Implementing and Configuring the Solution

This chapter presents the following major tasks:

Configuring a Point-to-Point and Multihop Ethernet Topology

This section addresses the following:

Figure 3-1 on page 3-2 illustrates the point-to-point and multihop Ethernet topology discussed in this section. Table 3-1 on page 3-3 lists the loopback and VLAN IP addresses for the headend, Dhub, and QAM switches.

Figure 3-1 Example Point-to-Point and Multihop Topology

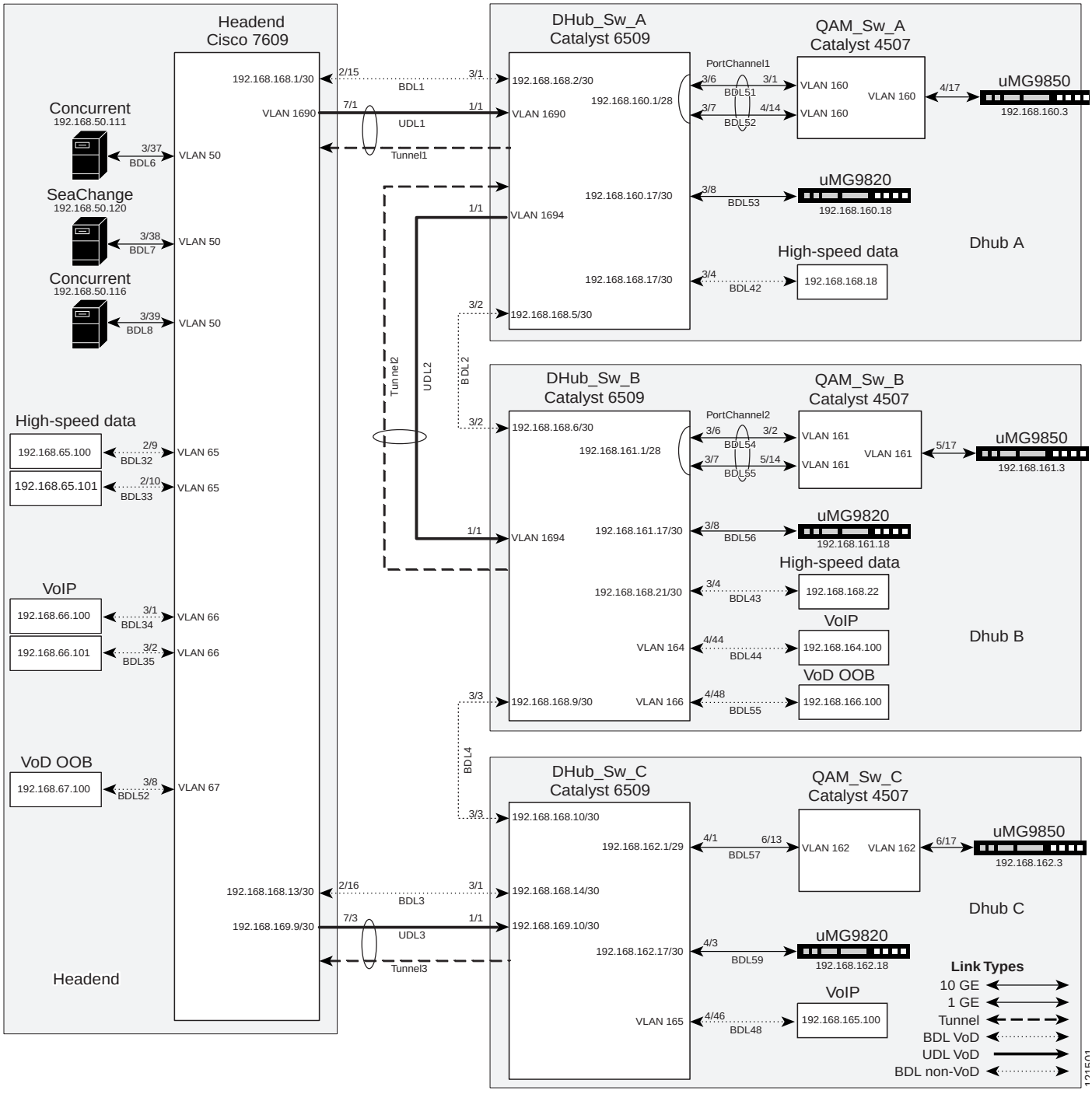

Table 3-1 Loopback and VLAN IP Addresses for Example Point-to-Point and Multihop Topology

Switch name	Loopback	VLAN
Headend	Loopback1: 10.10.10.10/32	VLAN 50: 192.168.50.1/24 (HSRP)
	Loopback3: 14.14.14.14/32	VLAN 65: 192.168.50.1/24
		VLAN 66: 192.168.65.1/24
		VLAN 67: 192.168.66.1/24
		VLAN 1690: 192.168.67.1/24
DHub_Sw_A	Loopback1: 11.11.11.11/32	VLAN 1690: 192.168.169.2/30
	Loopback2: 12.12.12.12/32	VLAN 1694: 192.168.169.5/30
DHub_Sw_B	Loopback2: 13.13.13.13/32	VLAN 164: 192.168.164.1/24
		VLAN 166: 192.168.166.1/24
		VLAN 1694: 192.168.169.6/30
DHub_Sw_C	Loopback3: 15.15.15.15/32	VLAN 165: 192.168.165.1/24
QAM_Sw_A		VLAN 160: 192.168.160.2/28
QAM_Sw_B		VLAN 161: 192.168.161.2/28
QAM_Sw_C		VLAN 162: 192.168.161.2/29

Configuring the Headend

This section addresses the configuration required on the switch labeled Headend in Figure 3-1 on page 3-2, to route multiple services from the headend switch to the Dhubs. The headend consists of VoD servers, VoIP equipment, high-speed data equipment, VoD OOB (out-of-band) equipment, and a Cisco 7609. A Cisco Catalyst 6509 can also be used, as they use the same supervisor engine.

Note For command references and best practices, 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

This section addresses the following:

- Confirming Hardware
- Establishing Quality of Service (QoS)
- Enabling OSPF and VRF-lite for Video-over-IP Traffic

- Enabling OSPF for Non-video Traffic
- Enabling Load Balancing
- Establishing Interfaces on the Headend Switch

These are configured on the Cisco 7609 labeled Headend in Figure 3-1 on page 3-2. For a complete configuration example, see Appendix A, "Sample Configuration for a Headend Switch."

Confirming Hardware

Before proceeding, it is beneficial to use the **show modules** command to confirm the hardware components and their versions for each switch.

The following is executed on Headend.

Step 1 Confirm hardware.

```
Headend# show modules

Mod Ports Card Type                                Model
--- ----- ---------------------------------------- ------------------
  1   16  Pure SFM-mode 16 port 1000mb GBIC       WS-X6816-GBIC
  2   16  Pure SFM-mode 16 port 1000mb GBIC       WS-X6816-GBIC
  3   48  CEF720 48 port 10/100/1000mb Ethernet   WS-X6748-GE-TX
  5    2  Supervisor Engine 720 (Active)          WS-SUP720-BASE
  7    4  CEF720 4 port 10-Gigabit Ethernet       WS-X6704-10GE


Mod Sub-Module                  Model              Hw
--- --------------------------- ------------------ -------
  1 Distributed Forwarding Card WS-F6K-DFC3A       2.0
  2 Distributed Forwarding Card WS-F6K-DFC3A       2.0
  3 Centralized Forwarding Card WS-F6700-CFC       1.2
  5 Policy Feature Card 3       WS-F6K-PFC3BXL     1.2
  5 MSFC3 Daughterboard         WS-SUP720          2.1
  7 Distributed Forwarding Card WS-F6700-DFC3A     2.1
```

Establishing Quality of Service (QoS)

This section addresses the configuration of QoS (see Routing and QoS, page 2-12) in the point-to-point and multihop topology depicted in Figure 3-1 on page 3-2, 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.

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. (See DSCP Features and Values Used in Release 2.0, page 2-20.) 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.

The following is configured on Headend.

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

Step 1 Enable QoS in global configuration mode.

```
mls qos
```

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

VoD server traffic has two levels of priority, high and low. The User Datagram Protocol (UDP) port range for the GE QAM gateways is divided in half, with the upper half considered high priority and the lower half considered low priority. In customer networks, assigning priorities depends on the service groups used by the customer.

Note "OOB" represents out-of-band traffic.

```
ip access-list extended acl_VoD_OOB
 remark Identify VoD OOB traffic.
 permit ip 192.168.67.0 0.0.0.255 any
ip access-list extended acl_VoIP
 remark Identify VoIP traffic.
 permit ip 192.168.66.0 0.0.0.255 any
ip access-list extended acl_high_speed_data
 remark Identify high speed data.
 permit ip 192.168.65.0 0.0.0.255 any
ip access-list extended acl_video_high
 remark Identify high priority VoD server traffic.
 permit udp 192.168.48.0 0.0.7.255 192.168.160.0 0.0.3.255 range 3329 6399
ip access-list extended acl_video_low
 remark Identify low priority VoD server traffic.
 permit udp 192.168.48.0 0.0.7.255 192.168.160.0 0.0.3.255 range 257 3327
```

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

```
class-map match-all class_VoD_OOB
  match access-group name acl_VoD_OOB
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_high_speed_data
  match access-group name acl_high_speed_data
class-map match-all class_video_high
  match access-group name acl_video_high
class-map match-all class_video_low
  match access-group name acl_video_low
```

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 the different types of traffic
  class class_VoD_OOB
   set dscp cs3
  class class_VoIP
   set dscp ef
  class class_high_speed_data
   set dscp default
  class class_video_high
```

```
 set dscp cs4
class class_video_low
 set dscp af41
```

Step 5 Change the default DSCP-to-CoS mapping for video traffic.

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. The highlighted values are for the non-video traffic. This table shows that high-speed data (DSCP = 0) is mapped to CoS = 0, VoD OOB (DSCP = 24) is mapped to CoS = 3, and VoIP (DSCP = 46) is mapped to CoS = 5. (Note that d1 corresponds to the *x*-axis value of the table, and d2 to the *y*-axis value.)

```
Headend# 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 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
```

In this configuration, the non-video traffic is carried on the GE interfaces. Use the following command on these interfaces to see if these CoS values are assigned to the correct transmit queues.

Note The following command has a large output and only the applicable excerpts are shown below. The CoS mappings are highlighted under the column labeled [cos-map].

```
show queueing interface gigabitEthernet 2/15

Interface GigabitEthernet2/15 queueing strategy:  Weighted Round-Robin

    Queueing Mode In Tx direction: mode-cos
    Transmit queues [type = 1p2q2t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       1         WRR low            2
       2         WRR high           2
       3         Priority           1


  Packets dropped on Transmit:
    BPDU packets:  0

    queue thresh    dropped  [cos-map]
    ------------------------------------------------
    1     1              0  [0 1 ]
    1     2              0  [2 3 ]
    2     1              0  [4 6 ]
    2     2              0* [7 ]
    3     1              0* [5 ]
                             * - shared transmit counter
```

From the output, we can see that high-speed data and VoD OOB traffic are put into Tx Queue 1, VoD OOB traffic is put into Tx Queue 2, and VoIP traffic is put into Tx Queue 3 (which is the priority queue). The default mappings from DSCP to CoS and from CoS to transmit queue are correct for the non-video traffic types.

Step 6 Confirm the CoS mappings for high- and low-priority video traffic.

Below is the same default DSCP-to-CoS mapping, but with the values for high- and low-priority video traffic highlighted. This table shows that both low-priority video (DSCP = 34) and high-priority video (DSCP = 32) are mapped to CoS = 4. The solution specifies that high-priority video traffic be put in the priority transmit queue, and low-priority video traffic be put in a nonpriority queue.

```
Headend# 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
```

Next we must look at a 10-GE transport interface to see how the CoS values are assigned to transmit queues.

Note The following command has a large output and only the applicable excerpts are shown below. The DSCP-to-CoS mappings are highlighted under the column labeled [cos-map].

```
Headend# show queueing interface tenGigabitEthernet 7/1

Interface TenGigabitEthernet7/1 queueing strategy:  Weighted Round-Robin
Queueing Mode In Tx direction: mode-cos
    Transmit queues [type = 1p7q8t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       01         WRR                 08
       02         WRR                 08
       03         WRR                 08
       04         WRR                 08
       05         WRR                 08
       06         WRR                 08
       07         WRR                 08
       08         Priority            01

  Packets dropped on Transmit:

    queue     dropped  [cos-map]
    ---------------------------------------------
    1               0  [0 1 ]
    2               0  [2 3 4 ]
    3               0  [6 7 ]
    4               0  []
    5               0  []
    6               0  []
    7               0  []
    8               0  [5 ]
```

We want to keep low-priority video traffic in Transmit Queue 2, but move high-priority video traffic to Transmit Queue 8. This requires us to modify the default DSCP-to-CoS mapping for a DSCP value of 32 from a CoS of 4 to a CoS of 5.

Step 7 Modify the default DSCP-to-CoS mapping to direct high-priority video traffic to the correct transmit queue.

```
mls qos map dscp-cos 32 to 5
```

Step 8 Confirm the revised DSCP-to-CoS mapping.

Looking at the DSCP-to-CoS mapping again, we can see that a DSCP value of 32 is mapped to a CoS of 5.

```
Headend# 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 05 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
```

Step 9 With the policy map created in Step 4, now apply it to all the ingress interfaces—for both video and non-video traffic.

```
service-policy input setDSCP
```

Step 10 Configure all non-ingress transport interfaces to trust the incoming DSCP markings, to maintain the DSCP marking applied at the network ingress interface.

```
mls qos trust dscp
```

Enabling OSPF and VRF-lite for Video-over-IP Traffic

The solution specification uses VRF-lite (VPN routing and forwarding) to allow video and non-video traffic to be routed independently. (For more information, see Using VRF-lite and Differentiated Services in a Converged Multiservice Architecture, page 2-18.) All interfaces that carry video traffic are put into a VRF routing table, and all interfaces that carry non-video traffic are put in the global routing table.

The following is configured on Headend.

Step 1 Define the VRF routing table.

The following command creates a VRF routing table and a Cisco Express Forwarding (CEF) table, both named “Video.” The **rd** command defines a route distinguisher, which can be in the form of *ASN:nn*, *IP-address:nn*, or *arbitrary-number:nn*.

```
ip vrf Video
 description Video traffic destined for DHubs
 rd 1000:1
```

Step 2 Associate all Layer 3 interfaces that carry video traffic with the VRF defined in Step 1.

For Headend, this includes VLANs 50 and 1690, and TenGigabitEthernet7/3. An interface cannot be assigned to both the “Video” VRF routing table and the global routing table at the same time.

Caution Be aware that executing this command on an interface removes the IP address if it was previously configured.

```
ip vrf forwarding Video
```

Step 3 Create the OSPF process and associate it with the VRF routing table defined in Step 1.

The **router ospf 100 vrf Video** command associates the “Video” VRF routing table with OSPF routing process 100. Because the solution does not use Border Gateway Protocol (BGP), the **capability vrf-lite** command is used to suppress specific checks on the switch when the OSPF process is associated with the VRF routing table. The network statements should include all interfaces that carry video traffic. This includes all VoD server ingress ports and the transport interfaces to the Dhubs.

```
router ospf 100 vrf Video
 log-adjacency-changes
 capability vrf-lite
 network 192.168.50.0 0.0.0.255 area 0
 network 192.168.169.0 0.0.0.3 area 0
 network 192.168.169.8 0.0.0.3 area 0
 network 192.168.169.32 0.0.0.3 area 0
 network 192.168.169.36 0.0.0.3 area 0
```

Note To configure passive interfaces in the OSPF process associated with the Video VRF table, include the **passive-interface** command in the global OSPF process.

Enabling OSPF for Non-video Traffic

The solution specification uses the global routing table for non-video traffic. All interfaces that carry non-video traffic are put into the global routing table. This includes VoIP ingress ports, VoD OOB ingress ports, high speed data ingress ports, the transport interfaces that carry this traffic and the loopback interfaces. The loopback interfaces serve as the endpoints for the GRE tunnels that are the bidirectional return paths for the unidirectional links between the headend and Dhubs.

The following is configured on Headend.

Step 1 Define a second OSPF routing process to carry non-video traffic.

```
router ospf 101
 log-adjacency-changes
 network 1.14.0.0 0.0.255.255 area 0
 network 10.10.10.10 0.0.0.0 area 0
 network 14.14.14.14 0.0.0.0 area 0
 network 192.168.65.0 0.0.0.255 area 0
 network 192.168.66.0 0.0.0.255 area 0
 network 192.168.67.0 0.0.0.255 area 0
 network 192.168.168.0 0.0.0.3 area 0
 network 192.168.168.12 0.0.0.3 area 0
```

Note To configure passive interfaces in the OSPF process associated with the Video VRF, include the **passive-interface** command in the global OSPF process.

Enabling Load Balancing

If multiple 10-GE links are required between the headend and a Dhub, caution should be taken when configuring load balancing. Simulations and lab tests have shown that the Cisco IOS Release 12.2.17d-SXB1 for the Cisco Catalyst 6500 series switches and the Cisco 7609 (both of which use Supervisor Engine 720) does not provide acceptable Layer 3 CEF load balancing of VoD server traffic across 2 through 8 equal-cost paths. For this reason, EtherChannel load balancing is recommended over Layer 3 CEF load balancing.

Although EtherChannels can be configured with up to 8 members, only sizes of 2, 4, or 8 members should be configured. These are the only size EtherChannels that provide acceptable load balancing for the VoD server traffic. The default EtherChannel load balancing must be modified to achieve the desired results. By default, the Layer 4 ports are not included in the algorithm, and so we require the destination Layer 4 port to be included in the algorithm by using the following command:

```
port-channel load-balance dst-port
```

Establishing Interfaces on the Headend Switch

This section addresses the following:

- Establishing a VLAN for VoD Server Traffic
- Establishing GE Interfaces for the VoD Servers
- Establishing VLANs for VoIP, High-Speed Data, and VoD OOB Traffic
- Establishing GE Interfaces for VoIP, High-Speed Data, and VoD OOB Traffic
- Establishing Bidirectional 1-GE Links to the Dhubs
- Establishing Unidirectional 10-GE Links to the Dhubs
- Establishing GRE Tunnels to the Dhubs

Establishing a VLAN for VoD Server Traffic

The VoD servers connect to Layer 2 interfaces on the headend switch and their traffic is aggregated into a VLAN. The following steps detail the configuration of the VLAN.

The following is configured on Headend.

Step 1 In global configuration mode, add the VLAN to the VLAN database.

```
vlan 50
```

Step 2 Create the VLAN interface.

```
interface Vlan50
 description VoD servers
```

Step 3 Disable the sending of Internet Control Message Protocol (ICMP) protocol-unreachable and host-unreachable messages. When enabled, host-unreachable messages are sent from the VLAN to the VoD server if the VLAN is unable to deliver packets to the ultimate destination—because it knows of no route to the destination address.

```
no ip unreachables
```

Step 4 Associate the VLAN with the Video VRF. (See Using VRF-lite and Differentiated Services in a Converged Multiservice Architecture, page 2-18.)

```
ip vrf forwarding Video
```

Step 5 Assign the VLAN a virtual IP address and virtual MAC address using Hot Standby Routing Protocol (HSRP). The **ip address 192.168.50.2 255.255.255.0** command assigns a physical IP address to the VLAN, and the MAC address is the burned-in address. The **standby 50 ip 192.168.50.1** command assigns a virtual IP address of 192.168.50.1 and a virtual MAC address of 0000.0c07.ac32 to the VLAN.

Caution Be sure to include a group number when using the **standby** command. Otherwise, the group number defaults to 0.

```
ip address 192.168.50.2 255.255.255.0
standby 50 ip 192.168.50.1
```

Note The **show interface vlan 50** command does not show the virtual IP and MAC addresses. You must use the **show standby** command to verify this information, as in the step below.

Step 6 Verify the virtual IP and MAC addresses.

```
Headend# show standby
Vlan50 - Group 50
  Local state is Active, priority 100
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 0.768
  Virtual IP address is 192.168.50.1 configured
  Active router is local
  Standby router is unknown
  Virtual mac address is 0000.0c07.ac32
  2 state changes, last state change 2w2d
  IP redundancy name is "hsrp-Vl50-50" (default)
```

Establishing GE Interfaces for the VoD Servers

The VoD servers connect to Layer 2 interfaces on the headend switch and their traffic is aggregated into a VLAN. The following steps detail the configuration of the GigabitEthernet 3/37 Layer 2 interface. GigabitEthernet 3/38 and 3/39 are configured similarly.

The following is configured on Headend.

Step 1 Create the Layer 2 interface and assign it to VLAN 50.

```
interface GigabitEthernet3/37
 description BDL6: Concurrent VoD server ingress (MH-4000-1)
 no ip address
 switchport
```

```
 switchport access vlan 50
 switchport mode access
```

Step 2 If using 10/100/1000-Mbps ports, we recommend that the speed and duplex be forced to 1000 Mbps and full duplex, respectively.

```
speed 1000
duplex full
```

Step 3 Disable the Cisco Discovery Protocol on the interface, because the VoD servers do not support it.

```
no cdp enable
```

Step 4 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
```

Step 5 Apply the "setDSCP" service policy that marks DSPC values in the inbound IP packets. (See DSCP Features and Values Used in Release 2.0, page 2-20.)

```
service-policy input setDSCP
```

Establishing VLANs for VoIP, High-Speed Data, and VoD OOB Traffic

In this configuration, Layer 2 interfaces and VLANs are used to connect the headend switch to resources for VoIP, high-speed data, and VoD OOB traffic. The following steps detail the configuration of a VLAN dedicated to high-speed data, VLAN 65. VLANs for VoIP (VLAN 66) and VoD OOB traffic (VLAN 67) are configured similarly.

Note Although Release 2.0 supports a multiservice architecture, interface configurations for VoIP, high-speed data, and VoD OOB equipment are beyond the scope of this solution. Vendor- and equipment-specific resources should be used to configure these interfaces properly.

Step 1 In global configuration mode, add the VLAN to the VLAN database.

```
vlan 65
```

Step 2 Create the VLAN interfaces.

```
interface Vlan65
 description High speed data
 ip address 192.168.65.1 255.255.255.0
```

Establishing GE Interfaces for VoIP, High-Speed Data, and VoD OOB Traffic

The following steps detail the configuration of GigabitEthernet 2/9, which is the Layer 2 interface for high-speed data. GigabitEthernet 2/10, GigabitEthernet 3/1 and 3/2, and GigabitEthernet 3/8 and 3/9 are configured similarly.

The following is configured on Headend.

Step 1 Create the Layer 2 interface and assign it to VLAN 65.

```
interface GigabitEthernet2/9
 description BDL32: High speed data
 no ip address
 switchport
 switchport access vlan 65
 switchport mode access
```

Step 2 Disable CDP on the interface, because the VoD servers do not support it.

```
no cdp enable
```

Step 3 Enable PortFast on the interface to bypass the listening and learning states in 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
```

Note This command should be used in conjunction with the global command **spanning-tree portfast bpduguard default**. The **bpduguard** command option configures the switch to disable any interface that is configured for PortFast and receives a Bridge Protocol Data Unit (BPDU). 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.

Step 4 Apply the "setDSCP" service policy that marks DSPC values in the inbound IP packets. (See DSCP Features and Values Used in Release 2.0, page 2-20.)

```
service-policy input setDSCP
```

Establishing Bidirectional 1-GE Links to the Dhubs

In this example, there are two 1-GE connections between the headend and the Dhubs. One is from Headend to DHub_Sw_A, and the other is from Headend to DHub_Sw_C. These connections carry VoIP and high-speed data, as well as VoD OOB, OSPF, and Address Resolution Protocol (ARP) traffic. All traffic on these interfaces is part of the global routing table, except for the GRE tunnels that provide the return paths for the 10-GE unidirectional links. GigabitEthernet2/16 is configured similarly.

The following is configured on Headend.

Step 1 Configure the Layer 3 bidirectional 1-GE interface.

```
interface GigabitEthernet2/15
 description BDL1: Non-video traffic to/from DHub_Sw_A (Gig3/1)
 ip address 192.168.168.1 255.255.255.252
```

Step 2 Since the DSCP values are marked at the ingress interfaces, the DSCP values of the inbound IP packets can be trusted on the transport interfaces. By default, these DSCP values are not trusted and are written with zeros. The following command must be entered on the transport interfaces so that they trust and not write over the DSCP values of the inbound IP packets.

```
mls qos trust dscp
```

Establishing Unidirectional 10-GE Links to the Dhubs

In this example, there are two 10-GE unidirectional connections between the headend and Dhub switches. The first is a multihop connection from Headend to DHub_Sw_A and DHub_Sw_B. The second is a point-to-point connection between Headend and DHub_Sw_C.

The multihop connection uses a split-optics 10-GE interface on DHub_Sw_A; the receive side of the interface terminates the unidirectional connection from Headend, and the transmit side initiates a second unidirectional connection to DHub_Sw_B. To configure more than one unidirectional subnet on the split-optics interface, you must use two VLANs and a trunk. This requires a VLAN on the Headend side of the 10-GE connection.

The following is configured on Headend.

Step 1 In global configuration mode, add the VLAN to the VLAN database.

```
vlan 1690
```

Step 2 Turn off STP for the VLAN. This allows the interface to come up immediately as soon as the link is up.

```
no spanning-tree vlan 1690
```

Step 3 Create the VLAN interface.

```
interface Vlan1690
 description Video traffic to/from DHub_Sw_A
```

Step 4 Associate the VLAN with the Video VRF.

```
ip vrf forwarding Video
```

Step 5 Assign the interface an IP address.

```
ip address 192.168.169.1 255.255.255.252
```

Step 6 Disable the sending of ICMP protocol-unreachable and host-unreachable messages. When enabled, host-unreachable messages are sent from the VLAN to the source if the VLAN is unable to deliver packets to the ultimate destination—because it knows of no route to the destination address.

```
no ip unreachables
```

Now that VLAN 1960 has been created, the unidirectional 10-GE interface can be configured as a trunk, which carries traffic for that VLAN.

The following is configured on Headend.

Step 1 Create the Layer 2 trunk interface and assign it to VLAN 1690. Configure the trunk for 802.1Q encapsulation with no negotiation.

```
interface TenGigabitEthernet7/1
 description UDL1: Video traffic to DHub_Sw_A (TenGig1/1)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1690
 switchport mode trunk
 switchport nonegotiate
```

Step 2 Configure the interface as a unidirectional send-only interface.

```
unidirectional send-only
```

Step 3 Turn off Weighted Random Early Discard (WRED) on Tx Queue 2. This enables tail drop in the event of oversubscription.

```
no wrr-queue random-detect 2
```

The configuration for this 10-GE link is less complex, because it is a point-to-point Layer 3 connection with no split optics.

Step 1 Configure the Layer 3 unidirectional interface between Headend and DHub_Sw_C, and associate it with the Video VRF.

```
interface TenGigabitEthernet7/3
 description UDL3: Video traffic to DHub_Sw_C (TenGig1/1)
 ip vrf forwarding Video
 ip address 192.168.169.9 255.255.255.252
```

Step 2 Configure the interface as a unidirectional send-only interface.

```
unidirectional send-only
```

Step 3 Turn off Weighted Random Early Discard (WRED) on Tx Queue 2. This enables tail drop in the event of over-subscription.

```
no wrr-queue random-detect 2
```

Establishing GRE Tunnels to the Dhubs

In this example, two GRE tunnels are required between the headend and Dhub switches. The first is the return path for the multihop connection from Headend to DHub_Sw_A, and the second is the return path for the point-to-point connection between Headend and DHub_Sw_C. Loopback interfaces (rather than physical interfaces) are used as endpoints of the tunnels, because loopback interfaces never go down, and each tunnel requires its own unique set of endpoints.

The following establishes the first GRE tunnel. This is the receive path for the unidirectional 10-GE interface between Headend and DHub_Sw_A. This trunk interface is associated with VLAN 1690.

The following is configured on Headend.

Step 1 Create a loopback interface to serve as the tunnel endpoint on Headend.

```
interface Loopback1
 description Endpoint for Tunnel1
 ip address 10.10.10.10 255.255.255.255
```

Note For the tunnel to be established, the loopback interface must be advertised in the global OSPF routing process.

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

```
interface Tunnel1
 description Vlan1690 Rx from DHub_Sw_A
 no ip address
```

Step 3 Configure the source and destination endpoints of the tunnel. The destination endpoint is on DHub_Sw_A.

```
tunnel source Loopback1
tunnel destination 11.11.11.11
```

Step 4 Configure UDLR for the tunnel. This tunnel represents the receive side of VLAN 1690.

```
tunnel udlr receive-only Vlan1690
```

Step 5 Associate the VLAN with the Video VRF.

```
ip vrf forwarding Video
```

The following establishes the second tunnel. This is the receive path for the unidirectional 10-GE interface between Headend and DHub_Sw_C.

Step 1 Create a loopback interface to serve as the tunnel endpoint on Headend.

```
interface Loopback3
 description Endpoint for Tunnel3
 ip address 14.14.14.14 255.255.255.255
```

Note For the tunnel to be established, the loopback interface must be advertised in the global OSPF routing process.

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

```
interface Tunnel3
 description UDL3 Rx from DHub_Sw_C
 no ip address
```

Step 3 Configure the source and destination endpoints of the tunnel. The destination endpoint is on DHub_Sw_C.

```
tunnel source Loopback3
tunnel destination 15.15.15.15
```

Step 4 Configure UDLR for the tunnel. This tunnel represents the receive side of TenGigabitEthernet7/3.

```
tunnel udlr receive-only TenGigabitEthernet7/3
```

Step 5 Associate the VLAN with the Video VRF table.

```
ip vrf forwarding Video
```

Configuring Dhub A

Dhub A consists of a Dhub switch (DHub_Sw_A), a QAM switch (QAM_Sw_A) with Cisco uMG9850 modules, and Cisco uMG9820 gateways. Refer to Figure 3-1 on page 3-2.

This section addresses the following:

- Confirming Hardware
- Establishing Quality of Service (QoS)
- Enabling OSPF and VRF-lite for Video-over-IP Traffic
- Enabling OSPF and VRF-lite for Video-over-IP Traffic
- Enabling OSPF for Non-video Traffic
- Establishing Interfaces

For a complete configuration example, see DHub_Sw_A Configuration in Appendix B, “Sample Configurations for Dhub Switches.”

Confirming Hardware

Before proceeding, it is beneficial to use the **show modules** command to confirm the hardware components and their versions for each switch.

The following is executed on DHub_Sw_A.

Step 1 Confirm hardware.

```
DHub_Sw_A# show modules

Mod Ports Card Type                                Model
--- ----- ---------------------------------------- ------------------
  1    4  CEF720 4 port 10-Gigabit Ethernet      WS-X6704-10GE
  3    8  8 port 1000mb GBIC Enhanced QoS        WS-X6408A-GBIC
  5    2  Supervisor Engine 720 (Active)         WS-SUP720-BASE


Mod Sub-Module                  Model              Hw
--- --------------------------- ------------------ -------
  1 Distributed Forwarding Card WS-F6700-DFC3A     2.1
  5 Policy Feature Card 3       WS-F6K-PFC3BXL     1.2
  5 MSFC3 Daughterboard         WS-SUP720          2.1
```

Establishing Quality of Service (QoS)

DHub_Sw_A receives traffic from Headend that has already been marked at the ingress points, so the transport ports on this Dhub switch are configured to trust the incoming DSCP values. This Dhub has a high-speed data ingress point, so the data entering here must be marked with the appropriate DSCP values.

The following is configured on DHub_Sw_A.

Step 1 In global configuration mode, enable QoS.

```
mls qos
```

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

In this configuration, only one type of traffic enters the network on DHub_Sw_A. Therefore, only one access list is defined to identify high-speed data traffic.

```
ip access-list extended acl_high_speed_data
 remark Identify high speed data traffic.
 permit ip 192.168.168.16 0.0.0.3 any
```

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

```
class-map match-all class_high_speed_data
 match access-group name acl_high_speed_data
```

Step 4 Create a policy map to set the DSCP value of the class created in Step 3.

```
policy-map setDSCP
 description Mark DSCP values for the different types of traffic.
 class class_high_speed_data
 set dscp default
```

Step 5 Change the default DSCP-to-CoS mapping. (See Establishing Quality of Service (QoS), page 3-4, for more information.)

```
mls qos map dscp-cos 32 to 5
```

Step 6 Apply the policy map to the high-speed data ingress interface GigabitEthernet3/4.

```
service-policy input setDSCP
```

Step 7 Configure all non-ingress transport interfaces to trust the incoming DSCP markings, to maintain the DSCP marking at the network ingress interface.

These interfaces are GigabitEthernet3/1, GigabitEthernet3/2, and TenGigabitEthernet1/1.

```
mls qos trust dscp
```

Enabling OSPF and VRF-lite for Video-over-IP Traffic

All interfaces that carry video traffic are put into a VRF routing table. For DHub_Sw_A, this includes the 10-GEs links from Headend, as well as to DHub_Sw_B and the QAM interfaces.

The following is configured on DHub_Sw_A.

Step 1 Define the VRF routing table.

The following command creates a VRF routing table and a Cisco Express Forwarding (CEF) table, both named “Video.” The **rd** command defines a route distinguisher, which can be in the form of *ASN:nn*, *IP-address:nn*, or *arbitrary-number:nn*.

```
ip vrf Video
 description Video traffic received from Headend
 rd 1000:2
```

Step 2 Associate all Layer 3 interfaces that carry video traffic with the VRF table defined in Step 1.

These interfaces are VLANs 1690 and 1694, Port-channel1, and GigabitEthernet3/8. An interface cannot be assigned to both the “Video” VRF routing table and the global routing table at the same time.

```
ip vrf forwarding Video
```

Caution Be aware that executing this command on an interface removes the IP address if it was previously configured.

Step 3 Create the OSPF process and associate it with the VRF defined in Step 1.

```
router ospf 100 vrf Video
 log-adjacency-changes
 capability vrf-lite
 network 192.168.160.0 0.0.0.255 area 0
 network 192.168.169.0 0.0.0.7 area 0
```

Note To configure passive interfaces in the OSPF process associated with the Video VRF, include the **passive-interface** command in the global OSPF process.

Enabling OSPF for Non-video Traffic

All interfaces that carry non-video traffic are put into the global routing table. For DHub_Sw_A this includes the high-speed data ingress port, the 1-GE transport interfaces that carry this traffic, and the loopback interfaces.

The following is configured on DHub_Sw_A.

Step 1 Define a second OSPF routing process to route non-video traffic.

```
router ospf 101
 log-adjacency-changes
 passive-interface default
 no passive-interface Vlan1690
 no passive-interface Vlan1694
 no passive-interface GigabitEthernet3/1
 no passive-interface GigabitEthernet3/2
 network 11.11.11.11 0.0.0.0 area 0
 network 12.12.12.12 0.0.0.0 area 0
 network 192.168.168.0 0.0.0.31 area 0
```

Note To configure passive interfaces in the OSPF process associated with the Video VRF, include the **passive-interface** command in the global OSPF process.

Establishing Interfaces

This section addresses the following:

Establishing a GE Interface for High-Speed Data

In this example, high-speed data enters DHub_Sw_A through a Layer 3 interface. The following steps detail the configuration of the GE interface.

Note Although Release 2.0 supports a multiservice architecture, interface configurations for VoIP, high-speed data, and VoD OOB equipment are beyond the scope of this solution. Vendor- and equipment-specific resources should be used to configure these interfaces properly.

The following is configured on DHub_Sw_A.

Step 1 Configure the Layer 3 interface.

```
interface GigabitEthernet3/4
 description BDL42: High speed data
 ip address 192.168.168.17 255.255.255.252
```

Step 2 Turn off Cisco Discovery Protocol.

```
no cdp enable
```

Step 3 Apply the “setDSCP” service policy that marks DSPC values in the inbound IP packets. (See DSCP Features and Values Used in Release 2.0, page 2-20.)

```
service-policy input setDSCP
```

Establishing Bidirectional 1-GE Links to Headend and DHub_Sw_B

In this example, there are two 1-GE connections between DHub_Sw_A and the other switches. One is to Headend, and the other is to DHub_Sw_B. These connections carry VoIP and high-speed data, as well as VoD OOB, OSPF, and ARP traffic. All traffic on these interfaces is part of the global routing table, except for the GRE tunnels that provide the return paths for the 10-GE unidirectional links. The configuration for GigabitEthernet3/1 is shown below, with GigabitEthernet3/2 configured similarly.

The following is configured on DHub_Sw_A.

Step 1 Configure the Layer 3 interface.

```
interface GigabitEthernet3/1
```

```
 description BDL1: Non-video traffic to/from Headend (Gig2/15)
 ip address 192.168.168.2 255.255.255.252
```

Step 2 Because the DSCP values are marked at the ingress interfaces, the DSCP values of the inbound IP packets can be trusted on the transport interfaces. By default, these DSCP values are not trusted and are written with zeros. The following command must be entered on the transport interfaces so that they trust and do not write over the DSCP values of the inbound IP packets.

```
mls qos trust dscp
```

Establishing Unidirectional 10-GE Links to Headend and DHub_Sw_B

In this example, there are two 10-GE unidirectional connections between Dhub_Sw_A and the other switches. The first is a receive-only link from Headend, and the second is a send-only link to DHub_Sw_B. Both of these connect to DHub_Sw_A at a single split-optics interface. (See Multihop Video, page 2-13.) To configure more than one unidirectional subnet on the split-optics interface, two VLANs and a trunk must be used.

The following is configured on DHub_Sw_A.

Step 1 In global configuration mode, add the VLANs to the VLAN database.

```
vlan 1690
vlan 1694
```

Step 2 Turn off STP for the VLANs.

This allows the interfaces to come up immediately as soon as the link is up.

```
no spanning-tree vlan 1690
no spanning-tree vlan 1694
```

Step 3 Create the VLAN interface for the unidirectional link from Headend, and associate the VLAN with the Video VRF.

```
interface Vlan1690
 description Video traffic to/from Headend
 ip vrf forwarding Video
 ip address 192.168.169.2 255.255.255.252
```

Step 4 Create the VLAN interface for the unidirectional link to DHub_Sw_B, and associate the VLAN with the Video VRF.

```
interface Vlan1694
 description Video traffic to/from DHub_Sw_B
 ip vrf forwarding Video
 ip address 192.168.169.5 255.255.255.252
```

Step 5 Create the Layer 2 trunk interface and allow both VLAN 1690 and VLAN 1694 to be routed on it.

Configure the trunk for 802.1Q encapsulation with no negotiation.

```
interface TenGigabitEthernet1/1
 description UDL1 Rx from Headend, UDL2 Tx to DHub_Sw_B
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1690,1694
 switchport mode trunk
 switchport nonegotiate
```

Note An “allowed” VLAN is one that can be on the trunk.

Step 6 Configure the interface to trust the inbound DSCP value in the IP packets.

```
mls qos trust dscp
```

Step 7 Turn off Weighted Random Early Discard (WRED) on Tx Queue 2. This enables tail drop in the event of over-subscription.

```
no wrr-queue random-detect 2
```

Establishing GRE Tunnels to Headend and DHub_Sw_B

In this example, there are two GRE tunnels on DHub_Sw_A. The first is the return path for the unidirectional 10-GE link from Headend, and the second is the return path for the 10-GE link to DHub_Sw_B. Loopback interfaces (rather than physical interfaces) are used as endpoints of the tunnels, because loopback interfaces never go down, and each tunnel requires its own unique set of endpoints.

The following establishes the first GRE tunnel on DHub_Sw_A. This is the transmit path for the unidirectional VLAN 1690.

The following is configured on DHub_Sw_A.

Step 1 Create a loopback interface to serve as the tunnel endpoint on Headend.

```
interface Loopback1
 description Endpoint for Tunnel1
 ip address 11.11.11.11 255.255.255.255
```

Note For the tunnel to be established, the loopback interface must be advertised in the global OSPF routing process.

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

```
interface Tunnel1
 description Vlan1690 Tx to Headend
 no ip address
```

Step 3 Configure the source and destination endpoints of the tunnel. The destination endpoint is on Headend.

```
tunnel source Loopback1
tunnel destination 10.10.10.10
```

Step 4 Configure UDLR for the tunnel. This tunnel represents the transmit side of VLAN 1690.

```
tunnel udlr send-only Vlan1690
```

Step 5 Associate the tunnel with the Video VRF.

```
ip vrf forwarding Video
```

Step 6 Configure the tunnel to carry ARP responses to requests received on the unidirectional 10-GE interface.

```
tunnel udlr address-resolution
```

The following establishes the second GRE tunnel on DHub_Sw_A. This is the receive path for the unidirectional VLAN 1694.

The following is configured on DHub_Sw_A.

Step 1 Create a loopback interface to serve as the tunnel endpoint on Headend.

```
interface Loopback2
 description Endpoint for Tunnel2
 ip address 12.12.12.12 255.255.255.255
```

Note For the tunnel to be established, the loopback interface must be advertised in the global OSPF routing process.

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

```
interface Tunnel2
 description Vlan1694 Rx from DHub_Sw_B
 no ip address
```

Step 3 Configure the source and destination endpoints of the tunnel. The destination endpoint is on DHub_Sw_B.

```
tunnel source Loopback2
tunnel destination 13.13.13.13
```

Step 4 Configure UDLR for the tunnel. This tunnel represents the receive side of VLAN 1694.

```
tunnel udlr receive-only Vlan1694
```

Step 5 Associate the tunnel with the Video VRF table.

```
ip vrf forwarding Video
```

Establishing Bidirectional 1-GE Links to QAM_Sw_A

In this example, there are two Cisco uMG9850s in Dhub A. These reside in the Cisco Catalyst 4507 switch named QAM_Sw_A, and receive traffic from DHub_Sw_A over two 1-GE links grouped into an EtherChannel. The DHub_Sw_A side of the EtherChannel is configured as a Layer 3 interface, and the QAM_Sw_A side is configured as a Layer 2 interface. The two Cisco uMG9850s are configured as hosts in the same VLAN as the EtherChannel. (See Implementing and Configuring the Cisco uMG9850 QAM Module, page 3-43.)

The following is configured on DHub_Sw_A.

Step 1 Configure the two 1-GE interfaces that are members of the EtherChannel, and associate these interfaces with the Video VRF. When the **channel-group 1 mode on** command is entered, the switch adds an interface for Port-channel1 to the running configuration.

```
interface GigabitEthernet3/6
```

```
 description BDL51: Video traffic to/from QAM_Sw_A (Gig3/1)
 ip vrf forwarding Video
 no ip address
 channel-group 1 mode on

interface GigabitEthernet3/7
 description BDL52: Video traffic to/from QAM_Sw_A (Gig4/14)
 ip vrf forwarding Video
 no ip address
 channel-group 1 mode on
```

Step 2 Configure the Layer 3 EtherChannel that was created as a result of Step 1. Associate the EtherChannel with the Video VRF.

```
interface Port-channel1
 description Video traffic to/from QAM_Sw_A (Gig3/1,Gig4/14)
 ip vrf forwarding Video
 ip address 192.168.160.1 255.255.255.240
```

Establishing the Cisco_uMG9850 GE Interfaces

In this example, interfaces are established to the Cisco uMG9850 modules in QAM_Sw_A.

The following is configured on DHub_Sw_A.

Step 1 In global configuration mode, add the VLAN to the VLAN database.

```
vlan 160
```

Step 2 Create the VLAN interface.

```
interface Vlan160
 description Video traffic to/from DHub_A_S7
 ip address 192.168.160.2 255.255.255.240
```

Step 3 Configure the two 1-GE interfaces as Layer 2 ports, and then configure them to be part of the EtherChannel. When the **channel-group 1 mode on** command is entered, the switch adds an interface for Port-Channel 1 to the running configuration.

```
interface GigabitEthernet3/1
 description BDL51: Video traffic to/from DHub_A_S7 (Gig3/6)
 switchport access vlan 160
 channel-group 1 mode on

interface GigabitEthernet4/14
 description BDL52: Video traffic to/from DHub_A_S7 (Gig3/7)
 switchport access vlan 160
 channel-group 1 mode on
```

Step 4 The Port-Channel interface was created as a result of Step 3, and needs only a description.

```
interface Port-channel1
 description Video traffic to/from DHub_A_S7 (Gig3/6,Gig3/7)
 switchport
 switchport access vlan 160
```

Step 5 Configure the Cisco uMG9850s with IP addresses and associate them with the VLAN created in Step 1. The two Cisco uMG9850s are located in switch slots 4 and 7.

```
video 4 route Vlan160 ip-address 192.168.160.3
```

```
video 7 route Vlan160 ip-address 192.168.160.4
```

Caution Because the two Cisco uMG9850s reside in the same VLAN, avoid removing either module while it is receiving data. Otherwise, the remaining module is flooded by data destined for the removed module. If the sum of the traffic destined for both modules is greater than 1 Gbps, the interface can be oversubscribed and packets are dropped.

Establishing Bidirectional 1-GE Links to the Cisco uMG9820

In this example, bidirectional 1-GE links are established to the Cisco uMG9820 gateway in Dhub A.

The following is configured on DHub_Sw_A.

Step 1 Configure the Layer 3 interface and associate it with the Video VRF.

```
interface GigabitEthernet3/8
 description BDL53: Video traffic to/from uMG9820
 ip vrf forwarding Video
 ip address 192.168.160.17 255.255.255.252
```

Step 2 Disable the sending of ICMP protocol-unreachable and host-unreachable messages.

```
no ip unreachables
```

Step 3 Configure the interface not to negotiate the 1-GE interface.

```
speed nonegotiate
```

Configuring Dhub B

Dhub B consists of a Dhub switch (DHub_Sw_B), a QAM switch (QAM_Sw_B) with Cisco uMG9850 modules, and Cisco uMG9820 gateways. Refer to Figure 3-1 on page 3-2.

This section addresses the following:

- Confirming Hardware
- Establishing Quality of Service (QoS)
- Enabling OSPF and VRF-lite for Video-over-IP Traffic
- Enabling OSPF for Non-video Traffic
- Establishing Interfaces

For a complete configuration example, see DHub_Sw_B Configuration in Appendix B, "Sample Configurations for Dhub Switches."

Confirming Hardware

Before proceeding, it is beneficial to use the **show modules** command to confirm the hardware components and their versions for each switch.

The following is executed on DHub_Sw_B.

Step 1 Confirm hardware.

```
DHub_SW_B# show modules

Mod Ports Card Type                                Model
--- ----- ---------------------------------------- ------------------
  1    4  CEF720 4 port 10-Gigabit Ethernet      WS-X6704-10GE
  2   24  CEF720 24 port 1000mb SFP              WS-X6724-SFP
  3    8  8 port 1000mb GBIC Enhanced QoS        WS-X6408A-GBIC
  4   48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45
  5    2  Supervisor Engine 720 (Active)         WS-SUP720-BASE


Mod Sub-Module                  Model              Hw
--- --------------------------- ------------------ -------
  1 Distributed Forwarding Card WS-F6700-DFC3A     2.2
  2 Centralized Forwarding Card WS-F6700-CFC       1.2
  5 Policy Feature Card 3       WS-F6K-PFC3BXL     1.2
  5 MSFC3 Daughterboard         WS-SUP720          2.0
```

Establishing Quality of Service (QoS)

DHub_Sw_B receives from DHub_Sw_A and DHub_Sw_C traffic that has already been marked at the ingress points, so these transport ports are configured to trust the incoming DSCP values. There are VoIP, high-speed data, and VoD OOB traffic ingress ports at this Dhub, so the data entering these ports must be marked with the appropriate DSCP values.

The following is configured on DHub_Sw_B.

Step 1 In global configuration mode, enable QoS.

```
mls qos
```

Step 2 Create access lists to identify the different service types in the network. In this configuration, three types of traffic enter the network on DHub_Sw_B.

```
ip access-list extended acl_VoD_OOB
 remark Identify VoD OOB traffic.
 permit ip 192.168.166.0 0.0.0.255 any
ip access-list extended acl_VoIP
 remark Identify VoIP traffic.
 permit ip 192.168.164.0 0.0.0.255 any
ip access-list extended acl_high_speed_data
 remark Identify high speed data.
 permit ip 192.168.168.20 0.0.0.3 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_high_speed_data
 match access-group name acl_high_speed_data
class-map match-all class_VoD_OOB
 match access-group name acl_VoD_OOB
```

Step 4 Create a policy map to set the DSCP value of the class created in Step 3.

```
policy-map setDSCP
 description Mark DSCP values for the different types of traffic
 class class_VoIP
 set dscp ef
 class class_VoD_OOB
 set dscp cs3
 class class_high_speed_data
 set dscp default
```

Step 5 Change the default DSCP-to-CoS mapping. (See Establishing Quality of Service (QoS), page 3-4, for more information.)

```
mls qos map dscp-cos 32 to 5
```

Step 6 Apply the policy map to ingress interfaces GigabitEthernet3/4, GigabitEthernet 4/44, and GigabitEthernet4/48.

```
service-policy input setDSCP
```

Step 7 Configure all non-ingress transport interfaces to trust the incoming DSCP markings, to maintain the DSCP marking at the network ingress interface.

```
mls qos trust dscp
```

Enabling OSPF and VRF-lite for Video-over-IP Traffic

All interfaces that carry video traffic are put into a VRF routing table. For DHub_Sw_B, this includes the 10-GE link from DHub_Sw_A and the QAM interfaces.

The following is configured on DHub_Sw_B.

Step 1 Define the VRF routing table.

The following command creates a VRF routing table and a Cisco Express Forwarding (CEF) table, both named "Video." The **rd** command defines a route distinguisher, which can be in the form of *ASN:nn*, *IP-address:nn*, or *arbitrary-number:nn*.

```
ip vrf Video
 description Video traffic received from Headend
 rd 1000:3
```

Step 2 Associate all Layer 3 interfaces that carry video traffic with the VRF defined in Step 1.

Apply the following to interfaces VLAN 1694, Port-channel2, and GigabitEthernet3/8. An interface cannot be assigned to both the Video VRF routing table and the global routing table at the same time.

```
ip vrf forwarding Video
```

Caution Be aware that executing this command on an interface removes the IP address if it has been configured.

Step 3 Create the OSPF process and associate it with the VRF defined in Step 1.

```
router ospf 100 vrf Video
 log-adjacency-changes
 capability vrf-lite
 network 192.168.161.0 0.0.0.255 area 0
 network 192.168.169.0 0.0.0.15 area 0
```

Note To configure passive interfaces in the OSPF process associated with the Video VRF table, include the **passive-interface** command in the global OSPF process.

Enabling OSPF for Non-video Traffic

All interfaces that carry non-video traffic are put into the global routing table. For DHub_Sw_B this includes the VoIP, high-speed data, and VoD OOB ingress ports, the transport interfaces that carry this traffic, and the loopback interfaces.

The following is configured on DHub_Sw_B.

Step 1 Define a second OSPF routing process to route non-video traffic.

```
router ospf 101
 log-adjacency-changes
 passive-interface default
 no passive-interface Vlan1694
 no passive-interface GigabitEthernet3/2
 no passive-interface GigabitEthernet3/3
 network 13.13.13.13 0.0.0.0 area 0
 network 192.168.164.0 0.0.0.255 area 0
 network 192.168.166.0 0.0.0.255 area 0
 network 192.168.168.0 0.0.0.63 area 0
```

Note To configure passive interfaces in the OSPF process associated with the Video VRF, include the **passive-interface** command in the global OSPF process.

Establishing Interfaces

This section addresses the following:

Establishing Interfaces for VoIP, High-Speed Data, and VoD OOB Traffic

In this example, high-speed data enters DHub_Sw_B through a Layer 3 interface, and VoIP and VoD OOB traffic enter through Layer 2 interfaces. The following steps detail the configuration of the 1-GE interfaces.

Note Although Release 2.0 supports a multiservice architecture, interface configurations for VoIP, high-speed data, and VoD OOB equipment are beyond the scope of this solution. Vendor- and equipment-specific resources should be used to configure these interfaces properly.

The following is configured on DHub_Sw_B.

Step 1 Configure the Layer 3 interface for high-speed data. Because this is an ingress interface, the “setDSCP” service policy is applied to the interface input.

```
interface GigabitEthernet3/4
 description BDL43: High speed data
 ip address 192.168.168.21 255.255.255.252
 no cdp enable
 service-policy input setDSCP
```

Step 2 Configure the VLAN and Layer 2 interface for VoIP traffic.

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

```
vlan 164
```

b. Create the VLAN interface.

```
interface Vlan164
 description VoIP traffic
 ip address 192.168.164.1 255.255.255.0
```

c. Create the Layer 2 interface.

Because this is an ingress interface, the “setDSCP” service policy is applied to the interface input.

```
interface FastEthernet4/44
 description VoIP traffic
 no ip address
 switchport
 switchport access vlan 164
 switchport mode access
 spanning-tree portfast
```

```
 service-policy input setDSCP
```

Step 3 Configure the VLAN and Layer 2 interface for VoD OOB traffic.

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

```
vlan 166
```

b. Create the VLAN interface.

```
interface Vlan166
 description VoD OOB traffic
 ip address 192.168.166.1 255.255.255.0
```

c. Create the Layer 2 interface.

Because this is an ingress interface, the "setDSCP" service policy is applied to the interface input.

```
interface FastEthernet4/48
 description VoD OOB traffic
 no ip address
 speed 100
 duplex full
 switchport
 switchport access vlan 166
 switchport mode access
 no cdp enable
 spanning-tree portfast
 service-policy input setDSCP
```

Establishing Bidirectional 1-GE Links to DHub_Sw_A and DHub_Sw_C

In this example, there are two 1-GE connections between DHub_Sw_B and the other switches. One is to DHub_Sw_A, and the other to DHub_Sw_C. These connections carry VoIP, high-speed data, VoD OOB, OSPF, and ARP traffic. All traffic on these interfaces is part of the global routing table, except for the GRE tunnels that provide the return paths for the 10-GE unidirectional links. The configuration for GigabitEthernet3/2 is shown below, with GigabitEthernet3/3 configured similarly.

The following is configured on DHub_Sw_B.

Step 1 Configure the Layer 3 interface.

```
interface GigabitEthernet3/2
 description BDL2: Non-video traffic to/from DHub_Sw_A (Gig3/2)
 ip address 192.168.168.6 255.255.255.252
```

Step 2 Since the DSCP values are marked at the ingress interfaces, the DSCP values of the inbound IP packets can be trusted on the transport interfaces. By default, these DSCP values are not trusted and are written with zeros. The following command must be entered on the transport interfaces so that they trust and do not write over the DSCP values of the inbound IP packets.

```
mls qos trust dscp
```

Establishing a Unidirectional 10-GE Link from DHub_Sw_A

In this example, there is one 10-GE unidirectional connection coming from Dhub_Sw_A. This is the second link of the multihop configuration between Headend, DHub_Sw_A, and DHub_Sw_B. The split-optics configuration on DHub_Sw_A requires a trunk with two unidirectional VLANs, so the 10-GE connection on DHub_Sw_B is configured similarly.

The following is configured on DHub_Sw_B.

Step 1 In global configuration mode, add the VLAN to the VLAN database.

```
vlan 1694
```

Step 2 Turn off STP for the VLAN. This allows the interfaces to come up immediately as soon as the link is up.

```
no spanning-tree vlan 1694
```

Step 3 Create the VLAN interface for the 10-GE unidirectional link from DHub_Sw_A and associate the VLAN with the Video VRF. Disable ICMP IP-unreachables messages from being sent from the interface.

```
interface Vlan1694
 description Video traffic to/from DHub_Sw_A
 ip vrf forwarding Video
 ip address 192.168.169.6 255.255.255.252
 no ip unreachables
```

Step 4 Create the Layer 2 trunk interface and assign it to VLAN 1694. Configure the trunk for 802.1Q encapsulation with no negotiation.

```
interface TenGigabitEthernet1/1
 description UDL2: Video traffic from DHub_Sw_A (TenGig1/1)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1694
 switchport mode trunk
 switchport nonegotiate
 no keepalive
```

Step 5 Configure the interface as a unidirectional receive-only interface.

```
unidirectional receive-only
```

Step 6 Configure the interface to trust the inbound DSCP value in the IP packets.

```
mls qos trust dscp
```

Establishing a GRE Tunnel to DHub_Sw_A

In this example, there is one GRE tunnel on DHub_Sw_B. This is the return path for the unidirectional 10GigE link from DHub_Sw_A. Loopback interfaces (rather than physical interfaces) are used as endpoints of the tunnels, because loopback interfaces never go down, and each tunnel requires it own unique set of endpoints.

The following is configured on DHub_Sw_B.

Step 1 Create a loopback interface to serve as the tunnel endpoint on Headend.

```
interface Loopback2
 description Endpoint for Tunnel2
```

```
ip address 13.13.13.13 255.255.255.255
```

Note For the tunnel to be established, the loopback interface must be advertised in the global OSPF routing process.

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

```
interface Tunnel2
 description UDL2 Tx to DHub_Sw_A
 no ip address
```

Step 3 Configure the source and destination endpoints of the tunnel. The destination endpoint is on DHub_Sw_A.

```
tunnel source Loopback2
tunnel destination 12.12.12.12
```

Step 4 Configure UDLR for the tunnel. This tunnel represents the transmit side of VLAN 1694.

```
tunnel udlr send-only Vlan1694
```

Step 5 Associate the tunnel with the Video VRF.

```
ip vrf forwarding Video
```

Step 6 Configure the tunnel to carry ARP responses to requests received on the unidirectional 10-GE interface.

```
tunnel udlr address-resolution
```

Establishing Bidirectional 1-GE Links to QAM_Sw_B Hosting the Cisco uMG9850

In this example, there is one Cisco uMG9850 in DHub_B. It resides in the Cisco Catalyst 4507 switch named QAM_Sw_B and receives traffic from DHub_Sw_B through two 1-GE links grouped into an EtherChannel. The DHub_Sw_B side of the EtherChannel is configured as a Layer 3 interface, and the QAM_Sw_B side is configured as a Layer 2 interface. The Cisco uMG9850 is configured as a host in the same VLAN as the EtherChannel.

The following is configured on DHub_Sw_B.

Step 1 Configure the two 1-GE interfaces that are members of the EtherChannel. Associate these interfaces with the Video VRF. When the **channel-group 2 mode on** command is entered, the switch adds an interface for Port-channel 2 to the running configuration.

```
interface GigabitEthernet3/6
 description BDL54: Video traffic to/from QAM_Sw_B (Gig3/2)
 ip vrf forwarding Video
 no ip address
 channel-group 2 mode on

interface GigabitEthernet3/7
 description BDL55: Video traffic to/from QAM_Sw_B (Gig5/14)
 ip vrf forwarding Video
 no ip address
 channel-group 2 mode on
```

Step 2 Configure the Layer 3 EtherChannel that was created as a result of Step 1. Associate the EtherChannel with the Video VRF.

```
interface Port-channel2
 description Video traffic to/from QAM_Sw_B (Gig3/2,Gig5/14)
 ip vrf forwarding Video
 ip address 192.168.161.1 255.255.255.240
```

Establishing the Cisco uMG9850 1-GE Interfaces on QAM_Sw_B

The following is configured on DHub_Sw_B.

Step 1 In global configuration mode, add the VLAN to the VLAN database.

```
vlan 161
```

Step 2 Create the VLAN interface.

```
interface Vlan161
 description Video traffic to/from DHub_B_S7
 ip address 192.168.161.2 255.255.255.240
```

Step 3 Configure the two 1-GE interfaces as Layer 2 ports, and then configure them to be part of the EtherChannel. When the **channel-group 2 mode on** command is entered, the switch adds an interface for Port-channel 2 to the running configuration.

```
interface GigabitEthernet3/2
 description BDL54: Video traffic to/from DHub_B_S7 (Gig3/6)
 switchport access vlan 161
 channel-group 2 mode on

interface GigabitEthernet5/14
 description BDL55: Video traffic to/from DHub_B_S7 (Gig3/7)
 switchport access vlan 161
 channel-group 2 mode on
```

Step 4 The Port-channel interface was created as a result of Step 3, and needs only a description.

```
interface Port-channel2
 description Video traffic to/from DHub_B_S7 (Gig3/6,Gig3/7)
 switchport
 switchport access vlan 161
```

Step 5 Configure the Cisco uMG9850 with an IP address and associate it with the VLAN created in Step 1. The Cisco uMG9850 is located in slot 5. See Implementing and Configuring the Cisco uMG9850 QAM Module, page 3-43.

```
video 5 route Vlan161 ip-address 192.168.161.3
```

Establishing Bidirectional 1-GE Links to the Cisco uMG9820

The following is configured on DHub_Sw_B.

Step 1 Configure the Layer 3 interface and associate it with the Video VRF table.

```
interface GigabitEthernet3/8
 description BDL56: Video traffic to/from uMG9820
 ip vrf forwarding Video
 ip address 192.168.161.17 255.255.255.252
```

Step 2 Disable the sending of ICMP protocol-unreachable and host-unreachable messages.

```
no ip unreachables
```

Step 3 Configure the interface not to negotiate the 1-GE interface.

```
speed nonegotiate
```

Configuring Dhub C

Dhub C consists of a Dhub switch (DHub_Sw_C), a QAM switch (QAM_Sw_C) with Cisco uMG9850 modules, and a Cisco uMG9820 gateway. Refer to Figure 3-1 on page 3-2.

This section addresses the following:

- Confirming Hardware
- Establishing Quality of Service (QoS)
- Enabling OSPF and VRF-lite for Video-over-IP Traffic
- Enabling OSPF for Non-video Traffic
- Establishing Interfaces

For a complete configuration example, see DHub_Sw_C Configuration in Appendix B, "Sample Configurations for Dhub Switches."

Confirming Hardware

Before proceeding, it is beneficial to use the **show modules** command to confirm the hardware components and their versions for each switch.

The following is executed on Headend.

Step 1 Confirm hardware.

```
DHub_Sw_C# show modules

Mod Ports Card Type                                Model
--- ----- ---------------------------------------- ------------------
  1    4  CEF720 4 port 10-Gigabit Ethernet      WS-X6704-10GE
  3   16  SFM-capable 16 port 1000mb GBIC        WS-X6516A-GBIC
  4   48  CEF720 48 port 10/100/1000mb Ethernet  WS-X6748-GE-TX
  5    2  Supervisor Engine 720 (Active)         WS-SUP720-BASE

Mod Sub-Module                  Model              Hw
--- --------------------------- ------------------ -------
  1 Distributed Forwarding Card WS-F6700-DFC3A     2.1
  4 Centralized Forwarding Card WS-F6700-CFC       2.0
  5 Policy Feature Card 3       WS-F6K-PFC3BXL     1.2
  5 MSFC3 Daughterboard         WS-SUP720          2.1
```

Establishing Quality of Service (QoS)

DHub_Sw_C receives from Headend and DHub_Sw_B traffic that has already been marked at the ingress points, so these transport ports are configured to trust the incoming DSCP values. There is a VoIP ingress point at this Dhub, so the data entering these points must be marked with the appropriate DSCP values.

The following is configured on DHub_Sw_C.

Step 1 In global configuration mode, enable QoS.

```
mls qos
```

Step 2 Create an access list to identify the VoIP traffic entering the network.

```
ip access-list extended acl_VoIP
 remark Identify VoIP traffic.
 permit ip 192.168.165.0 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
```

Step 4 Create a policy map to set the DSCP value of the class created in Step 3.

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

Step 5 Change the default DSCP-to-CoS mapping. (See Establishing Quality of Service (QoS), page 3-4, for more information.)

```
mls qos map dscp-cos 32 to 5
```

Step 6 Apply the policy map to the ingress interface GigabitEthernet3/4.

```
service-policy input setDSCP
```

Step 7 Configure all non-ingress transport interfaces to trust the incoming DSCP markings, to maintain the DSCP marking at the network ingress interface.

```
mls qos trust dscp
```

Enabling OSPF and VRF-lite for Video-over-IP Traffic

All interfaces that carry video traffic are put into a VRF routing table. For DHub_Sw_C, this includes the 10-GE link from Headend and the QAM interfaces.

The following is configured on DHub_Sw_C.

Step 1 Step 1 Define the VRF routing table.

The following command creates a VRF routing table and a Cisco Express Forwarding (CEF) table, both named “Video.” The **rd** command defines a route distinguisher, which can be in the form of *ASN:nn*, *IP-address:nn*, or *arbitrary-number:nn*.

```
ip vrf Video
 description Video traffic received from Headend
 rd 1001:4
```

Step 2 Associate all Layer 2 interfaces that carry video traffic with the VRF defined in Step 1.

This applies to TenGigabitEthernet1/1 and GigabitEthernet4/1. An interface cannot be assigned to both the “Video” VRF routing table and the global routing table at the same time.

```
ip vrf forwarding Video
```

Caution Be aware that executing this command on an interface removes the IP address if it has been previously configured.

Step 3 Create the OSPF process and associate it with the VRF defined in Step 1.

```
router ospf 100 vrf Video
 log-adjacency-changes
 capability vrf-lite
 network 192.168.162.0 0.0.0.255 area 0
 network 192.168.169.0 0.0.0.31 area 0
```

Note To configure passive interfaces in the OSPF process associated with the Video VRF, include the **passive-interface** command in the global OSPF process.

Enabling OSPF for Non-video Traffic

All interfaces that carry non-video traffic are put into the global routing table. For DHub_Sw_C this includes the VoIP ingress port, the transport interfaces that carry this traffic, and the loopback interfaces.

The following is configured on DHub_Sw_C.

Step 1 Define a second OSPF routing process to route non-video traffic.

```
router ospf 101
 log-adjacency-changes
 passive-interface default
 no passive-interface TenGigabitEthernet1/1
 no passive-interface GigabitEthernet3/1
 no passive-interface GigabitEthernet3/3
 network 15.15.15.15 0.0.0.0 area 0
 network 192.168.165.0 0.0.0.255 area 0
 network 192.168.168.8 0.0.0.7 area 0
```

Note To configure passive interfaces in the OSPF process associated with the Video VRF, include the **passive-interface** command in the global OSPF process.

Establishing Interfaces

This section addresses the following:

- Establishing an Interface for VoIP Traffic
- Establishing Bidirectional 1-GE Links to Headend and DHub_Sw_B
- Establishing a Unidirectional 10-GE Link from Headend
- Establishing a GRE Tunnel to Headend
- Establishing Bidirectional 1-GE Links to QAM_Sw_C Hosting the Cisco uMG9850
- Establishing the Cisco uMG9850 1-GE Interfaces on QAM_Sw_C
- Establishing Bidirectional 1-GE Links to the Cisco uMG9820

Establishing an Interface for VoIP Traffic

In this example, VoIP traffic enters DHub_Sw_C through a Layer 2 interface. The following steps detail the configuration of the 1-GE interface.

Note Although Release 2.0 supports a multiservice architecture, interface configurations for VoIP, high-speed data, and VoD OOB equipment are beyond the scope of this solution. Vendor- and equipment-specific resources should be used to configure these interfaces properly.

The following is configured on DHub_Sw_C.

Step 1 Configure the VLAN and Layer 2 interface for VoIP traffic.

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

```
vlan 165
```

b. Create the VLAN interface.

```
interface Vlan165
 description VoIP traffic
 ip address 192.168.165.1 255.255.255.0
```

c. Create the Layer 2 interface.

Because this is an ingress interface, the “setDSCP” service policy is applied to the interface input.

```
interface GigabitEthernet4/46
 description VoIP traffic
 no ip address
 load-interval 30
 switchport
 switchport access vlan 165
 switchport mode access
 spanning-tree portfast
 service-policy input setDSCP
```

Establishing Bidirectional 1-GE Links to Headend and DHub_Sw_B

In this example, there are two 1-GE connections between DHub_Sw_C and the other switches. One is to Headend and the other is to DHub_Sw_B. These connections carry VoIP, high-speed data, VoD OOB, OSPF, and ARP traffic. All traffic on these interfaces is part of the global routing table, except for the GRE tunnels that provide the return paths for the 10-GE unidirectional links. The configuration for GigabitEthernet3/1 is shown below, with GigabitEthernet3/3 configured similarly.

The following is configured on DHub_Sw_C.

Step 1 Configure the Layer 3 interface.

```
interface GigabitEthernet3/1
 description BDL3: Non-video traffic to/from Headend (Gig2/16)
 ip address 192.168.168.14 255.255.255.252
```

Step 2 Because the DSCP values are marked at the ingress interfaces, the DSCP values of the inbound IP packets can be trusted on the transport interfaces. By default, these DSCP values are not trusted and are written with zeros. The following command must be entered on the transport interfaces so that they trust and do not write over the DSCP values of the inbound IP packets.

```
mls qos trust dscp
```

Establishing a Unidirectional 10-GE Link from Headend

In this example, there is only one 10-GE unidirectional link from Headend to DHub_Sw_C.

The following is configured on DHub_Sw_C. For a complete configuration example of this and the other QAM switches, see Appendix C, "Sample Configurations for QAM Switches."

Step 1 Configure the Layer 3 interface.

```
interface TenGigabitEthernet1/1
 description UDL3: Video traffic from Headend (TenGig7/3)
```

Step 2 Associate the VLAN with the Video VRF.

```
ip vrf forwarding Video
```

Step 3 Assign the interface an IP address.

```
ip address 192.168.169.10 255.255.255.252
```

Step 4 Configure the interface as a unidirectional receive-only interface.

```
unidirectional receive-only
```

Step 5 Configure the interface to trust the inbound DSCP value in the IP packets.

```
mls qos trust dscp
```

Establishing a GRE Tunnel to Headend

In this example, there is one GRE tunnel on DHub_Sw_C. This is the return path for the unidirectional 10-GE link from Headend. Loopback interfaces (rather than physical interfaces) are used as endpoints of the tunnels, because loopback interfaces never go down, and each tunnel requires it own unique set of endpoints.

The following is configured on DHub_Sw_C.

Step 1 Create a loopback interface to serve as the tunnel endpoint on Headend.

```
interface Loopback3
 description Endpoint for Tunnel 3
 ip address 15.15.15.15 255.255.255.255
```

Note For the tunnel to be established, the loopback interface must be advertised in the global OSPF routing process.

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

```
interface Tunnel3
  description UDL3 Tx to Headend
  no ip address
```

Step 3 Configure the source and destination endpoints of the tunnel. The destination endpoint is on DHub_Sw_A.

```
tunnel source Loopback3
tunnel destination 14.14.14.14
```

Step 4 Configure UDLR for the tunnel. This tunnel represents the transmit side of TenGigabitEthernet1/1.

```
tunnel udlr send-only TenGigabitEthernet1/1
```

Step 5 Associate the tunnel with the Video VRF table.

```
ip vrf forwarding Video
```

Step 6 Configure the tunnel to carry ARP responses to requests received on the unidirectional 10-GE interface.

```
tunnel udlr address-resolution
```

Establishing Bidirectional 1-GE Links to QAM_Sw_C Hosting the Cisco uMG9850

In this example, there is one Cisco uMG9850 in Dhub C. It resides in the Cisco Catalyst 4507 switch named QAM_Sw_C and receives traffic from DHub_Sw_C through a Layer 3 1-GE link. The Layer 3 link carries traffic for only one Cisco uMG9850. The DHub_Sw_C side of the link is configured as a Layer 3 interface, and the QAM_Sw_C side is configured as a Layer 2 interface. The Cisco uMG9850 is configured as a host in the VLAN used for the Layer 2 interface.

The following is configured on DHub_Sw_C.

Step 1 Configure the 1-GE interface, and associate the interface with the Video VRF.

```
interface GigabitEthernet4/1
 description BDL57: Video traffic to QAM_Sw_C (Gig6/13)
 ip vrf forwarding Video
 ip address 192.168.162.1 255.255.255.248
```

Establishing the Cisco uMG9850 1-GE Interfaces on QAM_Sw_C

The following is configured on QAM_Sw_C.

Step 1 In global configuration mode, add the VLAN to the VLAN database.

```
vlan 162
```

Step 2 Create the VLAN interface.

```
interface Vlan162
 description Video traffic to/from DHub_C_S8
 ip address 192.168.162.2 255.255.255.248
```

Step 3 Configure the 1-GE interface as a Layer 2 port.

```
interface GigabitEthernet6/13
 description BDL57: Video traffic to/from DHub_C_S8 (Gig4/1)
```

```
 switchport access vlan 162
```

Step 4 Configure the Cisco uMG9850 with an IP address and associate it with the VLAN created in Step 1.

The Cisco uMG9850 is located in slot 6. See Implementing and Configuring the Cisco uMG9850 QAM Module, page 3-43.

```
video 6 route Vlan162 ip-address 192.168.162.3
```

Establishing Bidirectional 1-GE Links to the Cisco uMG9820

The following is configured on DHub_Sw_C.

Step 1 Configure the Layer 3 interface and associate it with the Video VRF.

```
interface GigabitEthernet4/3
 description BDL59: VoD traffic to uMG9820
 ip vrf forwarding Video
 ip address 192.168.162.17 255.255.255.252
```

Step 2 Disable the sending of ICMP protocol-unreachable and host-unreachable messages.

```
no ip unreachables
```

Step 3 Configure the interface not to negotiate the 1-GE interface.

```
speed nonegotiate
```

Implementing Optics

The following discussions present a variety of options for implementing the various optics and supervisory channels for the Cisco Gigabit-Ethernet Optimized VoD Solution:

- Implementing the Cisco ONS 15216 FlexLayer
- Implementing the Cisco ONS 15216 OSC-1510

Implementing the Cisco ONS 15216 FlexLayer

The Cisco Gigabit-Ethernet Optimized VoD Solution uses the Cisco ONS 15216 FlexLayer Solution to provide modular support for a variety of optical functions. A single chassis accommodates multiplex/demultiplex filters, combiner or splitter assemblies, and optical attenuators, providing for easy and cost-effective expansion.

Note For more about features and the various modules, refer to "Data Sheet: Cisco ONS 15216 Metropolitan Dense Wavelength Division Multiplexing 100-GHz FlexLayer Filter Solution," at the following URL:

http://www.cisco.com/warp/public/cc/pd/olpl/metro/15200/prodlit/flexp_ds.htm

To install and use the Cisco ONS 15216 FlexLayer and its various components, refer to *Cisco ONS 15216 FlexLayer User Guide, Release 1.0*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/ong/15216/flxlyr10/

Implementing the Cisco ONS 15216 OSC-1510

The Cisco ONS 15216 OSC-1510 can be used in the Cisco Gigabit-Ethernet Optimized VoD Solution to provide optical supervisory channel (OSC) communication to a site without the need for an optical add/drop multiplexer (OADM), (erbium-doped fiber amplifier (EDFA), or multiplexing/demultiplexing at that site. This passive single-channel 100-GHz device allows you to add or drop a protected OSC wavelength in each direction at any point of a DWDM link. The dropped supervisory channel is then sent to the receive gigabit interface converter (GBIC) port on the switch.

Note For a description of the Cisco ONS 15216 OSC-1510 and installation instructions, refer to *Cisco ONS 15216 OSC-1510 User Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/ong/15216/osc.htm

Although that document refers to the Cisco Catalyst 2950 switch, the Cisco ONS 15216 OSC-1510 is compatible with the Cisco Catalyst 4500 series switches.

Implementing and Configuring Cisco Video Gateways

Implementing and Configuring the Cisco uMG9820 QAM Gateway

For information on preparing, installing, starting, and configuring the Cisco uMG9820 QAM Gateway, as well as release notes, refer to Cisco uMG9820 QAM Gateway at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/vod/umg9820/index.htm

Implementing and Configuring the Cisco uMG9850 QAM Module

The four Cisco uMG9850s in our example design can be configured similarly. Two are in QAM_Sw_A, and one each is in QAM_Sw_B and QAM_Sw_C. The configurations are minimal, insofar as they mainly use default values without video management features.

For information on preparing, installing, and configuring the Cisco uMG9850 QAM Module, as well as release notes, refer to Cisco uMG9850 QAM Module at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/vod/umg9850/index.htm

This section discusses the general and QAM-specific configuration of the Cisco uMG9850 module in slot 4 of QAM_Sw_A. The I-GE links from QAM_Sw_A to DHub_Sw_A and the IP address of the module are described in Establishing the Cisco_uMG9850 GE Interfaces, page 3-24.

The following is configured on the Cisco uMG9850 in slot 4 of QAM_Sw_A.

Step 1 Confirm the location of modules in the QAM switch.

```
Switch# show modules

Chassis Type : WS-C4507R

Power consumed by backplane : 40 Watts

Mod Ports Card Type                                Model
---+-----+--------------------------------------+-----------------
 1     2  1000BaseX (GBIC) Supervisor(active)    WS-X4013+
 3     6  1000BaseX (GBIC)                       WS-X4306-GB
 4    15  24QAM 1SFP(1000BaseX) 1RJ45(10/100/100 WS-X4712-QAM-24B
 7    15  24QAM 1SFP(1000BaseX) 1RJ45(10/100/100 WS-X4712-UMG9850

 M Hw  Fw           Sw
--+--------------------------------+---+------------+----------------
 1 2.1 12.1(20r)EW1 12.1(20040401:01
 3 2.2
 4 5.9 12.1(20V)EWV 12.1(20V)EWV1
 7 1.0 12.1(20V)EWV 12.1(20V)EWV1
```

Step 2 Modify the default UDP port mapping.

The default mapping uses UDP port 57377 for program 1 on QAM4/1.1, and 57409 for program 1 on QAM4/1.2.

Tip To see a complete map, use the **show interface** *interface.qam* **video portmap** command.

The following command modifies the UDP port mapping to use 257 for program 1 on QAM4/1.1 and 513 for program 1 on QAM4/1.2

```
video 4 emulation-mode 24-qam-number
```

Note For more information, see the discussion of default and modified UDP port mappings in *Configuring the Cisco uMG9850 QAM Module* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/vod/umg9850/index.htm

Step 3 Configure the QAM frequencies.

The QAM*x*/*x*.1 and QAM*x*/*x*.2 outputs share an upconverter, so the frequencies are 6 MHz apart. Configuring one channel automatically configures the other. Here we configure the lower channel.

```
interface QAM4/11/1
 viceo frequency 771000000
```

The default values are not shown in the running configuration. The default QAM channel power level is 50 dBmV, and the defafult modulation format is 256QAM. To verify these settings, use the **show interface qam** *interface.qam* **video** command.

Step 4 (Optional) You can use the ASI monitor interface to monitor the MPEG transport streams before they are processed by the QAM modulator and upconverters. Only one QAM channel can be monitored at a time.

```
interface ASI4/15
 keepalive 5
 video route qam 4/1/1
```