidirectional Transport Interfaces on AR2

Bidirectional and unidirectional transport interfaces must be established between AR1 and DER and AR2.

The following is configured on AR2.

Note For additional details, see to Establishing Bidirectional and Unidirectional Interfaces for Transport on DER, page 4-66.

Step 1 Establish bidirectional transport interfaces.

a. Establish a bidirectional interface to and from AR1.

```
interface GigabitEthernet1/1
 description Transport to/from AR1 (Gig4/3)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,808,908
 switchport mode trunk
 no ip address
 load-interval 30
 carrier-delay msec 0
```

b. Proceed as in Step 1b through Step 2 of Establishing Bidirectional and Unidirectional Interfaces for Transport on DER, page 4-66.

c. Establish a bidirectional transport interface to AR3. Note the exception below.

```
interface GigabitEthernet1/5
 description Transport to/from AR3 (Gig4/3)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,812,912
 switchport mode trunk
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0

 spanning-tree cost 10 <---See Note below
```

Note Note that the spanning-tree cost is set to 10 on AR2. This breaks the loop for VLAN 90 (Layer 2) between AR2 and AR3, rather than somewhere else.

d. Proceed as in Step 1b through Step 2 of Establishing Bidirectional and Unidirectional Interfaces for Transport on DER, page 4-66.

Step 2 Establish unidirectional receive-only transport interfaces.

a. Establish a unidirectional receive-only transport interface to AR1. With the exceptions noted, the following is as in Step 1.

```
interface GigabitEthernet1/2
 description Transport from AR1 (Gig4/4)
 dampening
 ip address 192.168.253.26 255.255.255.252
```

b. Configure OSPF on the interface.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

c. Change the load interval from the default of 300.

```
 load-interval 30
```

Note Transmit-queue bandwidth thresholds and priority do not need to be applied to a receive-only interface.

d. Disable the link-negotiation protocol on the port.

```
 speed nonegotiate
```

e. Mark the interface as receive only.

```
 unidirectional receive-only
```

f. Repeat Step 2a through Step 2e, as appropriate, for the remaining unidirectional receive-only transport interfaces. Interface configurations are shown below.

Second unidirectional transport from AR1

```
interface GigabitEthernet1/3
 description Transport from AR1 (Gig4/5)
 dampening
 ip address 192.168.253.30 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 speed nonegotiate
 wrr-queue bandwidth 64 255
 wrr-queue queue-limit 40 50
 wrr-queue random-detect min-threshold 2 50 100
 wrr-queue random-detect max-threshold 1 100 100
 wrr-queue random-detect max-threshold 2 50 100
 wrr-queue cos-map 1 1 0
 wrr-queue cos-map 2 1 1
 wrr-queue cos-map 2 2 2 3 4 6 7
 mls qos trust dscp
 unidirectional receive-only
```

Third unidirectional transport from AR3

```
interface GigabitEthernet1/6
 description Transport from AR3 (Gig4/4)
 dampening
 ip address 192.168.253.38 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 speed nonegotiate
 wrr-queue bandwidth 64 255
 wrr-queue queue-limit 40 50
 wrr-queue random-detect min-threshold 2 50 100
 wrr-queue random-detect max-threshold 1 100 100
 wrr-queue random-detect max-threshold 2 50 100
 wrr-queue cos-map 1 1 0
 wrr-queue cos-map 2 1 1
 wrr-queue cos-map 2 2 2 3 4 6 7
 mls qos trust dscp
 unidirectional receive-only
```

Fourth unidirectional transport from AR3

```
interface GigabitEthernet1/7
 description Transport from AR3 (Gig4/5)
 dampening
 ip address 192.168.253.42 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 speed nonegotiate
 wrr-queue bandwidth 64 255
 wrr-queue queue-limit 40 50
 wrr-queue random-detect min-threshold 2 50 100
 wrr-queue random-detect max-threshold 1 100 100
 wrr-queue random-detect max-threshold 2 50 100
 wrr-queue cos-map 1 1 0
 wrr-queue cos-map 2 1 1
 wrr-queue cos-map 2 2 2 3 4 6 7
 mls qos trust dscp
 unidirectional receive-only
```

Establishing Tunnels on AR2

See Establishing Tunnels on DER, page 4-70.

Table 4-9 lists the loopback interfaces and corresponding tunnel interfaces configured on AR2.

Table 4-9 Corresponding Loopback and Tunnel Interfaces for AR2

Loopback Interface	Tunnel Interface

`interface Loopback24`
` description Endpoint for Tunnel24`
` ip address 10.10.10.26 255.255.255.255`
	`interface Tunnel24`
	` description Tx-side of Rx-only Gig1/2`
	` no ip address`
	` tunnel source 10.10.10.26`
	` tunnel destination 10.10.10.25`
	` tunnel udlr send-only GigabitEthernet1/2`
	` tunnel udlr address-resolution`

`interface Loopback28`
` description Endpoint for Tunnel28`
` ip address 10.10.10.30 255.255.255.255`
	`interface Tunnel28`
	` description Tx-side of Rx-only Gig1/3`
	` no ip address`
	` tunnel source 10.10.10.30`
	` tunnel destination 10.10.10.29`
	` tunnel udlr send-only GigabitEthernet1/3`
	` tunnel udlr address-resolution`

Table 4-9 Corresponding Loopback and Tunnel Interfaces for AR2 (continued)

Loopback Interface	Tunnel Interface
interface Loopback36 description Endpoint for Tunnel36 ip address 10.10.10.38 255.255.255.255	interface Tunnel36 description Tx-side of Rx-only Gig1/6 no ip address tunnel source 10.10.10.38 tunnel destination 10.10.10.37 tunnel udlr send-only GigabitEthernet1/6 tunnel udlr address-resolution
interface Loopback40 description Endpoint for Tunnel40 ip address 10.10.10.42 255.255.255.255	interface Tunnel40 description Tx-side of Rx-only Gig1/7 no ip address tunnel source 10.10.10.42 tunnel destination 10.10.10.41 tunnel udlr send-only GigabitEthernet1/7 tunnel udlr address-resolution

Establishing an Interface to a DSLAM on AR2

DSLAM2 is an Ericsson GE DSLAM. Note the differences in Step 1f.

The following is configured on AR2.

Step 1 Establish a 1-GE trunk to and from the uplink 1-GE port on the DSLAM.

a. Configure the trunk for 802.1q encapsulation, and assign the trunk to VLANs 90, 120, and 121.

```
interface GigabitEthernet2/1
 description Ericsson DSLAM
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,120,121
 switchport mode trunk

 no ip address
```

b. Prevent unknown unicast traffic from being flooded to the port.

```
 switchport block unicast
```

Note Occasionally, unknown unicast or multicast traffic is flooded to a switch port because a MAC address has timed out or has not been learned by the switch. (This condition is especially undesirable for a private VLAN isolated port.) To guarantee that no unicast or multicast traffic is flooded to the port, use the **switchport block unicast** or **switchport block multicast** commands.

c. Apply the “setDSCP” service policy to mark DSCP values in the inbound IP packets.

```
 service-policy input setDSCP
```

d. Change the load interval from the default of 300.

```
 load-interval 30
```

e. Disable Cisco Discovery Protocol (CDP) on the interface.

```
 no cdp enable
```

f. Enable PortFast on the interface to bypass the listening and learning states in Spanning Tree Protocol (STP). This allows the interface to move immediately from the blocking state to the forwarding state, rather than waiting for STP to converge.

```
spanning-tree portfast trunk
```

g. Proceed as in Step 1b through Step 2 of Establishing Bidirectional and Unidirectional Interfaces for Transport on DER, page 4-66. but with the following exceptions:

```
wrr-queue bandwidth 64 255 0

wrr-queue queue-limit 40 50 0

wrr-queue threshold 1 100 100 100 100 100 100 100 100
wrr-queue threshold 2 50 100 100 100 100 100 100 100

wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100

no wrr-queue random-detect 2

wrr-queue cos-map 2 1 1
wrr-queue cos-map 2 2 2 3 4 6 7
```

Step 2 Repeat Step 1 for additional Ericsson GE DSLAMs served by the switch.

Configuring OSPF Routing for Video and Voice Traffic on AR2

See Configuring OSPF Routing for Video and Voice Traffic on DER, page 4-71.

The following is configured on AR2.

Step 1 Define an OSPF routing process to route video traffic.

```
router ospf 100
 router-id 3.3.3.1
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 network 10.10.10.0 0.0.0.255 area 0
 network 192.168.254.0 0.0.0.255 area 0
 maximum-paths 8
```

Step 2 Define a second OSPF process to route VoIP traffic.

```
router ospf 101
 router-id 3.3.3.2
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan121
 network 192.168.121.0 0.0.0.255 area 0
 network 192.168.252.0 0.0.0.255 area 0
 maximum-paths 8
```

Step 3 Define a third OSPF process to route VoD transport traffic.

```
router ospf 102
 router-id 3.3.3.3
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan120
 network 192.168.120.0 0.0.0.255 area 0
 network 192.168.253.0 0.0.0.255 area 0
 maximum-paths 8
```

Configuring Spanning Tree on AR2

See Configuring Spanning Tree on DER, page 4-20.

The following is configured on AR2.

Step 1 Configure RTSP.

```
spanning-tree mode rapid-pvst
```

Step 2 Because the transport VLANs in the 1-GE ring are point-to-point networks, there is no risk of Layer 2 loops, so STP can be disabled on these VLANs.

```
no spanning-tree vlan 800, 812, 908, 912
```

Configuring AR3

This section addresses the configuration required on the switch labeled AR3 in Figure 4-1 on page 4-4, to route multiple services from AR3 to AR2 and DER.

See Configuring DNS Servers, page 4-2.

This section addresses the following:

- Configuring QoS on AR3
- Establishing and Configuring Interfaces on AR3
- Configuring OSPF Routing for Video and Voice Traffic on AR3
- Configuring Spanning Tree on AR3

Note For a complete configuration example, see Appendix B, "Sample DER and AR Switch Configurations for the 1-GE Asymmetric Topology."

Configuring QoS on AR3

See Overview of QoS on a Cisco Catalyst 4500 Series, page 4-74.

This section presents the following topics:

- Configuring Marking and Classification on AR3
- Configuring Mapping on AR3
- Configuring Queueing on AR3

Note For more information specific to QoS as applied to the solution, see Appendix C, "Understanding QoS as Implemented in the Solution."

Configuring Marking and Classification on AR3

Do the following to enable marking and classification on AR3.

Step 1 Enable QoS in global configuration mode.

```
qos
```

Step 2 Create access lists to identify the different service types in the network.

```
ip access-list extended acl_HSD
 remark Identify HSD traffic
 permit ip 192.168.90.0 0.0.0.255 any
ip access-list extended acl_VoD_signaling
 remark Identify VoD signaling traffic
 permit ip 192.168.130.0 0.0.0.255 192.168.10.102
 permit ip 192.168.130.0 0.0.0.255 192.168.10.103
ip access-list extended acl_VoIP
 remark Identify VoIP traffic
 permit ip 192.168.131.0 0.0.0.255 any
```

Step 3 Create class maps for the access lists created in Step 2.

```
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_VoD_signaling
  match access-group name acl_VoD_signaling
class-map match-all class_HSD
  match access-group name acl_HSD
```

Step 4 Create a policy map to set the DSCP values of the different classes created in Step 3.

```
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoIP
   set dscp ef
  class class_HSD
   set dscp default
  class class_VoD_signaling
   set dscp cs3
```

Step 5 Apply the policy map from Step 4 to the ingress interfaces using the following command.

```
service-policy input setDSCP
```

Note Specific interface examples of this and other interface commands are shown in the interface provisioning sections.

Step 6 To maintain the DSCP marking applied at the network ingress interface, configure all noningress transport interfaces to trust the incoming DSCP markings.

```
qos trust dscp
```

Configuring Mapping on AR3

To configure mapping on AR3, proceed as in Configuring Mapping on AR1, page 4-76.

Configuring Queueing on AR3

To configure queueing on AR3, proceed as in Configuring Queueing on AR1, page 4-77.

Establishing and Configuring Interfaces on AR3

Refer to Figure 4-2 on page 4-53.

This section addresses the following:

- Establishing VLANs for Services on AR3
- Establishing Bidirectional and Unidirectional Transport Interfaces on AR3
- Establishing Tunnels on AR3
- Establishing an Interface to a DSLAM on AR3

Establishing VLANs for Services on AR3

Before bidirectional and unidirectional transport interfaces can be configured, VLANs for the various services must be created. With the exception of VLAN 90 (high-speed data), these are all Layer 3 VLANs. (Refer to Table 4-2 on page 4-5.)

The following is configured on AR3.

Note For details, see Establishing VLANs for Services on DER, page 4-61.

Step 1 In global configuration mode, establish a Layer 2 VLAN for high-speed data (HSD). (No Layer 3 interface is required.)

```
vlan 90
name VLAN_90_HSD
```

Step 2 Establish a VLAN for video at the edge.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 130
name VLAN_130_Video
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan130
 description Video edge VLAN
 ip address 192.168.130.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

c. Enable PIM sparse mode. This is the aggregation VLAN for video traffic to the DSLAMs. Broadcast video is multicast addressed.

```
 ip pim sparse-mode
```

d. To ensure consistently fast PIM convergence times, statically join the aggregation VLAN for video at the AR to the multicast groups.

```
 ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
```

e. Change the load interval from the default of 300.

```
 load-interval 30
```

f. Change the ARP timeout from the default.

```
arp timeout 250
```

Note The default timeout for an entry in the ARP cache is 4 hours. The default timeout for an entry in the MAC address table is only 5 minutes. Because video traffic is mostly unidirectional, the MAC address table may not be refreshed within the 5-minute timeout. This causes video traffic to be flooded until the destination MAC address is found. To prevent this, reduce the ARP cache timeout to 250 seconds. This forces the switch to re-ARP for the entries in the ARP cache before the entries in the MAC address table time out, avoiding the disruptive behavior.

Step 3 Establish a VLAN for VoIP at the edge.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 131
name VLAN_131_VoIP
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan131
 description VoIP edge VLAN
 ip address 192.168.131.1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

Step 4 Establish a VLAN for VoIP transport to and from AR2.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 812
name VLAN_812_VoIP_to/from_AR2
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan812
 description VoIP transport to/from AR2
 ip address 192.168.252.13 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

Step 5 Repeat Step 4, as appropriate, to establish a VLAN for VoIP transport to and from DER.

```
vlan 816
name VLAN_808_VoIP_to/from_DER


interface Vlan816
 description VoIP transport to/from DER
 ip address 192.168.252.18 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

Step 6 Establish a VLAN for video transport to and from AR2.

a. In global configuration mode, add the VLAN to the VLAN database.

```
vlan 912
name VLAN_912_Video_to/from_AR2
```

b. In interface configuration mode, create and configure the VLAN interface.

```
interface Vlan912
 description Video transport to/from AR2
 ip address 192.168.254.13 255.255.255.252
```

c. Enable PIM sparse mode.

```
ip pim sparse-mode
```

d. Configure OSPF on the interface.

```
ip ospf network point-to-point
ip ospf hello-interval 1
```

Step 7 Repeat Step 6, as appropriate, to establish a VLAN for video transport to and from DER.

```
vlan 916
name VLAN_916_Video_to/from_DER


interface Vlan916
 description Video transport to/from DER
 ip address 192.168.254.18 255.255.255.252
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

Establishing Bidirectional and Unidirectional Transport Interfaces on AR3

Bidirectional and unidirectional transport interfaces must be established between AR1 and DER and AR2.

The following is configured on AR3.

Note For additional details, see Establishing Bidirectional and Unidirectional Interfaces for Transport on DER, page 4-66.

Step 1 Establish bidirectional transport interfaces.

a. Establish a bidirectional interface to and from DER.

```
interface GigabitEthernet3/1
 description Transport to/from DER (Gig7/9)
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,816,916
 switchport mode trunk
 load-interval 30
```

b. Configure this interface (and all noningress transport interfaces) to trust the incoming DSCP markings. (This maintains the DSCP marking applied at the network ingress interface.)

```
qos trust dscp
```

c. Set the transmit-queue bandwidth thresholds and priority.

```
tx-queue 1
  bandwidth percent 19
tx-queue 2
  bandwidth percent 80
tx-queue 3
  priority high
tx-queue 4
  bandwidth percent 1
```

d. Repeat Step 1a through Step 1c, as appropriate, to establish the bidirectional transport interface to AR2. Note the exception below.

```
interface GigabitEthernet4/3
 description Transport to/from AR2 (Gig1/5)
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,812,912
 switchport mode trunk
 load-interval 30
 qos trust dscp
 tx-queue 1
   bandwidth percent 19
 tx-queue 2
   bandwidth percent 80
 tx-queue 3
   priority high
 tx-queue 4
   bandwidth percent 1
 spanning-tree cost 10 <---See Note below
```

Note Note that the spanning-tree cost is set to 10 on AR3. This breaks the loop for VLAN 90 (Layer 2) between AR2 and AR3, rather than somewhere else.

Step 2 Establish unidirectional receive-only transport interfaces.

a. Establish a unidirectional receive-only interface to DER, With the exceptions noted, the following is as in Step 1.

```
interface GigabitEthernet3/3
 description Transport from DER (Gig7/11)
 dampening
 ip address 192.168.253.50 255.255.255.252
```

b. Configure OSPF on the interface.

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
```

c. Change the load interval from the default of 300.

```
 load-interval 30
```

Note Transmit-queue bandwidth thresholds and priority do not need to be applied to a receive-only interface.

d. Disable the link-negotiation protocol on the port.

```
 speed nonegotiate
```

e. Mark the interface as receive only.

```
 unidirectional receive-only
```

f. Repeat Step 2a through Step 2e, as appropriate, for the remaining unidirectional receive-only transport interfaces. Interface configurations are shown below.

Second unidirectional transport from DER

```
interface GigabitEthernet3/4
 description Transport from DER (Gig7/12)
 no switchport
 dampening
 ip address 192.168.253.54 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 speed nonegotiate
 unidirectional receive-only
```

Third unidirectional transport from DER

```
interface GigabitEthernet3/5
 description Transport from DER (Gig7/13)
 no switchport
 dampening
 ip address 192.168.253.58 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 speed nonegotiate
 qos trust dscp
 unidirectional receive-only
```

Fourth unidirectional transport from DER

```
interface GigabitEthernet3/6
 description Transport from DER (Gig7/14)
 no switchport
 dampening
 ip address 192.168.253.62 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 speed nonegotiate
 qos trust dscp
 unidirectional receive-only
```

Step 3 Establish unidirectional send-only transport interfaces.

a. Establish a unidirectional send-only transport interface to AR2. With the exception noted, the following is as in Step 1.

```
interface GigabitEthernet4/4
 description Transport to AR2 (Gig1/6)
 no switchport
 ip address 192.168.253.37 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 speed nonegotiate
 qos trust dscp
 tx-queue 1
   bandwidth percent 19
 tx-queue 2
   bandwidth percent 80
 tx-queue 3
   priority high
 tx-queue 4
   bandwidth percent 1
```

b. Mark the interface as send only.

```
 unidirectional send-only
```

c. Repeat Step 3a and Step 3b, as appropriate, for the second unidirectional send-only transport interface to AR2.

```
interface GigabitEthernet4/5
 description Transport to AR2 (Gig1/7)
 no switchport
 ip address 192.168.253.41 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 speed nonegotiate
 qos trust dscp
 tx-queue 1
   bandwidth percent 19
 tx-queue 2
   bandwidth percent 80
 tx-queue 3
   priority high
 tx-queue 4
   bandwidth percent 1
 unidirectional send-only
```

Establishing Tunnels on AR3

See Establishing Tunnels on DER, page 4-70.

Table 4-10 on page 4-108 lists the loopback interfaces and corresponding tunnel interfaces configured on AR3.

Table 4-10 Corresponding Loopback and Tunnel Interfaces for AR3

Loopback Interface	Tunnel Interface
interface Loopback36 description Endpoint for Tunnel36 ip address 10.10.10.37 255.255.255.255	interface Tunnel36 description Rx-side of Tx-only Gig4/4 no ip address tunnel source 10.10.10.37 tunnel destination 10.10.10.38 tunnel udlr receive-only GigabitEthernet4/4
interface Loopback40 description Endpoint for Tunnel40 ip address 10.10.10.41 255.255.255.255	interface Tunnel40 description Rx-side of Tx-only Gig4/5 no ip address tunnel source 10.10.10.41 tunnel destination 10.10.10.42 tunnel udlr receive-only GigabitEthernet4/5
interface Loopback48 description Endpoint for Tunnel48 ip address 10.10.10.50 255.255.255.255	interface Tunnel48 description Tx-side of Rx-only Gig3/3 no ip address tunnel source 10.10.10.50 tunnel destination 10.10.10.49 tunnel udlr send-only GigabitEthernet3/3 tunnel udlr address-resolution
interface Loopback52 description Endpoint for Tunnel52 ip address 10.10.10.54 255.255.255.255	interface Tunnel52 description Tx-side of Rx-only Gig3/4 no ip address tunnel source 10.10.10.54 tunnel destination 10.10.10.53 tunnel udlr send-only GigabitEthernet3/4 tunnel udlr address-resolution
interface Loopback56 description Endpoint for Tunnel56 ip address 10.10.10.58 255.255.255.255	interface Tunnel56 description Tx-side of Rx-only Gig3/5 no ip address tunnel source 10.10.10.58 tunnel destination 10.10.10.57 tunnel udlr send-only GigabitEthernet3/5 tunnel udlr address-resolution
interface Loopback60 description Endpoint for Tunnel60 ip address 10.10.10.62 255.255.255.255	interface Tunnel60 description Tx-side of Rx-only Gig3/6 no ip address tunnel source 10.10.10.62 tunnel destination 10.10.10.61 tunnel udlr send-only GigabitEthernet3/6 tunnel udlr address-resolution

Establishing an Interface to a DSLAM on AR3

Do the following to establish an interface to DSLAM3.

The following is configured on AR3.

Step 1 Establish a 1-GE trunk to and from the uplink 1-GE port on the DSLAM.

a. Configure the trunk for 802.1q encapsulation, and assign the trunk to VLANs 90, 110, and 111.

```
interface GigabitEthernet5/1
 description GigE trunk to/from DSLAM uplink GigE
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 90,130,131

 switchport mode trunk
```

b. Prevent unknown unicast traffic from being flooded to the port.

```
 switchport block unicast
```

Note Occasionally, unknown unicast or multicast traffic is flooded to a switch port because a MAC address has timed out or has not been learned by the switch. (This condition is especially undesirable for a private VLAN isolated port.) To guarantee that no unicast or multicast traffic is flooded to the port, use the **switchport block unicast** or **switchport block multicast** commands.

c. Apply the "setDSCP" service policy to mark DSCP values in the inbound IP packets.

```
 service-policy input setDSCP
```

d. Change the load interval from the default of 300.

```
 load-interval 30
```

e. Set transmit-queue bandwidth thresholds and priority.

```
 tx-queue 1
   bandwidth percent 19
 tx-queue 2
   bandwidth percent 80
 tx-queue 3
   priority high
 tx-queue 4
   bandwidth percent 1
```

f. Disable Cisco Discovery Protocol (CDP) on the interface.

```
 no cdp enable
```

g. Enable PortFast on the interface to bypass the listening and learning states in Spanning Tree Protocol (STP). This allows the interface to move immediately from the blocking state to the forwarding state, rather than waiting for STP to converge.

```
 spanning-tree portfast trunk
```

Step 2 Repeat Step 1 for all additional GE DSLAMs served by the switch.

Configuring OSPF Routing for Video and Voice Traffic on AR3

Refer to Configuring OSPF Routing for Video and Voice Traffic on DER, page 4-71.

The following is configured on AR3.

Step 1 Define an OSPF routing process to route video traffic.

```
router ospf 100
 router-id 4.4.4.1
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 network 10.10.10.0 0.0.0.255 area 0
 network 192.168.254.0 0.0.0.255 area 0
 maximum-paths 8
```

Step 2 Define a second OSPF process to route VoIP traffic.

```
router ospf 101
 router-id 4.4.4.2
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan131
 network 192.168.131.0 0.0.0.255 area 0
 network 192.168.252.0 0.0.0.255 area 0
 maximum-paths 8
```

Step 3 Define a third OSPF process to route VoD traffic.

```
router ospf 102
 router-id 4.4.4.3
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan130
 network 192.168.130.0 0.0.0.255 area 0
 network 192.168.253.0 0.0.0.255 area 0
 maximum-paths 8
```

Configuring Spanning Tree on AR3

See Configuring Spanning Tree on DER, page 4-20.

The following is configured on AR3.

Step 1 Configure RTSP.

```
spanning-tree mode rapid-pvst
```

Step 2 Because the transport VLANs in the 1-GE ring are point-to-point networks, there is no risk of Layer 2 loops, so STP can be disabled on these VLANs.

```
no spanning-tree vlan 812, 816, 912, 916
```