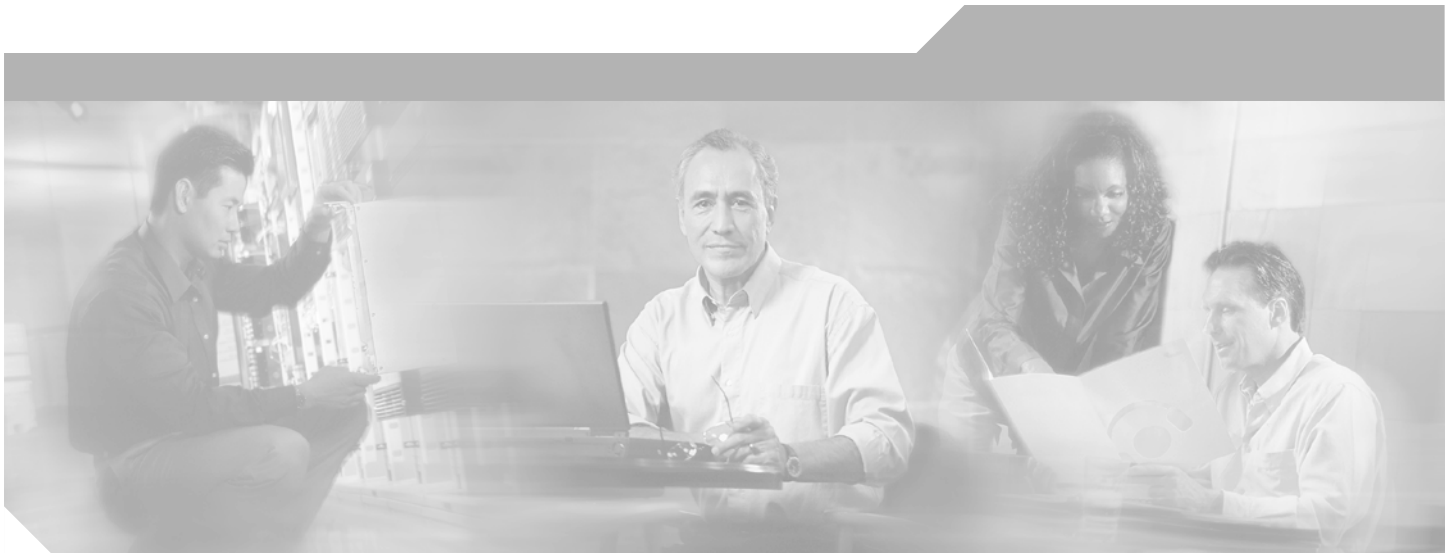


Cisco Gigabit-Ethernet Optimized Video Networking Solution for Cable Design and Implementation Guide, Release 3.0

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-8189-01

Cisco Gigabit-Ethernet Optimized Video Networking Solution for Cable Design and Implementation Guide, Release 3.0

Preface

This preface explains the objectives, intended audience, and organization of the Cisco Gibabit-Ethernet Optimized Video Networking Solution for Cable, Release 3.0.

Note "Release 3.0" is used to indicate that this solution follows in the development path provided by the Cisco Gigabit-Ethernet Optimized VoD Solution, while providing support beyond VoD—for digital broadcast and digital simulcast—in a hybrid fiber coax (HFC) infrastructure.

The solution supports major enhancements to established video networking architectures, particularly in the areas of IP multicast (IPmc) distribution for digital broadcast video services. This release includes the addition of architectural components to support resilient IPmc forwarding over existing IP transport networks, specifically, between encoders/multiplexers and ad splicers/groomers, as well as between ad splicers (in conjunction with a video groomer function) and edge QAM devices.

The preface also defines the conventions used to convey instructions and information, available related documentation, and the process for obtaining Cisco documentation and technical assistance.

This preface presents the following major topics:

Document Version and Solution Release

This is the first version of this document, which covers Release 3.0 of the Cisco Gibabit-Ethernet Optimized Video Networking Solution for Cable.

Document History

Document Version	Date	Notes
1	02/06/2006	This document was first released.

Document Objectives and Scope

This guide describes the architecture, the components, and the processes necessary for the design and implementation of the Cisco Gibabit-Ethernet Optimized Video Networking Solution for Cable, Release 3.0.

Note Third-party components are included in this architecture for completeness. Although some third-party components were used to test and validate this solution, Cisco cannot guarantee the performance and capability of that equipment. Refer to third-party documentation for details, as well as for support-related issues.

Audience

The target audience for this document is assumed to have basic knowledge of and experience with the installation and acceptance of the products covered by this solution. See Chapter 1, “Solution Overview.”

In addition, it is assumed that the user understands the procedures required to upgrade and troubleshoot optical transport systems and Ethernet switches and routers, with emphasis on Cisco 7600 series routers and Cisco Catalyst 6500 series switches.

Document Organization

The major sections of this document are as follows:

Section	Title	Major Topics
Chapter 1	Solution Overview	Introduces solution architecture and scope and components.
Chapter 2	Solution Architecture and Optimizations	Discusses hub and IP architecture, optimizing video and service availability, QoS, and upgrading and managing the network

Chapter 3	Implementing the Solution	Describes the configuration and implementation of the solution.
Chapter 4	Monitoring and Troubleshooting	Provides an introduction to monitoring and troubleshooting the Cisco equipment used in the solution.
Appendix A	Sample Configurations	Provides example configurations.

Related Documentation

Solution Documentation

This document, and *Release Notes for Cisco Gigabit-Ethernet Optimized Video Networking Solution for Cable, Release 1.0*, are available under the following URL:

http://www.cisco.com/univercd/cc/td/doc/solution/

Switch and Router Documentation

Documentation resources for the Cisco Catalyst 6500 series switches and the Cisco 7600 series routers are available below.

Cisco Catalyst 6500 Series Switches

For all hardware and software documentation for this series, go to the following URL:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Cisco 7600 Series Routers

For all hardware and software documentation for this series, go to the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html

Cisco IOS Documentation

Cisco IOS Release 12.2(18)SXF

For information specific to Cisco IOS Release 12.2(18)SXF, see Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.2SX, at the following URL:

http://www.cisco.com/en/US/partner/products/hw/switches/ps708/products_configuration_guide_book09186a00801609ea.html

Note In this solution, the Cisco 7600 series and the Cisco Catalyst 6500 series with the same supervisor engine (the Supervisor Engine 720) function identically, although the Cisco 7600 series was the subject of testing and is referenced predominantly.

Optical Component Documentation

Cisco DWDM GBICs

- *Cisco DWDM Gigabit Interface Converter Installation Guide*
  www.cisco.com/univercd/cc/td/doc/product/gbic_sfp/gbic_doc/78_15574.htm
- *Cisco Dense Wavelength Division Multiplexing GBICs Compatibility Matrix*
  www.cisco.com/univercd/cc/td/doc/product/gbic_sfp/gbic_doc/ol_4604.htm

Note Other references are provided as appropriate throughout this document.

Document Conventions

Command descriptions use the following conventions:

boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ **x** | **y** | **z** }	Alternate keywords are grouped in braces and separated by vertical bars.
[**x** | **y** | **z**]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use the following conventions:

`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.[1]
`italic screen` font	Arguments for which you supply values are in *`italic screen`* font.
——→	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control. For example, the key combination ^D in a screen display means hold down the Control key while you press the D key.

< >	Nonprinting characters, such as passwords, are in angle brackets in contexts where italic font is not available.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

1. As this document makes use of annotated configurations, the rigorous use of boldface type to indicate what the user must enter is relaxed.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Tips use the following conventions:

Tip Means the following information *will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Solution Overview

This chapter presents the following major topics:

Solution Description and Scope

The Cisco Gibabit-Ethernet Optimized Video Networking Solution for Cable, Release 3.0, encompasses major enhancements to existing video solutions in the areas of IP multicast (IPmc) distribution for analog and digital broadcast video services in an HFC infrastructure. This solution includes architectural components to support resilient IPmc forwarding over the existing IP transport network between the encoders/multiplexers, ad splicers and video groomers, and edge QAM (EQAM) devices.

Note Because ad splicers commonly integrate the video grooming function, the term “ad splicer” is understood here as incorporating that function.

The objective of the solution is to provide an architectural basis for the migration of digital and analog broadcast streams onto a converged IP transport network. This converged network includes transmission support for all services—VoD, digital and analog broadcast video, high-speed data (HSD), and VoIP.

The following improvements to the reference architecture are addressed:

- Maximizing service availability

  Includes consideration of source and path diversity, path resiliency, and control-plane rate limiting
- Optimizing video flows

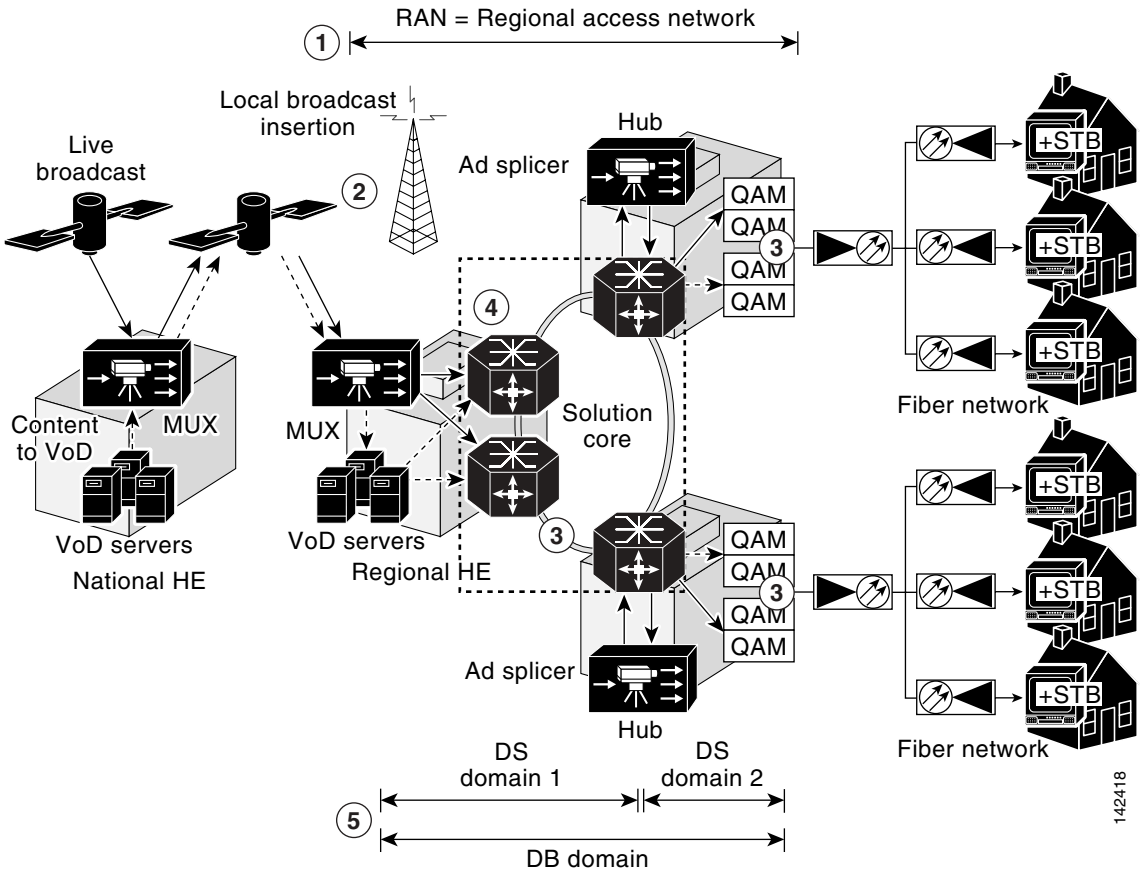
  Includes consideration of digital simulcast (DS) and digital broadcast (DB) flows and flow domains
- Optimizing quality of service (QoS)
- Upgrading the network

  Includes migrating from Any Source Multicast (ASM) to Source Specific Multicast (SSM)
- Using network management options
- Monitoring and troubleshooting

Generic Architecture and Scope

Figure 1-1 illustrates the reference architecture, a subset of a large network architecture as may be developed and maintained by a multiple services operator (MSO).

Figure 1-1 Reference Architecture



1. The focus of the solution is the regional access network (RAN), which serves a metropolitan area, and is made up of many market networks. A national headend (HE) pulls content from different sources and grooms traffic into transport streams for distribution (over satellite) to the regional headends.

   The solution focuses on the IP multicast (IPmc) distribution of digital simulcast (DS) and digital broadcast (DB) flows over the RAN.

   A single market network is depicted above. Each market network includes two aggregation routers (ARs) in the HE, with hub routers (HRs) in the hubs. Two source routers (SRs) (not shown) aggregate services that originate in the HE.

Note For simplicity, only one HR is shown in each hub. There are normally two HRs in a hub, to provide redundancy.

2. Regional headends in the RAN receive content from satellite and off-air antennas.

Multiple converged regional area networks (RANs) are connected to the Internet through peering points provided by an Internet service provider. RANs can be interconnected to each other, as well as to a national HE, through a QoS-enabled backbone.

A backbone can be used to interconnect RANs as well as other MSOs. The backbone makes it possible for the MSO to migrate off the satellite links and onto terrestrial network for transport stream distribution.

3. VoD and broadcast video traffic is switched or routed onto separate DWDM paths and to separate EQAM devices.
4. There are multiple sources for the broadcast and VoD traffic.
5. There are effectively three broadcast IPmc domains:

   Two DS domains:

   - One from the regional HE multiplexer to the ad splicer/groomer in the hub
   - One from the ad splicer in the hub to the EQAM devices

   One DB domain—from the regional HE to the EQAM devices

Because the regional HEs are dispersed throughout the RAN/market networks, and broadcast streams from each headend are forwarded across those networks, QoS is important to the delivery of the broadcast service.

Bidirectional 10-GE links are used for broadcast video, high-speed data (HSD), and VoIP services. These interconnects may consist of several 10-GE links bonded together by means of static portchannels or Layer 3 equal-cost multipath (ECMP) load balancing.

Note ECMP load balancing was not tested in this solution.

Separate links and routing protocols are used for VoD and broadcast services. Specifically, VoD uses dedicated 10-GE interfaces that are configured with static routing.

Solution Components

Cisco Equipment

The Cisco Gibabit-Ethernet Optimized Video Networking Solution for Cable, Release 3.0, consists of core Cisco components that are tested, documented, and fully supported by Cisco in the context of the solution. Table 1-1 on page 1-4 lists the Cisco hardware and software components that were tested.

Table 1-1 Cisco Hardware and Software Tested

Routers	Hardware	Software Release	Hardware Version
Cisco 7606, Cisco Catalyst 6509[1]	WS-SUP720	12.2(18)SXF	2.0, 2.3
	WS-SUP720-3BXL		4.3
	WS-SUP720-BASE		3.0
	WS-X6704-10GE		1.2, 2.2
	WS-X6724-SFP		2.2, 2.3
	WS-X6748-GE-TX		1.4, 2.1
	WS-F6700-DFC3A	N/A	2.1, 2.2
	WS-F6700-DFC3BXL		4.0, 5.0, 5.2
	WS-F6K-PFC3BXL		1.2, 1.6

1. In this solution, the Cisco 7600 series and the Cisco Catalyst 6500 series with the same supervisor engine function identically.

Third-Party Equipment

Third-party equipment is included to test the functionality of the Cisco routers/switches used in the solution. Table 1-1 on page 1-4 lists the third-party hardware and software components that were tested.

Note Cisco cannot guarantee support for the third-party equipment used in the solution.

Table 1-2 Third-Party Hardware and Software Tested

Component	Vendor and Model	Software Release	Hardware Release
Multiplexer, Ad splicer/groomer	Terayon DM 6400	netcp4.1 build 16	N/A
	BigBand Networks BMR1200	suite 2.11.1	
Edge QAM device	Motorola SEM v8	6.1.1	N/A

Solution Architecture and Optimizations

This chapter presents the following major topics:

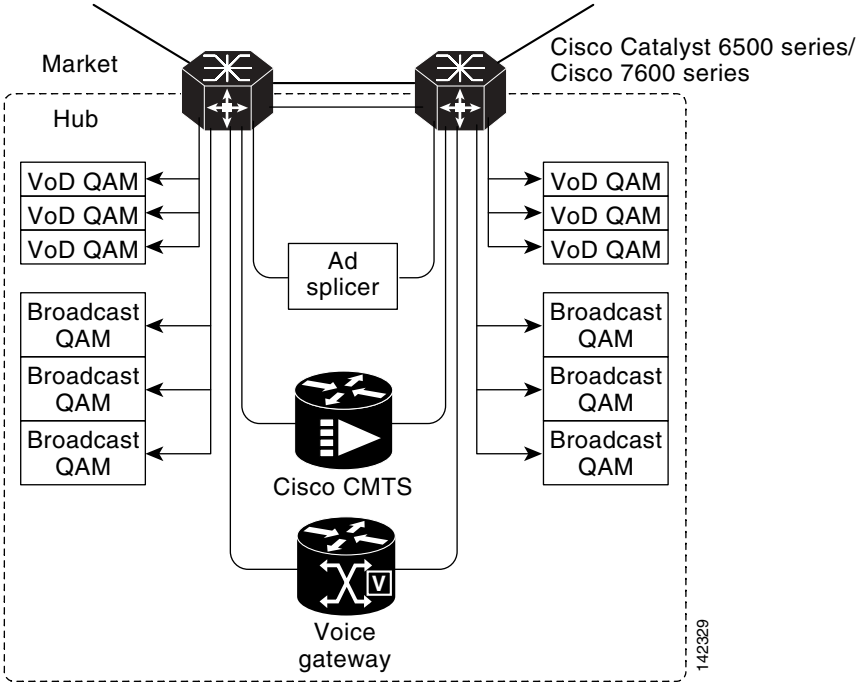
Hub and IP Architecture

Hub Architecture

Figure 2-1 on page 2-2 illustrates the hub architecture. Ad splicers receive incoming broadcast streams, and splice ads and groom streams into the proper channel lineup for a given neighborhood. The ad splicer in this case is dual-homed.

Broadcast video, HSD, and VoIP trunks are bidirectional 10-GE links. All access links (to the Cisco CMTS, the ad splicer, voice gateways, or EQAM devices) are 1-GE links.

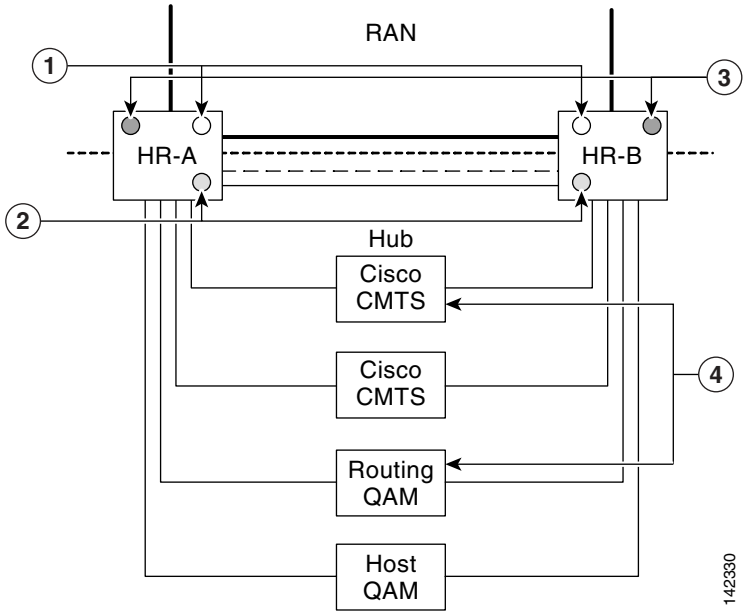
Figure 2-1 Hub Architecture



IP Architecture

Consider a network that is divided into two routing domains in the RAN (see Figure 2-2 on page 2-3). One routing domain consists of the loopback interfaces on the ARs and HRs, all physical interfaces on the ARs, and the trunk interfaces on the HRs. These are depicted as the links in (1) and the processes in (1) and (3). (Process 1 is the OSPF process for the RAN. Process 3 is the BGP process for the RAN.) The second routing domain consists of the remaining interfaces on the HRs and the IP addresses of the components in the hub (4). The HRs use OSPF (2) to inject a default route into the hub. Hub devices use OSPF (1) to advertise their loopback, link, and service routes to the HRs.

Figure 2-2 Routing Domains



1	OSPF process 1, area 0
2	OSPF process 2, area 1
3	BGP (iBGP[1])—Used to inject customer routes (statically defined on the Cisco 7600 series or Cisco Catalyst 6500 series into the RAN. Customer routes have next-hop router set to the loopback addresses of both routers.
4	Hub devices—Oblivious to routing architecture on the RAN. Hub devices see the defaults from the Cisco 7600 series or Cisco Catalyst 6500 series and other hub local routes.

1. Internal BGP. External BGP is referred to as eBGP.

As depicted in Table 2-1 on page 2-4, service routes (such as HSD customer prefixes from the Cisco CMTS and all DS/DB device addresses) are advertised in BGP by means of redistribution from the hub interior OSPF process 2. The redistributed prefixes have their next-hop addresses set to a RAN-advertised loopback, so that all service prefixes appear to the RAN to terminate at the HRs in Figure 2-2). If two routers are attached to a hub, then each router advertises its own and the other's hub loopback address, but sets the BGP next-hop addresses to its own hub loopback address.

Within the market network, the two ARs act as BGP route reflectors and all HRs act as route reflector clients. The ARs advertise all internal RAN BGP prefixes plus a default route. They do not advertise eBGP-learned prefixes.

Within the RAN, all ARs are peered with all other ARs. Loopback addresses are used as the router IDs.

Table 2-1 Service Route Configurations

HR-A Configuration	HR-B Configuration
interface loopback 1 ip address 30.0.0.1/32 ip address 30.0.0.2/32 secondary router ospf 2 network <Hub interfaces>[1] area 1 router ospf 1 network 30.0.0.1/32 area 0 network 30.0.0.2/32 area 0 network <RAN interfaces>[2] area 0 route-map hub-ospf-to-bgp permit 100 match ip address prefix-list hub-pfx set metric 100 set ip next-hop 30.0.0.1 router bgp 1 redistribute ospf 2 route-map hub-ospf-to-bgp	interface loopback 1 ip address 30.0.0.2/32 ip address 30.0.0.1/32 secondary router ospf 2 network <Hub interfaces> area 1 router ospf 1 network 30.0.0.2/32 area 0 network 30.0.0.1/32 area 0 network <RAN interfaces> area 0 route-map hub-ospf-to-bgp permit 100 match ip address prefix-list hub-pfx set metric 100 set ip next-hop 30.0.0.2 router bgp 1 redistribute ospf 2 route-map hub-ospf-to-bgp

1. Provide address, mask, and area for all hub interfaces.
2. Provide address, mask, and area for all RAN interfaces.

Understanding and Optimizing Video Flows

Overview

The video flows can be broken down into DS and DB flows. DS flows (prior to ad insertion) represent the capability of encoding all broadcast content (including analog streams) for transport across the IPmc network to the digital ad-insertion device. Following ad insertion, traffic flows from the ad splicers to the EQAMs. Original analog broadcast streams (digitized for IPmc transport) are converted back to analog streams at the EQAM device. DB flows (requiring no ad insertion) represent the capability of (1) unencrypting broadcast streams upon reception (from satellite or off the air), (2) sending all broadcast content across the IPmc network (unencrypted), and (3) reencrypting the streams at the EQAM device before sending content to the subscriber. There are primary and secondary sources for both DS and DB flows within the RAN.

Advertisements are spliced into live video streams by means of ad splicers. A single market may have as many as 40 ad zones, which are demographically grouped areas of a market that receive the same advertising content. A single hub can serve multiple ad zones. Because each ad splicer serves only a single ad zone, a hub with multiple ad zones contains a set of ad splicers for each ad zone. For example, if Hub A serves three ad zones and requires four splicers to cover the DS channel lineup, there is a total of 12 ad splicers in that hub (four for each of the three ad zones). Ad streams are delivered (by means of unicast) from ad sources in the RAN to the ad splicers in the hub over the bidirectional 10-GE interfaces.

Because of the current inability of the video edge equipment (QAM devices and ad splicers) to support IGMPv3, an ASM model of IPmc is generally being deployed today. The service provider can also deploy an SSM model using the SSM-mapping features supported on the Cisco 7600 series and the Cisco Catalyst 6500 series. Rendezvous points (RPs) are defined statically to provide deterministic flow

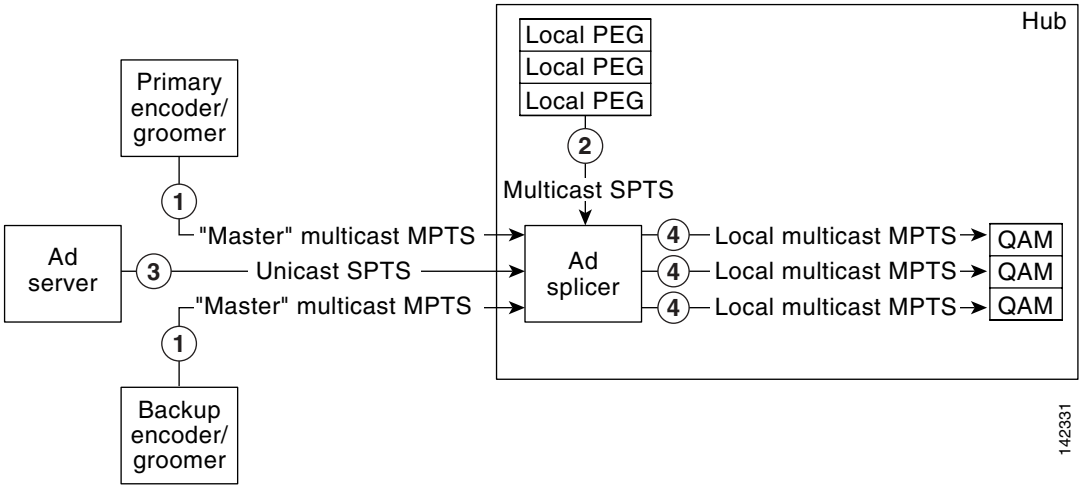
control across the RAN. The router closest to the source is the RP for that source—providing the added benefit of simplifying network operations and troubleshooting by maintaining the same path for shared and source multicast trees.

Note The transition from ASM to SSM is discussed in Upgrading the Network: Migrating from ASM to SSM, page 2-38.

DS Flows

DS flows originate from two sources (primary and secondary). Both flows are delivered to the ad splicers in each hub by means of multicast. The ad splicers splice the advertisement into the program streams before sending out the multicast traffic on a new multicast address to be delivered to the EQAM devices. DS flows can be seen as four component flows (see Figure 2-3 on page 2-5):

Figure 2-3 DS Flows



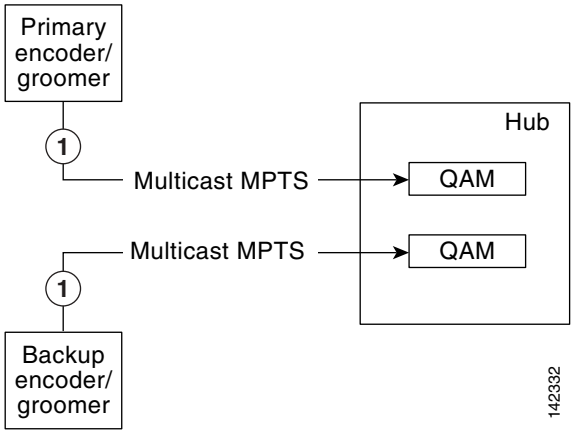
1	Generic “master” multiprogram transport stream (MPTS) multicast flows arrive from the market’s master headend(s) to ad splicers in each hub. DS master flows are typically comprised of 8 MPTS at 38 Mbps each, for a total network load of 304 Mbps. Markets likely have two DS master source locations, so that each hub receives two master flows, for a total of 608 Mbps.

2	Locally originated channels are single-program transport stream (SPTS) multicast flows from public, education, and government (PEG) access sources. A single site can have 50 to 100 PEG sources at 3.75 Mbps each.
3	Unicast advertisement video streams are dynamically fed into the video hubs from centralized ad servers. Standard definition (SD) ad insertion flows are sent at 3.75 Mbps. Conceivably hundreds of ad flows can simultaneously hit the RAN from the ad farm locations.
4	"Local" MPTS multicast flows that have had local advertisements digitally spliced into the master streams are combinations of the master MPTS flows and local PEG SPTS flows that have been rearranged to local channel lineups. Local flows stay entirely within a hub site and flow between the hub ad splicers and the EQAM devices. The aggregate bandwidth of the local MPTS flows is approximately the sum of flows 1 and 2 above.

DB Flows

As shown in Figure 2-4, DB flows originate from two sources (primary and secondary). Both flows are delivered to the EQAM devices in each hub by means of multicast. DB flows usually consist of 24 MPTS flows at 38 Mbps each, for a total network load of 912 Mbps.

Figure 2-4 DB Flows

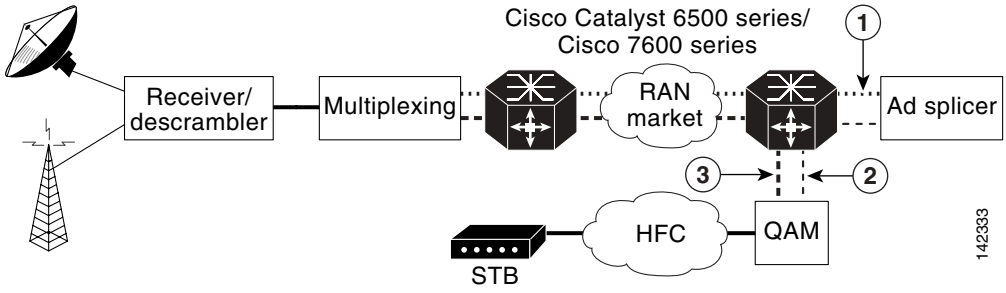


1	Generic "master" multiprogram transport stream (MPTS) multicast flows arrive from the market's master headend(s) to ad splicers in each hub. [For more detail, see description of (1) in Figure 2-3 on page 2-5.]

Flow Domains

The architecture for distributing broadcast video over the IP network includes breaking down IPmc into three different flow domains from the master HE to the customer, as illustrated in Figure 2-5.

Figure 2-5 IPmc Domains



1	DS flows (prior to ad splicing) stream from the master HEs to the ad splicer.
2	DS flows (following ad splicing) stream from the ad splicers to the EQAMs.
3	DB flows stream directly from the master HEs to the EQAM devices.

Note Two new multicast features are now available. For details, see Multicast Replication Mode Feature, page 3-18, and Local Egress Replication Feature, page 3-18.

Optimizing Service Availability

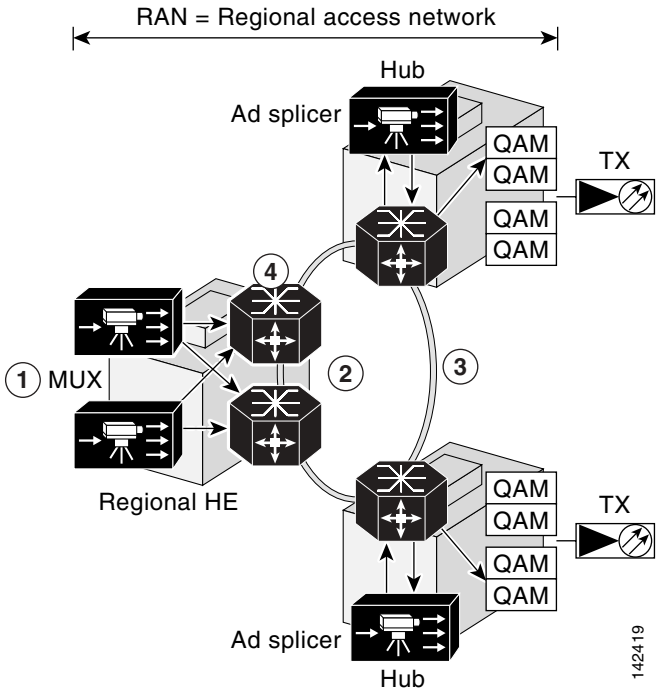
Broadcast video services are inherently real-time. Subscribers who experience an outage in the broadcast service cannot go back and continue where they left off when the outage is over. Also, broadcast services have much higher concurrent usage rates than other video services.

As such, broadcast video is given a high priority among subscriber services. (VoIP has the highest.) Thus the delivery of broadcast services must be highly available and reliable. The ultimate goal is to support hitless failover for IP and IPmc service. However, many customers initially support deploying IP and IPmc services with less than 1-second recovery. To support this, the architecture is being implemented to support resiliency in various places in the RAN.

All service-availability recommendations resulting from testing in this section are in support of Layer 2 and Layer 3 protocol interactions. (It is assumed that Layer 1 transport redundancy is orthogonal to this discussion.) Service availability is defined at the user interface: is there or is there not a picture on residential TV?

Figure 2-6 illustrates how diversity and resiliency, in conjunction with rate limiting, act to maintain high availability. The network links are engineered to 50% utilization. If traffic rates increase and are sustained above 70%, then additional trunks are added to the network.

Figure 2-6 Diversity and Resiliency with Rate Limiting



1	Duplicate sources provide source diversity.
2	Static mroutes, a digital video IGP (like EIGRP) or MBGP, with no shared links between sources, provides path diversity.
3	The use of PortChannel, with IGP-FC, provides path resiliency.
4	Control-plane rate limiting (using hardware rate limiters) protects CPU resources, helping to ensure service delivery.

The following diversity and resiliency topics are discussed below:

- Source Diversity
- Path Diversity
- Path Resiliency
- Hardware Rate Limiters

Source Diversity

In order to recover quickly from source failures, there are multiple (primary and secondary) satellite and off-air sources per RAN/market, as depicted previously. It is expected that the broadcast video sources (multiplexers and ad splicers) can source one or more IPmc groups per MPTS/SPTS. It is also expected that the IPmc receivers (ad splicers and EQAM devices) can support receiving the same transport stream from different IPmc groups. The intent is for the receiver to be able to identify a faulty stream from the primary source and “switch” immediately to the active secondary source.

Note A discussion of Any Source Multicast (ASM) mode and additional enhancements to provide a tertiary source using anycast Source Specific Multicast (SSM) mode is provided in Upgrading the Network: Migrating from ASM to SSM, page 2-38.

Establishing ad splicer redundancy is generally a "manual" process, whereby the ad splicers are configured in an N+1 design. When one ad splicer goes down, it is replaced by the backup ad splicer through a process that reconfigures the backup device with the configuration of the "downed" device. This process eliminates the need to do any reconfiguration of the EQAM itself.

Path Diversity

The purpose of having redundant sources in the RAN/market networks is to support service availability. However, service availability can be affected by least-cost path routing, because both sources may take the same path to a given destination. To alleviate this, the architecture includes three methods to separate the forwarding paths for different sources:

- Using Static mroutes
- Using MBGP
- Setting Preferred Routes in EIGRP

Using Static mroutes

Multicast routers maintain state about the incoming and outgoing interfaces for each (source, group) (S,G) pair. This state is used to decide which packets are to be discarded and which are to be forwarded. The table that the router maintains for holding this state information is called the multicast routing table. Each entry in this table corresponds to a unique (S,G) and is referred to as an mroute. Each mroute primarily contains four types of entries:

- The address of the multicast group
- The address of the corresponding source (or "*" for all sources)
- The incoming interface
- A list of outgoing interfaces.

In a ring configuration, the operator simply configures a static mroute to the primary source through the west interface, and a static mroute to the secondary source through the east interface. The following is the syntax of the **ip mroute** command:

[**no**] **ip mroute** *source mask* [*protocol as-number*] [**route-map** *map*] *rpf-address* | *interface* [*distance*]

One drawback to this option is that there is no ability to "reroute" to a given source in the event of a network failure.

Static mroutes must resolve "longest match" criteria, as well as have the lowest administrative distance (lower than that for PIM, BGP, and IGP).

Using MBGP

Multiprotocol Border Gateway Protocol (MBGP), on the other hand, is a bit more complex. MBGP requires the following guidelines:

- Every router in the RAN serves as a route reflector for both its upstream and downstream directly connected neighbor, making BGP "follow" the physical topology.
- Each route reflector must also set the next-hop attribute to itself.
- Interface peering must be used to avoid routing loops during link failure.
- Apply a specific policy in the IPv4 multicast address family on each BGP session, using the **set local-preference** command to set a preference for the source address (or addresses) at each hop.

Below is a sample configuration:

```
router bgp 100
 no bgp ipv4 uni default
 neighbor MCAST peer-group
 neighbor MCAST peer-group next-hop-self
 neighbor MCAST peer-group route-reflector-client
 neighbor <router 1> peer-group MCAST
 neighbor <router 2> peer-group MCAST
 address-family ipv4 multicast
  neighbor <router 1> activate
  neighbor <router 1> route-map UP-Policy in
  neighbor <router 2> activate
  neighbor <router 2> route-map DN-Policy in
!
route-map UP-Policy permit 10
 match ip address <primary source>
 set local-preference <number n>
!
route-map DN-Policy permit 10
 match ip address <secondary source>
 set local-preference <number m>
```

Setting Preferred Routes in EIGRP

Some MSOs currently use OSPF as the preferred IGP. OSPF (being a link-state protocol) does not support the ability to change the metric for an individual route. The solution needs a distance-vector routing protocol with a better administrative distance than OSPF; EIGRP is the logical choice. Table 2-2 lists the default administrative distance values of the protocols that Cisco supports.

Table 2-2 Default Administrative Distances for Supported Protocols

Route Source	Default Administrative Distance
Connected interface	0
Static route	1[1]
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
Open Shortest Path First (OSPF)	110
Intermediate System to Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140

Table 2-2 Default Administrative Distances for Supported Protocols

Route Source	Default Administrative Distance
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown	255[2]

1. Static route pointing is always 1, regardless of whether the pointing is to a next-hop IP address or to an outgoing interface.
2. If the administrative distance is 255, the router does not believe the source of that route and does not install the route in its routing table.

There are two primary methods for setting a preferred route in EIGRP:

- Use the **offset-list** command to modify the composite metric.
- Change the administrative distance.

Note For more information, see "Setting a Preferred Route by Influencing EIGRP Metrics," at the following URL: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800c2d96.shtml

Path Resiliency

Path resilience relies on the network's ability to reconverge to an alternate path for the following conditions:

- When there is a single link or node failure
- With multiple failures (separate link and node, or two links, or two nodes)

Note The failover of supervisor engines was not tested in this release of the solution.

PortChannel and Equal-Cost Multipath

There may be instances in which parallel paths are used to interconnect some aggregation routers and hub routers. PortChannel (or EtherChannel) facilitates the bundling of multiple links into a single Layer 3 logical interface. (The algorithm works best with a specific number of ports in the channel. The recommended numbers of ports are 2, 4, or 8.) Equal-cost multipath (ECMP) facilitates the bundling of multiple Layer 3 physical links.

There are things to consider:

- How is traffic load-balanced on the paths?
- What happens when one or two links in a path fail?

One advantage with PortChannel is the ability in Cisco IOS Release 12.2(18)SXF to use the EtherChannel Min-Link feature to specify a minimum number of ports for a PortChannel to be considered a valid path. This feature allows the user to set a minimum threshold for the number of links in an EtherChannel, so that if fewer than the specified number of links are available, the port channel interface fails over to a standby EtherChannel.

Note For information on how to implement this feature, see EtherChannel Min-Links Feature, page 3-17.

One advantage of ECMP is the ability to load balance based on (*,G) or (S,G) state. Another advantage of ECMP is its efficiency for handling IPmc replication.

However, there is no mechanism to "remove" an ECMP group from the forwarding table based on a minimum number of links. This can be resolved by using an N+1 redundancy model, where the total number of links in an ECMP group is at least one greater than the minimum number of links required to transport the services.

Note To enable the load splitting of multicast traffic across multiple equal-cost paths, use the **ip multicast multipath** command in global configuration mode. To disable this configuration, use the **no** form of this command. The syntax is as follows:

[**no**] **ip multicast** [**vrf** *vrf-name*] **multipath**

For more information, see the following:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca76c.html#wp1078508

IGP Fast Convergence

With the understanding that IPmc forwarding relies on IP reachability, then fast recovery of IPmc requires fast recovery of IP. Internal Gateway Protocol (IGP) fast convergence supports this objective in the solution.

The following URLs are helpful resources for fast convergence:

- Cisco IOS Software Release 12.2(18)SXF – New Features and Hardware Support

  http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/prod_bulletin0900aecd80327e21.html

- Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2

  http://www.cisco.com/en/US/partner/products/hw/switches/ps708/prod_release_note09186a00801c8339.html

Note With incremental shortest path first (iSPF) configured under open shortest path first (OSPF), a reload might occur. This problem is resolved in Release 12.2(18)SXD1. (CSCec22723)

Note If you configure aggressive OSPF hello timers and dead timers, then during periods of high CPU utilization, OSPF packets are not processed, resulting in OSPF declaring OSPF neighbors to be inoperative ("down"). This problem is resolved in Release 12.2(17d)SXB. (CSCec42160)

- OSPF Support for Fast Hellos

  http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a00801039b1.html
- OSPF Incremental SPF

  http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products_white_paper09186a008012db76.shtml
- OSPF Link-State Advertisement (LSA) Throttling

  http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products_feature_guide09186a0080161064.html
- OSPF Shortest Path First Throttling

  http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134ad8.html
- Bidirectional Forwarding Detection

  http://www.cisco.com/en/US/partner/products/ps6017/products_feature_guide09186a00803fbe87.html
- Bidirectional Forwarding Detection for OSPF

  http://www.cisco.com/en/US/tech/tk365/technologies_white_paper0900aecd80244005.shtml

Note BFD with OSPF support was added in Cisco IOS Release 12.2(18)SXE.

Hardware Rate Limiters

This section presents the following topics:

Introduction

As the service provider industry moves rapidly toward deployment of IP-based video services to consumers, IP transport networks are being engineered to handle extremely high levels of video traffic. These high levels of traffic introduce new service risks if traffic that is normally switched in hardware on routing platforms inadvertently reaches the CPU for processing. This section addresses the operation and use of security mechanisms on the Cisco 7600 platform known as hardware rate limiters (HWRLs).

Note The examples and assumptions in this discussion apply to the Cisco 7600 router with Sup720-3BXL and 6700-series dCEF modules (WS-X6704-10GE, WS-X6724-SFP, and WS-X6748-GETX) with DFC3A and DFC3BXL submodules.

With the threat of distributed denial of service (DDoS) attacks and misconfigurations on the routers and switches used for forwarding the video service, there is a need to rate-limit traffic that could adversely affect service delivery. It is assumed that any method of high-bandwidth traffic injection (either from the Internet or from a residential subscriber) is being marked/policed at the edges of the network, limiting trunk congestion in the network. However, this does not solve the problem of sending packets into the network that are required to be process-switched (rather than switched in hardware), and therefore taking processing resources away from critical network-control functions.

The Cisco 7600 series with the Supervisor Engine 720 has several mechanisms for protecting the control and management plane from performance impacts resulting from DDoS attacks and network misconfigurations.

Note In this solution, the Cisco 7600 series and the Cisco Catalyst 6500 series with the same supervisor engine function identically, although the Cisco 7600 series was the subject of testing and is referenced predominantly.

Caution The values and recommendations presented in this section are based on general assumptions about the traffic characteristics of a network, and should be verified by the customer before being considered for deployment in a production network.

Control Plane and Management Plane Protection

The vast majority of traffic generally travels through the router via the data plane; however, the switch processor (SP) and the route processor (RP) must handle certain packets. These packets are referred to as control plane packets in the remainder of the document.

The SP and RP are critical for system operations. In order to protect the switch's control plane effectively, it is first important to profile the CPU traffic to understand better which types of packets should be allowed to the CPU and how critical each of these packet types are. Packets bound to the CPU include the usual control and management plane traffic such as the following:

- Routing protocol packets (such as BGP, OSPF, EIGRP, and ISIS)
- First Hop Redundancy Protocol (FHRP) packets (such as HSRP, GLBP, and VRRP)
- Multicast control packets (such as IGMP and PIM
- Remote access and management traffic (such as SNMP, NTP, SSH, and TFTP)
- Monitoring and troubleshooting traffic (such as ICMP and Traceroute)
- Layer 2 protocol data units (such as STP, CDP, and VTP)

Some data-plane traffic may have to be processed in software as well. This type of traffic is referred to as data-plane "punt" traffic. Examples of software-processed data-plane packets include the following:

- Packets with IP options
- Packets with Time To Live (TTL) field equal to 1

- Packets whose destination prefix cannot be found in the routing table (also referred to as “FIB-miss” packets)
- Packets that require logging
- Packets that cannot be switched in hardware because a non-hardware-supported feature is applied to the packet
- Packets that are not classified by the hardware (such as AppleTalk and IPX in the Supervisor Engine 720)

A DoS attack targeting the Cisco 7600 series, which can be perpetrated either inadvertently or maliciously, typically involves high rates of traffic destined to the SP or RP itself. This can result in the following symptoms:

- Reduced service quality (such as poor video or voice quality)
- High RP or SP CPU utilization
- Route flaps due to loss of routing protocol updates or keepalives
- Unstable Layer 2 topology
- Slow or unresponsive interactive sessions with the command line interface (CLI)
- Processor resource exhaustion (such as memory and buffers)
- Indiscriminate drops of incoming packets

The Cisco 7600 series support a two-level defense that uses (1) control-plane policing (CoPP; see Note below) and (2) special-case CPU hardware rate limiters (HWRLs). CoPP is applied in hardware on a per-forwarding-engine basis at the Policy Feature Card (PFC) and Distributed Forwarding Card (DFC). The special-case CPU rate limiters are platform dependent, and are applied to rate-limit process-switched traffic going to the SP or RP.

Note Although CoPP is introduced here to aid in understanding a related mechanism, HWRL is the focus of the optimizations presented in this solution. In addition, IPv6 multicast rate limiters are outside the scope of this discussion.

Hardware rate limiters don't provide the same level of traffic-control granularity as CoPP, and are thus useful for cases where hardware CoPP cannot be used to classify particular types of traffic, or when the need to rate-limit the traffic is not dependent on the source and destination addresses. Such special packet types include packets with TTL equal to 1, packets that fail the MTU check, packets with IP options, and IP packets with errors.

CoPP and HWRL should be used in conjunction. However, be aware that the hardware rate limiters override the hardware CoPP policy for packets matching the rate limiter’s criteria. That is, if traffic matches a special-case rate limiter, it is never compared against the hardware CoPP policy. It is compared only against the software CoPP policy. Therefore, note the following Caution.

Caution Cisco strongly recommends ensuring that the CEF Receive rate limiter is disabled when CoPP is used. It is disabled by default. [See Rate-Limiting FIB (CEF) Receive Packets (Unicast), page 2-21.] To disable it if it is enabled, use the **no mls rate-limit unicast cef receive** command.

Note the following:

- To see the available HWRLs and their status, use the **show mls rate-limit** command. See show mls rate-limit, page 4-4.

- The Supervisor 720 forwarding engine provides 10 hardware registers to be used for HWRL. Eight of these registers are present in the Layer 3 forwarding engine of the DFC and PFC, and two of these registers are present in the Layer 2 forwarding engines. The registers are assigned on a first-come, first-serve basis. Should all registers be utilized, the only means to configure another HWRL is to free one register.

  There is no performance penalty for using all ten HWRLs. Hardware rate limiters are supported in all available Supervisor 720 Cisco IOS versions. However, some rate-limiters have been added over time.

- The rate limiters for RPF Failure, TTL Failure, and ICMP No Route (see Table 2-3 on page 2-17) share a single rate-limiter register. If any of these limiters is enabled, all of the limiters in this group share the same value and sometimes the same state (for example, ON/ON/ON). When the rate limiters are verified, if the members of this register are enabled through another feature, an ON-Sharing status (instead of an ON status) is displayed. The exception is the TTL failure rate limiter; its value shares the same value as the other members in the register if you have manually enabled the feature.

Solution-Specific HWRL Details and Examples

This section introduces a variety HWRLs and the commands to configure them, provides additional detail, and presents examples of HWRL configurations suitable to the solution. Testing has verified that the HWRL recommendations that follow do not affect the ability to deliver a residential video service.

Note For additional information, including information about all hardware rate limiters, see HWRL Resources, page 2-34.

Table 2-3 on page 2-17 shows the hardware-based rate limiters available on the Supervisor Engine 720, along with their descriptions. To rate-limit processed-switched traffic, HWRLs are implemented by means of the MultiLayer Switching (MLS) **limit** command), and operate at the switch chassis level.

Caution The recommendations and example values shown in the discussion that follows are generally suitable for the beginning of testing in a high-capacity video production network. Take care to ensure that proper testing in the actual network produces the desired results.

Table 2-3 Hardware Rate Limiters for the Supervisor Engine 720

Type	Short Description	Details/Implementation
Unicast	ACL Input (NAT, TCP int, reflexive ACLs, logon ACLs)	Rate-Limiting Ingress/Egress ACL Bridged Packets (Unicast), page 2-19
	ACL Output (NAT, TCP int, reflexive ACLs, logon ACL)	
	CEF Glean (ARP packets)	Rate-Limiting FIB (CEF) Glean Traffic (Unicast), page 2-20
	CEF Receive (Traffic destined to the router)	Rate-Limiting FIB (CEF) Receive Packets (Unicast), page 2-21
	ICMP No Route (ICMP unreachables for unroutable packets)	Rate-Limiting ICMP Unreachable Packets—No Route and ACL Drop (Unicast), page 2-21
	ICMP Redirect (Packets that require ICMP redirects)	Rate-Limiting ICMP Redirect Messages (Unicast), page 2-22
	IP Errors (Packets with IP checksum or length errors)	Rate-Limiting IP Error Packets (Unicast), page 2-22
	IP Features (Packets that support security, such as CBAC, auth-proxy, and IPsec traffic)	Rate-Limiting IP Features (Unicast), page 2-23
	IP Options (B/BXL) (Unicast traffic with IP options set)	Rate-Limiting IP Options (Unicast), page 2-24
	RPF Failure (Packets that fail uRPF check)	Rate-Limiting uRPF Check Failure Packets (Unicast), page 2-24
	VACL Logging (CLI notification of VACL denied packets)	Rate-Limiting VACL Logging Messages (Unicast), page 2-25

Table 2-3 Hardware Rate Limiters for the Supervisor Engine 720 (continued)

Type	Short Description	Details/Implementation
Multicast	Directly Connected (Local multicast on connected interface)	Rate-Limiting Directly Connected Packets (Multicast), page 2-26
	IGMP (IGMP packets)	Rate-Limiting Layer 2 IGMP Snooping Traffic (Multicast), page 2-27
	IP Options (B/BXL) (Multicast traffic with IP options set)	Rate-Limiting IP Options Packets (Multicast), page 2-27
	Multicast FIB-Miss (Packets with no mroute in the FIB)	Rate-Limiting FIB Miss Packets (Multicast), page 2-28
	Partial Shortcut (Partial shortcut entries)	Rate-Limiting Partially Switched Flows (Multicast), page 2-29
	Non-RPF Interface	Rate-Limiting Non-RPF Interfaces (Multicast), page 2-31
Layer 2[1]	L2PT (L2PT encapsulation/decapsulation)	Rate-Limiting Layer 2 Protocol Tunneling Packets, page 2-31
	PDU (Layer 2 PDUs)	Rate-Limiting Layer 2 PDU Packets, page 2-32
General[2]	MTU Failure[3] (Packets requiring fragmentation)	Rate-Limiting MTU Failure Packets, page 2-32
	TTL Failure[2] (Packets with TTL less than or equal to 1)	Rate-Limiting TTL Failure Packets, page 2-33

1. See Notes below.
2. Shared across the 10 hardware rate limiters.
3. Available only with the DFC3B and DFC3BXL.

Note Layer 2 HWRLs are not supported when the system is running in truncated mode. This occurs when the system contains classic line cards. If the system is running in truncated mode, the following error message is seen when Layer 2 HWRLs are configured:

```
Router(config)# mls rate-limit layer2 pdu 100

04:23:12: %MLS_RATE-4-NOT_SUPPORTED: This functionality is not configurable.
```

Note For a discussion of truncated mode, see "Configuring and Monitoring the Switch Fabric Functionality" at the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a008016113c.html#wp1051977

Rate-Limiting Ingress/Egress ACL Bridged Packets (Unicast)

Summary

This limits packets that are sent to the CPU as a result of an inbound/outbound (ingress/egress) access control list (ACL). The bridged packets are sent when the **log** keyword is used at the end of an Access Control Entry (ACE).

Details

ACEs with the **log** keyword are processed in software on the CPU, but the rest of the ACL is processed in hardware on the DFC. This HWRL can also be used to rate-limit the first packet of a flow for hardware-accelerated features such as NAT, WCCP, CBAC, Auth-Proxy, and TCP Intercept.

Note If this HWRL is enabled, ingress and egress ACLs use the same rate-limiter value.

The following configuration creates an egress ACE that punts packets to the CPU if conditions are met:

```
access-list 20 permit 192.168.0.0 0.0.31.255
access-list 20 permit 192.168.0.0 0.0.0.255
access-list 20 deny any any log

interface GigabitEthernet 7/1
 ip address 10.0.1.2 255.255.255.252
 ip access-group 20 out
```

Default

By default, this HWRL is disabled.

Recommendation

Cisco recommends that the ACE **log** keyword be used sparingly, and only for deny ACEs if possible.

Examples

The following example shows how to rate-limit the unicast packets from an ingress ACL bridge result to 1000 packets per second, and 10 packets in burst:

```
Router(config)# mls rate-limit unicast acl input 1000 10
```

The following example shows how to rate-limit the unicast packets from an ingress ACL bridge result to the same rate (1000 pps and 10 packets in burst) for egress ACL bridge results:

```
Router(config)# mls rate-limit unicast acl output 1000 10
```

If the values of the rate limiter are altered on either the ingress or the egress when both are enabled, both values are changed to that new value.

In the following example, the output rate is changed to 40000 pps:

```
Router(config)# mls rate-limit unicast acl output 40000 10
```

When you enter the **show mls rate-limit** command, both the ACL bridged in and the ACL bridged out display the new value of 40000 pps:

```
Router# show mls rate-limit

  Rate Limiter Type       Status      Packets/s   Burst

--------------------   ----------    ---------   -----

MCAST NON RPF           Off           -           -
MCAST DFLT ADJ          On            100000      100
MCAST DIRECT CON        Off           -           -
ACL BRIDGED IN          On            40000       10
ACL BRIDGED OUT         On            40000       10
IP FEATURES             Off
...
```

Rate-Limiting FIB (CEF) Glean Traffic (Unicast)

Summary

This does not limit Address Resolution Protocol (ARP) traffic, but rather provides the capability to rate-limit traffic that requires address resolution and requires that it be sent to the MSFC.

Details

Consider a router directly connected to a subnet with several hosts. The FIB table on the router maintains a prefix for the subnet instead of for individual host prefixes. This subnet prefix points to what is known as a “glean” adjacency. When traffic contains the destination of a host on a subnet that is locally connected to the router, but no ARP entry exists for that specific destination host, because the MAC address of the destination host is unknown, the glean adjacency is hit in the forwarding table and the traffic is sent directly to the CPU for ARP resolution.

This HWRL does not limit ARP packets, but instead provides the capability to rate-limit traffic that requires address resolution and requires that it be sent to the CPU. This reduces the possibility of an attacker overloading the CPU with such traffic needing ARP resolution.

Default

By default, this HWRL is disabled.

Recommendation

When this HWRL is enabled, the egress security ACL (and egress QoS) of the ingress interface is applied, resulting in dropped packets. The current workaround is either to (1) relax the egress security ACLs of ports facing the PCs or server, or (2) disable the HWRL. Ports facing only routers do not experience this issue, because routing protocols guarantee that ARP entries always exist for routers.

Note This restriction exists for systems running in either PFC3A or PFC3BXL mode.

Example

The following example shows how to rate-limit this traffic to the MSFC to 20000 pps and a burst of 60:

```
Router(config)# mls rate-limit unicast cef glean 20000 60
```

Rate-Limiting FIB (CEF) Receive Packets (Unicast)

Summary

This limits all unicast packets that are directed to the router's local IP addresses.

Caution This includes packets for routing protocols. Exercise extreme care when using this HWRL, to avoid disrupting network stability.

Details

Caution Do not enable the FIB receive rate limiter if you are using CoPP. The FIB receive rate limiter overrides the CoPP policies.

Default

By default, this HWRL is disabled.

Recommendation

Cisco recommends using CoPP, rather than enabling this HWRL, for more granular control-plane protection.

Example

The following example shows how to rate-limit traffic to 25000 pps with a burst of 60:

```
Router(config)# mls rate-limit unicast cef receive 25000 60
```

Rate-Limiting ICMP Unreachable Packets—No Route and ACL Drop (Unicast)

Summary

This limits traffic that requires the RP CPU to *generate* ICMP unreachable packets. It does *not* rate-limit ICMP traffic coming into the router.

Details

For example, when a host sends packets through a router in a suboptimal route path (for a destination not in the routing table, or that is denied by a security ACL or that matches a null route), the CPU sends ICMP unreachable messages to the host to correct the route path. If this traffic occurs continuously and is not rate-limited, the CPU continuously generates ICMP Unreachable messages, which increases CPU utilization.

If the **no ip unreachables** command is configured and an ACL is applied on an interface, then for that interface deny access control entries (ACEs) are processed in software on the CPU, and permit ACEs are processed in hardware.

Note the following:

- Not all unreachables are blocked by the **no ip unreachables** command. Some packets are still leaked to the RP. To block all unreachables, configure the following:

  mls rate-limit unicast ip icmp unreachable acl-drop 0

- If a default route exists in the topology, then unicast traffic never experiences a FIB miss. This HWRL is useful only in networks with no default route.

- The uRPF Failure, ICMP Unreachable, and IP Errors HWRLs all share the same rate limiter state and values.

Default

By default, this HWRL is disabled.

Recommendation

This HWRL is recommended to protect against large VoD streams that have routing misconfigurations, as well as against DoS flooding attacks.

Examples

The following example shows how to rate-limit the packets resulting from an ACL drop to 100 pps and a burst of 10:

```
Router(config)# mls rate-limit unicast ip icmp unreachable acl-drop 100 10
```

The following example shows how to rate-limit the packets that require generation of ICMP Unreachable messages because of a FIB miss (no route) to 80000 pps and burst to 70:

```
Router(config)# mls rate-limit unicast ip icmp unreachable no-route 80000 70
```

Rate-Limiting ICMP Redirect Messages (Unicast)

Summary

This allows you to rate-limit ICMP traffic.

Details

When a host sends packets through a nonoptimal router, the CPU sends ICMP-redirect messages to the host to correct its sending path. If this traffic occurs continuously, and is not rate-limited, the CPU continuously generates ICMP-redirect messages. To disable this behavior, apply the **no ip icmp redirect** command to the desired interface.

Default

By default, this HWRL is enabled.

Recommendation

This HRWL is not needed in cases where the **no ip icmp redirect** command is used in standard configurations].

Example

The following example shows how to rate-limit the ICMP redirects to 20000 pps, with a burst of 20 packets:

```
Router(config)# mls rate-limit unicast ip icmp redirect 20000 20
```

Rate-Limiting IP Error Packets (Unicast)

Summary

This limits the packets with IP checksum and length errors.

Details

When a packet reaches the PFC3 with an IP checksum error or a length inconsistency error, it must be sent to the CPU for further processing. An attacker might use the malformed packets to carry out a DoS attack, but the network administrator can configure a rate for these types of packets to protect the control path.

The following messages are seen in the logs if a malformed IP packet is received and the global **service internal** command is configured on the router:

```
Aug 23 15:03:03.747 UTC: %EARL_L3_ASIC-DFC2-3-INTR_WARN: EARL L3 ASIC: Non-fatal interrupt
Packet Parser block interrupt
Aug 23 15:03:15.643 UTC: %MLS_STAT-DFC2-4-IP_CSUM_ERR: IP checksum errors
Aug 23 15:46:43.553 UTC: %EARL_L3_ASIC-DFC2-3-INTR_WARN: EARL L3 ASIC: Non-fatal interrupt
Packet Parser block interrupt
Aug 23 15:46:45.637 UTC: %MLS_STAT-DFC2-4-IP_CSUM_ERR: IP checksum errors
```

A high rate of these malformed packets affects CPU utilization.

Default

By default, this HWRL is enabled.

Recommendation

IP errors can occur at very low frequency and should not affect the CPU. This HWRL shares the same state and values as the uRPF Failure, ICMP Unreachable, and IP Error rate limiters (which are recommended), and is on by default.

Example

The following example shows how to rate-limit IP errors sent to the MSFC to 100 pps with a burst of 10 packets:

```
Router(config)# mls rate-limit unicast ip errors 100 10
```

Rate-Limiting IP Features (Unicast)

Summary

This limits the number of packets sent first to the CPU to support security features, reducing the potential for overloading.

Details

The security features include authentication proxy (auth-proxy), IPsec, and inspection.

Authentication proxy is used to authenticate inbound or outbound users or both. These users are normally blocked by an access list, but with auth-proxy, the users can bring up a browser to go through the firewall and authenticate on a TACACS+ or RADIUS server (based on the IP address). The server passes additional access list entries down to the router to allow the users through after authentication. These ACLs are stored and processed in software, and if there are many users utilizing auth-proxy, the CPU may be overwhelmed. Rate limiting would be advantageous in this situation.

Note IPsec and inspection are also handled by the CPU and may require rate limiting. When the Layer 3 security feature rate limiter is enabled, all Layer 3 rate limiters for auth-proxy, IPsec, and inspection are enabled at the same rate.

Default

By default, this HWRL is disabled.

Recommendation

Cisco recommends using CoPP, rather than this HWRL, to control authentication traffic.

Example

The following example shows how to rate limit the security features to the CPU to 100000 pps with a burst of 10 packets:

```
Router(config)# mls rate-limit unicast ip features 100000 10
```

Rate-Limiting IP Options (Unicast)

Summary

This limits packets directed to the CPU for IP options processing. This includes packets that are tagged for loose or strict routing or that have the **record-route** option set.

Details

This HWRL is available only on systems running in PFC3B or PFC3BXL mode. It is not available on systems running PFC3A mode.

Default

By default, this HWRL is disabled.

Recommendation

Cisco recommends that this HWRL be used where PFC3B or PFC3BXL modes are available.

Example

The following example shows how to rate-limit traffic to 100 pps with a burst of 10:

```
Router(config)# mls rate-limit unicast ip options 100 10
```

Rate-Limiting uRPF Check Failure Packets (Unicast)

Summary

This limits packets that are sent to the CPU because they failed the Unicast Reverse Path Forwarding (uRPF) check. The uRPF checks validate that incoming packets on an interface are from a valid source, which minimizes the potential threat of DoS attacks from users using spoofed addresses.

Details

When spoofed packets fail the uRPF check, those failures can be sent to the CPU by an ACL that directs it. The uRPF check rate limiters allow you to rate-limit the packets per second that are bridged to the CPU when an ACL fails to eliminate an overload.

The uRPF checks validate that incoming packets on an interface are from a valid source, which minimizes the potential threat of DoS attacks from spoofed addresses. In a SUP720/PFC3A system (or a Sup7203BXL with DFC3A modules present), the use of an ACL can cause the uRPF check to become software processed. When an ACL is configured in the uRPF command, the PFC3 determines whether or not traffic is permitted by the ACL, as shown below.

```
interface GigabitEthernet7/1
 description Link to CMTS
 ip address 10.0.1.2 255.255.255.0
 ip verify unicast source reachable-via rx 20
 ip ospf cost 2
end

access-list 20 permit 192.168.124.0 0.0.0.255
access-list 20 permit 192.168.123.0 0.0.0.255
access-list 20 deny any any log
```

Packets permitted by the ACL are forwarded in hardware without a unicast RPF check, whereas packets denied by the ACL are sent to the MSFC-RP for a Unicast PRF check. Because the packets in a denial-of-service attack typically hit the deny ACE and are sent to the MSFC-RP for the Unicast PRF check, they can overload the CPU. On a Sup720 system you can rate-limit the amount of traffic being bridged to the MSFC-RP as a result of ACL failed.

- For a complete explanation of how uRPF check works, see the *Cisco IOS Security Configuration Guide, Release 12.2*: Other Security Features > Configuring Unicast Reverse Path Forwarding at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htm

- For an explanation of various options of configuring uRPF on the Cisco 7600 with Sup720 and PFC3 modules, see "Configuring Unicast Reverse Path Forwarding Check" at the following URL:

  http://www.cisco.com/en/US/customer/products/hw/switches/ps708/products_configuration_guide_chapter09186a0 080160a59.html#wp1021668

Note The uRPF Failure, ICMP Unreachable, and IP Errors HWRLs share the same rate limiter state and values.

Default

By default, this HWRL is disabled.

Recommendation

This HWRL is recommended. Enable this with a rate limit of 100 pps and a burst limit of 10 packets.

Example

The following example shows how to rate-limit the uRPF check failure packets sent to the MSFC to 100 pps with a burst of 10 packets:

```
Router(config)# mls rate-limit unicast ip rpf-failure 100 10
```

Rate-Limiting VACL Logging Messages (Unicast)

Summary

This limits packets sent to the CPU because of VLAN ACL (VACL) logging, to ensure that the CPU is not overwhelmed with logging tasks.

Details

VLAN ACLs are used to prevent individual IP hosts from communicating with each other within a single VLAN or across different VLANs. They are also used to filter and capture packets for Cisco 7600 service modules. Packets that are sent to the CPU because of VLAN-ACL logging can be rate limited to ensure

that the CPU is not overwhelmed with logging tasks. VACLs are processed in hardware, but the CPU does the logging. When VACL logging is configured on the router, IP packets that are denied in the VACL generate log messages.

- For more information, see "Configuring VLAN ACLs (VACLs)," in the Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.2SX, at the following URL:

  http://www.cisco.com/en/US/partner/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080160a7e.html

Default

By default, this HWRL is enabled.

Recommendation

This HWRL is not needed if VACLs are not used.

Example

The following example shows how to rate-limit logging requests to 5000 pps (the range for this rate limiter is from 10 to 5000 pps):

```
Router(config)# mls rate-limit unicast acl vacl-log 5000
```

Rate-Limiting Directly Connected Packets (Multicast)

Summary

This controls the rate at which Register messages are encapsulated on the first hop (source) router and forwarded to the RP before any receivers have joined.

Details

The multicast connected rate-limiter is designed to control the rate at which Register messages are encapsulated on the first hop (source) router and forwarded to the RP before any receivers have joined. Once a receiver joins the tree, an mroute is put into the FIB and the multicast traffic on that tree is then hardware switched, so this rate limiter is no longer used. This HWRL is useful when several high-rate sources start sending traffic, to limit the CPU utilization until the flow is installed in hardware. This can occur when the RP is not defined to be the source router (SR), as a result of a misconfiguration.

Note Multicast HWRLs have a burst limit of 255 packets.

Default

By default, this HWRL is disabled.

Recommendation

Cisco recommends the use of this HWRL to protect against situations where a new source begins transmitting at a high rate. This could be the case where the RP is not defined to be the source router, as a result of misconfiguration.

Example

The following example shows how to rate-limit the multicast packets to 100 pps with a burst of 250:

```
Router(config)# mls rate-limit multicast ipv4 connected 100 250
```

Rate-Limiting Layer 2 IGMP Snooping Traffic (Multicast)

Summary

This limits the number of Layer 2 IGMP packets destined for the supervisor engine when IGMP snooping is enabled.

Details

IGMP snooping listens to IGMP messages between the hosts and the supervisor engine, and is used to track which local interfaces in a VLAN should receive multicast flows for different groups.

Because of the way that incoming PIM packets are handled in hardware on the Supervisor Engine 720, this rate limiter is also effective for controlling the rate at which received PIM Register messages are sent to the CPU. This can be an effective filter against inadvertent or rogue unicast PIM Register messages being directed at an unsuspecting router.

Note Multicast HWRLs have a burst limit of 255 packets.

Note Cisco IOS Release 12.2(18)SXF requires that PIM snooping be enabled globally for this limiter to be effective against PIM message floods. This issue will be resolved in future versions of Cisco IOS Release 12.2SX code.

Default

By default, this HWRL is disabled.

Recommendation

In multicast networks a high number of IGMP messages do not normally hit the router. However, because this HWRL is also effective in protecting against unicast PIM Register messages being directed at a router, Cisco recommends using this HWRL as a protection against misconfigurations or denial of service (DoS) attacks.

Example

The following example shows how to rate-limit IGMP snooping traffic to 1000 pps and a burst of 10 packets:

```
Router(config)# mls rate-limit multicast ipv4 igmp 1000 10
```

Rate-Limiting IP Options Packets (Multicast)

Summary

This limits packets directed to the CPU for IP Options processing. This includes packets that are tagged for loose or strict routing or that have the **record-route** option set.

Details

This HWRL is available only on systems running in PFC3B or PFC3BXL mode. It is not available on systems running PFC3A mode.

Note Multicast HWRLs have a burst limit of 255 packets.

Default

By default, this HWRL is disabled.

Recommendation

Cisco recommends this HWRL be used where systems are running in PFC3BXL mode. It cannot be used in systems that are running in PFC3A mode.

Example

The following example shows how to rate-limit multicast IP options traffic to 100 pps and a burst of 10 packets:

```
Router(config)# mls rate-limit multicast ipv4 ip-options 100 10
```

Rate-Limiting FIB Miss Packets (Multicast)

Summary

This HWRL allows you to control multicast traffic that must be punted to the CPU that does not match an existing hardware entry in the mroute table. Packets that do not match an existing hardware (*,G) or (S,G) entry must be sent to the CPU for processing.

Details

The Forwarding Information Base (FIB) and Cisco Express Forwarding (CEF) tables contain information programmed into hardware about how to forward traffic, thus relieving the CPU of having to look up a destination for every packet in a flow. Keeping in mind that multicast lookups occur on a source, not on a destination, the CEF entries for multicast flows point to the upstream Reverse Path Forwarding (RPF) interface for a source [for (S,G) flows] or an RP [for (*,G) flows], rather than to a unicast flow's outgoing (forwarding) interface. A (*,G) or (S,G) entry can be programmed in hardware only if the unicast routing table can resolve the RPF interface of the RP or source address.

Hardware entries can be seen with the **show mls cef ip multicast tcam** *group* command. An entry with a source address of 0.0.0.0 corresponds to the (*,G) entry. Note the following example.

```
Router# show mls cef ip multicast tcam 239.16.1.40

Index  Group              Source             RPF/DF Interface
524638 239.16.1.40        172.16.3.2         Te4/1
1048258 239.16.1.40       0.0.0.0            Te4/1
```

There are potentially several situations where a FIB-miss could occur, such as where a static RP address is misconfigured, where the routing table has not fully converged after a network topology change, or following a **clear ip mroute** command.

Note Multicast HWRLs have a burst limit of 255 packets.

Note This HWRL shows up as "MCAST DFLT ADJ" in the output of the **show mls rate-limit** command. (See show mls rate-limit, page 4-4.)

Default

By default, this HWRL is enabled.

Recommendation

Cisco recommends that this HWRL be enabled at a very low rate (100 pps). In an Any Source Multicast (ASM) network, the FIB-miss adjacency is often hit because the router cannot switch traffic from the shared tree to the source tree because of routing misconfiguration or instability. If the rate for this HWRL is kept low, the router simply continues to forward traffic on the shared tree.

Example

The following example shows how to rate-limit the multicast FIB miss packets to 100 pps with a burst of 10:

```
Router(config)# mls rate-limit multicast ipv4 fib-miss 100 10
```

Rate-Limiting Partially Switched Flows (Multicast)

Summary

This limits the flows destined to the CPU for forwarding and replication.

Details

A multicast flow can be either fully or partially hardware switched or software switched. For a given multicast traffic flow, if at least one outgoing Layer 3 interface is multilayer switched, and at least one outgoing interface is not multilayer switched (no H-bit is set for hardware switching), the particular flow is considered partially switched, or" Partial-SC" (for partial shortcut). (See below.)

The output of the **show ip mroute** command indicates the current state of each flow.

- H—This flag indicates that the particular outgoing interface is hardware switched. This means that packets going out this interface for group G will be switched in hardware on the line card and not handled by the CPU.
- RPF-MFD—This flag indicates that the (*,G) or (S,G) traffic on the incoming interface will be completely switched in hardware. The multicast packets of this flow will not seen by the MSFC-RP. If all of the outgoing interfaces for this type entry have the "H" flag set, then the entry is considered to be fully hardware switched.
- Partial-SC—This flag indicates that the (*,G) or (S,G) entry's traffic will be sent to the MSFC-RP for further processing. In some situations all of the outgoing interfaces for (*,G) might be hardware switched (as indicated by the "H" flag) but the mroute entry can still show "Partial-SC". This occurs because the packets will have to be seen by the MSFC-RP to allow the flow to switch to the SPT. Table 2-4 on page 2-29 lists the cases when Partial-SC can occur on a router.

Table 2-4 Cases When Partial-SC Can Occur on a Router

Case	Description
"L" flag is in (*,G) or (S,G) entry	When "L" flag is present, the router has joined the group and the packet for the group should be seen by the router.
"C" flag is in (*,G) entry	When "C" flag is present, the router has at least one connected member (receiver) for the group G and the packet for the group should be seen by the router, if the SPT threshold is not set to infinity.

Table 2-4 Cases When Partial-SC Can Occur on a Router

Case	Description
"H" flag is not set in any OIF	The packet is switched in software for this interface. An interface may not be hardware switched when packets need to be fragmented, IP options are set in the packet, and so on.
One or more OIFs are in a tunnel interface	Prior to 12.2(18)SXE, the Sup720 does not support hardware switching of multicast into tunnel interfaces. Versions 12.2(18)SXE and on support hardware switching into point to point GRE tunnels.
First-hop router is registering to RP	While the first hop router is registering packets to the RP, the (S,G) flow is partially shortcut.

Because the OIFs that have the H-bit flag are switched in hardware, and remaining traffic is switched in software through the MSFC3, it may be desirable to rate limit the flow destined to the MSFC3 for forwarding and replication, which might otherwise increase CPU utilization.

The following shows how to identify a partially switched flow:

```
Router# show ip mroute

(*, 239.19.252.2), 1w5d/00:03:23, RP 172.16.9.69, flags: SJC
  Incoming interface: TenGigabitEthernet4/2, RPF nbr 172.16.9.169, Partial-SC
  Outgoing interface list:
    TenGigabitEthernet4/1, Forward/Sparse, 16:55:37/00:03:23, H
    GigabitEthernet3/3, Forward/Sparse, 1w5d/00:02:31, H
    GigabitEthernet2/14, Forward/Sparse, 1w5d/00:01:14, H

(172.16.11.171, 239.19.252.2), 1w5d/00:02:50, flags: T
  Incoming interface: TenGigabitEthernet4/2, RPF nbr 172.16.9.169, RPF-MFD
  Outgoing interface list:
    TenGigabitEthernet4/1, Forward/Sparse, 16:55:37/00:03:23, H
    GigabitEthernet2/14, Forward/Sparse, 1w5d/00:01:14, H
    GigabitEthernet3/3, Forward/Sparse, 1w5d/00:02:31, H
```

Note Multicast HWRLs have a burst limit of 255 packets.

Note The Multicast Partial-SC HWRL uses a special Layer 2 register that is applied globally, not on a per-DFC basis. It does not count against the 10-register limit for HWRLs. This special Layer 2 HWRL is not impacted by truncated mode like the other Layer 2 limiters.

Default

By default, this HWRL is enabled.

Recommendation

Because there are a number of situations in any source multicast (ASM) networks in which flows can be in a partial shortcut state, Cisco recommends the use of this HWRL.

Example

The following example shows how to rate-limit the partial shortcut flows to 500 pps with a burst of 250 packets:

```
Router(config)# mls rate-limit multicast ipv4 partial 500 250
```

Rate-Limiting Non-RPF Interfaces (Multicast)

Summary

This limits non-RPF traffic that is periodically leaked from a hardware-switched flow to the CPU.

Details

Once an (S,G) state is programmed in hardware on the line card, NetFlow hardware on the DFC3 is used to drop flows appearing on non-RPF interfaces. This HWRL is applied only to non-RPF traffic that is periodically leaked from a hardware switched flow to the CPU.

Note Multicast HWRLs have a burst limit of 255 packets.

Note The FIB-Miss limiter (see Rate-Limiting FIB Miss Packets (Multicast), page 2-28) should be used to control traffic for flows that are not programmed into hardware.

Default

By default, this HWRL is enabled.

Recommendation

Cisco does not recommend the use of this HWRL, because the rate-limiting behavior is not deterministic and may cause convergence speed issues.

Example

This example shows how to set the rate limiters for the IPv4 multicast packets failing the uRPF check:

```
Router(config)# mls rate-limit multicast ipv4 non-rpf 100
```

Rate-Limiting Layer 2 Protocol Tunneling Packets

Summary

This limits the Layer 2 protocol tunneling packets, which include control PDUs, CDP, STP, and VTP packets destined for the supervisor engine.

Details

These packets are encapsulated in software (rewriting the destination MAC address in the PDU), and then forwarded to a proprietary multicast address (01-00-0c-cd-cd-d0).

Default

By default, this HWRL is disabled.

Recommendation

Cisco does not recommend the use of this HWRL where Layer 2 protocols are not allowed on uncontrolled (customer-facing) interfaces in the RAN.

Example

The following example shows how to rate-limit Layer 2 protocol tunneling packets to 10000 pps with a burst of 10 packets:

```
Router(config)# mls rate-limit layer2 l2pt 10000 10
```

Rate-Limiting Layer 2 PDU Packets

Summary

This limits the number of Layer 2 Protocol Data Unit (PDU) packets (including BPDUs, DTP, PAgP, CDP, STP, and VTP packets) destined for the supervisor engine and not the CPU.

Details

This HWRL cannot be enabled if the Supervisor Engine 720 is operating in truncated mode.

Note You cannot enable the Layer 2 PDU rate limiter if the Cisco 7600 series router is operating in truncated mode.

Default

By default, this HWRL is disabled.

Recommendation

Cisco does not recommend the use of this HWRL where Layer 2 protocols are not allowed on uncontrolled (customer-facing) interfaces in the RAN.

Caution The overly aggressive use of this HWRL could have an adverse effect on network stability.

Example

The following example shows how to rate-limit Layer 2 PDUs to 20000 pps with a burst of 20 packets.

```
Router(config)# mls rate-limit layer2 pdu 20000 20
```

Rate-Limiting MTU Failure Packets

Summary

This limits packets that fail an MTU check. These are sent to the CPU and might overwhelm it.

Details

Similar to the TTL failure rate limiter, the rate limiter for MTU failures is supported for both unicast and multicast traffic. An MTU failure occurs when a packet whose DF (Don't Fragment) bit is set cannot be transmitted on an outbound interface because the MTU of the link is smaller than the packet size. The packet must then be sent to the CPU for further handling.

Default

By default, this HWRL is disabled.

Recommendation

This HWRL should not be needed where all interfaces in the RAN are either 1 GE or 10 GE and have a uniform MTU. If tunneling protocols are used in such a network, this HWRL may be useful.

Example

The following example shows how to rate-limit packets failing the MTU failure check from being sent to the MSFC to 100 pps with a burst of 10:

```
Router(config)# mls rate-limit all mtu 100 10
```

Rate-Limiting TTL Failure Packets

Summary

This limits packets that are sent to the MSFC because of a time-to-live (TTL) check failure (the packet's TTL has expired). As indicated by the **all** keyword in the following example, this rate limiter applies to both multicast and unicast traffic.

Details

TTL failure commonly occurs when routing loops are present in the network. However, some edge devices such as video encoders or servers can be misconfigured to source traffic with a low TTL value, resulting in a TTL failure before the packet reaches its destination. This situation results in high CPU utilization unless the TTL Failure HWRL is configured. This HWRL can be safely set to a very low number, because TTL-failed packets are dropped regardless and should be handled in hardware for CPU protection.

Default

By default, this HWRL is disabled.

Recommendation

This HWRL is recommended to protect against high-bandwidth (video) sources with misconfigured TTL that introduce a high rate of traffic into the network.

Example

The following example shows how to rate-limit the TTL failures to 100 pps with a burst of 10:

```
Router(config)# mls rate-limit all ttl-failure 100 10
```

Tips for Using HWRLs

Keep the following in mind when using HWRLs:

- Rate limiters override CoPP (control plan policing) policies.
- HWRLs are configured globally, not on interfaces. They are applied identically to each DFC-based line card.
- HWRLs can be applied or removed dynamically without affecting traffic flows.
- To return a HWRL to its default values and state (enabled or disabled), prepend the **default** keyword to the command, as in the following example:

  ```
  default mls rate-limit multicast connected
  ```

- HWRLs support unicast, multicast, IPv4, and IPv6 traffic only. They do not apply to broadcast or non-IP traffic (except for the Layer 2 PDU limiter). Use the traffic storm control feature for broadcast traffic.

Note For more information, see "Configuring Traffic-Storm Control" at the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a0080160ecc.html

- Unicast HWRLs cannot rate-limit multicast traffic, and vice-versa. General-category HWRLs affects both unicast and multicast packets. The Layer 2 HWRL category use two Layer 2 HWRL resources (other categories share eight Layer 3 rate limiter registers).
- If either the TTL failure or the MTU failure rate limiters are enabled, L2 multicast bridging does not work on PFC3A-based systems. This means that VLANs with both sources and receivers cannot have either of these HWRLs enabled if the system is in PFC3A mode.
- HWRLs do not have easily accessible counters. However, global TTL failure and MTU failure counters are available on the PFC3B/XL.)

Note See Viewing HWRL Counters, page 4-6.

- Traffic hitting two HWRLs is policed twice. If a packet hits two different HWRLs, it counts against the PPS rate of each one. For example, a FIB Miss packet that also hits the TTL Failure HWRL has both limiters applied.
- The IP options rate limiter is not supported on PFC3A.
- When using CoPP in combination with rate limiters, it is strongly recommended that you disable the CEF receive rate limiter, and instead use the CoPP to limit packets with the RP address as the destination IP address.
- The HWRL registers on the DFC are assigned on a first-come, first-served basis. If all registers are being utilized, the only way to configure another rate limiter is to free one register.
- The uRPF Failure, ICMP Unreachable, and IP Errors HWRLs share the same rate limiter state and values. ACL Bridged Input and Output share another limiter.
- The unicast and multicast **ip-option** keyword is supported in PFC3B or PFC3BXL mode only. If the system is running in PFC3A mode (that is, there are DFC3A modules present in the chassis), then this HWRL is not available.
- Layer 2 rate limiters are not supported when the system is running in truncated mode.

HWRL Resources

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

For additional information on HWRLs, refer to the following documents at their respective URLs:

- *Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.2SX*

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/index.htm
- **mls rate-limit** commands

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/m1.htm#wp1497651

- "Protecting the Cisco Catalyst 6500 Series Switches Against Denial-Of-Service Attacks"

  http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper0900aecd802ca5d6.shtml

QoS Fundamentals

When broadcast and on-demand video is carried over an IP network, there is an assumption that the video quality is not degraded when compared to other video transport alternatives, such as MPEG-2 streams transmitted directly over a QAM carrier as is done in cable networks today. To ensure that the degradation in video quality due to the IP transport network is negligible from a subscriber's point of view, most carriers allow the transport network to introduce (at most) one visible degradation in video quality about every two hours.

Note Each IP packet contains up to seven MPEG packets. These seven packets can contain any combination of I-frame, P-frame, B-frame, and audio packets for either a single-program transport stream (SPTS) or a multiple-program transport stream (MPTS). Although most manufacturers of set-top boxes implement some level of error concealment, any IP packet loss is expected to result in video or audio imperfections.

While this end-user requirement is similar to what is currently accepted for voice over IP services, the resulting allowed drop requirement for an IP transport network designed for video services is much more stringent than the requirement for VoIP. The reason for the difference in drop requirements between VoIP and video can be attributed to the support of algorithms used in VoIP that are designed to conceal dropouts in the voice signal caused by lost packets in the IP network. The result is that the IP network can drop a single voice packet without the listener noticing any degradation in voice quality. However, there is no such concealment algorithm for video. The result is that when the IP transport network drops a single video packet, there is a visible degradation of video quality of anywhere from a single frame up to one second, depending on the information that is lost.

Assuming a random loss pattern for video and voice packets, the resulting allowed drop rates for video and voice services are, respectively, 10^{-6} and 10^{-2}. The lower allowed drop rate for video means that both drops cause by congestion and drops caused by bit errors on physical links must be taken into account when one designs a transport network for video services.

The DiffServ architecture defines packet marking and scheduling behaviors that can be used ensure that video flows meet the required 10^{-6} drop rate when links are congested. Video over IP is typically carried in ~1400-byte packets. If bit errors are assumed to be distributed randomly, the resulting requirement for transport links is to ensure a bit error rate (BER) of $< 10^{-10}$.

The BER on optical links can be engineered to 10^{-14} or less by ensuring a high signal-to-noise ratio on those links. Thus video quality due to bit errors on these links should not be an issue.

Note Latency can also introduce degradations in video and audio quality. To minimize latency, keep buffers in the IP network as small as possible.

Because broadcast video, HSD, and VoIP share the same links, it is important to understand how to classify and queue traffic appropriately in order to eliminate the effect high link utilization has on the priority services (broadcast video and VoIP). Table 2-5 presents the details of QoS class and queue assignment for various traffic types.

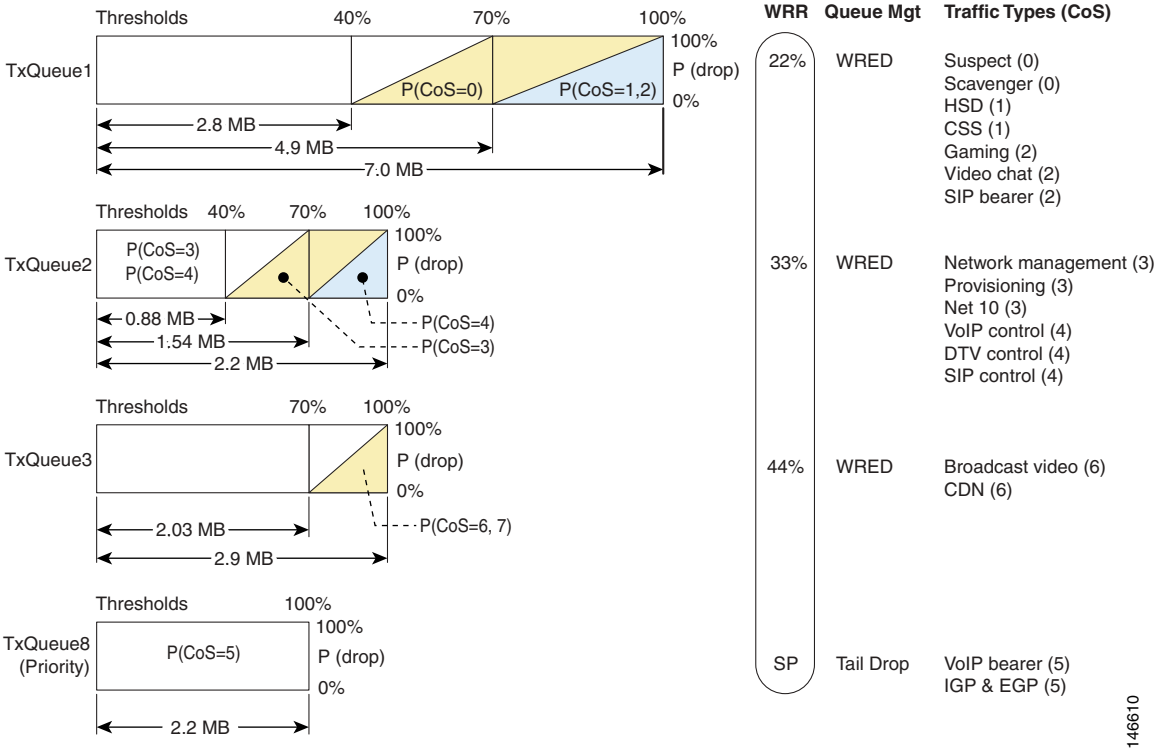
Table 2-5 QoS Class and Queue Assignment for Various Traffic Types

Traffic Type	Protocols	Addressing	Packet Size, bytes	Bitrate	Class/Queue
Suspect	Unknown (assume 1/2 UDP, 1/2 TCP)	Unknown (assume unicast)	Unknown (assume 1/4 100, 1/4 250, 1/4 500, 1/4 1000	>/= 0.1 Gbps	0/1
HSD	IMIX[1]	Unicast	IMIX	>/= 4 Gbps	1/1
Gaming	Unknown (assume UDP)	Unknown (assume unicast)	Unknown (assume 500)	Unknown (assume </= 0.25 Gbps	2/1
Network management	Unknown (assume 1/2 UDP, 1/2 TCP)	Unknown (use unicast to simplify)	100	Unknown (assume 0.1 Gbps	3/2
VoIP control	TCP	Unicast	64	</= 0.2 Gbps	4/2
Broadcast video	UDP	Multicast	1500	2.5 Gbps	6/3
Ad insertion	UDP	Unicast	1500	2 Gbps	6/3
VoIP bearer	UDP	Unicast	160	0.5 Gbps	5/8

1. Internet mix traffic

However, queuing alone is not sufficient, as different classes of traffic share queues. Therefore, one must understand how to set class limits/thresholds properly within each queue. Figure 2-7 on page 2-37 provides an example of defining traffic-class and queue thresholds.

Figure 2-7 Traffic Class and Queue Thresholds



Note the following:

- TxQueue4 through TxQueue7 are not used.
- Weighted random discard is enabled on TxQueue1 through TxQueue3. When queue utilization is between a minimum and a maximum threshold, random frames from a select number of streams with the CoS associated are dropped until the maximum threshold is reached. Subsequently all traffic with those CoS values is dropped.
- Tail drop is enabled on TxQueue8, the priority queue. When queue utilization exceeds 100%, all newly arriving frames are dropped.

Caution Traffic that does not originate from a source controlled by the carrier is considered untrusted, and should be marked as such.

Tip You can set values for Differentiated Services Code Point (DSCP), precedence, and type of service (ToS) for the traffic from datacenter servers [supporting, for example, network management systems (NMS), operational support systems (OSS), and middleware], as well as from video servers (video streamers, VoD servers), in two ways:

(1) If the servers support the functionality, configure the servers themselves to set the DSCP bits, trusting them on the network edge devices.

(2) Classify the traffic appropriately by setting the DSCP bits on the network edge devices.

For more information, see "Implementing Quality of Service Policies with DSCP" at the following URL:

http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml

Note For the details of implementing QoS in the solution, see Configuring Quality of Service, page 3-11.

Upgrading the Network: Migrating from ASM to SSM

IP multicast delivery modes differ only for the receiver hosts, not for the source hosts. A source host sends IP multicast packets with its own IP address as the IP source address of the packet and a group address as the IP destination address of the packet. The following topics are presented below.

- Any Source Multicast
- Source Specific Multicast
- Migration Options

Any Source Multicast

In the Any Source Multicast (ASM) delivery mode, an IP multicast receiver host can use any version of IGMP to join a multicast group. This group is notated as G in the routing table state notation. By joining this group, the receiver host is indicating that it wants to receive IP multicast traffic sent by any source to group G. The network delivers IP multicast packets from any source host with the destination address G to all receiver hosts in the network that have joined group G.

ASM requires group address allocation within the network. At any given time, an ASM group should be used by only a single application. When two applications use the same ASM group simultaneously, receiver hosts of both applications receive traffic from both application sources. This may result in unexpected excess traffic in the network. This situation may cause congestion of network links and malfunction of the application receiver hosts.

Note ASM usually operates in the 239/8 address range.

Source Specific Multicast

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core network technology for the Cisco implementation of IP multicast targeted for audio and video broadcast application environments.

In the SSM delivery mode, an IP multicast receiver host must use IGMP Version 3 (IGMPv3) to subscribe to channel (S,G). By subscribing to this channel, the receiver host indicates that it wants to receive IP multicast traffic sent by source host S to group G. The network delivers IP multicast packets from source host S to group G to all hosts in the network that have subscribed to the channel (S,G).

SSM does not require group address allocation within the network, only within each source host. Different applications running on the same source host must use different SSM groups. Different applications running on different source hosts can arbitrarily reuse SSM group addresses without causing any excess traffic on the network.

Note The default SSM address range is 232/8. However, it is user configurable.

Note For more information about IP multicast, including a discussion of Protocol Independent Multicast, see "IP Multicast Technology Overview" at the following URL:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008044524d.html

Most of the edge equipment deployed in MSO networks today is not yet capable of supporting IGMPv3 with SSM. Consequently, many MSOs have started deploying ASM for DS/DB services. In the ASM model, the rendezvous points (RPs) are the generally routers that are directly connected to the sources. The routers in the headends and the routers in the hubs are RPs for their respective IPmc domains (see Flow Domains, page 2-7).

In addition to the above-mentioned benefits, redundancy options are possible. Once the migration to an SSM model is complete, these redundancy options can be expanded to include Anycast SSM to provide a tertiary backup to the broadcast video feed from the headend.

Migration Options

For those interested in migrating from an ASM to an SSM model, there are four options:

1. Convert all clients (and routers) to IGMPv3/SSM simultaneously.
2. Leave clients as IGMPv2 and configure static SSM mapping on the Cisco 7600 series in the 232/8 address range.
3. Leave clients as IGMPv2 and configure dynamic SSM mapping (through DNS) on the Cisco 7600 series in the 232/8 address range.
4. Leave clients as IGMPv2 and configure static SSM mapping on the Cisco 7600 series in the 239/8 (ASM) address range.

Although the Cisco 7600 series can support any address range for SSM, the 232.*x*.*x*.*x* address range has been reserved for SSM.

Note A description of how to configure SSM mapping can be found in "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 Cisco 7600 series supports the SSM Safe Reporting feature, which ensures that group mode in the switch does not fall back to IGMPv2 mode in the presence of a mixture of IGMPv2 and IGMPv3 receivers in the same VLAN.

Note For more information, see "Configuring IGMP Snooping" at the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a0080435c36.html

Of the four migration options listed above, options 2 and 4 were tested. These options allow for the flexibility to migrate to an SSM model in the network, so that clients can migrate in a schedule manner when IGMPv3 support is available. The main difference between the two options is in the address space used for SSM: device configuration is expected to be less complex with option 4.

Network Management

It is likely that the MSO is concerned with device instrumentation, alerts, and troubleshooting. The resulting information and metrics can be applied to the verification of service or the alerting of faults. It is also useful in isolating problems. Network management can divided into two main areas: Instrumentation and Troubleshooting.

This section presents the following topics:

- Instrumentation
- IPmc Managers

Instrumentation

Two main areas of instrumentation are considered in the solution:

- IOS IPmc MIBs
- IPmc Syslog Messages

Note Testing was conducted with the node configured for egress replication.

IOS IPmc MIBs

Table 2-6 displays the available MIBs for monitoring IPmc. Because not all of these MIBs are available in all software releases, the table indicates which MIBs are available in Cisco IOS Release 12.2SX.

Note The following URL lists supported MIBs and provides additional useful information:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Table 2-6 Support for IPmc MIBs in Cisco IOS Release 12.2SX

Protocol	MIB	Supported?
IGMP	IGMP-MIB.my	Yes
	IGMP-STD-MIB.my	No
mroute	IPMROUTE-MIB.my	Yes
	IPMROUTE-STD-MIB.my	No
	CISCO-IPMROUTE-MIB.my	Yes
PIM[1]	PIM-MIB.my	Yes
	CISCO-PIM-MIB.my	Yes[2]
QoS	CISCO-CLASS-BASED-QOS-MIB.my	Yes
MSDP	MSDP-MIB.my	Yes
mVPN	CISCO-MVPN-MIB.my	No

1. Protocol Independent Multicast
2. Supported in Cisco IOS Release 12.2(18)SXD and later

The solution therefore focuses on the following MIBs:

- IGMP-MIB
- IPMROUTE-MIB
- CISCO-IPMROUTE-MIB
- PIM-MIB
- CISCO-PIM-MIB
- CISCO-CLASS-BASED-QOS-MIB

The CISCO-CLASS-BASED-QOS-MIB is supported only on WAN ports. Cisco Catalyst LAN ports are not Modular QoS CLI (MQC)-compliant, and therefore do not have the level of instrumentation found in the CISCO-CLASS-BASED-QOS-MIB. The Cisco 6704, 6724 and 6748 line cards all use a port ASIC with available QoS counters, as shown in Table 2-7:

Table 2-7 QoS Counters Available on Cisco 6704, 6724, and 6748 Line Cards

QoS Counters	Packets	Bytes
Packets/bytes transmitted per queue	No	No
Packets/bytes dropped per queue	Yes	No
Packets/bytes statistics (transmitted, randomly dropped, tail dropped) per threshold	No	No

Table 2-8 displays the traps that are available.

Table 2-8 Available Traps

Protocol	Trap
mroute	ciscoIpMRouteMissingHeartBeats
PIM	pimNeighborLoss
	ciscoPimRPMappingChange
	ciscoPimInvalidRegister
	ciscoPimInvalidJoinPrune
	ciscoPimInterfaceUp
	ciscoPimInterfaceDown
MSDP	msdpEstablished
	msdpBackwardTransition
mVPN	ciscoMvpnMvrfChange

Note For details on syntax on options, see "SNMP Commands" at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tfr/fft303.htm

Traps are enabled by the following commands:

snmp-server enable traps pim [**neighbor-change** | **rp-mapping-change** | **invalid-pim-message**]

snmp-server enable traps ipmulticast

IPmc Syslog Messages

There are many IPmc syslog messages, under the general categories shown in Table 2-9 on page 2-42.

Table 2-9 IPmc syslog Messages

Message Type	Message
mroute	ROUTELIMIT
	ROUTELIMITWARNING
	RPF_LOOKUP_LOOP
MDS	ROUTELIMIT
PIM	REG_ENCAP_INVALID
	INVALID_RP_REG
	INVALID_SRC_REG
	INVALID_RP_JOIN
	DEPRECATED_HELLO_TLV
	SR_INTERVAL_SETTING_ERR
AUTORP	OVERLAP

Table 2-9 IPmc syslog Messages (continued)

Message Type	Message
MDT	Various
MSDP	PEER_UPDOWN
	SA_LIMIT
	PKT_TOO_BIG
	PEER_IS_SELF
DVMRP	Various
MCAST	Various (Layer 2 Multicast

There is also a new command:

ip pim log-neighbor-changes

Note It is recommended that customers use a correlation engine such as the Cisco CNS Notification Engine to process syslog messages. For more information, see CNS Notification Engine at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cns_note/

IPmc Managers

Although customers may want to use existing management software to manage the IPmc network, the Cisco Multicast Manager is also suitable for this purpose.

Note For more information, see Cisco Multicast Manager at the following URL:

http://www.cisco.com/en/US/products/ps6337/index.html

Cisco Multicast Manager is a web-based network management application that is designed to aid in the monitoring and troubleshooting of multicast networks. Service providers and cable operators running video delivery systems and providing multicast billable services can benefit greatly from deploying Cisco Multicast Manager. Cisco Multicast Manager provides the following benefits:

- Early warning of problems in multicast networks
- In-depth troubleshooting and analysis capabilities
- On-demand, real-time, and historical reporting capabilities
- Optimization of network utilization and enhancement of services delivery over multicast-enabled networks

All multicast-capable devices running Cisco IOS® software, including Layer 2 switches, can be monitored by Cisco Multicast Manager.

Cisco Multicast Manager provides a rich set of monitoring and troubleshooting features, including the following:

- Rapid discovery of all PIM-enabled routers, verification of Cisco IOS® version and device type information, validation of IOS configuration, Internet Group Management Protocol (IGMP) version

- Graphical display of multicast network topologies, including forwarding-tree traces, PIM neighbors, PIM interface modes, multicast route tables, IGMP tables, Multicast Source Directory Protocol (MSDP) peers, and Session Advertisement (SA) cache information
- Proactive monitoring and analysis of active multicast groups and sources, group status, Rendezvous Point (RP) availability, multicast traffic statistics from source or received on any interface, Layer 2 multicast traffic, and throughput deltas
- Sophisticated ability to poll the following network entities:
  - RPs—to detect joins/leaves and group additions/removals
  - routers—to determine whether a given (S,G) exists, or traffic from the source exceeds a given threshold,
  - Layer 2 switches—to collect multicast traffic statistics on a given port or VLAN
  - multicast forwarding trees—to detect changes
  - unicast and/or multicast routing tables—to detect changes
- Detailed diagnostics and extensive reporting capabilities, including reports for the following:
  - RP polling
  - RP group threshold
  - Layer 2 threshold
  - “groups gone”
  - (S,G)
  - multicast tree
  - routing table
  - traffic tend (as graphs)
- Unicast/multicast address management, including a database to store and query on multicast addresses or blocks thereof, and querying capabilities addresses in the database

A number of MIBs are supported by Cisco Multicast Manager, including the following:

- PIM-MIB-V1SMI.my
- IPMROUTE-MIB-V1SMI.my
- IPMROUTE-STD-MIB-V1SMI.my
- IGMP-MIB-V1SMI.my
- IGMP-STD-MIB-V1SMI.my
- MSDP-MIB-V1SMI.my (not supported in 12.1)
- RFC1213-MIB.my
- IF-MIB-V1SMI.my
- CISCO-HSRP-MIB-V1SMI.my
- CISCO-CONFIG-COPY-MIB-V1SMI.my
- CISCO-STACK-MIB-V1SMI.my

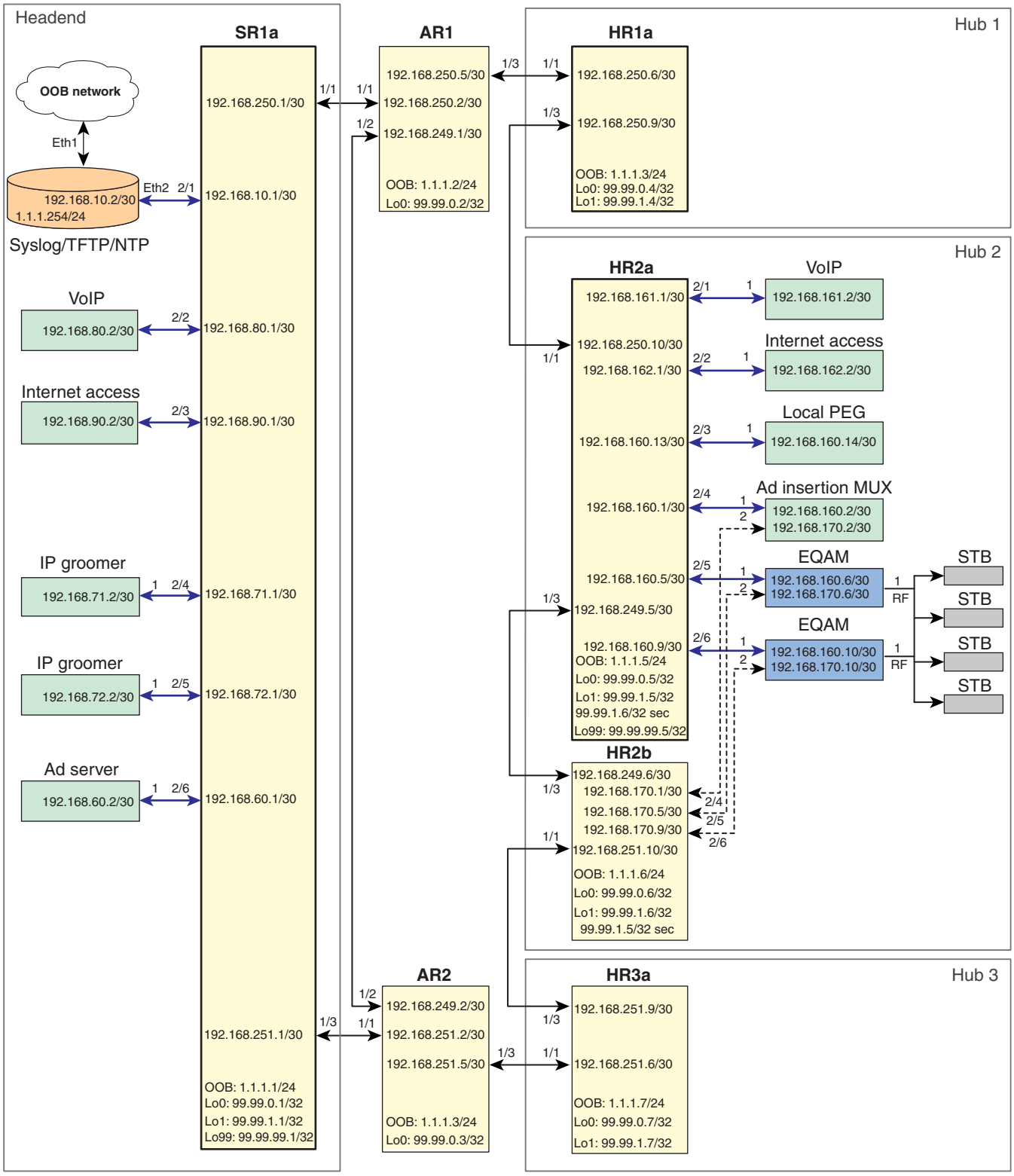
Implementing the Solution

This chapter presents the following major topics:

Network Topology

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

Figure 3-1 Network Topology



Basic Configuration: Configuring Global and Interface Attributes

The following tasks are presented:

- Configuring Routing
- Configuring Multicast

Configuring Routing

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

Note See IP Architecture, page 2-2.

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

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

To configure routing, perform the following tasks:

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

Configuring the RAN OSPF Process

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

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

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

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

```
log-adjacency-changes detail

maximum-paths 6
```

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

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

Step 4 Modify the SPF algorithm to converge more quickly.

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

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

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

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

Configuring the Hub OSPF Process

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

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

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

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

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

a. Define a prefix list.

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

b. Define a route map.

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

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

Configuring the iBGP Process

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

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

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

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

```
no synchronization

no auto-summary
```

Step 3 Enable the logging of BGP neighbor changes.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a. Define the prefix list.

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

b. Define the route map.

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

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

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

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

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

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

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

Step 3 Enable the logging of BGP neighbor changes.

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

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

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

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

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

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

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

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

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

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

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

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

Step 9 Define the networks to be advertised.

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

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

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

 route-map rmap_Ad-Insertion permit 100
  set metric 100

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

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

 route-map rmap_Voice permit 100
  set metric 100

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

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

route-map rmap_Hub2 permit 100
 set metric 100

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

Configuring Multicast

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

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

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

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

The following tasks are presented below:

- Configuring SSM
- Configuring IGMP

Configuring SSM

To configure SSM, do the following.

Step 1 Enable multicast routing.

```
ip multicast routing
```

Step 2 Enable SSM mapping.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
HR2a# show ip igmp ssm-mapping

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

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

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

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

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

Configuring IGMP

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

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

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

All Clients Support IGMPv2 Only

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

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

All Clients Support and Are Configured for IGMPv3

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

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

Configuring Quality of Service

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

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

The following tasks are presented below:

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

Configuring Marking and Classification

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

Step 1 Enable QoS in global configuration mode.

```
mls qos
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Configuring DSCP-to-CoS Mapping

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

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

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

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

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

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

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

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

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

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

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

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

Configuring CoS-to-Queue Mapping

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

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

Table 3-1 Line Card Characteristics

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Configuring Network Enhancements

This section presents the following major topics:

- Configuring New Features
- Configuring Hardware Rate Limiters

Configuring New Features

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

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

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

EtherChannel Min-Links Feature

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

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

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

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

Multicast Replication Mode Feature

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

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

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

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

Local Egress Replication Feature

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

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

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

Configuring Hardware Rate Limiters

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

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

Configuring Non-Solution-Specific Features

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

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

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

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

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

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

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

- IOS Command Lookup Tool

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

Monitoring and Troubleshooting

This chapter presents the following major topics:

Troubleshooting Multicast

Several commands can be used to troubleshoot IP multicast (IPmc) networks:

- mstat
- mrinfo
- mtrace

Note For more information, including syntax and examples, see "Monitoring and Maintaining IP Multicast" at the following URL:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00804453e7.html

mstat

Use this command to see the IPmc path in ASCII graphic format. It traces the path between any two points in the network, shows drops and duplicates, time to live (TTL) thresholds, and delays at each node in the network. It is very useful when you need to locate congestion points in the network, or focus on a router with high drop/duplicate counts. Duplicates are indicated in the output as "negative" drops.

mrinfo

Use this command to see IPmc neighbor router information, router capabilities and code version, IPmc interface information, TTL thresholds, metrics, protocol, and status. It is useful when you need to verify IPmc neighbors, confirm that bidirectional neighbor adjacency exists, and verify that tunnels are up in both directions.

mtrace

Use this command to see the IPmc path from the source to the receive. It traces the path between points in the networks, showing TTL thresholds and delay at each node. When troubleshooting, use this command to find where IPmc traffic flow stops, to verify the path of IPmc traffic, and to identify suboptimal paths.

Show Commands

Show commands are presented for the following categories:

- show ip
- show mls

show ip

The following commands provide useful information about IP routing:

- show ip igmp groups
- show ip igmp interface
- show ip pim neighbor
- show ip pim interface
- show ip mroute summary
- show ip mroute
- show ip mroute active
- show ip rpf
- show ip mroute count
- show ip pim rp mapping

Note For more information, including syntax and examples, see "Cisco IOS IP Command Reference, Volume 3 of 4: Multicast, Release 12.3, at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_chapter09186a008017cf20.html

show ip igmp groups

Use this command to see which IPmc groups are directly connected to the router, and which are learned by means of Internet Group Management Protocol (IGMP). You can use this command to verify that a source or receiver has actually joined the target group on the router interface. The "Last Reporter" column shows only one IGMP host, which indicates that it has sent either an unsolicited IGMP Join or IGMP Report in response to a IGMP Query from the Protocol Independent Multicast (PIM) router for that particular group. You should only see one "Last Reporter" per Group Address.

show ip igmp interface

Use this command to display IPmc-related information about an interface, and to verify that IGMP is enabled, that the correct version is running, the timers, Time To Live (TTL) threshold value, and that IGMP querier router are properly set. IGMP does not need to be configured on an interface. It is enabled by default when you configure **ip pim dense-mode | sparse-mode | sparse-dense-mode**.

show ip pim neighbor

Use this command to list the PIM neighbors discovered by the Cisco IOS.

show ip pim interface

Use this command to display information about interfaces configured for PIM. In addition, you can use it to verify that the correct PIM mode (dense or sparse) is configured on the interface, the neighbor count is correct, and the designated router (DR) is correct (which is critical for PIM sparse mode). Multi-access segments (such as Ethernet, Token Ring, FDDI) elect a DR based on highest IP address. Point-to-Point links do not display DR information.

show ip mroute summary

Use this command to display the summarized contents of the IPmc routing table. You can also use it to verify the active IPmc group(s) and which IPmc senders are active by looking at the timers and flags.

show ip mroute

Use this command to display the full contents of the IPmc routing table. When you troubleshoot, use this command to verify the following:

- The (S,G) and (*,G) state entries from the flags.
- Whether the incoming interface is correct. If it is not, check the unicast routing table.
- Whether the outgoing interface (or interfaces) is (or are) correct. For any that are incorrectly pruned, check the state in the downstream router.

show ip mroute active

Use this command to display the active traffic sources and groups above the threshold. When you troubleshoot, use it to verify active source groups, the traffic rate for each source, group (S,G) pair [you must have switched to Shortest Path Tree (SPT)], and to check if the target group IPmc traffic is being received. If the traffic is not being received, look for active traffic starting from the source towards the receiver.

show ip rpf

Use this command to display how IPmc routing does Reverse Path Forwarding (RPF). When you troubleshoot, use it to verify that the RPF information is correct. If it is not, check the unicast routing table for the source address. Also use the **ping** and **trace** commands on the source address to verify that unicast routing works. You may need to use Distance Vector Multicast Routing Protocol (DVMRP) routes or static mroutes to fix any unicast-multicast inconsistencies.

show ip mroute count

Use this command to verify that IPmc traffic is received, and to check on its flow rates and drops. If no traffic is received, work from the source to the receiver until you find where the traffic stops. You can also use this command to verify that traffic is being forwarded. If it is not, use the **show ip mroute** command to look for "Null Outgoing interface list" and RPF failures.

show ip pim rp mapping

Use this command to check the RP assignment by IPmc group range, and to verify that the source of RP learning (static or auto-RP) and the mapping are correct. If you find an error, check the local router configuration or auto-RP configuration.

show mls

The following command provides useful information about Multi-Layer Switching (MLS).

- show mls rate-limit
- show mls cef adjacency
- show mls statistics

show mls rate-limit

Use this command to see an exhaustive list of special-case hardware rate limiters (HWRLs). (See Hardware Rate Limiters, page 2-13.) The following output shows all HWRLs available as of Cisco IOS Release 12.2(18)SXE.

```
Router# show mls rate-limit

Load for five secs: 1%/0%; one minute: 1%; five minutes: 0%
Time source is NTP, 17:57:48.508 PST Mon Mar 28 2005

 Sharing Codes: S - static, D - dynamic
 Codes dynamic sharing: H - owner (head) of the group, g - guest of the group
```

```
  Rate Limiter Type       Status     Packets/s   Burst  Sharing
---------------------   ----------   ---------   -----  -------
        MCAST NON RPF   Off                  -       -     -
       MCAST DFLT ADJ   On              100000     100  Not sharing
     MCAST DIRECT CON   Off                  -       -     -
       ACL BRIDGED IN   Off                  -       -     -
      ACL BRIDGED OUT   Off                  -       -     -
          IP FEATURES   Off                  -       -     -
         ACL VACL LOG   On                2000       1  Not sharing
          CEF RECEIVE   Off                  -       -     -
            CEF GLEAN   Off                  -       -     -
     MCAST PARTIAL SC   On               100000     100  Not sharing
       IP RPF FAILURE   On                  100      10  Group:0 S
          TTL FAILURE   Off                  -       -     -
ICMP UNREAC. NO-ROUTE   On                  100      10  Group:0 S
ICMP UNREAC. ACL-DROP   On                  100      10  Group:0 S
        ICMP REDIRECT   Off                  -       -     -
          MTU FAILURE   Off                  -       -     -
      MCAST IP OPTION   Off                  -       -     -
      UCAST IP OPTION   Off                  -       -     -
          LAYER_2 PDU   Off                  -       -     -
           LAYER_2 PT   Off                  -       -     -
           IP ERRORS   On                   100      10  Group:0 S
         CAPTURE PKT   Off                  -       -     -
          MCAST IGMP   Off                  -       -     -
MCAST IPv6 DIRECT CON   Off                  -       -     -
MCAST IPv6 ROUTE CNTL   Off                  -       -     -
MCAST IPv6 *G M BRIDG   Off                  -       -     -
 MCAST IPv6 SG BRIDGE   Off                  -       -     -
 MCAST IPv6 DFLT DROP   Off                  -       -     -
MCAST IPv6 SECOND. DR   Off                  -       -     -
 MCAST IPv6 *G BRIDGE   Off                  -       -     -
```

show mls cef adjacency

See Viewing HWRL Counters, page 4-6.

show mls statistics

See Viewing HWRL Counters, page 4-6.

Debug Commands

The following debug commands provide useful information:

- debug ip pim
- debug ip mpacket
- debug ip mrouting

Note For more information, including syntax and examples, see "Cisco IOS Debug Command Reference, Release 12.2," at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a0080087363.html

debug ip pim

Use this command to display PIM packets received and sent, and to display PIM-related events.

debug ip mpacket

Use this command to display IP multicast packets received and sent,

debug ip mrouting

Use this command to display changes to the IP multicast routing table.

Viewing HWRL Counters

Note For background, see Hardware Rate Limiters, page 2-13.

Although Cisco IOS does not currently have a summarized CLI output of hardware rate limiter (HWRL) counters, it is possible to monitor some of the more interesting ones through module-specific commands. HWRLs are implemented as a series of special Cisco Express Forwarding (CEF) adjacencies, which can be seen with the **show mls cef adjacency special** command. The output below has been reduced to the more interesting HWRL adjacencies. Note that the limiter type is shown in parentheses for each index.

```
Router> show mls cef adjacency special

Index: 0        smac: 0000.0000.0000, dmac: 0000.0000.0000
                mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 1
                format: MULTICAST, flags: 0x2000000C00 (mcast_fib_fail)
                met2: 0, met3: 0
                packets: 0, bytes: 0

Index: 3        smac: 0000.0000.0000, dmac: 0000.0000.0000
                mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 0
                format: MULTICAST, flags: 0x2000000800 (mcast_fib_rpf_fail)
                met2: 0, met3: 0
                packets: 0, bytes: 0

Index: 5        smac: 0000.0000.0000, dmac: 0000.0000.0000
                mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 1
                format: MULTICAST, flags: 0x2000000C00 (mcast_dir_conn)
                met2: 0, met3: 0
                packets: 0, bytes: 0
```

HWRL counters for each distributed forwarding card (DFC) can be seen by issuing the **show mls cef adjacency entry** command for each module. If no module is specified then the counters are shown for the policy feature card (PFC). For example, to see counters for the FIB-Miss HWRL (Index 0 from the above output) in a system that has DFC-based modules in slots 1 and 4, issue the commands as shown below. The first command below (without the module subcommand) shows the counters from the PFC3 on the Sup720. The counters from this command show traffic limited on cards that do not have DFC3 submodules.

```
Router> show mls cef adjacency entry 0
```

```
Index: 0       smac: 0000.0000.0000, dmac: 0000.0000.0000
               mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 1
               packets: 0, bytes: 0
```

Note The above output is identical to what is retrieved when the module where the Sup720 is located is specified. In other words, the above command is the equivalent of issuing a **show mls cef adjacency entry 0 module 5** command when the Sup720 is in slot 5.

```
Router> show mls cef adjacency entry 0 module 1

Index: 0       smac: 0000.0000.0000, dmac: 0000.0000.0000
               mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 1
               packets: 656, bytes: 891424

Router> show mls cef adjacency entry 0 module 4

Index: 0       smac: 0000.0000.0000, dmac: 0000.0000.0000
               mtu: 9234, vlan: 0, dindex: 0x0, l3rw_vld: 1
               packets: 5004164, bytes: 6775638056
```

These counters are not currently accessible by means of SNMP.

TTL and MTU failures can be seen in the output of the **show mls statistics** command, as shown below.

Note TTL and MTU failure counters are available only with the DFC3B and DFC3BXL. These counters include all packets failing TTL and MTU checks, both by HWRLs and by MSFC-RP software processing.

```
Router# show mls statistics

<---snip--->
```

Note Statistics for Module 4 are shown below.

```
Errors
  MAC/IP length inconsistencies         : 0
  Short IP packets received             : 0
  IP header checksum errors             : 0
  TTL failures                          : 721386
  MTU failures                          : 0

<---snip--->
```

Note Statistics for Module 5 are shown below.

```
Errors
  MAC/IP length inconsistencies         : 0
  Short IP packets received             : 0
  IP header checksum errors             : 0
  TTL failures                          : 0
  MTU failures                          : 0

Total packets L3 Switched by all Modules: 2733893197353 @ 3651668 pps
```

Sample Configurations

This appendix presents sample configurations for the following:

Note See Network Topology, page 3-1.

Configuration for the Source Router

The following is the configuration for SR1a.

```
!#####################################################################
!
! Description
! ===========
! Video Networking Solution 3.0
! SR1a running-config
!
! Version Information
! ===================
! IOS
! ---
! 12.2(18)SXF
!
! Hardware
! --------
!
! Mod  Port Model              Serial !    Versions
! ---- ---- ------------------ ----------- --------------------
!   1    4  WS-X6704-10GE      SAL09337DN0 Hw : 2.2
!                                         Fw : 12.2(14r)S5
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-F6700-DFC3BXL   SAL09295P6K Hw : 5.0
!   2   48  WS-X6748-GE-TX     SAL090607K5 Hw : 2.1
!                                         Fw : 12.2(14r)S5
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-F6700-DFC3BXL   SAL09295P90 Hw : 5.0
```

```
!   5    2  WS-SUP720-3BXL     SAL09137GNV Hw : 4.3
!                                         Fw : 8.1(3)
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-SUP720          SAL091279RT Hw : 2.3
!                                         Fw : 12.2(17r)S2
!                                         Sw : 12.2(18)SXF
!           WS-F6K-PFC3BXL     SAL0912725W Hw : 1.6
!
!
!################################################################
!
!
upgrade fpd auto
version 12.2
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
service counters max age 5
no service dhcp
!
hostname SR1a
!
boot system disk0:s72033-adventerprisek9_wan-mz.122-18.SXF.bin

logging snmp-authfail
logging buffered 64000 informational
no logging console
enable password cisco123
!
no aaa new-model
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
no ip source-route
ip spd mode aggressive
!
!
!
ip cef accounting non-recursive
ip tftp source-interface Loopback0
no ip bootp server
ip multicast-routing
ip igmp ssm-map enable
no ip igmp ssm-map query dns
ip igmp ssm-map static acl_SSM-map-DB 192.168.71.2
ip igmp ssm-map static acl_SSM-map-DS 192.168.72.2
ip igmp ssm-map static acl_SSM-map-DS-post-splice 192.168.160.2
ip tcp window-size 65535
ip tcp path-mtu-discovery
ip telnet source-interface Loopback0
no ip domain-lookup
vtp domain SR1a
vtp mode transparent
mls ip multicast replication-mode ingress
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos map dscp-cos 16 18 20 to 3
```

```
mls qos map dscp-cos 26 28 30 to 4
mls qos map dscp-cos 34 36 38 to 6
mls qos map dscp-cos 40 42 44 to 2
mls qos map dscp-cos 48 to 5
mls qos
mls rate-limit multicast ipv4 fib-miss 10000 250
mls rate-limit multicast ipv4 connected 2500 250
mls rate-limit multicast ipv4 igmp 1000 10
mls rate-limit multicast ipv4 ip-options 1000 10
mls rate-limit multicast ipv4 partial 500 250
mls rate-limit unicast acl input 1000 10
mls rate-limit unicast acl output 1000 10
no mls rate-limit unicast acl vacl-log
mls rate-limit all ttl-failure 100 10
mls rate-limit all mtu-failure 100 10
no mls acl tcam share-global
mls cef error action freeze
!
!
!
!
!
!
!
!
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
  auto-sync standard
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
no spanning-tree vlan 1-4094
!
power redundancy-mode combined
error-detection packet-buffer action none
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
!
vlan internal allocation policy ascending
!
class-map match-all class_voice
  match access-group name acl_voice
class-map match-all class_broadcast-video
  match access-group name acl_broadcast-video
class-map match-all class_ad-server
  match access-group name acl_ad-server
class-map match-all class_video-signaling
  match access-group name acl_video-signaling
class-map match-all class_net-mgmt
  match access-group name acl_net-mgmt
class-map match-all class_internet-access
  match access-group name acl_internet-access
class-map match-all class_suspect
  match access-group name acl_permit-any
!
!
policy-map pmap_voice-port
  class class_voice
```

```
   trust dscp
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_broadcast-video-port
  class class_broadcast-video
   set dscp af41
  class class_video-signaling
   set dscp cs3
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_ad-server-port
  class class_ad-server
   set dscp af41
  class class_video-signaling
   set dscp cs3
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_net-mgmt-port
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_internet-access-port
  class class_internet-access
   set dscp 8
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
!
!
!
interface Loopback0
 description RAN Loopback
 ip address 99.99.0.1 255.255.255.255
!
interface Loopback1
 description Local Loopback
 ip address 99.99.1.1 255.255.255.255
!
interface Loopback99
 description ASM Multicast Rendevouz Point
 ip address 99.99.99.1 255.255.255.255
 ip pim sparse-mode
!
interface Null0
 no ip unreachables
!
interface TenGigabitEthernet1/1
 description Transport between AR1 (TenGig1/1)
 ip address 192.168.250.1 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
```

```
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/2
 no ip address
 shutdown
!
interface TenGigabitEthernet1/3
 description Transport between AR2 (TenGig1/1)
 ip address 192.168.251.1 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/4
 no ip address
 shutdown
!
interface GigabitEthernet2/1
 description Syslog/TFTP/NTP on PC0a (Eth2) dual-homed to 1.1.1.0/24
 ip address 192.168.10.1 255.255.255.252
 no ip redirects
 no ip proxy-arp
 no cdp enable
 service-policy input pmap_net-mgmt-port
!
interface GigabitEthernet2/2
 description Voice over IP
 ip address 192.168.80.1 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 no cdp enable
 service-policy input pmap_voice-port
!
interface GigabitEthernet2/3
 description Internet Access
 ip address 192.168.90.1 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 no cdp enable
 service-policy input pmap_internet-access-port
!
interface GigabitEthernet2/4
 description CherryPicker DM0a (Port 1) - DB
 ip address 192.168.71.1 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 no cdp enable
 service-policy input pmap_broadcast-video-port
!
interface GigabitEthernet2/5
 description CherryPicker DM0b (Port 1) - DS
 ip address 192.168.72.1 255.255.255.252
 no ip redirects
 no ip proxy-arp
```

```
 ip pim sparse-mode
 no cdp enable
 service-policy input pmap_broadcast-video-port
!
interface GigabitEthernet2/6
 description Ad Server Ad0a
 ip address 192.168.60.1 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 no cdp enable
 service-policy input pmap_ad-server-port
!
interface GigabitEthernet2/7
 no ip address
 shutdown
!
!
!  <<< omitted interface GigabitEthernet2/8 - interface GigabitEthernet2/47 >>>
!
!
interface GigabitEthernet2/48
 no ip address
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 description Management port for Syslog/TFTP/NTP
 ip address 1.1.1.1 255.255.255.0
 media-type rj45
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 100
 router-id 99.99.0.1
 max-metric router-lsa on-startup wait-for-bgp
 log-adjacency-changes detail
 timers throttle spf 400 400 4000
 passive-interface default
 no passive-interface TenGigabitEthernet1/1
 no passive-interface TenGigabitEthernet1/3
 network 99.99.0.0 0.0.255.255 area 0
 network 192.168.250.0 0.0.0.255 area 0
 network 192.168.251.0 0.0.0.255 area 0
 maximum-paths 6
!
router bgp 100
 no synchronization
 bgp router-id 99.99.0.1
 bgp log-neighbor-changes
 redistribute connected route-map rmap_Connected-to-BGP
 neighbor rr-server peer-group
 neighbor rr-server remote-as 100
 neighbor rr-server update-source Loopback0
 neighbor rr-server version 4
 neighbor rr-server send-community
 neighbor 99.99.0.2 peer-group rr-server
 neighbor 99.99.0.2 description AR1
 neighbor 99.99.0.3 peer-group rr-server
 neighbor 99.99.0.3 description AR2
```

```
 no auto-summary
!
ip classless
!
ip bgp-community new-format
no ip http server
ip pim ssm range acl_SSM-IPmc-range
!
ip access-list standard acl_SSM-IPmc-range
 permit 239.0.0.0 0.255.255.255
ip access-list standard acl_SSM-map-DB
 remark SSM mapping for DB blue/red
 permit 239.16.0.0 0.0.0.255
ip access-list standard acl_SSM-map-DS
 remark SSM mapping for DS blue/red
 permit 239.20.0.0 0.0.255.255
ip access-list standard acl_SSM-map-DS-post-splice
 remark SSM mapping for post splice DS blue/red
 permit 239.28.0.0 0.0.255.255
!
ip access-list extended acl_voice
 remark Identify voice traffic
 permit ip any 192.168.161.0 0.0.0.255

ip access-list extended acl_broadcast-video
 remark Identify broadcast video traffic (multicast on 239.x.x.x)
 permit ip any 239.0.0.0 0.255.255.255
ip access-list extended acl_ad-server
 remark Identify ad server traffic
 permit ip 192.168.60.0 0.0.0.255 any
ip access-list extended acl_video-signaling
 remark Identify video signaling
 permit ip any 192.168.61.0 0.0.0.255
ip access-list extended acl_net-mgmt
 remark Identify net management traffic (TFTP, Syslog, NTP, etc)
 permit ip 192.168.10.0 0.0.0.255 any
 permit ip any 192.168.10.0 0.0.0.255
ip access-list extended acl_internet-access
 remark Identify Internet access traffic
 permit ip 192.168.90.0 0.0.0.255 any
ip access-list extended acl_permit-any
 permit ip any any
!
!
ip prefix-list pl_Connected-to-BGP seq 5 permit 192.168.10.0/24 le 32
ip prefix-list pl_Connected-to-BGP seq 10 permit 192.168.60.0/24 le 32
ip prefix-list pl_Connected-to-BGP seq 15 permit 192.168.70.0/24 le 32
ip prefix-list pl_Connected-to-BGP seq 20 permit 192.168.71.0/24 le 32
ip prefix-list pl_Connected-to-BGP seq 25 permit 192.168.72.0/24 le 32
ip prefix-list pl_Connected-to-BGP seq 30 permit 192.168.73.0/24 le 32
ip prefix-list pl_Connected-to-BGP seq 30 permit 192.168.80.0/24 le 32
ip prefix-list pl_Connected-to-BGP seq 30 permit 192.168.90.0/24 le 32
!
logging event link-status default
logging trap debugging
logging source-interface Loopback0
logging 1.1.1.254
!
route-map rmap_Connected-to-BGP permit 100
 match ip address prefix-list pl_Connected-to-BGP
 set metric 100
 set ip next-hop 99.99.0.1
!
!
```

```
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
banner motd ^C
######################################################################


 Project = Video Networking Solution
 Switch = SR1a

 Chassis = 7606
 Slot1 = WS-X6704 (3BXL)
 Slot2 = WS-X6748 (3BXL)
 Slot5 = Sup720  (3BXL)


######################################################################
^C
!
line con 0
 exec-timeout 0 0
 history size 100
 transport preferred none
line vty 0 4
 exec-timeout 0 0
 password cisco123
 login
 history size 100
 transport preferred none
!
!
monitor event-trace timestamps
scheduler runtime netinput 300
ntp source Loopback0
ntp server 1.1.1.254
ntp update-calendar
no cns aaa enable
end
```

Configurations for the Aggregation Routers

The following configurations are presented:

Configuration for AR1

```
!#####################################################################
!
! Description
! ===========
! Video Networking Solution 3.0
! AR1 running-config
!
! Version Information
! ===================
! IOS
! ---
! 12.2(18)SXF
!
! Hardware
! --------
!
! Mod  Port Model              Serial #    Versions
! ---- ---- ------------------ ----------- -------------------------------------
!   1    4  WS-X6704-10GE      SAL09295RAQ Hw : 2.2
!                                         Fw : 12.2(14r)S5
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-F6700-DFC3BXL   SAL09285CDU Hw : 5.0
!   5    2  WS-SUP720-3BXL     SAL09232FNL Hw : 4.3
!                                         Fw : 8.1(3)
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-SUP720          SAL09232GDX Hw : 2.3
!                                         Fw : 12.2(17r)S2
!                                         Sw : 12.2(18)SXF
!           WS-F6K-PFC3BXL     SAL09222CTU Hw : 1.6
!
!#####################################################################
!
!
upgrade fpd auto
version 12.2
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
service counters max age 5
no service dhcp
!
hostname AR1
!
boot system disk0:s72033-adventerprisek9_wan-mz.122-18.SXF.bin
```

```
logging snmp-authfail
logging buffered 64000 informational
enable password cisco123
!
no aaa new-model
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
no ip source-route
ip spd mode aggressive
!
!
!
ip cef accounting non-recursive
ip tftp source-interface Loopback0
no ip bootp server
ip multicast-routing
ip igmp ssm-map enable
no ip igmp ssm-map query dns
ip igmp ssm-map static acl_SSM-map-DB 192.168.71.2
ip igmp ssm-map static acl_SSM-map-DS 192.168.72.2
ip igmp ssm-map static acl_SSM-map-DS-post-splice 192.168.160.2
ip tcp window-size 65535
ip tcp path-mtu-discovery
ip telnet source-interface Loopback0
no ip domain-lookup
ipv6 mfib hardware-switching replication-mode ingress
vtp domain AR1
vtp mode transparent
mls ip multicast replication-mode ingress
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos map dscp-cos 16 18 20 to 3
mls qos map dscp-cos 26 28 30 to 4
mls qos map dscp-cos 34 36 38 to 6
mls qos map dscp-cos 40 42 44 to 2
mls qos map dscp-cos 48 to 5
mls qos
mls rate-limit multicast ipv4 fib-miss 10000 250
mls rate-limit multicast ipv4 connected 2500 250
mls rate-limit multicast ipv4 igmp 1000 10
mls rate-limit multicast ipv4 ip-options 1000 10
mls rate-limit multicast ipv4 partial 500 250
mls rate-limit unicast acl input 1000 10
mls rate-limit unicast acl output 1000 10
no mls rate-limit unicast acl vacl-log
mls rate-limit unicast ip options 1000 10
mls rate-limit all ttl-failure 100 10
mls rate-limit all mtu-failure 100 10
no mls acl tcam share-global
mls cef error action freeze
!
!
!
!
!
!
!
!
!
!
redundancy
 mode sso
```

```
 main-cpu
  auto-sync running-config
  auto-sync standard
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
no spanning-tree vlan 1-4094
error-detection packet-buffer action none
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
!
vlan internal allocation policy ascending
!
!
interface Loopback0
 description RAN Loopback
 ip address 99.99.0.2 255.255.255.255
!
interface Null0
 no ip unreachables
!
interface TenGigabitEthernet1/1
 description Transport between SR1a (TenGig1/1)
 ip address 192.168.250.2 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/2
 description Transport between AR2 (TenGig1/2)
 ip address 192.168.249.1 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/3
 description Transport between HR1a (TenGig1/1)
 ip address 192.168.250.5 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/4
 no ip address
 shutdown
```

```
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 description Management port for Syslog/TFTP/NTP
 ip address 1.1.1.2 255.255.255.0
 media-type rj45
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 100
 router-id 99.99.0.2
 max-metric router-lsa on-startup wait-for-bgp
 log-adjacency-changes detail
 timers throttle spf 400 400 4000
 network 99.99.0.0 0.0.255.255 area 0
 network 192.168.249.0 0.0.0.255 area 0
 network 192.168.250.0 0.0.0.255 area 0
 maximum-paths 6
 default-information originate metric-type 1
!
router bgp 100
 no synchronization
 bgp router-id 99.99.0.2
 bgp log-neighbor-changes
 network 192.168.10.0 route-map rmap_Network-Management
 network 192.168.60.0 route-map rmap_Ad-Insertion
 network 192.168.71.0 route-map rmap_IPmc-DS-Source
 network 192.168.72.0 route-map rmap_IPmc-DB-Source
 network 192.168.80.0 route-map rmap_Voice
 network 192.168.90.0 route-map rmap_Internet-Access
 network 192.168.150.0 route-map rmap_Hub1
 network 192.168.160.0 route-map rmap_Hub2
 network 192.168.170.0 route-map rmap_Hub2
 network 192.168.180.0 route-map rmap_Hub3
 neighbor rr-client peer-group
 neighbor rr-client remote-as 100
 neighbor rr-client update-source Loopback0
 neighbor rr-client version 4
 neighbor rr-client route-reflector-client
 neighbor rr-client send-community
 neighbor ibgp peer-group
 neighbor ibgp remote-as 100
 neighbor ibgp update-source Loopback0
 neighbor ibgp version 4
 neighbor ibgp send-community
 neighbor 99.99.0.1 peer-group rr-client
 neighbor 99.99.0.1 description SR1a
 neighbor 99.99.0.3 peer-group ibgp
 neighbor 99.99.0.3 description AR2
 neighbor 99.99.0.4 peer-group rr-client
 neighbor 99.99.0.4 description HR1a
 neighbor 99.99.0.5 peer-group rr-client
 neighbor 99.99.0.5 description HR2a
 neighbor 99.99.0.6 peer-group rr-client
 neighbor 99.99.0.6 description HR2b
 neighbor 99.99.0.7 peer-group rr-client
 neighbor 99.99.0.7 description HR3a
 no auto-summary
!
```

```
ip classless
!
ip bgp-community new-format
no ip http server
ip pim ssm range acl_SSM-IPmc-range
!
ip access-list standard acl_SSM-IPmc-range
 permit 239.0.0.0 0.255.255.255
ip access-list standard acl_SSM-map-DB
 remark SSM mapping for DB blue/red
 permit 239.16.0.0 0.0.0.255
ip access-list standard acl_SSM-map-DS
 remark SSM mapping for DS blue/red
 permit 239.20.0.0 0.0.255.255
ip access-list standard acl_SSM-map-DS-post-splice
 remark SSM mapping for post splice DS blue/red
 permit 239.28.0.0 0.0.255.255
!
logging event link-status default
logging trap debugging
logging source-interface Loopback0
logging 1.1.1.254
!
route-map rmap_Network-Management permit 100
 set metric 100
!
route-map rmap_Ad-Insertion permit 100
 set metric 100
!
route-map rmap_IPmc-DS-Source permit 100
 set metric 100
!
route-map rmap_IPmc-DB-Source permit 100
 set metric 100
!
route-map rmap_Voice permit 100
 set metric 100
!
route-map rmap_Internet-Access permit 100
 set metric 100
!
route-map rmap_Hub1 permit 100
 set metric 100
!
route-map rmap_Hub2 permit 100
 set metric 100
!
route-map rmap_Hub3 permit 100
 set metric 100
!
!
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
banner motd ^C
##################################################################
```

```
 Project = Video Networking Solution
 Switch = AR1

 Chassis = 6509
 Slot1 = WS-X6704 (3BXL)
 Slot5 = Sup720  (3BXL)


##################################################################
^C
!
line con 0
 exec-timeout 0 0
 history size 100
 transport preferred none
line vty 0 4
 exec-timeout 0 0
 password cisco123
 login
 history size 100
 transport preferred none
!
scheduler runtime netinput 300
ntp clock-period 17179699
ntp source Loopback0
ntp update-calendar
ntp server 1.1.1.254
no cns aaa enable
end
```

Configuration for AR2a

```
!#####################################################################
!
! Description
! ===========
! Video Networking Solution 3.0
! AR2 running-config
!
! Version Information
! ===================
! IOS
! ---
! 12.2(18)SXF
!
! Hardware
! --------
!
! Mod  Port Model              Serial #    Versions
! ---- ---- ------------------ ----------- ----------------------
!   1    4  WS-X6704-10GE      SAD074706G4 Hw : 1.2
!                                         Fw : 12.2(14r)S5
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-F6700-DFC3A     SAD081603HC Hw : 2.2
!   5    2  WS-SUP720-3BXL     SAL09222B4P Hw : 4.3
!                                         Fw : 8.1(3)
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-SUP720          SAL09232GEE Hw : 2.3
!                                         Fw : 12.2(17r)S2
!                                         Sw : 12.2(18)SXF
!           WS-F6K-PFC3BXL     SAL09222CUH Hw : 1.6
!
!#####################################################################
!
!
upgrade fpd auto
version 12.2
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
service counters max age 5
no service dhcp
!
hostname AR2
!
boot system disk0:s72033-adventerprisek9_wan-mz.122-18.SXF.bin
logging snmp-authfail
logging buffered 64000 informational
enable password cisco123
!
no aaa new-model
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
no ip source-route
ip spd mode aggressive
```

```
!
!
!
ip cef accounting non-recursive
ip tftp source-interface Loopback0
no ip bootp server
ip multicast-routing
ip igmp ssm-map enable
no ip igmp ssm-map query dns
ip igmp ssm-map static acl_SSM-map-DB 192.168.71.2
ip igmp ssm-map static acl_SSM-map-DS 192.168.72.2
ip igmp ssm-map static acl_SSM-map-DS-post-splice 192.168.160.2
ip tcp window-size 65535
ip tcp path-mtu-discovery
ip telnet source-interface Loopback0
no ip domain-lookup
vtp domain AR2
vtp mode transparent
mls ip multicast replication-mode ingress
mls ip multicast egress local
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos map dscp-cos 16 18 20 to 3
mls qos map dscp-cos 26 28 30 to 4
mls qos map dscp-cos 34 36 38 to 6
mls qos map dscp-cos 40 42 44 to 2
mls qos map dscp-cos 48 to 5
mls qos
mls rate-limit multicast ipv4 fib-miss 10000 250
mls rate-limit multicast ipv4 connected 2500 250
mls rate-limit multicast ipv4 igmp 1000 10
mls rate-limit multicast ipv4 partial 500 250
mls rate-limit unicast acl input 1000 10
mls rate-limit unicast acl output 1000 10
no mls rate-limit unicast acl vacl-log
mls rate-limit all ttl-failure 100 10
mls rate-limit all mtu-failure 100 10
no mls acl tcam share-global
mls cef error action freeze
!
!
!
!
!
!
!
!
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
  auto-sync standard
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
no spanning-tree vlan 1-4094
error-detection packet-buffer action none
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
!
```

```
vlan internal allocation policy ascending
!
!
interface Loopback0
 description RAN Loopback
 ip address 99.99.0.3 255.255.255.255
!
interface Null0
 no ip unreachables
!
interface TenGigabitEthernet1/1
 description Transport between SR1a (TenGig1/3)
 ip address 192.168.251.2 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/2
 description Transport between AR1 (TenGig1/2)
 ip address 192.168.249.2 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/3
 description Transport between HR3a (TenGig1/1)
 ip address 192.168.251.5 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/4
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 description Management port for Syslog/TFTP/NTP
 ip address 1.1.1.3 255.255.255.0
 media-type rj45
!
interface Vlan1
 no ip address
```

```
 shutdown
!
router ospf 100
 router-id 99.99.0.3
 max-metric router-lsa on-startup wait-for-bgp
 log-adjacency-changes detail
 timers throttle spf 400 400 4000
 network 99.99.0.0 0.0.255.255 area 0
 network 192.168.249.0 0.0.0.255 area 0
 network 192.168.251.0 0.0.0.255 area 0
 maximum-paths 6
 default-information originate metric-type 1
!
router bgp 100
 no synchronization
 bgp router-id 99.99.0.3
 bgp log-neighbor-changes
 network 192.168.10.0 route-map rmap_Network-Management
 network 192.168.60.0 route-map rmap_Ad-Insertion
 network 192.168.71.0 route-map rmap_IPmc-DS-Source
 network 192.168.72.0 route-map rmap_IPmc-DB-Source
 network 192.168.80.0 route-map rmap_Voice
 network 192.168.90.0 route-map rmap_Internet-Access
 network 192.168.150.0 route-map rmap_Hub1
 network 192.168.160.0 route-map rmap_Hub2
 network 192.168.170.0 route-map rmap_Hub2
 network 192.168.180.0 route-map rmap_Hub3
 neighbor rr-client peer-group
 neighbor rr-client remote-as 100
 neighbor rr-client update-source Loopback0
 neighbor rr-client version 4
 neighbor rr-client route-reflector-client
 neighbor rr-client send-community
 neighbor ibgp peer-group
 neighbor ibgp remote-as 100
 neighbor ibgp update-source Loopback0
 neighbor ibgp version 4
 neighbor ibgp send-community
 neighbor 99.99.0.1 peer-group rr-client
 neighbor 99.99.0.1 description SR1a
 neighbor 99.99.0.2 peer-group ibgp
 neighbor 99.99.0.2 description AR1
 neighbor 99.99.0.4 peer-group rr-client
 neighbor 99.99.0.4 description HR1a
 neighbor 99.99.0.5 peer-group rr-client
 neighbor 99.99.0.5 description HR2a
 neighbor 99.99.0.6 peer-group rr-client
 neighbor 99.99.0.6 description HR2b
 neighbor 99.99.0.7 peer-group rr-client
 neighbor 99.99.0.7 description HR3a
 no auto-summary
!
ip classless
!
ip bgp-community new-format
no ip http server
ip pim ssm range acl_SSM-IPmc-range
!
ip access-list standard acl_SSM-IPmc-range
 permit 239.0.0.0 0.255.255.255
ip access-list standard acl_SSM-map-DB
 remark SSM mapping for DB blue/red
 permit 239.16.0.0 0.0.0.255
ip access-list standard acl_SSM-map-DS
```

```
 remark SSM mapping for DS blue/red
 permit 239.20.0.0 0.0.255.255
ip access-list standard acl_SSM-map-DS-post-splice
 remark SSM mapping for post splice DS blue/red
 permit 239.28.0.0 0.0.255.255
!
logging event link-status default
logging trap debugging
logging source-interface Loopback0
logging 1.1.1.254
!
route-map rmap_Network-Management permit 100
 set metric 100
!
route-map rmap_Ad-Insertion permit 100
 set metric 100
!
route-map rmap_IPmc-DS-Source permit 100
 set metric 100
!
route-map rmap_IPmc-DB-Source permit 100
 set metric 100
!
route-map rmap_Voice permit 100
 set metric 100
!
route-map rmap_Internet-Access permit 100
 set metric 100
!
route-map rmap_Hub1 permit 100
 set metric 100
!
route-map rmap_Hub2 permit 100
 set metric 100
!
route-map rmap_Hub3 permit 100
 set metric 100
!
!
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
banner motd ^C
######################################################################


 Project = Video Networking Solution
 Switch = AR2

 Chassis = 6509
 Slot1 = WS-X6704 (3A)
 Slot5 = Sup720  (3BXL)



######################################################################
^C
!
```

```
line con 0
 exec-timeout 0 0
 history size 100
 transport preferred none
line vty 0 4
 exec-timeout 0 0
 password cisco123
 login
 history size 100
 transport preferred none
!
monitor event-trace timestamps
scheduler runtime netinput 300
ntp clock-period 17179765
ntp source Loopback0
ntp update-calendar
ntp server 1.1.1.254
no cns aaa enable
end
```

Configurations for the Hub Routers

The following configurations are presented:

- Configuration for HR1a
- Configuration for HR2a
- Configuration for HR2b
- Configuration for HR3a

Configuration for HR1a

```
!#####################################################################
!
! Description
! ===========
! Video Networking Solution 3.0
! HR1a running-config
!
! Version Information
! ===================
! IOS
! ---
! 12.2(18)SXF
!
! Hardware
! --------
!
! Mod  Port Model              Serial #    Versions
! ---- ---- ------------------ ----------- -----------------------
!   1    4  WS-X6704-10GE      SAL09337DQA Hw : 2.2
!                                         Fw : 12.2(14r)S5
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-F6700-DFC3BXL   SAL09274W3N Hw : 5.0
!   2   24  WS-X6724-SFP       SAL093486ND Hw : 2.3
!                                         Fw : 12.2(14r)S5
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-F6700-DFC3BXL   SAL0930689L Hw : 5.2
!   5    2  WS-SUP720-3BXL     SAL09337GL6 Hw : 4.3
!                                         Fw : 8.1(3)
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-SUP720          SAL09337FTZ Hw : 2.3
!                                         Fw : 12.2(17r)S2
!                                         Sw : 12.2(18)SXF
!           WS-F6K-PFC3BXL     SAL09337FN8 Hw : 1.6
!
!#####################################################################
!
!
upgrade fpd auto
version 12.2
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
```

```
service timestamps log datetime msec localtime
no service password-encryption
service internal
service counters max age 5
no service dhcp
!
hostname HR1a
!
boot system disk0:s72033-adventerprisek9_wan-mz.122-18.SXF.bin
logging snmp-authfail
logging buffered 64000 informational
no logging console
enable password cisco123
!
no aaa new-model
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
no ip source-route
ip spd mode aggressive
!
!
!
ip cef accounting non-recursive
ip tftp source-interface Loopback0
no ip bootp server
ip multicast-routing
ip igmp ssm-map enable
no ip igmp ssm-map query dns
ip igmp ssm-map static acl_SSM-map-DB 192.168.71.2
ip igmp ssm-map static acl_SSM-map-DS 192.168.72.2
ip igmp ssm-map static acl_SSM-map-DS-post-splice 192.168.160.2
ip tcp window-size 65535
ip tcp path-mtu-discovery
ip telnet source-interface Loopback0
no ip domain-lookup
vtp domain HR1a
vtp mode transparent
mls ip multicast replication-mode ingress
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos map dscp-cos 16 18 20 to 3
mls qos map dscp-cos 26 28 30 to 4
mls qos map dscp-cos 34 36 38 to 6
mls qos map dscp-cos 40 42 44 to 2
mls qos map dscp-cos 48 to 5
mls qos
mls rate-limit multicast ipv4 fib-miss 10000 250
mls rate-limit multicast ipv4 connected 2500 250
mls rate-limit multicast ipv4 igmp 1000 10
mls rate-limit multicast ipv4 ip-options 1000 10
mls rate-limit multicast ipv4 partial 500 250
mls rate-limit unicast acl input 1000 10
mls rate-limit unicast acl output 1000 10
no mls rate-limit unicast acl vacl-log
mls rate-limit unicast ip options 1000 10
mls rate-limit all ttl-failure 100 10
mls rate-limit all mtu-failure 100 10
no mls acl tcam share-global
mls cef error action freeze
!
!
!
```

```
!
!
!
!
!
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
  auto-sync standard
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
no spanning-tree vlan 1-4094
!
power redundancy-mode combined
error-detection packet-buffer action none
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
!
vlan internal allocation policy ascending
!
class-map match-all class_voice
  match access-group name acl_voice
class-map match-all class_broadcast-video
  match access-group name acl_broadcast-video
class-map match-all class_ad-server
  match access-group name acl_ad-server
class-map match-all class_video-signaling
  match access-group name acl_video-signaling
class-map match-all class_net-mgmt
  match access-group name acl_net-mgmt
class-map match-all class_internet-access
  match access-group name acl_internet-access
class-map match-all class_suspect
  match access-group name acl_permit-any
!
!
policy-map pmap_voice-port
  class class_voice
   trust dscp
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_broadcast-video-port
  class class_broadcast-video
   set dscp af41
  class class_video-signaling
   set dscp cs3
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_ad-server-port
  class class_ad-server
   set dscp af41
  class class_video-signaling
   set dscp cs3
  class class_net-mgmt
```

```
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_net-mgmt-port
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_internet-access-port
  class class_internet-access
   set dscp 8
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
!
!
!
interface Loopback0
 description RAN Loopback
 ip address 99.99.0.4 255.255.255.255
!
interface Loopback1
 description Hub Loopback
 ip address 99.99.1.4 255.255.255.255
!
interface Null0
 no ip unreachables
!
interface TenGigabitEthernet1/1
 description Transport between AR1 (TenGig1/3)
 ip address 192.168.250.6 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip multicast boundary acl_Hub-only-IPmc
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/2
 no ip address
 shutdown
!
interface TenGigabitEthernet1/3
 description Transport between HR2a (TenGig1/1)
 ip address 192.168.250.9 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip multicast boundary acl_Hub-only-IPmc
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/4
 no ip address
 shutdown
```

```
!
!
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 description Management port for Syslog/TFTP/NTP
 ip address 1.1.1.4 255.255.255.0
 media-type rj45
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 100
 router-id 99.99.0.4
 max-metric router-lsa on-startup wait-for-bgp
 log-adjacency-changes detail
 timers throttle spf 400 400 4000
 passive-interface default
 no passive-interface TenGigabitEthernet1/1
 no passive-interface TenGigabitEthernet1/3
 network 99.99.0.0 0.0.255.255 area 0
 network 192.168.250.0 0.0.0.255 area 0
 maximum-paths 6
!
router bgp 100
 no synchronization
 bgp router-id 99.99.0.4
 bgp log-neighbor-changes
 redistribute connected route-map rmap_Connected-to-BGP
 neighbor rr-server peer-group
 neighbor rr-server remote-as 100
 neighbor rr-server update-source Loopback0
 neighbor rr-server version 4
 neighbor rr-server send-community
 neighbor 99.99.0.2 peer-group rr-server
 neighbor 99.99.0.2 description AR1
 neighbor 99.99.0.3 peer-group rr-server
 neighbor 99.99.0.3 description AR2
 no auto-summary
!
ip classless
!
ip bgp-community new-format
no ip http server
ip pim ssm range acl_SSM-IPmc-range
!
ip access-list standard acl_SSM-IPmc-range
 permit 239.0.0.0 0.255.255.255
ip access-list standard acl_SSM-map-DB
 remark SSM mapping for DB blue/red
 permit 239.16.0.0 0.0.0.255
ip access-list standard acl_SSM-map-DS
 remark SSM mapping for DS blue/red
 permit 239.20.0.0 0.0.255.255
ip access-list standard acl_SSM-map-DS-post-splice
 remark SSM mapping for post splice DS blue/red
 permit 239.28.0.0 0.0.255.255
!
ip access-list extended acl_voice
 remark Identify voice traffic
```

```
 permit ip any 192.168.80.0 0.0.0.255
ip access-list extended acl_broadcast-video
 remark Identify broadcast video traffic (multicast on 239.x.x.x)
 permit ip any 239.0.0.0 0.255.255.255
ip access-list extended acl_video-signaling
 remark Identify video signaling
 permit ip any 192.168.61.0 0.0.0.255
ip access-list extended acl_net-mgmt
 remark Identify net management traffic (TFTP, Syslog, NTP, etc)
 permit ip any 192.168.10.0 0.0.0.255
ip access-list extended acl_internet-access
 remark Identify Internet access traffic
 permit ip any 192.168.90.0 0.0.0.255
ip access-list extended acl_permit-any
 permit ip any any
!
ip access-list extended acl_qam-port
 remark Permit only video and signaling out port connected to QAM
 permit ip any any dscp af41
 permit ip any any dscp af43
 permit ip any any dscp cs3
 permit ip any any dscp cs6
 deny   ip any any
ip access-list standard acl_Hub-only-IPmc
 remark Multicast video in 239.255.0.0/16 must remain in Hub
 deny   239.255.0.0 0.0.255.255
 remark Allow all other IPmc to pass
 permit any
!
!
ip prefix-list pl_Connected-to-BGP seq 5 permit 192.168.150.0/24 le 32
logging event link-status default
logging trap debugging
logging source-interface Loopback0
logging 1.1.1.254
!
route-map rmap_Connected-to-BGP permit 100
 match ip address prefix-list pl_Connected-to-BGP
 set metric 100
 set ip next-hop 99.99.0.4
!
!
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
banner motd ^C
######################################################################


 Project = Video Networking Solution
 Switch = HR1a

 Chassis = 7606
 Slot1 = WS-X6704 (3BXL)
 Slot2 = WS-X6724 (3BXL)
 Slot5 = Sup720  (3BXL)
```

```
##################################################################
^C
!
line con 0
 exec-timeout 0 0
 history size 100
 transport preferred none
line vty 0 4
 exec-timeout 0 0
 password cisco123
 login
 history size 100
 transport preferred none
!
scheduler runtime netinput 300
ntp clock-period 17179872
ntp source Loopback0
ntp update-calendar
ntp server 1.1.1.254
no cns aaa enable
end
```

Configuration for HR2a

```
!#####################################################################
!
! Description
! ===========
! Video Networking Solution 3.0
! HR2a running-config
!
! Version Information
! ===================
! IOS
! ---
! 12.2(18)SXF
!
! Hardware
! --------
!
! Mod  Port Model              Serial #    Versions
! ---- ---- ------------------ ----------- ----------------------
!   1    4  WS-X6704-10GE      SAL09337DN3 Hw : 2.2
!                                         Fw : 12.2(14r)S5
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-F6700-DFC3BXL   SAL09295P64 Hw : 5.0
!   2   48  WS-X6748-GE-TX     SAD0805027C Hw : 1.4
!                                         Fw : 12.2(14r)S5
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-F6700-DFC3BXL   SAD0917016G Hw : 4.0
!   5    2  WS-SUP720-3BXL     SAL09169RG7 Hw : 4.3
!                                         Fw : 8.1(3)
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-SUP720          SAL09169UAY Hw : 2.3
!                                         Fw : 12.2(17r)S2
!                                         Sw : 12.2(18)SXF
!           WS-F6K-PFC3BXL     SAL091594SL Hw : 1.6
!
!#####################################################################
!
!
upgrade fpd auto
version 12.2
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
service counters max age 5
no service dhcp
!
hostname HR2a
!
boot system disk0:s72033-adventerprisek9_wan-mz.122-18.SXF.bin
logging snmp-authfail
logging buffered 64000 informational
no logging console
enable password cisco123
!
```

```
no aaa new-model
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
no ip source-route
ip spd mode aggressive
!
!
!
ip cef accounting non-recursive
ip tftp source-interface Loopback0
no ip bootp server
ip multicast-routing
ip igmp ssm-map enable
no ip igmp ssm-map query dns
ip igmp ssm-map static acl_SSM-map-DB 192.168.71.2
ip igmp ssm-map static acl_SSM-map-DS 192.168.72.2
ip igmp ssm-map static acl_SSM-map-DS-post-splice 192.168.160.2
ip tcp window-size 65535
ip tcp path-mtu-discovery
ip telnet source-interface Loopback0
no ip domain-lookup
vtp domain HR2a
vtp mode transparent
mls ip multicast replication-mode ingress
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos map dscp-cos 16 18 20 to 3
mls qos map dscp-cos 26 28 30 to 4
mls qos map dscp-cos 34 36 38 to 6
mls qos map dscp-cos 40 42 44 to 2
mls qos map dscp-cos 48 to 5
mls qos
mls rate-limit multicast ipv4 fib-miss 10000 250
mls rate-limit multicast ipv4 connected 2500 250
mls rate-limit multicast ipv4 igmp 1000 10
mls rate-limit multicast ipv4 ip-options 1000 10
mls rate-limit multicast ipv4 partial 500 250
mls rate-limit unicast acl input 1000 10
mls rate-limit unicast acl output 1000 10
no mls rate-limit unicast acl vacl-log
mls rate-limit unicast ip options 1000 10
mls rate-limit all ttl-failure 100 10
mls rate-limit all mtu-failure 100 10
no mls acl tcam share-global
mls cef error action freeze
!
!
!
!
!
!
!
!
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
  auto-sync standard
!
spanning-tree mode pvst
```

```
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
no spanning-tree vlan 1-4094
error-detection packet-buffer action none
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
!
vlan internal allocation policy ascending
!
class-map match-all class_voice
  match access-group name acl_voice
class-map match-all class_broadcast-video
  match access-group name acl_broadcast-video
class-map match-all class_ad-server
  match access-group name acl_ad-server
class-map match-all class_video-signaling
  match access-group name acl_video-signaling
class-map match-all class_net-mgmt
  match access-group name acl_net-mgmt
class-map match-all class_internet-access
  match access-group name acl_internet-access
class-map match-all class_suspect
  match access-group name acl_permit-any
!
!
policy-map pmap_voice-port
  class class_voice
   trust dscp
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_broadcast-video-port
  class class_broadcast-video
   set dscp af41
  class class_video-signaling
   set dscp cs3
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_ad-server-port
  class class_ad-server
   set dscp af41
  class class_video-signaling
   set dscp cs3
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_net-mgmt-port
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_internet-access-port
  class class_internet-access
   set dscp 8
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
!
```

```
!
!
interface Loopback0
 description RAN Loopback
 ip address 99.99.0.5 255.255.255.255
!
interface Loopback1
 description Hub Loopbacks
 ip address 99.99.1.6 255.255.255.255 secondary
 ip address 99.99.1.5 255.255.255.255
 no ip redirects
!
interface Loopback99
 description Multicast Rendevouz Point
 ip address 99.99.99.5 255.255.255.255
!
interface Null0
 no ip unreachables
!
interface TenGigabitEthernet1/1
 description Transport between HR1a (TenGig1/3)
 ip address 192.168.250.10 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip multicast boundary acl_Hub-only-IPmc
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/2
 no ip address
 shutdown
!
interface TenGigabitEthernet1/3
 description Transport between HR2b (TenGig1/3)
 ip address 192.168.249.5 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/4
 no ip address
 shutdown
!
interface GigabitEthernet2/1
 description Voice over IP VoIP2a
 ip address 192.168.161.1 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 no cdp enable
 service-policy input pmap_voice-port
!
interface GigabitEthernet2/2
```

```
 description Internet Access IA2a
 ip address 192.168.162.1 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 no cdp enable
 service-policy input pmap_internet-access-port
!
interface GigabitEthernet2/3
 description Local PEG video PEG2a
 ip address 192.168.160.13 255.255.255.252
 ip access-group acl_qam-port out
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 no cdp enable
 service-policy input pmap_broadcast-video-port
!
interface GigabitEthernet2/4
 description CherryPicker DM2a (Port 1) - Pre/Post-splice DS
 ip address 192.168.160.1 255.255.255.252
 ip access-group acl_qam-port out
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 no cdp enable
 service-policy input pmap_broadcast-video-port
!
interface GigabitEthernet2/5
 description Motorola SEM2a (GigE 1) - DS Post-splice
 ip address 192.168.160.5 255.255.255.252
 ip access-group acl_qam-port out
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 no cdp enable
 service-policy input pmap_broadcast-video-port
!
interface GigabitEthernet2/6
 description Motorola SEM2b (GigE 1) - DB
 ip address 192.168.160.9 255.255.255.252
 ip access-group acl_qam-port out
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 no cdp enable
 service-policy input pmap_broadcast-video-port
!
interface GigabitEthernet2/7
 no ip address
 shutdown
!
```

```
!
! <<<omitted interface GigabitEthernet2/8 - interface GigabitEthernet2/47
!
!
interface GigabitEthernet2/48
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 description Management port for Syslog/TFTP/NTP
 ip address 1.1.1.5 255.255.255.0
 media-type rj45
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 100
 router-id 99.99.0.5
 max-metric router-lsa on-startup wait-for-bgp
 log-adjacency-changes detail
 timers throttle spf 400 400 4000
 passive-interface default
 no passive-interface TenGigabitEthernet1/1
 no passive-interface TenGigabitEthernet1/3
 network 99.99.0.0 0.0.255.255 area 0
 network 192.168.249.0 0.0.0.255 area 0
 network 192.168.250.0 0.0.0.255 area 0
 maximum-paths 6
!
router bgp 100
 no synchronization
 bgp router-id 99.99.0.5
 bgp log-neighbor-changes
 redistribute connected route-map rmap_Connected-to-BGP
 neighbor rr-server peer-group
 neighbor rr-server remote-as 100
 neighbor rr-server update-source Loopback0
 neighbor rr-server version 4
 neighbor rr-server send-community
 neighbor 99.99.0.2 peer-group rr-server
 neighbor 99.99.0.2 description AR1
 neighbor 99.99.0.3 peer-group rr-server
 neighbor 99.99.0.3 description AR2
 no auto-summary
!
ip classless
!
ip bgp-community new-format
no ip http server
ip pim ssm range acl_SSM-IPmc-range
!
ip access-list standard acl_SSM-IPmc-range
 permit 239.0.0.0 0.255.255.255
ip access-list standard acl_SSM-map-DB
 remark SSM mapping for DB blue/red
 permit 239.16.0.0 0.0.0.255
ip access-list standard acl_SSM-map-DS
 remark SSM mapping for DS blue/red
 permit 239.20.0.0 0.0.255.255
```

```
ip access-list standard acl_SSM-map-DS-post-splice
 remark SSM mapping for post splice DS blue/red
 permit 239.28.0.0 0.0.255.255
!
ip access-list extended acl_voice
 remark Identify voice traffic
 permit ip any 192.168.80.0 0.0.0.255
ip access-list extended acl_broadcast-video
 remark Identify broadcast video traffic (multicast on 239.x.x.x)
 permit ip any 239.0.0.0 0.255.255.255
ip access-list extended acl_video-signaling
 remark Identify video signaling
 permit ip any 192.168.61.0 0.0.0.255
ip access-list extended acl_net-mgmt
 remark Identify net management traffic (TFTP, Syslog, NTP, etc)
 permit ip any 192.168.10.0 0.0.0.255
ip access-list extended acl_internet-access
 remark Identify Internet access traffic
 permit ip any 192.168.90.0 0.0.0.255
ip access-list extended acl_permit-any
 permit ip any any
!
ip access-list extended acl_qam-port
 remark Permit only video and signaling out port connected to QAM
 permit ip any any dscp af41
 permit ip any any dscp af43
 permit ip any any dscp cs3
 permit ip any any dscp cs6
 deny   ip any any
ip access-list standard acl_Hub-only-IPmc
 remark Multicast video in 239.255.0.0/16 must remain in Hub
 deny   239.255.0.0 0.0.255.255
 remark Allow all other IPmc to pass
 permit any
!
!
ip prefix-list pl_Connected-to-BGP seq 5 permit 192.168.160.0/24 le 32
logging event link-status default
logging trap debugging
logging source-interface Loopback0
logging 1.1.1.254
!
route-map rmap_Connected-to-BGP permit 100
 match ip address prefix-list pl_Connected-to-BGP
 set metric 100
 set ip next-hop 99.99.0.5
!
!
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
banner motd ^C
##################################################################


 Project = Video Networking Solution
 Switch = HR2a
```

```
 Chassis = 7606
 Slot1 = WS-X6704 (3BXL)
 Slot2 = WS-X6748 (3BXL)
 Slot5 = Sup720  (3BXL)


##########################################################################
^C
!
line con 0
 exec-timeout 0 0
 history size 100
 transport preferred none
line vty 0 4
 exec-timeout 0 0
 password cisco123
 login
 history size 100
 transport preferred none
!
scheduler runtime netinput 300
ntp clock-period 17179860
ntp source Loopback0
ntp update-calendar
ntp server 1.1.1.254
no cns aaa enable
end
```

Configuration for HR2b

```
!#####################################################################
!
! Description
! ===========
! Video Networking Solution 3.0
! HR2b running-config
!
! Version Information
! ===================
! IOS
! ---
! 12.2(18)SXF
!
! Hardware
! --------
!
! Mod  Port Model              Serial #    Versions
! ---- ---- ------------------ ----------- ---------------------
!   1    4  WS-X6704-10GE      SAD074604B5 Hw : 1.2
!                                         Fw : 12.2(14r)S5
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-F6700-DFC3A     SAD08150203 Hw : 2.1
!   2   24  WS-X6724-SFP       SAD091503A7 Hw : 2.2
!                                         Fw : 12.2(14r)S5
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-F6700-DFC3A     SAD08140B7D Hw : 2.1
!   5    2  WS-SUP720-BASE     SAD07510A0A Hw : 3.0
!                                         Fw : 7.7(1)
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-SUP720          SAD075109GK Hw : 2.0
!                                         Fw : 12.2(14r)S9
!                                         Sw : 12.2(18)SXF
!           WS-F6K-PFC3BXL     SAD0817029M Hw : 1.2
!
!#####################################################################
!
!
upgrade fpd auto
version 12.2
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
service counters max age 5
no service dhcp
!
hostname HR2b
!
boot system disk0:s72033-adventerprisek9_wan-mz.122-18.SXF.bin
logging snmp-authfail
logging buffered 64000 informational
enable password cisco123
!
no aaa new-model
```

```
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
no ip source-route
ip spd mode aggressive
!
!
!
ip cef accounting non-recursive
ip tftp source-interface Loopback0
no ip bootp server
ip multicast-routing
ip igmp ssm-map enable
no ip igmp ssm-map query dns
ip igmp ssm-map static acl_SSM-map-DB 192.168.71.2
ip igmp ssm-map static acl_SSM-map-DS 192.168.72.2
ip igmp ssm-map static acl_SSM-map-DS-post-splice 192.168.160.2
ip tcp window-size 65535
ip tcp path-mtu-discovery
ip telnet source-interface Loopback0
no ip domain-lookup
vtp domain HR2b
vtp mode transparent
mls ip multicast replication-mode ingress
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos map dscp-cos 16 18 20 to 3
mls qos map dscp-cos 26 28 30 to 4
mls qos map dscp-cos 34 36 38 to 6
mls qos map dscp-cos 40 42 44 to 2
mls qos map dscp-cos 48 to 5
mls qos
mls rate-limit multicast ipv4 fib-miss 10000 250
mls rate-limit multicast ipv4 connected 2500 250
mls rate-limit multicast ipv4 igmp 1000 10
mls rate-limit multicast ipv4 partial 500 250
mls rate-limit unicast acl input 1000 10
mls rate-limit unicast acl output 1000 10
no mls rate-limit unicast acl vacl-log
mls rate-limit all ttl-failure 100 10
mls rate-limit all mtu-failure 100 10
no mls acl tcam share-global
mls cef error action freeze
!
!
!
!
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
  auto-sync standard
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
no spanning-tree vlan 1-4094
!
power redundancy-mode combined
error-detection packet-buffer action none
diagnostic cns publish cisco.cns.device.diag_results
```

```
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
!
vlan internal allocation policy ascending
!
class-map match-all class_voice
  match access-group name acl_voice
class-map match-all class_broadcast-video
  match access-group name acl_broadcast-video
class-map match-all class_ad-server
  match access-group name acl_ad-server
class-map match-all class_video-signaling
  match access-group name acl_video-signaling
class-map match-all class_net-mgmt
  match access-group name acl_net-mgmt
class-map match-all class_internet-access
  match access-group name acl_internet-access
class-map match-all class_suspect
  match access-group name acl_permit-any
!
!
policy-map pmap_voice-port
  class class_voice
   trust dscp
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_broadcast-video-port
  class class_broadcast-video
   set dscp af41
  class class_video-signaling
   set dscp cs3
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_ad-server-port
  class class_ad-server
   set dscp af41
  class class_video-signaling
   set dscp cs3
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_net-mgmt-port
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_internet-access-port
  class class_internet-access
   set dscp 8
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
!
!
!
interface Loopback0
 description RAN Loopback
 ip address 99.99.0.6 255.255.255.255
```

```
!
interface Loopback1
 description Hub Loopbacks
 ip address 99.99.1.5 255.255.255.255 secondary
 ip address 99.99.1.6 255.255.255.255
 no ip redirects
!
interface Null0
 no ip unreachables
!
interface TenGigabitEthernet1/1
 description Transport between HR3a (TenGig1/3)
 ip address 192.168.251.10 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip multicast boundary acl_Hub-only-IPmc
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/2
 no ip address
 shutdown
!
interface TenGigabitEthernet1/3
 description Transport between HR2a (TenGig1/3)
 ip address 192.168.249.6 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/4
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 description Management port for Syslog/TFTP/NTP
 ip address 1.1.1.6 255.255.255.0
 media-type rj45
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 100
 router-id 99.99.0.6
 max-metric router-lsa on-startup wait-for-bgp
 log-adjacency-changes detail
 timers throttle spf 400 400 4000
 passive-interface default
```

```
 no passive-interface TenGigabitEthernet1/1
 no passive-interface TenGigabitEthernet1/3
 network 99.99.0.0 0.0.255.255 area 0
 network 192.168.249.0 0.0.0.255 area 0
 network 192.168.251.0 0.0.0.255 area 0
 maximum-paths 6
!
router bgp 100
 no synchronization
 bgp router-id 99.99.0.6
 bgp log-neighbor-changes
 redistribute connected route-map rmap_Connected-to-BGP
 neighbor rr-server peer-group
 neighbor rr-server remote-as 100
 neighbor rr-server update-source Loopback0
 neighbor rr-server version 4
 neighbor rr-server send-community
 neighbor 99.99.0.2 peer-group rr-server
 neighbor 99.99.0.2 description AR1
 neighbor 99.99.0.3 peer-group rr-server
 neighbor 99.99.0.3 description AR2
 no auto-summary
!
ip classless
!
ip bgp-community new-format
no ip http server
ip pim ssm range acl_SSM-IPmc-range
!
ip access-list standard acl_SSM-IPmc-range
 permit 239.0.0.0 0.255.255.255
ip access-list standard acl_SSM-map-DB
 remark SSM mapping for DB blue/red
 permit 239.16.0.0 0.0.0.255
ip access-list standard acl_SSM-map-DS
 remark SSM mapping for DS blue/red
 permit 239.20.0.0 0.0.255.255
ip access-list standard acl_SSM-map-DS-post-splice
 remark SSM mapping for post splice DS blue/red
 permit 239.28.0.0 0.0.255.255
!
ip access-list extended acl_voice
 remark Identify voice traffic
 permit ip any 192.168.80.0 0.0.0.255
ip access-list extended acl_broadcast-video
 remark Identify broadcast video traffic (multicast on 239.x.x.x)
 permit ip any 239.0.0.0 0.255.255.255
ip access-list extended acl_video-signaling
 remark Identify video signaling
 permit ip any 192.168.61.0 0.0.0.255
ip access-list extended acl_net-mgmt
 remark Identify net management traffic (TFTP, Syslog, NTP, etc)
 permit ip any 192.168.10.0 0.0.0.255
ip access-list extended acl_internet-access
 remark Identify Internet access traffic
 permit ip any 192.168.90.0 0.0.0.255
ip access-list extended acl_permit-any
 permit ip any any
!
ip access-list extended acl_qam-port
 remark Permit only video and sinaling out port connected to QAM
 permit ip any any dscp af41
 permit ip any any dscp af43
 permit ip any any dscp cs3
```

```
 permit ip any any dscp cs6
 deny   ip any any
ip access-list standard acl_Hub-only-IPmc
 remark Multicast video in 239.255.0.0/16 must remain in Hub
 deny   239.255.0.0 0.0.255.255
 remark Allow all other IPmc to pass
 permit any
!
!
ip prefix-list pl_Connected-to-BGP seq 5 permit 192.168.170.0/24 le 32
logging event link-status default
logging source-interface Loopback0
logging 1.1.1.254
!
route-map rmap_Connected-to-BGP permit 100
 match ip address prefix-list pl_Connected-to-BGP
 set metric 100
 set ip next-hop 99.99.0.6
!
!
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
banner motd ^C
######################################################################


 Project = Video Networking Solution
 Switch = HR2b

 Chassis = 7606
 Slot1 = WS-X6704 (3A)
 Slot2 = WS-X6748 (3A)
 Slot5 = Sup720  (3BXL)


######################################################################
^C
!
line con 0
 exec-timeout 0 0
 history size 100
 transport preferred none
line vty 0 4
 exec-timeout 0 0
 password cisco123
 login
 history size 100
 transport preferred none
!
scheduler runtime netinput 300
ntp clock-period 17179977
ntp source Loopback0
ntp update-calendar
ntp server 1.1.1.254
no cns aaa enable
end
```

Configuration for HR3a

```
!#####################################################################
!
! Description
! ===========
! Video Networking Solution 3.0
! HR3a running-config
!
! Version Information
! ===================
! IOS
! ---
! 12.2(18)SXF
!
! Hardware
! --------
!
! Mod  Port Model              Serial #    Versions
! ---- ---- ------------------ ----------- -------------------------------------
!   1    4  WS-X6704-10GE      SAL09337QJF Hw : 2.2
!                                         Fw : 12.2(14r)S5
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-F6700-DFC3A     SAD08240A5L Hw : 2.2
!   2   48  WS-X6748-GE-TX     SAL091052FB Hw : 2.1
!                                         Fw : 12.2(14r)S5
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-F6700-DFC3A     SAD0816029X Hw : 2.2
!   5    2  WS-SUP720-3BXL     SAL09337CES Hw : 4.3
!                                         Fw : 8.1(3)
!                                         Sw : 12.2(18)SXF
!                                         Sw1: 8.6(0.123)RFW8
!           WS-SUP720          SAL09316T46 Hw : 2.3
!                                         Fw : 12.2(17r)S2
!                                         Sw : 12.2(18)SXF
!           WS-F6K-PFC3BXL     SAL09337FPL Hw : 1.6
!
!#####################################################################
!
!
upgrade fpd auto
version 12.2
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
service counters max age 5
no service dhcp
!
hostname HR3a
!
boot system disk0:s72033-adventerprisek9_wan-mz.122-18.SXF.bin
logging snmp-authfail
logging buffered 64000 informational
enable password cisco123
!
no aaa new-model
```

```
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
no ip source-route
ip spd mode aggressive
!
!
!
ip cef accounting non-recursive
ip tftp source-interface Loopback0
no ip bootp server
ip multicast-routing
ip igmp ssm-map enable
no ip igmp ssm-map query dns
ip igmp ssm-map static acl_SSM-map-DB 192.168.71.2
ip igmp ssm-map static acl_SSM-map-DS 192.168.72.2
ip igmp ssm-map static acl_SSM-map-DS-post-splice 192.168.160.2
ip tcp window-size 65535
ip tcp path-mtu-discovery
ip telnet source-interface Loopback0
no ip domain-lookup
vtp domain HR3a
vtp mode transparent
mls ip multicast replication-mode ingress
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos map dscp-cos 16 18 20 to 3
mls qos map dscp-cos 26 28 30 to 4
mls qos map dscp-cos 34 36 38 to 6
mls qos map dscp-cos 40 42 44 to 2
mls qos map dscp-cos 48 to 5
mls qos
mls rate-limit multicast ipv4 fib-miss 10000 250
mls rate-limit multicast ipv4 connected 2500 250
mls rate-limit multicast ipv4 igmp 1000 10
mls rate-limit multicast ipv4 partial 500 250
mls rate-limit unicast acl input 1000 10
mls rate-limit unicast acl output 1000 10
no mls rate-limit unicast acl vacl-log
mls rate-limit all ttl-failure 100 10
mls rate-limit all mtu-failure 100 10
no mls acl tcam share-global
mls cef error action freeze
!
!
!
!
!
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
  auto-sync standard
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
no spanning-tree vlan 1-4094
!
power redundancy-mode combined
error-detection packet-buffer action none
```

```
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
!
vlan internal allocation policy ascending
!
class-map match-all class_voice
  match access-group name acl_voice
class-map match-all class_broadcast-video
  match access-group name acl_broadcast-video
class-map match-all class_ad-server
  match access-group name acl_ad-server
class-map match-all class_video-signaling
  match access-group name acl_video-signaling
class-map match-all class_net-mgmt
  match access-group name acl_net-mgmt
class-map match-all class_internet-access
  match access-group name acl_internet-access
class-map match-all class_suspect
  match access-group name acl_permit-any
!
!
policy-map pmap_voice-port
  class class_voice
   trust dscp
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_broadcast-video-port
  class class_broadcast-video
   set dscp af41
  class class_video-signaling
   set dscp cs3
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_ad-server-port
  class class_ad-server
   set dscp af41
  class class_video-signaling
   set dscp cs3
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_net-mgmt-port
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
policy-map pmap_internet-access-port
  class class_internet-access
   set dscp 8
  class class_net-mgmt
   set dscp cs2
  class class_suspect
   set dscp default
!
!
!
interface Loopback0
 description RAN Loopback
```

```
 ip address 99.99.0.7 255.255.255.255
!
interface Loopback1
 description Hub Loopback
 ip address 99.99.1.7 255.255.255.255
!
interface Null0
 no ip unreachables
!
interface TenGigabitEthernet1/1
 description Transport between AR2 (TenGig1/3)
 ip address 192.168.251.6 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip multicast boundary acl_Hub-only-IPmc
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/2
 no ip address
 shutdown
!
interface TenGigabitEthernet1/3
 description Transport between HR2b (TenGig1/1)
 ip address 192.168.251.9 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-mode
 ip multicast boundary acl_Hub-only-IPmc
 ip ospf network point-to-point
 ip ospf hello-interval 1
 wrr-queue cos-map 1 3 2
 wrr-queue cos-map 2 1 3
 wrr-queue cos-map 2 2 4
 mls qos trust dscp
!
interface TenGigabitEthernet1/4
 no ip address
 shutdown
!
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 description Management port for Syslog/TFTP/NTP
 ip address 1.1.1.7 255.255.255.0
 media-type rj45
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 100
 router-id 99.99.0.7
 max-metric router-lsa on-startup wait-for-bgp
 log-adjacency-changes detail
 timers throttle spf 400 400 4000
```

```
 passive-interface default
 no passive-interface TenGigabitEthernet1/1
 no passive-interface TenGigabitEthernet1/3
 network 99.99.0.0 0.0.255.255 area 0
 network 192.168.251.0 0.0.0.255 area 0
 maximum-paths 6
!
router bgp 100
 no synchronization
 bgp router-id 99.99.0.7
 bgp log-neighbor-changes
 redistribute connected route-map rmap_Connected-to-BGP
 neighbor rr-server peer-group
 neighbor rr-server remote-as 100
 neighbor rr-server update-source Loopback0
 neighbor rr-server version 4
 neighbor rr-server send-community
 neighbor 99.99.0.2 peer-group rr-server
 neighbor 99.99.0.2 description AR1
 neighbor 99.99.0.3 peer-group rr-server
 neighbor 99.99.0.3 description AR2
 no auto-summary
!
ip classless
!
ip bgp-community new-format
no ip http server
ip pim ssm range acl_SSM-IPmc-range
!
ip access-list standard acl_SSM-IPmc-range
 permit 239.0.0.0 0.255.255.255
ip access-list standard acl_SSM-map-DB
 remark SSM mapping for DB blue/red
 permit 239.16.0.0 0.0.0.255
ip access-list standard acl_SSM-map-DS
 remark SSM mapping for DS blue/red
 permit 239.20.0.0 0.0.255.255
ip access-list standard acl_SSM-map-DS-post-splice
 remark SSM mapping for post splice DS blue/red
 permit 239.28.0.0 0.0.255.255
!
ip access-list extended acl_voice
 remark Identify voice traffic
 permit ip any 192.168.80.0 0.0.0.255
ip access-list extended acl_broadcast-video
 remark Identify broadcast video traffic (multicast on 239.x.x.x)
 permit ip any 239.0.0.0 0.255.255.255
ip access-list extended acl_video-signaling
 remark Identify video signaling
 permit ip any 192.168.61.0 0.0.0.255
ip access-list extended acl_net-mgmt
 remark Identify net management traffic (TFTP, Syslog, NTP, etc)
 permit ip any 192.168.10.0 0.0.0.255
ip access-list extended acl_internet-access
 remark Identify Internet access traffic
 permit ip any 192.168.90.0 0.0.0.255
ip access-list extended acl_permit-any
 permit ip any any
!
ip access-list extended acl_qam-port
 remark Permit only video and sinaling out port connected to QAM
 permit ip any any dscp af41
 permit ip any any dscp af43
 permit ip any any dscp cs3
```

```
 permit ip any any dscp cs6
 deny   ip any any
ip access-list standard acl_Hub-only-IPmc
 remark Multicast video in 239.255.0.0/16 must remain in Hub
 deny   239.255.0.0 0.0.255.255
 remark Allow all other IPmc to pass
 permit any
!
ip prefix-list pl_Connected-to-BGP seq 5 permit 192.168.180.0/24 le 32
logging event link-status default
logging source-interface Loopback0
logging 1.1.1.254
!
route-map rmap_Connected-to-BGP permit 100
 match ip address prefix-list pl_Connected-to-BGP
 set metric 100
 set ip next-hop 99.99.0.7
!
!
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
banner motd ^C
######################################################################


 Project = Video Networking Solution
 Switch = HR3a

 Chassis = 7606
 Slot1 = WS-X6704 (3A)
 Slot2 = WS-X6748 (3A)
 Slot5 = Sup720  (3BXL)


######################################################################
^C
!
line con 0
 exec-timeout 0 0
 history size 100
 transport preferred none
line vty 0 4
 exec-timeout 0 0
 password cisco123
 login
 history size 100
 transport preferred none
!
scheduler runtime netinput 300
ntp clock-period 17179820
ntp source Loopback0
ntp update-calendar
ntp server 1.1.1.254
no cns aaa enable
end
```