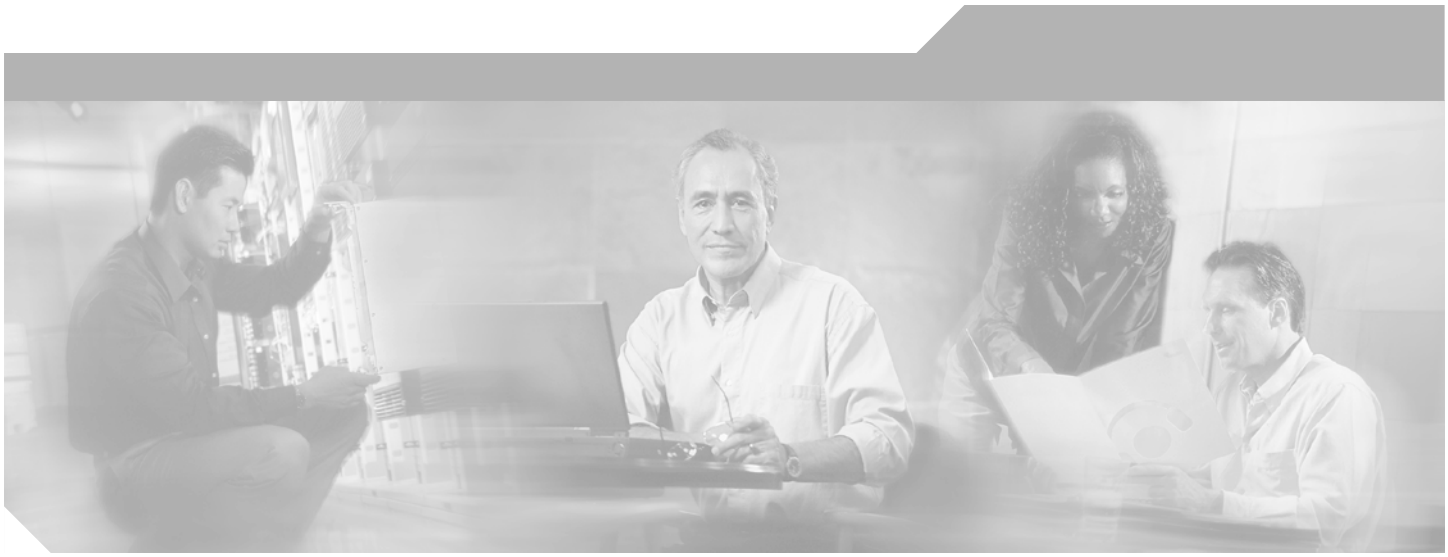


Cisco Wireline Video/IPTV Solution Design and Implementation Guide, Release 1.1

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-9153-01

Preface xi

Document Version and Solution Release xii

Document Objectives and Scope xii

Audience xii

Document Organization xii

Related Documentation xiii

Solution Documentation xiii

Switch and Router Documentation xiii

Cisco Catalyst 6500 Series Switches xiv

Cisco 7600 Series Routers xiv

Optical Component Documentation xiv

Cisco DWDM GBICs xiv

Document Conventions xiv

Obtaining Documentation xv

Cisco.com xv

Product Documentation DVD xvi

Ordering Documentation xvi

Documentation Feedback xvi

Cisco Product Security Overview xvii

Reporting Security Problems in Cisco Products xvii

Obtaining Technical Assistance xviii

Cisco Technical Support & Documentation Website xviii

Submitting a Service Request xviii

Definitions of Service Request Severity xix

Obtaining Additional Publications and Information xix

CHAPTER 1 **Solution Overview** 1-1

Solution Description and Scope 1-1

Generic Architecture and Scope 1-1

In Scope 1-2

Out of Scope 1-3

Solution Components 1-3

Cisco Equipment 1-3

Third-Party Equipment 1-3

Miscellaneous Solution Support 1-4
Operational Support Systems 1-4
Billing 1-4
EMC 1-4
Safety 1-4

CHAPTER 2 **Video Application Components and Architecture 2-1**

Video Application Components 2-1
Broadcast Video Components 2-2
Real-Time Encoder 2-2
Electronic Program Guide 2-3
Broadcast Client 2-3
VoD Components 2-3
Asset Distribution System 2-4
Navigation Server 2-4
Session Manager 2-4
Entitlement System 2-5
Video Pump 2-5
On-Demand Resource Manager 2-5
On-Demand Client 2-5
Common Broadcast Video and VoD Components 2-6
Conditional Access System and Encryption Engine 2-6
Broadcast Video Bandwidth Enforcement 2-7
Set-Top-Based Video Decryption and Video Decoder 2-7
Set-Top Box 2-7
Subscriber Database 2-8
Video Application Product Architecture 2-8
Middleware 2-9
VoD Server 2-9
Conditional Access System 2-9
Real-Time Encoder and Set-Top Box 2-10
Video Transport Architecture and Issues 2-10
Video Sites 2-10
Super Headend 2-10
Video Headend Office 2-10
Video Switching Office 2-11
Video Service Requirements 2-12
High Bandwidth 2-12
Asymmetric Bandwidth 2-12

Quality of Service 2-13
Service Availability 2-14
Broadcast Video Channel-Change Time 2-15
Potential Video Service Architectures 2-16
Network Requirements for Transport Services 2-17
Network Requirements for Managed Application Services 2-18
Service Mapping in a Triple-Play Architecture 2-19
Forwarding Architectures 2-20
Service-Availability and Bandwidth Requirements 2-20
Organizational Structure 2-21
IP Infrastructure Components 2-21
Service Mapping in the Release 1.1 Architecture 2-21
Triple-Play Architecture—Relation to Existing Standards 2-22
WT-101 Service Mapping 2-23
WT-101 QoS Architecture 2-28
WT-101 Layer 3 Edge Architecture 2-28
WT-101 Multicast Architecture 2-29
Solution Transport Recommendations Based on WT-101 2-33

CHAPTER 3 **Solution Transport Architecture** 3-1
Overview 3-1
Solution Components 3-3
Aggregation and Distribution Transport Architecture 3-4
Video Forwarding 3-4
Layer 3 Edge for Video Services 3-4
Video Forwarding Architecture 3-11
Multicast 3-15
Overview 3-15
Multicast Admission Control 3-16
Effect of Multicast on Channel-Change Performance 3-18
Multicast Configuration Options 3-23
IGMP Functionality in the STB 3-28
Internet Access Forwarding 3-28
Native Ethernet Aggregation 3-29
EoMPLS Aggregation 3-31
Voice Forwarding 3-33
Management 3-33
Management Transport 3-34
DHCP Configuration 3-34

STB Identification and Authorization 3-34
EMS/NMS 3-35
Redundancy 3-35
Video-Infrastructure Component Redundancy 3-35
Network Redundancy 3-36
Release 1.1 Configurations 3-36
Overview 3-37
Transport Components 3-37
Configuration 1: 10-GE Layer 3 Ring 3-38
Configuration 2: 1-GE plus 10-GE Hub and Spoke 3-39
Edge Transport Architecture 3-40
Overview 3-40
DSLAM Functions 3-41
RG Functions 3-41
EtherType Service Mapping in a Layer 2 RG 3-42
Physical Port-Based Traffic Mapping for the Multi-VC and VLAN Access Models 3-43
NAT/Layer 3 Functionality 3-44
QoS Architecture 3-46
Overview of DiffServ Architecture 3-47
DiffServ Architecture in the Solution 3-48
Administrative Boundaries 3-49
DiffServ-to-Layer-2 Mapping 3-50
Security and Additional Boundaries of Trust 3-50
Triple-Play QoS Analysis 3-51
Internet Access 3-51
Voice 3-51
Video 3-52
Voice plus Video Signaling 3-55
QoS in the Aggregation/Distribution Network 3-56
QoS in the Access Network 3-57
ATM Layer Scheduling 3-57
MAC/IP Layer Scheduling 3-59
VoD Admission Control 3-60
Overview 3-60
Integrated On-Path and Off-Path Admission Control 3-60

CHAPTER 4 **Implementing and Configuring the Solution** 4-1

Common Tasks 4-1

Configuring SSM Mapping with DNS Lookup 4-1

Configuring DNS Servers 4-2

Configuring SSM Mapping on All Switches 4-2

Configuring the Edge Switches for DNS Queries 4-3

(Optional) Enabling Option 82 on the ARs 4-4

Configuring the 10-GE Ring Topology 4-5

Introduction 4-5

Common Task: Configuring MPLS for HSD Service 4-9

Configuring DER1 4-11

Configuring QoS on DER1 4-11

Establishing and Configuring Interfaces on DER1 4-14

Configuring OSPF Routing for Video and Voice Traffic on DER1 4-22

Configuring DER2 4-23

Configuring QoS on DER2 4-23

Establishing and Configuring Interfaces on DER2 4-23

Configuring OSPF Routing for Video and Voice Traffic on DER2 4-23

Configuring AR1 4-24

Configuring QoS on AR1 4-24

Establishing and Configuring Interfaces on AR1 4-25

Configuring OSPF Routing for Video and Voice Traffic on AR1 4-30

Configuring AR2 4-30

Configuring QoS on AR2 4-30

Establishing and Configuring Interfaces on AR2 4-30

Configuring OSPF Routing for Video and Voice Traffic on AR2 4-30

Configuring AR3 4-31

Configuring QoS on AR3 4-31

Establishing and Configuring Interfaces on AR3 4-31

Configuring OSPF Routing for Video and Voice Traffic on AR3 4-31

Configuring the Hub-and-Spoke Topology 4-32

Introduction 4-32

Common Task: Configuring QinQ and Spanning Tree 4-35

Configuring DER1 4-36

Configuring QoS on DER1 4-36

Establishing and Configuring Interfaces on DER1 4-39

Configuring OSPF Routing for Video and Voice Traffic on DER1 4-49

Configuring QinQ and Spanning Tree on DER1 4-50

Configuring DER2 4-51

Configuring QoS on DER2 4-51
Establishing and Configuring Interfaces on DER2 4-51
Configuring OSPF Routing for Video and Voice Traffic on DER2 4-57
Configuring QinQ and Spanning Tree on DER2 4-57
Configuring AR1 4-58
Configuring QoS on AR1 4-58
Establishing and Configuring Interfaces on AR1 4-59
Configuring OSPF Routing for Video and Voice Traffic on AR1 4-65
Configuring QinQ and Spanning Tree on AR1 4-66
Configuring AR2 4-67
Configuring QoS on AR2 4-67
Establishing and Configuring Interfaces on AR2 4-68
Configuring OSPF Routing for Video and Voice Traffic on AR2 4-75
Configuring QinQ and Spanning Tree on AR2 4-76

CHAPTER 5 **Monitoring and Troubleshooting** 5-1
Network Time Protocol (NTP) 5-1
Syslog 5-2
Global Syslog Configuration 5-2
Interface Syslog Configuration 5-2
Useful Syslog Commands 5-2
no logging console 5-3
no logging monitor 5-3
logging buffered 16384 5-3
logging trap notifications 5-3
logging facility local7 5-3
logging host 5-3
logging source-interface loopback 0 5-3
service timestamps debug datetime localtime show-timezone msec 5-3
logging event 5-4
Quality of Service (QoS) 5-4
show class-map 5-4
show policy-map 5-4
show qos maps 5-5
show mls qos maps dscp-cos 5-5
show qos interface 5-6
show queueing interface 5-6
Multicast 5-11
show ip mroute 5-11

show ip mroute ssm 5-12
show ip mroute active 5-13
show ip pim neighbor 5-13
show ip igmp snooping 5-13
show ip igmp groups 5-14
show ip igmp ssm-mapping 5-14
show ip igmp membership 5-14
debug ip igmp 5-15
debug ip pim 5-15
debug domain 5-16
References 5-16

APPENDIX A **Sample DER and AR Switch Configurations for the 10-GE Ring Topology** A-1
Configuration for DER1 A-1
Configuration for DER2 A-10
Configuration for AR1 A-18
Configuration for AR2 A-35
Configuration for AR3 A-52

APPENDIX B **Sample DER and AR Switch Configurations for the Hub-and-Spoke Topology** B-1
Configuration for DER1 B-1
Configuration for DER2 B-11
Configuration for AR1 B-20
Configuration for AR2 B-36

APPENDIX C **Configuring Ericsson DSL Equipment** C-1
Network Diagram C-1
Hardware and Software Versions C-3
Configuring Ericsson Components C-4
Configuring the Switch C-4
Configuring the DSLAM C-4
Configuring the HAG C-6
atm.conf C-6
bridge.conf C-7
Creating Line Configurations C-8
Creating Services and Profiles C-9
Creating Services and Profiles for Video C-9
Creating Services and Profiles for Voice C-10

Creating Services and Profiles for Data C-11
Creating User Profiles and Adding Services C-12
Creating Profile 1 C-12
Creating Profile 2 C-14
Creating an IP Filter C-15
Special Issues C-15

APPENDIX D **Configuring UTStarcom DSL Equipment** D-1
Provisioning the Netman 4000 Application to Manage the DSLAM D-2
Configuring the DSLAM to Use the Netman 4000 Network Management Application D-2
Adding an AN-2000 B820 DSLAM Node to the Netman 4000 Network Management Application D-3
Configuring DSLAM Node Settings D-3
Configuring DSLAM Name and Contact Information (Optional) D-4
Configuring the DSLAM Node Address D-4
Configuring the ICM3 Ethernet Interface Line Card D-5
Viewing the Hardware and Software Version of the ICM3 Line Card D-5
Enabling IGMP Snooping for the DSLAM System D-6
Displaying Multicast Group Information D-6
Using Default Settings for Other ICM3 Card Parameters D-7
Activating the Internal Ethernet Interfaces of the ADSL Line Cards D-8
Activating the External GE Trunk Ports D-8
Disabling RSTP on the DSLAM D-9
Defining VLANs on the DSLAM to Support Triple-Play Services D-9
Configuring QoS on the ICM3 Controller Card D-10
Configuring the PCU Card on the DSLAM D-12
Configuring the ADSL Profiles D-13
Creating an ADSL2+ Profile D-13
Creating an ADSL2 Profile D-15
Configuring the IPADSL3A Line Cards D-17
Configuring the AN-2000 B820 DSLAM Card Modules D-18
Verifying the WAN Port D-19
Configuring and Activating the ADSL Ports D-20
Configuring ATM PVCs and Assigning Them to ADSL Ports D-20
Configuring the Number of MAC Addresses Supported per Port D-23
Configuring the Port Label Used for DHCP Option 82 D-23
Creating VLAN-to-PVC Mappings for Voice, Video, and Data D-24
Verifying the Access List Configuration on the DSLAM D-26
Configuring QoS for the IPADSL3A Line Cards D-26

Saving the Configuration D-27

Preface

This preface explains the objectives, intended audience, and organization of the Cisco Wireline Video/IPTV Solution, Release 1.1. The solution supports both broadcast video and video on demand (VoD) for the wireline market. This enables operators that use digital subscriber lines (DSL) and fiber to the neighborhood (FTTN) to offer not only video but also voice over IP (VoIP) and data (Internet access)—collectively referred to as "triple play"— over their existing infrastructure, now intelligently optimized for video service.

Note The first release of this solution was referred to as the "Cisco Gigabit-Ethernet Optimized IPTV/Video over Broadband Solution." The solutions are the same.

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, page xii
- Document Objectives and Scope, page xii
- Audience, page xii
- Document Organization, page xii
- Related Documentation, page xiii
- Document Conventions, page xiv
- Obtaining Documentation, page xv
- Documentation Feedback, page xvi
- Cisco Product Security Overview, page xvii
- Obtaining Technical Assistance, page xviii
- Obtaining Additional Publications and Information, page xix

Document Version and Solution Release

This is the first version of this document, which covers Release 1.1 of the Cisco Wireline Video/IPTV Solution.

Document History

Document Version	Date	Notes
1	06/06/2006	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 Cisco Wireline Video/IPTV Solution, Release 1.1. The primary focus of this release is on video over broadband functionality.

Note This document is primarily for Cisco products. To establish and maintain the third-party products and applications that may be a part of the Cisco Wireline Video/IPTV Solution, refer to the documentation provided by the vendors of those products.

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, with emphasis on Cisco Catalyst series switches).

Note This document addresses Cisco components only. It does not discuss how to implement third-party components typically required for a video service, such as VoD servers, encoders, headends, program guides, or DSLAMs.

Document Organization

The major sections of this document are as follows:

Section	Title	Major Topics
Chapter 1	Solution Overview	Introduces solution architecture and scope, components, and miscellaneous support topics.

Chapter 2	Video Application Components and Architecture	Discusses the segmentation of the video application architecture into logical components that are required for broadcast video and VoD services.
Chapter 3	Solution Transport Architecture	Discusses architectures for distribution, aggregation, edge transport, and quality of service. Introduces 10-GE ring and 1-GE and 10-GE hub-and-spoke configurations.
Chapter 4	Implementing and Configuring the Solution	Describes the configuration and implementation of the solution, and provides example implementations.
Chapter 5	Monitoring and Troubleshooting	Provides an introduction to monitoring and troubleshooting the Cisco switches used in the solution.
Appendix A	Sample DER and AR Switch Configurations for the 10-GE Ring Topology	Provides example configurations for distribution edge routers and aggregation routers for this topology.
Appendix B	Sample DER and AR Switch Configurations for the Hub-and-Spoke Topology	Provides example configurations for distribution edge routers and aggregation routers for this topology.
Appendix C	Configuring Ericsson DSL Equipment	Provides details related to the configuration of Ericsson DSL equipment.
Appendix D	Configuring UTStarcom DSL Equipment	Provides details related to the configuration of UTStarcom DSL equipment.

Related Documentation

Solution Documentation

This document, and *Release Notes for Cisco Wireline Video/IPTV Solution, Release 1.1*, are available under the following URLs:

http://www.cisco.com/en/US/netsol/ns340/ns394/ns158/ns88/networking_solutions_package.html

http://www.cisco.com/en/US/products/ps6902/tsd_products_support_series_home.html

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

Switch and Router Documentation

Documentation resources for the Cisco Catalyst switches and the Cisco 7609 router are available at the following URLs:

Note The Cisco 7600 series routers used in this solution functions as switches, and are considered to be a switches in this documentation.

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

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

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same 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=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, 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 send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments 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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—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.
- 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 to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*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.

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)—Your 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 operation 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 your network is impaired, but 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.

- 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, page 1-1
- Solution Components, page 1-3
- Miscellaneous Solution Support, page 1-4

Solution Description and Scope

The Cisco Wireline Video/IPTV Solution, Release 1.1, supports both broadcast video and video on demand (VoD) for the wireline market. This enables operators that use digital subscriber lines (DSL) and fiber to offer not only video but also voice over IP (VoIP) and data (Internet access)—collectively referred to as “triple play”— over their existing infrastructure, now intelligently optimized for video service. (The solution assumes that Internet access is already available.)

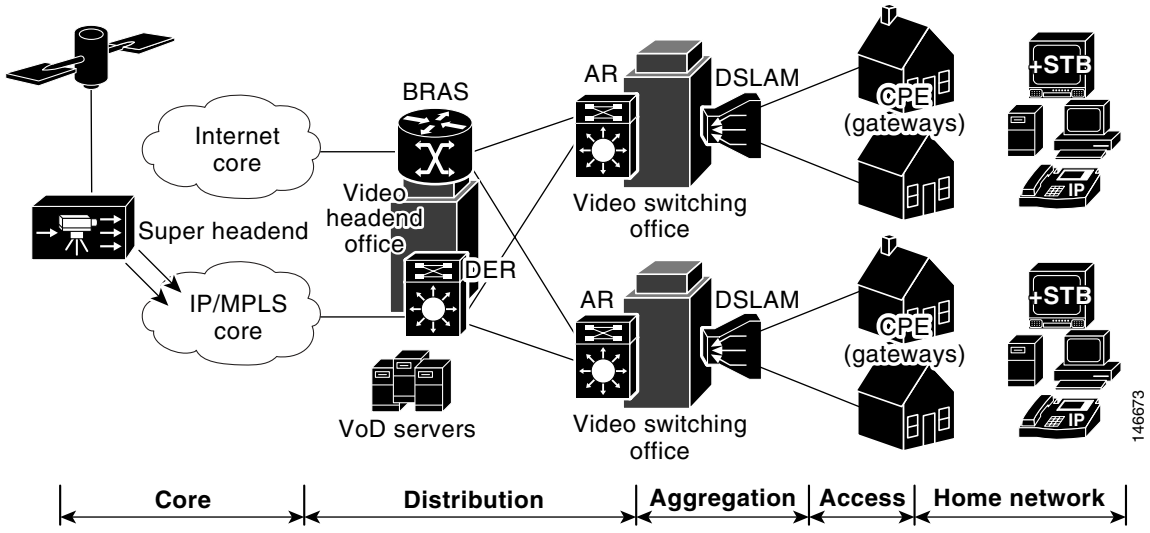
Generic Architecture and Scope

Figure 1-1 on page 1-2 presents a generic view of the Cisco GOVoBB Solution transport architecture. The shaded area shows the scope of solution testing and documentation. The solution uses a Gigabit-Ethernet (GE) transport network consisting of the following:

- A super headend (SHE), where live feeds for the broadcast video service are located
- A video headend office (VHO), where the video server complex resides
- A video switching office (VSO), where aggregation routers (ARs) that aggregate local or remotely attached GE DSLAMs are located

The regional access network, or RAN, consists of distribution, aggregation, and access layers. There is one SHE per region or network, and one VHE per metropolitan area. A distribution edge router (DER) provides transport for video traffic between the IP/MPLS core network and the VHO. The real-time encoder encodes and compresses analog signals. The VHO, in turn, is connected to the VSOs through one or more ARs. The customer premises equipment consists of residential gateways, or RGs. (RGs are also referred to as home access gateways, or HAGs.)

Figure 1-1 Cisco Wireline Video/IPTV Solution Transport Architecture: Generic View



Note For a detailed discussion of the transport architecture, see Chapter 2, "Video Application Components and Architecture."

In Scope

The scope of the solution comprises fully tested and supported Cisco components, as well as third-party components tested by Cisco. The following aspects of the solution are fully tested and supported:

- Ethernet switching and routing at VHO and VSO interfaces

Note Management is provided through the Cisco IOS command line interface (CLI) only. See also Operational Support Systems, page 1-4.]

- Multiservice fully converged backbone based on a ring or hub-and-spoke transport architecture

Table 1-1 summarizes the correspondence between site types and their transport network types.

Table 1-1 Site Types and Their Transport Network Types

Site Type	Super Headend	Video Headend Office	Video Switching Office	Residence
Transport Network Type	Core	Distribution	Aggregation	Home network

Out of Scope

Not included in the scope of the solution, but still required to support triple play, are items such as subscriber device authentication for one or more of the other nonvideo services. In addition, the architecture of this release places minimal requirements on the DSLAM. This allows the solution to work with as many third-party DSLAMs as possible.

Solution Components

Cisco Equipment

Release 1.1 consists of core Cisco components that are tested, documented, and fully supported by Cisco. Also, third-party equipment, although not fully supported by Cisco, has been selected and tested in conjunction with the core components, to increase the number of test cases and improve the overall quality of the solution in practical networks. The following Cisco equipment has been tested in the context of the solution:

- Cisco 7606 and 7609
- Cisco Catalyst 6509

Note For the details of solution components, see Solution Components, page 3-3.

Third-Party Equipment

For this release of the solution, Table 1-2 on page 1-3 lists the third-party vendors and the basic functionality they provide. (For detailed descriptions of video functions, see Video Application Components, page 2-1.)

Table 1-2 Component Partners and Basic Functionality

Vendor	Basic Functionality	Product Name/Model
Kasenna www.kasenna.com	VoD server	GigaBase
	Middleware	VForge foundation + Living Room application
Amino www.aminocom.com	Set-top box	STB 110
Ericsson www.ericsson.com	DSLAM, residential gateway	ECN320 Ethernet Controller Node, EDN312xp DSLAM, HM340d Home Access Gateway[1]
UTStarcom www.utstar.com		AN-2000 B820B IP DSLAM

1. Throughout this document, residential gateway (RG) is used to refer to the home access gateway (HAG).

Miscellaneous Solution Support

This section clarifies the degree to which other aspects of the solution and its implementation are supported in this first release.

Operational Support Systems

Release 1.1 does not certify element management systems (EMSs) or network management systems (NMSs) operated within the context of the Cisco Wireline Video/IPTV Solution architecture. Customers continue to provide such capabilities as applicable to their particular environments. All the management information base (MIB) components for the Cisco equipment are available from Cisco, and can be incorporated into the customer's current EMS.

Billing

Billing is outside the scope of this first release of the solution.

EMC

Release 1.1, with all its platforms, accessories, and components, complies with applicable electromagnetic compliance (EMC) standards.

Safety

Release 1.1, with all its platforms, accessories, and components, complies with applicable safety standards.

Video Application Components and Architecture

This chapter discusses the segmentation of the video application architecture into logical components that are required for broadcast video and video on demand (VoD) services. The function of each component is described, as well as the basic interfaces needed between each component and other components of the system.

This chapter describes possible video architectures and components only. For the actual tested implementation, see Chapter 4, "Implementing and Configuring the Solution."

Note Because there are currently few standards regarding application architectures for either broadcast or on-demand IPTV/video service over a DSL infrastructure, this solution makes no specific assumptions regarding the application architectures implemented by the vendors of specific video equipment. However, although there are few standards for video application architectures, the functionality implemented is fairly consistent from vendor to vendor.

For a list of the video components that were tested in this release, including product names and part numbers, see Table 3-1 on page 3-3.

This chapter presents the following major topics:

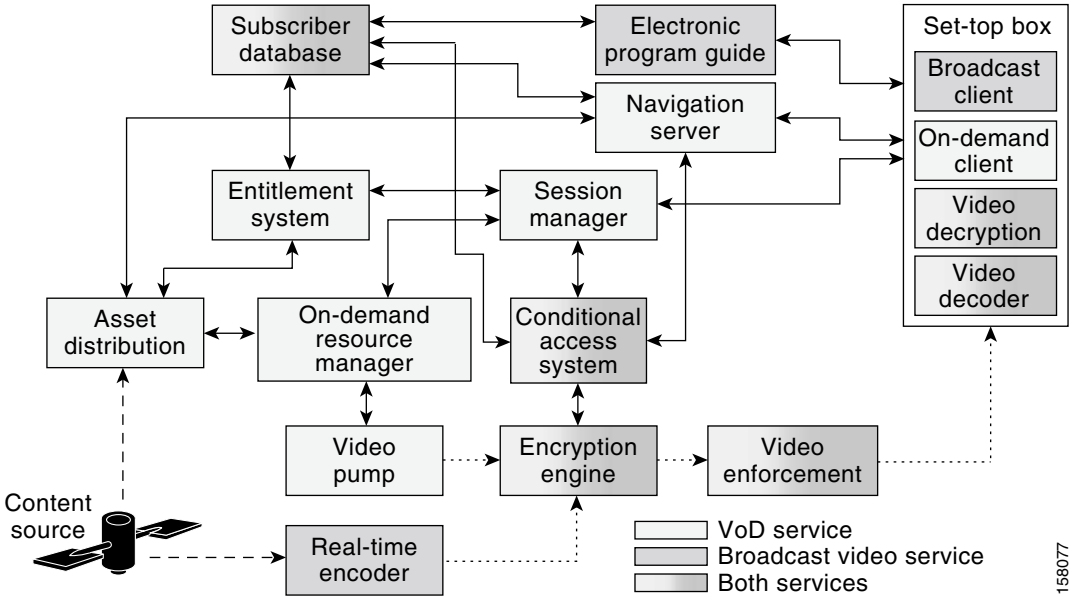
- Video Application Components, page 2-1
- Video Transport Architecture and Issues, page 2-10

Video Application Components

Figure 2-1 on page 2-2 illustrates the logical relationship of the application-layer video components needed to deliver broadcast video and VoD services, as well as the basic interfaces between components. Components can be categorized as follows:

- Broadcast Video Components
- VoD Components
- Common Broadcast Video and VoD Components

Figure 2-1 Video Application Component Architecture



Broadcast Video Components

Broadcast video components (see Figure 2-1) include the following:

- Real-Time Encoder
- Electronic Program Guide
- Broadcast Client

These are described below.

Real-Time Encoder

The real-time encoder takes a live feed from a broadcaster in either analog or digital format and converts it into a compressed digital stream that is encapsulated in IP packets. The input to the encoder may be in a digital format that uses MPEG-2 over synchronous media such as ASI, or it may be in an NTSC, PAL, SECAM, or other analog format. The output of the encoder is a digitally compressed stream that is encapsulated in IP headers and sent to a multicast address. The compression method used by the encoder may be either MPEG-2 or MPEG-4, while the IP-based transport encapsulation used is MPEG-2 transport over either UDP/IP or IP/UDP/RTP. because the real-timer encoder is configured to encode a specific channel, no control interfaces are required between it and other video components.

Electronic Program Guide

The electronic program guide (EPG) provides information about available broadcast channels to the broadcast client application running on the IP set-top box (STB). The EPG is often implemented as an HTTP server and formats available channel listings as web pages. The EPG application authenticates and authorizes a subscriber for broadcast services. The EPG may also provide a customized view of channel listings that is based on the packages a particular subscriber has subscribed to. Both of these functions require an interface between the EPG application and the subscriber database. In addition to providing a graphical listing of available channels, the EPG provides the IP multicast address to which the channel is sent in the IP network. The broadcast client uses this address in Internet Group Management Protocol (IGMP) messages that are sent during the processing of a channel change.

Broadcast Client

The broadcast client is an application process running on the STB that is responsible for providing the user and control interface for broadcast video services. The broadcast client, in conjunction with the EPG, implements a subscriber authentication interface for set-top-based services. Authentication is typically done by means of an application layer authentication protocol such as HTTP in conjunction with a shared secret such as a username/PIN pair.

The broadcast client displays available broadcast-channel information using data from the EPG and implements the control interface for channel change by means of IGMP. Since the DSL line may be capable of supporting the bandwidth of only a single broadcast channel, the IGMP process for changing channels must ensure that only a single video broadcast stream is sent to the STB at a time. The broadcast client implements this by sending an IGMP leave for the current channel and then waiting for a configurable period of time for the broadcast stream to stop. After this timer expires, the broadcast client sends an IGMP join for the new channel. The full channel-change time, documented in Broadcast Video Channel-Change Time, page 2-15, includes these IGMP factors as well as other factors specific to video compression. (See also Effect of Multicast on Channel-Change Performance, page 3-18.)

Note Current broadcast client applications support IGMPv2 instead of IGMPv3. Consequently, they do not directly support the use of Source Specific Multicast (SSM) in the IP transport network.

VoD Components

VoD components (see Figure 2-1 on page 2-2) include the following:

- Asset Distribution System
- Navigation Server
- Session Manager
- Entitlement System
- Video Pump
- On-Demand Resource Manager
- On-Demand Client

These are described below.

Asset Distribution System

The asset distribution system (ADS) takes video content from content providers and uses business rules to distribute that content to different locations in the video service provider's network. Video content may be provided to the ADS through a number of different methods. These methods include the use of pitcher/catcher systems, which receive video content from content providers over satellite links, and manual processes such as file copies from other network servers.

Standard video content objects include the actual MPEG video, images for display during content navigation, trailers, and metadata files that provide information about the files contained in the object. Metadata files often follow a standards-based format specified in the CableLabs Asset Distribution Specification.

The ADS may be used to modify the metadata of a video asset to add business rules such as the price of the video, the distribution window, the VoD subscription package that the video is part of, whether the content needed to be encrypted, and so on. On the basis of these business rules, the ADS replicates the video asset to the on-demand resource management component of video servers in different locations.

Navigation Server

The navigation server provides information about available VoD content to the on-demand client application running on the STB. The navigation server is often implemented as an HTTP server and formats available VoD content as web pages. The navigation server uses information provided by the asset management system to determine which VoD content to display to the subscriber. For subscription-based VoD services, the navigation server may use the information in the subscriber database to customize the view of the video content presented to the subscriber, depending on the packages the subscriber has purchased.

Session Manager

The session manager is the central point of communication for VoD session requests that originate from the on-demand client on the STB. It manages the life cycle of a video session and is responsible for arbitrating the various resources required to deliver the video stream associated with the on-demand session request. Many vendors of VoD equipment and software provide a logical "session manager" function, though this function goes by a variety of different names.

When the session manager receives an on-demand session request from an on-demand client application, it first uses the services of the entitlement system to determine whether the subscriber is authorized to view the requested video content. If the request is authorized, the entitlement server includes additional information in the authorization response, such as the encryption format to be used for the content.

When the session manager receives the authorization response, it determines the best VoD server complex to use for the session request, based on the subscriber's IP subnet. The session manager then contacts the on-demand resource manager for that VoD server complex to request a video pump for the session. If the VoD content needs to be encrypted in real time, the session manager contacts the conditional access system (CAS) to request a real-time encryption engine for the session. The CAS responds with the decryption keys to be used by the STB to decrypt the video stream.

After all of the resources for a VoD session request are obtained, the session manager responds to the on-demand client with information about the IP/UDP/RTP transport parameters for the video stream to the STB. If the stream is to be encrypted, the session manager (or a key manager with which it coordinates) includes the decryption keys for encrypted video content in the response as well. Finally, the session manager includes the IP address of the video pump that was selected for the session. The IP address of the VoD pump is needed by the on-demand client in order to send stream control requests through Real Time Streaming Protocol (RTSP)—such as pause, fast forward, rewind—for the session.

Entitlement System

The entitlement system is responsible for determining whether the movie requested by an on-demand client is authorized for viewing by the subscriber associated with that client. The entitlement system uses information from the ADS to build a database indicating which videos are associated with different on-demand subscription packages. When the entitlement system receives an entitlement request from the session manager, it uses this database to determine with which orderable on-demand package the requested video is associated. The entitlement system then uses the services of the subscriber database to determine whether the subscriber associated with the entitlement request is entitled to view the requested video.

Video Pump

The video pump is the streaming storage component of a VoD system. The video pump contains locally or remotely connected storage that is organized in such as way that it can send any piece of stored media at a known constant rate. The streaming portion of the video pump is responsible for pulling requested files from the storage system and for pacing the output of each requested file to the network though the use of a shaper. Video pumps must be capable of implementing basic stream control functionality, such as fast-forward and rewind, to respond to requests from the on-demand client during the playout of a media file.

In addition to being able to stream media out, video pumps are also responsible for ingesting media for storage in the storage subsystem. While in general the functionality of a video pump is fairly independent of media format, the ingest function may have functionality that is specific to a particular media format. An example of this type of media-format dependence is the generation of trick files for use with stream control functionality such as fast-forward and rewind. Video pumps used in broadband environments are typically capable of storing and streaming both MPEG-2 and MPEG-4 content.

On-Demand Resource Manager

The on-demand resource manager (ODRM) is responsible for managing the streaming resources and storage of a group of video pumps. The ODRM is responsible for locating and replicating content, as well as for allocating video pumps for the on-demand session requests it receives from the session manager.

On the ingest side, the ODRM is responsible for taking content received from an asset management system and replicating it to one or more of the video pumps it controls. The ODRM makes decisions on when and where to replicate content on the basis of such information as asset metadata and the demand for each title (as indicated by on-demand session requests).

On the streaming side, the ODRM responds to on-demand session requests from a session manager by locating a video pump that contains the requested title, has the capacity to stream the title, and is capable of reaching over the transport network the subscriber that generated the session request.

On-Demand Client

The on-demand client (ODC), an application process running on the STB, is responsible for providing the user and control interface for on-demand services. The ODC provides the user interface for browsing on-demand content using the services of the navigation server. The browsing interface of the ODC is typically implemented by means of an embedded HTTP-based browsing application.

The ODC interfaces to the session manager to make requests to stream on-demand content. It also interfaces to video pumps to make stream-control requests for movies that are actively being streamed.

Common Broadcast Video and VoD Components

Common broadcast video and VoD components (see Figure 2-1 on page 2-2) include the following:

- Conditional Access System and Encryption Engine
- Broadcast Video Bandwidth Enforcement
- Set-Top-Based Video Decryption and Video Decoder
- Set-Top Box
- Subscriber Database

These are described below.

Conditional Access System and Encryption Engine

The conditional access system (CAS) is responsible for the key management and distribution infrastructure associated with the encryption of video content. Video encryption is used as the second tier of protection against theft of content. The first tier of protection for both broadcast and on-demand services is performed as part of the on-demand and broadcast client applications running on the STB. These applications use the services of the EPG and navigation server to authenticate the subscriber and provide a customized view of available channels and content based on the services the subscriber has purchased. For on-demand services, the entitlement system also checks whether the subscriber is authorized to view requested titles, with the result that the ODC does not allow the subscriber to view unauthorized content. While application-layer authorization protects against the theft of content from authorized STBs, it does not protect the video stream itself. Video encryption using CAS provides this second layer of protection against theft and unauthorized viewing of video content.

Because conditional access adds an additional level of complexity and cost to a video delivery system, service providers typically use CAS-based encryption only on premium-tier broadcast channels and on-demand titles. For broadcast services, encryption must be done in real time as the video stream is delivered. For on-demand services, encryption may be done either in real time as the content is streamed or as part of the process of replicating content to video pumps. The process of encrypting video content as part of replication is called pre-encryption.

Video encryption may be done on either a tier or session basis. In tier-based video encryption, a single set of encryption/decryption keys is used for all of the video content associated with a particular service offering. Subscribers that are authorized to view the content associated with the service are delivered the decryption keys needed for that service ahead of time. Conditional access for broadcast video services is always implemented by means of tier-based encryption, because a single video stream may be viewed by many subscribers simultaneously. Decryption keys for broadcast video services are delivered in a secure manner to the STB through the EPG. In session-based video encryption, decryption keys for a piece of content are generated and delivered to the subscriber on a per-session basis. Session-based encryption may be used with VoD content. Because decryption keys are generated only on a per-session basis for session-based encryption, they may be used with either real-time or pre-encryption techniques.

In a typical CAS, the encryption of digital services can be achieved by using entitlement control messages (ECMs) and entitlement management messages (EMMs). In order to generate the final keys needed to decrypt a particular video stream, the STB must receive and decrypt the correct ECMs and EMMs. EMMs provide keys that can be decrypted only by a specific subscriber, while ECMs provide keys that are specific to a particular video stream. Because EMMs are specific to a subscriber, they are always generated ahead of time. Because ECMs are specific to a particular video stream, they may be generated ahead of time when pre-encryption is used, or they may be generated in real time when real-time encryption is used. ECMs are typically delivered in band as a component of the video stream.

Whether the content must be encrypted may be determined by a number of factors. For on-demand services, content providers can require content to be encrypted by enabling the "Encryption" field in the metadata file associated with the video asset. For broadcast services, the video service provider statically configures the video stream from real-timer encoders to be sent either directly to a multicast group or to a real-time encryption engine, depending on whether that channel is to be encrypted.

The encryption engine takes MPEG streams in and encrypts them in real time using encryption keys received from the CAS. Encryption engines typically use a DES algorithm for encryption.

Broadcast Video Bandwidth Enforcement

Broadcast video bandwidth enforcement is implemented as part of the functionality of the provider-edge aggregation router (AR) (sometimes referred to as the PE-Agg router). The AR enforces a maximum broadcast bandwidth limit by limiting the number of IGMP joins on the ranges of multicast addresses associated with broadcast video to a configured maximum on the aggregation links it controls. The mapping of video channels to multicast addresses can be done in such a way that the AR can associate the bandwidth for different classes of video (for example, standard definition or high definition) with different ranges of multicast addresses. IGMP join limits can then be set for each range of multicast addresses.

For more details on the network enforcement for video broadcast, refer to Multicast Admission Control, page 3-16.

Set-Top-Based Video Decryption and Video Decoder

The set-top box, or STB (see below), includes two components that are responsible for turning the incoming video stream, delivered as IP packets, into an uncompressed digital stream that can be directly turned into an analog TV signal ready for display by a television set. These components are the video decoder and the video decryptor.

The video decoder is responsible for decompressing the incoming video stream. It uses a decompression algorithm that is matched to the compression algorithm used by the real-time encoders for broadcast services. The video decoder may also support additional decompression algorithms for VoD services if VoD assets are compressed by a different algorithm than broadcast channels use.

The video decryptor is responsible for performing decryption on the video stream if the stream was encrypted by the encryption engine when real-time encryption is used, or by an offline encryptor when pre-encryption is used for on-demand assets.

Set-Top Box

The set-top box (STB) is the hardware and common software infrastructure component that is used by the on-demand and broadcast clients as well as by the video decryptor and the video decoder. The STB hardware typically consists of a general-purpose processor and video subsystem that produces an analog television output. The hardware may also include a hardware-based decoder and decryption subsystem. The STB software typically includes an embedded operating system, and may also include application infrastructure components such as a web browser.

The subscriber database contains service level information about each subscriber—for example, the services the subscriber is authorized to use, billing information, and so on. The subscriber database may also contain information that can be used for subscriber authentication. An example of this type of information is the username and password used by the EPG to identify and authenticate a subscriber for broadcast services.

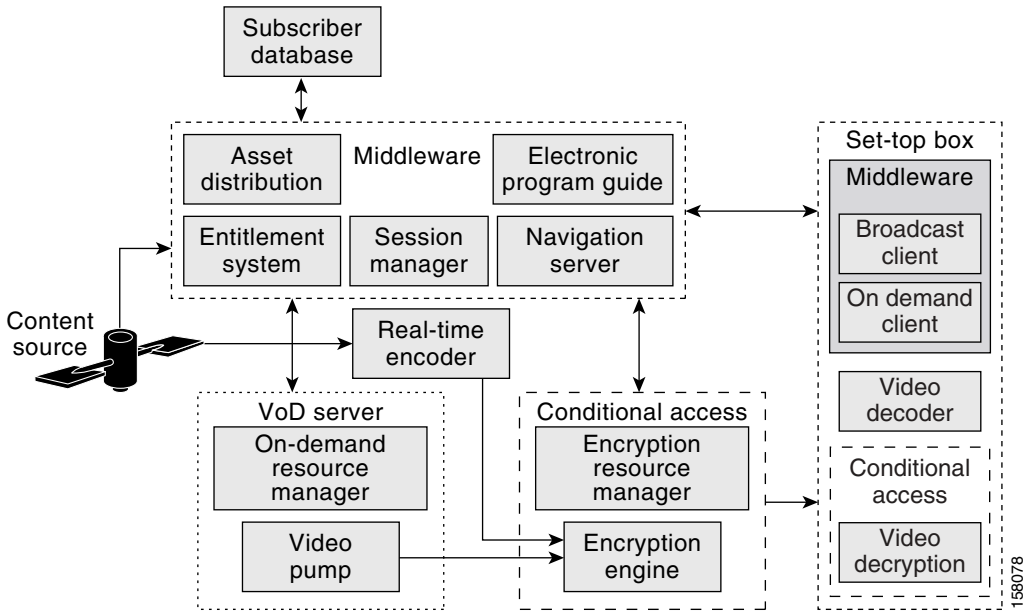
Subscriber Database

The subscriber database contains service-level information about each subscriber, for example, which services the subscriber is authorized to use, information used for billing, and so on. The subscriber database may also contain information that can be used for subscriber authentication. An example of this type of information is the username/password information that is used by the EPG to identify and authenticate a subscriber for broadcast services.

Video Application Product Architecture

This section describes how the logical components described previously are commonly combined into products that are supplied by current video-component vendors. Figure 2-2 illustrates how the video components presented in Figure 2-1 on page 2-2 are "bundled" into application products. This bundling reduces the number of products and vendors that must be integrated to build a complete video system. It also reduces the number of interfaces that must be agreed upon by vendors.

Figure 2-2 Common Video Application Product Architecture



Note The logical components described in this section represent functional blocks that are common to most video application architectures, and do not necessarily reflect how these functions are bundled into products by video equipment vendors.

The following classes of video products are needed to build a complete broadband video solution:

- Middleware
- VoD Server
- Conditional Access System
- Real-Time Encoder and Set-Top Box

These are described below.

Middleware

Middleware, as defined, has the role of gluing a number of logical components together into a more comprehensive IPTV/video software system. (Note that there are several different middleware implementations. Thus, the following description is a typical example for illustrative purposes.) Middleware implements the user interface for both broadcast and on-demand services. It is also used as the glue software that integrates products from other vendors into an application level solution. Middleware products are often used to integrate multiple VoD servers, conditional access systems, and set-top boxes from different vendors into the same deployment.

Middleware provides the client and server functionality that implements the user interface for both broadcast and on-demand services. The components that provide the client-side functionality are the broadcast and on-demand client applications on the STB, while the components that provide the server-side functionality are the electronic program guide and the navigation server.

Middleware uses the entitlement system and session manager components to integrate the VoD servers used in an on-demand service. The entitlement system integrates the asset ingest function of a VoD server, while the session manager integrates the session plane of the VoD server into an on-demand service.

Middleware uses the session manager and on-demand client to integrate CAS into an on-demand service. These components may be used to pass decryption keys from the conditional access system to the video decryption component in the STB. These components also determine when to use the services of the CAS based on the encryption requirements of the service and each asset associated with the service. Middleware uses the EPG and the broadcast client to integrate CAS into a broadcast service. The broadcast client determines when to use the services of the CAS based on information it obtains from the EPG on each broadcast channel.

VoD Server

The VoD server (one or several) implements storage and real-time streaming functionality for on-demand services. The VoD server consists of a set of video pumps that are managed by an on-demand resource manager. The VoD server integrates with middleware and may also be integrated with the CAS when preencryption is used.

Conditional Access System

The conditional access system (CAS) provides encryption and decryption services, as well as key generation and distribution functionality, for both broadcast and on-demand services. The CAS consists of the encryption resource manager, the encryption engine, and the video decryption process in the STB.

The CAS interfaces to middleware when session-based encryption is used for on-demand services. The CAS may also interface to middleware for encryption key distribution between the encryption resource manager and the decryption process on the STB. Finally, the CAS interfaces to VoD servers where preencryption is used for on-demand content.

Real-Time Encoder and Set-Top Box

The real-time encoder and STB components described in Real-Time Encoder, page 2-2, and Set-Top Box, page 2-7, respectively, are identical to product classes of the same name shown in Figure 2-2 on page 2-8.

Video Transport Architecture and Issues

To meet the end-to-end transport requirements for broadcast VoD services, the wireline video/IPTV transport architecture provides functional requirements and configuration recommendations for each switching node in the path from the VoD servers to the STBs. This section presents the following topics:

- Video Sites
- Video Service Requirements
- Potential Video Service Architectures
- Service Mapping in a Triple-Play Architecture

Note Although this solution is focused on video service, it must work within the context of a triple-play solution. Because wireline video/IPTV services are fairly new, vendors and service providers do not user the same terminology to describe the major sites. This section describes terminology commonly used for triple-play solutions.

Video Sites

The video sites described in this section are the super headend (SHE), the video headend office (VHO), and the video switching office (VSO). Figure 1-1 on page 1-2 shows the location and roles of the sites and components in a typical IPTV/VoBB deployment.

Super Headend

The SHE is where live feeds for the broadcast video service are located. This site contains the real-time encoders used for the broadcast video service, along with the asset distribution systems for on-demand services. This site may also contain back-office systems such as the subscriber database. Most wireline video/IPTV deployments have a single SHE site; this is the source of most of the multicast streams for the broadcast video service. The SHE typically resides in the core of the transport network.

Video Headend Office

The manned VHO is where the video server complex resides (as well as where optional local/PEG content may be inserted). The VHO is where the majority of the video pumps used for on-demand services are typically located. It is also where the real-time encoders for local television stations reside. A VHO typically serves a metropolitan area of between 100,000 and 1,000,000 homes. The VHO is equivalent to (and may be contained in) the same facility as the point of presence (POP) for Internet access services. Transport for video traffic between the VHO and IP/MPLS core network is provided by a distribution edge router (DER). The DER interconnects the core network and the local video sources to a high-bandwidth distribution network that carries both broadcast and on-demand video to VSOs.

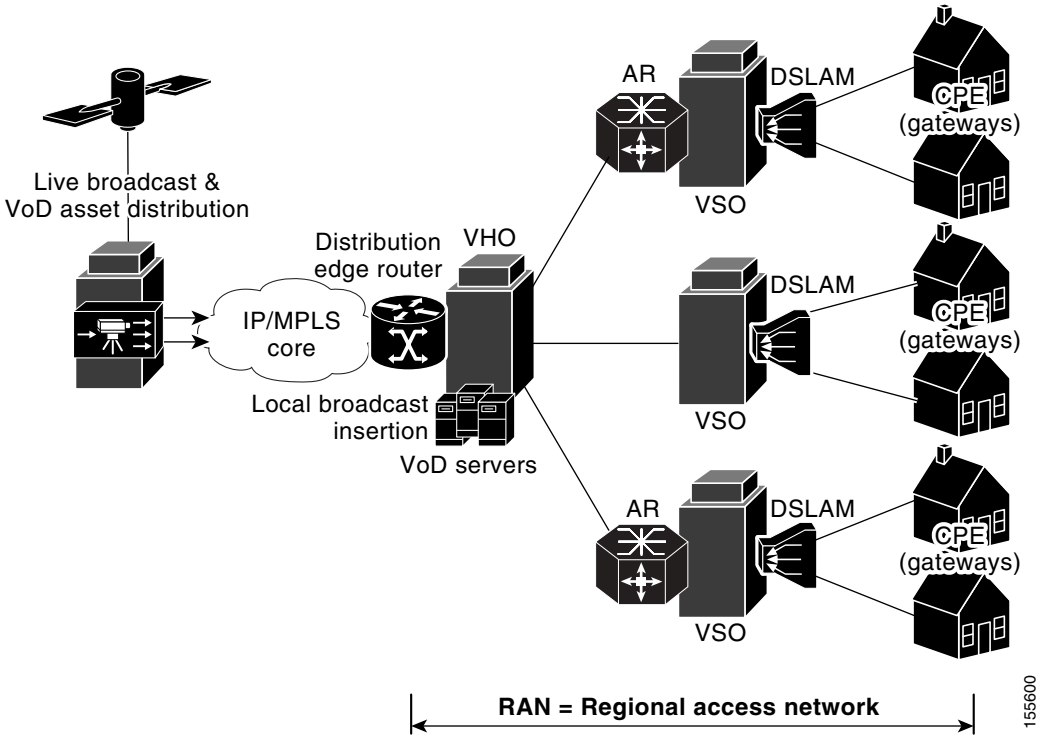
Video Switching Office

The VSOs house the aggregation routers that aggregate local or remotely attached GE DSLAMs. The VSO is typically located in the central switching office. The central switching office is the physical termination point for the majority of the copper loops for the residences it serves. Because ADSL and ADSL2+ rely on short loop lengths to obtain maximum training rates and throughput, the copper loops used for DSL service are often terminated at a location closer to the subscriber than the VSO. This means that the DSLAMs that the VSO aggregates may or may not be colocated in the VSO. The switching equipment in the VSO interconnects the aggregation and distribution networks. Traffic to and from the DSLAMs is aggregated by the aggregation router (AR).[1] The AR resides in intermediate and terminal VSOs.

In order to minimize the bandwidth requirements between the VSO and the VHO, a VSO may include local video pumps that are used to cache popular on-demand content. While the Release 1.1 transport architecture does not preclude the use of video pumps in the VSO, this configuration is not tested as part of the solution test effort.

Figure 2-3 presents an overview of the solution transport architecture

Figure 2-3 Solution Transport Architecture: Overview



1. The AR is sometimes referred to as the provider-edge aggregation router, or PE-Agg.

Video Service Requirements

In order to understand better some of the design tradeoffs associated with the transport architecture, it is important to understand common requirements for a video service and how an IP network can be optimized to meet these requirements. This section outlines some common requirements for broadcast video and VoD services. It also describes what design factors in the transport network are relevant to these requirements.

High Bandwidth

The amount of bandwidth that a network must be capable of transporting to support video services is typically an order of magnitude more than what is required to support voice and Internet access services. A standard-definition IP video stream that is carried as an MPEG-2 SPTS stream over RTP uses about 3.75 Mbps of bandwidth. A high-definition IP video stream using the same type of compression and transport uses about 15 Mbps of bandwidth.

These bandwidth requirements mean that a DSL access infrastructure that is designed for real-time video transport must be capable of carrying significantly more bandwidth than what is needed for VoIP and Internet access services. It also means that the DSL line itself is typically constrained to carrying only one or two video streams simultaneously. The result is that video over DSL service offerings must limit the service to one or two simultaneous broadcast channels or on-demand sessions to a household.

Because the video streams associated with on-demand services are unicast while the video streams associated with broadcast services are multicast, the amount of bandwidth required in the aggregation and distribution networks to carry on-demand streams is much greater than what is required for broadcast services. Also, because broadcast video services use multicast, the amount of bandwidth required in the access and distribution networks scales with the number of channels offered. As an example, a broadcast video service that uses MPEG-2 compression and offers 300 channels of standard-definition content requires approximately 1 Gbps/sec of capacity in the distribution network to handle worst-case usage patterns. Because on-demand services use unicast transport, the amount of bandwidth required in the distribution network scales with the number of subscribers and peak on-demand utilization rates the network is designed to carry. For example, a distribution network that is designed to deliver MPEG-2 compressed standard-definition content to 50,000 on-demand subscribers at a 10% peak take rate requires about 19 Gbps of capacity.

Asymmetric Bandwidth

Video traffic is inherently asymmetric, as both broadcast video and VoD flows are unidirectional. The only traffic that is sent in the upstream direction of either service is control traffic that is used to instantiate the video flow. For on-demand services, this control traffic is the session and resource signaling that is described as part of the component descriptions in Video Application Components, page 2-1. For broadcast services, the control traffic is IGMP and PIM signaling that is used to instantiate the multicast flow for the broadcast channel.

Because of this asymmetry, the cost of the distribution network can be reduced by incorporating unidirectional links in the transport path. One of the transport alternatives tested in the previous release of the solution included unidirectional transport in the distribution network.

Note Unidirectional transport, tested in Release 1.0, was not explicitly tested for the current release. For configurations that use asymmetric bandwidth, see the *Cisco Gigabit-Ethernet Optimized IPTV/Video over Broadband Solution Design and Implementation Guide, Release 1.0*.

Quality of Service

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 digital video transport alternatives, such as MPEG-2 directly over a QAM modulation carrier used in both cable and satellite networks today. To ensure that any 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.

While this end-user requirement is similar to what is currently accepted for voice over IP (VoIP) 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 how video and voice are processed by video STBs and VoIP phones and gateways. VoIP phones and gateways typically support algorithms 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. Because of the compression algorithms used, and the amount of information carried in a single video over IP packet, current-generation STBs do not support concealment algorithms such as those used for VoIP services. 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 10^{-6} and 10^{-2}, respectively. The lower allowed drop rate for video means that both drops caused 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 to ensure that video flows meet the required 10^{-6} drop rate when links are congested. (QoS Architecture, page 3-46, provides details on the QoS architecture for the solution.)

Packet drops due to bit errors on physical links need to be addressed on a link-by-link basis. Note that the link-layer technologies used in video networks use cyclic redundancy check (CRC) algorithms to ensure that packets with errors are not delivered. This means that a single bit error in a video packet results in that packet being dropped when the CRC is performed. Video over IP is typically carried in packets that are approximately 1400 bytes. If bit errors are assumed to be distributed randomly, the resulting requirement for transport links is to ensure a bit error rate (BER) of less than 10^{-10}.

The BER on optical links can be engineered to 10^{-14} or less by ensuring a high signal-to-noise ratio (SNR) on those links. Because Release 1.1 of the solution uses optical connectivity in the access and distribution networks, the degradation in video quality resulting from bit errors on these links should not be an issue.

However, packet drops due to bit errors on the DSL line can have a significant effect on video quality. The SNR on a DSL line varies as a result of many factors, including loop length, proximity to noise sources, and so on. In addition, the SNR may vary over time because of factors such as corrosion at connection points, moisture, and so on. Consequently, it may be very difficult to qualify a DSL line to ensure a BER of less than 10^{-10} at the time of installation.

Multiple technologies are available to deal with bit errors on the DSL line. Some common technologies are DSL-based forward error correction (FEC) interleaving, and real-time retransmission (RTR). While the Release 1.1 of the solution does not include the testing of these technologies, future versions of the solution will include technologies to deal with bit errors on the DSL line.

DSL-based forward error correction (FEC) and interleaving is a standards-based method of improving the bit error characteristics on the DSL line by including additional error correction information in the DSL bit stream. The error correction information and data are interleaved to make the DSL bit stream more resilient to instantaneous line hits. While this technology improves the resilience of the DSL line

with respect to bit errors, it significantly increases the transmission delay for packets sent over the line. This increased transmission delay does not affect video services. However, it may have a significant impact on highly interactive services such as network-based gaming applications. Because of the above factors, DSL-based FEC and interleaving may not be the best technology for improving loss characteristics resulting from bit errors on the DSL line.

RTR is an IP transport-layer function that enables the transport stack on an STB to provide feedback to a video transmitter when a video packet is dropped by the network. If the transmitter can resend the dropped packet to the STB before that packet's playout time, then the STB can insert the resent packet into the jitter buffer and continue processing as if the packet were never lost. Because the jitter buffer of most IP STBs is around 200 msec, RTR methods work if the whole retransmission process takes less than 200 msec. An example transport standard that implements RTR is the RTP retransmission standard specified in the AVT Working Group of IETF. RTP retransmission supports the real-time retransmission of both unicast and multicast streams, so it is applicable to both VoD and broadcast video services.

RTR has a couple of advantages over DSL FEC and interleaving for video and other services. Because RTR is a transport layer function, it can be enabled for only the video service where low loss rates are required. RTR also does not cause any additional delay to either video or interactive applications. RTR can be used to make up for loss anywhere in the path between the transmitter and the STB. Finally, RTR does not result in increased bandwidth when the path between the transmitter and the STB are not experiencing loss. The down side of RTR is the fact that it requires application support in both the STB and the transmitter. In addition, RTR schemes experience performance problems as the round trip time (RTT) between the STB and the RTR-enabled transmitter increases and as the number of STBs served by an RTR-enabled multicast transmitter increases.

Service Availability

Service providers deploying video services often have different availability requirements for VoD and broadcast video services, as contrasted below.

Broadcast video services are inherently real time. A subscriber who experiences an outage in the broadcast service cannot come back and continue watching at that point when the outage is over. Because of this and the higher usage rates associated with broadcast services, the availability associated with broadcast services must be very high.

In contrast, the customer disruptions associated with an outage in VoD services are typically much less problematic. A subscriber who experiences an outage in a VoD service can come back at a later time and replay the content—either from the point of disruption or from the beginning. In addition, the peak usage rates associated with VoD are typically between 10 and 20% of the subscriber population. This is much lower than the peak usage rates for broadcast services.

Because of the above factors, service providers have much higher availability requirements for broadcast services than for on-demand services. Consequently, the differing availability requirements between the two services may result in differing transport requirements for each service. For example, the high-availability requirement for broadcast video typically results in the requirement that there be redundant transport paths between the DER and AR nodes of the distribution network. (See Figure 2-3 on page 2-11.) Because of the higher bandwidth and lower availability requirements associated with VoD services, the topologies used for these services may not necessarily require redundant transport paths.

The service-mapping architecture documented in Release 1.0 of the solution enables distribution network designs that provide path redundancy for both services, as well as a cost-optimized distribution design that provides path redundancy for broadcast services only. (While Release 1.1 of the solution does not include network designs that offer different levels of path redundancy for different services, Release 1.0 does.) In addition, the quality of service (QoS) architecture includes DiffServ marking for broadcast and on-demand services, allowing the network to drop VoD traffic preferentially over broadcast traffic

in the event of a network outage. Finally, the solution supports redundant broadcast video encoders, as well as a method to fail over in a timely manner from one encoder to another. Both of these features are included in the network designs illustrated and tested in this release of the solution.

Broadcast Video Channel-Change Time

An important aspect of a broadcast video service is the amount of time it takes for the system to respond to a channel-change request from a subscriber. While the channel-change time for current analog broadcast services is perceived by the subscriber to be instantaneous, the channel-change time for digital broadcast services is between one and one-and-a-half seconds. The majority of this time is due to the differential encoding and decoding methods used to compress digital video streams.

To reduce the amount of bandwidth required for digital video transmission, compression methods such as MPEG compress the video frames of a digital video stream into three different types of frames. These frames are called I-frames, B-frames, and P-frames. An I-frame is a compressed version of all of the information in one frame of a video stream. An MPEG decompressor can recreate the original frame using just the information in the I-frame. A P-frame is an incrementally encoded video frame that can be decoded with the information in the preceding anchor frame (I-frame or P-frame). A B-frame is an incrementally encoded video frame that can be decoded with the information in the preceding and following anchor frames (I-frame or P-frame).

Because of incremental coding, an important factor in how long it takes to change a channel for a digital video service is the I-frame gap. The I-frame gap defines how often I-frames are included in the MPEG stream. Shorter I-frame gaps result in shorter channel-change times, while longer I-frame gaps result in longer channel-change times.

When a digital broadcast service is run over a DSL access infrastructure, the following additional factors must be added to the delay caused by the I-frame gap:

- STB performance in processing a channel-change request
- Multicast latency in terminating the IP video feed associated with the “tuned from” channel
- Multicast latency in joining the IP video feed associated with the “tuned to” channel
- Whether or not the “tuned to” channel is encrypted by means of a CAS
- Delay to the next cryptoperiod and the time needed to acquire CAS/DRM (digital rights management) decryption keys before the decryption of the “tuned to” channel begins
- Delay in refilling the jitter buffer for the decoder in the STB

The goal of this solution is to provide subscribers with a channel-change experience similar to that currently experienced for digital broadcast services. Most of the additional channel-change delay associated with a DSL access infrastructure is due to the amount of time it takes for the network to stop sending the multicast stream for the “tuned from” channel and to begin sending the multicast stream for the “tuned to” channel. Multicast Admission Control, page 3-16, provides a recommendation for a scalable multicast architecture that best meets the channel-change requirements for broadcast video services.

Potential Video Service Architectures

One aspect of a transport architecture for video that must be considered initially is how the service provider sells the video service to the subscriber. This section examines how two potential video service-level agreement (SLA) models affect the requirements of a transport network implemented to deliver the service to the subscriber.

- The SLA for a video transport service is based on transport parameters. A typical transport-based SLA includes factors such as maximum bandwidth, packet-loss rate guarantees, and jitter and latency guarantees.
- The SLA for an application service is based on service-level parameters. A typical video application-based SLA includes the following:
  - The number of simultaneous video channels (live or on-demand) a subscriber a is authorized to view
  - The broadcast channel line-up (basic or premium tier) that the subscriber has signed up for
  - Any subscription VoD content that the subscriber has signed up for

The services the network provides to deliver a transport-based SLA as opposed to an application-based SLA are very different. Table 2-1 provides an overview of the technologies used to deliver the basic functionality of a transport service as opposed to an application service.

Table 2-1 Service-Delivery Technologies: Transport vs. Application

Service Type	Transport Service	Managed Application Service
SLA	Transport parameters: • Bandwidth • Max. drop • Max. latency • Etc.	Video application SLA: • Number of STBs • Basic vs. premium tier
Subscriber authentication/ identification	Network based (examples): • PPPoE • DHCP[1] authorization • Per-subscriber VLANs • DHCP option 82 • PPPoE[2] tags	Application based: • Video middleware
SLA enforcement	Network based: • Per-subscriber shaping/policing	Application based: • Based on application signaling
QoS	Per subscriber: • Gold, silver, bronze • Classification • Queueing	Aggregate: • Single queue for video service

1. Dynamic Host Control Protocol
2. Point-to-Point Protocol over Ethernet

The two SLA models are examined in detail in the following sections:

- Network Requirements for Transport Services
- Network Requirements for Managed Application Services

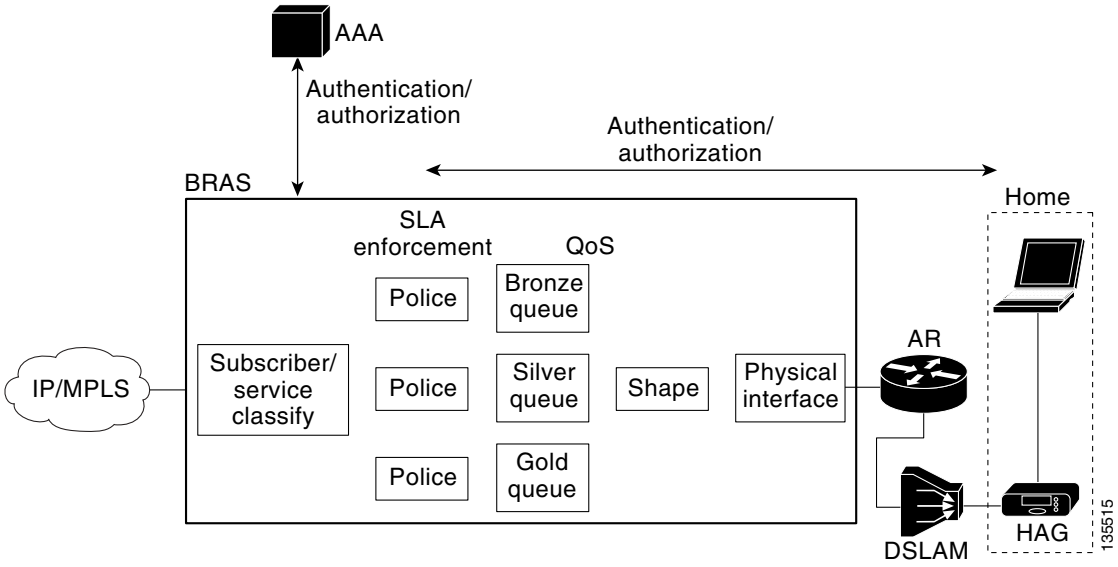
Network Requirements for Transport Services

Subscriber authentication and identification for a transport service is done at the transport layer. Subscriber authentication technologies rely on shared secrets such as passwords or private/public key pairs to establish a trust relationship between the subscriber and the network. Subscriber identification technologies use a well-known property of a subscriber (such as the DSL line to which the subscriber is attached) to identify all packets coming from or to the subscriber. Transport SLA enforcement requires a subscriber identification technology and may also include a subscriber authentication technology.

Common subscriber-authentication technologies used for a transport service include Challenge Handshake Authentication Protocol (CHAP) used with Point-to-Point Protocol over Ethernet (PPPoE) and Dynamic Host Control Protocol (DHCP)-based authentication used with native IP. These technologies are used to authenticate a subscriber transport session. To enforce a subscriber's transport SLA at the transport layer in PPPoE environments, every packet associated with a subscriber's transport session can be identified with a PPPoE session ID that is specified as part of the PPPoE tunnel encapsulation. In native IP environments, every packet associated with a subscriber's transport session can be identified by using the IP source/MAC address of the packet. Note that both PPPoE-based and native IP-based architectures could also use a VLAN tag to identify the traffic associated with a particular transport session. Either VLAN tags or DHCP option 82 could be used to associate a transport session with an access line such as a DSL line. Note also that an identification technology could be used to enforce a subscriber transport SLA without the use of an explicit subscriber-authentication protocol.

SLA enforcement and the resulting QoS architecture used for transport services rely on per-subscriber shaping, as well as on per-subscriber, per-service classification, policing, queueing, and scheduling. SLA enforcement is typically implemented in the same node that terminates the transport session (PPPoE or DHCP). Packets are classified per subscriber according to the transport session identifiers described above. The downstream traffic for each subscriber is typically shaped to a maximum rate based on the parameters of the transport SLA. If the transport SLA sold to the subscriber includes more than one class of service (gold, silver, or bronze), then additional classification, queuing, and scheduling are done to enforce and guarantee the transport parameters of the SLA associated with each class. For transport services, the node that terminates the transport session and enforces the subscriber SLA is typically the broadband remote-access server (BRAS). Figure 2-4 on page 2-18 illustrates the per-subscriber control and data plane functionality used by the network to implement a transport service.

Figure 2-4 Per-Subscriber Control and Data-Plane Functionality Used to Implement a Transport Service

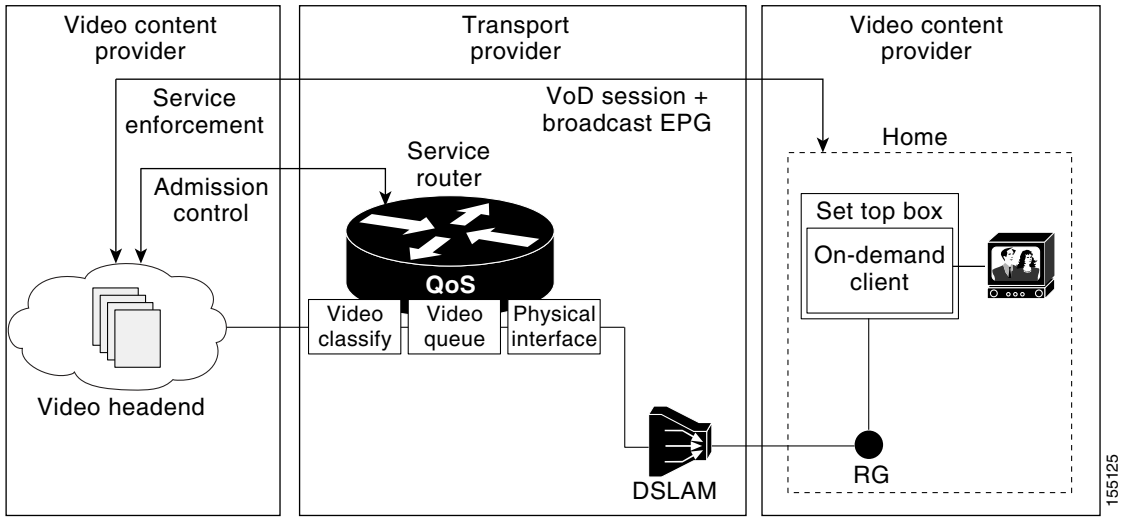


Network Requirements for Managed Application Services

Subscriber authentication for an application service is implemented by means of application-aware components. For example, Electronic Program Guide, page 2-3, describes how subscriber authentication for a video service is typically implemented as part of the electronic program guide (EPG) function. The EPG, a component of video middleware, often authenticates a subscriber's video STB by means of an application-layer challenge such as an HTTP authentication challenge. If the EPG is not able to authenticate the STB, the subscriber cannot use the STB for broadcast video services. SLA enforcement for a managed application service is also performed by application-aware components. As an example, the number of simultaneous video streams that a subscriber may have active for a video application service is limited by a combination of (1) the number of authorized STBs the subscriber has in the home, and (2) the video session limits enforced by the video middleware.

Because SLA enforcement for a managed application service is performed by application-aware components, the QoS architecture required to support an application-aware service can be greatly simplified. Instead of having shapers and queues per subscriber, QoS architectures that use class-based classification and scheduling, such as the DiffServ architecture, can be used for QoS. Figure 2-5 on page 2-19 illustrates the application and transport architecture used to implement a video application service.

Figure 2-5 Application and Transport Architecture Used to Implement a Video Application Service



While an Internet access service is typically sold as a transport service, a video service may be sold to a subscriber as ether a transport or an application service. From the discussion above, the transport architecture needed for an application service is significantly different from that needed for an application service.

The Release 1.1 transport architecture is optimized for service providers that sell video as a managed application service. In the solution transport network design, architectural tradeoffs have been made with this assumption in mind.

Service Mapping in a Triple-Play Architecture

An important aspect of the transport network for a triple-play architecture is how much support the network provides in isolating each service. This section addresses the following topics:

- Forwarding Architectures
- Service-Availability and Bandwidth Requirements
- Organizational Structure
- IP Infrastructure Components
- Service Mapping in the Release 1.1 Architecture

Minimally, the network must provide the ability to meet the delay and drop requirements for each service when multiple services share the same physical link. This capability is inherent in the QoS architecture of the solution. (See QoS Architecture, page 3-46.)

In addition, the network may be configured to provide separate forwarding and routing domains for each service. This level of service mapping is very useful when a service provider wants to manage separately the address space, topology, and IP infrastructure associated with each service. The following subsections explain why a service provider may want to have different transport attributes for different sets of services.

Forwarding Architectures

The transport architecture associated with different services may require the use of different encapsulations and therefore different types of packet forwarding. If one creates separate logical topologies for different services, these services can be forwarded by means of different forwarding techniques. The paragraphs below illustrate how the different transport architectures of Internet access and video services require that there be separate logical forwarding planes for the two service categories.

As explained in Potential Video Service Architectures, page 2-16, Internet access service is typically sold as a transport service. In a DSL environment, this typically results in a transport architecture that uses a PPPoE session from a CPE device to a BRAS that authenticates subscriber sessions and enforces the SLA associated with that session. Because PPPoE encapsulation requires an 802.3 header, PPPoE packets must be forwarded by means of Layer 2 switching between the PPPoE client (the CPE device) and the PPPoE server (the BRAS).

Also from Potential Video Service Architectures, page 2-16, the transport architecture in the solution assumes that the SLA for video services is an application SLA. Because authentication and enforcement are application services implemented in application components, there is no need to use a Layer 2 tunneling protocol such as PPPoE or a transport-layer authentication and enforcement component such as a BRAS for video services. Instead, video services can use IP encapsulation between the STB and the video infrastructure components described in Video Application Components, page 2-1. Since IP encapsulation is used, there is no need to forward packets between STBs and the video infrastructure components in the VHO using only Layer 2 switching. The solution transport architecture described in this document uses a combination of Layer 2 and Layer 3 forwarding for broadcast video and VoD services.

Note that the Internet access transport architecture described above requires that the access, aggregation, and distribution networks switch Internet access packets at Layer 2, while the video transport architecture allows these networks to switch video packets at either Layer 2 or Layer 3. To allow Layer 3 switching for video and Layer 2 switching for Internet access, the network must be configured into separate logical topologies that are switched by means of different encapsulations and packet switching functions (Layer 2 vs. Layer 3). In the two configuration models presented in this design and implementation guide (see Release 1.1 Configurations, page 3-36), the transport architecture separates these logical topologies as follows:

- In the 10-GE ring model, the aggregation and distribution networks separate the topologies by means of IPv4 for voice and video services, and Multiprotocol Label Switching (MPLS) for high-speed data (HSD).
- In the 1-GE plus 10-GE hub-and-spoke model, the aggregation and distribution networks are separated by means of 802.1q VLANs for the different services.

Service-Availability and Bandwidth Requirements

Because different services have different service-availability and bandwidth requirements, a service provider could potentially reduce the cost of the network while maintaining the requirements for each service by creating separate logical topologies for different services.

As an example of different service availability requirements, Service Availability, page 2-14, describes the different availability and bandwidth requirements of broadcast video and VoD services. A service provider could optimize the network for both services by creating separate logical topologies for each service. These topologies could be created by using VRF-based technologies such as MPLS VPN or VRF-lite. [VRF stands for virtual private network (VPN) routing and forwarding, as well as a VRF instance.] In addition, the separate logical topologies could be created by populating the routing table with multiple instances of routing processes running on the different topologies and not exchanging routes between these processes. The differing availability requirements for broadcast video and VoD

may lead to a transport requirement that the network must provide redundant paths for broadcast video but not for VoD. To meet this requirement cost-effectively, separate logical topologies can be created for the two services. The logical topology for broadcast video maps the address space associated with real-time encoders and STBs into a topology with redundant physical paths, while the address space associated with VoD servers and STBs maps into a VRF with nonredundant physical paths.

Note Test configurations did not include the use of VRF technologies to map services to different VRFs.

Organizational Structure

A service provider may have an organizational structure in which different services are managed by different organizations. The ability to map different services to different logical topologies allows each organization to manage and debug the transport as well as the IP infrastructure components separately.

IP Infrastructure Components

When different services are managed by different organizations within a service provider, it may be operationally simpler to have separate IP infrastructure components such as Dynamic Host Configuration Protocol (DHCP) servers for different services. Using different DHCP servers for different services allows the IP address spaces for these services to be managed separately. It also allows the DHCP servers to be configured separately for different services without having to use static configuration on the DHCP server to associate different CPE devices with different services.

Service Mapping in the Release 1.1 Architecture

Because of the transport architecture issues described in Forwarding Architectures, page 2-20, it is unlikely that early wireline video/IPTV deployments use a unified transport architecture for all services. Because of this, Release 1.1 uses a service mapping architecture in which traffic associated with each service is forwarded to or received from a separate logical access topology at the CPE device. This service-based logical topology separation is continued through the aggregation and distribution networks.

This transport architecture allows traffic associated with different services to be aggregated or terminated at different sites by means of different infrastructure components. This architecture allows traffic associated with Internet access services to be aggregated at a BRAS, while traffic associated with video services (specifically the managed video application service types) is terminated by means of the video infrastructure components described in Video Transport Architecture and Issues, page 2-10.

Video Forwarding Architecture, page 3-11, describes how service mapping is implemented in the aggregation and distribution networks in Release 1.1, while Edge Transport Architecture, page 3-40, describes alternatives for implementing service mapping at the CPE device and in the access network.

Triple-Play Architecture—Relation to Existing Standards

The DSL Forum publishes specifications for DSL-based access and aggregation transport architectures. The TR-25 and TR-59 specifications currently published by the DSL Forum specify the access and aggregation infrastructure requirements and architectural alternatives for an ATM-based DSL aggregation infrastructure. The DSL Forum is currently finalizing a new specification, labeled WT-101, that specifies the access and aggregation infrastructure requirements and architectural alternatives for an Ethernet-based DSL aggregation infrastructure. The following topics are addressed in this section:

- WT-101 Service Mapping
- WT-101 QoS Architecture
- WT-101 Layer 3 Edge Architecture
- WT-101 Multicast Architecture
- Solution Transport Recommendations Based on WT-101

Note The draft specification referenced here is "DSL Forum Working Text WT-101, Revision 8: Migration to Ethernet Based DSL Aggregation—for Architecture and Transport Working Group," August 2005, edited by Amit Cohen and Ed Shrum.

The following discussion presents an overview of the architectural issues in the draft specification. The configurations presented in this design and implementation guide show what was actually tested.

WT-101 defines the changes to interfaces and components that are implied by moving from an ATM and Ethernet aggregation infrastructure for DSL. The aggregation architecture described in WT-101 can be translated into other access technologies besides DSL. Examples of such technologies that the architecture described in WT-101 can be leveraged across are Passive Optical Network (PON) [including Broadband PON (BPON) and GigaPON (GPON)] and Metro Ethernet aggregation.

To document the changes from ATM to Ethernet aggregation, WT-101 specifies two architectural interfaces as part of the DSL and Ethernet aggregation network:

- The U-interface specifies the encapsulations used on the DSL line itself.
- The V-interface specifies the encapsulations used on the Ethernet interfaces between the DSLAM and the BRAS.

WT-101 also specifies requirements for a set of architecture components used as part of the Ethernet aggregation architecture. The components specified by WT-101 are access nodes, aggregation nodes, and the broadband network gateway (encompassing the functionality of the BRAS in the solution architecture). The access node in WT-101 is the DSLAM, which terminates the DSL line and uses Ethernet uplinks towards the aggregation network. Aggregation nodes in WT-101 perform Layer 2 Ethernet aggregation, while the BRAS terminates subscriber transport sessions and acts as the Layer 3 edge device.

The solution transport architecture is consistent with the requirements and architectural alternatives documented in WT-101. However, while WT-101 defines a framework of architectural alternatives for DSL aggregation based on Ethernet, it does not specify or recommend a particular architectural model for DSL-based triple-play services. This section documents the architectural model recommended to support the solution, using the terminology and context of WT-101.

WT-101 Service Mapping

One of the architectural requirements specified in WT-101 is the ability to map different services in a residential environment to different logical topologies in the access and aggregation infrastructure. When different services are mapped to different logical topologies, these services are terminated in different Layer 3 edge devices (that is, the BRAS). When different services are mapped to different logical topologies, this logical mapping typically originates at the CPE device in the home. Because this mapping originates at the CPE device, the architecture specified in WT-101 must specify architectural alternatives for carrying this mapping as part of the encapsulations used in both the access and aggregation networks.

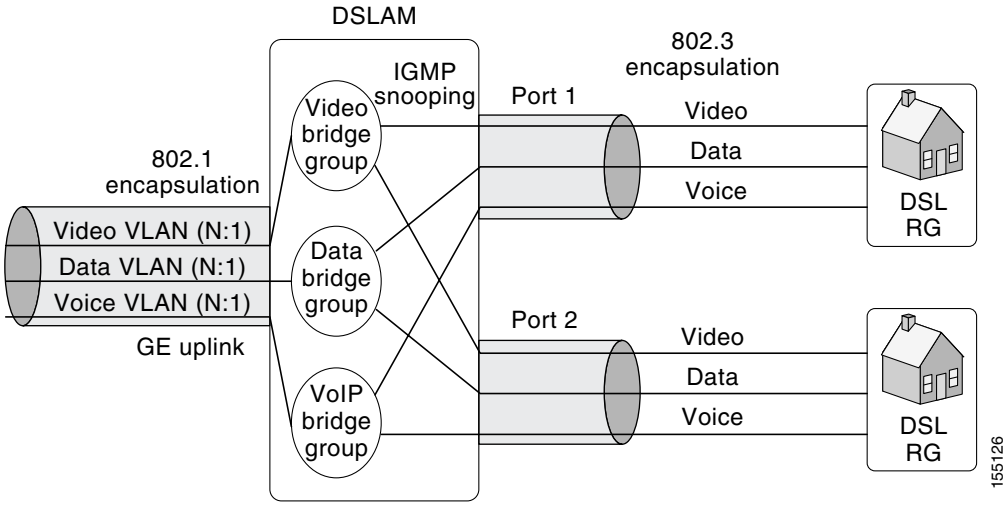
Service Mapping in the Access Network

WT-101 specifies three architectural choices for carrying this mapping on the DSL access lines. This document refers to these choices as multi-VC access architecture, EtherType architecture, and multi-VLAN architecture.

Multi-VC Access Architecture

In the multi-VC architecture, separate ATM virtual circuits (VCs) are used to distinguish the address spaces for the different services. These VCs are also used to provide the proper QoS characteristics for each service. Figure 2-6 illustrates a multi-VC access architecture where the DSLAM/BPoN optical line terminal (OLT) maps ATM VCs on the DSL line to service VLANs in the GE uplink.

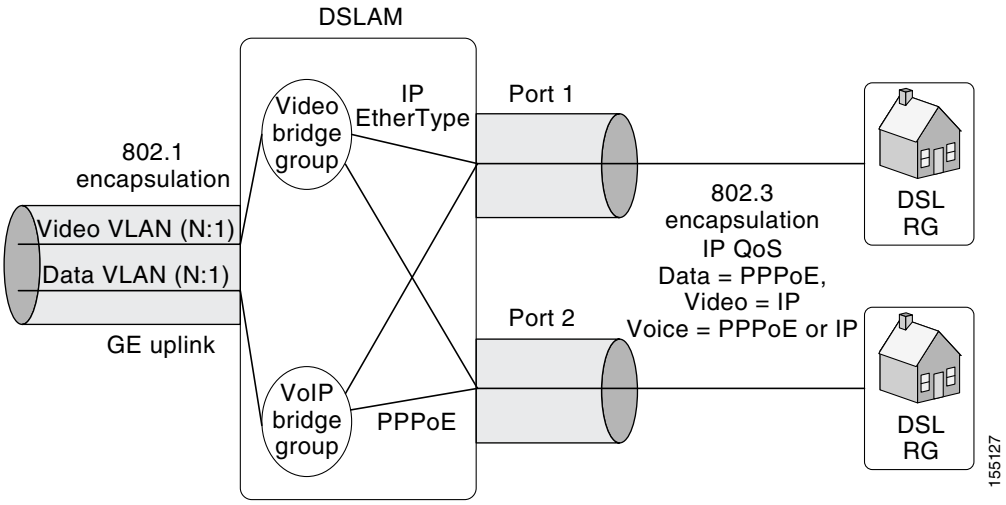
Figure 2-6 Multi-VC Access Architecture



EtherType Access Architecture

In the EtherType access architecture, the EtherType field of Ethernet packets is used to distinguish between two different address spaces. In this architecture the Internet access service is assumed to use PPPoE encapsulation, while the video service is assumed to use IP encapsulation. When PPP and IP packets are carried over Ethernet, the EtherType field can be used to distinguish between these two types of packets. In the EtherType model the voice service must be carried in one of the two topologies represented by these two values of the EtherType field. Because a single VC is used for all services, the EtherType model assumes that Ethernet- or IP-layer QoS is used to provide the proper quality of service for each of the services. Figure 2-7 illustrates the EtherType access architecture, where the DSLAM maps the Ethertype value on the DSL line to service VLANs in the GE uplink.

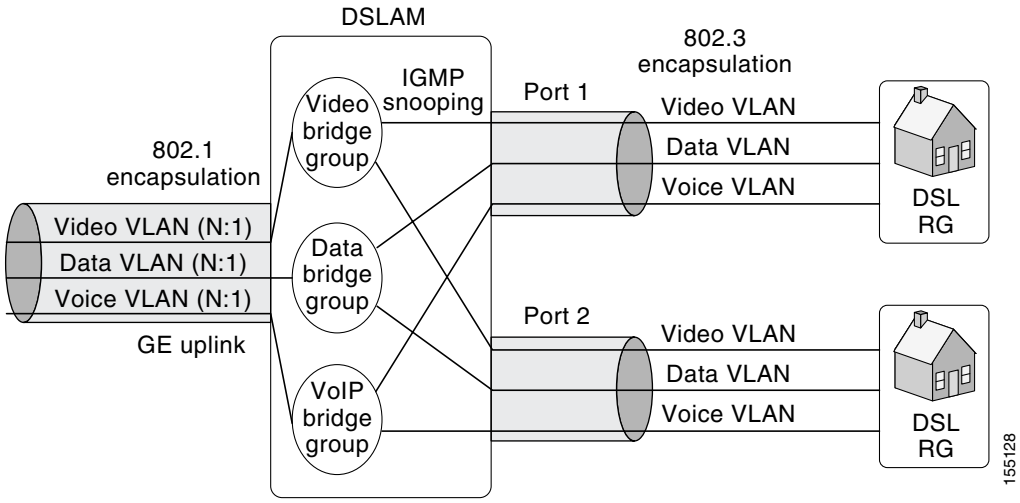
Figure 2-7 EtherType Access Architecture



Multi-VLAN Access Architecture

In the multi-VLAN access architecture, 802.1q encapsulation is used on the DSL line, and separate VLAN IDs are used to distinguish the address spaces for the different services. The DSLAM may then map these VLAN IDs on the GE uplink to a separate set of VLAN IDs that identify the address space on that link. Because a single VC is used for all services, the VLAN model assumes that Ethernet or IP-layer QoS is used to provide the proper quality of service for each of the services. Figure 2-8 on page 2-25 illustrates the VLAN access architecture, where the DSLAM maps the VLAN ID on the DSL line to service VLANs in the GE uplink.

Figure 2-8 Multi-VLAN Access Architecture



Service Mapping in the Aggregation Network

WT-101 also specifies two alternative VLAN architectures for mapping residential services to VLANs in the Ethernet aggregation network. The alternatives are called the N:1 VLAN architecture and the 1:1 VLAN architecture. The N:1 and 1:1 VLAN architectures are in fact defined in WT-101 as methods of mapping subscriber lines and services to VLANs. The N:1 model maps many subscriber lines and services to a single VLAN, while the 1:1 model maps each subscriber line to a separate VLAN.

N:1 VLAN Model

In the N:1 VLAN model, multiple subscribers and services are mapped to the same VLAN in the Ethernet aggregation network. There are many possibilities for mapping groups of subscribers and services to VLANs in this model. For example, each VLAN in the N:1 model may be used to aggregate all the subscribers associated with a particular service. When service mapping is implemented by means of the N:1 model, all the subscribers associated with a particular service and DSLAM are mapped to a single VLAN. The DSLAM performs an Ethernet bridging function between the DSL lines aggregated into a VLAN and the upstream Ethernet VLAN. One of the security issues associated with Ethernet bridging in WT-101 is that one subscriber may be able to snoop another subscriber's Ethernet frames. To alleviate this concern, WT-101 specifies that the DSLAM must support the ability to perform split-horizon forwarding between the DSL lines and the Ethernet uplink.

One of the architectural requirements of WT-101 is that subscriber transport sessions (PPPoE or DHCP sessions) be associated with the DSL line from which the session originated. Because a single VLAN in the N:1 VLAN model can represent many subscriber lines, the VLAN ID itself cannot be used to associate a DSL with a subscriber. WT-101 uses extensions to the transport session protocols themselves to provide subscriber line identification in the N:1 VLAN model. WT-101 specifies the use of PPPoE tags to provide the subscriber line ID function with PPoE sessions, and specifies the use of DHCP option 82 to provide the subscriber line ID function for DHCP sessions.

1:1 VLAN Model

In the 1:1 VLAN model, each subscriber line is identified in the aggregation network by means of a separate VLAN ID. This architecture is very similar to the original ATM-based DSL aggregation architecture, because each subscriber in the ATM architecture is identified at the BRAS by a separate ATM virtual circuit. Because of the number of bits in an 802.1q VLAN tag, Layer 2 aggregation networks that support more than 4096 subscribers must use 802.1ad encapsulation (Q in Q) to support the 1:1 VLAN model. In this model, the DSLAMs must map each DSL line to a separate VLAN tag on the Ethernet uplink. When 802.1q encapsulation is used, the DSLAM must map each DSL line to a separate 802.1q VLAN ID. When 802.1ad encapsulation is used, the DSLAM must map each DSL line to a separate set of inner and outer 802.1ad tags. The DSLAM forwarding model used for 1:1 VLAN aggregation is a simple cross connect model. The DSLAM simply forwards all packets from (or to) a specific DSL line and access service identification tag (VC, VLAN, or EtherType value) to (or from) a specific VLAN ID on the upstream GE port.

While WT-101 does not specify the mapping between a DSL line and a set of 802.1ad tags, a straightforward mapping that simplifies the requirements of the Layer 2 aggregation network involves mapping a DSL line ID to the inner VLAN ID (C-tag) and a unique DSLAM ID to the outer VLAN ID (S-tag). When this form of mapping is used, a Layer 2 aggregation network that supports only 802.1q encapsulation can be used for aggregation, because service mapping for N:1 services is performed by means of an 802.1q tag and for 1:1 services by means of 802.1ad S-tag. Figure 2-9 on page 2-27 illustrates a multi-VC access architecture, where the DSLAM maps voice and video VCs to service (N:1) VLANs, while Internet access VCs are mapped to per-subscriber (1:1) VLANs. Figure 2-10 on page 2-27 illustrates a single-VC access architecture, where the DSLAM maps voice and video VCs to service (N:1) VLANs, while Internet access VCs are mapped to per-subscriber (1:1) VLANs.

When service mapping is used in the Layer 2 aggregation network, the 1:1 VLAN model can be used for some services, while the N:1 VLAN model can be used for other services. The solution transport architecture makes use of this functionality to enable the Internet access service to use 1:1 VLANs, while the video service uses N:1 VLANs. When the 1:1 VLAN service is implemented by means of 802.1ad encapsulation, the 1:1 subscriber-line-to-VLAN mapping scheme described in the previous paragraph can be configured to ensure that the S-tag generated by the DSLAM for the Internet access service is different from the 802.1q tag generated for the video service. This configuration enables the Layer 2 aggregation network to separate the logical topologies for Internet access and video by using only the 802.1q VLAN/802.1ad S-tag.

Figure 2-9 1:1 + N:1 Service Mapping in a Multi-VC Access Architecture

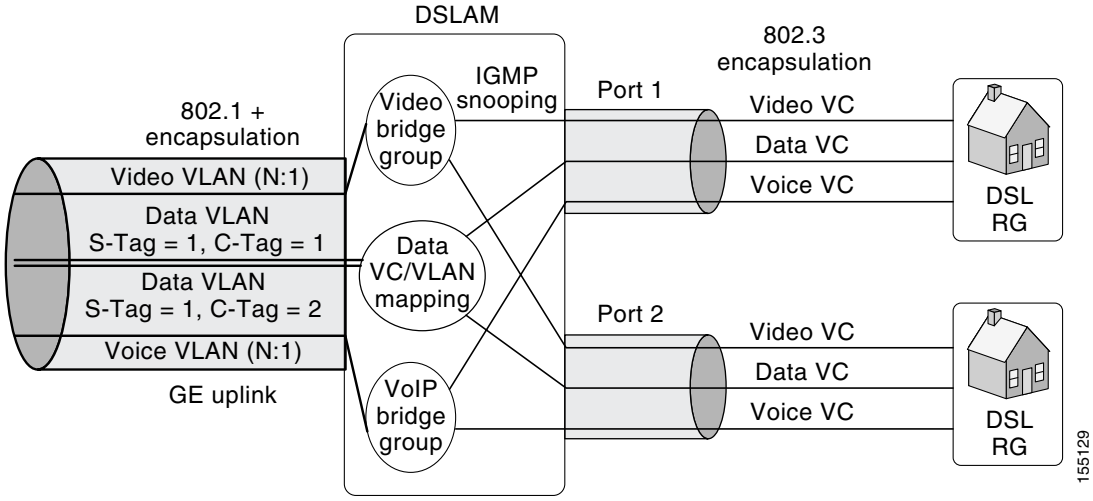
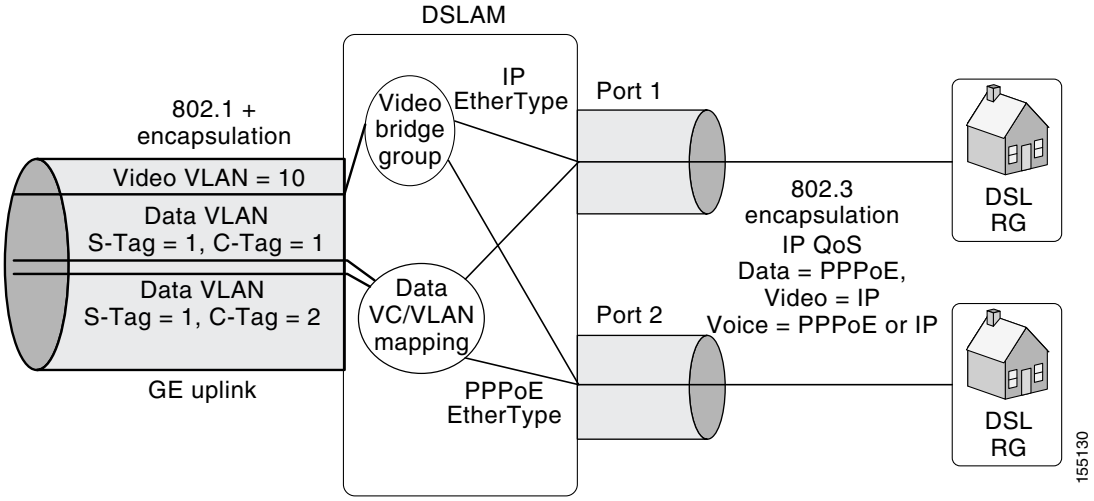


Figure 2-10 1:1 + N:1 Service Mapping in an EtherType Access Architecture



WT-101 QoS Architecture

The requirements specified in WT-101 enable either a centralized or distributed QoS architecture to be implemented in the access and aggregation networks.

Centralized QoS Architecture

In the centralized QoS architecture, all QoS functionality is implemented in the BRAS if the Layer 2 aggregation nodes and DSLAMs are not QoS capable. In this architecture, the BRAS essentially models both the aggregation and access networks by using the three-level hierarchical shaping and scheduling algorithms described in DSL Forum TR-59. The centralized QoS model also assumes that all traffic for all downstream services goes through a single BRAS node.

Note For more information, see "Technical Report, DSL Forum TR-059: DSL Evolution—Architecture Requirements for the Support of QoS-Enabled IP Services," at the following URL:

www.dslforum.org/techwork/tr/TR-059.pdf

A centralized QoS architecture in which all QoS is implemented in the BRAS implies that all multicast replication is also done centrally in the BRAS. WT-101 Multicast Architecture, page 2-29, provides details of both the centralized and distributed multicast replication architectures associated with the WT-101 specification.

Distributed QoS Architecture

In a distributed QoS architecture, all QoS is implemented by means of schedulers on physical links. In a this architecture, any physical link that can experience congestion requires a packet scheduler that is capable of classifying and scheduling multiple classes of traffic. The IETF DiffServ architecture (RFC 2475) is an example of a distributed QoS architecture.

The transport architecture relies on a distributed QoS architecture. (For details, see QoS Architecture, page 3-46.)

WT-101 Layer 3 Edge Architecture

The requirements specified in WT-101 enable either a single or multiple Layer 3 edge architecture to be implemented.

Single Layer 3 Edge

In a single Layer 3 edge architecture, all services are terminated in a single BRAS node. The single edge architecture is required in networks that use a centralized QoS model.

Multiple Layer 3 Edge

In the multiple Layer 3 edge architecture, different services may be terminated in different Layer 3 edge nodes. This could be done by mapping different services to different VLAN IDs at the DSLAM, or it could be done through ARP resolution to different Layer 3 edge nodes serving different service-specific subnets.

The solution transport architecture uses a multiple Layer 3 edge architecture, where different services are mapped to different VLANs at the DSLAM.

WT-101 Multicast Architecture

The requirements specified in WT-101 support either a centralized or a distributed replication model for multicast replication.

Centralized Replication

In the centralized replication architecture, all multicast replication is performed at the BRAS. This has a fairly significant impact on the bandwidth used for a video broadcast service, because all broadcast video streams are essentially unicast from the BRAS. (For an analysis of the bandwidth usage associated with centralized vs. distributed multicast replication architectures, see Distributed vs. Centralized Replication Bandwidth, page 2-29.)

While not explicitly specified in WT-101, there is an implicit assumption that all multicast replication be performed in the BRAS when the centralized QoS architecture is used. The reason this assumption is implied is because when multicast traffic is replicated at a node downstream of the BRAS, that node essentially injects traffic that has not been modeled in the hierarchical scheduler of the BRAS. The traffic that is injected could then cause congestion at the node performing replication, resulting in video packets being dropped because of that congestion.

Section 6.3.2.2 of WT-101 (“IGMP Correlation at the BNG for HS and User Statistics”) describes a method by which the BRAS could potentially change the shaping rate of a shaper dynamically, to avoid congestion from a downstream node that performs multicast replication based on the receipt of IGMP messages. Unfortunately, this scheme has timing issues associated with the IGMP state machine. These timing issues could potentially cause packet drops for the video service during channel-change events. The timing issue with the IGMP state machine is that IGMP is inherently a nonacknowledged asynchronous protocol. A node such as a DSLAM or aggregation switch that uses IGMP snooping to perform multicast replication can start the replication associated with incoming IGMP messages before the BRAS ever modifies the downstream shaping rate based on the receipt of that IGMP message. This timing window could be on the order of hundreds of milliseconds, and could result in video packets being lost because of congestion during this period.

Distributed Replication

In the distributed replication architecture, the Layer 3 edge, aggregation, and access nodes all perform replication. Layer 3 capable nodes perform replication using IP multicast, while Layer 2 capable nodes perform replication using IGMP snooping. When distributed replication is used, there is an implicit assumption that the N:1 VLAN architecture is used for multicast video. A single VLAN is required for multicast video to enable a single copy of the multicast video stream to be replicated to multiple subscribers.

The use of distributed replication also implies that a distributed QoS architecture is used. Distributed replication implies distributed QoS, because there are multiple points in the network that can inject video traffic that needs to be isolated at the QoS layer from other traffic (such as Internet access traffic). With distributed replication, any node that performs multicast replication must also be capable of scheduling multiple QoS classes on the physical link the replication is performed on.

Distributed vs. Centralized Replication Bandwidth

Because broadcast video streams are unicast from the BRAS in the centralized replication model, the amount of bandwidth needed for the broadcast video service in the distribution network scales with the number of subscribers—as opposed to the number of broadcast channels offered. Because there are typically many more subscribers served by single BRAS than the number of broadcast channels offered by a broadcast service, the result is that much more bandwidth is used for the broadcast service than with

a distributed replication architecture. The bandwidth savings associated with distributed replication results in more bandwidth being available in the distribution and aggregation networks for nonguaranteed bandwidth services such as Internet access.

Statistical Analysis

The section describes a statistical analysis model that was used to compare the bandwidth used for distributed vs. centralized multicast replication. The analysis uses probability to determine the amount of bandwidth that would be needed to serve a population of subscribers using a broadcast TV service.

In this analysis, each subscriber is modeled as a random process selecting a channel to watch according to a given probability distribution across all possible channels. Given a group of channels, the average bandwidth required by the channels in use is calculated, given the "popularity" probabilities of the channels.

Because we are interested in determining the average number of channels in use, we can consider the channels to be probabilistically independent of each other and consider the channels one at a time.

For a single channel, the probability that this channel is idle is calculated as follows:

Let

p = P{a subscriber will tune to this channel}

N = Number of subscribers subtended by the given AR or DSLAM

so that

$$P\{\text{channel is idle}\} = (1 - p)^N$$

For multiple channels, we sum the above expression.

Let

C = Number of channels

p_k = P{a subscriber will tune to k^{th} channel}

so that the average number of channels in use, C_{IU}, is

$$C_{IU} = \sum_{k=1}^{C} [1 - (1 - p_k)^N]$$

Here, bandwidth = C_{IU}.

When centralized replication is used, one channel is being transmitted to every active subscriber, so the same channel can be transmitted multiple times if it is being viewed by multiple subscribers.

Let

r = Total channel take rate or the P{subscriber is active} or sum over all channels of p_k, the channel popularity

N = Number of subscribers

Here, bandwidth = Nr.

The graphs below chart the results of the statistical analysis described above, which compares bandwidth used in centralized vs. distributed multicast replication. Figure 2-11 on page 2-31 shows the bandwidth savings for distributed vs. centralized multicast replication with a population of 5000 subscribers, while Figure 2-12 on page 2-31 shows the bandwidth savings for distributed vs. centralized multicast replication with a population of 200 subscribers.

Figure 2-11 Bandwidth for Centralized vs. Distributed Replication with 5000 Subscribers

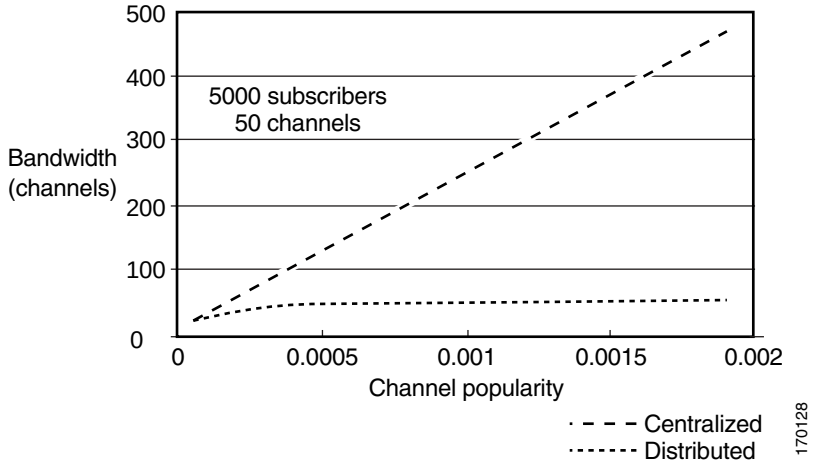
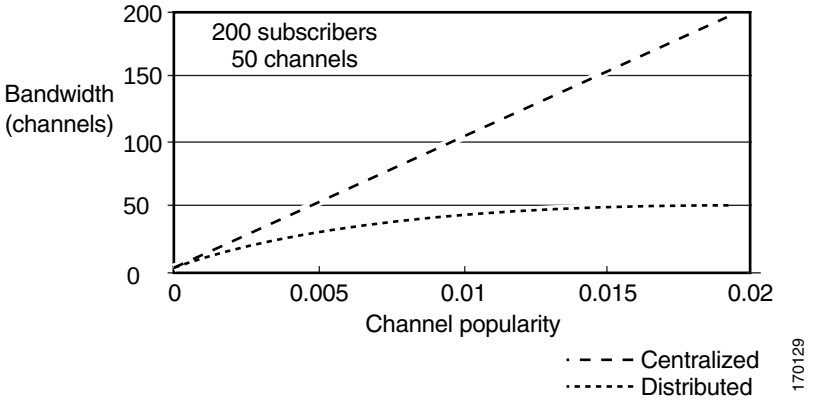


Figure 2-12 Bandwidth for Centralized vs. Distributed Replication with 200 Subscribers



In the centralized replication model, each channel is sent as a unicast stream from the replication source. Because of this, the bandwidth scales linearly with the number of subscribers, as opposed to the number of channels. In the distributed replication model, only one copy of each channel is sent, independent of the number of subscribers watching it. Consequently, the amount of bandwidth that is sent in the distributed replication model is capped at the bandwidth determined by the number of channels that are broadcast.

As illustrated in Figure 2-11 and Figure 2-12, the amount of bandwidth saved in the distributed replication model increases with the number of subscribers served. This is because the bandwidth scales in the distributed replication model with the number of channels, while the bandwidth scales in the centralized replication model with the number of subscribers.

Bandwidth Provisioning Model

In addition to providing additional bandwidth for services such as Internet access, distributed replication can also save on the amount of bandwidth that needs to be provisioned for the combination of broadcast video and VoD services in the distribution and aggregation networks. When broadcast video and VoD services are deployed to set-top boxes (STBs), each STB is typically capable of consuming a single broadcast or on-demand video stream.

The following presents a variety of useful equations.

Bandwidth Requirement for Aggregation and Distribution Networks for VoD

Because VoD services are delivered as unicast streams from a video headend, the amount of bandwidth that needs to be provisioned in the aggregation and distribution networks for a VoD service can be determined by the following equation:

Bandwidth = *Video_Subs* * *Stream_Bandwidth* * (*Peak_Take_Rate* / 100)

where

Video_Subs = Number of subscribers served by a node

Stream_Bandwidth = Amount of bandwidth per video stream

Peak_Take_Rate = Maximum expected use of the service as a percentage of video subscribers

Bandwidth Requirement for Broadcast Video with Unicast Centralized Replication

If the broadcast video service is delivered from the BRAS as unicast streams through the use of centralized replication, then the amount of bandwidth that needs to be provisioned for the broadcast service can be determined by using the same formula above.

Bandwidth Requirement for Broadcast Video with Distributed Multicast Replication

If the broadcast video service is delivered by means of distributed multicast replication, then the amount of bandwidth required for the broadcast service can be determined by the following equation:

Bandwidth = *Min* (*Video_Subs*, *Num_Channels*) * *Stream_Bandwidth*

where

Num_Channels = Number of channels delivered by the broadcast service

Bandwidth Requirement for Broadcast and On-Demand Video with Distributed Replication

When a VoD service is combined with a broadcast service that is delivered by means of distributed replication, the bandwidth for the broadcast and VoD services can be added to determine the total bandwidth required for both services. The following equation can be used to determine the amount of bandwidth required when a VoD service is combined with a broadcast service that uses distributed replication.

Bandwidth = *Video_Subs* * *Stream_Bandwidth* * (*VoD_Peak_Take_Rate* / 100) +
Min (*Video_Subs*, *Num_Channels*) * *Stream_Bandwidth*

where

VoD_Peak_Take_Rate = Maximum expected usage of the VoD service as a percentage of video subscribers

Bandwidth Requirement for Broadcast and On-Demand Video with Centralized Replication

When a VoD service is combined with a broadcast service delivered by means of centralized replication, the fact that an STB can consume a single VoD or broadcast stream results in the following equation to determine the required bandwidth for both services:

Bandwidth = *Video_Subs* * *Stream_Bandwidth* * *Max* (*VoD_Peak_Take_Rate*, *Broadcast_Peak_Take_Rate*)

where

Broadcast_Peak_Take_Rate = Maximum expected use of the broadcast service as a percentage of video subscribers

Because the peak take rate for the broadcast service is typically much higher than that for the VoD service, the amount of bandwidth that is needed for broadcast and VoD services can be much higher when the broadcast service is delivered as unicast streams rather than by means of distributed replication.

The example below uses the following numbers to determine the amount of bandwidth needed to implement a hypothetical video service that uses both distributed and centralized replication architectures for the broadcast video service.

Video_Subs = Number of video subscribers serviced by BRAS = 30,000

Num_Channels = 200

Stream_Bandwidth = 3.75 Mbps

VoD_Peak_Take_Rate = 10%

Broadcast_Peak_Take_Rate = 40%

In this example, the amount of bandwidth needed for the combined VoD and broadcast service from the BRAS when distributed replication is used is 12.75 Gbps, while the amount of bandwidth needed when centralized replication is used is 45 Gbps.

Solution Transport Recommendations Based on WT-101

The solution transport architecture uses distributed multicast replication (as described in WT-101 Multicast Architecture, page 2-29) to ensure maximum bandwidth efficiency for the broadcast video service. The use of distributed multicast replication means that a per-service (N:1) VLAN must be used for broadcast video traffic.

The solution transport architecture also uses a per-service VLAN for the VoD service. The use of per-service VLANs for both the broadcast video (multicast) and VoD (unicast) services enables the use of an aggregate—as opposed to a per-subscriber—QoS and forwarding model for video services. Potential Video Service Architectures, page 2-16, provides the background for why aggregate forwarding and QoS models are preferred for managed application services such as broadcast video, VoD, and voice.

While the solution transport architecture uses per-service VLANs for managed application services such as voice and video, it supports both per-service and per-subscriber (1:1) VLAN architectures for transport services such as Internet access. Service Mapping in the Aggregation Network, page 2-25, describes how a per-service VLAN architecture for managed application services such as video can be combined with a per-subscriber VLAN architecture for transport services such as Internet access.

As noted in Service Mapping in the Aggregation Network, page 2-25, WT-101 specifies that the access node or DSLAM is responsible for performing all VLAN tagging for both per-service and per-subscriber VLAN architectures. For per-subscriber (1:1) VLAN architectures, this means that the DSLAM must be capable of creating 802.1ad-encapsulated packets. Unfortunately, most DSLAMs do not currently support this capability. For this reason, this document recommends the use of per-service (N:1) VLANs

for the Internet access service. Internet Access Forwarding, page 3-28, describes network designs for the Internet access service that include both per-service and per-subscriber VLAN architectures. The per-subscriber VLAN architecture described in that section makes use of DSLAM features that are not available on all DSLAM platforms.

The solution transport architecture uses a multiple Layer 3 edge architecture whereby different services are mapped to different VLANs at the DSLAM.

Service Mapping in the Access Network, page 2-23, describes the models included in WT-101 regarding how to distinguish among multiple service topologies on the DSL line. The solution transport architecture supports both the single-VC and multi-VC models of distinguishing different services on the DSL line. Edge Transport Architecture, page 3-40, describes the solution edge-transport architecture, which includes both the single-VC and multi-VC models in the DSL access network.

Service Mapping in the Aggregation Network, page 2-25, describes the transport session technologies used for services in WT-101. Because the solution transport architecture terminates the video service at a different Layer 3 edge node than does the Internet access service, different transport sessions are used for these services. Also, because the Internet access service is terminated in a BRAS, the solution transport architecture supports the use of both PPPoE and IP/DHCP as the encapsulation/transport session technologies for the Internet access service. The solution transport architecture supports IP/DHCP as the encapsulation/transport session technology for video services. IP/DHCP was chosen for video services because it makes multicast replication much more straightforward in Layer 2 capable nodes such as the DSLAM. These nodes perform replication by means of IGMP snooping. If PPPoE were used for video services, then these nodes would need to perform replication by snooping for IGMP messages inside of a PPPoE session. This is quite a bit more complex than performing native IGMP snooping, because the DSLAM would need to become PPPoE-session-aware as well as IGMP-aware.

The fact that the solution transport architecture uses distributed replication means that it also uses distributed QoS. Distributed replication implies distributed QoS because there are multiple points in the network that can inject video traffic, which must be isolated at the QoS layer from other traffic such as Internet access traffic. With distributed replication, any node that performs multicast replication must also be capable of scheduling multiple QoS classes on the physical link on which the replication is performed. As described in Potential Video Service Architectures, page 2-16, the QoS functionality on the BRAS is used simply to enforce the transport SLA for the Internet access service.

Solution Transport Architecture

The Cisco Wireline Video/IPTV Solution transport architecture is subdivided into recommendations for the access, aggregation, and distribution networks. While the service mapping architecture used in Release 1.1 includes requirements regarding how a residential gateway (RG) interfaces to the home network, it does not include any recommendations for the technologies or configurations used in that network. The Release 1.1 transport architecture also does not include recommendations for the core network. Because of this, the solution test environment combines the video application components of both the super headend (SHE) and video headend office (VHO) sites into a single combined topology that connects aggregation routers (ARs) to a distribution edge router (DER).

This chapter presents the following major topics:

- Overview, page 3-1
- Aggregation and Distribution Transport Architecture, page 3-4
- Release 1.1 Configurations, page 3-36
- Edge Transport Architecture, page 3-40
- QoS Architecture, page 3-46

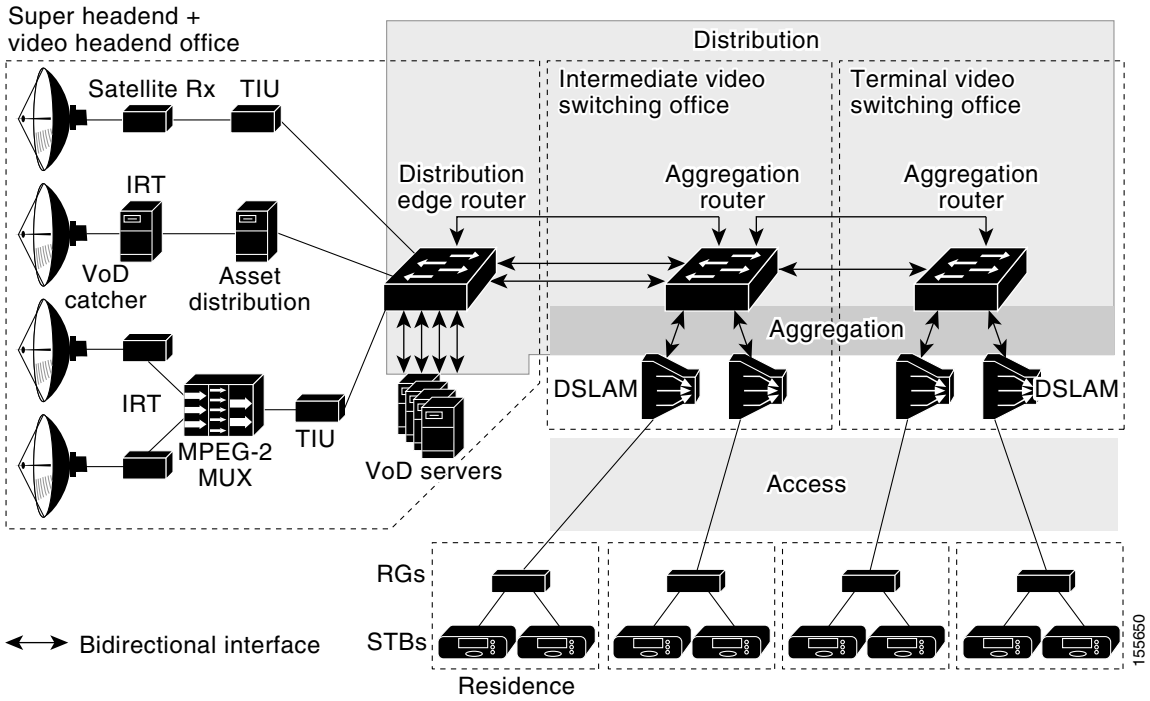
Overview

Figure 3-1 on page 3-2 illustrates the transport layers of the general VoD transport architecture described in Common Broadcast Video and VoD Components, page 2-6. These layers are the subject of the recommendations in this document.

While the solution transport architecture focuses on video, there is an implicit assumption that the network be able to support a full triple-play environment. Consequently, the transport architecture includes a common quality of service (QoS) architecture for video, voice, and Internet access services. Because the transport architecture is based on the service mapping model described in Video Transport Architecture and Issues, page 2-10, the actual transport architecture used for Internet access and voice services may differ from the video transport architecture described in this document.

To ensure that the video transport architecture works in a triple-play environment, solution testing included a test bed environment in which the transport network was configured to support all three services. Because solution testing was focused on video, it included the application, control, and transport environment for video services. Testing only included enough testing of the Internet access and voice services to ensure that an example forwarding architecture for these services can coexist with video, and that the common QoS architecture specified in this document meets the jitter and packet-loss requirements for each service.

Figure 3-1 IPTV/Video over Broadband Transport Architecture: Solution Core



Note This document specifies an example of how the transport network may be configured to support Internet access and voice services. The example configurations described in this document for those services are provided to ensure a fully specified solution test environment. However, these example configurations are not intended to constitute Cisco's recommendation for a proposed transport architecture for those services.

While the transport architecture includes configuration recommendations for all of the transport layers shown in Figure 3-1, this document includes example configurations only for the transport components that are implemented by means of Cisco products. These components are the DER and AR. Because the DER and ARs are the switching components that implement the distribution and aggregation networks, more detailed configuration information is provided for this portion of the network.

Note Figure 1-1 on page 1-2 illustrates the focus of solution testing.

Solution Components

Table 3-1 lists the network architecture components used in Release 1.1 of the solution, with additional information. For detail regarding interfaces, see Table 3-5 on page 3-37.

Table 3-1 Network Architecture Components

Network Role	Vendor	System	Product Number
DER, AR	Cisco	Catalyst switch	7609, 6509
		• Supervisor	WS-SUP720-3BXL
		• 10 GE x 4 optic	WS-X6704-10GE
		• 1 GE x 24 optic	WS-X6724-SFP
		• 48-port copper Ethernet	WS-X6748-GE-TX
DSLAM	Ericsson	Ethernet DSL Access ECN320	FAB 801 3908
		EDN312xp, version R3, revision R1A, ADSL2, ADSL2+	FAB 801 4246
	UTStarcom	AN-2000 DSLAM Node (16 cards w/ 24 ADSL ports each)	AN-2000 B820
HAG	Ericsson	HM340d, version 2, ADSL2 CPE modem	ZAT 759 94/A101
VoD server	Kasenna	GigaBase Media Server	GB-MS-BASEA-LB
			GB-MS-GIGE-COP
Application server		Living Room Application Server	LR-VSIF-HWSW
IP STB	Amino	STB	110

Aggregation and Distribution Transport Architecture

As described in Video Transport Architecture and Issues, page 2-10, the transport architecture uses service mapping to support the capability of having separate routing and forwarding planes for different services. This functionality is used in the aggregation and distribution networks to enable a separate logical and physical transport architecture that is optimized for the delivery of video.

This section describes how the transport architecture is optimized for video. Because an important requirement of the transport architecture is that it also must support a triple-play environment, this section also describes an example distribution and aggregation network configuration for voice and Internet access.

This section presents the following topics:

- Video Forwarding, page 3-4
- Multicast, page 3-15
- Internet Access Forwarding, page 3-28
- Voice Forwarding, page 3-33
- Management, page 3-33
- Redundancy, page 3-35

Video Forwarding

This section presents the following topics related to the delivery of video services:

- Layer 3 Edge for Video Services
- Video Forwarding Architecture

Layer 3 Edge for Video Services

One of the primary architectural decisions that must be made in specifying a transport architecture for video services is where the Layer 3 edge of the transport network should be for video services. Figure 3-2 on page 3-5 illustrates the points in the network where the Layer 3 edge may reside, as well as the issues and benefits associated with each location. There are three points: the DSLAM, the AR, or the DER. This section describes the issues and benefits associated with each of these options, as well as the design choice that was made for Release 1.1.

Figure 3-2 Potential Layer 3 Edge Points for Video

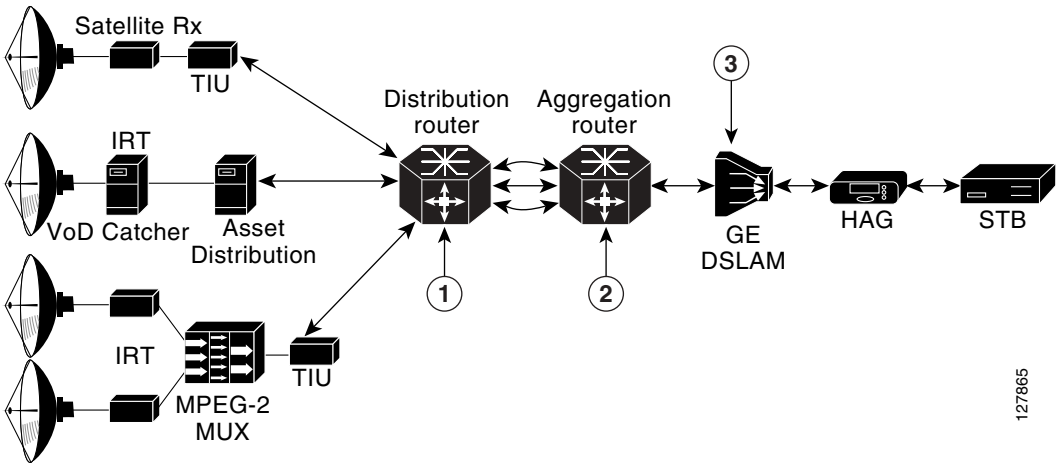


Table 3-2 summarizes issues and benefits for edge points 1, 2, and 3 in the above figure. The paragraphs that follow address issues to related to DSLAM-based, DER-based, and AR-based Layer 3 edge points.

Table 3-2 Issues and Benefits for Layer 3 Edge Points for Video

Edge point	Issue	Benefit
1	ARP/forward table scaling	Is consistent among services.
	MAC table scaling	
	Complex video VLAN topology	
	Potential problems with multicast path failover	
2	Is different for video and Internet access	Supports secure Source Specific Multicast (SSM) in distribution network.
		Supports anycast in distribution network.
		Supports multicast load balancing in distribution network.
		Supports fast failover of video encoders.
		Supports unidirectional transport in distribution network.
3	Requires IP-capable DSLAM	
	Complicates IP address management	

DSLAM-Based Layer 3 Edge

Because of their location at the edge of the network, DSLAMs have traditionally performed Layer 2 switching functions. This has kept the function of the DSLAM fairly simple and has also made DSLAMs simple to manage. However, a Layer 3-capable DSLAM is more complex to build, and therefore more complex to manage.

Issue: DSLAM Complexity

A DSLAM that supports Layer 3 functionality must be capable of a number of functions besides Layer 3 forwarding. For example, a Layer 3-capable DSLAM must be able to support a DHCP relay function. This function requires that the IP address of a DHCP server as well as the IP subnet that the DSLAM is associated with must be configured on the DSLAM. The DSLAM must also support and be configured for IP routing protocols to enable dynamic routing from the AR.

Issue: Complex Subscriber-Address Management

An IP-capable DSLAM must have an IP subnet allocated to it to allow IP packets to be routed to it. This complicates IP address management, because a separate IP subnet must be allocated for each DSLAM. This also makes IP address management for the residence more complex, as separate IP address pools must be allocated for each DSLAM.

DER-Based Layer 3 Edge

The DER may also be at the Layer 3 edge for video. With this type of design, forwarding in both the aggregation and distribution networks is performed at Layer 2. While such a design is consistent with common designs for PPPoE-based Internet access services, it creates a number of scaling issues for both the ARs and the DER. This design can also create issues for video services, because of the flooding associated with common learning-bridge architectures.

Issue: Scaling for the Layer 2 MAC Table and Layer 3 Forwarding Table

To understand the scaling issues associated with this design, it is useful to look at the number of STBs that may be aggregate by a single DER. To provide worst-case scaling numbers, we use the following numbers for a hypothetical VoBB deployment:

- Each DSLAM serves 400 video subscribers.
- Each AR aggregates 40 DSLAMs.
- The DER aggregates 10 ARs.

Therefore, in this example, the DER is aggregating 160,000 subscribers.

When the DER is configured as the Layer 3 edge for video services, all STBs that are connected through that router are in the same IP subnet. If the subnet is aggregated as a single Layer 2 topology, each of the ARs aggregated by the DER need to support MAC table forwarding entries for all of the STBs on that subnet. This amounts to 160,000 MAC table entries for each AR. This requirement drives up the cost of ARs, because each MAC table entry requires a hardware content-addressable memory (CAM) table entry. There are methods that use separate VLANs to divide the distribution layer topology into simpler Layer 2 topologies that are aggregated at the DER. These methods reduce the MAC table scaling requirements for the ARs, but result in a more complex Layer 2 topology to administer in the distribution network.

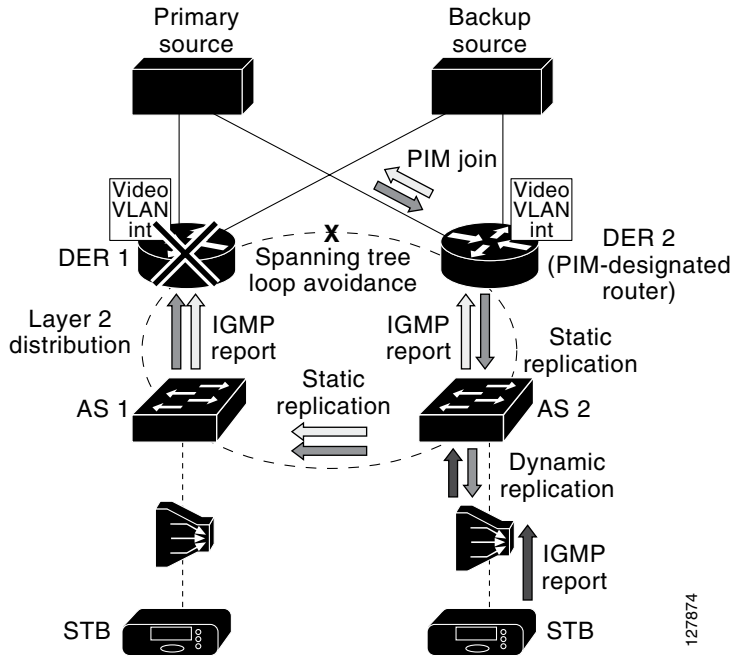
Another issue with configuring the DER as the Layer 3 edge for video services is that this router must maintain a separate ARP table entry and forwarding table adjacency for each STB aggregated through it. In our previous example, this amounts to 160,000 such adjacencies. Such a large number again results

in higher cost for this router, because each forwarding adjacency uses a separate hardware ternary CAM (TCAM) entry. By comparison, if the Layer 3 edge in the example above were moved to the AR, this device would need to support only 16,000 ARP table entries and forwarding adjacencies.

Issue: Multicast Configuration Complexity and Transport Inefficiencies

A network design that aggregates multicast video traffic at Layer 2 results in a complex multicast configuration, as well as in significant inefficiencies in multicast traffic behavior. Figure 3-3 illustrates the configuration complexity and transport inefficiencies when a Layer 2 distribution network is used for multicast video.

Figure 3-3 Multicast Convergence with Layer 2 Distribution



When multicast video is aggregated at Layer 2, the resulting design typically uses more than one DER for redundancy. As a result, the PIM protocol state machine elects a designated router (DR). The DR is responsible for registering sources and sending upstream join and prunes on behalf of the members of the subnet (VLAN). In addition, the network selects an IGMP querier for the served subnet. The IGMP querier is responsible for sending IGMP queries on the subnet served by the redundant IP edge routers.

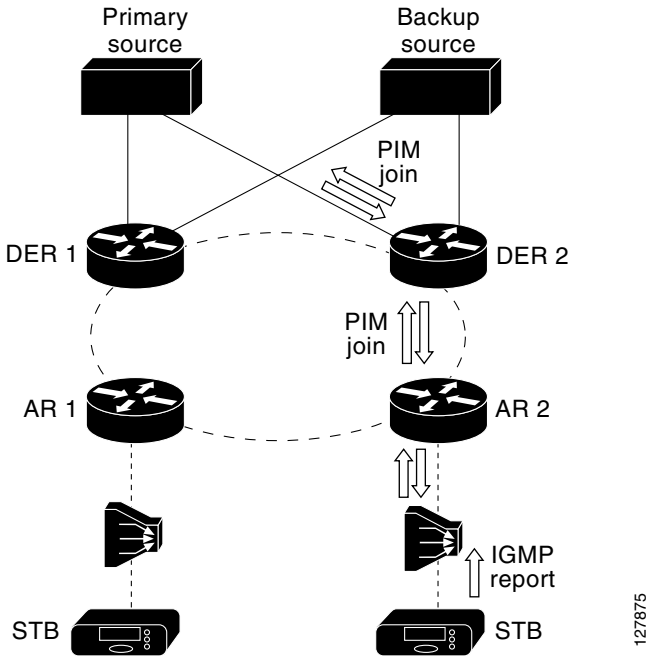
Each aggregation switch (AS) is responsible for replicating multicast streams from the distribution network to aggregation ports that have subscribers joined to them. As shown in Figure 3-3, there are two potential sources inserting video into the distribution network. These are DER 1 and DER 2. Because either of these two sources may be used to send multicast traffic onto the ring, each aggregation switch must send IGMP joins up both of the uplinks. This IGMP behavior makes it very difficult for the Layer 2 switches to determine when and when not to replicate multicast traffic on the distribution ring. To make multicast work properly in this type of environment, each port on each switch must be configured to replicate packets dynamically by using IGMP or statically. Ports that are configured to replicate dynamically send the traffic associated with a multicast group only if there has been an IGMP join issued for that multicast group. Ports that are configured to replicate statically send all multicast traffic all the time, independently of whether an IGMP join has been issued. In the case of Figure 3-3, each upstream

port on each switch must be configured for static replication, because the downstream multicast traffic could potentially flow from either direction on the ring. This configuration results in additional complexity when multicast is configured on redundant topologies.

In addition to being more complex to configure in a redundant topology, multicast is less efficient. This is because multicast streams must be sent everywhere in the Layer 2 ring, independently of where an IGMP join was issued. Figure 3-3 on page 3-7 illustrates an example multicast replication in a Layer 2 environment. Here the subscriber has issued a channel-change request from the STB attached to AR 2. The channel-change request results in an IGMP join message being propagated in both directions of the distribution network to both DER 1 and DER 2. DER 2 has been elected as the designated router, so it translates the IGMP join into a PIM join, while DER 1 ignores the IGMP join request. As a result of the IGMP join, DER 2 sends the multicast stream to the ring. Because AS 2 is using IGMP snooping on the downstream link, it is the only switch that replicates the stream to the DSLAM. Note, however, that the multicast traffic gets propagated all the way through the Layer 2 ring to DER 1. Each switch must replicate the traffic to other switches on the ring, because it is very difficult to determine where to send the multicast traffic on the ring based on IGMP snooping alone. DER 1 drops the multicast traffic when it receives it, because it does not have any "downstream" requestors for the stream. The result of using Layer 2 in the distribution network is that bandwidth is wasted on the distribution ring, because the multicast stream must be sent everywhere—independently of which nodes on the ring have asked for the traffic.

Figure 3-4 illustrates multicast operation and traffic flow when a Layer 3 distribution network is used for video. Here all nodes in the redundant topology are in the same Layer 3 topology. This results in simpler configuration as well as a more efficient traffic flow pattern. IP multicast is inherently different from Layer 2 forms of replication, because the multicast tree is built from PIM messages that are routed from the edge of the IP network to the source by means of reverse-path routing. Reverse-path routing is essentially the same as destination-based routing, except that the path to the source is looked up on the basis of the IP source address. This figure illustrates how the PIM messages are routed to the source and how the multicast distribution tree is built more efficiently as a result.

Figure 3-4 Multicast Traffic Flow with Layer 3 Distribution



In this figure, the subscriber has again issued a channel-change request from the STB attached to AR 2. The request results in an IGMP join message being sent to DER 2. Release 1.1 of the solution uses Source Specific Multicast (SSM), along with SSM mapping, as the IP multicast technology for the broadcast video service. As a result, AR 2 can translate the IGMP join request into the IP address of the encoder that is being used to generate that stream. With the IP source address, AR 2 uses reverse-path routing to decide where to send an PIM message. In this case, the shortest path to the primary source is through DER 2.

Once PIM state is established, DER 2 replicates the multicast stream to AR 2, which in turn sends the multicast stream to the DSLAM and the STB. Note that the multicast stream is not replicated throughout the distribution ring as it was in the Layer 2 scenario. This is because reverse-path route lookup results in a multicast tree that is built from the source directly to the nodes that requested the traffic. The result of using Layer 3 in the distribution network is an IP multicast environment that is simpler to configuration and more efficient in bandwidth use than are Layer 2 environments.

AR-Based Layer 3 Edge

When the AR is configured as the Layer 3 edge for video, the network is typically configured so that the AR is located at a different point in the network than the Layer 3 edge for Internet access services. This type of configuration may be considered not as architecturally “clean” as having the Layer 3 edge for all services located at the same point in the network. However, as described below, these issues are far outweighed by the benefits of using a Layer 3 distribution network for video services. Release 1.1 of the solution uses an AR-based Layer 3 edge to take advantage of these benefits.

Note that the AR may not be the node that directly aggregates the GE uplinks from DSLAMs. The AR is defined as the first node in the physical topology that aggregates enough subscribers that either path or node redundancy is required for video services. In a ring topology, the AR is defined as the node that connects the ring to a nonredundant hub-and-spoke aggregation architecture. In a hub-and-spoke topology, the AR is defined as the first node that includes redundant uplinks to the distribution network. In topologies where the AR does not terminate the GE uplinks from DSLAMs, there may be a Layer 2 aggregation network between the DSLAMs and the AR that does not include either path or node redundancy. Layer 2 Aggregation Alternatives, page 3-14, provides details on Layer 2 aggregation schemes that may be used between DSLAMs and the AR.

The sections below provide details on some of the benefits that make the AR the best choice as the Layer 3 edge in a video topology.

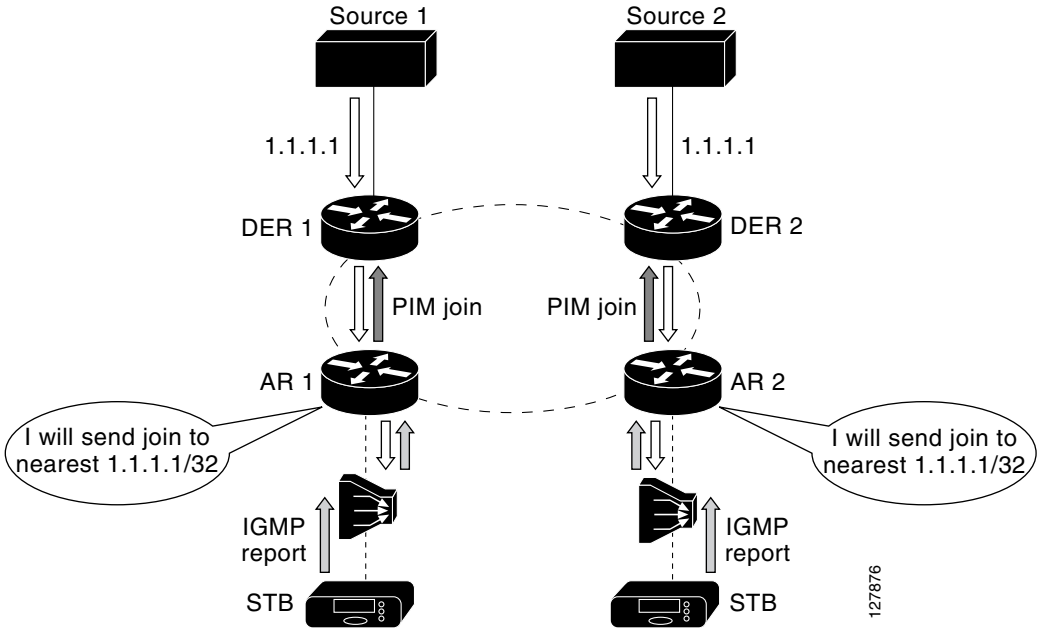
Benefit: Source-Specific Multicast

When the AR is configured as the Layer 3 edge for video services, the distribution network can take advantage of IP multicast features such as Source Specific Multicast (SSM). SSM is a technology that enables the network to build a separate distribution tree for each multicast source. SSM simplifies the operational complexity of configuring a multicast network, because it does not require the configuration of a rendezvous point (RP) to allow multicast forwarding as non-source-specific multicast technologies do. In addition, SSM only creates a multicast distribution tree to a specific multicast source address. SSM is considered more secure than non-source-specific multicast, because the multicast client must know both the multicast destination address and the multicast source address in order to join the multicast group. To create a source-specific multicast tree, SSM relies on IGMPv3 signaling from multicast hosts. IGMPv3 includes the multicast source address in the multicast join request. Because current-generation STBs do not support IGMPv3 signaling, the AR can be configured to map IGMPv2 requests received from the aggregation network to PIM SSM (S, G) (source, group) messages in the distribution network. This translation process maps the multicast destination address specified by the STBs in IGMP messages to a combination of multicast source and destination addresses in PIM messages. Release 1.1 of the solution uses SSM mapping at the AR to provide SSM support for STBs that do not support IGMPv3.

Benefit: Anycast Support

When the AR is configured as the Layer 3 edge for video, the distribution network can take advantage of "anycast" support for either the load balancing or the fast failover of video encoders. IP multicast technology natively supports the ability for "anycasting" of IP multicast sources. With anycasting, one configures two or more multicast sources that are sending to the same IP multicast group (with the same multicast destination address) and have the same IP source address. When used with PIM sparse mode, IP multicast technology uses a reverse path lookup to determine which IP source is closest to any particular PIM edge node. The result is that the replication path for a single multicast group can consist of a separate multicast tree for each broadcast encoder. Figure 3-5 illustrates the use of anycasting for load sharing between multiple video encoders.

Figure 3-5 Anycast-Based Load Sharing between Video Encoders

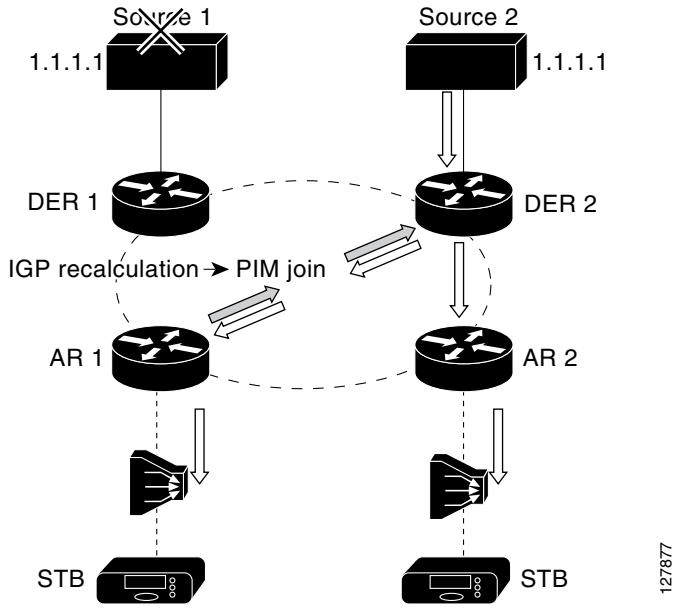


Note that the ability to instantiate multiple multicast replication trees for the same multicast destination is not possible when Layer 2 switching is used. Because each node in a Layer 2 network simply uses IGMP snooping to determine when to replicate packets, anycasting in a Layer 2 domain would result in having the stream from each multicast source replicated to all multicast destinations. Because of this, anycasting is applicable only within the context of a Layer 3 switching environment.

Benefit: Fast Failover of Video Encoders

In addition to supporting load sharing among multicast sources, anycasting can be used to support the fast failover of video encoders. When anycasting technology is combined with the ability of the network to detect the failure of an encoder, routing protocols reconverge. This reconvergence results in the reverse path from the ARs to the DER being recalculated to take into account that the location of the multicast source that has been changed. The IP reconvergence then triggers PIM to resend a join request along the path to the new multicast source. Figure 3-6 on page 3-11 illustrates the use of anycast technology to implement the fast failover of redundant video broadcast sources. Release 1.1 of the solution uses this technology to implement fast failover between redundant broadcast encoders.

Figure 3-6 Fast Multicast Source Failover Using Anycast



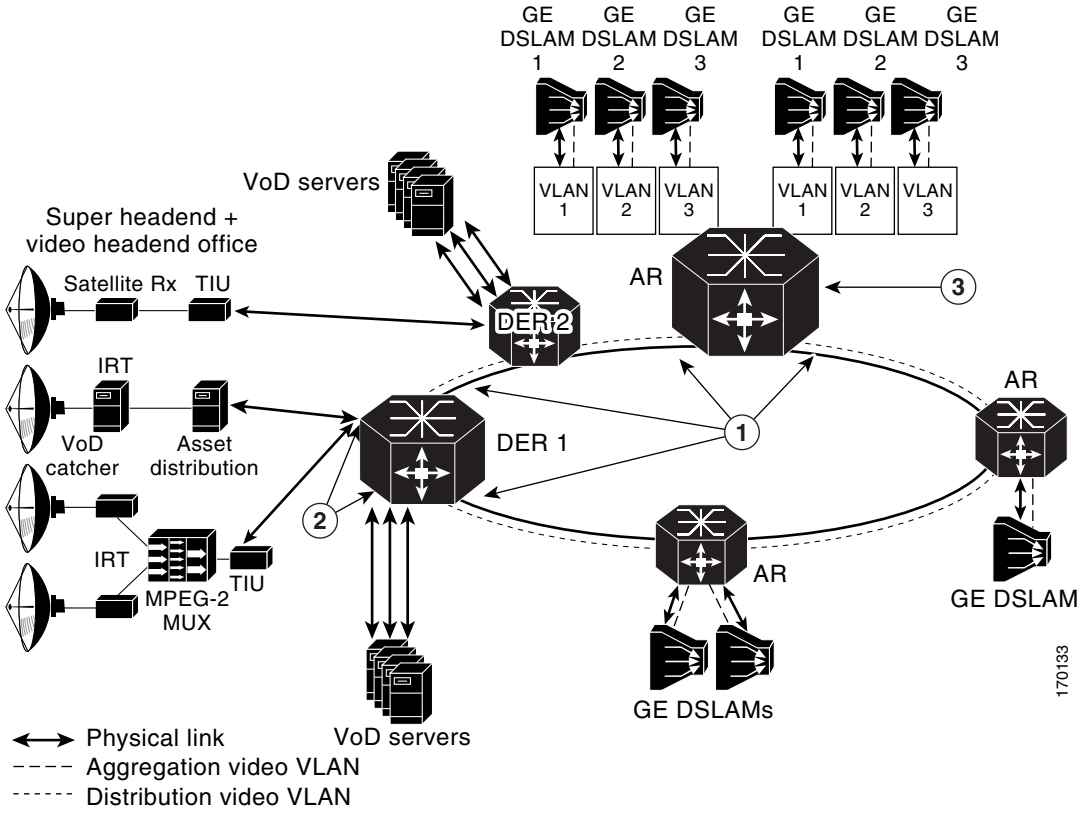
Benefit: Asymmetric Networking

Finally, when the AR is configured as the Layer 3 edge for video, the distribution network can be configured to support asymmetric bandwidth for video services in the distribution network. The traffic pattern associated with broadcast video and VoD services is extremely asymmetric. Each video channel or session requires multiple megabits of bandwidth in the downstream direction, while the upstream traffic is limited to control signaling for the service. Asymmetric networking allows the network to be configured for more bandwidth in the downstream direction than in the upstream direction. This reduces the cost of the transport network, because it allows the network provider to take advantage of optical components such as wavelength division multiplexing (WDM) transponders and other optical equipment that can be deployed in a unidirectional manner.

Video Forwarding Architecture

Once the choice is made to position the Layer 3 edge for video at the AR, the aggregation/distribution forwarding configuration becomes fairly straightforward. The service mapping architecture used in the solution results in the GE link from each DSLAM being configured for three separate 802.1q VLANs to aggregate Internet access, voice, and video services. Figure 3-7 on page 3-12 illustrates the overall video forwarding architecture discussed in this section.

Figure 3-7 Video Forwarding Architecture



1	Video SVI or MPLS interfaces
2	Video interfaces
3	Loopback interface

AR Configuration

The AR has a set of interfaces connecting to the distribution network and a set of aggregation interfaces connecting to DSLAMs. The AR is configured to switch packets between the distribution and aggregation interfaces at Layer 3. Separate VLANs are configured for each service on the downstream interfaces connected to the DSLAMs. The video configuration of the upstream interface depends on whether the Layer 2 backhaul technology used for Internet access is based on native Ethernet or EoMPLS aggregation. (For details on native Ethernet and EoMPLS configurations for Internet access, see Internet Access Forwarding, page 3-28.)

When native Ethernet aggregation is used for Internet access service, each upstream port connected to the distribution network is configured to use 802.1q encapsulation (VLAN trunking) and includes separate VLANs for transport services (Internet access) and managed application services (voice and video). The video VLAN of each upstream and downstream port is terminated in a separate Layer 3 switched virtual interface (SVI). This configuration causes video coming in on any physical port to be switched at Layer 3 to any other physical port.

Note The VLAN IDs used for video on each of the physical upstream ports must be different from the VLAN IDs configured on the downstream ports connected to the aggregation links.

When EoMPLS technology is used for Layer 2 backhaul of the Internet access service, the MPLS tags associated with the EoMPLS tunnels can be used to distinguish between the Internet access service and managed application services such as voice and video. This can be used to simplify the configuration of the distribution network, by (1) configuring a single IP interface for each physical port in the distribution network, and (2) restricting MPLS label distribution only to routes associated with the EoMPLS tunnel endpoints (which are configured as loopback interfaces on the aggregation and distribution edge routers). In this configuration, each distribution port is configured as a Layer 3 routed port on which MPLS tag encapsulation is enabled. Because MPLS label distribution is restricted only to routes pointing to the EoMPLS tunnel endpoints, all traffic associated with managed services such as voice and video remains IP encapsulated.

In the downstream direction, the AR terminates the video VLAN of each GE link from each connected DSLAM in a separate SVI. Each SVI is configured as IP unnumbered, so each SVI obtains its IP address from a loopback interface. Because all of the SVIs obtain their IP addresses from a common configured loopback interface, all of the video SVIs associated with downstream ports can share the same IP subnet. This makes dynamic IP address assignment for the STBs that are aggregated by the AR simpler and more efficient, because the STBs can all share the same IP address pool in a dynamic address server (such as a DHCP server).

DER Configuration

The downstream ports of the DER are configured identically to the upstream ports of the AR. (Refer to Figure 3-7 on page 3-12.) Depending on whether Layer 2 Ethernet or EoMPLS aggregation is used for the Internet access service, the video stream is terminated, respectively, in either an SVI bound to a Layer 2 VLAN, or a Layer 3 routed interface bound to the physical port. (For details of the configuration of the upstream ports of the AR, see AR Configuration, page 3-12.)

Note One difference between the AR and DER is that different services may be aggregated by different DERs. This allows the different services to be aggregated at different sites if necessary.

In the solution, video components such as video servers and real-time encoders are connected to redundant DERs. A load-sharing scheme provides video redundancy. This means that the VoD servers and broadcast video encoders connected to each of these routers are actively sending video during normal operation. Ports connecting video components to a DER may be configured at either physical Layer 3 switched ports or Layer 2 ports terminated in an SVI. To simplify address management, ports connecting VoD servers and real-time encoders may all be configured to be in the same Layer 2 VLAN, which is terminated in a single SVI.

IP Routing

To enable dynamic routing specific to video, a routing process is configured on the ARs and DERs. This routing process is configured only on the video SVI interfaces. This enables the video topology to converge at Layer 3 independently of the topologies for the voice and Internet access services.

Note Solution testing used Open Shortest Path First (OSPF) as the routing protocol for video.

Layer 2 Aggregation Alternatives

While the AR may be directly connected to the GE uplinks of the DSLAMs it aggregates, there may be network topologies with insufficient subscriber density to warrant having DSLAMs directly connected to an aggregation router. In these types of topologies, there may be a Layer 2 aggregation network between the DSLAM and the AR.

Note While this section describes an architecture that may be used for Layer 2 aggregation between DSLAMs and ARs, the solution test topologies described in Release 1.1 Configurations, page 3-36, do not include Layer 2 aggregation as part of the test topology.

The solution transport architecture specifies that the AR is where the Layer 3 edge for video should be. The transport architecture also specifies that the AR is defined as the first node in the physical topology that aggregates enough subscribers to require either path or node redundancy for video services. Given these transport requirements, it is important that the Layer 2 aggregation network between DSLAMs and the AR does not include either path or node redundancy. One way to identify such an aggregation network is that it does not require spanning tree algorithms to be configured in order to avoid bridging loops.

When a Layer 2 aggregation network is used between DSLAMs and the AR, it is also important that the number of subscribers aggregated at a single AR not cause forwarding table or ARP table scalability issues for the AR. (For some of the issues associated with forwarding and ARP table scalability, see Issue: Scaling for the Layer 2 MAC Table and Layer 3 Forwarding Table, page 3-6.) A general rule that can be used in network design to avoid scalability issues in the AR is that no more than 30,000 subscribers should be aggregated in a single AR.

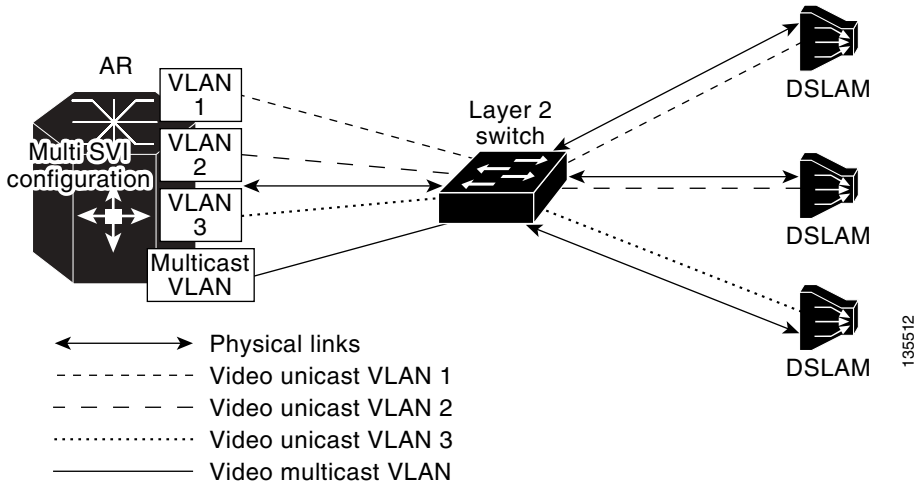
The Layer 2 aggregation design described in this section prevents security issues in the DSL aggregation network that are associated with the flooding used in standard bridge-learning algorithms. To simplify the requirements of the aggregation switches, this design assumes that the switches support only standard bridge-learning algorithms, and do not support controlled flooding algorithms that prevent upstream packets from being flooded on down stream links. This design also assumes that aggregation switches are capable of segregating MAC broadcast domains through 802.1q VLAN tagging.

Under the above design assumptions, the Layer 2 aggregation design uses a separate VLAN ID per service per DSLAM. The use of a separate VLAN ID per service per DSLAM means that all MAC layer flooding on the aggregation switch is constrained to a single DSLAM per service. This prevents the security issues associated with MAC layer flooding, but it also means that separate copies of video broadcast channels must be sent to each VLAN—resulting in bandwidth being wasted on the link between the aggregation switch and aggregation router. To prevent multiple copies of video being sent on the link between the aggregation switch and the aggregation router, the Layer 2 aggregation design uses a separate multicast VLAN on which all multicast video traffic is sent. The multicast VLAN carries all broadcast video traffic between the aggregation router and the aggregation switch. The use of a separate multicast VLAN means that the aggregation switch that supports Layer 2 aggregation **must** be capable of performing IGMP snooping and replication between the single upstream multicast VLAN and the video VLAN on each downstream link. Cisco switches support a feature called Multicast VLAN Registration (MVR) to implement this function.

When the aggregation router is configured to use a Layer 2 aggregation network, the multi-SVI configuration described in AR Configuration, page 3-12, for the downstream aggregation links must be used. In addition to this SVI configuration, the AR must have one additional SVI configured for the multicast VLAN. This VLAN has the IP multicast features described in Multicast Configuration Options, page 3-23, configured on it.

Figure 3-8 on page 3-15 illustrates aggregation at Layer 2.

Figure 3-8 Layer 2 Aggregation



Multicast

This section presents the following topics related to multicast:

- Overview
- Multicast Admission Control
- Effect of Multicast on Channel-Change Performance
- Multicast Configuration Options

Overview

A major component of the transport architecture is the multicast transport architecture for video. As stated previously, a Layer 3 forwarding architecture for video is used between the DER and the AR. The video topology is separated from the voice and Internet access topologies by means of a separate VLAN for video. This VLAN carries both unicast VoD streams as well as multicast broadcast-video streams.

PIM for multicast is enabled on the video VLAN interfaces on the DERs and ARs, along with OSPF. This enables a video-specific multicast topology to be built. PIM sparse mode is used for the broadcast video service.

The IGMP/PIM boundary for multicast occurs at the SVIs on the AR that are associated with the GE ports from the DSLAMs. IGMP joins are translated to PIM joins at the SVI.

Source Specific Multicast (SSM) is used in the Layer 3 network. SSM simplifies the operational complexity of configuring a multicast network, because it does not require the configuration of a rendezvous point (RP) to allow multicast forwarding as non-source-specific multicast technologies do. In addition, SSM only creates a multicast distribution tree to a specific multicast source address. SSM is considered more secure than non-source-specific multicast, because the multicast client must know not only the multicast destination address, but also the multicast source address, in order to join the multicast group.

Because SSM builds multicast replication trees that are specific to the IP address of the multicast source, there is an implicit requirement that all multicast join requests (IGMP/PIM joins) must include the address (or addresses) of the multicast source (or sources) in the request. While video STB applications could learn both the multicast source and destination address for each broadcast video channel through the electronic program guide (EPG), current-generation applications receive only the multicast destination address from the EPG. As a result, these applications send IGMPv2 join requests that contain only the destination multicast address in the request. The solution works around this by translating IGMPv2 requests that contain only the destination multicast address into SSM PIM join requests that contain both the multicast source and destination address at the AR. The ability to map the multicast destination address contained in IGMPv2 requests to a source/destination pair is called SSM mapping. To map between multicast destination addresses and source/destination pairs, SSM mapping can be configured to use either statically configured maps on each AR, or the services of a Domain Name System (DNS) server that contains a single map for all ARs. The solution uses the DNS-based approach to simplify the administration of this map.

Figure 3-9 on page 3-17 illustrates the multicast features used in the solution with the aggregation and distribution networks.

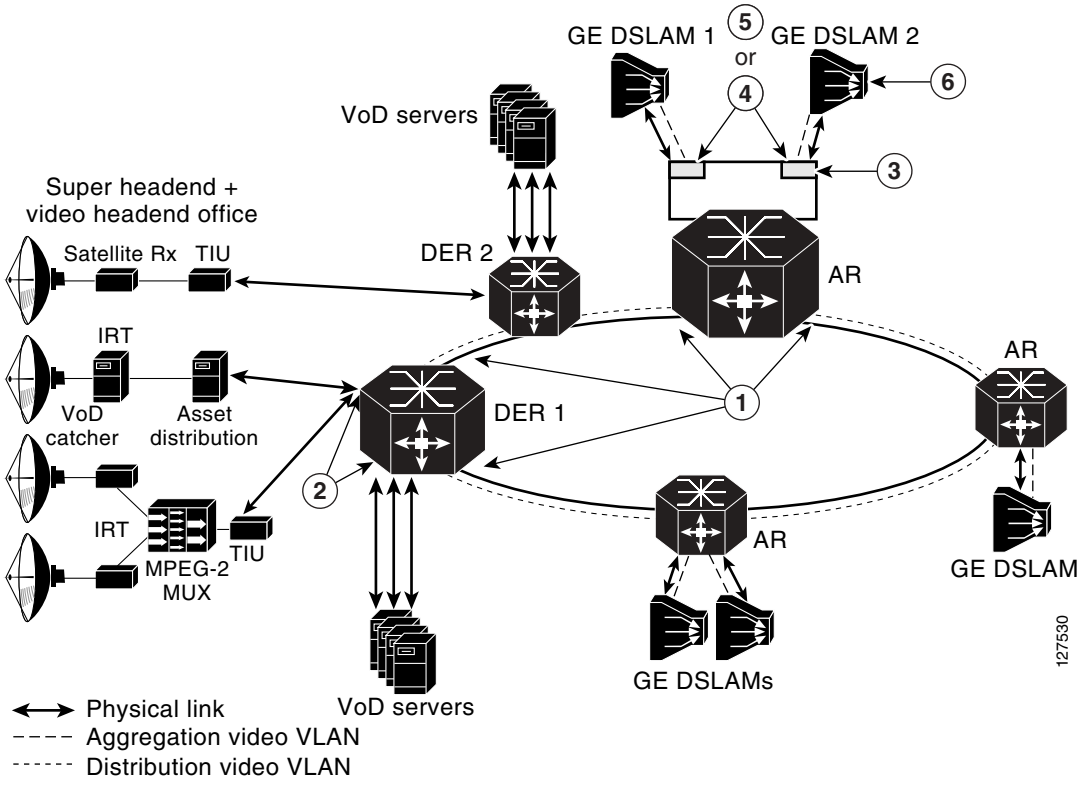
Multicast Admission Control

The Release 1.1 architectural design supports the ability to perform a network-based connection admission control (CAC) function for the broadcast video service. In some broadcast video deployments, it may not be reasonable to support the transmission of all of the broadcast channels offered by the video service on the links between the AR and DSLAMs at the same time. For example, a broadcast video service may offer 150 standard-definition channels and 20 channels of high-definition television. If the channels are encoded by means of MPEG-2, the bandwidth required to support the transmission of all channels simultaneously is 862 Mbps. To ensure that there is no congestion in the queue used for the broadcast video service, bandwidth must be reserved on the GE aggregation links to the DSLAMs. This can be done by simply subtracting the bandwidth used for broadcast video from the bandwidth pools used by the application components of the other services (such as voice and VoD) that require guaranteed bandwidth. In the example above, if the amount of bandwidth that was reserved for broadcast video was based on supporting all channels simultaneously, only 138 Mbps of bandwidth would be available for voice and VoD. This is not enough bandwidth to implement a reasonable VoD service.

The amount of bandwidth reserved for broadcast video can by controlled by implementing an admission control function for that service. This can be implemented by limiting the number of broadcast streams that are replicated on a particular link. Because the GE aggregation links between the AR and the DSLAM are typically the most likely links to be oversubscribed, they are the best place to enforce a stream limit. When stream limits are used for broadcast video, there is a probability that an IGMP join sent by the broadcast video client application as a result of a channel-change request will fail. Because IGMP signaling has no acknowledgement associated with it, there is no explicit failure indication associated with a failed IGMP join request. Instead, a failed IGMP join request simply results in the requested MPEG stream not being delivered to the STB. The subscriber sees a blank picture as the result of a failed channel-change request. While this user interface is nonoptimal, it is consistent with what video subscribers currently experience when a broadcast channel is not available for some reason.

When a CAC function is used for broadcast video, it is important that the service provider sets the stream limit high enough that subscribers very seldom experience failures as a result of a channel-change request. This can be done by using statistical analysis methods such as Erlang analysis. The statistical analysis described in Static IP Multicast Joins on the AR, page 3-26, is an example of the type of analysis that can be used to determine what the stream limit should be set to in order to ensure a low blocking factor for a group of broadcast channels.

Figure 3-9 Multicast Forwarding Architecture



1	Video subinterface with SSM multicast forwarding, PIM sparse mode
2	Video interface with SSM multicast forwarding, PIM sparse mode
3	DNS-based SSM mapping, static multicast group
4	IGMP snooping or static IGMP join
5	IGMP snooping with report suppression
6	IGMP fast-leave processing

In the solution, the AR can enforce a maximum broadcast bandwidth limit limiting the number of IGMP joins on the ranges of multicast addresses associated with broadcast video to a configured maximum on the aggregation links that the router controls. This is done by means of the **ip igmp limit** command. The mapping of video channels to multicast addresses can be done in such a way that the AR can associate the bandwidth for different classes of video (standard definition, high definition, and so on) with different ranges of multicast addresses. IGMP join limits can then be set for each range of multicast addresses.

Caution The **ip igmp limit** command on an AR can be used only when that AR is not performing SSM mapping. For details, see *Release Notes for Cisco Wireline Video/IPTV Solution, Release 1.1.*

For example, a service provider may choose to exclude some video channels from the video CAC function and instead reserve bandwidth for all of the channels that are excluded from that function. This configuration may be useful for managing popular channels that the service provider wants to ensure are never blocked. These channels can be excluded from the CAC function by simply not associating an IGMP limit with their multicast addresses.

When the **ip igmp limit** command is configured on an AR, that router can enforce a maximum broadcast-bandwidth limit by limiting the number of IGMP joins on the ranges of multicast addresses associated with broadcast video to a configured maximum on the aggregation links that the router controls. The mapping of video channels to multicast addresses can be done in such a way that the AR can associate the bandwidth for different classes of video (standard definition, high definition, and so on) with different ranges of multicast addresses. IGMP join limits can then be set for each range of multicast addresses. For example, a service provider may choose to exclude some video channels from the video CAC function and instead reserve bandwidth for all of the channels that are excluded from that function. This configuration may be useful for managing popular channels that the service provider wants to ensure are never blocked. These channels can be excluded from the CAC function by simply not associating an IGMP limit with their multicast addresses.

Effect of Multicast on Channel-Change Performance

One of the important aspects of a broadcast video service that this solution characterizes is the effect of multicast join and leave latency on channel-change performance. This section documents the multicast configurations that testing has evaluated, and makes recommendations that achieve the following design goals:

- Efficiency in bandwidth use
- Scalability to large numbers of subscribers
- Minimal impact on channel-change performance

Table 3-3 on page 3-19 illustrates the major components of channel-change latency. Note that the largest factor in the channel-change delay is the I-frame delay associated with the video decoder. (The I-frame is a keyframe used in MPEG video compression.) As the table indicates, multicast performance should not have a significant effect on channel-change delay.

Table 3-3 Major Components of Channel-Change Latency

Channel-Change Latency Factor	Typical Latency, msec
Multicast leave for old channel	50
Delay for multicast stream to stop	150 [1]
Multicast join for new channel	50–300
Jitter buffer fill	200
Conditional access delay[2]	200–600
I-frame delay	500–1000

1. Assumes that the DSLAM implements IGMP fast-leave processing.
2. The conditional access delay is applicable to broadcast channels that are encrypted by means of a conditional access system (CAS) that modifies decryption keys periodically and carries updated decryption keys in-band in the video stream. The STB must wait for the latest set of decryption keys to be delivered in the video stream before it can perform any decoding. The amount of time associated with this delay depends on how often the CAS sends updated decryption information in the video stream.

Analysis of Multicast Bandwidth vs. Delay

The best approach to use for an IGMP/multicast configuration is based on a tradeoff between bandwidth and delay. IP multicast natively supports the ability to perform replication on a stream only when that stream is requested by a downstream device. While IP multicast and IGMP natively support dynamic replication, each can be configured always to replicate multicast data for a particular channel or channel group to any node in the network. When a channel or channel group is always replicated from the source to a particular node, that node is said to be configured for static joins of the channel or channel group. The benefit of configuring static joins at a particular node is that no channel-change latency is associated with dynamic signaling and replication from the source to the node on which static joins are configured. The down side of configuring static joins at a node is that the video streams for the channels that are statically joined are always sent whether a subscriber is watching them or not.

Statistical analysis can be used to determine when the benefits of static joins (less channel-change latency) outweigh the costs (additional bandwidth usage). This section describes the statistical analysis that was done as part of the solution to determine the recommendations for where in the network static joins should and should not be configured.

The behavior of a population of subscribers can be modeled statistically to determine, for a population of subscribers, the probability of at least one subscriber in the group being tuned to a set of television channels. If the probability of at least one subscriber being tuned to each of the channels in a broadcast channel group is fairly high, then the amount of bandwidth that is saved by performing dynamic joins on that group of channels is statistically insignificant. When statistical analysis shows insignificant bandwidth savings for a group of channels, static joins can be used on those channels without having a significant impact on the amount of bandwidth on the GE aggregation links.

The factors used in this analysis included the following:

- The number of subscribers in a video broadcast population
- The number of channels in the broadcast channel group
- The popularity of each channel in this broadcast group

The number of video subscribers served by a particular node depends on where that node is located in the network. Based on common expected video service take rates, the number of subscribers served by a DSLAM is typically about 500 while the number of subscribers served by an AR is typically about 5000.

The following is a statistical analysis model that is helpful in determining when to use dynamic joins, and when to use static joins.

Analysis of Dynamic Joins in a Video over IP Environment

Each subscriber is modeled as a random process selecting a channel to watch according to a given probability distribution across all possible channels. Given a group of channels, we would like to calculate the average number of channels in use, given the "popularity" probabilities of the channels. Because we are interested in determining the average number of channels in use, we can consider the channels to be probabilistically independent of each other and consider the channels one at a time.

For a single channel, the probability that this channel is idle is calculated as follows:

Let

p = P{a subscriber tunes to this channel}

N = number of subscribers subtended by the given AR or DSLAM

so that

P{channel is idle} = $(1-p)^N$

For multiple channels, we sum the above expression.

Let

C = number of channels

p_k = P{a subscriber tunes to k^{th} channel}

so that the average number of channels in use, C_{IU}, is

$$C_{IU}=\sum_{k=1}^{C}[1-(1-p_k)^N]$$

Channel-Change Latency Probabilities

When subscribers change channels, if they change to a channel that is not part of a static join and that no one else is watching, they experience some latency while the dynamic join is established before they can view the channel's content.

We assume that when there is a channel-change event, the probability a particular channel is changed to is proportional to that channel's popularity. This assumption can be combined with the above calculated P{channel is idle} and the knowledge of which channels are associated with static or dynamic joins to determine the probability that a given channel change results in the latency associated with establishing a dynamic join.

Let

D = the set of all channels involved in dynamic joins

P_L = P{a channel change experiences latency due to a newly created dynamic join}

so that

$$P_L = \frac{\sum_{k \in D} p_k (1-p_k)^N}{\sum_{k=1}^{C} p_k}$$

Analysis

Given a set of channels with probabilities p_k, they can be ranked from highest to lowest p_k. Then, once they are ranked, we can have a cutoff value so that channels with higher p_k get a static join and those with lower p_k get a dynamic join. The questions then are, for a given cutoff,

- What is the bandwidth use (relative to the all static-join case)?
- What is the probability of channel-change latency?

As an example, consider a 150-channel system with an exponential decay function for

P{subscriber tunes to k^{th} channel}

Figure 3-10 graphs the channel popularity for this example.

Figure 3-10 Channel Popularity for a 150-Channel System

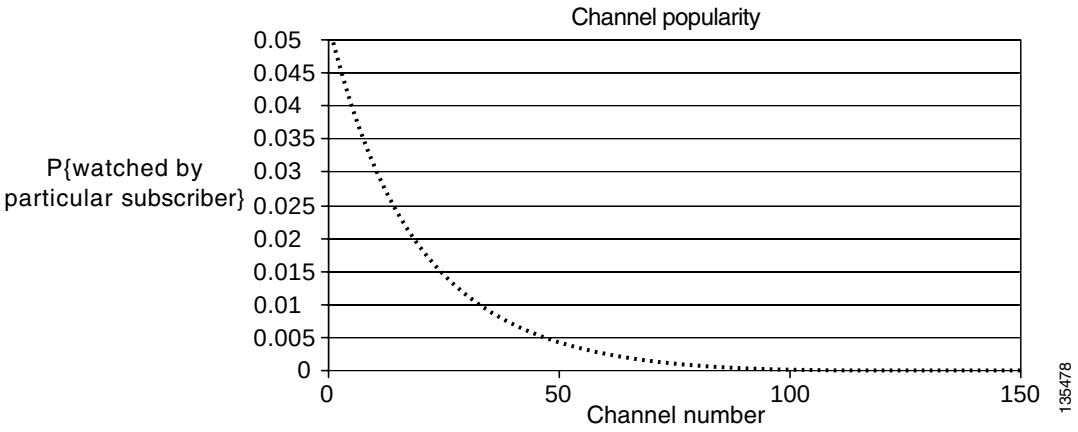
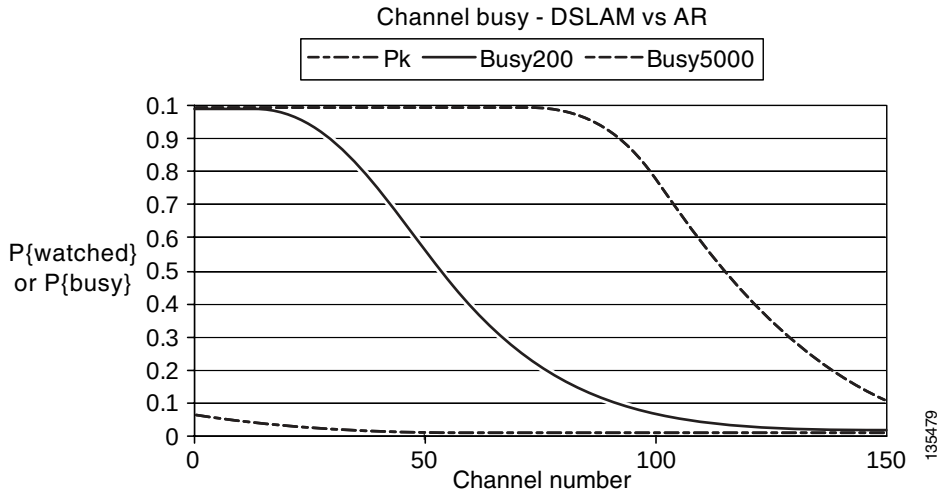


Figure 3-11 add curves showing the probability that a given channel is busy for subscriber bases of 200 (at a DSLAM) or 5000 (at an AR).

Figure 3-11 Probability a Given Channel is Busy for Subscriber Bases of 200 (at a DSLAM) or 50000 (at an AR)



The important thing to note here is that the *P*{busy} curve shifts dramatically to the right when the number of subscribers is increased from 200 to 5000.

Figure 3-12 and Figure 3-13 on page 3-23 show the tradeoff between average bandwidth requirements and channel-change latency probability for a DSLAM and an AR, respectively. The horizontal axis is the fraction of channels moved from a static join to a dynamic join. The two curves show the bandwidth required (as a percentage of bandwidth required in the static join case) and the probability of channel-change latency. (The two curves in each figure are shown on different scales to make them both visible.)

Figure 3-12 Tradeoff Between Average Bandwidth Requirements and Channel-Change Latency Probability for a DSLAM (200 Subscribers)

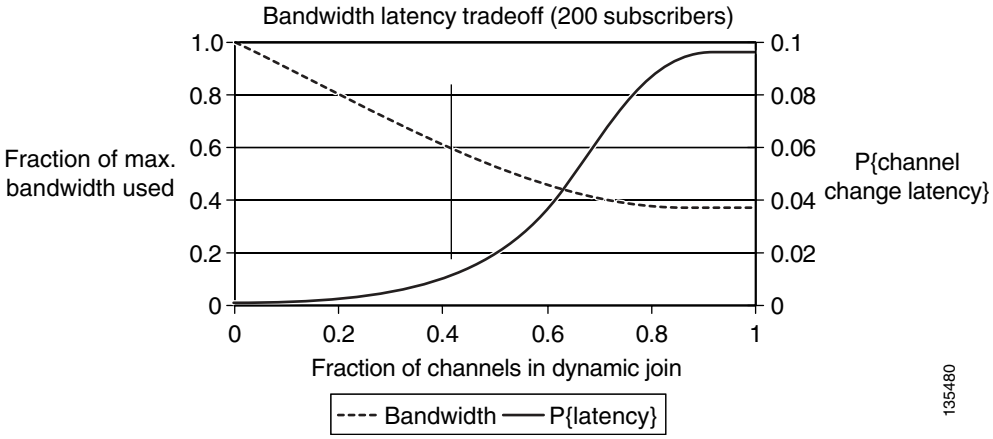


Figure 3-13 Tradeoff Between Average Bandwidth Requirements and Channel-Change Latency Probability for an AR (5000 Subscribers)

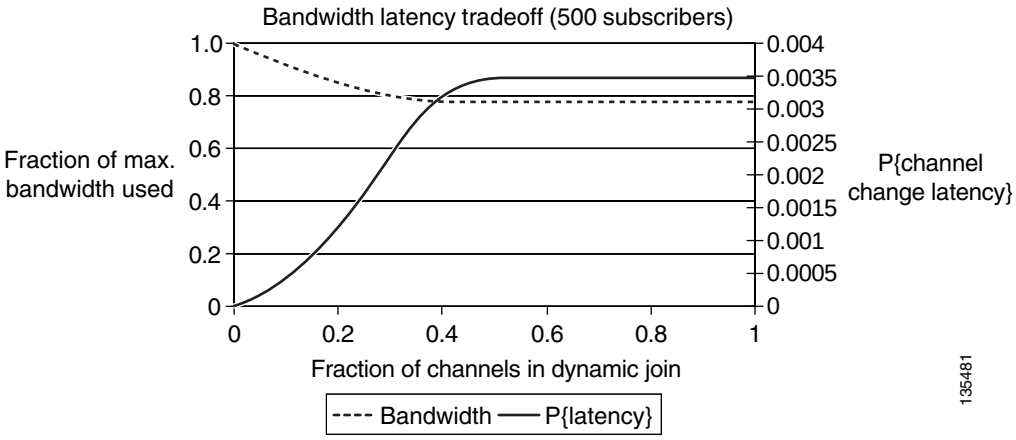


Figure 3-12 shows the tradeoff for the DSLAM (200 subscribers). There seems to be substantial opportunity in using dynamic joins where about half the bandwidth can be saved with a channel-change latency probability of about 1 in 50 (0.02). (See the vertical black line in the graph.)

Figure 3-13 shows the tradeoff for the AR (5000 subscribers). In this case, the best possible bandwidth savings is about 20%, even with all channels in dynamic joins. Here the channel-change latency probability is uniformly low, with a maximum value of about 1 in 300.

From the statistical analysis results described above, you can see that there is a typically a significant bandwidth savings to be gained (~60%) by using dynamic joins at the DSLAM. Because of this, we recommend that the multicast configuration models used on the links between the AR and the DSLAM take advantage of the dynamic replication capabilities native to IP multicast. Also from these results, it can be seen that the benefit of using dynamic vs. static joins at the AR depends heavily on the popularity of a channel or channel group. It may be best to join popular channels statically, and join less-popular channels dynamically. Static IP Multicast Joins on the AR, page 3-26, describes additional analysis that was performed to determine when it is best to perform static vs. dynamic joins of a channel group on the AR.

Multicast Configuration Options

From the above analysis, the solution architecture assumes that multicast traffic is replicated by means of dynamic Internet Group Management Protocol (IGMP) signaling on the GE aggregation links between ARs and DSLAMs, and also on the DSL access links between the DSLAM and HAG. The following sections detail the multicast configuration options included in the solution.

IGMP-Based Replication in the DSLAM

Because the DSLAM performs packet switching at Layer 2, it must use a Layer 2 method of implementing multicast replication based on dynamic signaling. In the transport architecture, the DSLAM performs multicast replication by means of IGMP snooping. A Layer 2 switching node that implements IGMP snooping uses the IGMP state machine to determine when to perform multicast replication to a particular link.

Transparent IGMP Snooping vs. IGMP Proxy-Routing Functionality

Note that the recommendation for the transport architecture is to use transparent IGMP snooping and not an IGMP proxy function. IGMP snooping, as defined in the DSL Forum WT-101 specification, is a function whereby the DSLAM uses IGMP messages and the associated IGMP state machine to determine when to perform replication of an incoming multicast stream on outgoing DSL lines. When transparent IGMP snooping is used, the DSLAM appears totally transparent to the IGMP signaling path. It does not modify IGMP messages in either the upstream or downstream directions. WT-101 defines IGMP proxy-routing as a function whereby the DSLAM acts as an IGMP router to STBs, and as a host to upstream routers. With an IGMP proxy-routing function, the DSLAM can statically join multicast streams coming from the AR and replicate them on demand, based on IGMP messages coming from the STBs.

IGMP proxy-routing functionality is not recommended on the DSLAM for a couple of reasons. First, the IGMP proxy-routing function complicates both the operation and configuration of IGMP signaling. This is because the signaling path is now split into two separate IGMP sessions between the STB and the AR. Second, the main benefit of an IGMP proxy function is to allow the DSLAM to join multicast groups statically from the AR and perform dynamic replication to the DSL line. As shown from the analysis in Analysis of Multicast Bandwidth vs. Delay, page 3-19, the benefits of statically joining broadcast channels at the DSLAM (decreased channel-change latency) are far outweighed by the cost (additional bandwidth on the GE aggregation links).

Note Some, and only some, DSLAMs support IGMP snooping with report suppression. When IGMP snooping with report suppression is configured on a DSLAM, the DSLAM forwards only the first IGMP join request for a particular multicast address on the upstream GE link. In addition, the DSLAM sends an IGMP leave request only when it sees a single DSL line currently joined to the multicast stream. This behavior reduces the number of IGMP joins and leaves that the AR must process, and some have recommend its use to provide a more scalable IGMP snooping configuration.

Cisco has load tested IGMP signaling on the Cisco 7600 series, for example, and no join or leave performance degradation was experienced with over 10,000 IGMP messages (join/leaves) per second. Thus, although the Release 1.1 multicast architecture does not require IGMP report suppression on the DSLAM, using this report suppression feature does not cause any issues with the multicast architecture.

IGMP Immediate Leave Processing

To meet the channel-change time requirements, the DSLAM must perform IGMP snooping with immediate leave processing. Immediate leave processing, as defined by WT-101, is a modification of the normal IGMP Version 2 host state machine. In IGMPv2, when a router (IGMP server) receives an IGMP leave request from a host (IGMP client), it must first send an IGMP group-specific query to learn whether other hosts on the same multi-access network are still requesting to receive traffic. If after a specific time no host replies to the query, the router stops forwarding the traffic. This query process is required because, in IGMP Versions 1 and 2, IGMP membership reports are suppressed if the same report has already been sent by another host in the network. Therefore, it is impossible for the router to know reliably how many hosts on a multi-access network are requesting to receive traffic.

The requirement of making IGMP queries and waiting for a response can be removed if there is only a single video STB per DSL line that is making IGMP requests. In this case, when an STB sends an IGMP leave request, the DSLAM can safely and immediately stop sending the multicast stream down the DSL line from which the request came. The ability for a node that supports IGMP snooping to stop sending a multicast stream immediately on the receipt of an IGMPv2 leave request is called immediate leave processing. The solution requires that DSLAMs support IGMP snooping with immediate leave processing.

However, IGMP snooping with immediate leave processing does not work when more than one STB is connected to a DSL line. The problem with immediate leave processing is that if two STBs attached to the same DSL line are tuned to the same channel, the first STB that tunes off that channel causes the DSLAM to stop sending the multicast stream for that channel. This in turn causes the second STB to stop receiving video. The workaround for this problem requires additional functionality in both the STBs and the DSLAM. STBs **must** always send IGMPv2 join and leave requests during a channel-change operation, independently of whether other STBs on the same network segment are currently joined to the same multicast group. The DSLAM **must** keep track of the IP source address associated with each IGMP join and leave request. The DSLAM stops sending a multicast stream to a particular DSL line when all of the IGMP hosts (as specified by the IP source address in each IGMP message) have issued IGMP leave requests. (In fact, these modifications to the IGMPv2 state machine are required in order to make IGMP hosts compliant with IGMPv3.)

Multicast Replication in the AR

Because the AR forms the IGMP/PIM boundary, multicast replication is triggered by IGMP messages that are received on the GE uplinks from the DSLAMs.

Because the AR potentially aggregates many subscribers, it must be capable of processing a high volume of IGMP join and leave requests if many subscribers are changing channels at the same time.

The solution testing effort characterized the performance of IGMP on the AR by flooding the AR with a constant rate of IGMP join and leave requests, in order to determine the effect on CPU performance in the AR, as well as on the network multicast join delay that contributes to the channel-change performance experienced by an STB. To determine that, an IGMP host makes an IGMP join request for a multicast address that is currently not being sent on the GE aggregation link while the AR is being flooded with IGMP join and leave requests for a different multicast address. The test measures the amount of time it takes from the time the join is sent until the time the stream is delivered, both when the AR is not busy and when it is under various IGMP load conditions.

The performance test described above will be used to provide a recommendation for the maximum number of video broadcast subscribers that should be aggregated by the aggregation router platforms that will be tested as part of the solution when they are configured to use IGMP snooping. To provide this recommendation, the results of the performance test will be first translated into a maximum number of joins / leaves that the aggregation router can process per second before significantly affecting channel change performance. An increase in IGMP join latency of 500 msec from an unloaded to a loaded condition will be considered a significant increase in this testing.

The maximum IGMP performance can be translated to a maximum number of subscribers by using a worst-case channel-change scenario. The scenario used for this recommendation is an event where a significant percentage of the subscribers viewing a popular channel tune off from that channel at the same time (within 1 second). An example of this type of event is a commercial break during a popular program. The IGMP performance required for this type of event can be determined by taking into account the total number of video subscribers, the popularity of the channel, and the percentage of subscribers that tune off that channel at the same time. The performance requirement can obtained by using the following formula:

*IGMP_Perf = Num_Subscribers * Channel_Popularity * TuneOff_Factor*

where

IGMP_Perf (IGMP performance) = Number of IGMP joins or leaves that a platform can process in 1 second

Channel_Popularity = Percentage of total subscribers tuned to a popular channel.

TuneOff_Factor = Percentage of subscribers that tune off the channel at the same time. (Solution worst-case assumption is 50%.)

In deployments where performance testing shows that IGMP snooping should not be used by itself on the AR, the AR can be configured to use static IP multicast joins, or the DSLAM can be configured to use IGMP snooping with IGMP report suppression on the DSLAM. Both of these alternatives are described below.

Static IP Multicast Joins on the AR

If the AR is configured to use static IP multicast joins, all of the multicast streams that are configured with static joins are sent through the distribution network to the AR independently of whether or not IGMP requests have been made by STBs.

Statistical analysis can be used to determine when the use of static joins in the AR does not result in a significant amount of additional bandwidth on the GE aggregation links. The results of this statistical analysis are shown below.

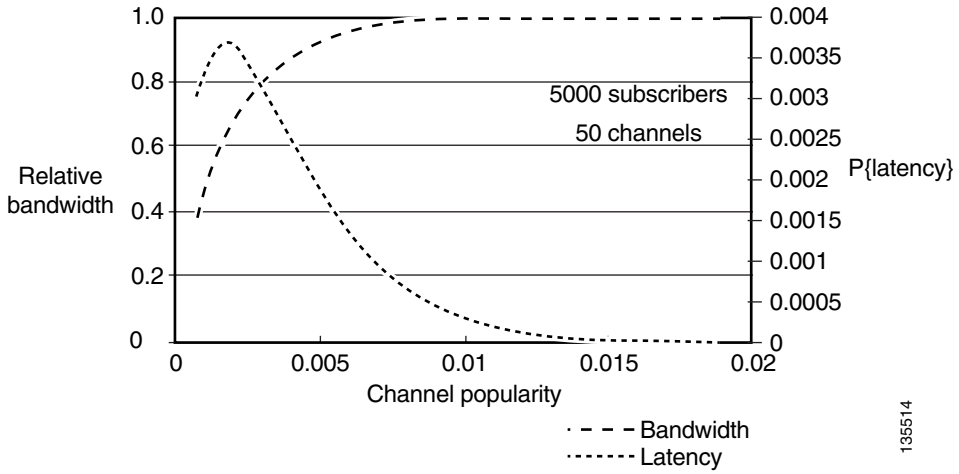
Each service provider must decide, for each channel group, whether that channel group should be a static join or a dynamic join, based on a balance of configuration overhead vs. delay probabilities. Table 3-4 summarizes the factors and formulas used in this analysis.

Table 3-4 Summary of Statistical Analysis

Inputs	Outputs	Formulas
Number of subscribers, N	Bandwidth use of dynamic join vs. static join, B	$B = 1–(1–p)^N$ = dynamic-join bandwidth relative to static-join bandwidth
Number of channels, C	Probability of channel-change latency, L	$L = Cp(1-p)^N$ = contribution to total channel-change latency by this channel group, if joined dynamically
Average channel popularity, p		

Figure 3-14 illustrates the results of the statistical analysis model for bandwidth/latency tradeoff at the AR. Here fixed values are used for the number of channels in a channel group (C = 50) and the number of subscribers served by the node (N = 5000). Note how bandwidth and latency vary with average channel popularity.

Figure 3-14 Bandwidth and Latency vs. Channel Popularity: 5000 Subscribers at the AR



Based on the above, we can make a general recommendation that channel groups with an average per-channel popularity of 0.05% or less should be joined dynamically at the AR, while channel groups with an average per-channel popularity of greater than 0.05% could be joined statically.

Note From Figure 3-14, the probability of any additional latency being caused by dynamic multicast joins is at most 0.37%—and typically much less. Because of this, the additional configuration effort required to set up static groups may not result in much benefit other than 100% consistent delay, because it is very rare for a subscriber to experience the additional delay associated with the IGMP join time.

IGMP Snooping with Report Suppression on the DSLAM

In situations where there are issues with the configuration shown in IGMP-Based Replication in the DSLAM, page 3-23, IGMP snooping on the AR can be combined with IGMP snooping and report suppression on the DSLAMs to provide a more scalable IGMP snooping configuration. When IGMP snooping with report suppression is configured on a DSLAM, the DSLAM forwards only the first IGMP join request for a particular multicast address on the upstream GE link. In addition, the DSLAM sends an IGMP leave request only when it sees a single DSL link currently joined to the multicast stream. This behavior reduces the number of IGMP joins and leaves that the AR must process, enabling the AR to scale to a larger number of subscribers.

Note Not all DSLAMs support this feature, so it cannot be used universally. For these reasons, IGMP snooping with report suppression should be used only in scenarios where the configuration model described in IGMP-Based Replication in the DSLAM, page 3-23 cannot be used.

IGMP Functionality in the STB

As described in Broadcast Client, page 2-3, the broadcast client in the video STB is responsible for implementing channel-change requests from a subscriber by issuing an IGMP leave followed by an IGMP join.

Because the bandwidth on the DSL line is often limited, the broadcast client on the STB typically implements the channel-change function by sending an IGMP leave, waiting for the video stream from the channel that is being tuned away to stop, and then an IGMP join. The broadcast client **must** support IGMPv2, because version 2 is the first release of IGMP that provides the ability for a client to signal explicitly when it wants to leave a multicast group. Broadcast clients that support IGMPv2 **should** also send IGMP joins during a channel change, independently of whether other STBs have also sent IGMP joins for the same channel.

Note This behavior is in fact consistent with the IGMP state machine required to support the IGMPv3 state machine documented in RFC 3376. This modified IGMP behavior is needed in order to support fast leave processing in the DSLAM with multiple STBs in the home.

Broadcast clients **should** also support IGMPv3. In addition to IGMP state machine enhancements, the support of IGMPv3 by the broadcast client enables the client to specify one or more IP source addresses of broadcast encoders from which it wishes to receive the broadcast channel. To support this function, the electronic program guide (EPG) must be updated to send both the multicast group address as well as a list of the IP addresses of real-time encoders that may be used for each broadcast channel. When the broadcast client as well as the EPG are updated to support IGMPv3, the multicast solution is significantly simplified, because Source Specific Multicast (SSM) is supported from the STB all the way to the real-time encoder. As a result, there is no need to turn on SSM mapping in the AR.

Internet Access Forwarding

Because different services in the transport architecture use different logical topologies, the forwarding architecture for Internet access may be different from that for video. The Internet access forwarding architecture used in the solution provides an example of how Internet access can be implemented alongside a video service.

The solution uses Layer 2 forwarding in the aggregation and distribution networks for Internet access. An example Internet access service that could be implemented by this type of architecture would be PPPoE aggregation to a broadband remote-access server (BRAS) that is connected to the DER. The solution transport architecture supports both VLAN per service (N:1) and VLAN per subscriber (1:1) models in the aggregation network for Internet access service.

Release 1.1 includes two example Layer 2 forwarding architectures for the Internet access service:

- Native Ethernet aggregation with 1:1 VLANs
- Ethernet over MultiProtocol Label Switching (EoMPLS)-based aggregation with N:1 VLANs

Both of these models are described in the following sections:

- Native Ethernet Aggregation
- EoMPLS Aggregation

Native Ethernet Aggregation

The native Ethernet aggregation model tested in Release 1.1 uses 1:1 VLANs for Internet access service and N:1 VLANs for voice and video services. As explained in Solution Transport Recommendations Based on WT-101, page 2-33, most current-generation DSLAMs do not support the ability to impose the 802.1ad VLAN tags required for 1:1 VLAN architectures that need to scale to more than 4096 subscribers. Because of this, the 1:1 VLAN model used in Release 1.1 for Internet access is limited to DSLAMs that support dual GE uplinks. The dual GE uplinks enable the DSLAM to map managed application services (video and voice) to one GE uplink, and transport services (Internet access) to the other GE uplink. This mapping enables the DSLAM to encapsulate both the 1:1 Internet access service and the N:1 video and voice services by means of 802.1q encapsulation. Because 1:1 services and N:1 services are segregated on different GE uplinks, the AR can impose an outer S-Tag on packets arriving on the GE link associated with 1:1 services, while not modifying the encapsulation of packets arriving on the GE link associated with N:1 services. Figure 3-15 illustrates the operation of a dual GE uplink DSLAM for 1:1 VLANs when the multi-VC access architecture described in Multi-VLAN Access Architecture, page 2-24, is used, while Figure 3-16 on page 3-30 illustrates the operation of a dual GE uplink DSLAM for 1:1 VLANs when the EtherType access architecture is used.

Figure 3-15 Multi-VC Access with Dual GE Uplinks and 1:1 VLANs for Internet Access

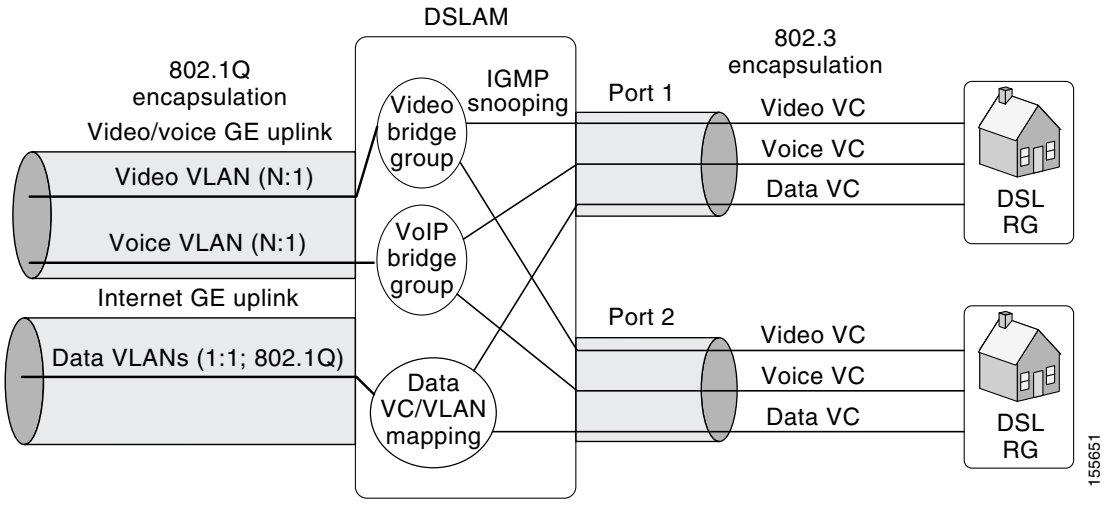
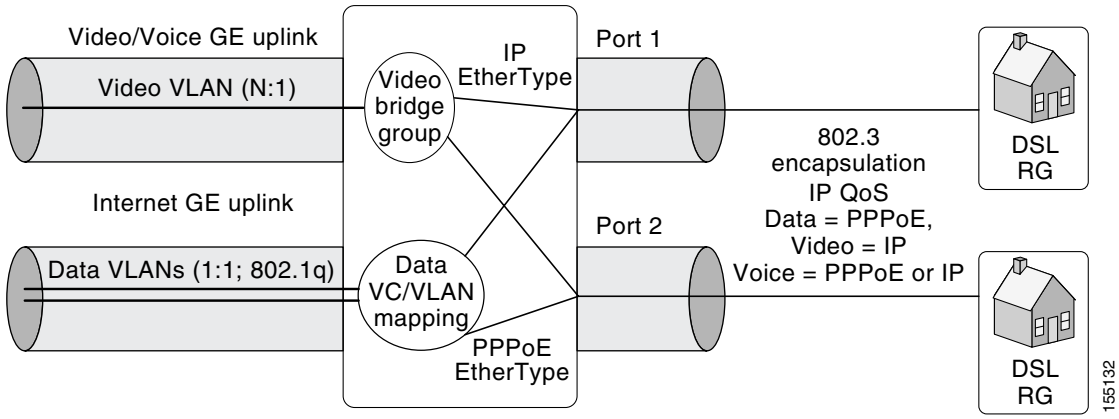


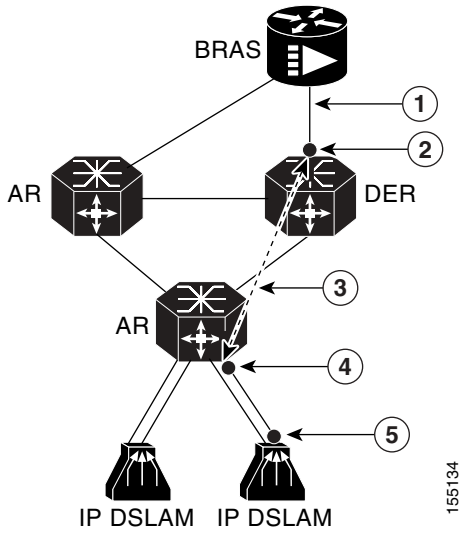
Figure 3-16 EtherType Access with Dual GE Uplinks and 1:1 VLANs for Internet Access [fix spelling]



Because the Ethernet aggregation architecture of Release 1.1 uses 1:1 VLANs for Internet access, the S-Tag that is imposed by the AR is different for each DSLAM connected to it. This configuration makes the VLAN topology look like a hub-and-spoke topology with a separate logical network between each DSLAM and the two DERs. Spanning tree is configured to break the link between the DERs to avoid a forwarding loop. After the spanning tree converges, the VLAN topology looks like separate point-to-point connections between each AR and the DERs. This logical topology conserves MAC address forwarding entries on both the ARs and DERs, because each VLAN now connects only two physical ports. MAC learning algorithms are not needed when a logical topology consists of only two physical ports, because each MAC frame that arrives at one port is always sent on the other port. Figure 3-17 on page 3-31 illustrates the Layer 2 forwarding model used in the solution for the Internet access service (native Ethernet aggregation).

Note Solution testing provides only enough testing of the Internet access service to ensure that the transport network forwards frames correctly, and that the Quality of Service (QoS) configuration provides the guarantees required for each service. Because of this, solution testing includes only traffic sources and sinks that emulate Internet access traffic patterns.

Figure 3-17 Layer 2 Forwarding for Native Ethernet Aggregation



1	Internet traffic (1:1)
2	QinQ—SP outer tag removed
3	Dot1q tunnel
4	QinQ—SP outer tag added
5	• 802.1q trunk—carrying 1:1 VLAN • Internet traffic (1:1)—1 VLAN per subscriber

EoMPLS Aggregation

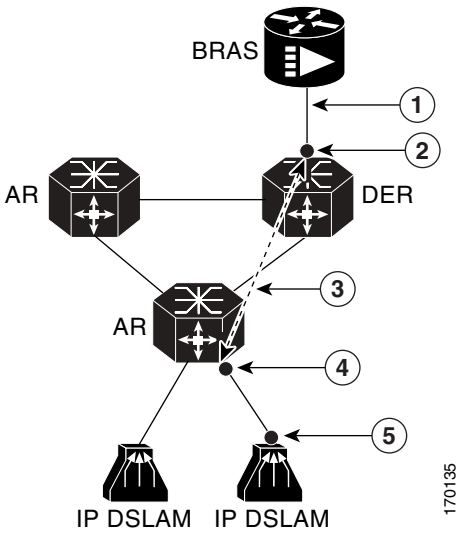
EoMPLS backhaul is sometimes preferred for Layer 2 aggregation over native Ethernet, because MPLS supports traffic engineering functionality and faster reconvergence for link failures than spanning-tree-based algorithms.

The EoMPLS aggregation model used in Release 1.1 uses the MPLS tags associated with the EoMPLS tunnels to distinguish between the Internet access service and managed application services such as voice and video. This can be used to simplify the configuration of the distribution network, by (1) configuring a single IP interface for each physical port in the distribution network, and (2) restricting MPLS label distribution only to routes associated with the EoMPLS tunnel endpoints (which are configured as loopback interfaces on the aggregation and distribution edge routers). In this configuration, each distribution port is configured as a Layer 3 routed port on which MPLS tag encapsulation is enabled. Because MPLS label distribution is restricted only to routes pointing to the EoMPLS tunnel endpoints, all traffic associated with managed services such as voice and video remains IP encapsulated.

As explained in Service Mapping in the Aggregation Network, page 2-25, the use of N:1 VLANs in the aggregation network for Internet access implies that the DSLAM must support a method to provide subscriber line ID (SLID) for transport sessions as part of the session establishment process, Because the solution focuses on video services, service-specific features such as SLID for the Internet access service were not tested as part of the solution.

Figure 3-18 on page 3-32 illustrates the EoMPLS forwarding model used in Release 1.1.

Figure 3-18 Forwarding Model for EoMPLS Aggregation



1	• Internet traffic (N:1) • 802.1q trunk to AR
2	EoMPLS circuits terminated on subinterface • Original VLAN tag maintained • 802.1q trunk—1 VLAN per DSLAM
3	EoMPLS tunnel
4	• EoMPLS circuits terminate on Layer 3 subinterface on AR • VLAN tag maintained through EoMPLS circuit
5	• 801.1q trunk—carrying 1 VLAN • Internet traffic (N:1)—1 VLAN per DSLAM

Each DSLAM is configured to provide a unique 802.1q VLAN tag for the Internet access service. This VLAN is injected into an EoMPLS pseudowire at the AR by configuring a Layer 3 interface for the VLAN and connecting the Internet access VLAN to an EoMPLS pseudowire by means of the Cisco IOS **xconnect** command. This command multiplexes one or more EoMPLS tunnel or pseudowires through an MPLS label switch path (LSP). The EoMPLS tunnel is configured between loopback interfaces on the ARs and DERs. The EoMPLS tunnel is terminated at the DER in a Layer 3 interface configured on a GE port connected to the BRAS. Multiple DSLAMs can be aggregated onto the same upstream port by terminating multiple EoMPLS tunnels on the same Layer 3 interface.

Redundancy to protect against link failures in the Internet access service can be implemented by using the MPLS Traffic Engineering Fast Reroute feature. MPLS supports MPLS fast reroute by configuring diverse LSPs between the two endpoints of the pseudowire. This method provides resiliency combined with 50-msec failover for link failure, but it does not provide resiliency in the case of the failure of a node that terminates the EoMPLS tunnel.

To provide resiliency for node failures such as the failure of a DER or a BRAS, the MPLS Virtual Private LAN Service (VPLS) feature can be used to connect the Internet access VLAN to a set of VPLS tunnels that are terminated in redundant DERs.

Note This design alternative was not tested as part of the solution, because the use of VPLS implies that higher-function line cards (such as the SIP-600) must be used on the AR.

For more information about VPLS, see "Virtual Private LAN Services (VPLS)" at the following URL:

http://www.cisco.com/en/US/products/ps6648/products_ios_protocol_option_home.html

Voice Forwarding

Because the solution transport architecture uses an N:1 VLAN architecture in the aggregation network, the forwarding architecture for voice services may be different from that for video and Internet access. Depending on the VLAN and forwarding configuration in the distribution network, voice traffic may be forwarded as part of the Internet access topology, as part of the video topology, or in a separate topology all by itself.

If voice is forwarded as part of the Internet access topology, it is forwarded at the AR at Layer 2 to the BRAS, along with the Internet access traffic. In this model, the BRAS must provide QoS for the voice service as well as enforce the service level agreement (SLA) for the Internet access service. This model may be used by service providers who have already deployed a voice service through the BRAS and want to use the solution architecture to provide video services through a distributed IP network-based approach.

If voice is forwarded through its own logical topology, it is carried on a separate VLAN in both the aggregation and distribution networks. If a separate VLAN is used for voice, a separate routing process is configured for voice and includes all of the voice interfaces on the AR and DERs.

The voice forwarding architecture tested in the solution provides an example of how a voice service may be implemented alongside video and Internet access services. In Release 1.1 testing, the voice service is forwarded by means of the video topology. This means that voice packets are forwarded through the distribution network on the same logical topology that is used for video services. (See Figure 3-7 on page 3-12.)

Management

Aspects of management include the separation of services, the management of address spaces, element and network management systems, and service monitoring. These topics are addressed below:

- Management Transport
- DHCP Configuration
- EMS/NMS

Management Transport

The hybrid architecture supported in Release 1.1 of the solution provides the flexibility to allow service providers either to manage each service independently or use a common infrastructure for all services. The level of sharing among services can be controlled by configuring a subset of the IP address to be shared, and deploying common infrastructure components within the shared IP address space. A service provider could thereby share some components such as DHCP and DNS servers, while making other components such as VoD servers specific to the video service.

Solution testing included the configuration and testing of the scenarios where DNS and DHCP servers are shared across services. In Release 1.1, a separate management subnet is configured for components that may be shared across services such as DHCP and DNS servers as well as management hosts and as element management systems (EMS) and network management systems (NMS). These components are connected to the DER through either a separate physical port or a separate VLAN than are devices associated with video or voice services. Also in Release 1.1, the address spaces associated with different services such as voice and video are separated by configuring a separate routing process per service. The management subnetwork can be shared across services by including the interface associated with that subnetwork in the routing process associated with each service.

DHCP Configuration

To enable dynamic address allocation for the devices in the home, the network is configured to support Dynamic Host Configuration Protocol (DHCP). Because the AR is the Layer 3 edge device, DHCP relay functionality is configured on the downstream video VLAN interface of that router. The helper address used with DHCP relay points to a DHCP server located in the management network.

Release 1.1 supports a segmented address allocation scheme that uses a separate DHCP address pool per service. With segmented address allocation, there may be separate address pools associated with each service terminated in the AR. Each address pool is shared by all of the devices aggregated by the AR that are associated with a particular service.

STB Identification and Authorization

As described in Electronic Program Guide, page 2-3, the EPG component that is part of video middleware is responsible for authenticating subscribers for both the broadcast video and VoD services. Because video subscribers are authenticated at the application layer by video middleware components, there is no requirement for the network to authenticate the video subscriber at the transport layer. While subscriber authentication is not required, service providers may choose to provide a level of authentication for the video STB to ensure that this component is authorized for use on the network. This section identifies some of the DHCP-based methods that may be used for this simplified form of identification.

In some environments, the service provider may choose to identify and authenticate video subscribers for DHCP purposes by identifying the DSL port that connects the subscriber's STB to the network. This information may be used in addition to the MAC address of the subscriber's STB to enable the service provider to make a more stringent check that the STB is authorized for use on the network. In these environments the DSLAM must be capable of snooping DHCP requests from devices in the home network and inserting a DSL port ID in the DHCP request by means of DHCP option 82. The DHCP server can then extract this port ID from the DHCP request and use it to identify the subscriber. DHCP option 82 is described in RFC 3046.

Note that because the AR is acting as a DHCP relay agent in the solution, a DSLAM that supports DHCP option 82 appears as a trusted downstream (closer to the client) network element (bridge) between the relay agent (the AR) and the client (the STB). In this mode the DSLAM inserts DHCP option 82

information but does not set the “giaddr” field in the DHCP request. In addition, because the DSLAM is not acting as a DHCP relay agent, it does not modify the destination MAC address of the DHCP request but simply forwards this address by means of Layer 2 forwarding. The DSL Forum WT-101 specification specifies both the DSLAM requirements for DHCP option 82 as well as a recommended common format for providing DSLAM and line ID as part of the relay-agent information included with DHCP option 82.

EMS/NMS

Release 1.1 of the solution does not include the integration of element management or network management systems into a video transport solution. The Cisco command line interface (CLI) is the method of configuring the Cisco platforms included in the solution.

Redundancy

The solution addresses fast recovery from the failure of video infrastructure components, as well as of network components in the distribution network, such as physical links or network switching components. Solution testing looked at the recovery characteristics associated with failures of video components such as the VoD servers used for on-demand services and the real-time encoders used for broadcast services.

Note Testing focused on Cisco equipment, with generic failures tested on ingress ports for video services. Only multicast reconvergence was tested.

In addition, solution testing has determined how to optimize the network reconvergence time associated with the failures of links in the distribution network, as well as with the failure of a DER.

This section discusses two types of redundancy:

- Video-Infrastructure Component Redundancy
- Network Redundancy

Video-Infrastructure Component Redundancy

Figure 3-7 on page 3-12 illustrates how the transport architecture supports the redundancy of video infrastructure components such as VoD servers and real-time encoders. The solution test bed included redundant video pumps and real-time encoders attached to redundant DERs.

The solution relies on application-layer failover between the redundant video pumps attached to the DERs in one or more video headends. The video server must support the ability to load-balance VoD sessions between the video pumps attached to the redundant DERs. In addition, a video server must be capable of detecting the failure of a video pump and routing new VoD requests from STBs to still-active video servers in the event of the failure of a video pump.

Solution testing has also characterized the recovery time associated with the failure of real-time encoders by using anycast services. As discussed in Benefit: Fast Failover of Video Encoders, page 3-10, anycast technology can be used to support the ability to detect and recover from the failure of a real-time encoder in the time it takes for the network to reconverge. Release 1.1 testing used redundant real-time encoders configured with the same IP source address attached to the redundant DERs to implement the failover of encoders by using anycast.

Testing simulated the signaling of an encoder (broadcast source) failure, which effectively removes the host route for the failed encoder from the DER. The multicast network between the DERs and the ARs then reconverge. The result is that all that the IP multicast trees for the affected broadcast channel consist of sources from the encoder that is still available.

Network Redundancy

The transport architecture uses dynamic IP routing in the distribution network. This means that the failure of either a physical link or a DER should cause both unicast and multicast routing in the IP transport network to reconverge.

Solution testing has characterized the average and maximum reconvergence times for both unicast and multicast in the event of a link failure or the failure of a DER in the distribution network. The reconvergence trigger events that have been characterized by testing include the following:

- Both an interface and DWDM loss of signal (LOS) caused by a fiber cut
- The failure of a line card within a switching platform
- The loss of an entire DER

Average and worst-case reconvergence times were measured by measuring how long video streams are disrupted at the STB. Testing has also characterized the effect on video quality of the loss of IP video to the STB. During testing, the IP video stream was disrupted for different periods of time (50, 100, 200, 500, and 1000 msec) in order to determine quantitatively the effect of this on video quality. Using this reconvergence and video quality information, the service provider should be able to determine accurately the effect of various network outages in various locations in the video transport network.

Solution testing has also determined the optimal configuration for IP unicast and multicast parameters to optimize reconvergence time for video. Finally, testing has determined the ability of the Quality of Service configuration described in QoS Architecture, page 3-46 to enable the service provider to degrade on-demand services without affecting video broadcast services in the event of a failure in the distribution network.

Note The solution does not include the use of redundant ARs to provide physical-link redundancy to GE DSLAMs.

Release 1.1 Configurations

Two physical distribution-network topologies based on the transport architecture described in Aggregation and Distribution Transport Architecture, page 3-4 were tested for Release 1.1. Both distribution topologies are based on GE rings between the video headend office and video switching offices.

This section presents the following topics:

- Overview
- Transport Components
- Configuration 1: 10-GE Layer 3 Ring
- Configuration 2: 1-GE plus 10-GE Hub and Spoke

Overview

One topology (referred to as Configuration 1) uses a 10-GE ring between the VHO and VSOs. This configuration uses symmetric bandwidth around the ring to provide physical link redundancy for all services. The other topology (referred to as Configuration 2) uses 1-GE and 10-GE links between the distribution edge routers and aggregation routers. This topology provides physical link redundancy for the Internet access, voice, and broadcast video services, but it does not provide full redundancy for VoD services. In the event of a link failure, VoD services are degraded without affecting any of the other services through the use of the QoS architecture described in QoS Architecture, page 3-46.

Transport Components

Table 3-5 lists the Cisco transport components tested for both configurations.

Table 3-5 Transport Components Tested for Both Configurations

Network Role	Line Card Role	System	Product Number	Interface Type
DER		Cisco router/switch	7600 series, 6500 series	
		Supervisor	WS-SUP720-3BXL[1]	N/A
	DER <–> AR	10 GE x 4 optic	WS-X6704-10GE	XENPAK-10GB-LR
	DER <–> VoD servers	1 GE x 24 optic	WS-X6724-SFP	1GE-SR/LR/DWDM
		48-port copper Ethernet	WS-X6748-SFP	1GE-COPP-SR or -LR
AR		Cisco router/switch	7609, 6509	
		Supervisor	WS-SUP720-3BXL	N/A
	DER <–> AR, AR <–> AR	10 GE x 4 optic	WS-X6704-10GE	XENPAK-10GB-LR
	AR <–> DSLAM	1 GE x 24 optic	WS-X6724-SFP	1GE-SR/LR/DWDM

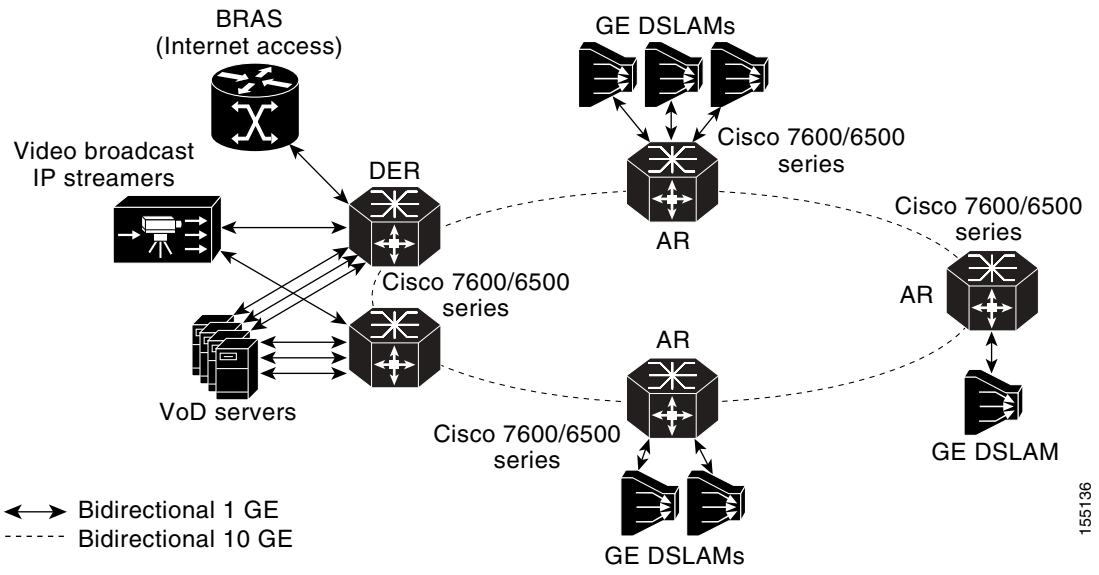
1. All line cards use the Distributed Forwarding Card, WS-F6700-DFC3BXL.

Configuration 1: 10-GE Layer 3 Ring

Figure 3-19 on page 3-38 illustrates the 10-GE-based symmetric ring topology used in Release 1,1. This topology uses the aggregation/distribution transport architecture described in Aggregation and Distribution Transport Architecture, page 3-4, with the Layer 3 edge for video and voice services at the AR. The Internet access aggregation model tested in this topology is EoMPLS, as discussed in EoMPLS Aggregation, page 3-31.

The 10-GE topology shown in Figure 3-19 on page 3-38 provides fiber redundancy for all services. A link cut anywhere on the ring results in traffic from all services being rerouted in the other direction around the ring. Solution testing included a test scenario where the failure of a link in the 10-GE ring and the resulting rerouting of video traffic results in steady-state congestion of video traffic on the remaining 10-GE links. In this scenario the QoS configuration described in QoS Architecture, page 3-46, is used to cause only the VoD flows to be affected while not affecting the broadcast video service at all.

Figure 3-19 Configuration 1: 10-GE Ring

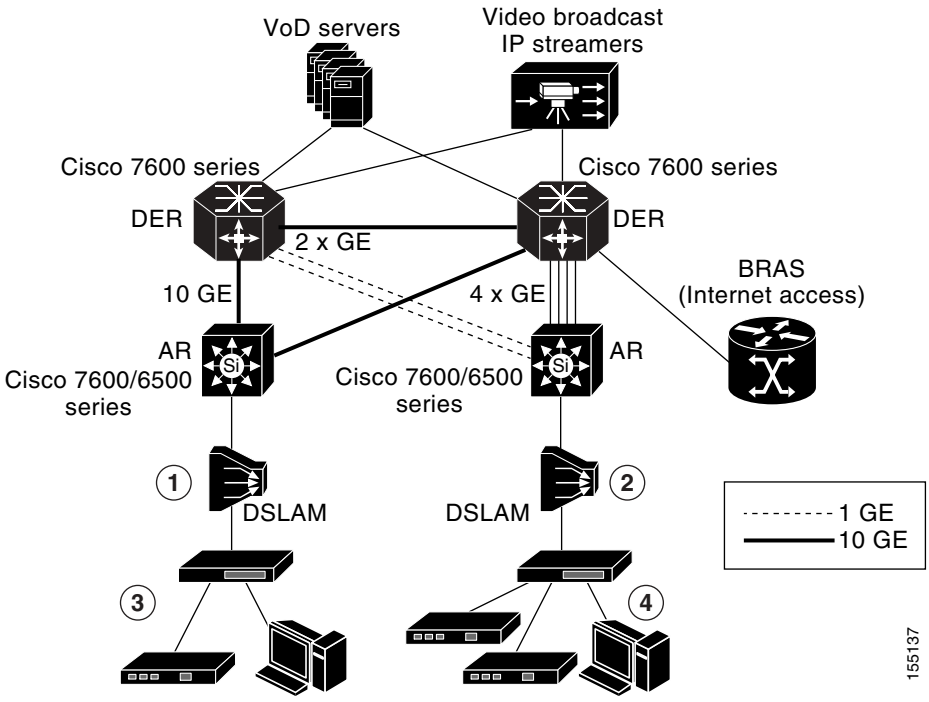


The 10-GE topology shown in Figure 3-19 on page 3-38 provides fiber redundancy for all services. A link cut anywhere on the ring results in traffic from all services being rerouted in the other direction around the ring. Solution testing includes a test scenario where the failure of a link in the 10-GE ring and the resulting rerouting of video traffic results in steady-state congestion of video traffic on the remaining 10-GE links. In this scenario, the QoS configuration described in QoS Architecture, page 3-46, causes the VoD flows to be affected, while not affecting the broadcast video service at all.

Configuration 2: 1-GE plus 10-GE Hub and Spoke

Figure 3-20 on page 3-39 illustrates a topology that includes 1-GE and 10-GE links between the DERs and ARs. Redundancy is obtained by connecting each AR to a pair of DERs through 1-GE or 10-GE links. This topology uses the aggregation/distribution transport architecture described in Aggregation and Distribution Transport Architecture, page 3-4, with the Layer 3 edge for video and voice services at the AR. The Internet access aggregation model tested in this topology is native Ethernet aggregation, as described in Native Ethernet Aggregation, page 3-29.

Figure 3-20 Configuration 2: 1-GE plus 10-GE Hub and Spoke



Note For a 10-GE symmetric ring configuration that used the Cisco 4500 series and Cisco 4948-10GE for the ARs, see the following discussion in the design and implementation guide for the previous release:

http://www.cisco.com/univercd/cc/td/doc/solution/vobbsols/vob1/vbdig/vbdsgn1.htm#wp1167435

Edge Transport Architecture

The edge transport architecture specifies how traffic from the voice, Internet access, and video services are aggregated in separate logical topologies in the aggregation and access networks. The edge network consists of the GE aggregation links between the ARs, the DSLAMs, the DSL links, and the RG.

Note While the solution specifies the interfaces between the home network and the RG that are needed to support service mapping, it does not specify either the transport technology or architecture that is used in the home to support service mapping.

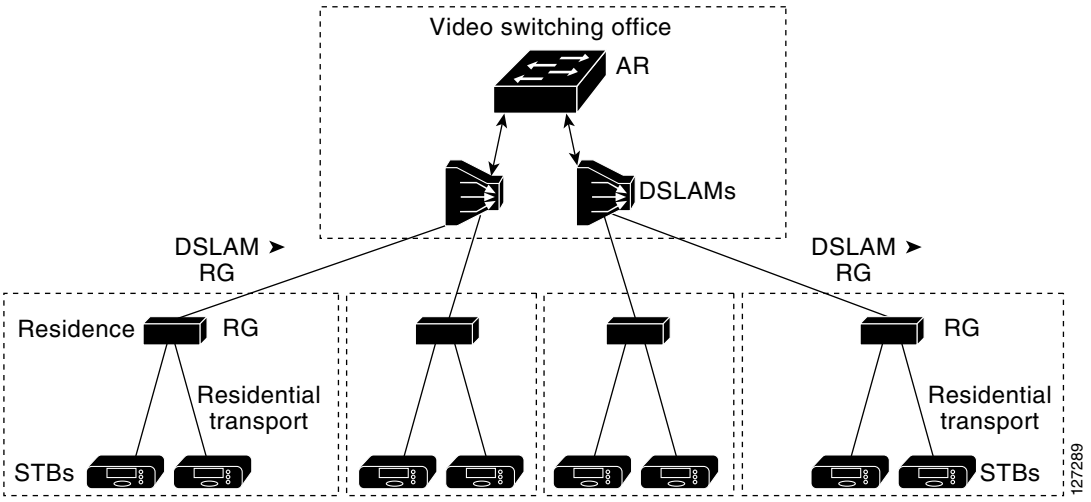
This section presents the following topics:

- Overview, page 3-40
- DSLAM Functions, page 3-41
- RG Functions, page 3-41

Overview

Figure 3-21 illustrates the nodes and links in the edge network.

Figure 3-21 Edge Transport Network



As described previously in AR Configuration, page 3-12, voice, video, and Internet access services are separated on the aggregation GE links by assigning each service to a separate 802.1q VLAN. On the DSL link, services are separated by using a separate ATM PVC or a separate 802.1q VLAN tag per service. The DSLAM and RG each include the service with which a packet is associated as part of the algorithms for switching packets.

DSLAM Functions

The solution uses an Ethernet DSLAM that performs MAC layer switching between the ATM VCs on the DSL links and the GE uplink. Mac layer bridging in the DSLAM is enabled through the use of RFC 2684 bridged encapsulation on each VC of the DSL link.

To enable service mapping, the solution architecture supports a number of models for mapping different service topologies to identifiers in the access and aggregation infrastructures. WT-101 Service Mapping, page 2-23, describes the models specified in DSL Forum document WT-101 for mapping services to topology identifiers in both the access and aggregation infrastructures. (The WT-101 specification specifies requirements for IGMP-based replication in DSLAMs.) The solution architecture can support any of the models outlined in that section, as long as the DSLAM implements the features implied by these models. The WT-101 specification specifies the DSLAM tagging and forwarding requirements for each of models outlined in WT-101 Service Mapping, page 2-23.

To support broadcast video services, the DSLAM **must** support an IGMP snooping algorithm. The DSLAM uses IGMP snooping to determine the DSL ports to which it should replicate incoming IP multicast packets. IGMPv2 snooping allows the DSLAM to track IGMPv2 state for each DSL port and IP multicast destination; it replicates multicast packets to a particular multicast destination to the DSL ports that are actively joined to that multicast destination.

RG Functions

The residential gateway, or RG,[1] performs physical adaptation as well as Layer 2 bridging between one or more physical media in the home and the upstream DSL link that uses RFC 2684 bridged encapsulation. The transport architecture does not make any assumptions regarding the physical media used for triple-play services within the home.

The transport architecture also assumes that the home devices that terminate the IP streams for video and Internet access services are typically not integrated into the HAG. Because of this, the architecture assumes that the physical media within the home are capable of transporting IP packets, and use a Layer 2 encapsulation method that can be translated to an 802.3 transport header in a straightforward manner.

For the voice service, the RG may include an integrated voice gateway that translates VoIP into one or more FXS ports that connect to telephone wiring in the home via one or more RJ-11 ports. In this case, there is no need to carry VoIP traffic within the home network.

Table 3-6 on page 3-42 specifies some potential physical media and the associated Layer 2 encapsulations that a RG may have to translate to the upstream DSL link with RFC 2684 bridged encapsulation.

1. Also referred to as a home access gateway, or HAG.

Table 3-6 Potential Home Wiring Technologies Requiring RG Support

Physical media	Layer 2 Encapsulation
Air	802.11
Category 5 cable	802.3
Coaxial cable	Media over Coax Alliance (MoCA)
	HomePhoneNetwork Alliance (HomePNA v3)
Power line	HomePlug Alliance
Phone line	HomePhoneNetwork Alliance (HomePNA v3)

In Release 1.1 the RG is responsible for identifying the service topology with which each device in the home network should be associated. This is a very important aspect of the service mapping architecture, because it has implications for how services are delivered to the home network, and on the design of the home network itself.

In Release 1.1, service mapping in the home is implemented by mapping each device in the home to a primary service topology (voice, video, or Internet access). Service Mapping in the Access Network, page 2-23, describes the technologies used to implement service mapping on the DSL line.

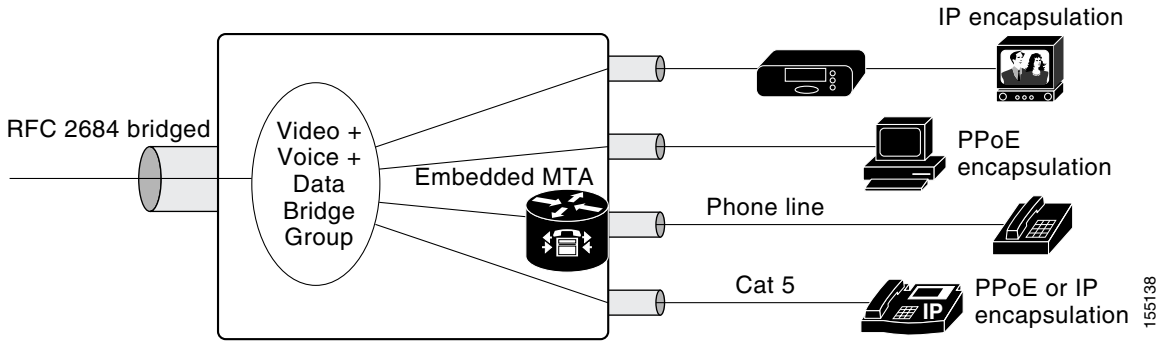
The methods by which packets from the home network are mapped to an upstream service topology depend very much on the technology used to the identify the topology on the DSL line itself. The sections below describe how service mapping can be implemented in both Layer 2 HAGs and HAGs capable of Layer 3 Network Address Translation (NAT) for each of methods described in Service Mapping in the Access Network, page 2-23, for mapping service topologies in the access network.

EtherType Service Mapping in a Layer 2 RG

When EtherType-based service mapping is used with a Layer 2 capable HAG, the transport session initiated by each device in the home determines the upstream service topology with which that device is associated. This model assumes that PCs associated with the Internet access service use PPPoE encapsulation for their transport sessions, while STBs associated with the video service use IP encapsulation for their transport sessions. IP phones or embedded VoIP hosts may be associated with either the video or data topologies, and so may use either a PPPoE or IP transport client.

Because service mapping with the EtherType model is essentially performed by the transport host in each home device, the RG itself does not play a role in the service mapping function. The RG simply performs a MAC-layer bridging function between the ports connected to the home network and the upstream ATM VC associated with the DSL line. Figure 3-22 on page 3-43 illustrates this mapping topology.

Figure 3-22 EtherType Service Mapping in a Layer 2 RG



Physical Port-Based Traffic Mapping for the Multi-VC and VLAN Access Models

The physical port-based method of traffic mapping takes advantage of the fact that most existing home wiring uses separate physical media for each of the triple-play services. The physical wiring of most homes today includes telephone wiring to telephones for telephony services, coax wiring to television sets or STBs for video services, and may include Category 5 wiring for Internet access services.

An RG could take advantage of this existing wiring to provide service mapping by including an embedded VoIP host for the voice service, terminating MoCA or HPNAv3 over coax wiring for the video service, and terminating either 802.11 or 802.3 for the Internet access service. Because each of these services is terminated in the RG by means of different physical media, the RG can determine the upstream VLAN or ATM VC with which to associate each packet by determining which physical port the packet arrived on. Figure 3-23 illustrates physical port-based traffic mapping in the RG for the multi-VC access model, while Figure 3-24 on page 3-44 illustrates the same for the multi-VLAN access model.

Figure 3-23 Physical Port-Based Traffic Mapping with Multi-VC Access Architecture

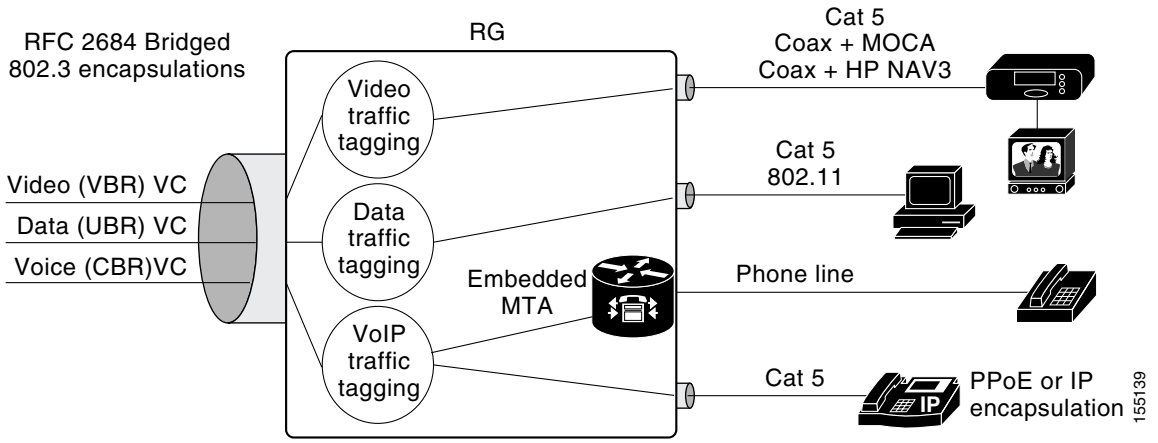
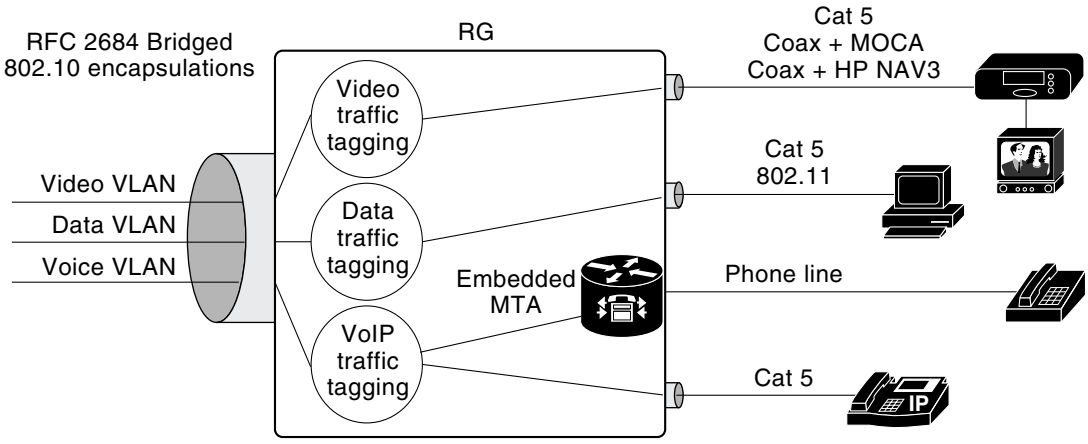


Figure 3-24 Physical Port-Based Traffic Mapping with Multi-VLAN Access Architecture



One issue with physical port-based traffic mapping is that it enforces a rather rigid mapping of home devices to services. As home network technologies become more ubiquitous, it may not be practical to use the physical media to which a device is connected to associate that device with a particular service. In these environments, it may be more practical to use other methods of mapping between the home network and multiple upstream service topologies. NAT/Layer 3 Functionality, below, provides an example of how to achieve this by using NAT/Layer 3 functionality in a HAG.

NAT/Layer 3 Functionality

To limit the number of IP addresses the service provider must allocate in the home network, and to allow home devices associated with different services to communicate with each other, the RG may include NAT/Layer 3 functionality.

An RG that implements Layer 3/NAT functionality as well as a service mapping function must be capable of mapping each device in a home network to an external transport client that is associated with that service topology. For example, if the voice, video, and data service are each associated with their own service topology, the NAT-capable RG must support a separate DHCP or PPPoE transport client state machine for each of these upstream topologies. Each client may be in a separate external subnetwork and have its own IP address assigned to it.

A Layer 3 RG that supports service mapping must map the source IP address of each device in the home to the IP address of the external client with which the device has been associated as part of the NAT translation function. The mapping between home devices and the associated external client could be statically configured, or it could be learned dynamically through DHCP options such as DHCP option 60 (vendor specific attributes).

A Layer 3 RG implements a local DHCP server that is used to allocate local IP addresses to devices within the home network. All devices within the home network are assigned to a single IP subnetwork whose address is configured in the HAG. When the RG receives a DHCP request from a home device, it creates a NAT entry that maps between that client's IP address and the external address of the client with which the device is associated. This external address can be used to determine the external client and resulting service topology with which the home device is associated.

Because all of the addresses in the home network are assigned by the RG to be in a single IP subnet, devices in the home that are associated with different services can communicate by means of standard IP host functionality. An RG that implements NAT/Layer 3 functionality should also implement standard MAC-layer learning and forwarding functionality between the physical ports attached to the home

network. This functionality enables all devices in the home network to communicate independently of the physical port to which they are attached. Because the home network is typically capable of carrying much more bandwidth than is generated as part of the broadcast video service, the MAC-layer forwarding function in the RG may broadcast Ethernet frames received from the DSL port with a destination MAC address in the multicast address range to all downstream ports.

An RG that implements NAT/Layer 3 functionality **must** implement an IGMP snooping function, in order to enable multicast streams to bypass the NAT logic and be sent directly to the home network without performing address translation. The IGMP snooping function on the RG **must not** repress any IGMP report messages from home devices. This is needed to enable the DSLAM to implement a fast-leave algorithm that tracks IGMP requests from each home network device. With the introduction of high-definition streams, the home network may not be capable of carrying much more bandwidth than is generated by the broadcast video service. Because of this, the MAC layer forwarding function in the RG **should** only send Ethernet frames received from the DSL port with a destination MAC/IP address to home network ports in an active IGMP session.

An RG that implements NAT/Layer 3 functionality **must** support a local ARP function for devices on the home network. The ARP function responds to ARP requests for nonlocal IP addresses (IP addresses that have not been locally allocated by the HAG's DHCP server) with its own MAC address.

An RG that implements NAT functionality **must** implement stateful inspection for Real Time Streaming Protocol (RTSP, RFC 2326) and Session Initiation Protocol (SIP, RFC 3261) as part of the NAT function. RTSP is the most common session-signaling protocol for a VoD session initiated by video STBs, while SIP is the most common session-signaling protocol for IP telephony applications. Stateful inspection is required by NAT functions that support RTSP and SIP because these protocols specify the IP address and Layer 4 port values for video and voice media streams in the payload of signaling messages.

The following figures illustrate how Layer 3 functionality in the RG can be used to implement a service mapping function on the DSL line. Figure 3-25 illustrates service mapping with the multi-VC access architecture, while Figure 3-26 on page 3-46 illustrates service mapping with the EtherType access architecture.

Figure 3-25 NAT/Layer 3 Functionality in the HAG: Multi-VC Access Architecture

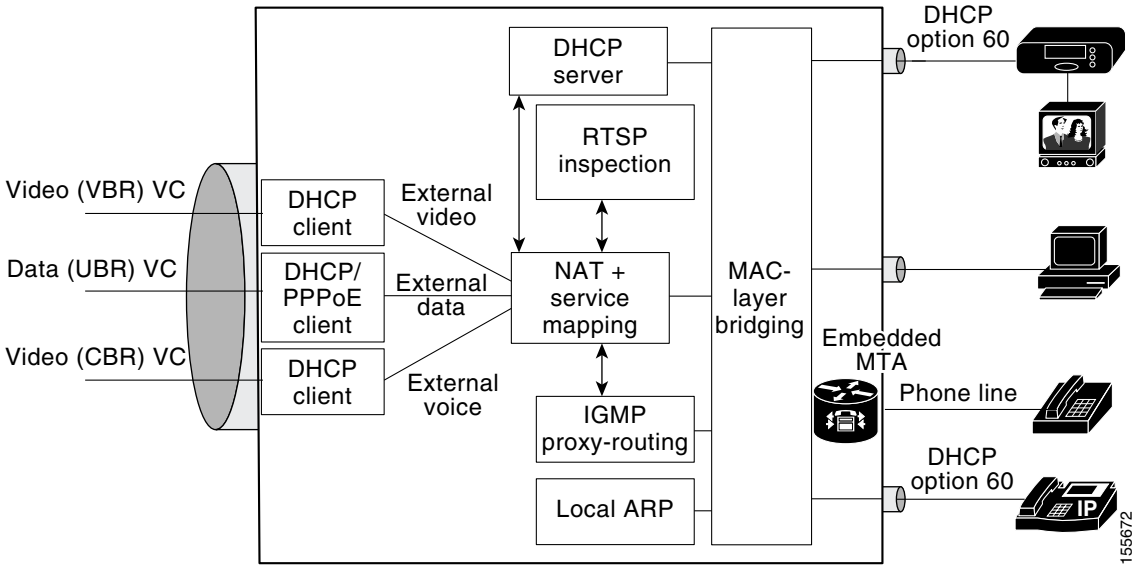
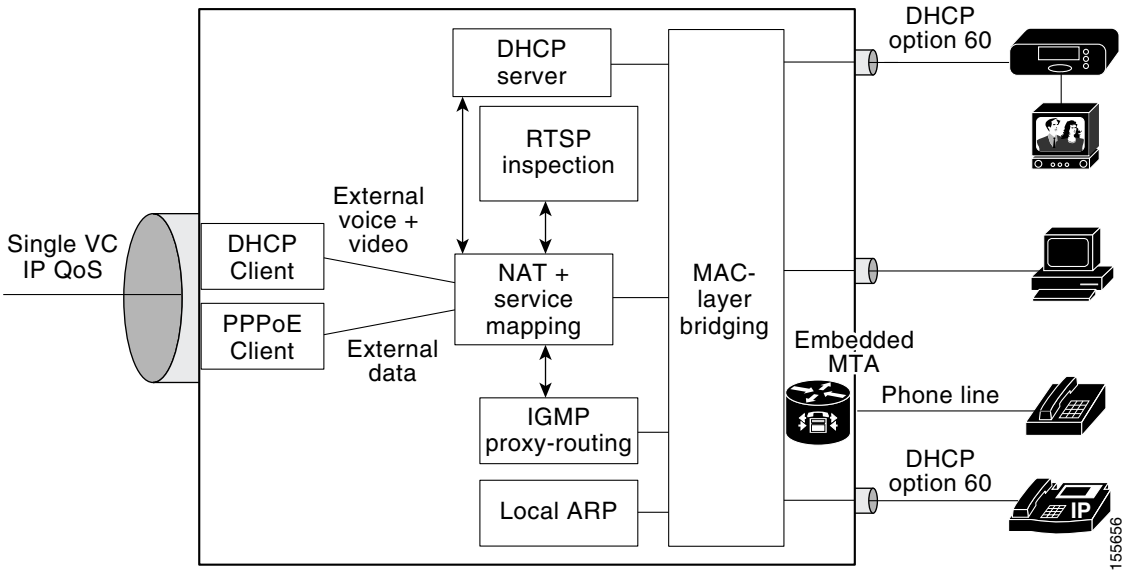


Figure 3-26 NAT/Layer 3 Functionality in the HAG: EtherType Access Architecture



QoS Architecture

The Quality of Service (QoS) architecture in the solution is based on the IETF Differentiated Services (DiffServ) Architecture described in RFC 2475. The DiffServ architecture assumes that each node in a transport network that is connected to physical links where congestion can occur **must** be capable of scheduling packets from different services separately. In an environment where all services are not aggregated at the BRAS, the DSL access links between home access gateways (HAGs) and DSLAMs, as well as the aggregation links between DSLAMs and aggregation routers, can become congested. This means that aggregation routers, DSLAMs, and HAGs **must** be capable of basic DiffServ functionality.

This section presents the following topics:

- Overview of DiffServ Architecture
- DiffServ Architecture in the Solution
- Triple-Play QoS Analysis
- QoS in the Aggregation/Distribution Network
- QoS in the Access Network

Overview of DiffServ Architecture

The DiffServ architecture specifies different requirements for nodes at administrative boundaries than for nodes in the interior of a DiffServ domain. A DiffServ domain is defined as an area where all nodes are configured with the same DiffServ policies for QoS. The edge of a DiffServ domain is the administrative boundary of that domain.

In the DiffServ architecture, nodes at administrative boundaries must implement a superset of the functionality that nodes in the interior of a DiffServ domain implement. Nodes at administrative boundaries must be capable of rate-limiting traffic coming into a DiffServ domain by using a rate-limiting technology such as policing or shaping. Nodes at administrative boundaries must also be capable of marking traffic that is supposed to have different per-hop behaviors, by using separate DSCP code points. An example of a node at the edge of a DiffServ domain in a residential triple-play architecture is the HAG. While the RG is managed by the service provider, the home network typically is not. Because of this, the RG must associate packets that arrive from ports attached to the home network with a service and its associated QoS. The functionality that the RG implements to classify and mark traffic from the home network is an example of the DiffServ functionality required at administrative boundaries.

All nodes in a DiffServ domain that may experience packet congestion must be capable of classifying packets by means of a DiffServ code point (DSCP) and implementing the specified DiffServ per-hop behavior (PHB) accordingly. This functionality must be implemented on nodes in the interior of a DiffServ network as well as on nodes at an administrative boundary.

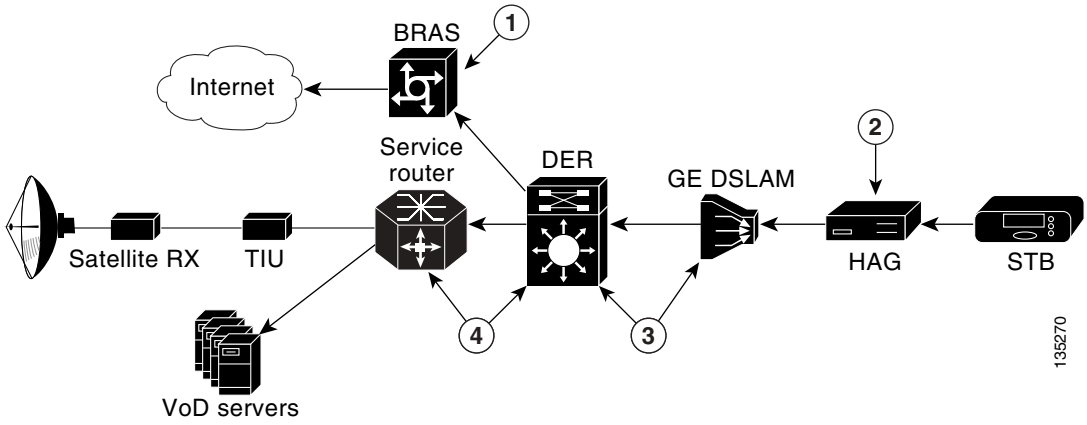
The DiffServ architecture described in RFC 2475 assumes that all nodes where congestion can occur are capable of implementing QoS functionality at the IP layer. One can extend this basic architecture to nodes that implement QoS functionality at Layer 2 by mapping the DiffServ PHBs specified by DiffServ code points to Layer 2 functionality at the edges of the Layer 2 network. An example of a Layer 2 technology that implements QoS is ATM. The ATM specification defines its own methods of obtaining QoS by using functionality that is part of ATM switching. The ATM traffic-management specification defines classes of service that must be implemented by ATM switching nodes as well as by the nodes at the edge of an ATM network that implement the Segmentation and Reassembly (SAR) function. Examples of services classes defined by the ATM traffic-management specification are Constant Bit Rate (CBR), Variable Bit Rate (VBR), and Unspecified Bit Rate (UBR). In a DSL environment, each of the ATM CoS values can be mapped to a DiffServ PHB without sacrificing the overall QoS requirements of the network.

While the edge of a DiffServ domain represents one level of boundary of trust, service providers (SPs) may choose to implement a second, more secure boundary of trust within the interior of the DiffServ domain. For example, while the functions the RG are considered functions of a boundary of trust, the RG may be compromised because it is not located within the SP's premises. Because of this, an SP may choose to implement additional enforcement functions such as policing at a location in the network that is considered more secure.

DiffServ Architecture in the Solution

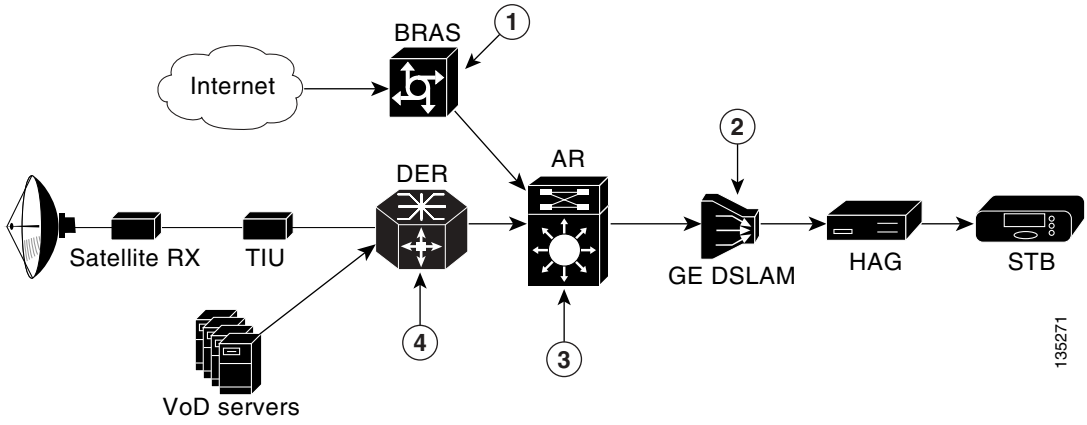
This section describes how the Cisco Wireline Video/IPTV Solution uses the DiffServ architecture to implement QoS in support of triple play. Figure 3-27 illustrates the upstream QoS and security functionality used in the solution, while Figure 3-28 on page 3-49 illustrates the downstream QoS and security functionality used.

Figure 3-27 Upstream QoS and Security



1	Internet access service enforcement (per-subscriber policing)
2	Administrative boundary (service-based marking); DiffServ-to-Layer 2 mapping (802.1p, ATM CoS)
3	VoD boundary of trust (per-flow policing of signaling)
4	Broadcast video boundary of trust (multicast access lists, IGMP policing)

Figure 3-28 Downstream QoS and Security



1	Internet access service enforcement (per-subscriber policing, shaping, queueing)
2	DiffServ-to-Layer 2 mapping (ATM CoS)
3	DiffServ-to-Layer 2 mapping (802.1p)
4	Video administrative boundary (service-based marking)

Administrative Boundaries

When the DiffServ architecture is mapped to the solution transport architecture, the DiffServ administrative boundaries can be mapped to specific nodes, as discussed below.

In the upstream direction, the administrative boundary is the RG. While the RG is managed by the SP, the home network typically is not. Because of this, the RG must associate packets that arrive from ports attached to the home network with a service and its associated QoS. Because the RG is at the edge of the SP's DiffServ domain, it **should** be capable of writing a configurable DSCP to each upstream packet, based on the service associated with that packet, by means of the service classification rules described in EtherType Service Mapping in a Layer 2 RG, page 3-42.

The service mapping architecture ensures that the video headend infrastructure resides in a separate logical topology from other services such as Internet access. Because of this, the video headend topology is managed by the SP and can be contained within a single DiffServ administrative domain. If VoD servers and real-time encoders are capable of marking the video streams, as well as the control traffic, with the appropriate DSCP values, then there is no need for the video topology to implement DiffServ edge functionality in the downstream direction. If the VoD servers or real-time encoders are not capable of implementing the DiffServ marking functionality, then the DER should perform this function on their behalf.

DiffServ-to-Layer-2 Mapping

In most DSL/Ethernet aggregation architectures, the access and aggregation networks include nodes that are not capable of supporting IP-layer QoS. In such architectures, the DSLAM and the RG typically implement both packet forwarding and QoS algorithms at Layer 2. QoS in the Access Network, page 3-57, provides the details of how DiffServ-to-Layer-2 Mapping is used to provide proper scheduling behavior in the DSL access network.

Security and Additional Boundaries of Trust

While the edge of a DiffServ domain represents one level of a boundary of trust, SPs may choose to implement a second, more secure boundary of trust within the interior of the DiffServ domain. While the RG limits upstream traffic by means of its ATM-based scheduling functionality, the RG is not located within the SP's premises and may therefore be compromised.

The solution architecture specifies additional functionality that is used to provide additional security for both VoD and broadcast video services, as discussed below.

For VoD services a second upstream policing function is implemented on the aggregation platforms located in either the video switching office or the video headend office. The upstream policing function uses the per-flow policing functionality of the Cisco Catalyst 6000 and Cisco Catalyst 7600 series switches used in the solution to limit the amount of upstream video signaling traffic for VoD to a specified upper limit. With per-flow policing, each upstream flow is recognized dynamically in hardware, and for each new flow a separate hardware-based policer is instantiated. Each policer limits the amount of traffic that is passed upstream to a configured maximum bandwidth and burst size. The bandwidth and burst rate of the upstream policer are determined by the expected maximum bandwidth and burst that video signaling is expected to generate. Any traffic that exceeds the per-flow rate or burst size is dropped.

To limit control-plane-based denial of service (DoS) attacks on the broadcast video service, IGMP access lists can be used on DSLAMs and ARs to restrict multicast join requests to the multicast address range that is known to be valid for the video broadcast service. Any IGMP join requests that fall outside of this address range are dropped. Note that this function is not intended as an enforcement method to limit subscribers to the set of broadcast channels they are authorized to view. The Conditional Access System (CAS) described in Conditional Access System and Encryption Engine, page 2-6 is typically used to implement this function.

In addition to IGMP access lists, DSLAMs and ARs can also restrict the rate at which multicast join requests are accepted by the network through the upstream policing of IGMP traffic. In the AR, IGMP policing can be configured by policing all traffic that matches the IP protocol ID for IGMP to a rate that is less than the maximum performance determined by IGMP performance testing.

Triple-Play QoS Analysis

This section describes the analysis behind the DiffServ PHBs and the resulting scheduling QoS configuration recommendations used in Release 1.1 of the solution. This discussion assumes a residential triple-play service with Internet access, voice, and video services. Internet access is assumed to be a best-effort service, with the customer's service-level agreement (SLA) specifying only a maximum (but not a guaranteed minimum) rate. Voice and video are assumed to be managed application services, where the SP provides the subscriber with a video STB and sells the subscriber a video or voice SLA.

An example of a video SLA that an SP may offer is a single channel of VoD or broadcast video delivered to each STB for which the subscriber signs up. The subscriber may sign up for basic or premium-tier broadcast services, and may also sign up for a set of VoD services offered by the provider. The maximum number of STBs that the subscriber may sign up for is limited by the following:

- The type of video service the subscriber requests (for example, standard vs. high definition)
- The video encoding technology used by the SP (for example, MPEG-2 vs. MPEG-4)
- The total amount of DSL bandwidth available to the subscriber

Internet Access

If Internet access is sold as a best-effort service, the DiffServ Default PHB can be used to schedule packets classified as belonging to the Internet access service. The DiffServ Default PHB is described in RFC 2474. The DiffServ PHB provides a best-effort packet-scheduling behavior.

On the aggregation and distribution edge routers, the Default PHB is implemented by using a weighted scheduler that is configured for a minimum bandwidth guarantee. This configuration ensures that Internet access traffic does not significantly affect jitter, latency, or drop for packets associated with the voice or video services.

Voice

End-to-end latency and jitter are very important for a VoIP service. A typical end-to-end jitter requirement for a carrier-class VoIP service is 60 msec. Low jitter and latency are essential to a voice service because the additional delay that results from both factors makes conversations less of an interactive experience, degrading the telephone user's experience.

While delay is an extremely important factor for a successful voice service, the drop requirements for a voice service are not as stringent as they are for video. The reasons that packet drop requirements are not as stringent for a voice service as for a video service are due to digital-to-analog translation algorithms available in current VoIP endpoint implementations. These implementations include a concealment algorithm that can conceal the effects of the loss of a 30-msec voice sample. This means that a packet loss that causes less than a 30-msec loss of digital audio results in an analog signal with no noticeable impairment to the user. With voice concealment algorithms it takes a loss of two or more consecutive 20-msec voice samples to result in a perceptible loss of voice quality. A drop rate of 1% in a voice stream results in a loss that could not be concealed every three minutes when concealment algorithms are taken into account. A 0.25% drop rate results in a loss that could not be concealed once every 53 minutes on average.

Because of this stringent latency requirement, voice services use the DiffServ EF (Express Forwarding) PHB. The DiffServ EF PHB is described in RFC 3246. The EF PHB defines a scheduling behavior that guarantees an upper bound on per-hop jitter that can be caused by packets from non-EF services.

On the aggregation and distribution edge routers, the EF PHB is implemented by means of a priority scheduling algorithm. This algorithm ensures that voice packets can only be delayed by at most one packet serialization time by nonvoice packets per network hop. This delay amounts to a maximum of 12 microsec per hop on 1-GE links configured for a 1500-byte MTU.

Video

While voice has stringent jitter and latency requirements and a relaxed loss requirement, video has a very stringent loss requirement and a relatively relaxed jitter requirement.

Current video-encryption technologies are not resilient to a loss of information in the compressed video stream. As a result, the loss of a single IP packet in a video stream typically causes a noticeable degradation of video quality. The hit to video quality can vary from pixelization across a few frames to a video stream that is frozen for up to 1 second depending on which information in the video stream is lost. The result is that the packet loss requirements for video are extremely stringent. Because of the lack of a concealment algorithm for video, the allowed drop rate for a video service with at most one visible defect per hour is 10^{-6}.

The maximum jitter requirement for video can be determined by examining the maximum channel change delay for broadcast video. Broadcast Video Channel-Change Time, page 2-15, describes the components of channel change delay for a broadcast video over IP service. From Table 3-3 on page 3-19, the component of channel-change delay associated with the jitter buffer on the STB is typically around 200 msec; the size of this buffer determines the maximum allowed jitter—200 msec—for a VoIP service.

Because traffic associated with the Internet access service is carried in a best-effort queue, it does not have a significant impact on jitter for video. However, because voice is carried in a priority queue, it does have an impact on jitter for video. The impact of voice on video jitter is minimized by the fact that in most triple-play deployments, the link utilization of voice traffic is not a significant amount of the total link bandwidth. When the relatively loose jitter requirement for video (200 msec) is taken into account, the relatively low link utilization does not result in video jitter above the maximum limit.

Because of the above factors, video flows are scheduled by means of the DiffServ AF PHB. (The DiffServ AF PHB is described in RFC 2597.) While the AF PHB does not provide as stringent a jitter guarantee as the EF PHB used for voice, it can be used to guarantee a maximum jitter/latency and drop rate for a class of packets. RFC 2597 defines four different classes of the AF PHB. To maintain consistency with current IETF DiffServ marking conventions, this document uses the AF4 PHB. This means that all video flows are marked with a DiffServ code point in the AF 4X range. In addition to four scheduling classes, the AF PHB makes it possible to provide four different drop characteristics for each scheduling class. These different drop characteristics are called drop precedence values. Broadcast Video vs. Video on Demand, page 3-54, provides details on how the different availability requirements of broadcast video and VoD traffic can be implemented by using different drop precedence values within the AF PHB.

On the aggregation and distribution routers, the AF PHB is implemented by means of a weighted scheduling algorithm. To ensure the packet loss and drop requirements for video, the weight configured on the video queue should be greater than the combined bandwidth of the traffic associated with both services under normal operating conditions. Broadcast Video vs. Video on Demand, page 3-54, provides specific recommendations for the weight that should be applied to this queue.

Burst Accumulation

The last factor that must be taken into account in determining QoS requirements for video is burst accumulation. Burst accumulation is an instantaneous burst of traffic that is caused by multiple sources of video transmitted through an IP network. If two or more sources are unsynchronized, there is a probability that the packets they generate are transmitted at exactly the same time. If this traffic converges at an intermediate physical link, the link experiences an instantaneous build up of packets. As these bursts of packets are transmitted to downstream routers, the bursts becomes even larger. This is called burst accumulation. Burst accumulation is influenced by a number of factors, including the following:

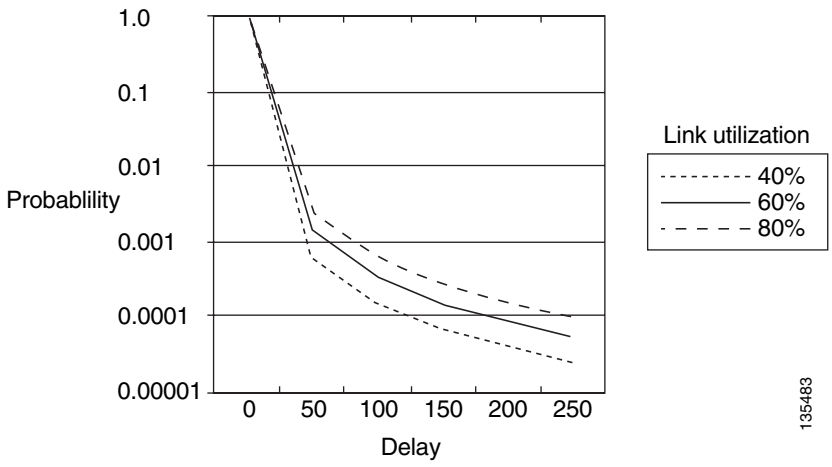
- The number of sources in the network
- The number of hops between the sources and the receivers
- The amount of video traffic carried on network links

Burst accumulation may be characterized by means of probability analysis. A typical burst-accumulation analysis shows the probability of a burst of a particular size based on the number of sources, the number of hops between the sources and the receivers, and the amount of video traffic carried on network links. A burst results in either (1) network jitter, if the router has enough buffering for the burst; or (2) a packet drop, if there is not enough buffering to handle the burst.

Figure 3-29 provides an example of what a set of burst-accumulation curves look like. (This is an example only and does not represent the data from an actual simulation.) In this example, the number of hops and the number of video sources have been fixed, with separate curves for different values of video link utilization. Note that as the probability decreases, the maximum delay increases. When probability curves such as these are mapped to network design constraints, the probabilities can be mapped to the maximum allowed end-to-end drop rate for a class of traffic, and the delay can be mapped to the maximum amount of jitter that can be expected for one or more flows within a class of traffic. For video, the maximum jitter number has two implications for the transport network and for the video STB:

- The network must have enough buffering to buffer worst-case flows. If there is not enough buffering, the large bursts result in packet loss instead of delay.
- The video STBs must have a large enough jitter buffer to hold the maximum burst size.

Figure 3-29 Example Burst-Accumulation Curves



When burst accumulation is applied to video, the low allowed drop rate for video (10^{-6}) should be mapped to the same probability value on a burst-accumulation probability curve. From Figure 3-29 on page 3-53, this low probability is associated with a relatively high maximum delay. If the probability curves were based on real data, the STBs would need 250 msec of buffering to make up for network jitter to a probability of 10^{-5}. It would also mean that the network would need to provide 250 msec of buffering for these worst-case flows.

In current video deployments, the effects of burst accumulation are dramatically reduced by the fact that there are very few sources of video in the network. In current deployments, the sources of video for VoD services are video servers that are located in video headends. The video servers in each headend stream video only to the STBs served by that headend. In addition, the sources of video for broadcast video services are typically located in a single super headend as well as in local headends. The result is that each STB receives broadcast video and VoD streams from at most two locations in the network.

However, burst accumulation may become more of a factor for video services in the future, as diverse VoD and broadcast video content is distributed to VoD servers and broadcast encoders located at multiple points in the network. When video streams destined to a group of STBs can originate from many different locations in the network, video streams from many different sources may converge at multiple locations in the network. In such an environment, both the jitter buffers on STBs, as well as the amount of buffering available in routers in the network, will need to increase.

Broadcast Video vs. Video on Demand

The QoS requirements for video do not change depending on the service with which the video is associated. For example, the allowed drop rate (10^{-6}) and maximum jitter (200 msec) allowed for both broadcast video and VoD services are the same.

Even though the QoS requirements for these two services are the same, the availability requirements typically are not. As described in Service Availability, page 2-14, the availability requirements for a broadcast video service are typically higher than those of a VoD service. In addition, High Bandwidth, page 2-12, explains why the amount of bandwidth consumed by VoD services is typically much higher than that of broadcast video services in aggregation and distribution networks. Because of the different availability and bandwidth requirements associated with both video services, service providers may decide to reduce the cost of the video transport network by not providing as much backup bandwidth for VoD services as for broadcast video services. When transport networks are designed in this way, a network failure should result in reduced capacity of the VoD service, while not affecting the broadcast video service.

VoD Admission Control, page 3-60, describes the video admission control (VAC) function used in Release 1.1 of the solution. When this functionality is used in the network, a network failure that reduces the amount of transport capacity for video results in the admission control function accepting fewer VoD requests than under normal circumstances. This functionality also results in the failure of existing VoD sessions if the number of existing sessions is greater than the capacity the network can support in its degraded state.

Even with VAC, after a reconvergence event the links carrying video become congested for a period of time if the failover path does not support as much bandwidth as the primary path. This behavior results from a delay—between the time the network reconverges and the time the RSVP state is refreshed—during which the new path for VoD flows is taken into account. QoS can be used to prevent the congestion due to excess VoD flows from affecting the broadcast video service. The drop precedence characteristic of the AF PHB can be used to ensure this behavior in the event of a network failure.

The solution has implemented a VoD priority queueing mechanism that may help users until VAC is available. (For details, see Configuring QoS on DER1, page 4-11.) QoS can be configured to ensure that in the event of a link failure that causes reduced video capacity, only VoD flows are affected. The drop precedence characteristic of the AF PHB can be used to ensure this behavior in the event of a network failure.

Drop precedence associated with the DiffServ AF PHB is implemented in the solution architecture by marking all broadcast video traffic with DSCP value AF41, and marking VoD traffic with DSCP values AF42 and AF43 (high- and low-priority packets, respectively). This marking can be done either by the VoD servers and real-time encoders, or by the service router for VoD servers and encoders that do not support DiffServ marking capabilities.

The two DiffServ drop-precedence behaviors are configured by configuring separate queue thresholds for VoD and broadcast traffic on the weighted queue configured for the AF PHB. Queue thresholds set a limit on the effective queue length for a particular class of traffic that is less than the size of the physical queue. Queue-threshold algorithms are run when packets are received at an egress interface before the packets are entered into the output queue. Threshold algorithms can provide simple algorithms such as tail drop or more complex algorithms such as weighted random early discard (WRED). A tail-drop algorithm compares the current queue length to the length of the threshold configured for a particular class of traffic and drops the packet if the current queue length is greater than the configured threshold. Video packets are not transmitted by means of reliable transport protocols that implement congestion-avoidance mechanisms such as TCP/IP. Consequently, simple threshold algorithms such as tail drop should be used for video, because a WRED algorithm may cause video packets to be dropped even when the configured queue limit is not reached.

To ensure that VoD packets are dropped before broadcast video packets in the event of link congestion, a queue threshold is configured for packets marked with AF42 and AF43. The size of this threshold should be the expected ratio of VoD traffic to all video traffic (VoD + broadcast) on the egress link multiplied by the configured queue length. In the distribution network, the ratio of VoD traffic to all video traffic is often between 50% and 80%. If a link ever gets congested with video traffic because of an unexpected network failure, the queue threshold configured for VoD ensures that VoD packets are dropped before they are entered into the output queue.

Voice plus Video Signaling

Both voice and video services use IP-based signaling to set up and tear down subscriber-initiated sessions. For voice services, Session Initiation Protocol (SIP) is often used to set up and tear down telephone calls between subscribers. For VoD services, Real Time Streaming Protocol (RTSP) is often used to set up sessions to a VoD server that streams on-demand content. The subscriber-initiated signaling protocol used to change channels for broadcast video services is IGMP.

Both voice and video signaling require better than best-effort treatment in order to have an effective service. Drops of signaling packets delay session setup. Since RTSP and SIP normally use TCP as a reliable transport protocol, the additional delay is caused by dropped packets within the period of a TCP retransmission window. The service that is most affected by drops of signaling packets is broadcast video. This is because channel-change latency has the most stringent requirements of the three services described, and IGMP does not include a reliable transport method.

To ensure that voice and video session-setup latency is not adversely affected by interface congestion, voice and video signaling are scheduled by means of a class selector PHB. The recommended DiffServ code point (DSCP) to use for voice and video signaling is CS3. On the AR and DER, the class selector PHB is implemented by means of a weighted scheduling algorithm. To ensure that signaling packets are not dropped in the event of congestion, the weight configured on the queue should be greater than the maximum bandwidth expected for voice and video signaling traffic under normal operating conditions.

QoS in the Aggregation/Distribution Network

In the solution architecture, downstream packet scheduling in the aggregation and distribution networks is implemented by means of line-card-based scheduling algorithms to implement the DiffServ PHBs recommended for the voice, video, and Internet access services. (For discussions of the DiffServ PHB and line-card-based scheduling algorithms used for Internet access, voice, video, and voice and video signaling, respectively, see Internet Access, page 3-51; Voice, page 3-51; Video, page 3-52; and Voice plus Video Signaling, page 3-55.)

Based on the DiffServ DSCP values and associated PHBs for each of the four traffic classes listed above, there is an implied assumption that line cards in the aggregation and distribution networks should support four queues (one priority, three weighted) as well as one threshold to differentiate broadcast video from VoD traffic. Although some of the line cards used in the solution transport architecture support only three queues, this in fact does not turn out to be a problem, because the QoS architecture carries video traffic as well as voice plus video signaling in two weighted queues. Both video and voice plus video signaling use the AF PHB, both classes of traffic can be scheduled by using the same queue on the line card without adversely affecting either class of traffic. Combining both classes in the same queue also simplifies configuration, because queue weights need to be configured for only two weighted queues.

Table 3-7 on page 3-57 provides the recommendations for line card configuration using the DiffServ recommendations described in Internet Access, page 3-51; Voice, page 3-51; Video, page 3-52; and Voice plus Video Signaling, page 3-55.

Note Some of the broadcast video and video on demand traffic classes shown the table are relevant only in the downstream direction. Consequently, the queue weight recommendation shows different values for the downstream and upstream directions.

In addition to DiffServ-based scheduling, the aggregation router sets the 802.1p value of packets being sent on aggregation links according to the DSCP value in each packet. Table 3-7 on page 3-57 also provides the recommendations for marking the 802.1p value in the Ethernet header based on an IP packet's DSCP value.

If the density of the DSLAM is such that the Ethernet uplink can become congested, the DSLAM **must** include upstream scheduling functionality. Since Ethernet-capable DSLAMs forward Ethernet frames by means of MAC-layer switching, they typically implement QoS on the Ethernet uplink by using MAC-layer classification techniques. This is done either by (1) associating the incoming ATM VC of an upstream packet with a service and an associated QoS scheduling class, or (2) or by using the 802.1p marking on the packet to associate the packet with a specific scheduling class. DSLAMs compliant with the solution's QoS architecture **must** be capable of associating the incoming ATM VC of an upstream packet with a service and an associated QoS scheduling class. DSLAMs compliant with the solution's QoS architecture **should** be capable of using the 802.1p marking on upstream packets, to associate them with a specific scheduling class. Note that this second form of classification on the DSLAM implies that the RG **should** be capable of marking the 802.1p value of upstream Ethernet frames according to the service with which the RG associates a packet.

Table 3-7 Recommendations for Configuring Line Cards for Access/Aggregation Networks

Service	DiffServ PHB	DiffServ DSCP Value	Line Card Queue	Queue Weight	Queue Threshold
Broadcast video	Assured Forwarding (AF)	AF41	Weighted (1)	80% downstream,[1] 20% upstream[2]	N/A
VoD		AF42, AF43			*VoD*/(*VoD* + *Broadcast*) * *Queue_Length*
Voice + video signaling	Class Selector (CS)	CS3			N/A
Voice	Expedited Forwarding (EF)	EF	Priority	N/A	
Internet access	Default	0	Weighted (2)	UBR	

1. The downstream queue weight for video is a recommendation that assumes all video traffic consumes no more than 70% of the physical link bandwidth for the link being configured. If the expected ratio of video traffic to total link bandwidth is significantly less, then a lower queue weight may be used.
2. The upstream queue weight for video takes into account only voice plus video signaling, because broadcast video and VoD traffic is unidirectional. The actual value used for the queue weight may vary, depending on the expected ratio of signaling traffic compared to total link bandwidth.

QoS in the Access Network

The RG is located at the DiffServ administrative boundary in the upstream direction. While the RG is managed by the service provider, the home network typically is not. Consequently, the RG must associate packets that arrive from ports attached to the home network with a service and its associated QoS. Because the RG is at the edge of the SP's DiffServ domain, it **should** be capable of writing a configurable DiffServ code point to each upstream packet according to the service with which it has associated that packet, using the service classification rules described in EtherType Service Mapping in a Layer 2 RG, page 3-42. For HAGs that implement DSCP marking, the DSCP value with which the RG marks each packet based on service classification follows the conventions illustrated in Table 3-8 on page 3-58.

The solution provides two potential methods for implementing packet scheduling in the access network. The method used depends on the capabilities of the DSLAM and the HAG. ATM Layer Scheduling, below, describes the required method of packet scheduling based on the ATM layer scheduling methods. MAC/IP Layer Scheduling, page 3-59, describes an additional optional method of packet scheduling, based on MAC/IP-layer scheduling, that DSLAMs and HAGs may use.

ATM Layer Scheduling

Both the DSLAM and the RG include ATM Segmentation and Reassembly (SAR) functionality. The ATM SAR function encapsulates IP packets in ATM AAL-5 frames and segments each frame into ATM cells. The ATM SAR function that is incorporated in HAGs and DSLAMs is typically capable of implementing the cell-scheduling algorithms required for most of the ATM classes of service defined in the ATM traffic management specification. Consequently, the solution QoS architecture requires support for ATM-layer Quality of Service (QoS) for scheduling across the DSL link.

The use of ATM-layer QoS in the RG means that the RG **must** be capable of mapping the service with which it associated with each upstream packet to the appropriate ATM Class of Service (CoS). The use of ATM-layer QoS in the DSLAM means that the DSLAM **must** be capable of mapping the incoming

VLAN of downstream packets and the service with which that VLAN is associated to the appropriate ATM CoS on the DSL line. In addition, the DSLAM **should** be capable of mapping the incoming 802.1p value of downstream packets to the appropriate ATM CoS. Note that this second form of classification on the DSLAM relies on the AR to set the 802.1p value in Ethernet frames before they are sent on the aggregation links to the DSLAM.

When ATM scheduling is provided on the DSL line by means of multiple VCs with an ATM SAR function, it provides both scheduling and a link fragmentation and interleaving (LFI) functionality. LFI may be needed for voice services when the amount of upstream bandwidth available on the DSL line is below 400 kbps. LFI is needed in this case because the serialization delay for a single 1500-byte packet could exceed 30 msec on the DSL line (30 msec is about half of the end-to-end jitter budget for a voice service). When multiple ATM VCs are configured on the DSL line, the ATM SAR function breaks each IP packet into a sequence of 53-byte cells and then schedules each cell by means of ATM-based scheduling algorithms. This process ensures that the maximum delay that may be experienced by a voice packet because of the serialization of video or data packets is 1 msec on a 400-kbps DSL link.

Table 3-8 shows the mapping between traffic classes, DiffServ Per Hop Behavior (PHB), and ATM-based scheduling through Class of Service (CoS). Triple-Play QoS Analysis, page 3-51, provides details on the analysis used to determine the mapping used in the solution between services and DiffServ PHBs.

Table 3-8 DiffServ-to-ATM CoS Mapping

Traffic Class	DiffServ PHB	DiffServ DSCP Value	ATM CoS	SCR Value
Broadcast video	Assured Forwarding (AF)	AF41	VBR	Expected bandwidth (bps) * 1.25
VoD		AF42		
Video signaling	Class Selector (CS)	CS3		
Voice	Expedited Forwarding (EF)	EF	CBR	
Voice signaling	Class Selector (CS)	CS3		
Internet access	Default	0	UBR	—

This table also provides a recommendation for configuring the sustained cell rate (SCR) for VBR and CBR virtual circuits (VCs). The expected bandwidth that is used to calculate the SCR for the voice and video VCs can be determined by multiplying the maximum number of voice and video streams by the maximum bandwidth per stream that is expected on the DSL line. Additional bandwidth may also need to be added to take into account voice and video signaling through the VC. Note that the recommended SCR values shown in the table provide about 25% extra bandwidth over what is required to support the expected bandwidth value. This is because the SCR value for CBR and VBR VCs is used to guarantee a minimum rate and also enforce a maximum rate for traffic through that VC. The additional 25% value ensures that the maximum rate enforcement does not degrade the voice and video services during normal operation.

MAC/IP Layer Scheduling

Some DSLAMs and HAGs support the ability to schedule packets by means of DiffServ-based scheduling algorithms. Edge Transport Architecture, page 3-40, describes an optional method that uses 802.1q VLAN tags that the DSLAM and RG can also use to identify the service topology with which each packet on the DSL line is associated. In environments where both the DSLAM and RG support DiffServ-based packet scheduling and 802.1q encapsulations on the DSL line to identify service topology, a single ATM VC can be used between the RG and the DSLAM.

When a single ATM VC is configured between the RG and the DSLAM, the 802.1q marking is used to identify the service topology with which the VC is associated, while either the DSCP value or the 802.1p value is used to classify packets for scheduling. In addition to being able to mark the DSCP value in upstream packets, an RG that supports a single ATM VC configuration **should** support the ability to mark the 802.1p value in upstream packets on the basis of the service classification described in EtherType Service Mapping in a Layer 2 RG, page 3-42.

Table 3-9 shows the mapping between traffic classes, DiffServ PHBs, and DiffServ-based scheduling algorithms on the DSL line. Triple-Play QoS Analysis, page 3-51, provides details on the analysis used to determine the mapping used in the solution between services and DiffServ PHBs.

Table 3-9 DiffServ-to-MAC-Based Scheduling

Service	DiffServ PHB	DiffServ DSCP Value	802.1p Value	Queue	Queue Weight
Broadcast video	Assured Forwarding (AF)	AF41	4	Weighted (1)	80% downstream,[1] 20% upstream[2]
VoD		AF42	2		
Voice + video signaling		AF11	1		
Voice	Expedited Forwarding (EF)	EF	5	Priority	N/A
Internet access	Default	0	0	Weighted (2)	UBR

1. The downstream queue weight for video is a recommendation that assumes all video traffic consumes no more than 70% of the physical link bandwidth for the link being configured. If the expected ratio of video traffic to total link bandwidth is significantly less, then a lower queue weight may be used.
2. The upstream queue weight for video takes into account only voice plus video signaling, because broadcast video and VoD traffic is unidirectional. The actual value used for the queue weight may vary, depending on the expected ratio of signaling traffic compared to total link bandwidth.

When a single ATM VC is used between the DSLAM and the HAG, IP-based link fragmentation and interleaving functionality may be needed on the RG and DSLAM. LFI may be needed for voice services when the amount of upstream bandwidth available on the DSL line is below 400 kbps. LFI is needed in this case because the serialization delay for a single 1500-byte packet could exceed 30 msec on the DSL line (30 msec is about half of the end-to-end jitter budget for a voice service). DSLAMs and HAGs that support the DiffServ-based scheduling and 802.1q-based service-mapping functionality required in single-VC environments **should** also support the ability to implement LFI across the DSL line by means of Multilink Point-to-Point Protocol (MLPPP).

VoD Admission Control

Overview

Video on demand can be challenging to keep up with. If the service is more successful than is forecasted, then the bandwidth consumed between the subscribers and the VoD server complex can become oversubscribed. For example, if we assumed a peak concurrency of 20% of all STBs watching on-demand content at the same time, then a central office supporting 10,000 subscribers would need 2,000 streams at peak, or roughly 4 to 7 Gbps, depending on which codec is used to support standard definition. Add high-definition on-demand content, and the bandwidth demand can be quite large.

What happens when demand rises above the peak concurrency that one assumed in designing the network or VoD service capacity? If a particular VoD server complex cannot service a particular request, the request may get rerouted to another VoD server complex that has capacity. If the network capacity over a link or set of links is exceeded, allowing too many VoD sessions to be set up could cause an excessive packet-drop rate for all the video streams, resulting in many subscribers perceiving an outage!

Instead, an integrated network-based admission control can deliver a “could not be serviced at that time” signal to the requesting STB if a video session cannot be supported because of oversubscription anywhere in the network or service. While no one likes a busy signal, the possibility of a mass degradation of the VoD service is much worse! It is easy to imagine that the service could “know” which streams are ending soon, and, thus could provide more-sophisticated busy messages—giving the subscriber more choices for a delayed start of the VoD stream, alternative video service offerings, commerce opportunities, and the like.

Integrated On-Path and Off-Path Admission Control

A VoD admission control (VAC) solution must be able to take into account complex network topologies that have redundant and load-sharing paths in the transport network, as well as access-link utilization or business policies that may be enforcing other types of constraints on the subscriber’s service. To do this, the network’s routers, in coordination with policy managers and on-demand servers or managers, need to perform a collective admission control function, called Integrated VoD Admission Control (IVAC).

First, Cisco has developed an in-path method to perform admission control for the complex core and distribution network topologies found in next-generation network (NGN) designs. This method uses RSVP for in-path signaling, sent by the VoD server or a component on its behalf before the VoD session is started. The RSVP message traverses the same exact path the VoD session uses, thus tracking in real time any changes in the complex network topologies in the core and distribution layers. Along the path, Cisco IP routers perform a bandwidth accounting function, either allowing the session or denying it if bandwidth is not available for that VoD stream. Having IP, or Layer 3, routing present on every network element, from the VoD server complex to the AR in the central office makes this in-path admission control possible.

Second, to prevent a video stream from being sent to an STB if the access link to a subscriber's home doesn't have enough capacity to carry the stream, the VoD server or a network component in the path mechanism sends a request to an off-path component. This component may be a policy server that is keeping track of the access network, usually a simple and static topology. The policy server can check to see if the access link has enough unused bandwidth, as well as check for business policies that may or may not allow the stream to be supported, in order to allow or deny the session at that time. An off-path component is not recommended as a way to perform admission control for the core and distribution layers, where tracking real-time any changes in the complex network topologies is difficult

at best. Consequently, the combination of in-path admission control with an off-path policy server at the edge is the most reliable and efficient way for an admission control solution to decide whether or not a new VoD stream should be allowed to a specific subscriber.

The VAC and related bandwidth accounting, when added to a DiffServ QoS architecture that defines packet marking and scheduling behaviors, can be used to ensure that the video streams allowed to be set up can meet the required 10^{-6} packet-drop rate. Combining the different admission control technologies with DiffServ QoS allows Cisco to offer a simplified queueing strategy and have all the video traffic shared the same queue. This avoids complex and very costly centralized, hierarchical queueing strategies.

Implementing and Configuring the Solution

This chapter begins with tasks common to the 10-GE ring and hub-and-spoke topologies used in the Cisco Cisco Wireline Video/IPTV Solution:

- Common Tasks, page 4-1

It then presents the details of configuring each topology:

- Configuring the 10-GE Ring Topology, page 4-5
- Configuring the Hub-and-Spoke Topology, page 4-32

Note For command references and best practices for the Layer 3 switches used, see the following:

— Cisco 7600 Series Routers:

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

— Cisco Catalyst 6500 Series Switches:

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

Common Tasks

The following common tasks have general applicability and should be considered early in the implementation process:

- Configuring SSM Mapping with DNS Lookup
- (Optional) Enabling Option 82 on the ARs

Configuring SSM Mapping with DNS Lookup

As discussed in Multicast, page 3-15, Source Specific Multicast (SSM) is used simplify the configuration of a multicast network, and is common to both topologies. The solution uses edge devices that do not support IGMPv3. The switches accept IGMPv2 messages and convert these to IGMPv3 by resolving the source IP address of the multicast group by means of either a static mapping or a DNS resource record. This solution uses a DNS lookup method.

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

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

The following tasks are presented:

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

Configuring DNS Servers

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

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

Step 2 Configure the following parameters, as appropriate:

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

b. All other multicast IP addresses from the same source

c. The multicast domain

d. The timeout (optional)

)

Configuring SSM Mapping on All Switches

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

Step 1 Enable multicast routing.

```
ip multicast routing
```

Step 2 Enable SSM mapping.

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

Note Although the document Source Specific Multicast (SSM) Mapping, referenced above, states that the **ip igmp ssm-map enable** command needs to be configured only on switches that are connected to IGMP clients, it was found that this led to inconsistent recovery times during solution network failure and recovery tests. A majority of the time, recovery was fast, but occasionally recovery times were poor. It was found that configuring this command on the headend switch, recovery times were more consistent, although slightly slower than the best recovery times when SSM mapping was not configured on the headend switch.

Step 3 Enable SSM on the edge switches. The default IP address range for SSM is 232.0.0.0 to 232.255.255.255.

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

Configuring the Edge Switches for DNS Queries

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

Step 1 Configure the domain for multicast video.

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

Step 2 Configure the IP address of the first DNS.

```
ip name-server 10.1.10.10
```

Step 3 Configure the IP address of the second DNS.

```
ip name-server 10.1.11.10
```

(Optional) Enabling Option 82 on the ARs

The DHCP relay agent information option (option 82) enables a Dynamic Host Configuration Protocol (DHCP) relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP address or other parameter-assignment policies.

Note For more information, see "DHCP Option 82 Support for Routed Bridge Encapsulation" at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_white_paper09186a0080087ad8.shtml

The default behavior on the switches used in the solution is to reset the option 82 field in DHCP packets. If the gateway address is set to all zeros in the DHCP packet and the relay information option is already present in the packet, the DHCP relay agent discards the packet. Consequently, where DSLAMs are configured to insert option 82 in the DHCP packets from the set-top box (STB), this default behavior must be overridden. This is done on each aggregation router (AR) connected to a DSLAM that is configured to support option 82, with the following global command:

ip dhcp relay information trust-all

This configures all interfaces on the router as trusted sources of the DHCP relay information option.

Configuring the 10-GE Ring Topology

This section presents the following major topics:

- Introduction
- Common Task: Configuring MPLS for HSD Service
- Configuring DER1
- Configuring DER2
- Configuring AR1
- Configuring AR2
- Configuring AR3

Introduction

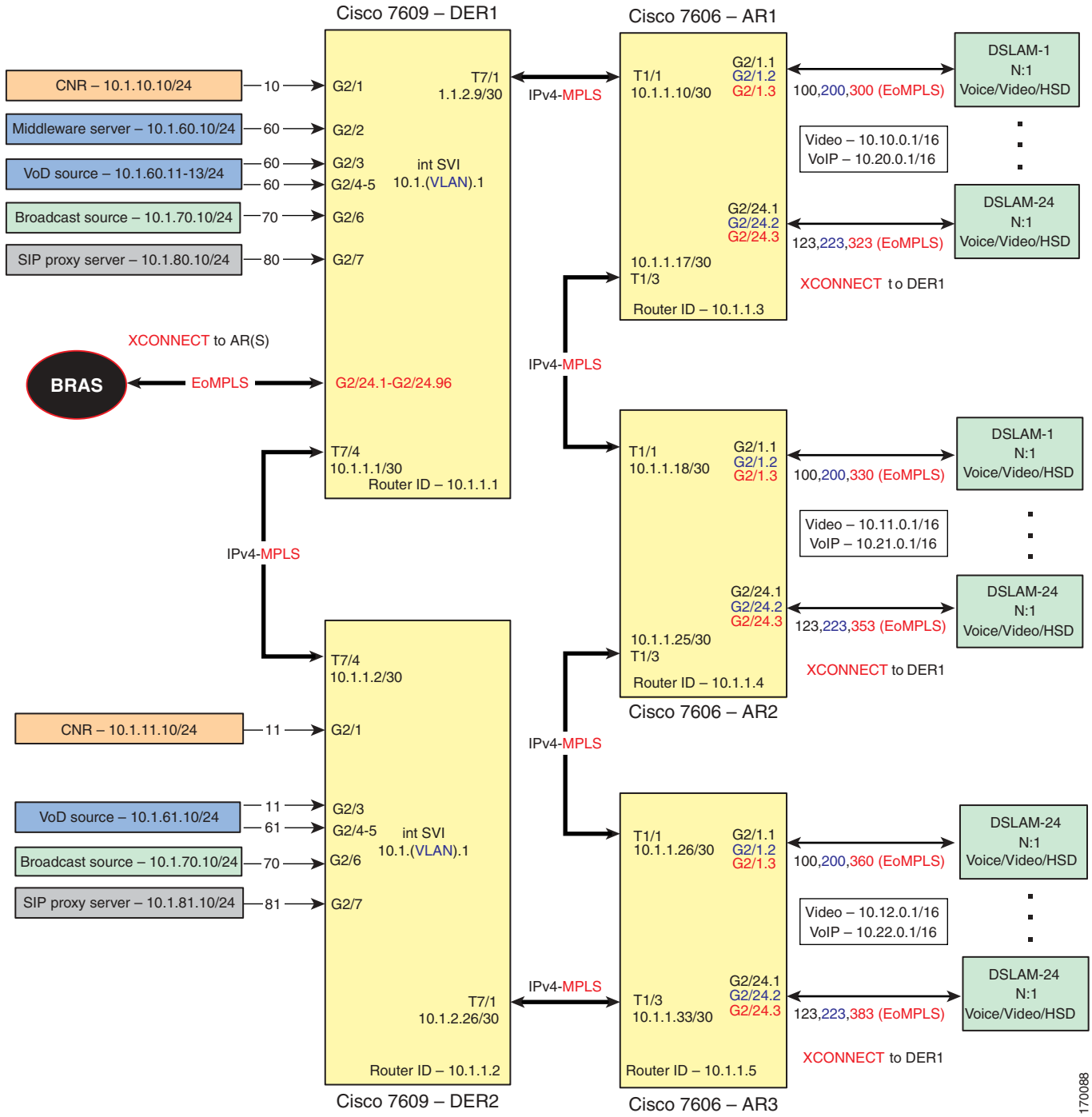
Figure 4-1 on page 4-6 illustrates the 10-GE ring topology used in the solution. (See Configuration 1: 10-GE Layer 3 Ring, page 3-38.) All video sources and VoIP servers are connected to ports on the distribution edge routers (DERs). With two DERs in the topology, we can provide source, node, and network redundancy for each of the aggregation routers (ARs). Policy maps are applied to the DER ingress ports in order to mark the DSCP values of the different service types. In this example, only DER1 is connected to a middleware server.

Traffic is routed among DERs and ARs through 10-GE bidirectional transport links. Transport links are Layer 3 ports, and carry both IPv4 and Multiprotocol Label Switching (MPLS) packets. Video and VoIP traffic is routed over the transport links as native IPv4 packets. HSD is routed over the same transport links, but is encapsulated in MPLS through Ethernet over MPLS (EoMPLS) point-to-point connections. A single OSPF process is needed for the routing protocol.

The topology assumes that each DSLAM is configured to use the N:1 model for the three services—video, VoIP, and high-speed data (HSD). Therefore, each DSLAM is assigned three unique VLANs, one VLAN per service. (Note that VLANs have local significance, and are not bridged between DSLAMs attached to a common AR.)

The residential gateways (RGs) used in the test bed provided service mapping based on physical ports, as described in Physical Port-Based Traffic Mapping for the Multi-VC and VLAN Access Models, page 3-43.

Figure 4-1 10-GE Ring Topology



The switches in Figure 4-1 use the line cards, hardware versions, and IOS versions listed in Table 4-1 on page 4-7.

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

Switch	Module	Line Card	Hardware Version	IOS Release	Submodule	Hardware Version
DER1, DER2	1	WS-X6724-SFP[1]	2.3	12.2(18)SXF2	WS-F6700-DFC3BXL	5.2
	2					
	5	WS-SUP720-BASE	3.1		WS-F6K-PFC3BXL	1.2
					WS-SUP720 (MFSC)	2.1
	7	WS-X6704-10-GE	2.2		WS-F6700-DFC3BXL	4.0
AR1	1	WS-X6704-10GE	2.2		WS-F6700-DFC3BXL	4.0
	2	WS-X6724-SFP	2.3		WS-F6K-DFC3BXL	5.2
	5	WS-SUP720-3BXL	4.3		WS-F6K-PFC3BXL	1.6
					WS-SUP720 (MFSC)	2.3
AR2	1	WS-X6704-10GE	2.2		WS-F6700-DFC3BXL	4.0
	2	WS-X6724-SFP	2.3		WS-F6700-DFC3BXL	5.2
	5	WS-SUP720-3BXL	4.3		WS-F6K-PFC3BXL	1.6
					WS-SUP720 (MFSC)	2.3
AR3	1	WS-X6704-10GE	2.2		WS-F6700-DFC3BXL	4.0
	2	WS-X6724-SFP	2.3		WS-F6700-DFC3BXL	5.2
	5	WS-SUP720-3BXL	4.3		WS-F6K-PFC3BXL	1.6
					WS-SUP720 (MFSC)	2.3

1. WS-X6748-GE-TX line cards, version 2.2, were also tested. To simplify the configuration details, they are not shown here.

Table 4-2 on page 4-8 lists VLANs, their descriptions (service types), and IP addresses, for the DER and ARs in Figure 4-1 on page 4-6. A range of VLANs is required for each AR, with one VLAN per DSLAM required to support EoMPLS for HSD.

Note To simplify the configuration, only 11 DSLAMs per AR are shown.

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

Node	VLAN	Description	IP Address
DER1	10	Management: CNR (DHCP, DNS, FTP, TFTP, Syslog servers)	10.1.10.1/24
	60	VoD sources and middleware	10.1.60.1/24
	70	Digital broadcast sources	10.1.70.1/24
	80	VoIP—SIP proxy server	10.1.80.1/24
	300–323	HSD VLAN range for DSLAMs connected to AR1	Bridged
	330–353	HSD VLAN range for DSLAMs connected to AR2	
	360–383	HSD VLAN range for DSLAMs connected to AR3	
	Routed	Transport to/from DER2	10.1.1.1/30
		Transport to/from AR1	10.1.1.9/30
		To/from AR2	10.1.1.17/30
DER2	11	Management: CNR (DHCP, DNS, FTP, TFTP, Syslog servers)	10.1.11.1/24
	61	VoD sources	10.1.61.1/24
	70	Digital broadcast sources	10.1.70.1/24
	81	VoIP—SIP proxy server	10.1.81.1/24
	Routed	To/from DER1	10.1.1.2/30
		To/from AR1	10.1.1.34/30
	Routed (subinterface)	HSD traffic—to/from BRAS	Bridged
AR1	Routed	To/from DER1	10.1.1.10/30
		To/from AR2	10.1.1.17/30
	Routed (subinterface)	Subscriber video (N:1)	10.10.0.1/16
			10.20.0.1/16
		High-speed data (N:1) to/from UTStarcom DSLAM (EoMPLS)	Bridged (VLANs 300–323)
AR2	Routed	To/from AR1	10.1.1.18/30
		To/from AR3	10.1.1.25/30
	Routed (subinterface)	Subscriber video (N:1)	10.11.0.1/16
			10.21.0.1/16
		High-speed data (N:1) to/from UTStarcom DSLAM (EoMPLS)	Bridged (VLANs 330–353)
AR3	Routed	To/from AR1	10.1.1.26/30
		To/from DER2	10.1.1.33/30
	Routed (subinterface)	Subscriber video (N:1)	10.12.0.1/16
			10.22.0.1/16
		High-speed data (N:1) to/from UTStarcom DSLAM (EoMPLS)	Bridged (VLANs 360–383)

Table 4-3 lists the parameters used to configure the residential gateway (RG) tested in this topology.

Note See RG Functions, page 3-41, and Appendix C, "Configuring Ericsson DSL Equipment."

Table 4-3 RG Configuration Parameters

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

1. Permanent virtual connection
2. Virtual path identifier
3. Virtual connection identifier
4. Peak cell rate
5. Sustained cell rate
6. Maximum burst size
7. The *x* corresponds to the AR number 1, 2, or 3 in the corresponding VLAN

Common Task: Configuring MPLS for HSD Service

Because EoMPLS is used on the trunk to the BRAS (as well as between the ARs and the DSLAMs), MPLS is required to support high-speed data (HSD) on the transport links between the DER and AR nodes.

Note For more information, see "Ethernet over MPLS for the Cisco 7600 Series Internet Routers" at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121ex/121ex8a/eompls9.htm

Table 4-4 lists the loopback addresses used for MPLS. Loopback3 is used throughout for this purpose.

Table 4-4 Loopback Addresses for MPLS

Node	Loopback3 Address
DER1	10.1.254.1/32
DER2	10.1.254.2/32
AR1	10.1.254.3/32
AR2	10.1.254.4/32
AR3	10.1.254.5/32

Do the following in global configuration mode to enable MPLS on all nodes. (Loopback interfaces are later established on each node for MPLS in interface configuration mode.)

Step 1 Configure the default MPLS LDP protocol as LDP. Configure this command in global configuration mode to set all MPLS interfaces to LDP.

```
mpls label protocol ldp
```

Step 2 Configure MPLS to advertise by means of the loopback interface.

```
tag-switching advertise-tags for LOOPBACK
tag-switching tdp router-id Loopback3 force
```

Step 3 Configure an access list to identity non-MPLS traffic. By default, all IPv4 packets are transmitted over MPLS. To prevent video and VoIP traffic from being routed over MPLS configure the following.

```
no tag-switching advertise-tags
ip access-list standard LOOPBACK
 permit 10.1.254.0 0.0.0.255
```

Step 4 To complete the configuration, proceed to “Establishing 10-GE Interfaces for Transport” for each node in the ring.

Configuring DER1

This section addresses the configuration required on the switch labeled DER1 in Figure 4-1 on page 4-6, to route multiple services from that switch to the ARs.

See Configuring DNS Servers, page 4-2.

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

This section addresses the following:

- Configuring QoS on DER1
- Establishing and Configuring Interfaces on DER1
- Configuring OSPF Routing for Video and Voice Traffic on DER1

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

Configuring QoS on DER1

This section presents the following topics:

- Overview of QoS on a Cisco 7600 Series and Cisco Catalyst 6500 Series
- Configuring Marking and Classification on DER1
- Configuring Mapping on DER1

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

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

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

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

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

Configuring Marking and Classification on DER1

Do the following to enable marking and classification on DER1.

Step 1 Enable QoS in global configuration mode.

```
mls qos
```

Step 2 Configure ingress multicast replication mode and disable automatic detection of the replication mode (enabled by default).

```
mls ip multicast replication-mode ingress
```

Note Ingress replication of multicast is required on both DER1 and DER2.

Step 3 Create access lists to identify the different service types in the network

```
ip access-list extended acl_VoD_and_SIP_signaling
 permit tcp 10.1.60.0 0.0.0.255 any
 permit tcp 10.1.61.0 0.0.0.255 any
 permit tcp 10.1.80.0 0.0.0.255 any
 permit tcp 10.1.81.0 0.0.0.255 any

ip access-list extended acl_video_VoD
 permit udp 10.1.60.0 0.0.0.255 any
 20 permit udp 10.1.61.0 0.0.0.255 any

ip access-list extended acl_video_broadcast
 permit udp 10.1.70.0 0.0.0.255 232.0.0.0 0.255.255.255
```

Step 4 Create class maps for the access lists created in Step 2.

```
class-map match-all class_VoIP
 match access-group name acl_VoIP
class-map match-all class_VoD_and_SIP_signaling
 match access-group name acl_VoD_and_SIP_signaling
class-map match-all class_video_broadcast
 match access-group name acl_video_broadcast
class-map match-all class_video_VoD
 match access-group name acl_video_VoD
```

Step 5 Create a policy map to set the DSCP values of the different classes created in Step 4.

```
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoD_and_SIP_signaling
   set dscp cs3
  class class_video_broadcast
   set dscp af41
  class class_video_VoD
   set dscp af42
  class class_VoIP
   set dscp ef
```

Step 6 Apply the policy map from Step 4 to the ingress interfaces by using the following command.

```
service-policy input setDSCP
```

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

Step 7 To maintain the DSCP marking applied at the network ingress interface, configure all noningress transport interfaces to trust the incoming DSCP markings.

```
mls qos trust dscp
```

Configuring Mapping on DER1

For background, see the following:

- QoS Packet Marking

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

- Understanding and Configuring QoS

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_18a/config/qos.htm#59874

Do the following to configure mapping on DER1.

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

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

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

DER1# **show mls qos maps dscp-cos**

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

This table shows the following default mapping (36 corresponds to DSCP AF41):

Service Type	DSCP	CoS
Broadcast video	36	4

Step 2 Change the Cisco 7600 and Cisco Catalyst 6500 DSCP-to-CoS mapping for broadcast video to match the specifications of the solution. (The other default mappings for other services do not need to be changed.)

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

Service Type	DSCP	CoS
Broadcast video	36	2

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

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

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

```
DER1# show mls qos maps dscp-cos

DSCP-CoS Mapping Table (dscp = d1d2)
d1 : d2 0  1  2  3  4  5  6  7  8 9
0 : 00 00 00 00 00 00 00 00 01 01
1 : 01 01 01 01 01 01 02 02 02 02
2 : 02 02 02 02 03 03 03 03 03 03
3 : 03 03 04 04 04 04 02 04 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
```

Establishing and Configuring Interfaces on DER1

Refer to Figure 4-1 on page 4-6.

This section addresses the following:

- Establishing VLANs for Services on DER1
- Establishing an EoMPLS Interface to the BRAS
- Establishing 1-GE Interfaces for Servers and Management on DER1
- Establishing 10-GE Interfaces for Transport on DER1

Establishing VLANs for Services on DER1

Before the 1-GE interfaces can be configured, VLANs for the various services must be created. (See Table 4-2 on page 4-8.)

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

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

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

```
vlan 10
name VLAN_10_Management
```

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

```
interface Vlan10
 description Management VLAN (Middleware, DNS, DHCP, etc)
 ip address 10.1.10.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

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

```
load-interval 30
```

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

Unicast Video Aggregation

```
vlan 60
name VLAN_60_Unicast_Video


interface Vlan60
 description VoD server VLAN (Unicast Video)
 ip address 10.1.60.1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

VoIP

```
vlan 80
name VLAN_80_VoIP


interface Vlan80
 description VoIP gateway VLAN
 ip address 10.1.80.1 1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

Step 2 Establish a VLAN for multicast video aggregation.

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

```
vlan 70
name VLAN_70_Multicast_Video
```

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

```
interface Vlan70
 description Broadcast video source VLAN (Multicast Video)
 ip address 10.1.70.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

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

```
ip pim sparse-mode
```

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

```
load-interval 30
```

Establishing an EoMPLS Interface to the BRAS

Do the following to establish an Ethernet over Multiprotocol Label Switching (EoMPLS) interface to the broadband remote access server (BRAS).

Note Connections to multiple BRASs are likely. This example illustrates only one connection.

Step 1 Establish a 1-GE interface.

```
interface GigabitEthernet2/24
 description To/From BRAS for 10GE Ring EoMPLS
 no ip address
```

Step 2 Configure interface link detection options, such as **carrier-delay** (to reduce the time to detect a link failure), and **dampening** (to minimize the effects of flapping links).

```
carrier-delay msec 0
dampening
```

Step 3 Change the load interval from the default of 300.

```
load-interval 30
```

Step 4 Configure Quality of Service (QoS) on the interface.

Note For a detailed discussion, see Step 2 of Configuring QoS on DER1, page 4-11.

```
wrr-queue bandwidth 64 255 0
wrr-queue queue-limit 40 50 0
wrr-queue threshold 2 80 100 100 100 100 100 100 100
wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
no wrr-queue random-detect 2
wrr-queue cos-map 1 1 0 1
wrr-queue cos-map 2 2 3 4 6 7
```

Step 5 Configure EoMPLS for HSD to the ARs.

a. Establish a subinterface on AR1 for video services for DSLAM1. A subinterface is a Layer 3 port with a VLAN association. DSLAM1 will use VLAN 300 for video services. The dot1q ID is the same as the VLAN ID. (See Table 4-2 on page 4-8.)

```
interface GigabitEthernet2/24.1
 description HSD to/from DSLAM1 on AR1
 encapsulation dot1Q 300
```

Note No service policy is applied here. By default, HSD is treated as “untrusted” (DSCP = 0).

b. Bind the attachment circuit to a pseudowire VC (in this case, the VLAN just established), using the **xconnect** *peer_router_id vcid* **encapsulation mpls** command. The VC maps a tunnel to a subinterface port.

```
xconnect 10.1.254.3 300 encapsulation mpls
```

c. Repeat Step 5a and Step 5b for AR2 and AR3.

```
interface GigabitEthernet2/24.2
 description HSD to/from DSLAM1 on AR2
 encapsulation dot1Q 330
 xconnect 10.1.254.4 330 encapsulation mpls
!
interface GigabitEthernet2/24.3
 description HSD to/from DSLAM1 on AR3
 encapsulation dot1Q 360
 xconnect 10.1.254.5 360 encapsulation mpls
```

d. Repeat Step 5a through Step 5c for the remaining HSD VLANs.

Establishing 1-GE Interfaces for Servers and Management on DER1

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

The following is configured on DER1.

Step 1 Establish an interface.

a. Establish an interface for the Cisco Network Registrar (CNR) primary server.

```
interface GigabitEthernet2/1
 description CNR ingress/egress (DHCP, DNS, TFTP, SysLog)
 no ip address
```

b. Configure the interface as a Layer 2 access port and assign it to VLAN 10.

```
switchport
switchport mode access
switchport access vlan 10
```

c. Configure interface link detection options, such as **carrier-delay** (to reduce the time to detect a link failure), and **dampening** (to minimize the effects of flapping links).

```
carrier-delay msec 0
dampening
```

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

```
load-interval 30
```

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

```
no cdp enable
```

f. Enable PortFast on the interface to bypass the listening and learning states in Spanning Tree Protocol (STP).

Note This allows the interface to move immediately from the blocking state to the forwarding state, rather than waiting for STP to converge.

```
spanning-tree portfast
```

g. Configure the switch to disable any interfaces that are configured for PortFast and receive a Bridge Protocol Data Unit (BPDU).

```
spanning-tree bpduguard enable
```

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

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

```
service-policy input setDSCP
```

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

Kasenna Middeware Server

```
interface GigabitEthernet2/2
 description Kasenna Middleware Server ingress/egress
 switchport
 switchport access vlan 10
```

Kasenna VoD Pump Management Port (Eth0)

```
interface GigabitEthernet2/3
 description VoD Pump ingress/egress
 switchport
 switchport access vlan 60
```

Kasenna VoD Pump (HPN0)

```
interface GigabitEthernet2/3
 description VoD Pump (HPN0) ingress/egress
 switchport
 switchport access vlan 60
```

Kasenna VoD Pump (HPN1)

```
interface GigabitEthernet2/3
 description VoD Pump (HPN1) ingress/egress
 switchport
 switchport access vlan 60
```

Broadcast Server (Multicast)

```
interface GigabitEthernet2/6
 description Broadcast Video ingress/egress
 switchport
 switchport access vlan 70
```

VoIP—SIP Proxy Server

```
interface GigabitEthernet2/7
 description SIP Proxy Server ingress/egress
 switchport
 switchport access vlan 80
```

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

Establishing 10-GE Interfaces for Transport on DER1

The 10-GE trunk interfaces create the ring topology from DER1 through the ARs and back to the DER2. The following is configured on DER1.

Step 1 Establish an interface to and from DER2.

a. Establish the interface.

```
interface TenGigabitEthernet7/4
 description Transport to/from Ring AR1 (TenGig1/1)
 ip address 10.1.1.1 255.255.255.252
```

b. Configure interface link detection options, such as **carrier-delay** (to reduce the time to detect a link failure), and **dampening** (to minimize the effects of flapping links).

Note The **restart** command option is applied on start up to reduce the possibility of routing "black holes" during startup (where upper layers converge before lower layers do).

```
carrier-delay msec 0
dampening 5 1000 2000 20 restart 16000
```

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

```
load-interval 30
```

d. Change the PIM query interval from the default of 30 seconds.

```
ip pim query-interval 100 msec
```

Note It was determined in testing that convergence times improve if the PIM hello interval is less than one second. For more information about the **ip pim query-interval** command, see the following:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123tip3r/ip3_i2gt.htm#wp1069550

e. Enable PIM sparse mode. This is the ingress port for broadcast video traffic, which is multicast addressed. Change the PIM **query-interval** from the default of 30 seconds for PIM fast convergence.

```
ip pim sparse-mode
```

f. Configure OSPF on the transport VLAN interface.

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

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

Step 2 Configure QoS on the interface.

Note The 10-GE transport links from the DER to the ARs require modifications to the transmit queues. There are eight transmit queues, but this solution uses only three. For more information, see "Buffers, Queues, and Thresholds on Catalyst 6500 Series Ethernet Modules" at the following URL:

http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/buffe_wp.htm

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

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

b. Configure the CoS-to-TxQueue mapping on the 10-GE transport interfaces. HSD (CoS = 0) remains in TxQueue1 and VoIP (CoS = 5) remains in TxQueue8. Video is separated into two classes, one class for broadcast video (CoS = 4) and one class for VoD video (CoS = 2). The other three CoS values are associated with TxQueue2.

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

Note TxQueue1 and TxQueue8 use the default mappings. TxQueue2 has three thresholds: Threshold 1 = CoS 1, Threshold 2 = CoS 2, and Threshold 3 = CoS 3, 4, 6, and 7.

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

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

d. Configure the TxQueue thresholds.

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

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

TxQueue2 uses tail drop for queue congestion management. VoD is assigned to the threshold 1 and is dropped once the queue reaches 80% utilization. VoD signaling, network signaling, and broadcast video are assigned to the third threshold 2 and are dropped once the queue reaches 100% utilization.

```
wrr-queue threshold 2 80 100 100 100 100 100 100 100
no wrr-queue random-detect 2
```

e. Configure the bandwidth of the weighted queues.

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

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

f. Configure the size of the weighted queues.

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

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

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

```
mls qos trust dscp
```

Step 3 Establish an interface to and from AR1.

h. Establish the interface to AR1

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

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

Step 4 Configure MPLS on the transport interfaces.

Note Ensure that MPLS is enabled globally. See Common Task: Configuring MPLS for HSD Service, page 4-9.

a. Establish a loopback interface for MPLS.

```
interface loopback 3
 description Loopback interface for MPLS
 ip address 10.1.254.1 255.255.255.255
```

b. Enable MPLS on the transport interface.

```
tag-switching ip
```

c. Set the size of the maximum transmission unit (MTU) to account for the additional packet overhead required for MPLS.

```
mtu 9216
```

Configuring OSPF Routing for Video and Voice Traffic on DER1

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

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

```
router ospf 100
 router-id 10.1.1.1
 log-adjacency-changes
```

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

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

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

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

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

```
timers lsa arrival 100
```

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

d. The following command sets incremental SPF (iSPF) updates for LSA type 1 and LSA type 2 within an area. Enabling iSPF can minimize the affect of SPF changes within an area to only those routers where the change is relevant, thus reducing the time spent calculating SPF.

```
ispf
```

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

```
passive-interface Vlan10
passive-interface Vlan60
passive-interface Vlan70
passive-interface Vlan80
```

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

```
network 10.1.1.0 0.0.0.3 area 0
network 10.1.1.8 0.0.0.3 area 0
network 10.1.10.0 0.0.1.255 area 0
network 10.1.60.0 0.0.0.255 area 0
network 10.1.70.0 0.0.0.255 area 0
network 10.1.70.0 0.0.0.255 area 0
network 10.1.80.0 0.0.0.255 area 0
```

g. To support load sharing, set the maximum number of parallel routes the IP routing protocol supports (installs in a routing table).

```
maximum-paths 8
```

Configuring DER2

The configuration on DER2 is essentially the same as that on DER1, except that IP addresses and VLAN IDs differ, and no connection is made to a BRAS. The topics are summarized, with references, below.

- Configuring QoS on DER2
- Establishing and Configuring Interfaces on DER2
- Configuring OSPF Routing for Video and Voice Traffic on DER2

Configuring QoS on DER2

Proceed as in Configuring QoS on DER1, page 4-11.

Establishing and Configuring Interfaces on DER2

Proceed as in Establishing and Configuring Interfaces on DER1, page 4-14.

For IP addresses and VLAN IDs, see Table 4-2 on page 4-8.

For MPLS on transport interfaces, see Common Task: Configuring MPLS for HSD Service, page 4-9.

Configuring OSPF Routing for Video and Voice Traffic on DER2

Proceed as in Configuring OSPF Routing for Video and Voice Traffic on DER1, page 4-22

Configuring AR1

This section addresses the configuration required on the switch labeled AR1 in Figure 4-1 on page 4-6, to route multiple services from AR1 to DER1 and AR2.

See Configuring DNS Servers, page 4-2.

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

This section addresses the following:

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

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

Configuring QoS on AR1

See Overview of QoS on a Cisco 7600 Series and Cisco Catalyst 6500 Series, page 4-11. This section presents the following topics:

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

Configuring Marking and Classification on AR1

Do the following to enable marking and classification on AR1.

Step 1 Enable QoS in global configuration mode.

```
mls qos
```

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

```
ip access-list extended acl_VoD_and_SIP_signaling
 permit ip any host 10.1.10.10
 permit ip any host 10.1.60.0 0.0.0.255
 permit ip any host 10.1.61.10 0.0.0.255
 permit ip any host 10.1.80.10 0.0.0.255
 permit ip any host 10.1.81.10 0.0.0.255

ip access-list extended acl_VoIP
 permit udp any any range 16384 32767
 permit udp any range 16384 32767 any
```

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

```
class-map match-all class_VoIP
 match access-group name acl_VoIP
class-map match-all class_VoD_and_SIP_signaling
 match access-group name acl_VoD_and_SIP_signaling
```

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

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

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

```
service-policy input setDSCP
```

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

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

```
mls qos trust dscp
```

Configuring Mapping on AR1

To configure mapping on AR1, proceed as in Configuring Mapping on DER1, page 4-13.

Establishing and Configuring Interfaces on AR1

Refer to Figure 4-1 on page 4-6.

This section addresses the following:

- Establishing VLANs for Services on AR1
- Establishing 10-GE Interfaces for Transport on AR1
- Configure Service Mapping for Video and VoIP Services on AR1
- Establishing 1-GE Subinterfaces to DSLAMs on AR1

Establishing VLANs for Services on AR1

Proceed as in Establishing VLANs for Services and Transport on DER1, page 4-39, but make changes to IP addresses and VLAN IDs as indicated in Table 4-2 on page 4-8.

Establishing 10-GE Interfaces for Transport on AR1

The 10-GE trunk interfaces provide the transport between AR1 and DER1 and AR2.

Note For additional details, see Establishing 10-GE Interfaces for Transport on DER1, page 4-19.

Step 1 Establish a Layer 3 interface on AR1 to and from DER1.

a. Establish the Layer 3 interface. (See Table 4-2 on page 4-8.)

```
interface TenGigabitEthernet1/1
```

```
description Transport to/from DER1 (TenGig7/1)
dampening 5 1000 2000 20 restart 16000
ip address 10.1.1.10 255.255.255.252
ip pim query-interval 100 msec
ip pim sparse-mode
ip ospf network point-to-point
ip ospf hello-interval 1
load-interval 30
carrier-delay msec 0
```

b. Proceed as in Step 2 of Establishing 10-GE Interfaces for Transport on DER1, page 4-19.

```
wrr-queue bandwidth 64 255 0 0 0 0 0
wrr-queue queue-limit 40 50 0 0 0 0 0
wrr-queue threshold 2 80 100 100 100 100 100 100 100
wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
no wrr-queue random-detect 2
wrr-queue cos-map 1 1 0 1
wrr-queue cos-map 2 2 3 4 6 7
mls qos trust dscp
```

Step 2 Repeat Step 1, as appropriate, to establish a Layer 3 interface on AR1 to and from AR2.

```
interface TenGigabitEthernet1/3
 description Transport to/from AR2 (TenGig1/1)
 dampening 5 1000 2000 20 restart 16000
 ip address 10.1.1.17 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 mls qos trust dscp
```

Configure Service Mapping for Video and VoIP Services on AR1

Service mapping on each DSLAM is achieved by using VLANs, with a single set of VLANs allocated to each DSLAM. There is a single VLAN per DSLAM, meaning that a VLAN defined on an AR will not span multiple DSLAMs on the AR. One VLAN is for video service, a second VLAN is for VoIP services, and a third VLAN is for high-speed data (HSD) services. (See Table 4-2 on page 4-8.)

IP unnumbered is used to reduce the operational overhead associated with assigning unique IP subnets per VLAN. With IP unnumbered we can reduce operational overhead on the AR by assigning one /16 subnet to a service for all DSLAMs aggregated by the AR. With the exception of HSD, all interfaces are Layer 3 subinterfaces. HSD subinterfaces use EoMPLS at Layer 2 to bridge traffic across an MPLS transport link to a BRAS.

Note For additional details, see Establishing VLANs for Services on AR1, page 4-25.

Do the following to configure service mapping for video and VoIP services on AR1.

Step 1 In global configuration mode, establish and configure loopback interfaces as follows.

a. Establish two loopback interfaces, one for video services and one for VoIP services.

```
interface Loopback0
 description Address block for Video Services on AR1
 ip address 1.10.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30


interface Loopback1
 description Address block for VoIP services on AR1
 ip address 1.20.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30
```

b. In global configuration mode, configure IP unnumbered to use “connected” host routes.

```
ip dhcp route connected
```

Establishing 1-GE Subinterfaces to DSLAMs on AR1

Do the following to establish 1-GE subinterfaces to DSLAMs on AR1.

Step 1 Establish an interface on AR1 to DSLAM1.

a. Establish the interface and corresponding three subinterfaces for each service.

```
interface GigabitEthernet2/1
 description 802.1q Interface To DSLAM-1
 no ip address
```

b. Disable Cisco Discovery Protocol on the interface.

```
no cdp enable
```

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

```
load-interval 30
```

d. Proceed as in Step 2 of Establishing 10-GE Interfaces for Transport on DER1, page 4-19.

```
wrr-queue bandwidth 64 255 0
wrr-queue queue-limit 40 50 0
wrr-queue threshold 2 80 100 100 100 100 100 100
wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100
wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100
no wrr-queue random-detect 2
wrr-queue cos-map 1 1 0 1
wrr-queue cos-map 2 2 3 4 6 7
```

Note The cos-map value 2 2 2 is a default setting on 1-GE interfaces.

e. Establish a subinterface on AR1 for video services for DSLAM1. A subinterface is a Layer 3 port with a VLAN association. DSLAM1 will use VLAN100 for video services.

```
interface GigabitEthernet2/1.1
 description Video edge VLAN
 encapsulation dot1Q 100
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
```

f. Apply the policy map established in Configuring Mapping on AR1, page 4-25, to the subinterface.

```
service-policy input setDSCP
```

g. Enable PIM sparse mode. This is the aggregation VLAN for video traffic to the DSLAMs, and broadcast video is multicast addressed.

```
ip pim sparse-mode
```

h. Configure OSPF on the transport VLAN interface.

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

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

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

Note For more information, 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

j. Change the ARP timeout from the default.

```
arp timeout 250
```

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

k. Establish a subinterface on AR1 for VoIP services for DSLAM1. DSLAM1 will use VLAN200 for VoIP services.

```
interface GigabitEthernet2/1.2
 description Voice edge VLAN
 encapsulation dot1Q 200
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
```

l. Apply the policy map established in Configuring Mapping on AR1, page 4-25, to the subinterface.

```
service-policy input setDSCP
```

m. Establish a subinterface on AR1 for HSD services for DSLAM1. DSLAM1 uses EoMPLS for HSD services.

```
interface GigabitEthernet2/1.3
 description HSD edge VLAN
 encapsulation dot1Q 300
```

Note No service policy is applied here. By default, HSD is treated as "untrusted" (DSCP = 0).

n. Bind the attachment circuit to a pseudowire VC (in this case, the VLAN just established), using the **xconnect** *peer_router_id vcid* **encapsulation mpls** command. The VC maps a tunnel to a subinterface port to the same loopback address.

```
xconnect 10.1.254.3 300 encapsulation mpls
```

Note For example, you configure a corresponding **xconnect** to AR1 on *peer_router_id* 1.1.254.3.

Step 2 Configure MPLS on the transport interfaces.

Note Ensure that MPLS is enabled globally. See Common Task: Configuring MPLS for HSD Service, page 4-9.

a. Establish a loopback interface for MPLS.

```
interface loopback 3
 description Loopback interface for MPLS
 ip address 10.1.254.2 255.255.255.255
```

b. Enable MPLS on the transport interface.

```
tag-switching ip
```

c. Set the size of the maximum transmission unit (MTU) to account for the additional packet overhead required for MPLS.

```
mtu 9216
```

Configuring OSPF Routing for Video and Voice Traffic on AR1

For background and details, refer to Configuring OSPF Routing for Video and Voice Traffic on DER1, page 4-22.

Do the following to configure OSPF routing for video and voice traffic on AR1.

Step 1 Define an OSPF routing process on AR1. This process associates the transport VLANs for video and VoIP VLANs for all DSLAMs to be served by AR1.

```
router ospf 100
 router-id 10.1.1.3
 ispf
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 network 10.1.1.8 0.0.0.3 area 0
 network 10.1.1.16 0.0.0.3 area 0
 network 10.1.254.3 0.0.0.0 area 0
 network 10.10.0.1 0.0.255.255 area 0
 network 10.20.0.1 0.0.255.255 area 0
```

Configuring AR2

The configuration on AR2 is essentially the same as that on AR1, except that IP addresses differ. The topics are summarized, with references, below.

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

Configuring QoS on AR2

Proceed as in Configuring QoS on DER1, page 4-11.

Establishing and Configuring Interfaces on AR2

Proceed as in Establishing and Configuring Interfaces on DER1, page 4-14.

For IP addresses and VLAN IDs, see Table 4-2 on page 4-8.

For MPLS on transport interfaces, see Common Task: Configuring MPLS for HSD Service, page 4-9.

Configuring OSPF Routing for Video and Voice Traffic on AR2

Proceed as in Configuring OSPF Routing for Video and Voice Traffic on DER1, page 4-22

Configuring AR3

The configuration on AR3 is essentially the same as that on AR1 and AR2, except that IP addresses differ. The topics are summarized, with references, below.

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

Configuring QoS on AR3

Proceed as in Configuring QoS on DER1, page 4-11.

Establishing and Configuring Interfaces on AR3

Proceed as in Establishing and Configuring Interfaces on DER1, page 4-14.

For IP addresses and VLAN IDs, see Table 4-2 on page 4-8.

For MPLS on transport interfaces, see Common Task: Configuring MPLS for HSD Service, page 4-9.

Configuring OSPF Routing for Video and Voice Traffic on AR3

Proceed as in Configuring OSPF Routing for Video and Voice Traffic on DER1, page 4-22

Configuring the Hub-and-Spoke Topology

This section presents the following major topics:

- Introduction, page 4-32
- Common Task: Configuring QinQ and Spanning Tree
- Configuring DER1, page 4-36
- Configuring DER2, page 4-23
- Configuring AR1, page 4-58
- Configuring AR2, page 4-67

Introduction

Figure 4-2 on page 4-33 illustrates the hub-and-spoke topology used in the solution. (See Configuration 2: 1-GE plus 10-GE Hub and Spoke, page 3-39.) All video sources and VoIP servers are connected to ports on the distribution edge routers (DERs). With two DERs in the topology we are able to provide source, node, and network redundancy for each of the aggregation routers (ARs). Policy maps are applied to the DER ingress ports in order to mark the DSCP values of the different service types. In this example, only DER1 is connected to a middleware server.

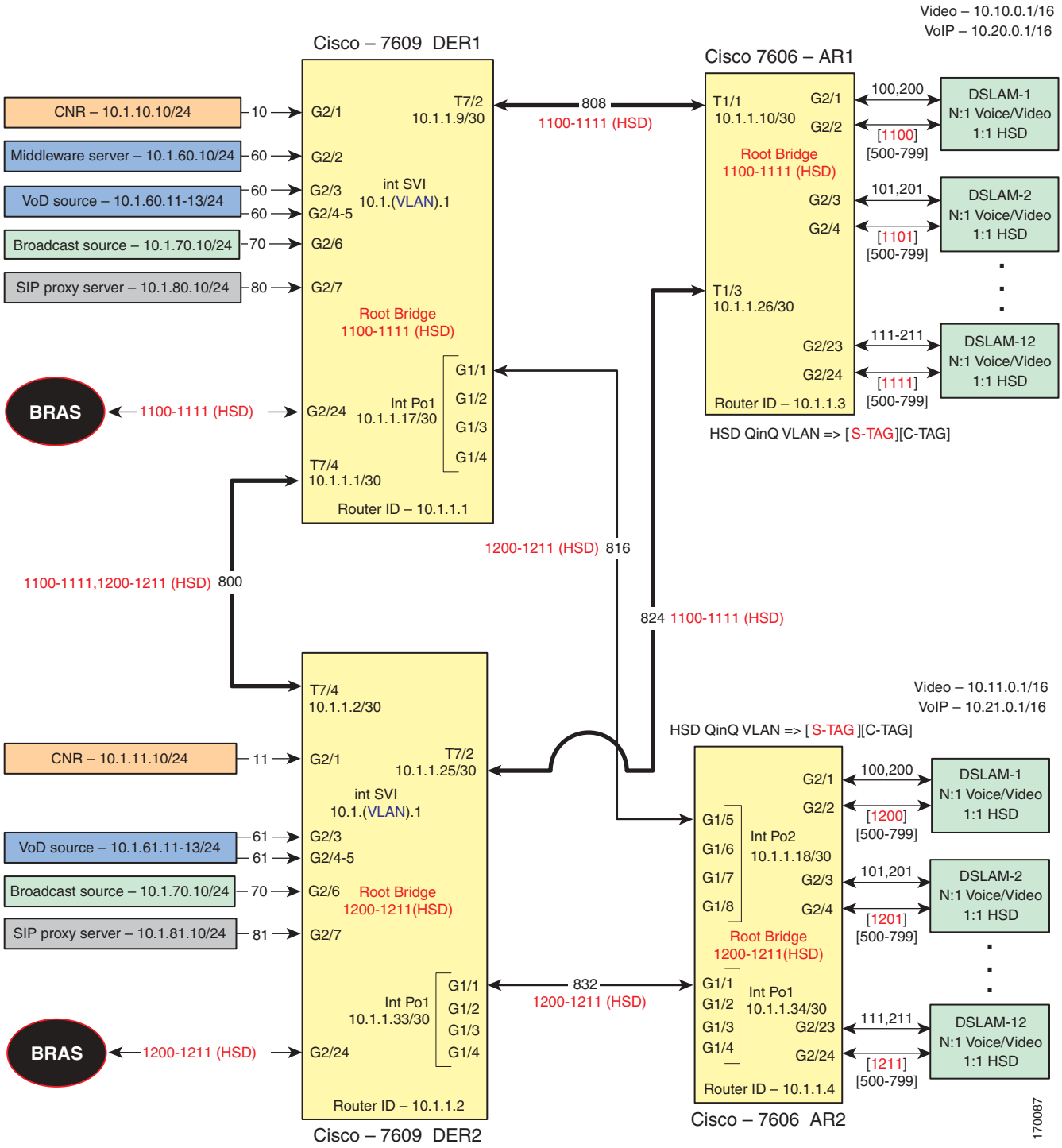
Traffic is routed among DERs and ARs over 10-GE bidirectional and Nx1-GE transport links. Transport links are Layer 2 switchports that are defined as IEEE 802.1q trunks. Each transport link or trunk carries two VLANs; video and VoIP traffic is in one VLAN, and HSD or Internet traffic is in the second VLAN. IEEE 802.1q is needed, because HSD traffic is bridged on the transport links.

The hub-and-spoke topology assumes that each DSLAM uses the N:1 model for video and voice services, (one VLAN per service), and uses the 1:1 model for HSD services (one VLAN per subscriber). (Note that VLANs have local significance, and are not be bridged between DSLAMs attached to a common AR.)

The 1:1 model for HSD traffic does not scale, because of the number of service provider VLANs required to implement this model. Dot1q tunneling (QinQ) is used to reduce the number of VLANs required in the service provider network for HSD.

The residential gateways (RGs) used in the test bed provided service mapping based on physical ports, as described in Physical Port-Based Traffic Mapping for the Multi-VC and VLAN Access Models, page 3-43.

Figure 4-2 Hub-and-Spoke Topology



The switches in Figure 4-2 use the line cards, hardware versions, and IOS versions listed in Table 4-6 on page 4-34.

Table 4-5 Hardware and IOS Versions for the Hub-and-Spoke Topology

Switch	Module	Line Card	Hardware Version	IOS Release	Submodule	Hardware Version
DER1, DER2	1	WS-X6724-SFP	2.3	12.2(18)SXF2	WS-F6700-DFC3BXL	5.2
	2				WS-F6700-DFC3BXL	4.0
	5	WS-SUP720-BASE	3.1		WS-F6K-PFC3BXL	1.2
					WS-SUP720 (MFSC3)	2.1
	7	WS-X6704-10-GE	2.2		WS-F6700-DFC3BXL	4.0
AR1	1	WS-X6704-10-GE	2.2		WS-F6700-DFC3BXL	4.0
	2	WS-X6724-SFP	2.3		WS-F6700-DFC3BXL	5.2
	5	WS-SUP720-BASE	3.1		WS-F6K-PFC3BXL	1.6
					WS-SUP720 (MFSC3)	2.3
AR2	1	WS-X6704-10GE	2.2		WS-F6700-DFC3BXL	4.0
	2	WS-X6724-SFP	2.2		WS-F6700-DFC3BXL	5.2
	5	WS-SUP720-BASE	3.1		WS-F6K-PFC3BXL	1.6
					WS-SUP720 (MFSC3)	2.3

Table 4-2 lists VLANs, their descriptions (service types), and IP addresses, for the DER and ARs in Figure 4-2 on page 4-33.

Table 4-6 VLANs, Descriptions, and IP Addresses for the Hub-and-Spoke Topology

Node	VLAN	Description	IP Address
DER1	10	Management: CNR (DHCP, DNS, FTP, TFTP, Syslog servers), middleware server	10.1.10.1/24
	60	VoD sources	10.1.60.1/24
	70	Digital broadcast sources	10.1.70.1/24
	80	VoIP—SIP proxy server	10.1.80.1/24
	800	To/from DER2	10.1.1.1/30
	808	To/from AR1	10.1.1.9/30
	816	To/from AR2	10.1.1.17/30
	1100–1111	HSD traffic to/from BRAS	Bridged
DER2	11	Management: CNR (DHCP, DNS, FTP, TFTP, Syslog servers)	10.1.11.1/24
	61	VoD sources	10.1.61.1/24
	70	Digital broadcast sources	10.1.70.1/24
	81	VoIP—SIP proxy server	10.1.81.1/24
	800	To/from DER1	10.1.1.2/30
	824	To/from AR1	10.1.1.25/30
	832	To/from AR2	10.1.1.33/30
	1200–1111	HSD traffic to/from BRAS	Bridged

Table 4-6 VLANs, Descriptions, and IP Addresses for the Hub-and-Spoke Topology (continued)

Node	VLAN	Description	IP Address
AR1	808	To/from DER1	10.1.1.10/30
	824	To/from DER2	10.1.1.26/30
	100–111	Subscriber video (N:1)	10.10.0.1/16
	200–211	Subscriber voice (N:1)	10.20.0.1/16
	1100–1111	High-speed data (1:1) to/from UTStarcom DSLAM (QinQ—S-TAG)	Bridged
AR2	816	To/from DER1	10.1.1.18/30
	832	To/from DER2	10.1.1.34/30
	100–111	Subscriber video (N:1)	10.11.0.1/16
	200–211	Subscriber voice (N:1)	10.21.0.1/16
	1200–1211	High-speed data (1:1) to/from UTStarcom DSLAM (QinQ—S-TAG)	Bridged

Table 4-3 on page 4-9 lists the parameters used to configure the residential gateway (RG). They are the same as those for the 10-GE symmetric topology.

Note See RG Functions, page 3-41.

Common Task: Configuring QinQ and Spanning Tree

QinQ is used to connect HSD subscribers to a BRAS on one of the DER nodes, where dot1q tunnels terminate on the BRAS. This supports the requirement to have 1:1 VLANs on the DSLAM, where one VLAN is assigned to each subscriber for HSD. Assuming there are 300 subscribers per DSLAM, this would require 300 VLANs per DSLAM—making VLAN scalability an issue for the service provider. The AR port connecting the DSLAM to the service provider network adds an outer S-TAG to inner C-TAG, meaning one service provider VLAN is required per DSLAM.

HSD VLANs are bridged on the service provider network. In a hub-and-spoke network, each AR creates a Layer 2 loop that forces the provider to run spanning tree. Disable MAC address learning on the DER to conserve on MAC forwarding entries. MAC address learning is not needed when a logical topology consists of only two physical ports, because each MAC frame that arrives at one port is always sent on the other port. To create a two-port topology on the DER, configure each AR as the spanning tree root for its HSD VLANs. This causes Spanning Tree Protocol (STP) to block at the transport link between DER1 and DER2, creating point-to-point Layer 2 links between DER and AR. To improve STP time, the four switches are configured for IEEE 802.1w Rapid Spanning Tree Protocol (RSTP).

VLANs defined on AR1 are used for HSD traffic, with one service provider VLAN per DSLAMs. Each AR supports a maximum of 30 DSLAMs. Table 4-7 lists the VLAN ranges for the ARs.

Table 4-7 VLAN Ranges for ARs

Node	VLAN Range
AR1	1100–1111
AR2	1200–1211

Configuring DER1

This section addresses the configuration required on the switch labeled DER1 in Figure 4-2 on page 4-33, to route multiple services from that switch to the ARs.

See Configuring DNS Servers, page 4-2.

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

This section addresses the following:

- Configuring QoS on DER1
- Establishing and Configuring Interfaces on DER1
- Configuring OSPF Routing for Video and Voice Traffic on DER1
- Configuring QinQ and Spanning Tree on DER1

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

Configuring QoS on DER1

This section presents the following topics:

- Overview of QoS on a Cisco 7600 Series and Cisco Catalyst 6500 Series
- Configuring Marking and Classification on DER1
- Configuring Mapping on DER1

Note For more information specific to QoS as applied to the solution, see Appendix C, "Configuring Ericsson DSL Equipment."

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

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

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

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

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

Configuring Marking and Classification on DER1

Do the following to enable marking and classification on DER1.

Step 1 Enable QoS in global configuration mode.

```
mls qos
```

Step 2 Configure ingress multicast replication mode and disable automatic detection of the replication mode (enabled by default).

```
mls ip multicast replication-mode ingress
```

Note For more information, see "Configuring IPv4 Multicast VPN Support" at the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a0080435d12.html

Step 3 Create access lists to identify the different service types in the network.

```
ip access-list extended acl_VoD_and_SIP_signaling
 permit tcp 10.1.60.0 0.0.0.255 any
 permit tcp 10.1.61.0 0.0.0.255 any
 permit tcp 10.1.80.0 0.0.0.255 any
 permit tcp 10.1.81.0 0.0.0.255 any

ip access-list extended acl_video_VoD
 permit udp 10.1.60.0 0.0.0.255 any
 permit udp 10.1.61.0 0.0.0.255 any

ip access-list extended acl_video_broadcast
permit udp 10.1.70.0 0.0.0.255 232.0.0.0 0.255.255.255
```

Step 4 Create class maps for the access lists created in Step 2.

```
class-map match-all class_VoIP
 match access-group name acl_VoIP
class-map match-all class_VoD_and_SIP_signaling
 match access-group name acl_VoD_and_SIP_signaling
class-map match-all class_video_broadcast
 match access-group name acl_video_broadcast
class-map match-all class_video_VoD
 match access-group name acl_video_VoD
```

Step 5 Create a policy map to set the DSCP values of the different classes created in Step 3.

```
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoD_and_SIP_signaling
   set dscp cs3
  class class_video_broadcast
   set dscp af41
  class class_video_VoD
```

```
   set dscp af42
  class class_VoIP
   set dscp ef
```

Step 6 Apply the policy map from Step 4 to the ingress interfaces using the following command.

```
service-policy input setDSCP
```

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

Step 7 To maintain the DSCP marking applied at the network ingress interface, configure all noningress transport interfaces to trust the incoming DSCP markings.

```
mls qos trust dscp
```

Configuring Mapping on DER1

Do the following to configure mapping on DER1.

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

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

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

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

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

This table shows the following mapping (36 corresponds to AF41):

Service Type	DSCP	CoS
Broadcast video	36	4

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

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

Service Type	DSCP	CoS
Broadcast video	36	2

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

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

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

```
DER1# show mls qos maps dscp-cos
DSCP-CoS Mapping Table (dscp = d1d2)
d1 : d2  0  1  2  3  4  5  6  7  8  9
---------------------------------------
 0 :    00 00 00 00 00 00 00 00 01 01
 1 :    01 01 01 01 01 01 02 02 02 02
 2 :    02 02 02 02 03 03 03 03 03 03
 3 :    03 03 04 04 04 04 02 04 01 04
 4 :    05 05 05 05 05 05 05 05 06 06
 5 :    06 06 06 06 06 06 07 07 07 07
 6 :    07 07 07 07
```

Establishing and Configuring Interfaces on DER1

Refer to Figure 4-2 on page 4-33.

This section addresses the following:

- Establishing VLANs for Services and Transport on DER1
-
- Establishing 1-GE Interfaces for Servers and Management on DER1
- Establishing 10-GE Interfaces for Transport on DER1
- Establishing Nx1-GE Interfaces for Transport on DER1

Establishing VLANs for Services and Transport on DER1

Before the 1-GE and 10-GE interfaces can be configured, VLANs for the various services must be created. With the exception of the VLAN range for high-speed data (HSD), these are all Layer 3 VLANs. (See Table 4-6 on page 4-34.)

Do the following to establish VLANs for services and transport on DER1.

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

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

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

```
vlan 10
name VLAN_10_Management
```

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

```
interface Vlan10
 description Management VLAN (Middleware, DNS, DHCP, etc)
 ip address 10.1.10.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

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

```
load-interval 30
```

d. Establish a VLAN for unicast video aggregation.

```
vlan 60
name VLAN_60_Unicast_Video


interface Vlan60
 description VoD server VLAN (Unicast Video)
 ip address 10.1.60.1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

e. Establish a VLAN for VoIP.

```
vlan 80
name VLAN_80_VoIP


interface Vlan80
 description VoIP gateway VLAN
 ip address 10.1.80.1 1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

Step 2 Establish a VLAN for multicast video aggregation.

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

```
vlan 70
name VLAN_70_Multicast_Video
```

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

```
interface Vlan70
 description Broadcast video source VLAN (Multicast Video)
 ip address 10.1.70.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

c. Change the PIM query interval from the default of 30 seconds.

```
ip pim query-interval 100 msec
```

Note It was determined in testing that convergence times improve if the PIM hello interval is less than one second. For more information about the **ip pim query-interval** command, see the following:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123tip3r/ip3_i2gt.htm#wp1069550

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

```
ip pim sparse-mode
```

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

```
load-interval 30
```

Step 3 In global configuration mode, establish a range of VLANs for HSD. (No Layer 3 interface is required.)

```
vlan 1100-1111,1200-1211
```

Step 4 Establish VLANs for transport. The first is to and from DER1.

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

```
vlan 800
 name Video/Voice_To/From_DER2
```

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

```
interface Vlan800
 description Transport VLAN to/from DER2
 ip address 10.1.1.1 255.255.255.252
```

c. Change the PIM query interval from the default of 30 seconds.

```
ip pim query-interval 100 msec
```

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

```
 ip pim sparse-mode
```

e. Configure OSPF on the transport VLAN interface.

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

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

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

```
 load-interval 30
```

Step 5 Establish the remaining transport VLANs and configure the interfaces as in Step 2.

Voice/Video to/From AR1

```
vlan 808
 name Video/Voice_To/From_AR1


interface Vlan808
 description Transport VLAN to/from AR1
 ip address 10.1.1.9 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Voice/Video to/From AR2

```
vlan 816
 name Video/Voice_To/From_AR2


interface Vlan816
 description Transport VLAN to/from AR2
 ip address 10.1.1.17 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

g. Because the transport links are point-to-point, there is no risk of Layer 2 loops, so Spanning Tree Protocol (STP) can be disabled on these VLANs.

```
no spanning-tree vlan 800,808,816
```

Establishing a Tunnel to the BRAS

Do the following to establish a dot1q tunnel interface to the broadband remote-access server (BRAS). (See Common Task: Configuring QinQ and Spanning Tree, page 4-35.)

Note Connections to multiple BRASs are likely. This example illustrates only one connection.

Step 1 Establish a 1-GE interface.

```
interface GigabitEthernet2/24
 description BRAS for HSD (Dot1q-Tunnel)
 switchport
 switchport mode trunk
 no ip address
```

h. Configure the trunk for 802.1q encapsulation.

```
switchport trunk encapsulation dot1q
```

i. Assign the trunk to the HSD VLAN ranges, 1100–1111 and 1200–1211.

```
switchport trunk allowed vlan 1100-111,1200-1211
```

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

```
load-interval 30
```

k. Configure interface link detect options, such as **carrier-delay**, to reduce the time to detect a link failure, and **dampening** to minimize the effects of flapping links.

Step 2 Repeat Step 1, as required, for additional BRAS interfaces.

Establishing 1-GE Interfaces for Servers and Management on DER1

VoD servers, high-speed data sources, and management resources connect to Layer 2 interfaces on DER1, and their traffic is aggregated into the appropriate service VLANs.

The following is configured on DER1.

Step 1 Establish an interface.

a. Establish an interface for the CNR server.

```
interface GigabitEthernet2/1
 description CNR ingress/egress (DHCP, DNS, TFTP, SysLog)
 no ip address
```

b. Configure the interface as a Layer 2 access port and assign it to VLAN 10.

```
switchport
switchport mode access
switchport access vlan 10
```

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

```
load-interval 30
```

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

```
no cdp enable
```

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

```
spanning-tree portfast
```

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

```
spanning-tree bpduguard enable
```

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

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

```
service-policy input setDSCP
```

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

Cisco Network Registrar (CNR)—Primary Server

```
interface GigabitEthernet2/1
 description CNR ingress/egress (DHCP, DNS, TFTP, SysLog)
 switchport
 switchport access vlan 10
```

Kasenna Middeware Server

```
interface GigabitEthernet2/2
 description Kasenna Middleware Server ingress/egress
 switchport
 switchport access vlan 60
```

Kasenna VoD Pump Management Port (Eth0)

```
interface GigabitEthernet2/3
 description VoD Pump ingress/egress
 switchport
 switchport access vlan 60
```

Kasenna VoD Pump (HPN0)

```
interface GigabitEthernet2/4
 description VoD Pump (HPN0) ingress/egress
 switchport
 switchport access vlan 60
```

Kasenna VoD Pump (HPN1)

```
interface GigabitEthernet2/5
 description VoD Pump (HPN1) ingress/egress
 switchport
 switchport access vlan 60
```

Broadcast Server (multicast)

```
interface GigabitEthernet2/6
 description Broadcast Video ingress/egress
 switchport
 switchport access vlan 70
```

VoIP—SIP Proxy Server

```
interface GigabitEthernet2/7
 description SIP Proxy Server ingress/egress
 switchport
 switchport access vlan 80
```

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

Establishing 10-GE Interfaces for Transport on DER1

The 10-GE trunk interfaces create the hub-and-spoke topology from DER1 to AR1 and DER2. Both bidirectional and unidirectional trunking interfaces and VoD unidirectional transport are established.

Do the following to establish 10-GE transport interfaces on DER1.

Step 1 Establish an interface to and from AR1.

a. Establish the interface.

```
interface TenGigabitEthernet7/1
 description Transport to/from AR1 (TenGig7/1)
 no ip address
```

b. Configure the trunk for 802.1q encapsulation.

```
switchport trunk encapsulation dot1q
```

c. Configure the port as a switchport IEEE 802.1q trunk.

```
switchport
switchport mode trunk
```

d. Assign VLAN 808, and VLAN range 1100–1111 to the trunk. (See Table 4-6 on page 4-34.)

```
switchport trunk allowed vlan 808,1100-1111
```

e. Configure interface link detection options, such as **carrier-delay** (to reduce the time to detect a link failure), and **dampening** (to minimize the effects of flapping links).

Note The **restart** command option is applied on start up to reduce the possibility of routing "black holes" during startup (where upper layers converge before lower layers do).

```
carrier-delay msec 0
dampening 5 1000 2000 20 restart 16000
```

Note The above nondefault settings are applied to transport links only.

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

```
load-interval 30
```

Step 2 Configure QoS on the interface.

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

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

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

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

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

Note TxQueue1 and TxQueue8 use the default mappings. TxQueue2 has three thresholds: Threshold 1 = CoS 1, Threshold 2 = CoS 2, and Threshold 3 = CoS 3, 4, 6, and 7.

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

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

d. Configure the TxQueue thresholds.

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

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

TxQueue2 uses tail drop for queue congestion management. VoD is assigned to threshold 1 and is dropped once the queue reaches 80% utilization. VoD signaling, network signaling, and broadcast video are assigned to the third threshold 2 and are dropped once the queue reaches 100% utilization.

```
wrr-queue threshold 2 80 100 100 100 100 100 100 100
no wrr-queue random-detect 2
```

e. Configure the bandwidth of the weighted queues.

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

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

f. Configure the size of the weighted queues.

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

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

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

```
mls qos trust dscp
```

Step 3 Proceed as in Step 1 through Step 3 above to establish an interface to and from DER2, but with the following differences in interface and allowed VLANs.

```
interface TenGigabitEthernet7/4
 description Transport to/from DER2 (TenGig7/4)

 switchport trunk allowed vlan 800,1100-1111,1200-1211
```

Establishing Nx1-GE Interfaces for Transport on DER1

The Nx1-GE trunk interfaces create the hub-and-spoke topology. A single 1-GE interface is illustrated below, but up to eight such interfaces can be used to establish eight equal-cost paths that use Cisco Express Forwarding (CEF) load balancing. (See Table 4-6 on page 4-34.)

Do the following to configure a single 1-GE interface on DER1.

Step 1 Establish a 1-GE interface to and from AR2.

a. Establish the interface.

```
interface GigabitEthernet1/1
 description Transport to/from AR2 (Gig1/5)
 switchport
 switchport mode trunk
 no ip address
```

b. Configure the trunk for 802.1q encapsulation.

```
switchport trunk encapsulation dot1q
```

c. Assign the trunk to VLANs 816 and 1200–1211.

```
switchport trunk allowed vlan 816,1200-1211
```

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

```
load-interval 30
```

e. Configure interface link detection options, such as **carrier-delay** to reduce the time to detect a link failure, and **dampening** to minimize the effects of flapping links.

Note The **restart** command option is applied on start up to reduce the possibility of routing "black holes" during startup (where upper layers converge before lower layers do).

```
carrier-delay msec 0
dampening 5 1000 2000 20 restart 16000
```

Step 2 Repeat Step 1 for any additional 1-GE transport interfaces as required.

Step 3 Configure QoS on the first port in the 4x1-GE port channel.

Note The Nx1-GE transport links from DER1 to the ARs require modifications to the transmit queues. There are eight transmit queues, but this solution uses only three.

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

```
queue thresh cos-map
---------------------------------------
1     1      0
1     2      1
2     1      2
2     2      3 4
3     1      6 7
4     1      5
```

b. Configure the CoS-to-TxQueue mapping on the 10-GE transport interfaces. HSD (CoS = 0) remains in TxQueue1 and VoIP (CoS = 5) remains in TxQueue8. Video is separated into two classes, one class for broadcast video (CoS = 4) and one class for VoD video (CoS = 2). The other three CoS values are associated with TxQueue2.

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

TxQueue1 and TxQueue8 use the default mappings. TxQueue2 has three thresholds: Threshold 1 = CoS 1, Threshold 2 = CoS 2, and Threshold 3 = CoS 3, 4, 6, and 7.

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

```
queue thresh cos-map
---------------------------------------
1     1      0 1
2     1      2
2     2      3 4 6 7
4     1      5
```

d. Configure the TxQueue thresholds.

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

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

TxQueue2 uses tail drop for queue congestion management. VoD is assigned to the threshold 1 and is dropped once the queue reaches 80% utilization. VoD signaling, network signaling, and broadcast video are assigned to the third threshold 2 and are dropped once the queue reaches 100% utilization.

```
wrr-queue threshold 2 80 100 100 100 100 100 100 100
no wrr-queue random-detect 2
```

e. Configure the bandwidth of the weighted queues.

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

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

f. Configure the size of the weighted queues.

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

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

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

```
mls qos trust dscp
```

Step 4 For the remaining three ports, proceed as in Step 3a through Step 3g.

Configuring OSPF Routing for Video and Voice Traffic on DER1

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

Do the following to configure OSPF for video and voice traffic on DER1.

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

```
router ospf 100
 router-id 10.1.1.1
 log-adjacency-changes
```

Step 2 Modify various timer parameters.

a. Use the following command to enable OSPF SPF throttling, modifying the timers, and provide fast convergence: **timers throttle spf** spf-*start spf-hold spf-max-wait*

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

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

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

c. Use the following command to control the minimum interval for accepting the same LSA: **timers lsa arrival** *milliseconds*

```
timers lsa arrival 100
```

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

Step 3 Use the following command to set incremental SPF updates for LSA type 1 and LSA type 2 within an area. Enabling iSPF can minimize the effect of SPF changes within an area to only those routers where the change is relevant, thus reducing the time spent calculating SPF.

```
ispf
```

Step 4 Apply the **passive-interface** command to the aggregation VLANs.

```
passive-interface Vlan10
passive-interface Vlan60
passive-interface Vlan70
passive-interface Vlan80
```

Step 5 Advertise the networks in the first OSPF routing process.

```
network 10.1.1.0 0.0.0.3 area 0
network 10.1.1.8 0.0.0.3 area 0
network 10.1.10.0 0.0.1.255 area 0
network 10.1.60.0 0.0.0.255 area 0
network 10.1.70.0 0.0.0.255 area 0
network 10.1.80.0 0.0.0.255 area 0
```

Step 6 To support load sharing, set the maximum number of parallel routes the IP routing protocol supports (installs in a routing table).

```
maximum-paths 8
```

Configuring QinQ and Spanning Tree on DER1

Do the following in global configuration mode to configure QinQ and spanning tree parameters on DER1. (See Common Task: Configuring QinQ and Spanning Tree, page 4-35.)

Step 1 Create the HSD VLAN ranges for AR1 and AR2, respectively.

```
vlan 1100-1111,1200-1211
```

Step 2 Enable QinQ tunneling.

```
vlan dot1q tag native
```

Step 3 Disable MAC address learning globally for the HSD VLANs.

```
no mac-address-table learning vlan 1100-1111,1200-1211
```

Step 4 Configure DER1 as the primary root node for all HSD VLANs defined on AR1, using the **root primary** option.

```
spanning-tree vlan 1100-1111 root primary diameter 2
```

Step 5 Configure RSTP.

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

Configuring DER2

This section addresses the configuration required on the switch labeled DER2 in Figure 4-2 on page 4-33, to route multiple services from that switch to the ARs. The configuration of DER2 is identical to that of DER1, with the exceptions noted below.

See Configuring DNS Servers, page 4-2.

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

This section addresses the following:

- Configuring QoS on DER2
- Establishing and Configuring Interfaces on DER2
- Configuring OSPF Routing for Video and Voice Traffic on DER2, page 4-57
- Configuring QinQ and Spanning Tree on DER2, page 4-57

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

Configuring QoS on DER2

Proceed as in Configuring QoS on DER1, page 4-36. The configurations are identical on both DERs.

Establishing and Configuring Interfaces on DER2

Proceed as in Establishing and Configuring Interfaces on DER1, page 4-39, but with the changes noted below:

- Establishing VLANs for Services and Transport on DER2
- Establishing 10-GE Interfaces for Transport on DER2

Establishing VLANs for Services and Transport on DER2

Before the 1-GE interfaces can be configured, VLANs for the various services must be created. With the exception of the VLAN range for high-speed data (HSD), these are all Layer 3 VLANs. (See Table 4-6 on page 4-34.)

Do the following to establish VLANs for services and transport on DER2.

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

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

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

```
vlan 11
name VLAN_11_Management
```

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

```
interface Vlan11
 description Management VLAN (CNR - DNS, DHCP, etc)
 ip address 10.1.11.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

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

```
load-interval 30
```

d. Establish a VLAN for unicast video aggregation.

```
vlan 61
name VLAN_61_Unicast_Video


interface Vlan61
 description VoD server VLAN (Unicast Video)
 ip address 10.1.61.1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

e. Establish a VLAN for VoIP.

```
vlan 81
name VLAN_80_VoIP


interface Vlan81
 description VoIP gateway VLAN
 ip address 10.1.81.1 1 255.255.255.0
 no ip redirects
 no ip unreachables
 load-interval 30
```

Step 2 Establish a VLAN for multicast video aggregation.

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

```
vlan 70
name VLAN_70_Multicast_Video
```

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

```
interface Vlan70
 description Broadcast video source VLAN (Multicast Video)
 ip address 10.1.70.1 255.255.255.0
 no ip redirects
 no ip unreachables
```

c. Change the PIM query interval from the default of 30 seconds.

```
ip pim query-interval 100 msec
```

Note It was determined in testing that convergence times improve if the PIM hello interval is less than one second. For more information about the **ip pim query-interval** command, see the following:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123tip3r/ip3_i2gt.htm#wp1069550

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

```
ip pim sparse-mode
```

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

```
load-interval 30
```

Step 3 In global configuration mode, establish a range of VLANs for HSD. (No Layer 3 interface is required.)

```
vlan 1100-1111,1200-1211
```

Step 4 Establish VLANs for transport. Proceed as in Step 4 of Establishing VLANs for Services and Transport on DER1, page 4-39. The VLANs and interfaces are summarized below.

a. Establish the VLANs and configure the interfaces as in Step 2.

Voice/Video to/From DER1

```
vlan 800
 name Video/Voice_To/From_DER1


interface Vlan800
 description Transport VLAN to/from DER2
 ip address 10.1.1.2 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Voice/Video to/From AR1

```
vlan 824
 name Video/Voice_To/From_AR1


interface Vlan824
 description Transport VLAN to/from AR1
 ip address 10.1.1.25 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Voice/Video to/From AR2

```
vlan 832
 name Video/Voice_To/From_AR2


interface Vlan832
 description Transport VLAN to/from AR2
 ip address 10.1.1.33 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

b. Because the transport links are point-to-point, there is no risk of Layer 2 loops, so Spanning Tree Protocol (STP) can be disabled on these VLANs.

```
no spanning-tree vlan 800,824,832
```

Step 5 In global configuration mode, establish a range of VLANs for HSD. (No Layer 3 interface is required.)

```
vlan 1100-1111,1200-1211
```

Establishing 10-GE Interfaces for Transport on DER2

Do the following to establish 10-GE interfaces for transport on DER2.

Step 1 Proceed as in Establishing 10-GE Interfaces for Transport on DER1, page 4-44, but with the exceptions noted in Step 2.

Step 2 Make the following changes in interface numbers.

Video/VoIP Transport to/from DER1

```
interface TenGigabitEthernet7/4
 description Transport to/from DER1 (TenGig7/4)
 ip address 10.1.1.2 255.255.255.252

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

 load-interval 30
```

Video/VoIP Transport to/from AR2

```
interface TenGigabitEthernet7/1
 description Transport VLAN to/from AR2 (TenGig1/1)
 ip address 10.1.1.34 255.255.255.252

 ip pim sparse-mode
 ip pim query-interval 100 msec
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30

 carrier-delay msec 0
 dampening 5 1000 2000 20 restart 16000
```

Establishing 1-GE Interfaces for Servers and Management on DER2

Step 1 Make the following changes in the VLAN number as shown below. The remainder of the configuration is as for DER1.

CNR Server

```
interface GigabitEthernet2/1
 description CNR ingress/egress (DHCP, DNS, TFTP, SysLog)
 no ip address

 switchport
 switchport mode access
 switchport access vlan 11

 load-interval 30

 no cdp enable

 spanning-tree portfast
 spanning-tree bpduguard enable

 service-policy input setDSCP
```

Cisco Network Registrar (CNR)—Primary Server

```
interface GigabitEthernet2/1
 description CNR ingress/egress (DHCP, DNS, TFTP, SysLog)
 switchport
 switchport access vlan 11
```

Kasenna VoD Pump Management Port (Eth0)

```
interface GigabitEthernet2/3
 description VoD Pump ingress/egress
 switchport
 switchport access vlan 61
```

Kasenna VoD Pump (HPN0)

```
interface GigabitEthernet2/4
 description VoD Pump (HPN0) ingress/egress
 switchport
 switchport access vlan 61
```

Kasenna VoD Pump (HPN1)

```
interface GigabitEthernet2/5
 description VoD Pump (HPN1) ingress/egress
 switchport
 switchport access vlan 61
```

Broadcast Server (Multicast)

```
interface GigabitEthernet2/6
 description Broadcast Video ingress/egress
 switchport
 switchport access vlan 70
```

VoIP—SIP Proxy Server

```
interface GigabitEthernet2/7
 description SIP Proxy Server ingress/egress
 switchport
 switchport access vlan 81
```

Establishing 10-GE Interfaces for Transport on DER2

Step 1 Proceed as in Establishing 10-GE Interfaces for Transport on DER1, page 4-19, but with the following changes in interface and IP address as noted below.

10-GE Interface to/from AR1

```
interface TenGigabitEthernet7/4
 description Transport to/from AR1 (TenGig7/4)
 ip address 10.1.1.2 255.255.255.252

 load-interval 30

 carrier-delay msec 0
 dampening 5 1000 2000 20 restart 16000

 ip pim sparse-mode
 ip pim query-interval 100 msec

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

10-GE Interface to/from AR2

```
interface TenGigabitEthernet7/1
 description Transport to/from AR2 (TenGig1/3)
 dampening 5 1000 2000 20 restart 16000
 ip address 10.1.1.34 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 mls qos trust dscp
```

Establishing Nx1-GE Interfaces for Transport on DER2

Proceed as in Establishing Nx1-GE Interfaces for Transport on DER1, page 4-47.

Configuring OSPF Routing for Video and Voice Traffic on DER2

Do the following to configure OSPF routing for video and voice traffic on DER2.

Step 1 Proceed as in Configuring OSPF Routing for Video and Voice Traffic on DER2, page 4-57, but with the following exceptions.

Step 2 Define the OSPF routing process for video traffic for the following router ID.

```
router ospf 100
 router-id 10.1.1.2
 log-adjacency-changes
```

Step 3 Apply the **passive-interface** statements to these aggregation VLANs.

```
passive-interface Vlan11
passive-interface Vlan61
passive-interface Vlan70
passive-interface Vlan81
```

Step 4 Advertise these networks in the first OSPF routing process.

```
network 10.1.1.0 0.0.0.3 area 0
network 10.1.1.32 0.0.0.3 area 0
network 10.1.11.0 0.0.1.255 area 0
network 10.1.61.0 0.0.0.255 area 0
network 10.1.70.0 0.0.0.255 area 0
network 10.1.81.0 0.0.0.255 area 0
```

Step 5 To support load sharing, set the maximum number of parallel routes the IP routing protocol supports (installs in a routing table).

```
maximum-paths 8
```

Configuring QinQ and Spanning Tree on DER2

Refer to Configuring QinQ and Spanning Tree on DER1, page 4-50.

Do the following to in global configuration mode to configure QinQ and spanning tree on DER2. Configuring DER2 is essentially the symmetrical opposite of what was done on DER1.

Step 1 Create the HSD VLAN ranges for AR1 and AR2, respectively.

```
vlan 1100-1111,1200-1211
```

Step 2 Enable QinQ tunneling.

```
vlan dot1q tag native
```

Step 3 Disable MAC address learning globally for the HSD VLANs.

```
no mac-address-table learning vlan 1100,1200-1211
```

Step 4 Configure RSTP.

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

Configuring AR1

This section addresses the configuration required on the switch labeled AR1 in Figure 4-2 on page 4-33, to route multiple services from AR1 to DER1 and DER2.

See Configuring DNS Servers, page 4-2.

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

This section addresses the following:

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

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

Configuring QoS on AR1

See Overview of QoS on a Cisco 7600 Series and Cisco Catalyst 6500 Series, page 4-11. This section presents the following topics:

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

Configuring Marking and Classification on AR1

Do the following to enable marking and classification on AR1.

Step 1 Enable QoS in global configuration mode.

```
mls qos
```

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

```
ip access-list extended acl_VoD_and_SIP_signaling
 permit ip any host 10.1.10.10
 permit ip any 10.1.60.0 0.0.0.255
 permit ip any 10.1.61.0 0.0.0.255
 permit ip any 10.1.80.0 0.0.0.255
 permit ip any 10.1.81.0 0.0.0.255

ip access-list extended acl_VoIP
 permit udp any any range 16384 32767
 permit udp any range 16384 32767 any
```

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

```
class-map match-all class_VoIP
 match access-group name acl_VoIP
class-map match-all class_VoD_and_SIP_signaling
 match access-group name acl_VoD_and_SIP_signaling
```

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

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

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

```
service-policy input setDSCP
```

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

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

```
mls qos trust dscp
```

Configuring Mapping on AR1

To configure mapping on AR1, proceed as in Configuring Mapping on DER1, page 4-38.

Establishing and Configuring Interfaces on AR1

Refer to Figure 4-2 on page 4-33.

This section addresses the following:

- Configuring IP Unnumbered for Video and VoIP Services on AR1
- Establishing VLANs for Services on AR1
- Establishing 10-GE Interfaces for Transport on AR1
- Establishing 1-GE Interfaces to a DSLAM on AR1

Note 10-GE interfaces are configured on AR1, but port channels are not.

Configuring IP Unnumbered for Video and VoIP Services on AR1

Service mapping on each DSLAM is achieved by using VLANs, with a single VLAN allocated to video and VoIP services represented as N:1. High-speed data (HSD) traffic requires a single VLAN per subscriber, notated as 1:1. VLANs are not bridged on the AR; in other words, a VLAN defined on the AR does not span multiple DSLAMs on that AR. Consequently, IP unnumbered is used to reduce the operational overhead associated with assigning unique IP subnets per DSLAM. With IP unnumbered we can reduce operational overhead on the AR by assigning one /16 subnet to a service for all DSLAMs aggregated by an AR. With the exception of HSD, all interfaces are Layer 3 subinterfaces. The 1:1 requirement for HSD service increases the number of VLANs required in the services provider's network. To reduce the number of required VLANs, QinQ is used. (See Table 4-6 on page 4-34.)

Note For additional details, see Establishing VLANs for Services and Transport on DER1, page 4-39.

Step 1 In global configuration mode, configure IP unnumbered by establishing two loopback interfaces, one for video services and one VoIP services.

```
interface Loopback0
 description Address block for Video Services on AR1
 ip address 10.10.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30


interface Loopback1
 description Address block for VoIP services on AR1
 ip address 10.20.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30
```

Step 2 In global configuration mode, configure IP unnumbered to use "connected" host routes.

```
ip dhcp route connected
```

Establishing VLANs for Services on AR1

Before 1-GE interfaces and 10-GE trunks can be configured, VLANs for the various services must be created. With the exception of the VLAN range for high-speed data (HSD), these are all Layer 3 VLANs. (Refer to Table 4-6 on page 4-34.)

Do the following to establish VLANs for services on AR1.

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

```
vlan 1100-1111
```

Step 2 Establish a range of VLANs for video at the edge.

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

```
vlan 100-111
```

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

```
interface range Vlan100-111
 description Video edge VLAN on DSLAM
 no ip redirects
 no ip unreachables
```

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

```
ip pim sparse-mode
```

d. To ensure consistently fast PIM convergence times, statically join the aggregation VLAN range 100 through 111 for video at the AR to the multicast groups.

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

e. Change the ARP timeout from the default.

```
arp timeout 250
```

Step 3 Establish a range of VLANs for VoIP at the edge.

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

```
vlan 200-211
```

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

```
interface range Vlan200-211
 description VoIP edge VLAN on DSLAM
 no ip redirects
 no ip unreachables
```

c. Change the load interval from the default of 300 for VLAN range.

```
 load-interval 30
```

Step 4 Establish VLANs for transport. The first is to and from DER1.

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

```
vlan 808
name VLAN_808_Video_VoIP_to/from_DER1
```

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

```
interface Vlan808
 description Transport to/from DER1 (TenGig7/1)
 ip address 10.1.1.10 255.255.255.252
```

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

```
ip pim sparse-mode
```

d. Configure OSPF on the transport VLAN interface.

```
ip ospf network point-to-point
```

```
 ip ospf hello-interval 1
```

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

```
load-interval 30
```

f. Repeat Step 4a through Step 4d, as appropriate, to establish a VLAN for video/VoIP transport to and from DER2.

```
vlan 824
name VLAN_824_Video_VoIP_to/from_DER2

interface Vlan824
 description Transport to/from DER2 (TenGig7/1)
 ip address 10.1.1.26 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Establishing 10-GE Interfaces for Transport on AR1

The 10-GE trunk interfaces provide the transport from AR1 to DER1 and DER2.

Note For additional details, see Establishing 10-GE Interfaces for Transport on DER1, page 4-44.

Do the following to establish 10-GE interfaces for transport on AR1.

Step 1 Establish an interface to and from DER1.

a. Establish the interface to and from DER1, configure the trunk for 802.1q encapsulation, and assign it to VLANs 808 and 1100 through 1111. (Refer to Table 4-6 on page 4-34.)

```
interface TenGigabitEthernet1/1
 description Transport to/from DER1 (TenGig7/1)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 808, 1100-1111
 switchport mode trunk
 dampening 5 1000 2000 20 restart 16000
 no ip address
 load-interval 30
 carrier-delay msec 0
```

b. Proceed as in Step 2 of Establishing 10-GE Interfaces for Transport on DER1, page 4-44.

```
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 mls qos trust dscp
```

Step 2 Establish an interface to and from DER2.

a. Repeat Step 1, as appropriate, to establish an interface to and from DER2 and assign it to VLANs 824 and 1100 through 1111.

```
interface TenGigabitEthernet1/3
 description Transport to/from DER2 (TenGig7/1)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 824, 1100-1111
 switchport mode trunk
 dampening 5 1000 2000 20 restart 16000
 no ip address
 load-interval 30
 carrier-delay msec 0
```

b. Proceed as in Step 2 of Establishing 10-GE Interfaces for Transport on DER1, page 4-44.

```
wrr-queue bandwidth 64 255 0 0 0 0 0
wrr-queue queue-limit 40 50 0 0 0 0 0
wrr-queue threshold 2 80 100 100 100 100 100 100 100
wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
no wrr-queue random-detect 2
wrr-queue cos-map 1 1 0 1
wrr-queue cos-map 2 2 3 4 6 7
mls qos trust dscp
```

Establishing 1-GE Interfaces to a DSLAM on AR1

Two 1-GE interfaces are connected to and from each DSLAM. DSLAMs have two uplinks that are configured as IEEE 802.1q trunks. The first DSLAM uplink carries two VLANs, one video VLAN and one VoIP VLAN. The second DSLAM uplink carries one HSD VLAN per subscriber. QinQ is used with HSD to reduce the number of VLANs required in the service provider's network. (See Common Task: Configuring QinQ and Spanning Tree, page 4-35.) Each QinQ tunnel (one per DSLAM) is terminated upstream on a BRAS that is connected to a DER (in our case, DER1).

Do the following to establish 1-GE interfaces to a DSLAM on AR1.

Step 1 Establish an interface to DSLAM1 uplink 1.

a. Establish the interface and assign it to VLANs 100 and 200.

```
interface GigabitEthernet2/1
 description GigE trunk for video and VoIP to/from DSLAM uplink GigE
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,200
 switchport mode trunk
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
```

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

```
load-interval 30
```

c. Change the ARP timeout from the default.

```
arp timeout 250
```

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

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

```
no cdp enable
```

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

```
spanning-tree portfast
```

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

```
spanning-tree bpduguard enable
```

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

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

```
service-policy input setDSCP
```

Step 2 Establish an interface to DSLAM1 uplink 2.

a. Establish the interface and assign it to VLAN 1100.

```
interface GigabitEthernet2/2
 description GigE QinQ port for HSD to/from DSLAM uplink GigE
 switchport
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
```

Note No QoS policy is required on the HSD interface, so all HSD packets are rewritten to the default DSCP value, 0.

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

```
load-interval 30
```

c. Proceed as in Step 2 of Establishing 10-GE Interfaces for Transport on DER1, page 4-44.

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

```
no cdp enable
```

e. Set the Service Provider outer VLAN tag, or S-TAG, for the HSD VLANs. Assign one tag from the range of VLANs listed in Table 4-7 on page 4-35.

```
switchport access vlan 1100
```

f. Set the port mode to QinQ (dot1q tunnel).

```
switchport mode dot1q-tunnel
```

Configuring OSPF Routing for Video and Voice Traffic on AR1

Do the following to configure OSPF for video and voice traffic on AR1.

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

```
router ospf 100
 router-id 10.1.1.3
 log-adjacency-changes
```

Step 2 Modify various timer parameters.

a. Use the following command to enable OSPF SPF throttling, modifying the timers, and provide fast convergence: **timers throttle spf** spf-*start spf-hold spf-max-wait*

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

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

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

c. Use the following command to control the minimum interval for accepting the same LSA: **timers lsa arrival** *milliseconds*

```
timers lsa arrival 100
```

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

Step 3 Use the following command to set incremental SPF updates for LSA type 1 and LSA type 2 within an area. Enabling iSPF can minimize the effect of SPF changes within an area to only those routers where the change is relevant, thus reducing the time spent calculating SPF.

```
ispf
```

Step 4 Advertise the networks in the first OSPF routing process.

```
network 10.1.1.8 0.0.0.3 area 0
network 10.1.1.24 0.0.0.3 area 0
network 10.10.0.0 0.0.255.255 area 0
network 10.20.0.0 0.0.255.255 area 0
```

Step 5 To support load sharing, set the maximum number of parallel routes the IP routing protocol supports (installs in a routing table).

```
maximum-paths 8
```

Configuring QinQ and Spanning Tree on AR1

See Common Task: Configuring QinQ and Spanning Tree, page 4-35.

Do the following in global configuration mode to configure QinQ and spanning tree parameters on AR1.

Step 1 Create the HSD VLAN ranges.

```
vlan 1100-1111,1200-1211
```

Step 2 Enable QinQ tunneling.

```
vlan dot1q tag native
```

Step 3 Configure RSTP.

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

Configuring AR2

This section addresses the configuration required on the switch labeled AR2 in Figure 4-2 on page 4-33, to route multiple services from AR2 to DER1 and DER2.

See Configuring DNS Servers, page 4-2.

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

This section addresses the following:

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

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

Configuring QoS on AR2

See Overview of QoS on a Cisco 7600 Series and Cisco Catalyst 6500 Series, page 4-11. This section presents the following topics:

- Configuring Marking and Classification on AR2
- Configuring Mapping on AR1

Configuring Marking and Classification on AR2

Do the following to enable marking and classification on AR2.

Step 1 Enable QoS in global configuration mode.

```
mls qos
```

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

```
ip access-list extended acl_VoD_and_SIP_signaling
 permit tcp 10.1.60.0 0.0.0.255 any
 permit tcp 10.1.61.0 0.0.0.255 any
 permit tcp 10.1.80.0 0.0.0.255 any
 permit tcp 10.1.81.0 0.0.0.255 any

ip access-list extended acl_VoIP
 permit udp any any range 16384 32767
 permit udp any range 16384 32767 any
```

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

```
class-map match-all class_VoIP
 match access-group name acl_VoIP
class-map match-all class_VoD_and_SIP_signaling
 match access-group name acl_VoD_and_SIP_signaling
```

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

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

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

```
service-policy input setDSCP
```

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

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

```
mls qos trust dscp
```

Configuring Mapping on AR2

To configure mapping on AR2, proceed as in Configuring Mapping on AR1, page 4-59.

Establishing and Configuring Interfaces on AR2

Refer to Figure 4-2 on page 4-33.

This section addresses the following:

- Configuring IP Unnumbered for Video and VoIP Services on AR2
- Establishing VLANs for Services on AR2
- Establishing Nx1-GE Interfaces for Transport on AR2
- Establishing 1-GE Interfaces to a DSLAM on AR2

Note Port channels are configured on AR2, but 10-GE interfaces are not.

Configuring IP Unnumbered for Video and VoIP Services on AR2

For background, see Configuring IP Unnumbered for Video and VoIP Services on AR1, page 4-60.

Do the following to configure IP unnumbered for video and VoIP services on AR2.

Step 1 In global configuration mode, configure IP unnumbered by establishing two loopback interfaces, one for video services and one for VoIP services.

```
interface Loopback0
 description Address block for Video Services on AR2
 ip address 10.11.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30
```

```
interface Loopback1
 description Address block for VoIP services on AR2
 ip address 10.21.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30
```

Step 2 In global configuration mode, configure IP unnumbered to use "connected" host routes.

```
ip dhcp route connected
```

Establishing VLANs for Services on AR2

Before 1-GE interfaces and 10-GE trunks can be configured, VLANs for the various services must be created. With the exception of the high-speed data (HSD) VLAN range, these are all Layer 3 VLANs. (Refer to Table 4-6 on page 4-34.)

Do the following to establish VLANs for services on AR2.

Step 1 In global configuration mode, establish a range of VLANs for HSD. (No Layer 3 interface is required.)

```
vlan 1200-1211
```

Step 2 Establish a range of VLANs for video at the edge.

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

```
vlan 100-111
```

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

```
interface range Vlan100-111
 description Video edge VLAN on DSLAM
 no ip redirects
 no ip unreachables
```

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

```
 ip pim sparse-mode
```

d. To ensure consistently fast PIM convergence times, statically join the aggregation VLAN range 100 through 111 for video at the AR to the multicast groups.

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

e. Change the ARP timeout from the default.

```
arp timeout 250
```

Step 3 Establish a range of VLANs for VoIP at the edge.

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

```
vlan 200-211
```

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

```
interface range Vlan200-211
 description VoIP edge VLAN on DSLAM
 no ip redirects
 no ip unreachables
```

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

```
 load-interval 30
```

Step 4 Establish VLANs for video and VoIP transport. The first is to and from DER1.

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

```
vlan 816
name VLAN_816_Video_VoIP_to/from_DER1
```

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

```
interface Vlan816
 description Transport to/from DER1 (TenGig7/1)
 ip address 10.1.1.18 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

c. Configure OSPF on the transport VLAN interface.

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

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

```
load-interval 30
```

e. Repeat Step 4a through Step 4d, as appropriate, to establish a VLAN for video and VoIP transport to and from DER2.

```
vlan 832
name VLAN_832_Video_VoIP_to/from_DER2

interface Vlan832
 description Transport to/from DER2 (TenGig7/1)
 ip address 10.1.1.34 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

Establishing Nx1-GE Interfaces for Transport on AR2

Do the following to establish Nx1-GE interfaces on AR2. (See Table 4-6 on page 4-34.)

Step 1 Proceed as in Establishing Nx1-GE Interfaces for Transport on DER1, page 4-47.

Step 2 Establish a 1-GE interface to and from DER1.

a. Establish the interface.

```
interface GigabitEthernet1/5
 description Transport to/from DER1 (GigE1/1)
 switchport
 switchport mode trunk
 no ip address
 no keepalive
```

b. Configure the trunk for 802.1q encapsulation.

```
switchport trunk encapsulation dot1q
```

c. Assign the trunk to VLAN 816 and VLAN range 1200–1211.

```
switchport trunk allowed vlan 816,1200-1211
```

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

```
load-interval 30
```

e. Configure interface link detect options, such as **carrier-delay**, to reduce the time to detect a link failure, and **dampening** to minimize the effects of flapping links.

Note The **restart** command option is applied on start up to reduce the possibility of routing "black holes" during startup (where upper layers converge before lower layers do).

```
carrier-delay msec 0
dampening 5 1000 2000 20 restart 16000
```

Step 3 Establish a 1-GE interface to and from DER2.

a. Establish the interface.

```
interface GigabitEthernet1/5
 description Transport to/from DER2 (GigE1/1)
 switchport
 switchport mode trunk
 no ip address
 no keepalive
```

b. Configure the trunk for 802.1q encapsulation.

```
switchport trunk encapsulation dot1q
```

c. Assign the trunk to VLAN 832 and VLAN range 1200–1211.

```
switchport trunk allowed vlan 832,1200-1211
```

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

```
load-interval 30
```

e. Configure interface link detect options, such as **carrier-delay**, to reduce the time to detect a link failure, and **dampening** to minimize the effects of flapping links.

Note The **restart** command option is applied on start up to reduce the possibility of routing "black holes" during startup (where upper layers converge before lower layers do).

```
carrier-delay msec 0
dampening 5 1000 2000 20 restart 16000
```

Step 4 Repeat Step 1 and Step 2 for additional 1-GE transport links as required.

Step 5 Configure QoS on a 1-GE transport link.

Note The Nx1-GE transport links from the DER to the ARs require modifications to the transmit queues. There are eight transmit queues, but this solution uses only three.

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

```
queue thresh cos-map
---------------------------------------
1     1      0
1     2      1
2     1      2
2     2      3 4
3     1      6 7
4     1      5
```

b. Configure the CoS-to-TxQueue mapping on the 10-GE transport interfaces. HSD (CoS = 0) remains in TxQueue1 and VoIP (CoS = 5) remains in TxQueue4. Video is separated into two classes, one class for broadcast video (CoS = 4) and one class for VoD video (CoS = 2). The other three CoS values are associated with TxQueue2.

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

Note TxQueue2 has two thresholds: Threshold 1 = CoS 2 (default) and Threshold 2 = CoS 3, 4, 6, and 7.

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

```
queue thresh cos-map
---------------------------------------
1     1      0 1
2     1      2
2     2      3 4 6 7
4     1      5
```

d. Configure the TxQueue thresholds.

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

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

TxQueue2 uses tail drop for queue congestion management. VoD is assigned to threshold 1 and is dropped once the queue reaches 80% utilization. VoD signaling, network signaling, and broadcast video are assigned to threshold 2 and are dropped once the queue reaches 100% utilization.

```
wrr-queue threshold 2 80 100 100 100 100 100 100 100
no wrr-queue random-detect 2
```

e. Configure the bandwidth of the weighted queues.

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

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

f. Configure the size of the weighted queues.

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

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

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

```
mls qos trust dscp
```

Step 6 Repeat Step 5 for any additional 1-GE transport links.

Establishing 1-GE Interfaces to a DSLAM on AR2

Two 1-GE interfaces are connected to and from each DSLAM. DSLAMs have two uplinks that are configured as IEEE 802.1q trunks. The first DSLAM uplink carries two VLANs, one video VLAN and one VoIP VLAN. The second DSLAM uplink carries one HSD VLAN per subscriber. QinQ is used for HSD to reduce the number of VLANs required in the service provider's network. Each QinQ tunnel (one per DSLAM) is terminated upstream on a BRAS that is connected to a DER (in our case, to DER1).

Do the following to establish 1-GE interfaces to a DSLAM on AR2.

Step 1 Establish an interface to DSLAM1 uplink 1.

a. Establish the interface and assign it to VLANs 100 and 200.

```
interface GigabitEthernet2/1
 description GigE trunk for video and VoIP to/from DSLAM uplink GigE
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,200
 switchport mode trunk
 no ip address
```

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

```
service-policy input setDSCP
```

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

```
load-interval 30
```

d. Proceed as in Step 2 of Establishing 10-GE Interfaces for Transport on DER1, page 4-44.

```
wrr-queue bandwidth 64 255 0
wrr-queue queue-limit 40 50 0
wrr-queue threshold 2 80 100 100 100 100 100 100 100
```

```
wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
no wrr-queue random-detect 2
wrr-queue cos-map 1 1 0 1
wrr-queue cos-map 2 2 3 4 6 7
```

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

```
no cdp enable
```

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

```
spanning-tree portfast
```

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

```
spanning-tree bpduguard enable
```

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

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

```
service-policy input setDSCP
```

Step 2 Establish an interface to DSLAM1 uplink 2.

a. Establish the interface and assign it to VLAN 1100.

```
interface GigabitEthernet2/2
 description GigE QinQ port for HSD to/from DSLAM uplink GigE
 switchport
 no ip address
```

Note No QoS policy is required on the HSD interface, so all HSD packets are rewritten to the default DSCP value, 0.

b. Set the Service Provider outer VLAN tag, or S-TAG, for the HSD VLANs.

```
switchport access vlan 1200
```

c. Set the port mode to QinQ (dot1q tunnel).

```
switchport mode dot1q-tunnel
```

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

```
 load-interval 30
```

e. Proceed as in Step 2 of Establishing 10-GE Interfaces for Transport on DER1, page 4-44.

```
wrr-queue bandwidth 64 255 0
wrr-queue queue-limit 40 50 0
wrr-queue threshold 2 80 100 100 100 100 100 100 100
```

```
wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
no wrr-queue random-detect 2
wrr-queue cos-map 1 1 0 1
wrr-queue cos-map 2 2 3 4 6 7
```

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

```
no cdp enable
```

Configuring OSPF Routing for Video and Voice Traffic on AR2

Do the following to configure OSPF for video and voice traffic on AR2.

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

```
router ospf 100
 router-id 10.1.1.4
 log-adjacency-changes
```

Step 2 Modify various timer parameters.

a. Use the following command to enable OSPF SPF throttling, modifying the timers, and provide fast convergence: **timers throttle spf** spf-*start spf-hold spf-max-wait*

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

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

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

c. Use the following command to control the minimum interval for accepting the same LSA: **timers lsa arrival** *milliseconds*

```
timers lsa arrival 100
```

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

Step 3 Use the following command to set incremental SPF updates for LSA type 1 and LSA type 2 within an area. Enabling iSPF can minimize the effect of SPF changes within an area to only those routers where the change is relevant, thus reducing the time spent calculating SPF.

```
ispf
```

Step 4 Advertise the networks in the first OSPF routing process.

```
network 10.1.1.16 0.0.0.3 area 0
network 10.1.1.32 0.0.0.3 area 0
network 10.11.0.0 0.0.255.255 area 0
network 10.21.0.0 0.0.255.255 area 0
```

Step 5 To support load sharing, set the maximum number of parallel routes the IP routing protocol supports (installs in a routing table).

```
maximum-paths 8
```

Configuring QinQ and Spanning Tree on AR2

See Common Task: Configuring QinQ and Spanning Tree, page 4-35.

Do the following in global configuration mode to configure QinQ and spanning tree parameters on AR2.

Step 1 Create the HSD VLAN ranges.

```
vlan 1100-1111,1200-1211
```

Step 2 Enable QinQ tunneling.

```
vlan dot1q tag native
```

Step 3 Configure RSTP.

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

Monitoring and Troubleshooting

This chapter provides an introduction to monitoring and troubleshooting the Cisco Ethernet switches in the Cisco Wireline Video/IPTV Solution, Release 1.1.

The following major topics are presented:

- Network Time Protocol (NTP), page 5-1
- Syslog, page 5-2
- Quality of Service (QoS), page 5-4
- Multicast, page 5-11
- References, page 5-16

Network Time Protocol (NTP)

It is important to ensure that all devices in the network are accurately synchronized to the same time source. This allows network events to be correlated (for example, for accounting, event logging, fault analysis, security incident response, and network management). The Network Time Protocol (NTP), RFC 1305, synchronizes timekeeping among a set of distributed time servers and clients.

Note There are a number of ways to configure NTP, and describing NTP completely is beyond the scope of this document. A number of resources are available on Cisco.com and the Internet regarding NTP configuration.

At a minimum, the Cisco switches should be configured as NTP clients for a reliable time source, by means of the following commands:

```
clock timezone PST -8
clock summer-time PDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00

clock calendar-valid
ntp server <NTP server IP address>
ntp update-calendar
```

Syslog

Cisco IOS Software has the capability to do UNIX system logging (syslog) to a UNIX syslog server. The Cisco UNIX syslog format is compatible with 4.3 Berkeley Standard Distribution (BSD) UNIX. System logging is useful for monitoring interface status, security alerts, environmental conditions, CPU processes, and many other events on the router can be captured and analyzed by means of UNIX syslog. Management platforms such as Cisco Resource Manager Essentials (RME) and Network Analysis Toolkit (NATKit) make powerful use of syslog information to collect inventory and configuration changes.

The following is a summary and description of the recommended IOS configuration for syslog.

Global Syslog Configuration

Configure the following in global configuration mode:

```
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging host-ip
logging source-interface loopback 0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
```

Interface Syslog Configuration

Configure the following in interface configuration mode on interfaces of interest:

```
logging event link-status
logging event bundle-status
```

Useful Syslog Commands

The following syslog commands are particularly useful:

- no logging console
- no logging monitor
- logging buffered 16384
- logging trap notifications
- logging facility local7
- logging host
- logging source-interface loopback 0
- service timestamps debug datetime localtime show-timezone msec
- logging event

no logging console

By default, all system messages are sent to the system console. Console logging is a high-priority task in Cisco IOS Software. This function was primarily designed to generate error messages to the system operator prior to a system failure. It is recommended that console logging be disabled in all device configurations to avoid a situation where the router/switch might hang while waiting for a response from a terminal. Console messages can, however, be useful during trouble isolation. In these instances, console logging should be enabled by means of the **logging console level** command, to obtain the desired level of message logging. Logging levels range from 0 to 7.

no logging monitor

This command disables logging for terminal lines other than the system console. If monitor logging is required (by means of **logging monitor debugging** or another command option), it should be enabled at the specific logging level required for the activity (see above).

logging buffered 16384

The **logging buffered** command should be added to log system messages in the internal log buffer. The logging buffer is circular. Once the logging buffer is filled, older entries are overwritten by newer entries. The size of the logging buffer is user-configurable and is specified in bytes. The size of the system buffer varies by platform. 16384 is a good default and should provide adequate logging in most cases.

logging trap notifications

This command provides notification (level 5) messaging to the specified syslog server. The default logging level for all devices (console, monitor, buffer, and traps) is debugging (level 7). Leaving the trap logging level at 7 produces many extraneous messages that are of little or no concern to the health of the network. It is recommended that the default logging level for traps be set to 5.

logging facility local7

This command sets the default logging facility/level for UNIX system logging. The syslog server receiving these messages should be configured for the same facility/level.

logging host

This command sets the IP address of the UNIX syslog server.

logging source-interface loopback 0

This command sets the default IP source address for the syslog messages. Hard coding the logging source address makes it easier to identify the host that sent the message.

service timestamps debug datetime localtime show-timezone msec

By default, log messages are not time stamped. Use this command to enable the time stamping of log messages and configure the time stamping of system debug messages. Time stamping enhances real-time debugging by providing the relative timing of logged events. This information is especially useful when

customers send debugging output to technical support personnel for assistance. To enable the time stamping of system debug messages, use the above command in global configuration mode. This only has an affect when debugging is enabled.

logging event

The **logging event link-status** command enables logging related to link status. The **logging event bundle-status** command enables logging related to bundle status.

Quality of Service (QoS)

The following commands are useful in troubleshooting QoS:

- show class-map
- show policy-map
- show qos maps
- show mls qos maps dscp-cos
- show qos interface
- show queueing interface

show class-map

To verify the class map for QoS classification, use the **show class-map** command.

```
DER# show class-map

 Class Map match-all class_VoIP (id 1)
   Match access-group name acl_VoIP

 Class Map match-any class-default (id 0)
   Match any

 Class Map match-all class_video_VoD_high (id 2)
   Match access-group name acl_video_VoD_high

 Class Map match-all class_video_VoD_low (id 3)
   Match access-group name acl_video_VoD_low

 Class Map match-all class_video_broadcast (id 4)
   Match access-group name acl_video_broadcast

 Class Map match-all class_VoD_signaling (id 5)
   Match access-group name acl_VoD_signaling

 Class Map match-all class_HSD (id 6)
   Match access-group name acl_HSD
```

show policy-map

To verify the policy map for QoS marking, use the **show policy-map** command.

```
DER# show policy-map
```

```
 Policy Map setDSCP
     Description: Mark DSCP values for ingress traffic
   Class class_VoIP
     set dscp ef
   Class class_HSD
     set dscp default
   Class class_VoD_signaling
     set dscp cs3
   Class class_video_broadcast
     set dscp af41
   Class class_video_VoD_high
     set dscp af42
   Class class_video_VoD_low
     set dscp af43
```

show qos maps

On Cisco Catalyst 4500 and Cisco Catalyst 4948-10GE switches, use the **show qos maps** command to verify the DSCP-to-TxQueue and DSCP-to-CoS mappings.

```
AR2# show qos maps

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

<omitted DSCP policing table>

DSCP-CoS Mapping Table (dscp = d1d2)
d1 : d2  0  1  2  3  4  5  6  7  8  9
------------------------------------
 0 :    00 00 00 00 00 00 00 00 01 01
 1 :    01 01 01 01 01 01 02 02 02 02
 2 :    02 02 02 02 03 03 03 03 03 03
 3 :    03 03 04 04 04 04 02 04 01 04
 4 :    05 05 05 05 05 05 05 05 06 06
 5 :    06 06 06 06 06 06 07 07 07 07
 6 :    07 07 07 07

<omitted CoS to DSCP mapping table>
```

show mls qos maps dscp-cos

On the Cisco Catalyst 6500 and Cisco 7600 switches, use the **show mls qos maps dscp-cos** command to verify the DSCP-to-CoS mappings.

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

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

```
1 :    01 01 01 01 01 01 02 02 02 02
2 :    02 02 02 02 03 03 03 03 03 03
3 :    03 03 04 04 04 04 02 04 01 04
4 :    05 05 05 05 05 05 05 05 06 06
5 :    06 06 06 06 06 06 07 07 07 07
6 :    07 07 07 07
```

show qos interface

On the Cisco Catalyst 4500 and Cisco Catalyst 4948-10GE switches, use the **show qos interface** *type slot/module* to verify the QoS state, port trust state, queue bandwidth, priority queue, and queue size.

```
AR2# show qos interface tenGigabitEthernet 1/1

QoS is enabled globally
Port QoS is enabled
Administrative Port Trust State: 'dscp'
Operational Port Trust State: 'dscp'
Trust device: none
Default DSCP: 0 Default CoS: 0
Appliance trust: none
Tx-Queue   Bandwidth   ShapeRate   Priority   QueueSize
             (bps)       (bps)               (packets)
  1        1900000000  disabled    N/A        2080
  2        8000000000  disabled    N/A        2080
  3        2500000000  disabled    high       2080
  4        100000000   disabled    N/A        2080
```

show queueing interface

On the Cisco Catalyst 6500 and Cisco 7600 switches, use the **show queueing interface** *type slot/module* command to verify the queueing strategy, priority queue, WRR bandwidths, queue sizes, thresholds, CoS-to-queue mappings, and queue drops.

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

Interface TenGigabitEthernet7/1 queueing strategy:  Weighted Round-Robin
  Port QoS is enabled
  Trust state: trust DSCP
  Extend trust state: not trusted [COS = 0]
  Default COS is 0
    Queueing Mode In Tx direction: mode-cos
    Transmit queues [type = 1p7q8t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       01         WRR                 08
       02         WRR                 08
       03         WRR                 08
       04         WRR                 08
       05         WRR                 08
       06         WRR                 08
       07         WRR                 08
       08         Priority            01

    WRR bandwidth ratios:   64[queue 1] 255[queue 2]   0[queue 3]   0[queue 4]   0[queue
5]   0[queu
e 6]   0[queue 7]
    queue-limit ratios:     40[queue 1]  50[queue 2]   0[queue 3]   0[queue 4]   0[queue
5]   0[queu
```

```
e 6]   0[queue 7]

    queue tail-drop-thresholds
    --------------------------
    1     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    2     45[1] 85[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    3     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    4     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    5     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    6     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    7     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]

    queue random-detect-min-thresholds
    ----------------------------------
      1    75[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      2    40[1] 70[2] 70[3] 70[4] 70[5] 70[6] 70[7] 70[8]
      3    70[1] 70[2] 70[3] 70[4] 70[5] 70[6] 70[7] 70[8]
      4    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      5    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      6    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      7    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]

    queue random-detect-max-thresholds
    ----------------------------------
      1    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      2    70[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      3    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      4    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      5    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      6    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      7    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]

    WRED disabled queues:      2  4  5  6  7

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

```
    4     5
    4     6
    4     7
    4     8
    5     1
    5     2
    5     3
    5     4
    5     5
    5     6
    5     7
    5     8
    6     1
    6     2
    6     3
    6     4
    6     5
    6     6
    6     7
    6     8
    7     1
    7     2
    7     3
    7     4
    7     5
    7     6
    7     7
    7     8
    8     1      5

    Queueing Mode In Rx direction: mode-cos
    Receive queues [type = 8q8t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       01         WRR                 08
       02         WRR                 08
       03         WRR                 08
       04         WRR                 08
       05         WRR                 08
       06         WRR                 08
       07         WRR                 08
       08         WRR                 08

    WRR bandwidth ratios:  100[queue 1]   0[queue 2]   0[queue 3]   0[queue 4]   0[queue
5]   0[queu
e 6]   0[queue 7]   0[queue 8]
    queue-limit ratios:    100[queue 1]   0[queue 2]   0[queue 3]   0[queue 4]   0[queue
5]   0[queu
e 6]   0[queue 7]   0[queue 8]

    queue tail-drop-thresholds
    --------------------------
    1     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    2     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    3     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    4     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    5     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    6     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    7     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    8     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]

    queue random-detect-min-thresholds
    ----------------------------------
      1    40[1] 40[2] 50[3] 50[4] 50[5] 50[6] 50[7] 50[8]
```

```
  2    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  3    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  4    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  5    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  6    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  7    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  8    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]

queue random-detect-max-thresholds
----------------------------------
  1    70[1] 80[2] 90[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  2    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  3    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  4    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  5    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  6    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  7    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
  8    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]

WRED disabled queues:      1  2  3  4  5  6  7  8

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

```
  6      2
  6      3
  6      4
  6      5
  6      6
  6      7
  6      8
  7      1
  7      2
  7      3
  7      4
  7      5
  7      6
  7      7
  7      8
  8      1
  8      2
  8      3
  8      4
  8      5
  8      6
  8      7
  8      8


Packets dropped on Transmit:

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

Packets dropped on Receive:

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

Multicast

The following commands are useful in troubleshooting multicast:

- show ip mroute
- show ip mroute ssm
- show ip mroute active
- show ip pim neighbor
- show ip igmp snooping
- show ip igmp groups
- show ip igmp ssm-mapping
- show ip igmp membership
- debug ip igmp
- debug ip pim
- debug domain

show ip mroute

To see the details of the multicast routing table, use the **show ip mroute** command. The output of this command also shows the legend for the flags.

```
AR3# show ip mroute

IP Multicast Routing Table

Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,

L - Local, P - Pruned, R - RP-bit set, F - Register flag,

T - SPT-bit set, J - Join SPT, M - MSDP created entry,

X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,

U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel

Y - Joined MDT-data group, y - Sending to MDT-data group

Outgoing interface flags: H - Hardware switched, A - Assert winner

Timers: Uptime/Expires

Interface state: Interface, Next-Hop or VCD, State/Mode

(192.168.70.101, 232.1.5.220), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan130, Forward/Sparse, 1w1d/00:01:46, H

(192.168.70.101, 232.1.5.221), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0
```

```
Outgoing interface list:

Vlan130, Forward/Sparse, 1w1d/00:01:46, H

(192.168.70.101, 232.1.5.222), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan130, Forward/Sparse, 1w1d/00:01:46, H

(192.168.70.101, 232.1.5.223), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:
```

show ip mroute ssm

To verify the source-specific multicast (SSM) mapping of multicast groups to multicast sources, use the **show ip mroute ssm** command. With this command, you can also verify the path of the multicast ingress and egress interface(s).

Tip To see the legend for the flags field, you must use the **show ip mroute** command.

```
AR2# show ip mroute ssm

(192.168.70.101, 232.1.5.220), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan130, Forward/Sparse, 1w1d/00:01:40, H

(192.168.70.101, 232.1.5.221), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan130, Forward/Sparse, 1w1d/00:01:40, H

(192.168.70.101, 232.1.5.222), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:

Vlan130, Forward/Sparse, 1w1d/00:01:40, H

(192.168.70.101, 232.1.5.223), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:
```

```
Vlan130, Forward/Sparse, 1w1d/00:01:40, H

(192.168.70.101, 232.1.5.216), 1w4d/stopped, flags: sTI

Incoming interface: Null, RPF nbr 0.0.0.0

Outgoing interface list:
```

show ip mroute active

To verify the bitrate of a multicast group, use the **show ip mroute active** command.

```
AR2# show ip mroute active

Active IP Multicast Sources - sending >= 4 kbps

Group: 232.255.0.1, (?)
   Source: 192.168.71.105 (1.0.255.232.coronado.net)
     Rate: 334 pps/3517 kbps(1sec), 2829 kbps(last 30 secs), 2703 kbps(life avg)

<rest of the output omitted>
```

show ip pim neighbor

To verify the protocol-independent multicast (PIM) neighbors, use the **show ip pim neighbor** command.

```
AR2# show ip pim neighbor

PIM Neighbor Table
Neighbor          Interface               Uptime/Expires    Ver   DR
Address                                                           Prio/Mode
192.168.254.9     Vlan908                 1d16h/00:01:34    v2    1 / S
192.168.254.18    Vlan916                 1d16h/00:01:24    v2    1 / DR S
```

show ip igmp snooping

To verify IGMP snooping on the switch and interfaces, use the **show ip igmp snooping** command.

```
AR2# show ip igmp snooping

Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             : Enabled
IGMPv3 snooping           : Enabled
Report suppression        : Enabled
TCN solicit query         : Disabled
TCN flood query count     : 2

Vlan 1:
--------
IGMP snooping                       : Enabled
IGMPv2 immediate leave              : Disabled
Explicit host tracking              : Enabled
Multicast router learning mode      : pim-dvmrp
CGMP interoperability mode          : IGMP_ONLY

Vlan 70:
--------
```

```
IGMP snooping                          : Enabled
IGMPv2 immediate leave                 : Disabled
Explicit host tracking                 : Enabled
Multicast router learning mode         : pim-dvmrp
CGMP interoperability mode             : IGMP_ONLY

<rest of output omitted>
```

show ip igmp groups

To verify IGMP group membership on a switch, use the **show ip igmp groups** command.

```
AR2# show ip igmp groups

IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
232.255.0.1      Vlan120                  1d17h     stopped   0.0.0.0
232.255.0.2      Vlan120                  1d17h     stopped   0.0.0.0
232.255.0.3      Vlan120                  1d17h     stopped   0.0.0.0
232.255.0.5      Vlan120                  1d17h     stopped   0.0.0.0
232.255.0.12     Vlan120                  1d17h     stopped   0.0.0.0
224.0.1.40       Vlan120                  1d16h     00:02:56  192.168.120.1
```

show ip igmp ssm-mapping

To verify the SSM mapping configuration on the switch, use the **show ip igmp ssm-mapping** command.

```
AR3# show ip igmp ssm-mapping

SSM Mapping  : Enabled
DNS Lookup   : Enabled
Mcast domain : coronado.net
Name servers : 192.168.11.101
```

show ip igmp membership

Another command to verify IGMP group membership, which provides some additional information compared to the previous command, is the **show ip igmp membership** command.

```
AR2# show ip igmp membership

Flags: A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, U - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP, the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (G))
Reporter:
       <mac-or-ip-address> - last reporter if group is not explicitly tracked
       <n>/<m>      - <n> reporter in include mode, <m> reporter in exclude

 Channel/Group                 Reporter        Uptime   Exp.  Flags  Interface
/*,232.255.0.1                 0.0.0.0         1d17h    stop  2MA    Vl120
 192.168.71.105,232.255.0.1                    1d17h    stop  SA     Vl120
/*,232.255.0.2                 0.0.0.0         1d17h    stop  2MA    Vl120
 192.168.71.105,232.255.0.2                    1d17h    stop  SA     Vl120
/*,232.255.0.3                 0.0.0.0         1d17h    stop  2MA    Vl120
 192.168.71.105,232.255.0.3                    1d17h    stop  SA     Vl120
```

```
/*,232.255.0.5                  0.0.0.0         1d17h    stop  2MA    Vl120
 192.168.71.105,232.255.0.5                     1d17h    stop  SA     Vl120
/*,232.255.0.12                 0.0.0.0         1d17h    stop  2MA    Vl120
 192.168.71.105,232.255.0.12                    1d17h    stop  SA     Vl120
 *,224.0.1.40                   192.168.120.1   1d16h    02:22 2LA    Vl120
```

debug ip igmp

To troubleshoot IGMP issues, use the **debug ip igmp** command. The debug output indicates IGMP membership queries, membership responses, and the conversion of IGMPv2 to IGMPv3 through DNS lookup.

```
AR2# debug ip igmp

IGMP debugging is on
AR2#
*Aug  8 14:20:53.039: IGMP(0): Received v2 Query on Vlan908 from 192.168.254.9
AR2#
*Aug  8 14:21:16.880: IGMP(0): Send v2 general Query on Vlan120
*Aug  8 14:21:16.880: IGMP(0): Set report delay time to 8.4 seconds for 224.0.1.40 on
Vlan120
*Aug  8 14:21:16.880: IGMP(0): Send v2 general Query on Vlan916
AR2#
*Aug  8 14:21:25.881: IGMP(0): Send v2 Report for 224.0.1.40 on Vlan120
*Aug  8 14:21:25.881: IGMP(0): Received v2 Report on Vlan120 from 192.168.120.1 for
224.0.1.40
*Aug  8 14:21:25.881: IGMP(0): Received Group record for group 224.0.1.40, mode 2 from
192.168.120.1
 for 0 sources
*Aug  8 14:21:25.881: IGMP(0): Updating EXCLUDE group timer for 224.0.1.40
*Aug  8 14:21:25.881: IGMP(0): MRT Add/Update Vlan120 for (*,224.0.1.40) by 0
AR2#
*Aug  8 14:21:39.089: IGMP(0): Convert IGMPv2 static (*, 232.255.0.1) to IGMPv3 with 1
source(s) using DNS
*Aug  8 14:21:39.089: IGMP(0): Convert IGMPv2 static (*, 232.255.0.2) to IGMPv3 with 1
source(s) using DNS
*Aug  8 14:21:39.089: IGMP(0): Convert IGMPv2 static (*, 232.255.0.3) to IGMPv3 with 1
source(s) using DNS
*Aug  8 14:21:39.089: IGMP(0): Convert IGMPv2 static (*, 232.255.0.5) to IGMPv3 with 1
source(s) using DNS
*Aug  8 14:21:39.089: IGMP(0): Convert IGMPv2 static (*, 232.255.0.12) to IGMPv3 with 1
source(s) using DNS
```

debug ip pim

To troubleshoot PIM issues, use the **debug ip pim** command. The output indicates join and prune messages for PIM.

```
AR2# debug ip pim

PIM debugging is on
AR2#
*Aug  8 14:23:04.149: PIM(0): Building Periodic Join/Prune message for 232.255.0.1
*Aug  8 14:23:04.149: PIM(0): Insert (192.168.71.105,232.255.0.1) join in nbr
192.168.254.18's queue
*Aug  8 14:23:04.149: PIM(0): Building Join/Prune packet for nbr 192.168.254.18
*Aug  8 14:23:04.149: PIM(0): Adding v2 (192.168.71.105/32, 232.255.0.1), S-bit Join
*Aug  8 14:23:04.149: PIM(0): Send v2 join/prune to 192.168.254.18 (Vlan916)
```

debug domain

To troubleshoot domain name server (DNS) lookup issues, use the **debug domain** command.

```
AR2# debug domain

Aug  8 21:28:34.274: Domain: query for 1.0.255.232.coronado.net type 1 to 192.168.11.101
Aug  8 21:28:34.274: DOM: dom2cache: hostname is 1.0.255.232.coronado.net, RR type=1,
class=1, ttl=43200, n=4
Reply received ok
```

References

The following documents provide practical tips on configuring the switches used in the solution.

- *Best Practices for Catalyst 6500/6000 Series and Catalyst 4500/4000 Series Switches Running Cisco IOS Software*, at the following URL:

  http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products_white_paper09186a00801b49a4.shtml#cg24

- *Cisco ISP Essentials: Essential IOS Features Every ISP Should Consider,* by Barry Green and Philip Smith, at the following URL:

  http://wwwin-cons.cisco.com/~philsmit/isp/workshop/afnog2004/inet2000/adv-bgp/iosess29.pdf

Note A Cisco Connection Online (CCO) password may be required to access these documents.

Sample DER and AR Switch Configurations for the 10-GE Ring Topology

This appendix presents sample distribution edge router (DER) and aggregation router (AR) switch configurations for the symmetric 10-GE topology described in Configuration 1: 10-GE Layer 3 Ring, page 3-38. The following configurations are presented:

- Configuration for DER1, page A-1
- Configuration for DER2, page A-10
- Configuration for AR1, page A-18
- Configuration for AR2, page A-35
- Configuration for AR3, page A-52

Note See Configuring the 10-GE Ring Topology, page 4-5.

Configuration for DER1

```
Building configuration...

Current configuration : 52268 bytes
!
! Last configuration change at 13:02:28 PDT Mon May 15 2006
! NVRAM config last updated at 13:04:45 PDT Mon May 15 2006
!
upgrade fpd auto
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service counters max age 10
!
hostname DER1
!
boot system disk0:s72033-advipservicesk9_wan-mz.122-18.SXF2.bin
logging snmp-authfail
enable password cisco
!
no aaa new-model
clock timezone PST -8
clock summer-time PDT recurring
```

```
ip subnet-zero
!
!
!
ip cef load-sharing algorithm original
ip multicast-routing
ip igmp ssm-map enable
ip domain multicast coronado.net
no ip domain-lookup
ip domain-name coronado.net
ip name-server 10.1.10.10
ipv6 mfib hardware-switching replication-mode ingress
vtp mode transparent
mpls label protocol ldp
no tag-switching advertise-tags
tag-switching advertise-tags for LOOPBACK
tag-switching tdp router-id Loopback3 force
mls ip cef load-sharing full
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 36 to 2
mls qos
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 rapid-pvst
spanning-tree portfast bpduguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
no spanning-tree vlan 800,808
!
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
port-channel per-module load-balance
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 10
 name VLAN_10_Management
!
vlan 60
 name VLAN_60_VoD
!
```

```
vlan 70
 name VLAN_70_Multicast_Video

vlan 80
 name VLAN_80_Voice
!
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_VoD_and_SIP_signaling
  match access-group name acl_VoD_and_SIP_signaling
class-map match-all class_video_broadcast
  match access-group name acl_video_broadcast
class-map match-all class_video_VoD
  match access-group name acl_video_VoD
!
!
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoD_and_SIP_signaling
   set dscp cs3
  class class_video_broadcast
   set dscp af41
  class class_video_VoD
   set dscp af42
  class class_VoIP
   set dscp ef
!
!
!
interface Loopback3
 description Loopback for MPLS Services
 ip address 10.1.254.1 255.255.255.255
 ip ospf network point-to-point
!
interface GigabitEthernet2/1
 description Management VLAN (CNR - DHCP, DNS, SysLog)
 switchport
 switchport access vlan 10
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/2
 description Middleware Server (Kasenna LivingRoom Server)
 switchport
 switchport access vlan 60
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
```

```
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/3
 description Kasenna Gigabase Server - Management Interface (Eth0)
 switchport
 switchport access vlan 60
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/4
 description Kasenna Gigabase Server - VoD Pump (HPN0)
 switchport
 switchport access vlan 60
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/5
 description Kasenna Gigabase Server - VoD Pump (HPN1)
 switchport
 switchport access vlan 60
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
```

```
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/6
 description Minerva Video Streamer - Multicast Video
 switchport
 switchport access vlan 70
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/7
 description VoIP SIP Server
 switchport
 switchport access vlan 80
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
<---output omitted--->
!
interface GigabitEthernet2/24
 description To/From BRAS for 10GE Ring EoMPLS
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
```

```
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/24.1
 description HSD to/from DSLAM1 on AR1
 encapsulation dot1Q 300
 xconnect 10.1.254.3 300 encapsulation mpls
!
interface GigabitEthernet2/24.2
 description HSD to/from DSLAM1 on AR2
 encapsulation dot1Q 330
 xconnect 10.1.254.4 330 encapsulation mpls
!
interface GigabitEthernet2/24.3
 description HSD to/from DSLAM1 on AR3
 encapsulation dot1Q 360
 xconnect 10.1.254.5 360 encapsulation mpls
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface TenGigabitEthernet7/1
 description Transport to/from AR1 (TenGig1/1)
 dampening 5 1000 2000 20 restart 16000
 mtu 9216
 ip address 10.1.1.9 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 tag-switching ip
 mls qos trust dscp
!
<---output omitted--->
!
interface TenGigabitEthernet7/4
 description Transport to/from DER2 (TenGig7/4)
 dampening 5 1000 2000 20 restart 16000
 mtu 9216
 ip address 10.1.1.1 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
```

```
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 tag-switching ip
 mls qos trust dscp
!
interface Group-Async2
 physical-layer async
 no ip address
 encapsulation slip
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description Management VLAN (CNR - DNS, DHCP, etc)
 ip address 10.1.10.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan60
 description VoD Server VLAN (Unicast Video)
 ip address 10.1.60.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan70
 description Broadcast video source VLAN (Multicast Video)
 ip address 10.1.70.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan80
 description VoIP Gateway VLAN
 ip address 10.1.80.1 255.255.255.0
 load-interval 30
!
router ospf 100
 router-id 10.1.1.1
 ispf
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan10
 passive-interface Vlan60
 passive-interface Vlan70
 passive-interface Vlan80
 network 10.1.1.0 0.0.0.3 area 0
 network 10.1.1.8 0.0.0.3 area 0
```

```
 network 10.1.10.0 0.0.0.255 area 0
 network 10.1.60.0 0.0.0.255 area 0
 network 10.1.70.0 0.0.0.255 area 0
 network 10.1.80.0 0.0.0.255 area 0
 network 10.1.254.1 0.0.0.0 area 0
 maximum-paths 8
!
ip classless
!
no ip http server
ip pim ssm default
!
ip access-list standard LOOPBACK
 permit 10.1.254.0 0.0.0.255
!
ip access-list extended acl_VoD_and_SIP_signaling
 permit tcp 10.1.60.0 0.0.0.255 any
 permit tcp 10.1.61.0 0.0.0.255 any
 permit tcp 10.1.80.0 0.0.0.255 any
 permit tcp 10.1.81.0 0.0.0.255 any
ip access-list extended acl_VoIP
 permit udp any any range 16384 32767
 permit udp any range 16384 32767 any
ip access-list extended acl_video_VoD
 permit udp 10.1.60.0 0.0.0.255 any
 permit udp 10.1.61.0 0.0.0.255 any
ip access-list extended acl_video_broadcast
 permit udp 10.1.70.0 0.0.0.255 232.0.0.0 0.255.255.255
!
logging event link-status default
logging trap debugging
logging 10.1.10.10
!
!
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
banner login ^CC
**********************************************************************
*
*   DDDDDD      EEEEEEEE    RRRRRRR        11
*   DD    DD    EE          RR    RR     1111
*   DD    DD    EE          RR    RR       11
*   DD    DD    EEEEE       RRRRRR         11
*   DD    DD    EE          RR   RR        11
*   DD    DD    EE          RR    RR       11
*   DDDDDD      EEEEEEEE    RR     RR   11111111
*
* Switch = Cisco7609
* Console =
* Topology = Service Router
*
**********************************************************************
```

```
^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
scheduler runtime netinput 300
ntp clock-period 17180005
ntp update-calendar
ntp server 10.1.60.10 prefer
no cns aaa enable
end
```

Configuration for DER2

```
Building configuration...

Current configuration : 52507 bytes
!
! Last configuration change at 13:02:51 PDT Mon May 15 2006
! NVRAM config last updated at 13:02:52 PDT Mon May 15 2006
!
upgrade fpd auto
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service counters max age 10
!
hostname DER2
!
boot system disk0:s72033-advipservicesk9_wan-mz.122-18.SXF2.bin
logging snmp-authfail
enable password cisco
!
no aaa new-model
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
!
!
ip cef load-sharing algorithm original
ip multicast-routing
ip igmp ssm-map enable
ip domain multicast coronado.net
no ip domain-lookup
ip domain-name coronado.net
ip name-server 10.1.10.10
ipv6 mfib hardware-switching replication-mode ingress
vtp mode transparent
mpls label protocol ldp
no tag-switching advertise-tags
tag-switching advertise-tags for LOOPBACK
tag-switching tdp router-id Loopback3 force
mls ip cef load-sharing full
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 36 to 2
mls qos
no mls acl tcam share-global
mls cef error action freeze
!
!
!
!
!
!
!
!
!
!
redundancy
 mode rpr-plus
```

```
 main-cpu
  auto-sync startup-config
  auto-sync running-config
  auto-sync standard
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
port-channel per-module load-balance
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 11
 name VLAN_11_Management
!
vlan 61
 name VLAN_61_VoD
!
vlan 70
 name VLAN_70_Multicast_Video

vlan 81
 name VLAN_81_Voice
!
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_VoD_and_SIP_signaling
  match access-group name acl_VoD_and_SIP_signaling
class-map match-all class_video_broadcast
  match access-group name acl_video_broadcast
class-map match-all class_video_VoD
  match access-group name acl_video_VoD
!
!
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoD_and_SIP_signaling
   set dscp cs3
  class class_video_broadcast
   set dscp af41
  class class_video_VoD
   set dscp af42
  class class_VoIP
   set dscp ef
!
!
!
interface Loopback3
 description Loopback for MPLS Services
 ip address 10.1.254.2 255.255.255.255
 ip ospf network point-to-point
!
interface GigabitEthernet2/1
 description Management VLAN (CNR - DHCP, DNS, SysLog)
 switchport
 switchport access vlan 11
 switchport mode access
 dampening
 no ip address
```

```
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/2
 no ip address
 shutdown
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/3
 description Kasenna Gigabase Server - Management Interface (Eth0)
 switchport
 switchport access vlan 61
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/4
 description Kasenna Gigabase Server - VoD Pump (HPN0)
 switchport
 switchport access vlan 61
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
```

```
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/5
 description Kasenna Gigabase Server - VoD Pump (HPN1)
 switchport
 switchport access vlan 61
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/6
 description Minerva Video Streamer - Multicast Video
 switchport
 switchport access vlan 70
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/7
 description VoIP SIP Server
 switchport
 switchport access vlan 81
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
```

```
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
<---output omitted--->
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface TenGigabitEthernet7/1
 description Transport to/from AR3 (TenGig1/3)
 dampening 5 1000 2000 20 restart 16000
 mtu 9216
 ip address 10.1.1.34 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 tag-switching ip
 mls qos trust dscp
!
<---output omitted--->
!
interface TenGigabitEthernet7/4
 description Transport to/from DER1 (TenGig7/4)
 dampening 5 1000 2000 20 restart 16000
 mtu 9216
 ip address 10.1.1.2 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 tag-switching ip
 mls qos trust dscp
!
interface Group-Async5
 physical-layer async
 no ip address
 encapsulation slip
!
```

```
interface Vlan1
 no ip address
 shutdown
!
interface Vlan11
 description Management VLAN (CNR - DNS, DHCP, etc)
 ip address 10.1.11.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan61
 description VoD Server VLAN (Unicast Video)
 ip address 10.1.61.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan70
 description Broadcast video source VLAN (Multicast VLAN)
 ip address 10.1.70.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan81
 description VoIP Gateway VLAN
 ip address 1.1.81.1 255.255.255.0
 load-interval 30
!
router ospf 100
 router-id 10.1.1.2
 ispf
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan11
 passive-interface Vlan61
 passive-interface Vlan70
 passive-interface Vlan81
 network 10.1.1.0 0.0.0.3 area 0
 network 10.1.1.32 0.0.0.3 area 0
 network 10.1.11.0 0.0.0.255 area 0
 network 10.1.61.0 0.0.0.255 area 0
 network 10.1.70.0 0.0.0.255 area 0
 network 10.1.81.0 0.0.0.255 area 0
 network 10.1.254.2 0.0.0.0 area 0
 maximum-paths 8
!
ip classless
!
no ip http server
ip pim ssm default
!
ip access-list standard LOOPBACK
 permit 10.1.254.0 0.0.0.255
!
ip access-list extended acl_VoD_and_SIP_signaling
 permit tcp 10.1.60.0 0.0.0.255 any
```

```
 permit tcp 10.1.61.0 0.0.0.255 any
 permit tcp 10.1.80.0 0.0.0.255 any
 permit tcp 10.1.81.0 0.0.0.255 any
ip access-list extended acl_VoIP
 permit udp any any range 16384 32767
 permit udp any range 16384 32767 any
ip access-list extended acl_video_VoD
 permit udp 10.1.60.0 0.0.0.255 any
 permit udp 10.1.61.0 0.0.0.255 any
ip access-list extended acl_video_broadcast
 permit udp 10.1.70.0 0.0.0.255 232.0.0.0 0.255.255.255
!
logging event link-status default
logging trap debugging
logging 10.1.10.10
!
!
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
```

```
!
banner login ^CC
**********************************************************************
*
*   DDDDDD      EEEEEEEE    RRRRRRR     22222222
*   DD    DD    EE          RR    RR          22
*   DD    DD    EE          RR    RR          22
*   DD    DD    EEEEE       RRRRRR      22222222
*   DD    DD    EE          RR   RR     22
*   DD    DD    EE          RR    RR    22
*   DDDDDD      EEEEEEEE    RR     RR   22222222
*
* Switch = Cisco7609
* Console =
* Topology = Service Router
*
**********************************************************************




^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
monitor event-trace timestamps
ntp clock-period 17179964
ntp update-calendar
ntp server 10.1.60.10 prefer
no cns aaa enable
end
```

Configuration for AR1

```
Building configuration...

Current configuration : 44349 bytes
!
! Last configuration change at 12:06:46 PDT Fri May 19 2006
! NVRAM config last updated at 11:58:25 PDT Fri May 19 2006
!
upgrade fpd auto
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service compress-config
service counters max age 10
!
hostname AR1
!
boot system flash disk0:s72033-advipservicesk9_wan-mz.122-18.SXF2.bin
logging snmp-authfail
enable password cisco
!
no aaa new-model
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
!
ip dhcp relay information trust-all
!
ip cef load-sharing algorithm original
ip multicast-routing
ip igmp ssm-map enable
ip domain multicast coronado.net
no ip domain-lookup
ip domain-name coronado.net
ip name-server 10.1.10.10
ipv6 mfib hardware-switching replication-mode ingress
vtp mode transparent
mpls label protocol ldp
no tag-switching advertise-tags
tag-switching advertise-tags for LOOPBACK
tag-switching tdp router-id Loopback3 force
mls ip cef load-sharing full
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos map dscp-cos 36 to 2
mls qos
no mls acl tcam share-global
mls cef error action freeze
!
!
!
!
!
!
!
!
!
!
redundancy
```

```
 mode sso
 main-cpu
  auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
power redundancy-mode combined
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
port-channel per-module load-balance
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_VoD_and_SIP_signaling
  match access-group name acl_VoD_and_SIP_signaling
!
!
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoIP
   set dscp ef
  class class_VoD_and_SIP_signaling
   set dscp cs3
!
!
!
interface Loopback0
 ip address 10.10.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30
!
interface Loopback1
 ip address 10.20.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30
!
interface Loopback3
 ip address 10.1.254.3 255.255.255.255
 ip ospf network point-to-point
!
interface TenGigabitEthernet1/1
 description Transport to/from DER1 (TenGig7/1)
 dampening 5 1000 2000 20 restart 16000
 mtu 9216
 ip address 10.1.1.10 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
```

```
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 tag-switching ip
 mls qos trust dscp
!
<---output omitted--->
!
interface TenGigabitEthernet1/3
 description Transport to/from AR2 (TenGig1/1)
 dampening 5 1000 2000 20 restart 16000
 mtu 9216
 ip address 10.1.1.17 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 tag-switching ip
 mls qos trust dscp
!
<---output omitted--->
!
interface GigabitEthernet2/1
 description 802.1q Interface To Ericsson DSLAM-1
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
!
interface GigabitEthernet2/1.1
 description Video edge VLAN
 encapsulation dot1Q 100
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/1.2
 description Voice edge VLAN
 encapsulation dot1Q 200
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/1.3
 description HSD edge VLAN
 encapsulation dot1Q 300
```

```
 xconnect 1.1.254.1 300 encapsulation mpls
!
interface GigabitEthernet2/2
 description 802.1q Interface To Ericsson DSLAM-2
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
!
interface GigabitEthernet2/2.1
 description Video edge VLAN
 encapsulation dot1Q 101
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/2.2
 description Voice edge VLAN
 encapsulation dot1Q 201
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/2.3
 description HSD edge VLAN
 encapsulation dot1Q 301
 xconnect 1.1.254.1 301 encapsulation mpls
!
interface GigabitEthernet2/3
 description 802.1q Interface To Ericsson DSLAM-3
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/3.1
 description Video edge VLAN
 encapsulation dot1Q 102
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/3.2
 description Voice edge VLAN
 encapsulation dot1Q 202
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/3.3
```

```
 description HSD edge VLAN
 encapsulation dot1Q 302
 xconnect 1.1.254.1 302 encapsulation mpls
!
interface GigabitEthernet2/4
 description 802.1q Interface To Ericsson DSLAM-4
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/4.1
 description Video edge VLAN
 encapsulation dot1Q 103
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/4.2
 description Voice edge VLAN
 encapsulation dot1Q 203
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/4.3
 description HSD edge VLAN
 encapsulation dot1Q 303
 xconnect 1.1.254.1 303 encapsulation mpls
!
interface GigabitEthernet2/5
 description 802.1q Interface To Ericsson DSLAM-5
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/5.1
 description Video edge VLAN
 encapsulation dot1Q 104
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/5.2
 description Voice edge VLAN
 encapsulation dot1Q 204
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/5.3
```

```
 description HSD edge VLAN
 encapsulation dot1Q 304
 xconnect 1.1.254.1 304 encapsulation mpls
!
interface GigabitEthernet2/6
 description 802.1q Interface To Ericsson DSLAM-6
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/6.1
 description Video edge VLAN
 encapsulation dot1Q 105
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/6.2
 description Voice edge VLAN
 encapsulation dot1Q 205
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/6.3
 description HSD edge VLAN
 encapsulation dot1Q 305
 xconnect 1.1.254.1 305 encapsulation mpls
!
interface GigabitEthernet2/7
 description 802.1q Interface To Ericsson DSLAM-7
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/7.1
 description Video edge VLAN
 encapsulation dot1Q 106
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/7.2
 description Voice edge VLAN
 encapsulation dot1Q 206
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/7.3
```

```
 description HSD edge VLAN
 encapsulation dot1Q 306
 xconnect 1.1.254.1 306 encapsulation mpls
!
interface GigabitEthernet2/8
 description 802.1q Interface To Ericsson DSLAM-8
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/8.1
 description Video edge VLAN
 encapsulation dot1Q 107
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/8.2
 description Voice edge VLAN
 encapsulation dot1Q 207
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/8.3
 description HSD edge VLAN
 encapsulation dot1Q 307
 xconnect 1.1.254.1 307 encapsulation mpls
!
interface GigabitEthernet2/9
 description 802.1q Interface To Ericsson DSLAM-9
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/9.1
 description Video edge VLAN
 encapsulation dot1Q 108
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/9.2
 description Voice edge VLAN
 encapsulation dot1Q 208
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/9.3
```

```
 description HSD edge VLAN
 encapsulation dot1Q 308
 xconnect 1.1.254.1 308 encapsulation mpls
!
interface GigabitEthernet2/10
 description 802.1q Interface To Ericsson DSLAM-10
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/10.1
 description Video edge VLAN
 encapsulation dot1Q 109
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/10.2
 description Voice edge VLAN
 encapsulation dot1Q 209
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/10.3
 description HSD edge VLAN
 encapsulation dot1Q 309
 xconnect 1.1.254.1 309 encapsulation mpls
!
interface GigabitEthernet2/11
 description 802.1q Interface To Ericsson DSLAM-11
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/11.1
 description Video edge VLAN
 encapsulation dot1Q 110
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/11.2
 description Voice edge VLAN
 encapsulation dot1Q 210
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/11.3
```

```
 description HSD edge VLAN
 encapsulation dot1Q 310
 xconnect 1.1.254.1 310 encapsulation mpls
!
interface GigabitEthernet2/12
 description 802.1q Interface To Ericsson DSLAM-12
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/12.1
 description Video edge VLAN
 encapsulation dot1Q 111
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/12.2
 description Voice edge VLAN
 encapsulation dot1Q 211
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/12.3
 description HSD edge VLAN
 encapsulation dot1Q 311
 xconnect 1.1.254.1 311 encapsulation mpls
!
interface GigabitEthernet2/13
 description 802.1q Interface To Ericsson DSLAM-13
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/13.1
 description Video edge VLAN
 encapsulation dot1Q 112
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/13.2
 description Voice edge VLAN
 encapsulation dot1Q 212
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/13.3
```

```
 description HSD edge VLAN
 encapsulation dot1Q 312
 xconnect 1.1.254.1 312 encapsulation mpls
!
interface GigabitEthernet2/14
 description 802.1q Interface To Ericsson DSLAM-14
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/14.1
 description Video edge VLAN
 encapsulation dot1Q 113
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/14.2
 description Voice edge VLAN
 encapsulation dot1Q 213
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/14.3
 description HSD edge VLAN
 encapsulation dot1Q 313
 xconnect 1.1.254.1 313 encapsulation mpls
!
interface GigabitEthernet2/15
 description 802.1q Interface To Ericsson DSLAM-15
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/15.1
 description Video edge VLAN
 encapsulation dot1Q 114
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/15.2
 description Voice edge VLAN
 encapsulation dot1Q 214
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/15.3
```

```
 description HSD edge VLAN
 encapsulation dot1Q 314
 xconnect 1.1.254.1 314 encapsulation mpls
!
interface GigabitEthernet2/16
 description 802.1q Interface To Ericsson DSLAM-16
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/16.1
 service-policy input setDSCP
!
interface GigabitEthernet2/16.2
 description Voice edge VLAN
 encapsulation dot1Q 215
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/16.3
 description HSD edge VLAN
 encapsulation dot1Q 315
 xconnect 1.1.254.1 315 encapsulation mpls
!
interface GigabitEthernet2/17
 description 802.1q Interface To Ericsson DSLAM-17
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/17.1
 description Video edge VLAN
 encapsulation dot1Q 116
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/17.2
 description Voice edge VLAN
 encapsulation dot1Q 216
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/17.3
 description HSD edge VLAN
 encapsulation dot1Q 316
 xconnect 1.1.254.1 316 encapsulation mpls
!
interface GigabitEthernet2/18
```

```
 description 802.1q Interface To Ericsson DSLAM-18
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/18.1
 description Video edge VLAN
 encapsulation dot1Q 117
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/18.2
 description Voice edge VLAN
 encapsulation dot1Q 217
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/18.3
 description HSD edge VLAN
 encapsulation dot1Q 317
 xconnect 1.1.254.1 317 encapsulation mpls
!
interface GigabitEthernet2/19
 description 802.1q Interface To Ericsson DSLAM-19
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/19.1
 description Video edge VLAN
 encapsulation dot1Q 118
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/19.2
 description Voice edge VLAN
 encapsulation dot1Q 218
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/19.3
 description HSD edge VLAN
 encapsulation dot1Q 318
 xconnect 1.1.254.1 318 encapsulation mpls
!
interface GigabitEthernet2/20
```

```
 description 802.1q Interface To Ericsson DSLAM-20
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/20.1
 description Video edge VLAN
 encapsulation dot1Q 119
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/20.2
 description Voice edge VLAN
 encapsulation dot1Q 219
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/20.3
 description HSD edge VLAN
 encapsulation dot1Q 319
 xconnect 1.1.254.1 319 encapsulation mpls
!
interface GigabitEthernet2/21
 description 802.1q Interface To Ericsson DSLAM-21
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/21.1
 description Video edge VLAN
 encapsulation dot1Q 120
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/21.2
 description Voice edge VLAN
 encapsulation dot1Q 220
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/21.3
 description HSD edge VLAN
 encapsulation dot1Q 320
 xconnect 1.1.254.1 320 encapsulation mpls
!
interface GigabitEthernet2/22
```

```
 description Agilent 101-4
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/22.1
 description Video edge VLAN
 encapsulation dot1Q 121
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/22.2
 description Voice edge VLAN
 encapsulation dot1Q 221
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/22.3
 description HSD edge VLAN
 encapsulation dot1Q 321
 xconnect 1.1.254.1 321 encapsulation mpls
!
interface GigabitEthernet2/23
 description 802.1q Interface To Ericsson DSLAM-23
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/23.1
 description Video edge VLAN
 encapsulation dot1Q 122
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/23.2
 description Voice edge VLAN
 encapsulation dot1Q 222
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/23.3
 description HSD edge VLAN
 encapsulation dot1Q 322
 xconnect 1.1.254.1 322 encapsulation mpls
!
```

```
interface GigabitEthernet2/24
 description 802.1q Interface To Ericsson DSLAM-24
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/24.1
 description Video edge VLAN
 encapsulation dot1Q 123
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/24.2
 description Voice edge VLAN
 encapsulation dot1Q 223
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/24.3
 description HSD edge VLAN
 encapsulation dot1Q 323
 xconnect 1.1.254.1 323 encapsulation mpls
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
 media-type rj45
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 100
 router-id 10.1.1.3
 ispf
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 network 10.1.1.9 0.0.0.3 area 0
 network 10.1.1.17 0.0.0.3 area 0
 network 10.1.254.3 0.0.0.0 area 0
 network 10.10.0.0 0.0.255.255 area 0
 network 10.20.0.0 0.0.255.255 area 0
!
ip classless
!
no ip http server
ip pim ssm default
!
ip access-list standard LOOPBACK
```

```
 permit 10.1.254.0 0.0.0.255
!
ip access-list extended acl_VoD_and_SIP_signaling
 permit ip any host 10.1.10.10
 permit ip any 10.1.60.0 0.0.0.255
 permit ip any 10.1.61.0 0.0.0.255
 permit ip any 10.1.80.0 0.0.0.255
 permit ip any 10.1.81.0 0.0.0.255
ip access-list extended acl_VoIP
 permit udp any any range 16384 32767
 permit udp any range 16384 32767 any
!
logging event link-status default
logging trap debugging
logging 10.1.10.10
!
!
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
!
banner login ^CCC
**********************************************************************
*
*     AA    RRRRRRR     11
*    AAAA   RR   RR   1111
*   AA  AA  RR   RR     11
*   AAAAAA  RR RRR      11
*   AAAAAA  RR  RR      11
*   AA  AA  RR   RR     11
*   AA  AA  RR    RR  111111
*
* Switch = Catalyst7606
* Console =
* Topology = 10GE Ring
*
**********************************************************************




^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
monitor event-trace timestamps
ntp clock-period 17180100
```

```
ntp update-calendar
ntp server 10.1.60.10 prefer
no cns aaa enable
end
```

Configuration for AR2

```
Building configuration...

Current configuration : 33538 bytes
!
! Last configuration change at 12:06:17 PDT Fri May 19 2006
! NVRAM config last updated at 23:23:04 PDT Tue May 2 2006
!
upgrade fpd auto
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service counters max age 10
!
hostname AR2
!
boot system flash disk0:s72033-advipservicesk9_wan-mz.122-18.SXF2.bin
logging snmp-authfail
enable password cisco
!
no aaa new-model
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
!
ip dhcp relay information trust-all
!
ip cef load-sharing algorithm original
ip multicast-routing
ip igmp ssm-map enable
ip domain multicast coronado.net
no ip domain-lookup
ip domain-name coronado.net
ip name-server 10.1.10.10
ipv6 mfib hardware-switching replication-mode ingress
vtp mode transparent
mpls label protocol ldp
no tag-switching advertise-tags
tag-switching advertise-tags for LOOPBACK
tag-switching tdp router-id Loopback3 force
mls ip cef load-sharing full
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos map dscp-cos 36 to 2
mls qos
no mls acl tcam share-global
mls cef error action freeze
!
!
!
!
!
!
!
!
!
!
redundancy
 mode sso
```

```
 main-cpu
  auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
power redundancy-mode combined
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
port-channel per-module load-balance
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_VoD_and_SIP_signaling
  match access-group name acl_VoD_and_SIP_signaling
class-map match-all class_HSD
  match access-group name acl_HSD
!
!
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoIP
   set dscp ef
  class class_VoD_and_SIP_signaling
   set dscp cs3
!
!
!
interface Loopback0
 ip address 10.11.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30
!
interface Loopback1
 ip address 10.21.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30
!
interface Loopback3
 ip address 10.1.254.4 255.255.255.255
 ip ospf network point-to-point
!
interface TenGigabitEthernet1/1
 description Transport to/from AR1 (TenGig1/3)
 dampening 5 1000 2000 20 restart 16000
 mtu 9216
 ip address 10.1.1.18 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
```

```
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 tag-switching ip
 mls qos trust dscp
!
<---output omitted--->
!
interface TenGigabitEthernet1/3
 description Transport to/from AR3 (TenGig1/1)
 dampening 5 1000 2000 20 restart 16000
 mtu 9216
 ip address 10.1.1.25 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 tag-switching ip
 mls qos trust dscp
!
<---output omitted--->
!
interface GigabitEthernet2/1
 description 802.1q Interface To Ericsson DSLAM-1
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
!
interface GigabitEthernet2/1.1
 description Video edge VLAN
 encapsulation dot1Q 100
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/1.2
 description Voice edge VLAN
 encapsulation dot1Q 200
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/1.3
 description HSD edge VLAN
```

```
 encapsulation dot1Q 330
 xconnect 1.1.254.1 330 encapsulation mpls
!
interface GigabitEthernet2/2
 description 802.1q Interface To Ericsson DSLAM-2
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
!
interface GigabitEthernet2/2.1
 description Video edge VLAN
 encapsulation dot1Q 101
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/2.2
 description Voice edge VLAN
 encapsulation dot1Q 201
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/2.3
 description HSD edge VLAN
 encapsulation dot1Q 331
 xconnect 1.1.254.1 331 encapsulation mpls
!
interface GigabitEthernet2/3
 description 802.1q Interface To Ericsson DSLAM-3
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/3.1
 description Video edge VLAN
 encapsulation dot1Q 102
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/3.2
 description Voice edge VLAN
 encapsulation dot1Q 202
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
```

```
interface GigabitEthernet2/3.3
 description HSD edge VLAN
 encapsulation dot1Q 332
 xconnect 1.1.254.1 332 encapsulation mpls
!
interface GigabitEthernet2/4
 description 802.1q Interface To Ericsson DSLAM-4
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/4.1
 description Video edge VLAN
 encapsulation dot1Q 103
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/4.2
 description Voice edge VLAN
 encapsulation dot1Q 203
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/4.3
 description HSD edge VLAN
 encapsulation dot1Q 333
 xconnect 1.1.254.1 333 encapsulation mpls
!
interface GigabitEthernet2/5
 description 802.1q Interface To Ericsson DSLAM-5
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/5.1
 description Video edge VLAN
 encapsulation dot1Q 104
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/5.2
 description Voice edge VLAN
 encapsulation dot1Q 204
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
```

```
interface GigabitEthernet2/5.3
 description HSD edge VLAN
 encapsulation dot1Q 334
 xconnect 1.1.254.1 334 encapsulation mpls
!
interface GigabitEthernet2/6
 description 802.1q Interface To Ericsson DSLAM-6
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/6.1
 description Video edge VLAN
 encapsulation dot1Q 105
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/6.2
 description Voice edge VLAN
 encapsulation dot1Q 205
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/6.3
 description HSD edge VLAN
 encapsulation dot1Q 335
 xconnect 1.1.254.1 335 encapsulation mpls
!
interface GigabitEthernet2/7
 description 802.1q Interface To Ericsson DSLAM-7
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/7.1
 description Video edge VLAN
 encapsulation dot1Q 106
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/7.2
 description Voice edge VLAN
 encapsulation dot1Q 206
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
```

```
interface GigabitEthernet2/7.3
 description HSD edge VLAN
 encapsulation dot1Q 336
 xconnect 1.1.254.1 336 encapsulation mpls
!
interface GigabitEthernet2/8
 description 802.1q Interface To Ericsson DSLAM-8
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/8.1
 description Video edge VLAN
 encapsulation dot1Q 107
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/8.2
 description Voice edge VLAN
 encapsulation dot1Q 207
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/8.3
 description HSD edge VLAN
 encapsulation dot1Q 337
 xconnect 1.1.254.1 337 encapsulation mpls
!
interface GigabitEthernet2/9
 description 802.1q Interface To Ericsson DSLAM-9
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/9.1
 description Video edge VLAN
 encapsulation dot1Q 108
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/9.2
 description Voice edge VLAN
 encapsulation dot1Q 208
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
```

```
interface GigabitEthernet2/9.3
 description HSD edge VLAN
 encapsulation dot1Q 338
 xconnect 1.1.254.1 338 encapsulation mpls
!
interface GigabitEthernet2/10
 description 802.1q Interface To Ericsson DSLAM-10
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/10.1
 description Video edge VLAN
 encapsulation dot1Q 109
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/10.2
 description Voice edge VLAN
 encapsulation dot1Q 209
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/10.3
 description HSD edge VLAN
 encapsulation dot1Q 339
 xconnect 1.1.254.1 339 encapsulation mpls
!
interface GigabitEthernet2/11
 description 802.1q Interface To Ericsson DSLAM-11
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/11.1
 description Video edge VLAN
 encapsulation dot1Q 110
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/11.2
 description Voice edge VLAN
 encapsulation dot1Q 210
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
```

```
interface GigabitEthernet2/11.3
 description HSD edge VLAN
 encapsulation dot1Q 340
 xconnect 1.1.254.1 340 encapsulation mpls
!
interface GigabitEthernet2/12
 description 802.1q Interface To Ericsson DSLAM-12
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/12.1
 description Video edge VLAN
 encapsulation dot1Q 111
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/12.2
 description Voice edge VLAN
 encapsulation dot1Q 211
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/12.3
 description HSD edge VLAN
 encapsulation dot1Q 341
 xconnect 1.1.254.1 341 encapsulation mpls
!
interface GigabitEthernet2/13
 description 802.1q Interface To Ericsson DSLAM-13
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/13.1
 description Video edge VLAN
 encapsulation dot1Q 112
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/13.2
 description Voice edge VLAN
 encapsulation dot1Q 212
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
```

```
interface GigabitEthernet2/13.3
 description HSD edge VLAN
 encapsulation dot1Q 342
 xconnect 1.1.254.1 342 encapsulation mpls
!
interface GigabitEthernet2/14
 description 802.1q Interface To Ericsson DSLAM-14
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/14.1
 description Video edge VLAN
 encapsulation dot1Q 113
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/14.2
 description Voice edge VLAN
 encapsulation dot1Q 213
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/14.3
 description HSD edge VLAN
 encapsulation dot1Q 343
 xconnect 1.1.254.1 343 encapsulation mpls
!
interface GigabitEthernet2/15
 description 802.1q Interface To Ericsson DSLAM-15
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/15.1
 description Video edge VLAN
 encapsulation dot1Q 114
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/15.2
 description Voice edge VLAN
 encapsulation dot1Q 214
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
```

```
interface GigabitEthernet2/15.3
 description HSD edge VLAN
 encapsulation dot1Q 344
 xconnect 1.1.254.1 344 encapsulation mpls
!
interface GigabitEthernet2/16
 description 802.1q Interface To Ericsson DSLAM-16
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/16.1
 service-policy input setDSCP
!
interface GigabitEthernet2/16.2
 description Voice edge VLAN
 encapsulation dot1Q 215
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/16.3
 description HSD edge VLAN
 encapsulation dot1Q 345
 xconnect 1.1.254.1 345 encapsulation mpls
!
interface GigabitEthernet2/17
 description 802.1q Interface To Ericsson DSLAM-17
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/17.1
 description Video edge VLAN
 encapsulation dot1Q 116
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/17.2
 description Voice edge VLAN
 encapsulation dot1Q 216
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/17.3
 description HSD edge VLAN
 encapsulation dot1Q 346
 xconnect 1.1.254.1 346 encapsulation mpls
!
```

```
interface GigabitEthernet2/18
 description 802.1q Interface To Ericsson DSLAM-18
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/18.1
 description Video edge VLAN
 encapsulation dot1Q 117
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/18.2
 description Voice edge VLAN
 encapsulation dot1Q 217
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/18.3
 description HSD edge VLAN
 encapsulation dot1Q 347
 xconnect 1.1.254.1 347 encapsulation mpls
!
interface GigabitEthernet2/19
 description 802.1q Interface To Ericsson DSLAM-19
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/19.1
 description Video edge VLAN
 encapsulation dot1Q 118
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/19.2
 description Voice edge VLAN
 encapsulation dot1Q 218
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/19.3
 description HSD edge VLAN
 encapsulation dot1Q 348
 xconnect 1.1.254.1 348 encapsulation mpls
!
```

```
interface GigabitEthernet2/20
 description 802.1q Interface To Ericsson DSLAM-20
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/20.1
 description Video edge VLAN
 encapsulation dot1Q 119
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/20.2
 description Voice edge VLAN
 encapsulation dot1Q 219
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/20.3
 description HSD edge VLAN
 encapsulation dot1Q 349
 xconnect 1.1.254.1 349 encapsulation mpls
!
interface GigabitEthernet2/21
 description 802.1q Interface To Ericsson DSLAM-21
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/21.1
 description Video edge VLAN
 encapsulation dot1Q 120
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/21.2
 description Voice edge VLAN
 encapsulation dot1Q 220
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/21.3
 description HSD edge VLAN
 encapsulation dot1Q 350
 xconnect 1.1.254.1 350 encapsulation mpls
!
```

```
interface GigabitEthernet2/22
 description Agilent 101-4
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/22.1
 description Video edge VLAN
 encapsulation dot1Q 121
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/22.2
 description Voice edge VLAN
 encapsulation dot1Q 221
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/22.3
 description HSD edge VLAN
 encapsulation dot1Q 351
 xconnect 1.1.254.1 351 encapsulation mpls
!
interface GigabitEthernet2/23
 description 802.1q Interface To Ericsson DSLAM-23
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/23.1
 description Video edge VLAN
 encapsulation dot1Q 122
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/23.2
 description Voice edge VLAN
 encapsulation dot1Q 222
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/23.3
 description HSD edge VLAN
 encapsulation dot1Q 352
 xconnect 1.1.254.1 352 encapsulation mpls
```

```
!
interface GigabitEthernet2/24
 description 802.1q Interface To Ericsson DSLAM-24
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/24.1
 description Video edge VLAN
 encapsulation dot1Q 123
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/24.2
 description Voice edge VLAN
 encapsulation dot1Q 223
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/24.3
 description HSD edge VLAN
 encapsulation dot1Q 353
 xconnect 1.1.254.1 353 encapsulation mpls
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
 media-type rj45
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 100
 router-id 10.1.1.4
 ispf
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 network 10.1.1.16 0.0.0.3 area 0
 network 10.1.1.24 0.0.0.3 area 0
 network 10.1.254.4 0.0.0.0 area 0
 network 10.11.0.0 0.0.255.255 area 0
 network 10.21.0.0 0.0.255.255 area 0
!
ip classless
!
no ip http server
ip pim ssm default
!
```

```
ip access-list standard LOOPBACK
 permit 10.1.254.0 0.0.0.255
!
ip access-list extended acl_VoD_and_SIP_signaling
 permit ip any host 10.1.10.10
 permit ip any 10.1.60.0 0.0.0.255
 permit ip any 10.1.61.0 0.0.0.255
 permit ip any 10.1.80.0 0.0.0.255
 permit ip any 10.1.81.0 0.0.0.255
ip access-list extended acl_VoIP
 permit udp any any range 16384 32767
 permit udp any range 16384 32767 any
!
logging event link-status default
logging trap debugging
logging 10.1.10.10
!
!
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
!
banner login ^CCC
**********************************************************************
*
*    AA    RRRRRRR   222222
*   AAAA   RR   RR       22
*  AA  AA  RR   RR       22
*  AAAAAA  RR RRR    22222
*  AAAAAA  RR  RR    22
*  AA  AA  RR   RR   22
*  AA  AA  RR    RR  222222
*
* Switch = Catalyst7606
* Console =
* Topology = 10GE Ring
*
**********************************************************************




^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
!
```

```
ntp clock-period 17180088
ntp update-calendar
ntp server 10.1.60.10 prefer
no cns aaa enable
end
```

Configuration for AR3

```
Building configuration...

Current configuration : 36379 bytes
!
! No configuration change since last restart
!
upgrade fpd auto
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service counters max age 10
!
hostname AR3
!
boot system flash disk0:s72033-advipservicesk9_wan-mz.122-18.SXF2.bin
logging snmp-authfail
enable password cisco
!
no aaa new-model
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
!
ip dhcp relay information trust-all
!
ip cef load-sharing algorithm original
ip multicast-routing
ip igmp ssm-map enable
ip domain multicast coronado.net
no ip domain-lookup
ip domain-name coronado.net
ip name-server 10.1.10.10
ipv6 mfib hardware-switching replication-mode ingress
vtp mode transparent
mpls label protocol ldp
no tag-switching advertise-tags
tag-switching advertise-tags for LOOPBACK
tag-switching tdp router-id Loopback3 force
mls ip cef load-sharing full
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos map dscp-cos 36 to 2
mls qos
no mls acl tcam share-global
mls cef error action freeze
!
!
!
!
!
!
!
!
!
!
redundancy
 mode sso
 main-cpu
```

```
  auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
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
port-channel per-module load-balance
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_VoD_and_SIP_signaling
  match access-group name acl_VoD_and_SIP_signaling
class-map match-all class_HSD
  match access-group name acl_HSD
!
!
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoIP
   set dscp ef
  class class_VoD_and_SIP_signaling
   set dscp cs3
!
!
!
interface Loopback0
 ip address 10.12.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30
!
interface Loopback1
 ip address 10.22.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30
!
interface Loopback3
 ip address 10.1.254.5 255.255.255.255
 ip ospf network point-to-point
!
interface TenGigabitEthernet1/1
 description Transport to/from AR2 (TenGig1/3)
 dampening 5 1000 2000 20 restart 16000
 mtu 9216
 ip address 10.1.1.26 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
```

```
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 tag-switching ip
 mls qos trust dscp
!
<---output omitted--->
!
interface TenGigabitEthernet1/3
 description Transport to/from DER2 (TenGig7/1)
 dampening 5 1000 2000 20 restart 16000
 mtu 9216
 ip address 1.1.2.25 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 tag-switching ip
 mls qos trust dscp
 spanning-tree portfast trunk
!
<---output omitted--->
!
interface GigabitEthernet2/1
 description 802.1q Interface To Ericsson DSLAM-1
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
!
interface GigabitEthernet2/1.1
 description Video edge VLAN
 encapsulation dot1Q 100
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/1.2
 description Voice edge VLAN
 encapsulation dot1Q 200
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/1.3
```

```
 description HSD edge VLAN
 encapsulation dot1Q 360
 xconnect 1.1.254.1 360 encapsulation mpls
!
interface GigabitEthernet2/2
 description 802.1q Interface To Ericsson DSLAM-2
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
!
interface GigabitEthernet2/2.1
 description Video edge VLAN
 encapsulation dot1Q 101
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/2.2
 description Voice edge VLAN
 encapsulation dot1Q 201
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/2.3
 description HSD edge VLAN
 encapsulation dot1Q 361
 xconnect 1.1.254.1 361 encapsulation mpls
!
interface GigabitEthernet2/3
 description 802.1q Interface To Ericsson DSLAM-3
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/3.1
 description Video edge VLAN
 encapsulation dot1Q 102
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/3.2
 description Voice edge VLAN
 encapsulation dot1Q 202
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
```

```
!
interface GigabitEthernet2/3.3
 description HSD edge VLAN
 encapsulation dot1Q 362
 xconnect 1.1.254.1 362 encapsulation mpls
!
interface GigabitEthernet2/4
 description 802.1q Interface To Ericsson DSLAM-4
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/4.1
 description Video edge VLAN
 encapsulation dot1Q 103
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/4.2
 description Voice edge VLAN
 encapsulation dot1Q 203
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/4.3
 description HSD edge VLAN
 encapsulation dot1Q 363
 xconnect 1.1.254.1 363 encapsulation mpls
!
interface GigabitEthernet2/5
 description 802.1q Interface To Ericsson DSLAM-5
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/5.1
 description Video edge VLAN
 encapsulation dot1Q 104
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/5.2
 description Voice edge VLAN
 encapsulation dot1Q 204
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
```

```
!
interface GigabitEthernet2/5.3
 description HSD edge VLAN
 encapsulation dot1Q 364
 xconnect 1.1.254.1 364 encapsulation mpls
!
interface GigabitEthernet2/6
 description 802.1q Interface To Ericsson DSLAM-6
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/6.1
 description Video edge VLAN
 encapsulation dot1Q 105
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/6.2
 description Voice edge VLAN
 encapsulation dot1Q 205
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/6.3
 description HSD edge VLAN
 encapsulation dot1Q 365
 xconnect 1.1.254.1 365 encapsulation mpls
!
interface GigabitEthernet2/7
 description 802.1q Interface To Ericsson DSLAM-7
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/7.1
 description Video edge VLAN
 encapsulation dot1Q 106
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/7.2
 description Voice edge VLAN
 encapsulation dot1Q 206
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
```

```
!
interface GigabitEthernet2/7.3
 description HSD edge VLAN
 encapsulation dot1Q 366
 xconnect 1.1.254.1 366 encapsulation mpls
!
interface GigabitEthernet2/8
 description 802.1q Interface To Ericsson DSLAM-8
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/8.1
 description Video edge VLAN
 encapsulation dot1Q 107
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/8.2
 description Voice edge VLAN
 encapsulation dot1Q 207
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/8.3
 description HSD edge VLAN
 encapsulation dot1Q 367
 xconnect 1.1.254.1 367 encapsulation mpls
!
interface GigabitEthernet2/9
 description 802.1q Interface To Ericsson DSLAM-9
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/9.1
 description Video edge VLAN
 encapsulation dot1Q 108
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/9.2
 description Voice edge VLAN
 encapsulation dot1Q 208
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
```

```
!
interface GigabitEthernet2/9.3
 description HSD edge VLAN
 encapsulation dot1Q 368
 xconnect 1.1.254.1 368 encapsulation mpls
!
interface GigabitEthernet2/10
 description 802.1q Interface To Ericsson DSLAM-10
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/10.1
 description Video edge VLAN
 encapsulation dot1Q 109
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/10.2
 description Voice edge VLAN
 encapsulation dot1Q 209
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/10.3
 description HSD edge VLAN
 encapsulation dot1Q 369
 xconnect 1.1.254.1 369 encapsulation mpls
!
interface GigabitEthernet2/11
 description 802.1q Interface To Ericsson DSLAM-11
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/11.1
 description Video edge VLAN
 encapsulation dot1Q 110
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/11.2
 description Voice edge VLAN
 encapsulation dot1Q 210
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
```

```
!
interface GigabitEthernet2/11.3
 description HSD edge VLAN
 encapsulation dot1Q 370
 xconnect 1.1.254.1 370 encapsulation mpls
!
interface GigabitEthernet2/12
 description 802.1q Interface To Ericsson DSLAM-12
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/12.1
 description Video edge VLAN
 encapsulation dot1Q 111
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/12.2
 description Voice edge VLAN
 encapsulation dot1Q 211
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/12.3
 description HSD edge VLAN
 encapsulation dot1Q 371
 xconnect 1.1.254.1 371 encapsulation mpls
!
interface GigabitEthernet2/13
 description 802.1q Interface To Ericsson DSLAM-13
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/13.1
 description Video edge VLAN
 encapsulation dot1Q 112
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/13.2
 description Voice edge VLAN
 encapsulation dot1Q 212
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
```

```
!
interface GigabitEthernet2/13.3
 description HSD edge VLAN
 encapsulation dot1Q 372
 xconnect 1.1.254.1 372 encapsulation mpls
!
interface GigabitEthernet2/14
 description 802.1q Interface To Ericsson DSLAM-14
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/14.1
 description Video edge VLAN
 encapsulation dot1Q 113
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/14.2
 description Voice edge VLAN
 encapsulation dot1Q 213
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/14.3
 description HSD edge VLAN
 encapsulation dot1Q 373
 xconnect 1.1.254.1 373 encapsulation mpls
!
interface GigabitEthernet2/15
 description 802.1q Interface To Ericsson DSLAM-15
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/15.1
 description Video edge VLAN
 encapsulation dot1Q 114
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/15.2
 description Voice edge VLAN
 encapsulation dot1Q 214
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
```

```
!
interface GigabitEthernet2/15.3
 description HSD edge VLAN
 encapsulation dot1Q 374
 xconnect 1.1.254.1 374 encapsulation mpls
!
interface GigabitEthernet2/16
 description 802.1q Interface To Ericsson DSLAM-16
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/16.1
 service-policy input setDSCP
!
interface GigabitEthernet2/16.2
 description Voice edge VLAN
 encapsulation dot1Q 215
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/16.3
 description HSD edge VLAN
 encapsulation dot1Q 375
 xconnect 1.1.254.1 375 encapsulation mpls
!
interface GigabitEthernet2/17
 description 802.1q Interface To Ericsson DSLAM-17
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/17.1
 description Video edge VLAN
 encapsulation dot1Q 116
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/17.2
 description Voice edge VLAN
 encapsulation dot1Q 216
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/17.3
 description HSD edge VLAN
 encapsulation dot1Q 376
 xconnect 1.1.254.1 376 encapsulation mpls
```

```
!
interface GigabitEthernet2/18
 description 802.1q Interface To Ericsson DSLAM-18
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/18.1
 description Video edge VLAN
 encapsulation dot1Q 117
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/18.2
 description Voice edge VLAN
 encapsulation dot1Q 217
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/18.3
 description HSD edge VLAN
 encapsulation dot1Q 377
 xconnect 1.1.254.1 377 encapsulation mpls
!
interface GigabitEthernet2/19
 description 802.1q Interface To Ericsson DSLAM-19
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/19.1
 description Video edge VLAN
 encapsulation dot1Q 118
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/19.2
 description Voice edge VLAN
 encapsulation dot1Q 218
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/19.3
 description HSD edge VLAN
 encapsulation dot1Q 378
 xconnect 1.1.254.1 378 encapsulation mpls
```

```
!
interface GigabitEthernet2/20
 description 802.1q Interface To Ericsson DSLAM-20
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/20.1
 description Video edge VLAN
 encapsulation dot1Q 119
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/20.2
 description Voice edge VLAN
 encapsulation dot1Q 219
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/20.3
 description HSD edge VLAN
 encapsulation dot1Q 379
 xconnect 1.1.254.1 379 encapsulation mpls
!
interface GigabitEthernet2/21
 description 802.1q Interface To Ericsson DSLAM-21
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/21.1
 description Video edge VLAN
 encapsulation dot1Q 120
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/21.2
 description Voice edge VLAN
 encapsulation dot1Q 220
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/21.3
 description HSD edge VLAN
 encapsulation dot1Q 381
 xconnect 1.1.254.1 381 encapsulation mpls
```

```
!
interface GigabitEthernet2/22
 description Agilent 101-4
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/22.1
 description Video edge VLAN
 encapsulation dot1Q 121
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/22.2
 description Voice edge VLAN
 encapsulation dot1Q 221
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/22.3
 description HSD edge VLAN
 encapsulation dot1Q 381
 xconnect 1.1.254.1 381 encapsulation mpls
!
interface GigabitEthernet2/23
 description 802.1q Interface To Ericsson DSLAM-23
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/23.1
 description Video edge VLAN
 encapsulation dot1Q 122
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/23.2
 description Voice edge VLAN
 encapsulation dot1Q 222
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/23.3
 description HSD edge VLAN
 encapsulation dot1Q 382
```

```
 xconnect 1.1.254.1 382 encapsulation mpls
!
interface GigabitEthernet2/24
 description 802.1q Interface To Ericsson DSLAM-24
 no ip address
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/24.1
 description Video edge VLAN
 encapsulation dot1Q 123
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 service-policy input setDSCP
!
interface GigabitEthernet2/24.2
 description Voice edge VLAN
 encapsulation dot1Q 223
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 service-policy input setDSCP
!
interface GigabitEthernet2/24.3
 description HSD edge VLAN
 encapsulation dot1Q 383
 xconnect 1.1.254.1 383 encapsulation mpls
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 media-type rj45
!
interface Vlan1
 no ip address
 shutdown
!
!
router ospf 100
 router-id 10.1.1.5
 ispf
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 network 10.1.1.24 0.0.0.3 area 0
 network 10.1.1.32 0.0.0.3 area 0
 network 10.1.254.5 0.0.0.0 area 0
 network 10.12.0.0 0.0.255.255 area 0
 network 10.22.0.0 0.0.255.255 area 0
!
ip classless
!
no ip http server
ip pim ssm default
```

```
!
ip access-list standard LOOPBACK
 permit 10.1.254.0 0.0.0.255
!
ip access-list extended acl_VoD_and_SIP_signaling
 permit ip any host 10.1.10.10
 permit ip any 10.1.60.0 0.0.0.255
 permit ip any 10.1.61.0 0.0.0.255
 permit ip any 10.1.80.0 0.0.0.255
 permit ip any 10.1.81.0 0.0.0.255
ip access-list extended acl_VoIP
 permit udp any any range 16384 32767
 permit udp any range 16384 32767 any
!
logging event link-status default
logging trap debugging
logging 10.1.10.10

!
!
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
```

```
!
banner login ^CCC
**********************************************************************
*
*    AA    RRRRRRR   333333
*   AAAA   RR   RR       33
*  AA  AA  RR   RR       33
*  AAAAAA  RR RRR      3333
*  AAAAAA  RR  RR        33
*  AA  AA  RR   RR       33
*  AA  AA  RR    RR  333333
*
* Switch = Catalyst7606
* Console =
* Topology = 10GE Ring
*
**********************************************************************




^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
scheduler runtime netinput 360
ntp clock-period 17180081
ntp update-calendar
ntp server 10.1.60.10 prefer
no cns aaa enable
end
```

Sample DER and AR Switch Configurations for the Hub-and-Spoke Topology

This appendix presents sample distribution edge router (DER) and aggregation router (AR) switch configurations for the asymmetric 1-GE topology described in Configuration 2: 1-GE plus 10-GE Hub and Spoke, page 3-39. The following configurations are presented:

- Configuration for DER1, page B-1
- Configuration for DER2, page B-11
- Configuration for AR1, page B-20
- Configuration for AR2, page B-36

Note See Configuring the Hub-and-Spoke Topology, page 4-32.

Configuration for DER1

```
Building configuration...

Current configuration : 52268 bytes
!
! Last configuration change at 13:02:28 PDT Mon May 15 2006
! NVRAM config last updated at 13:04:45 PDT Mon May 15 2006
!
upgrade fpd auto
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service counters max age 10
!
hostname DER1
!
boot system disk0:s72033-advipservicesk9_wan-mz.122-18.SXF2.bin
logging snmp-authfail
enable password cisco
!
no aaa new-model
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
```

```
!
!
ip cef load-sharing algorithm original
ip multicast-routing
ip igmp ssm-map enable
ip domain multicast coronado.net
no ip domain-lookup
ip domain-name coronado.net
ip name-server 10.1.10.10
ipv6 mfib hardware-switching replication-mode ingress
vtp mode transparent
mls ip cef load-sharing full
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 36 to 2
mls qos
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 rapid-pvst
spanning-tree portfast bpduguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
no spanning-tree vlan 800,808,816
!
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
port-channel per-module load-balance
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 10
 name VLAN_10_Management
!
vlan 60
 name VLAN_60_VoD
!
vlan 70
 name VLAN_70_Multicast_Video
!
vlan 80
 name VLAN_80_Voice
```

```
!
vlan 800
 name Video/Voice_To/From_DER2
!
vlan 808
 name Video/Voice_To/From_AR1
!
vlan 816
 name Video/Voice_To/From_AR2
!
vlan 1100-1111,1200-1211
!
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_VoD_and_SIP_signaling
  match access-group name acl_VoD_and_SIP_signaling
class-map match-all class_video_broadcast
  match access-group name acl_video_broadcast
class-map match-all class_video_VoD
  match access-group name acl_video_VoD
!
!
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoD_and_SIP_signaling
   set dscp cs3
  class class_video_broadcast
   set dscp af41
  class class_video_VoD
   set dscp af42
  class class_VoIP
   set dscp ef
!
!
!
!
interface GigabitEthernet1/1
 description Transport to/from AR2 (GigE1/5)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 816,1200-1211
 switchport mode trunk
 dampening 5 1000 2000 20 restart 16000
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 mls qos trust dscp
!
<---output omitted--->
!
interface GigabitEthernet2/1
 description Management VLAN (CNR - DHCP, DNS, SysLog)
 switchport
 switchport access vlan 10
 switchport mode access
 dampening
```

```
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/2
 description Middleware Server (Kasenna LivingRoom Server)
 switchport
 switchport access vlan 60
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/3
 description Kasenna Gigabase Server - Management Interface (Eth0)
 switchport
 switchport access vlan 60
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/4
 description Kasenna Gigabase Server - VoD Pump (HPN0)
 switchport
 switchport access vlan 60
 switchport mode access
 dampening
 no ip address
```

```
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/5
 description Kasenna Gigabase Server - VoD Pump (HPN1)
 switchport
 switchport access vlan 60
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/6
 description Minerva Video Streamer - Multicast Video
 switchport
 switchport access vlan 70
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/7
 description VoIP SIP Server
 switchport
 switchport access vlan 80
 switchport mode access
 dampening
 no ip address
 load-interval 30
```

```
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
<---output omitted--->
!
interface GigabitEthernet2/24
 description BRAS for HSD (Dot1q-Tunnel)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1100-1111,1200-1211
 switchport mode trunk
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface TenGigabitEthernet7/1
 description Transport to/from AR1 (TenGig1/1)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 808,1100-1111
 switchport mode trunk
 dampening 5 1000 2000 20 restart 16000
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 mls qos trust dscp
!
<---output omitted--->
!
```

```
interface TenGigabitEthernet7/4
 description Transport to/from DER2 (TenGig7/4)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 800,1100-1111,1200-1211
 switchport mode trunk
 dampening 5 1000 2000 20 restart 16000
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 mls qos trust dscp
!
interface Group-Async2
 physical-layer async
 no ip address
 encapsulation slip
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description Management VLAN (CNR - DNS, DHCP, etc)
 ip address 10.1.10.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan60
 description VoD Server VLAN (Unicast Video)
 ip address 10.1.60.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan70
 description Broadcast video source VLAN (Multicast Video)
 ip address 10.1.70.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan80
 description VoIP Gateway VLAN
 ip address 10.1.80.1 255.255.255.0
 load-interval 30
!
interface Vlan800
 description Transport VLAN to/from DER2
 ip address 10.1.1.1 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
```

```
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan808
 description Transport VLAN to/from AR1
 ip address 10.1.1.9 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan816
 description Transport VLAN to/from AR2
 ip address 10.1.1.17 255.255.255.252
 ip pim query-interval 500 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
router ospf 100
 router-id 10.1.1.1
 ispf
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan10
 passive-interface Vlan60
 passive-interface Vlan70
 passive-interface Vlan80
 network 10.1.1.0 0.0.0.3 area 0
 network 10.1.1.8 0.0.0.3 area 0
 network 10.1.1.16 0.0.0.3 area 0
 network 10.1.10.0 0.0.0.255 area 0
 network 10.1.60.0 0.0.0.255 area 0
 network 10.1.70.0 0.0.0.255 area 0
 network 10.1.80.0 0.0.0.255 area 0
 network 10.1.254.1 0.0.0.0 area 0
 maximum-paths 8
!
ip classless
!
no ip http server
ip pim ssm default
!
ip access-list standard LOOPBACK
 permit 10.1.254.0 0.0.0.255
!
ip access-list extended acl_VoD_and_SIP_signaling
 permit tcp 10.1.60.0 0.0.0.255 any
 permit tcp 10.1.61.0 0.0.0.255 any
 permit tcp 10.1.80.0 0.0.0.255 any
 permit tcp 10.1.81.0 0.0.0.255 any
ip access-list extended acl_VoIP
 permit udp any any range 16384 32767
 permit udp any range 16384 32767 any
ip access-list extended acl_video_VoD
 permit udp 10.1.60.0 0.0.0.255 any
 permit udp 10.1.61.0 0.0.0.255 any
ip access-list extended acl_video_broadcast
 permit udp 10.1.70.0 0.0.0.255 232.0.0.0 0.255.255.255
```

```
!
logging event link-status default
logging trap debugging
logging 10.1.10.10
!
!
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
banner login ^CC
**********************************************************************
*
*   DDDDDD      EEEEEEEE    RRRRRRR         11
*   DD    DD    EE          RR    RR      1111
*   DD    DD    EE          RR    RR        11
*   DD    DD    EEEEE       RRRRRR          11
*   DD    DD    EE          RR   RR         11
*   DD    DD    EE          RR    RR        11
*   DDDDDD      EEEEEEEE    RR     RR   11111111
*
* Switch = Cisco7609
* Console =
* Topology = Service Router
*
**********************************************************************




^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
scheduler runtime netinput 300
ntp clock-period 17180005
ntp update-calendar
ntp server 10.1.60.10 prefer
no mac-address-table learning vlan 1100
no mac-address-table learning vlan 1101
no mac-address-table learning vlan 1102
no mac-address-table learning vlan 1103
no mac-address-table learning vlan 1104
no mac-address-table learning vlan 1105
no mac-address-table learning vlan 1106
no mac-address-table learning vlan 1107
no mac-address-table learning vlan 1108
no mac-address-table learning vlan 1109
```

```
no mac-address-table learning vlan 1110
no mac-address-table learning vlan 1111
no mac-address-table learning vlan 1200
no mac-address-table learning vlan 1201
no mac-address-table learning vlan 1202
no mac-address-table learning vlan 1203
no mac-address-table learning vlan 1204
no mac-address-table learning vlan 1205
no mac-address-table learning vlan 1206
no mac-address-table learning vlan 1207
no mac-address-table learning vlan 1208
no mac-address-table learning vlan 1209
no mac-address-table learning vlan 1210
no mac-address-table learning vlan 1211
no cns aaa enable
end
```

Configuration for DER2

```
Building configuration...

Current configuration : 52507 bytes
!
! Last configuration change at 13:02:51 PDT Mon May 15 2006
! NVRAM config last updated at 13:02:52 PDT Mon May 15 2006
!
upgrade fpd auto
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service counters max age 10
!
hostname DER2
!
boot system disk0:s72033-advipservicesk9_wan-mz.122-18.SXF2.bin
logging snmp-authfail
enable password cisco
!
no aaa new-model
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
!
!
ip cef load-sharing algorithm original
ip multicast-routing
ip igmp ssm-map enable
ip domain multicast coronado.net
no ip domain-lookup
ip domain-name coronado.net
ip name-server 10.1.10.10
ipv6 mfib hardware-switching replication-mode ingress
vtp mode transparent
mls ip cef load-sharing full
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 36 to 2
mls qos
no mls acl tcam share-global
mls cef error action freeze
!
!
!
!
!
!
!
!
!
!
redundancy
 mode rpr-plus
 main-cpu
  auto-sync startup-config
  auto-sync running-config
  auto-sync standard
```

```
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
no spanning-tree vlan 800,824,832
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
port-channel per-module load-balance
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 11
 name VLAN_11_Management
!
vlan 61
 name VLAN_61_VoD
!
vlan 70
 name VLAN_70_Multicast_Video
!
vlan 81
 name VLAN_81_Voice
!
!
vlan 800
 name Video/Voice_To/From_DER1
!
vlan 824
 name Video/Voice_To/From_AR1
!
vlan 832
 name Video/Voice_To/From_AR2
!
vlan 1100-1111,1200-1211
!
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_VoD_and_SIP_signaling
  match access-group name acl_VoD_and_SIP_signaling
class-map match-all class_video_broadcast
  match access-group name acl_video_broadcast
class-map match-all class_video_VoD
  match access-group name acl_video_VoD
!
!
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoD_and_SIP_signaling
   set dscp cs3
  class class_video_broadcast
   set dscp af41
  class class_video_VoD
   set dscp af42
  class class_VoIP
   set dscp ef
!
<---output omitted--->
!
interface GigabitEthernet1/1
 description Transport to/from AR2 (GigE1/1)
```

```
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 832,1200-1211
 switchport mode trunk
 dampening 5 1000 2000 20 restart 16000
 no ip address
 load-interval 30
 carrier-delay msec 0
 no keepalive
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 mls qos trust dscp
!
<---output omitted--->
!
interface GigabitEthernet2/1
 description Management VLAN (CNR - DHCP, DNS, SysLog)
 switchport
 switchport access vlan 11
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/2
 no ip address
 shutdown
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet2/3
 description Kasenna Gigabase Server - Management Interface (Eth0)
 switchport
 switchport access vlan 61
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
```

```
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/4
 description Kasenna Gigabase Server - VoD Pump (HPN0)
 switchport
 switchport access vlan 61
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/5
 description Kasenna Gigabase Server - VoD Pump (HPN1)
 switchport
 switchport access vlan 61
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/6
 description Minerva Video Streamer - Multicast Video
 switchport
 switchport access vlan 70
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
```

```
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
interface GigabitEthernet2/7
 description VoIP SIP Server
 switchport
 switchport access vlan 81
 switchport mode access
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input setDSCP
!
<---output omitted--->
!
interface GigabitEthernet2/24
 description BRAS for HSD (Dot1q-Tunnel)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1100-1111,1200-1211
 switchport mode trunk
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface TenGigabitEthernet7/1
 description Transport to/from AR1 (TenGig1/3)
 switchport
 switchport trunk encapsulation dot1q
```

```
 switchport trunk allowed vlan 824,1100-1111
 switchport mode trunk
 dampening 5 1000 2000 20 restart 16000
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 mls qos trust dscp
!
<---output omitted--->
!
interface TenGigabitEthernet7/4
 description Transport to/from DER1 (TenGig7/4)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 800,1100-1111,1200-1211
 switchport mode trunk
 dampening 5 1000 2000 20 restart 16000
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 mls qos trust dscp
!
interface Group-Async5
 physical-layer async
 no ip address
 encapsulation slip
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan11
 description Management VLAN (CNR - DNS, DHCP, etc)
 ip address 10.1.11.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan61
 description VoD Server VLAN (Unicast Video)
 ip address 10.1.61.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan70
 description Broadcast video source VLAN (Multicast Video)
 ip address 10.1.70.1 255.255.255.0
```

```
 no ip redirects
 no ip unreachables
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan81
 description VoIP Gateway VLAN
 ip address 10.1.81.1 255.255.255.0
 load-interval 30
!
interface Vlan800
 description Transport VLAN to/from DER2
 ip address 10.1.1.2 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan824
 description Transport VLAN to/from AR1
 ip address 10.1.1.25 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan832
 description Transport VLAN to/from AR2
 ip address 10.1.1.33 255.255.255.252
 ip pim query-interval 500 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
router ospf 100
 router-id 10.1.1.2
 ispf
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 passive-interface Vlan10
 passive-interface Vlan60
 passive-interface Vlan70
 passive-interface Vlan80
 network 10.1.1.0 0.0.0.3 area 0
 network 10.1.1.24 0.0.0.3 area 0
 network 10.1.1.32 0.0.0.3 area 0
 network 10.1.11.0 0.0.0.255 area 0
 network 10.1.61.0 0.0.0.255 area 0
 network 10.1.70.0 0.0.0.255 area 0
 network 10.1.81.0 0.0.0.255 area 0
 maximum-paths 8
!
ip classless
!
no ip http server
ip pim ssm default
```

```
!
ip access-list extended acl_VoD_and_SIP_signaling
 permit tcp 10.1.60.0 0.0.0.255 any
 permit tcp 10.1.61.0 0.0.0.255 any
 permit tcp 10.1.80.0 0.0.0.255 any
 permit tcp 10.1.81.0 0.0.0.255 any
ip access-list extended acl_VoIP
 permit udp any any range 16384 32767
 permit udp any range 16384 32767 any
ip access-list extended acl_video_VoD
 permit udp 10.1.60.0 0.0.0.255 any
 permit udp 10.1.61.0 0.0.0.255 any
ip access-list extended acl_video_broadcast
 permit udp 10.1.70.0 0.0.0.255 232.0.0.0 0.255.255.255
!
logging event link-status default
logging trap debugging
logging 10.1.10.10
!
!
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
!
banner login ^CC
**********************************************************************
*
*   DDDDDD      EEEEEEEE    RRRRRRR     22222222
*   DD    DD    EE          RR    RR          22
*   DD    DD    EE          RR    RR          22
*   DD    DD    EEEEE       RRRRRR      22222222
*   DD    DD    EE          RR   RR     22
*   DD    DD    EE          RR    RR    22
*   DDDDDD      EEEEEEEE    RR     RR   22222222
*
* Switch = Cisco7609
* Console =
* Topology = Service Router
*
**********************************************************************




^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
```

```
!
monitor event-trace timestamps
ntp clock-period 17179964
ntp update-calendar
ntp server 10.1.60.10 prefer
no mac-address-table learning vlan 1100
no mac-address-table learning vlan 1101
no mac-address-table learning vlan 1102
no mac-address-table learning vlan 1103
no mac-address-table learning vlan 1104
no mac-address-table learning vlan 1105
no mac-address-table learning vlan 1106
no mac-address-table learning vlan 1107
no mac-address-table learning vlan 1108
no mac-address-table learning vlan 1109
no mac-address-table learning vlan 1110
no mac-address-table learning vlan 1111
no mac-address-table learning vlan 1200
no mac-address-table learning vlan 1201
no mac-address-table learning vlan 1202
no mac-address-table learning vlan 1203
no mac-address-table learning vlan 1204
no mac-address-table learning vlan 1205
no mac-address-table learning vlan 1206
no mac-address-table learning vlan 1207
no mac-address-table learning vlan 1208
no mac-address-table learning vlan 1209
no mac-address-table learning vlan 1210
no mac-address-table learning vlan 1211
no cns aaa enable
end
```

Configuration for AR1

```
Building configuration...

Current configuration : 51974 bytes
!
! Last configuration change at 13:03:49 PDT Mon May 15 2006
! NVRAM config last updated at 13:03:50 PDT Mon May 15 2006
!
upgrade fpd auto
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service counters max age 10
!
hostname AR1
!
boot system flash disk0:s72033-advipservicesk9_wan-mz.122-18.SXF2.bin
logging snmp-authfail
enable password cisco
!
no aaa new-model
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
!
ip dhcp relay information trust-all
!
ip cef load-sharing algorithm original
ip multicast-routing
ip igmp ssm-map enable
ip domain multicast coronado.net
no ip domain-lookup
ip domain-name coronado.net
ip name-server 10.1.10.10
ipv6 mfib hardware-switching replication-mode ingress
vtp mode transparent
mls ip cef load-sharing full
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos map dscp-cos 36 to 2
mls qos
no mls acl tcam share-global
mls cef error action freeze
!
!
!
!
!
!
!
!
!
!
redundancy
 mode sso
 main-cpu
  auto-sync startup-config
  auto-sync running-config
  auto-sync standard
```

```
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
no spanning-tree vlan 100-111,211,808,824
spanning-tree vlan 1100-1111 priority 24576
spanning-tree vlan 1100-1111 forward-time 7
spanning-tree vlan 1100-1111 max-age 10
!
power redundancy-mode combined
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
port-channel per-module load-balance
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 100-111,200-211,808,824,1100-1111
!
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_VoD_and_SIP_signaling
  match access-group name acl_VoD_and_SIP_signaling
!
!
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoIP
   set dscp ef
  class class_VoD_and_SIP_signaling
   set dscp cs3
!
!
!
interface Loopback0
 ip address 10.10.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30
!
interface Loopback1
 ip address 10.20.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30
!
interface TenGigabitEthernet1/1
 description Transport to/from DER1 (TenGig7/1)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 808,1100-1111
 switchport mode trunk
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
```

```
 wrr-queue cos-map 2 2 3 4 6 7
 mls qos trust dscp
!
<---output omitted--->
!
interface TenGigabitEthernet1/3
 description Transport to/from DER2 (TenGig7/1)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 824,1100-1111
 switchport mode trunk
 dampening
 no ip address
 load-interval 30
 carrier-delay msec 0
 wrr-queue bandwidth 64 255 0 0 0 0 0
 wrr-queue queue-limit 40 50 0 0 0 0 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 mls qos trust dscp
!
<---output omitted--->
!
interface GigabitEthernet2/1
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,200
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/2
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1100
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
```

```
interface GigabitEthernet2/3
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 101,201
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/4
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1101
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/5
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 102,202
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/6
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1102
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
```

```
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/7
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 103,203
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/8
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1103
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/9
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 104,204
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
```

```
!
interface GigabitEthernet2/10
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1104
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/11
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 105,205
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/12
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1105
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/13
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 106,206
 switchport mode trunk
 no ip address
```

```
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/14
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1106
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/15
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 107,207
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/16
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1107
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
```

```
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/17
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 108,208
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/18
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1108
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/19
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 109,209
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/20
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1109
 switchport mode dot1q-tunnel
 no ip address
```

```
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/21
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 110,210
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/22
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1110
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/23
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 111,211
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
```

```
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/24
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1111
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan100
 description Video edge VLAN (DSLAM-1)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
 load-interval 30
 arp timout 250
!
interface Vlan101
 description Video edge VLAN (DSLAM-2)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
```

```
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
 load-interval 30
 arp timout 250
!
interface Vlan102
 description Video edge VLAN (DSLAM-3)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
 load-interval 30
 arp timout 250

!
interface Vlan103
 description Video edge VLAN (DSLAM-4)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
 load-interval 30
 arp timout 250

!
interface Vlan104
 description Video edge VLAN (DSLAM-5)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
 load-interval 30
 arp timout 250

!
```

```
interface Vlan105
 description Video edge VLAN (DSLAM-6)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
 load-interval 30
 arp timout 250

!
interface Vlan106
 description Video edge VLAN (DSLAM-7)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
 load-interval 30
 arp timout 250

!
interface Vlan107
 description Video edge VLAN (DSLAM-8)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
 load-interval 30
 arp timout 250

!
interface Vlan108
 description Video edge VLAN (DSLAM-9)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
```

```
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
 load-interval 30
 arp timout 250

!
interface Vlan109
 description Video edge VLAN (DSLAM-10)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
 load-interval 30
 arp timout 250

!
interface Vlan110
 description Video edge VLAN (DSLAM-11)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
 load-interval 30
 arp timout 250

!
interface Vlan111
 description Video edge VLAN (DSLAM-12)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 no ip igmp snooping
 ip igmp static-group 232.1.1.1 source ssm-map
 ip igmp static-group 232.1.1.2 source ssm-map
 ip igmp static-group 232.1.1.3 source ssm-map
 ip igmp static-group 232.1.1.4 source ssm-map
 ip igmp static-group 232.1.1.5 source ssm-map
 ip igmp static-group 232.1.1.6 source ssm-map
 ip igmp static-group 232.1.1.7 source ssm-map
 ip igmp static-group 232.1.1.8 source ssm-map
```

```
 ip igmp static-group 232.1.1.9 source ssm-map
 ip igmp static-group 232.1.1.10 source ssm-map
 load-interval 30
 arp timout 250

!
interface Vlan200
 description Voice edge VLAN (DSLAM-1)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan201
 description Voice edge VLAN (DSLAM-2)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 no ip igmp snooping
 load-interval 30
!
interface Vlan202
 description Voice edge VLAN (DSLAM-3)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan203
 description Voice edge VLAN (DSLAM-4)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan204
 description Voice edge VLAN (DSLAM-5)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan205
 description Voice edge VLAN (DSLAM-6)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan206
 description Voice edge VLAN (DSLAM-7)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan207
 description Voice edge VLAN (DSLAM-8)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan208
 description Voice edge VLAN (DSLAM-9)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan209
 description Voice edge VLAN (DSLAM-10)
 ip unnumbered Loopback1
```

```
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan210
 description Voice edge VLAN (DSLAM-11)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan211
 description Voice edge VLAN (DSLAM-12)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan808
 description Video/Voice Transport to/from DER1
 ip address 10.1.1.10 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan824
 description Video/Voice Transport to/from DER2
 ip address 10.1.1.26 255.255.255.252
 ip pim query-interval 100 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
router ospf 100
 router-id 10.1.1.3
 ispf
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 network 10.1.1.8 0.0.0.3 area 0
 network 10.1.1.24 0.0.0.3 area 0
 network 10.10.0.0 0.0.255.255 area 0
 network 10.20.0.0 0.0.255.255 area 0
 maximum-paths 8
!
ip classless
!
no ip http server
ip pim ssm default
!
ip access-list extended acl_VoD_and_SIP_signaling
 permit ip any host 10.1.10.10
 permit ip any 10.1.60.0 0.0.0.255
 permit ip any 10.1.61.0 0.0.0.255
 permit ip any 10.1.80.0 0.0.0.255
 permit ip any 10.1.81.0 0.0.0.255
ip access-list extended acl_VoIP
 permit udp any any range 16384 32767
 permit udp any range 16384 32767 any
!
logging trap debugging
logging 10.1.10.10
!
```

```
!
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
banner login ^CCC
**************************************************************************
*
*    AA    RRRRRRR     11
*   AAAA   RR   RR   1111
*  AA  AA  RR   RR     11
*  AAAAAA  RR RRR      11
*  AAAAAA  RR  RR      11
*  AA  AA  RR   RR     11
*  AA  AA  RR    RR  111111
*
* Switch = Catalyst7609
* Console =
* Topology = Hub & Spoke
*
**************************************************************************




^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
monitor event-trace timestamps
ntp clock-period 17179866
ntp update-calendar
ntp server 10.1.60.10 prefer
no cns aaa enable
end
```

Configuration for AR2

```
Building configuration...

Current configuration : 42149 bytes
!
! Last configuration change at 01:57:54 PDT Sun Apr 30 2006
! NVRAM config last updated at 21:19:47 PDT Thu Apr 27 2006
!
upgrade fpd auto
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service counters max age 5
!
hostname AR2
!
boot system disk0:s72033-advipservicesk9_wan-mz.122-18.SXF2.bin
logging snmp-authfail
enable password cisco
!
no aaa new-model
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
!
!
ip multicast-routing
ip igmp ssm-map enable
ip domain multicast coronado.net
no ip domain-lookup
ip domain-name coronado.net
ip name-server 10.1.10.10
ipv6 mfib hardware-switching replication-mode ingress
vtp mode transparent
mls ip cef load-sharing full
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos map dscp-cos 36 to 2
mls qos
no mls acl tcam share-global
mls cef error action freeze
!
!
!
!
!
!
!
!
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
no spanning-tree optimize bpdu transmission
```

```
spanning-tree extend system-id
no spanning-tree vlan 100-111,200-211,816,832
spanning-tree vlan 1200-1211 priority 24576
spanning-tree vlan 1200-1211 forward-time 7
spanning-tree vlan 1200-1211 max-age 10
!
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
port-channel per-module load-balance
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 100-111,200-211,816,832,1200-1211
!
class-map match-all class_VoIP
  match access-group name acl_VoIP
class-map match-all class_VoD_and_SIP_signaling
  match access-group name acl_VoD_and_SIP_signaling
!
!
policy-map setDSCP
 description Mark DSCP values for ingress traffic
  class class_VoIP
   set dscp ef
  class class_VoD_and_SIP_signaling
   set dscp cs3
!
!
!
interface Loopback0
 ip address 1.11.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30
!
interface Loopback1
 ip address 1.21.0.1 255.255.0.0
 ip ospf network point-to-point
 load-interval 30
!
!
interface GigabitEthernet1/1
 description Transport to/from DER2 (GigE 1/1)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 832,1200-1211
 switchport mode trunk
 dampening 5 1000 2000 20 restart 16000
 no ip address
 load-interval 30
 carrier-delay msec 0
 no keepalive
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 mls qos trust dscp
!
```

```
<---output omitted--->
!
interface GigabitEthernet1/5
 description Transport to/from DER1 (GigE 1/1)
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 816,1200-1211
 switchport mode trunk
 dampening 5 1000 2000 20 restart 16000
 no ip address
 load-interval 30
 carrier-delay msec 0
 no keepalive
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 mls qos trust dscp
 channel-group 2 mode desirable
!
<---output omitted--->
!
interface GigabitEthernet2/1
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,200
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/2
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1200
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/3
```

```
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 101,201
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/4
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1201
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/5
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 102,202
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/6
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1202
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
```

```
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/7
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 103,203
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/8
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1203
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/9
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 104,204
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
```

```
interface GigabitEthernet2/10
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1204
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/11
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 105,205
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/12
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1205
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/13
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 106,206
 switchport mode trunk
 no ip address
 load-interval 30
```

```
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/14
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1206
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/15
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 107,207
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/16
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1207
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
```

```
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/17
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 108,208
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/18
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1208
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/19
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 109,209
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/20
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1209
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
```

```
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/21
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 110,210
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/22
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1210
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet2/23
 description Connection To UTSI DSLAM N:1 Video and Voice VLAN
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 111,211
 switchport mode trunk
 no ip address
 load-interval 30
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
```

```
 wrr-queue cos-map 2 2 3 4 6 7
 service-policy input setDSCP
!
interface GigabitEthernet2/24
 description Connection To UTSI DSLAM 1:1 HSD
 switchport
 switchport access vlan 1211
 switchport mode dot1q-tunnel
 no ip address
 logging event link-status
 wrr-queue bandwidth 64 255 0
 wrr-queue queue-limit 40 50 0
 wrr-queue threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 1 75 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 no wrr-queue random-detect 2
 wrr-queue cos-map 1 1 0 1
 wrr-queue cos-map 2 2 3 4 6 7
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan100
 description Video edge VLAN (DSLAM-1)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 load-interval 30
!
interface Vlan101
 description Video edge VLAN (DSLAM-2)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 load-interval 30
!
interface Vlan102
 description Video edge VLAN (DSLAM-3)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 load-interval 30
!
interface Vlan103
 description Video edge VLAN (DSLAM-4)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 load-interval 30
!
interface Vlan104
 description Video edge VLAN (DSLAM-5)
```

```
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 load-interval 30
!
interface Vlan105
 description Video edge VLAN (DSLAM-6)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 load-interval 30
!
interface Vlan106
 description Video edge VLAN (DSLAM-7)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 load-interval 30
!
interface Vlan107
 description Video edge VLAN (DSLAM-8)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 load-interval 30
!
interface Vlan108
 description Video edge VLAN (DSLAM-9)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 load-interval 30
!
interface Vlan109
 description Video edge VLAN (DSLAM-10)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 load-interval 30
!
interface Vlan110
 description Video edge VLAN (DSLAM-11)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 load-interval 30
!
interface Vlan111
 description Video edge VLAN (DSLAM-12)
 ip unnumbered Loopback0
 ip helper-address 10.1.10.10
 ip pim sparse-mode
 no ip igmp snooping
 load-interval 30
!
interface Vlan200
 description Voice edge VLAN (DSLAM-1)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan201
 description Voice edge VLAN (DSLAM-2)
 ip unnumbered Loopback1
```

```
 ip helper-address 10.1.10.10
 no ip igmp snooping
 load-interval 30
!
interface Vlan202
 description Voice edge VLAN (DSLAM-3)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan203
 description Voice edge VLAN (DSLAM-4)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan204
 description Voice edge VLAN (DSLAM-5)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan205
 description Voice edge VLAN (DSLAM-6)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan206
 description Voice edge VLAN (DSLAM-7)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan207
 description Voice edge VLAN (DSLAM-8)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan208
 description Voice edge VLAN (DSLAM-9)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan209
 description Voice edge VLAN (DSLAM-10)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
interface Vlan210
 description Voice edge VLAN (DSLAM-11)
 ip unnumbered Loopback1
 ip helper-address 1.1.10.10
 load-interval 30
!
interface Vlan211
 description Voice edge VLAN (DSLAM-12)
 ip unnumbered Loopback1
 ip helper-address 10.1.10.10
 load-interval 30
!
```

```
interface Vlan816
 description Transport to/from DER1
 ip address 10.1.1.18 255.255.255.252
 ip pim query-interval 500 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
interface Vlan832
 description Transport to/from DER2
 ip address 10.1.1.34 255.255.255.252
 ip pim query-interval 500 msec
 ip pim sparse-mode
 ip ospf network point-to-point
 ip ospf hello-interval 1
 load-interval 30
!
router ospf 100
 router-id 10.1.1.4
 ispf
 log-adjacency-changes
 timers throttle spf 10 100 1000
 timers throttle lsa all 1 10 1000
 timers lsa arrival 100
 network 10.1.1.16 0.0.0.3 area 0
 network 10.1.1.32 0.0.0.3 area 0
 network 10.11.0.0 0.0.255.255 area 0
 network 10.21.0.0 0.0.255.255 area 0
 maximum-paths 8
!
ip classless
!
no ip http server
ip pim ssm default
!
ip access-list extended acl_VoD_and_SIP_signaling
 permit ip any host 10.1.10.10
 permit ip any 10.1.60.0 0.0.0.255
 permit ip any 10.1.61.0 0.0.0.255
 permit ip any 10.1.80.0 0.0.0.255
 permit ip any 10.1.81.0 0.0.0.255
ip access-list extended acl_VoIP
 permit udp any any range 16384 32767
 permit udp any range 16384 32767 any
!
logging trap debugging
logging 10.1.10.10
!
!
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
banner login ^CCCCCCC
**********************************************************************
*
*    AA    RRRRRRR   222222
*   AAAA   RR   RR       22
```

```
*  AA  AA  RR   RR       22
*  AAAAAA  RR RRR    22222
*  AAAAAA  RR  RR    22
*  AA  AA  RR   RR   22
*  AA  AA  RR    RR  222222
*
* Switch = Catalyst7609
* Console =
* Topology = Hub & Spoke
*
**********************************************************************




^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 transport input lat pad mop udptn telnet rlogin ssh nasi acercon
!
monitor event-trace timestamps
ntp clock-period 17180031
ntp update-calendar
ntp server 10.1.60.10 prefer
no cns aaa enable
end
```

Configuring Ericsson DSL Equipment

This chapter presents key details of configuring the Ericsson DSL equipment as used in the solution, and presents the following topics:

- Network Diagram, page C-1
- Hardware and Software Versions, page C-3
- Configuring Ericsson Components, page C-4
- Special Issues, page C-15

Note Ericsson DSL equipment was tested in this solution. In addition, this appendix does not provide detailed information about Ericsson products. Refer to Ericsson user documentation for further information.

Note Numbers representing VLANs and IP addresses were derive from various phases of testing and are meant to be used for examples only. Replace these numbers with those required by your particular installation.

Network Diagram

Figure C-1 on page C-2 illustrates an example network of Ericsson DSL equipment. A Public Ethernet Manager (PEM) terminal communicates with an Ethernet Controller Node (here an ECN320), which in turn aggregates traffic from one or more Ethernet DSLAM Nodes (here an EDN312xp DSLAM). The DSLAM, in turn, communicates with an HM340d home access gateway (HAG).

Table C-1 on page C-2 lists the VLANs, their descriptions, and addresses for the ECN320 and EDN312xp DSLAM. Table C-2 on page C-3 lists the configuration parameters for the HM340d.

Figure C-1 Example Ericsson Network

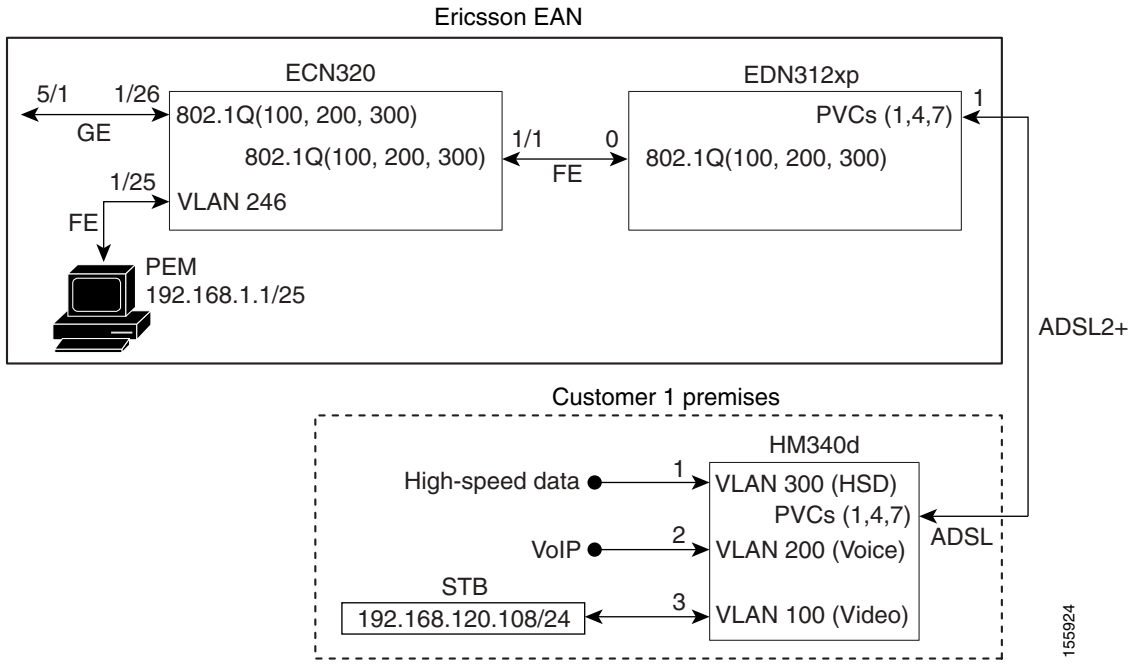


Table C-1 ECN320 and EDN312xp DSLAM VLANs, Descriptions, and IP Addresses

Node	VLAN	Description	IP Address
ECN320	300	High-speed data	Layer 2
	100	Video	Layer 2
	200	VoIP	Layer 2
	246	External interface	192.168.1.100/25
	247	Internal interface	10.0.100.1/16
	248	Untagged	10.1.100.1/24
EDN312xp DSLAM	330	High-speed data	Layer 2
	100	Video	Layer 2
	200	VoIP	Layer 2
	247	Internal interface	10.0.100.?/16
	248	Untagged	10.1.100.?/24

Table C-2 HM340d Configuration Parameters

Traffic	VLAN	HAG Ports	PVC[1]	VPI[2]	VCI[3]	Encapsulation	Service Class	PCR[4]	SCR[5]	MBS[6]
HSD	300	0	1	8	35	LLC	UBR	—	—	—
VoIP	200	1	4	0	51		CBR	—	300	—
Video	100	2	7	8	59		VBR-RT	1200	600	10

1. Permanent virtual connection
2. Virtual path identifier
3. Virtual connection identifier
4. Peak cell rate
5. Sustained cell rate
6. Maximum burst size

Hardware and Software Versions

Table C-3 on page C-3 lists the hardware and software versions for the Ericsson equipment.

Table C-3 Hardware and Software Versions for Ericsson Equipment

Equipment	Hardware Version	Software Version
Switch	ECN320, R01	CXC 132 7380 R3C06
DSLAM	EDN312xp, R1	CXC 132 8112 R2C05
RG	HM340dp Home Access Gateway, ZAT 759 89/1, R1A	CXC 132 7758 R2A

Configuring Ericsson Components

The following tasks are presented in the general order in which they should occur:

- Configuring the Switch, page C-4
- Configuring the DSLAM, page C-4
- Configuring the HAG, page C-6
- Creating Line Configurations, page C-8
- Creating Services and Profiles, page C-9
- Creating User Profiles and Adding Services, page C-12

Configuring the Switch

To configure the Ericsson ECN320 switch, use Hyperterminal or a similar application to set parameters as follows:

Interface	Area	Parameter and Setting
Management interface toward PEM	External interface	vlan = 246
		IP = 192.168.1.100
		Netmask = 255.255.255.0
Management interface toward internal nodes	Internal interface	vlan = 247
		IP = 10.0.100.1
		Netmask = 255.255.0.0
		Untagged vlan = 248
		IP = 10.0.100.1
		Netmask = 255.255.255.0

To save the completed configuration, use the following command:

config save-configuration

Configuring the DSLAM

To configure the access network on the EDN312xp DSLAM, use Ericsson's Network Configuration Manager Application and set parameters as follows:

Choose ...	Area	Parameter and Setting
Network > *Line Terminations and Regions*	Region	Region Name = Root

Choose ...	Area	Parameter and Setting
Network Elements >	DHCP Server	Name = DHCPServer
		Region = (root)
		Lease Time = 11520
	Domain File Server	IP addr = 192.168.1.1
		FTP User = ftpuser
		FTP PW = ericsson
		Remote Storage Login = eda-mp
		Remote Storage PW = ericsson
		Region = (root)
	NTP Server	IP addr = 192.168.1.1
	PEM[1] Domain Service	IP addr = 192.168.1.1
		Region = (root)
Networks >	IP Network	ID = 192.168.1.0
		Mask = 255.255.255.0
		GW = 192.168.1.20
		Max Ethernet Frame Size = 1526
	Domain Subnets	Name = Subnet1
		DHCP Server = DHCPServer
		Domain File Server = 192.168.1.1
		PEM Domain Service = DomainService
		NTP Server = 192.168.1.1
	IP Ranges	Network ID = 192.168.1.0
		Network Mask = 255.255.255.0
		Lower Limit = 192.168.1.50
		Upper Limit = 192.168.1.100

1. Public Ethernet Manager, Ericsson's DSLAM configuration application.

Note For more information on these configurations, see the document *Ericsson EDA Network and System Administration*.

Configuring the HAG

Two files are used to configure the Ericsson HM340d HAG:

- **atm.conf** describes the ATM permanent virtual circuits (PVCs) that are configured in the HAG, allowing PVC Ethernet frames to be bridged in accordance with RFC 2684. This filed is used for both the user profiles that are created. (See Creating Services and Profiles, page C-9.)
- **bridge.conf** maps the ports on the HAG to a specific VLAN/PVC number. This filed is copied and edited as appropriate for both the user profiles that are created.

Note For HAG configuration parameters, see Table C-2 on page C-3. For more information, refer to the document *Ericsson Service Gateway HM340d Operator's Guide*.

Because the HAG configuration files used in the solution are not the Ericsson defaults, you must edit the default files to configure the HAG to forward the three VLANs and services. This information is part of the DSLAM service configurations, and must also be included in the HAG configuration.

Note Data is on port 1, voice is on port 2, and video is on ports 3 and 4. The DSLAM ports are physically labeled 1 through 4 on the outside of the HAG, although in the file bridge.conf these numbers correspond to 0 through 3.

Edit the default files to conform to the following.

atm.conf

The following shows the atm.conf file used for both user profiles.

```
# atm.conf -- ATM PVC configuration

# Each line in this file will result in a ATM PVC being configured, and on this PVC
ethernet frames will be bridged (RFC 2684).


# ATM PVC Interface number 0 (zero) is the management PVC.

PVC           VPI   VCI Encap     Service Class    Parms

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

0             12     35  llc      nrtvbr           300 150 10

1              8     35  llc      ubr

2              0     35  llc      ubr

3              0     43  llc      ubr_pcr          600

4              0     51  llc      cbr              300

5              8     51  llc      nrtvbr           600 300 10

6              8     43  llc      rtvbr            600 300 10

7              8     59  llc      rtvbr            1200 600 10
```

bridge.conf

The following shows the bridge.conf file used for Profile1.

```
# bridge.conf -- virtual/software ethernet bridge configuration


# The information in this file determines which logical ethernet bridges should be
present.



# Each line is a bridge with the members as a space-separated list, were each member is
either a PVC or a tagged or untagged ethernet port. A PVC member is listed as "pvcN" where
N is the ATM PVC identifier from the /etc/atm.conf   configuration file. An untagged port
member is listed as "portN", and a tagged port as "tagged-portN", were N is the port
number (0-3, inclusive).

Each logical port (PVC, tagged or untagged ethernet port) may only be a member of one
bridge. If one untagged port (for example "port2") is used, the corresponding tagged port
("tagged-port2") may not be used, and vice versa.


# VLAN id                  Members

   300        port0           pvc1

   100         port2           pvc7

   200         port1           pvc4
```

The following shows the bridge.conf file used for Profile2. Note the addition of port 3.

```
# bridge.conf -- virtual/software ethernet bridge configuration


# The information in this file determines which logical ethernet bridges should be
present.


# Each line is a bridge with the members as a space-separated list, were each   member is
either a PVC or a tagged or untagged ethernet port. A PVC member is listed as "pvcN" where
N is the ATM PVC identifier from the /etc/atm.conf   configuration file. A untagged port
member is listed as "portN", and an tagged port as "tagged-portN", were N is the port
number (0-3, inclusive).

Each logical port (PVC, tagged or untagged ethernet port) may only be a member of one
bridge. If one untagged port (for example "port2") is used, the corresponding tagged port
("tagged-port2") may not be used, and vice versa.


# VLAN id                  Members

   300         port0           pvc1

   100        port2 port3     pvc7

   200        port1           pvc4
```

Creating Line Configurations

Line configurations are required to establish communication between the DSLAM and the HAG. A separate line configuration is used be each profile.

Using the Ericsson PEM configuration application, choose **Service Configuration > DSL Line**, and set (or confirm) parameters are as follows:

Profile	Area	Parameter	Setting
1	Channel 0	Name	OneVideoVoiceDataLow
		Transmission mode	Autodetect
		Min. bit rate downstream	7008
		Min. bit rate upstream	512
		Max. bit rate downstream	24000
		Max. bit rate upstream	1408
		Interleave delay downstream	0
		Interleave delay upstream	0
	Line	Transmit PSD	Priority to rate
		Target SNR margin downstream	6.0
		Target SNR margin upstream	6.0
		Max. SNR margin downstream	6.0
		Max. SNR margin upstream	6.0
		Rate adaptation mode	Disabled
2	Channel 0	Name	TwoVideoVoiceDataLow
		Transmission mode	Autodetect
		Min. bit rate downstream	7008
		Min. bit rate upstream	512
		Max. bit rate downstream	24000
		Max bit rate upstream	1408
		Interleave delay downstream	0
		Interleave delay upstream	0
	Line	Transmit PSD	Priority to rate
		Target SNR margin downstream	6.0
		Target SNR margin upstream	6.0
		Max. SNR margin downstream	6.0
		Max. SNR margin upstream	6.0
		Rate adaptation mode	Disabled

Creating Services and Profiles

Using the PEM configuration application, create services and user profiles for video, voice, and data. These services create the bridge between the Ethernet VLAN services for video, voice and data and the ATM PVC (VPI/VCI pairs).

Creating Services and Profiles for Video

Creating a Video Service

To create a video service using the Ericsson PEM configuration application, choose *Service Configuration* > *Action* > *Create New*, and set (or confirm) parameters as follows:

Parameter	Setting
Service Name	Video
Customer Service type	Video
CPE access method	Static IP
Relay agent configuration	Not used
IP settings	Enable IGMP snooping (checked)
Broadcast Allowed	Not checked
Default Gateway	192.168.120.1
Enable Mac forced forwarding	Checked
Enable virtual Mac address	Checked
Connections allowed	2
ATM Service Class	VBR-rt
VPI	8
VCI	59
Enable upstream policing	Checked
VLAN Usage	Service VLAN preconfigured to all switches
Ethernet Priority	5
VLAN ID	100

Creating Video Bandwidth Profiles

Create two different bandwidth configurations (profiles) for video. These can be applied to the video service configuration depending on the profile the user is using.

To create video bandwidth profiles using the Ericsson PEM configuration application, choose **Service Configuration > Video > Bandwidth > Create**, and set parameters as follows:

Profile	Parameter	Setting
1	Name	VideoLowBW
	PCR Down/Up	6016/512
	SCR Down/Up	5014/128
	MBS Down/Up	30/30
2	Name	VideoBW
	PCR Down/Up	10016/512
	SCR Down/Up	10016/128
	MBS Down/Up	30/30

Creating Services and Profiles for Voice

Creating a Voice Service

To create a voice service using the Ericsson PEM configuration application, choose **Service Configuration > Action > Create New**, and set (or confirm) parameters as follows:

Parameter	Setting
Service Name	Voice
Customer Service type	Voice
CPE access method	Static IP
Relay agent configuration	Not used
IP settings	Enable IGMP snooping (not checked)
Broadcast Allowed	Not checked
Default Gateway	192.168.121.1
Enable Mac forced forwarding	Checked
Enable virtual Mac address	Checked
Connections allowed	1
ATM Service Class	CBR
VPI	0
VCI	51
Enable upstream policing	Checked
VLAN Usage	Service VLAN preconfigured to all switches

Parameter	Setting
Ethernet Priority	6
VLAN ID	200

Creating a Voice Bandwidth Profile

Create a single bandwidth configuration (profile) for voice. This can be applied to the voice service configuration for both Profile 1 and Profile 2.

To create video bandwidth profiles using the Ericsson PEM configuration application, choose **Service Configuration > Voice > Bandwidth > Create**, and set parameters as follows:

Profile	Parameter	Setting
1, 2	Name	VoiceBW
	Down/Up	320/320
	IP address	192.168.121.107/24

Creating Services and Profiles for Data

Creating a Data Service

To create a data service using the Ericsson PEM configuration application, choose **Service Configuration > Action > Create New**, and set (or confirm) parameters as follows:

Parameter	Setting
Service Name	Data
Customer Service type	Data
CPE access method	Transparent LAN
Relay agent configuration	Not used
IP settings	Enable IGMP snooping (not checked)
Broadcast Allowed	N/A
Enable Mac forced forwarding	N/A
Enable virtual Mac address	N/A
ATM Service Class	UBR
VPI	8
VCI	35
Enable upstream policing	Checked
VLAN Usage	Service VLAN preconfigured to all switches
Ethernet Priority	0
VLAN ID	300

Note No IP address is required because a transparent VLAN for data service is used. A filter is not applicable.

Creating Data Bandwidth Profiles

Create two different bandwidth configurations (profiles) for data. These can be applied to the data service configuration depending on the profile the user is using.

To create video bandwidth profiles using the Ericsson PEM configuration application, choose **Service Configuration > Data > Bandwidth > Create**, and set parameters as follows:

Profile	Parameter	Setting
1	Name	DataLowBW
	PCR Down/Up	1152/512
	SCR Down/Up	N/A
	MBS Down/Up	N/A
2	Name	DataBW
	PCR Down/Up	1728/512
	SCR Down/Up	N/A
	MBS Down/Up	N/A

Creating User Profiles and Adding Services

Line and service configurations must be completed before you can user profiles.

The following tasks use the Ericsson PEM configuration application to create two user profiles and add video, voice, and data services.

Creating Profile 1

Do the following to create Profile 1 and add services.

Step 1 Create the profile.

a. Choose **Service Configuration > End User > New EDA End-User**.

b. Under Customer number, enter **User101**.

c. Choose **End User > Line Setup**.

d. Under Line Configuration, select **OneVideoVoiceDataLow**.

Step 2 Add video service.

a. In the Add Customized Services window, click **Add**.

b. From the drop-down menu, choose **Video**.

c. Under Bandwidth, choose VideoLowBW.

d. For Static IP Address, enter **192.168.120.109**.

e. For a filter, choose **FilterAll**.

Note This filter is created in Creating an IP Filter, page C-15.

Step 3 Add voice service.

a. In the Add Customized Services window, click **Add**.

b. From the drop-down menu, choose **Voice**.

c. Under Bandwidth, choose **VoiceBW**.

d. For the IP Address, enter **192.168.121.107**.

e. For a filter, choose **FilterAll**.

Step 4 Add data service.

a. In the Add Customized Services window, click **Add**.

b. From the drop-down menu, choose **Data**.

c. Under Bandwidth, choose **DataLowBW**.

Note No IP address is required because a transparent VLAN for data service is used. A filter is not applicable.

d. Set the EDN Name and EDF position used by the PEM to identify the line configuration for this user:

EAN Name: **ECN320-192-168-1-100**

MDF Position: **1.0.1**

e. Select **Line Activate** and **Apply** to activate User101 with the line and service configuration.

Note The connection status LED on the PEM should be green.

Creating Profile 2

Do the following to create Profile 2 and add services.

Step 1 Create the profile.

a. Choose **Service Configuration > End User > New EDA End-User**.

b. Under Customer number, enter **User102**.

c. Choose **End User > Line Setup**.

d. Under Line Configuration, select **TwoVideoVoiceDataLow**.

Step 2 Add video service.

a. In the Add Customized Services window, click **Add**.

b. From the drop-down menu, choose **Video**.

c. Under Bandwidth, choose **VideoBW**.

d. For Static IP Address, enter **192.168.120.108**, **192.168.120.110**

e. For a filter, choose **FilterAll**.

Step 3 Add voice service.

a. In the Add Customized Services window, click **Add**.

b. From the drop-down menu, choose **Voice**.

c. Under Bandwidth, choose **VoiceBW**.

d. For the IP Address, enter **192.168.121.107**.

e. For a filter, choose **FilterAll**.

Step 4 Add data service.

a. In the Add Customized Services window, click **Add**.

b. From the drop-down menu, choose **Data**.

c. Under Bandwidth, choose **DataBW**.

Note No IP address is required because a transparent VLAN for data service is used. A filter is not applicable.

d. Set the EDN Name and EDF position used by the PEM to identify the line configuration for this user:

EDN Name: **ECN320-192-168-1-100**

MDF Position: **1.0.2**

e. Select **Line Activate** and **Apply** to activate User102 with the line and service configuration.

Note The connection status LED on the PEM should be green.

Creating an IP Filter

If a static IP address is used as part of a video, voice, or data service configuration, an IP filter must be applied for the static IP address to work. Ericsson does not provide a default filter that allows all addresses in the downstream direction to be passed through to the HAG. At least one IP address must be entered into the filter, with that IP address to be marked as "allow" or "deny." Because the **range** command is not supported in the filter configuration in the downstream direction, each address through which traffic is allowed to pass must be entered individually into the filter.

A workaround is to create a filter that denies only one IP address in the downstream direction. The IP address to deny can be any IP address that will not be used to send to, or receive from, the HAG attached to the DSLAM line port for this service configuration. This solution is easier than attempting to add all the IP addresses of all devices that will be sending to, or receiving from, the device attached to the port of the HAG.

Do the following to create an IP filter.

Step 1 Using the Ericsson PEM configuration application, choose **Service Configuration > New EDA Filter**.

Step 2 Under Configuration name, enter **FilterAll**.

Step 3 Uncheck the box labeled "ICMP security enabled."

Step 4 Create an upstream filter to allow a range of IP addresses.

a. Select the **Up Stream** tab.

b. Enter **192.168.0.0 – 255.255.255.255**

c. Click **Allow**.

d. Click **OK**.

Step 5 Create a downstream filter to deny one IP address and allow all other addresses.

a. Select the **Down Stream** tab.

b. To create a filter that allows any IP addresses except the following (any IP address not used in the system), enter **172.2.2.2**.

c. Click **Deny**.

d. Click **OK**.

Step 6 Assign the filter to the desired service and line configuration.

Special Issues

Note the following special issues:

1. If multicast (broadcast) video is to be delivered to the STB through the DSLAM, the Service Configuration for Video must have IGMP snooping enabled.
2. At the time of this printing, Ericsson DSL equipment does not support IGMP version 3. If IGMPv3 commands are sent to the Ericsson equipment, messages are discarded and the broadcast is not played through the STB. Consequently, Cisco switches connected to the Ericsson ECN320 switch must send IGMPv2 commands to the Ericsson equipment.

Configuring UTStarcom DSL Equipment

The UTStarcom DSLAM AN-2000 B820 consists of a chassis capable of holding up to 16 ADSL line cards. These line cards support ADSL, ADSL2, and ADSL2+ residential gateways (RGs). Each ADSL line card has 24 ADSL ports that can be used to connect to 24 RGs. Each line card must be configured separately.

In addition to the ADSL cards, the chassis also contains an ICM3 controller card, which controls the GE trunk ports as well as global chassis parameters, such as QoS and VLAN definitions.

A network management application, called Netman 4000, is used to configure the ICM3 and the ADSL line cards.

This chapter presents key details of configuring the UTStarcom DSL equipment as used in the solution, and presents the following topics:

- Provisioning the Netman 4000 Application to Manage the DSLAM, page D-2
- Configuring the ICM3 Ethernet Interface Line Card, page D-5
- Configuring the PCU Card on the DSLAM, page D-12
- Configuring the ADSL Profiles, page D-13
- Configuring the IPADSL3A Line Cards, page D-17

Note UTStarcom DSL equipment was tested in this solution. This appendix does not provide detailed information about UTStarcom products. Refer to UTStarcom user documentation for further information.

Note Numbers representing VLANs and IP addresses were derive from various phases of testing and are meant to be used for examples only. Replace these numbers with those required by your particular installation.

Provisioning the Netman 4000 Application to Manage the DSLAM

Do the following to configure the DSLAM IP addresses and use the Netman 4000 Network Management Application to recognize and provision the DSLAM.

- Configuring the DSLAM to Use the Netman 4000 Network Management Application
- Adding an AN-2000 B820 DSLAM Node to the Netman 4000 Network Management Application
- Configuring DSLAM Node Settings
- Configuring DSLAM Name and Contact Information (Optional)
- Configuring the DSLAM Node Address

Note For details, refer to the *UTStarcom AN-2000 B820 IP DSLAM Operations Manual, Release 2.4*.

Configuring the DSLAM to Use the Netman 4000 Network Management Application

Do the following to configure the DSLAM to use the Netman 4000 Network Management Application.

Step 1 Connect an Ethernet cable between Netman 4000 Dell PC laptop and the NMS In port on the back of the PCU module of the AN-2000 B820.

Step 2 Connect the PC's serial (DS9 connector) port to the ICM3's debug/console port.

Step 3 Start Hyperteminal session 9600/N/8/1.

Step 4 At the login prompt, login as **admin** with the password **AdMiN123**.

Step 5 Type **ip show ip** to check your current out-of-band IP configuration. The default IP address is 10.20.x.x.

Step 6 Set the IP address for the management system as follows.

a. At the system prompt, enter the command as shown below.

```
AN2000_IB# ip management address 99.98.97.96, netmask 255.255.255.0
```

b. When prompted to change the network address, answer **yes**.

c. Wait 10 to 15 seconds, then use another PC to ping your LAN gateway to verify the connection.

Step 7 Set the IP address of the Netman 4000 Dell PC to **99.98.97.90**. You should then be able to telnet from the PC to the AN-2000 B820's address, 99.98.97.96.

Step 8 Using a console or telnet, telnet to AN-2000 B820. Configure the node as follows to allow SNMP access for your NMS, which is located at 99.98.97.90.

```
AN2000_IB# snmp netman-destination 99.98.97.90 primary
```

Step 9 Save the configuration.

```
AN2000_IB# save config
```

Adding an AN-2000 B820 DSLAM Node to the Netman 4000 Network Management Application

Do the following to add an AN-2000 B820 DSLAM node to the Netman 4000 Network Management Application.

Step 1 Start the Netman 4000 server by clicking the **StartNetmanLite** icon on the desktop of the Dell PC.

Step 2 To use the GUI interface of the Netman Application, launch Internet Explorer and type the following in the Address field:

```
http://99.98.97.90:9090
```

Step 3 Log in as user **root**, with password **public**.

The UTStarcom Network Management System window appears, indicating "NetmanLite 4000 version 2.4.6.15P7" at the bottom of the window.

Step 4 Click the **Please Click, Enter** message.

Step 5 Click the **Edit Lock** icon (the second icon from the top left of the window). Devices cannot be added unless this icon is selected (indicated by a dark gray background).

Step 6 Move the cursor to the window labeled **root** (right side of screen) and right click.

Step 7 Choose **Create NE** from the drop-down list. The Create NE window appears.

a. Under **NE Type**, choose **IP DSLAM**.

b. Under **NE Label**, enter a name for a new DSLAM (for example, **DSLAM_1**).

c. Under **IP Address**, enter the address of the new DSLAM (for example, **99.98.97.96**).

d. Click **OK** to close the window.

Note If the device is added properly, the new DSLAM (named DSLAM_1) appears under "root" in the Physical View window (left side of screen). In addition, a red DSLAM icon labeled DSLAM_1 is displayed in the window labeled "root."

Step 8 Double-click **DSLAM_1**.

A new window labeled DSLAM_1 is displayed.

Step 9 Click the node on the left side of the window under the "root" icon to see the shelf (node) and all the cards in the chassis.

Configuring DSLAM Node Settings

Do the following to configure DSLAM node settings. A node refers to a UTStarcom DSLAM system.

Step 1 Click the newly configured node on left side of the screen.

Step 2 Click the **Configuration** tab at the top of the window.

Step 3 Choose the **Node ID** menu item.

Step 4 Give the DSLAM a node ID it can pass along for a PPPoE session, to identify the node uniquely. Enter **9876**.

Note The Node ID can be any string that identifies the UTStarcom DSLAM system uniquely.

Step 5 Click **Apply**.

Configuring DSLAM Name and Contact Information (Optional)

Do the following to configure the DSLAM name and contact information. (Though not required, this may be useful for network management.)

Step 1 Choose **Node > System**.

Step 2 Enter information about the **System Name**, **Location**, and **Contact**.

Step 3 Click **Apply**.

Step 4 Click the **Configuration** tab and choose **Save** from the drop-down menu.

Configuring the DSLAM Node Address

Do the following to configure the DSLAM node address.

Step 1 Choose **Node > IP Address**.

Step 2 Confirm the default or set the values shown below.

Area	Parameter	Setting
ICMP IP Address	Address	99.98.97.96
	Subnet Mask	255.255.255.0
IP Pool for Line Card	Starting IP Address	192.168.100.1
	Subnet Mask	255.255.255.0
	IP Pool Size	33
Trap Destination to Netman	Destination 1: 99.98.97.90	
	Destination 2: 0.0.0.0	
IP Pool for Standby IP Address	Address	192.168.200.1
	Subnet Mask	255.255.255.0
	IP Pool Size	2

Step 3 Choose **Node > NMP Access**.

Step 4 Confirm the default or set the values shown below.

Area	Parameter	Setting
Telnet	NMP access	Enabled

Configuring the ICM3 Ethernet Interface Line Card

The ICM3 card on the DSLAM controls the GE trunk ports that connect the DSLAM to the Cisco aggregation routers (ARs). It also controls QoS mapping of VLANs coming into the DSLAM, as well as the IGMP traffic entering the DSLAM from the trunks. This section presents the following tasks:

- Viewing the Hardware and Software Version of the ICM3 Line Card
- Enabling IGMP Snooping for the DSLAM System
- Displaying Multicast Group Information
- Using Default Settings for Other ICM3 Card Parameters
- Activating the Internal Ethernet Interfaces of the ADSL Line Cards
- Activating the External GE Trunk Ports
- Disabling RSTP on the DSLAM
- Defining VLANs on the DSLAM to Support Triple-Play Services
- Configuring QoS on the ICM3 Controller Card

Viewing the Hardware and Software Version of the ICM3 Line Card

Do the following to view the hardware and software versions of the ICM3 line card.

Step 1 Choose **Node > Shelf1 > SlotA:Active ICM3**.

Step 2 Confirm the following hardware and software versions, which were tested in the solution.

Parameter	Setting
Hardware Version	2990082200
Software Version	2.3.1.11

Enabling IGMP Snooping for the DSLAM System

Do the following to enable IGMP snooping on the DSLAM system.

Step 1 Choose **Node > Shelf1 > SlotA:Active ICM3**.

Step 2 Click the **IGMP** tab.

Step 3 Confirm or set the following as indicated.

Parameter	Setting
IGMP Snooping	Enabled
Unknown Group	Drop (do not forward groups that are not requested)
IGMP Router	Leave all items unchecked

Step 4 Click **Apply**.

Displaying Multicast Group Information

Do the following to display multicast group information.

Step 1 Choose **Node > Shelf1 > SlotA:Active ICM3**.

Step 2 Click the **Multicast Group** tab.

Step 3 Do no configuration here. However, you can see the active multicast groups, the VLANs ID of the groups, and line card to which a group is forwarded.

Using Default Settings for Other ICM3 Card Parameters

Do the following to use default settings for other ICM3 card parameters.

Note Redundancy features of the DSLAM were not used in solution testing.

Step 1 Choose **Node > Shelf1 > SlotA:Active ICM3**.

Step 2 Click the **Switch** tab, and use the following default values.

Parameter	Setting
DFL Frames	Discard
Aging Timer	300
VLAN ID	1
Static Entries	None shown

Step 3 Click the **Mirror** tab and use the following default values.

Parameter	Setting
Mirror Port	None
Mirror Receive Port	None
Mirror Transport Port	None

Step 4 Click the **Trunk Port** tab and verify that there are no settings.

Step 5 Click the **Protection Link** tab and select **G1** and **G2**.

Step 6 Click the **Redundancy Support** and use the following default values.

Parameter	Setting
Standby ICM Status	Admin Prohibited
Standby ICM Redundancy Support	Prohibited

Activating the Internal Ethernet Interfaces of the ADSL Line Cards

Do the following to activate the internal Ethernet interfaces of the ADSL line cards.

Step 1 Choose **Node > Shelf1 > SlotA:Active ICM3 > Ethernet Port**.

Step 2 Choose **Ethernet Port > Internal Ethernet Port**.

Step 3 Confirm that each IPADSL3A line card installed in the DSLAM is shown with the Operational Status of Enabled.

Activating the External GE Trunk Ports

Do the following to activate the external GE trunk ports.

Step 1 Choose **Node > Shelf1 > SlotA:Active ICM3 > Ethernet Port**.

Step 2 Click the **External Ethernet Ports** tab.

Step 3 Double-click **G1** to select it, and configure it as follows.

Parameter	Setting
Port ID	G1
Administrative State	Unlocked (enabled)
Speed Duplex	N/A
Flow Control	On
Incoming Speed Limit	Disable
Outgoing Speed Limit	Disable
Broadcast Rate Threshold	300

Step 4 Click **Apply**.

Step 5 Choose G2 and configure it is as in Step 3. except change the **Port ID** to **G2**.

Step 6 Click **Apply**.

Disabling RSTP on the DSLAM

Do the following to disable RTSP on the DSLAM.

Step 1 Choose **Node > Shelf1 > SlotA:Active ICM3 > RSTP**.

Step 2 Set **RSTP** to **Disable.** This is because of the use of dual GE links.

Step 3 Click **Apply**.

Defining VLANs on the DSLAM to Support Triple-Play Services

Do the following to define VLANs on the DSLAM to support triple-play services.

Note You must first define VLANs under the **ICM3** menu, then assign them to individual DSL ports under the **Slot** configuration.

Step 1 Choose **Node > Shelf1 > SlotA:Active ICM3 > VLAN**.

Step 2 Confirm or select the following.

Parameter	Setting
Unknown VLAN	Discard
Ingress Check	Enabled

Note The internal ADSL line cards each have an associated internal Ethernet port that is used to pass traffic from the trunk port to the line card. ADSL Ethernet line cards are shown as l1, l2, l3, and so on. The line cards must be associated with the VLANs that carry data to them. VLANs remain tagged when passed from the trunk port to the line card, or from the line card to the trunk port and out to the AR.

Step 3 Create the new VLAN to be used for broadcast and VOD traffic. To do this, click the **Add** key and enter the following information.

Parameter	Setting
VLAN ID	100
VLAN Name	VideoVlan100
Tagged Port	11, 12, 13, G1
Untagged Port	None

Step 4 Click **Apply**.

Step 5 Create the new VLAN to be used for voice traffic. To do this, select the **Add** key and enter the same information as in Step 3, except change **VLAN ID** to **200**.

Step 6 Click **Apply**.

Note In the hub-and-spoke topology, each DSL port (user) is assigned a unique VLAN to carry the data service. For testing in this release of the solution, VLANs 500–550 were reserved as the data VLANs. One unique VLAN must be defined per user. For test purposes, three data VLANs were defined. The VLANs are tagged when entering or exiting the line card or the G2 trunk port connecting the DSLAM to the AR.

Step 7 To create a unique data VLAN per user, where all data VLANs are assigned to DSLAM GE Port 2, do the following.

a. Click the **Add** key, and enter the following to define the first data VLAN.

Parameter	Setting
VLAN ID	500
VLAN Name	DataVlan500
Tagged Port	l1, G2
Untagged Port	None

b. Click **Apply**.

c. To define the second data VLAN, proceed as in Step 7a, but change **VLAN ID** to **501** and **VLAN Name** to **DataVlan501**.

d. Click **Apply**.

e. To define the third data VLAN, proceed as in Step 7a, but change **VLAN ID** to **502** and **VLAN Name** to **DataVlan502**.

f. Click **Apply**.

Step 8 Click the **Configuration** tab and choose **Save** from the drop-down menu.

Configuring QoS on the ICM3 Controller Card

Do the following to configure QoS on the ICM3 controller card.

Step 1 Choose **Node > Shelf1 > SlotA:Active ICM3 > QoS**.

Step 2 Click the **Priority** tab.

Step 3 Click **l1** to highlight Line Card 1.

a. Click the **DSCP Priority** field (right column).

b. From the drop-down menu, choose **Map DSCP to 802.1p**.

c. Click **Apply**.

d. Repeat Step 3a through Step 3c for each line card shown in the menu.

Step 4 Click **G1** to highlight the port.

a. Click the **DSCP Priority** field.

b. If this feature is disabled, choose **Select Map DSCP to 802.1p** from the drop-down menu.

c. Click **Apply**.

Step 5 Select **G2** to highlight the port, then proceed as in Step 4 and click **Apply**.

Step 6 Click the **Configuration** tab and choose **Save** from the drop-down menu.

Step 7 Click the **DSCP Priority** tab. All the IEEE 802.1p Priority fields on the right side of the screen should be set to 0, by default.

a. Change the following DSCP values to map to the selected IEEE 802.1p Priority as shown below.

Tip To change the priority, click the DSCP value and click on the right side of the screen under IEEE 8021p Priority. Then select the priority from the drop-down menu, clicking **Apply** after each change.

Parameter	Setting
DSCP 0	Priority 0
DSCP 24	Priority 4
DSCP 34	Priority 4
DSCP 36	Priority 4
DSCP 46	Priority 7

Note The mapping of DSCP to 802.1p Priority, and the remapping of the 802.1p bits as described above, forces the DSLAM to use the correct downstream priority queue for each service when data is sent to the residential gateway. There are three queues available in the downstream direction. The following table explains how the voice, video, data services are mapped to the ATM queues on the DSLAM.

Triple-Play Service	DSCP Value	Remapped 802.1p Value	ATM Queue
High-speed data	0	0	0 (low)
Signaling for video	24	4	1 (medium)
VoD	34	4	
Multicast/broadcast video	36	4	
Voice	46	7	2 (high)

b. Click the **Configuration** tab and choose **Save** from the drop-down menu.

Step 8 Click the **Queue Mapping** tab and accept the default values, which should be as follows.

IEEE 802.1p Priority	CoS Traffic Class
0	2
1	0
2	1

IEEE 802.1p Priority	CoS Traffic Class
3	3
4	4
5	5
6	6
7	7

Step 9 Click the **L2 Scheduling** tab and use the default values, which should be as follows.

Parameter	Setting
Scheduling Method	Strict priority
Weighted Round Robin	Not selected

Configuring the PCU Card on the DSLAM

Do the following to configure the PCU card on the DSLAM.

Note The defaults are used to configure the PCU card.

Step 1 Click the **PCU** tab and confirm the following.

Parameter	Value
Hardware Version	1.3
Software Version	1.7

Step 2 Click the **Clock Source** tab and confirm that no external clock is selected.

Step 3 Click the **Alarm Indication** tab and confirm the following.

Parameter	Setting
Pin Label	Not configured
Severity	Warning
Level	Never Raise Alarm

Step 4 Click the **PDP** tab and confirm the following.

Parameter	Setting
PDP Collect Alarm from PDP	Disabled
Control Alarm from PDP	Disabled
Control Buzzer on PDP	Disabled

Configuring the ADSL Profiles

The DSLAM supports ADSL, ADSL2, and ADSL+ residential gateways. This section presents the following tasks:

- Creating an ADSL2+ Profile
- Creating an ADSL2 Profile

Creating an ADSL2+ Profile

This profile works for the Linksys WAG54GP2 RG and other RGs which support ADSL2+. Do the following to create an ADSL2+ profile.

Step 1 Using the Netman application, double-click a DSLAM to configure under the Physical View window.

Step 2 Click the **Provisioning** tab (lower left).

Step 3 In the window with the name of the node, click the **Profile** tab and choose **ADSL Line Profile** from the menu.

Step 4 Click **Add** at the bottom of the **ADSL Line Profile** window and confirm or enter the following settings:

Parameter	Setting
Profile Name	ADSL2+
Line Standard	ADSL2Plus/ADSL2/ReA DSL2/G.dmt Annex A Automode
Annex Type	Annex A
Downstream Spectrum	Double
Upstream Spectrum	Single

Step 5 Click **Next**. The following should be set by default.

Parameter	Setting
Trellis Coding	On
Rate Mode	Adaptive at Runtime
Target Downstream SNR Margin (dB)	6
Downstream Upshift SNR Margin (dB)	9
Downstream Min Downshift Time (0–16383 s)	60
Downstream Bit Swapping	Enable
Target Upstream SNR Margin (dB)	6
Upstream Bit Swapping	Enable
Spectrum Mask	No mask
Transmission Mode	FDM
Max Downstream SNR Margin (dB)	31
Downstream Downshift SNR Margin (dB)	3
Downstream Min Upshift Time (0–16383 s)	60
Max Upstream SNR Margin (dB)	31
ATM Header Compression	Disable

Step 6 Click **Next**, then confirm or enter the following.

Parameter	Setting
Downstream Latency	Interleave
Downstream Interleave delay (ms)	8
Downstream Min Rate (kbps)	11000
Downstream Max Rate (kbps)	32736
Upstream Latency	Interleave
Upstream Interleave Delay (ms)	8
Upstream Min Rate (kbps)	980
Upstream Max Rate (kbps)	1536

Step 7 Click **Apply**.

Step 8 Click the **Configuration** tab and choose **Save** from the drop-down menu.

Creating an ADSL2 Profile

Do the following to create an ADSL2 profile.

Note This profile can be used with the Ericsson HM340dp Residential Gateway, which supports ADSL2.

Step 1 In the Physical View window, double-click a DSLAM to configure.

Step 2 Click the **Provisioning** tab.

Step 3 In the window with the name of the node, click the **Profile** tab and choose **ADSL Line Profile** from the menu.

Step 4 Click **Add** at the bottom of the **ADSL Line Profile** window and confirm or enter the following settings:

Parameter	Setting
Profile Name	ADSL2
Line Standard	ADSL2/ReADSL2/G.dmt Annex A Automode
Annex Type	Annex A
Downstream Spectrum	Single
Upstream Spectrum	Single

Step 5 Click **Next**. The following should be set by default.

Parameter	Setting
Trellis Coding	On
Rate Mode	Adaptive at Runtime
Target Downstream SNR Margin (dB)	6
Downstream Upshift SNR Margin (dB)	9
Downstream Min Downshift Time (0–16383 s)	60
Downstream Bit Swapping	Enable
Target Upstream SNR Margin (dB)	6
Upstream Bit Swapping	Enable
Spectrum Mask	No mask
Transmission Mode	FDM
Max Downstream SNR Margin (dB)	31
Downstream Downshift SNR Margin (dB)	3
Downstream Min Upshift Time (0–16383 s)	60
Max Upstream SNR Margin (dB)	31
ATM Header Compression	Disable

Step 6 Click **Next**, then confirm or enter the following.

Parameter	Setting
Downstream Latency	Interleave
Downstream Interleave Delay (ms)	8
Downstream Min Rate (kbps)	8764
Downstream Max Rate (kbps)	12032
Upstream Latency	Interleave
Upstream Interleave Delay (ms)	8
Upstream Min Rate (kbps)	720
Upstream Max Rate (kbps)	1536

Step 7 Click **Apply**.

Step 8 Click the **Configuration** tab and choose **Save** from the drop-down menu.

Tip After the RG has trained, do the following to see the actual upstream and downstream bandwidths for that ADSL line: Choose **Node > Shelf1 > Slot 1 > ADSL Port**, and click the **Port** tab. ADSL ports and their status are displayed.

Note Both the ADSL and ADSL2+ ADSL line profile use Automode. This means the RG runs in its native mode, whether it is ADSL or ADSL2+.

Note The default ADSL Profile applied by the DSLAM works with most CPEs, but it will run at lower upstream and downstream bandwidths than the ADSL2 configuration described above. The default profile, *Adslprof_def*, can support the maximum downstream rate of 8064 kbps and the maximum upstream rate of 864 kbps. This rate is only adequate enough to support one STB. If two STBs are to be supported, the ADSL2 or ADSL2+ profile should be selected for the ADSL Line Profile.

Configuring the IPADSL3A Line Cards

This section presents the following tasks:

- Configuring the AN-2000 B820 DSLAM Card Modules
- Verifying the WAN Port
- Configuring and Activating the ADSL Ports
- Configuring ATM PVCs and Assigning Them to ADSL Ports
- Configuring the Number of MAC Addresses Supported per Port
- Configuring the Port Label Used for DHCP Option 82
- Creating VLAN-to-PVC Mappings for Voice, Video, and Data
- Verifying the Access List Configuration on the DSLAM
- Configuring QoS for the IPADSL3A Line Cards
- Saving the Configuration

Configuring the AN-2000 B820 DSLAM Card Modules

Each DSL line card acts a separate DSLAM unit, and must be configured separately.

Do the following to configure the AN-2000 B820 DSLAM card modules.

Step 1 In the Physical View window, double-click a DSLAM to configure.

Step 2 Click the **Provisioning** tab.

Step 3 Choose **Node > Shelf1 > Slot1:IPADSL3A**, and check the IPADSL3A line card hardware and software version. The versions tested in the solution are shown below:

Parameter	Value
Hardware Revision	2990084000:B1
Software Version	5.2.1.8

Step 4 From the window on the right, click the **Customized Filter** tab and confirm or set values as shown below:

Parameter	Setting
Semi-Static Forwarding	Disabled
Gateway ARP Filter	Disabled
Gateway IP Address	0.0.0.0
Aging Timer	14400
Unknown LAN	N/A
Upstream Multicast Filter	Disabled
IGMP Last Query Interval	2
IGMP No Response Leave	2
ARP Tracking	Disabled
NetBIOS Filter	Uplink Only or Disabled
DHCP Filter	Disabled
DFL Counter	10
IGMP Snooping	Enabled, Discard Unknown
DHCP Option 82	Enabled
IGMP Last Query Count	1
IGMP No Response Leave Query Count	1

Step 5 Click **Apply**.

Note If IGMP Snooping is enabled but Forward Unknown is also enabled, the broadcast will continue to be forwarded to devices that did not request it, causing multicast flooding and macroblocking to be displayed on attached STBs.

Step 6 Click the **PPPoE Intermediate Agent** tab (top right) and choose **Enabled**.

Step 7 Click **Apply**.

Note The PPPoE Intermediate Agent Enable field allows the DSLAM node ID and port information to be added to any PPPoE request.

Step 8 (Optional) If DHCP Option 82 is to be used, click the **Packet Policing** tab (at the top of the right menu).

a. For each port that will use DHCP, click the port to select it.

Tip To select multiple ports, click the first port, hold the shift key down, and click the last port.

b. Click the **DHCP** check box under IP Address Assignment. Do not click any other fields.

c. Click **Apply**.

Step 9 Click the **Configuration** tab and choose **Save** from the drop-down menu. The configuration is saved in the DSLAM's flash memory.

Verifying the WAN Port

Each IPADSL3A card has an integrated WAN port. This port is enabled automatically.

Do the following to verify that the WAN port is up and running.

Step 1 Choose **Node > Shelf1 > Slot1 > WAN Port**.

Verify the following:

Parameter	Setting
Administrative State	Unlocked
Operational State	Enabled
Actual Speed	100 Mbps
Duplex	Full

Note If the Administrative State is Locked, or if the Operational State is Disabled, the card may not be installed properly in the chassis, or it may be defective.

Configuring and Activating the ADSL Ports

ASDL2, and ADSL2+ line profiles must be created before they can be assigned to an ADSL line. (See Creating an ADSL2+ Profile, page D-13, and Creating an ADSL2 Profile, page D-15.) The profile *adslprof_def* has default values and is always available. It works well with one STB, but does not allow enough bandwidth to support two broadcast video streams.

Do the following to configure and activate the ADSL ports.

Step 1 Attach a configured RG to the ADSL line. (For an RG configuration, see Configuring Ericsson DSL Equipment, page C-1.)

Step 2 Choose **Node > Shelf1 > Slot1:IPADSL Port**, and click the **ADSL Port** tab.

Step 3 Click **Assign Profile** (bottom of screen).

Step 4 From the menu, choose **Profile ADSL2** for the Ericsson 340dp RG, or **ADSL2+** for the Linksys WAG54GP2 RG or another ADSL2+ RG.

Step 5 Click **OK**.

Note ADSL line configuration cannot be changed unless the port is locked (deactivated). After changes are made, the port needs to be unlocked in order to activate it.

Step 6 Click the ADSL line again to highlight it, then click to unlock and activate the port.

Note The DSL or Link light on the ADSL RG should light up and stay on. Also, the Port LED on the IPADSL3A card should light up, to show that the line is active. To see the downstream and upstream bit rates once the port is activated, choose the **ADSL Port** menu.

Configuring ATM PVCs and Assigning Them to ADSL Ports

You need to create three permanent virtual circuits (PVCs) and assign to them to ADSL ports (DSL lines). A PVC pair must be created for each service: voice, video, and data.

Do the following to create ATM PVCs and assign them to ADSL ports.

Step 1 Create the PVC to be used for the video service.

a. In the Physical View window, double-click a DSLAM to configure.

b. Click the **Provisioning** tab.

c. Choose **Node > Shelf1 > Slot1 > ATM VC**.

The ATM VC window appears.

d. Click the **Add** button at the bottom of the window.

e. From the list, select the ports to which to assign the PVC.

Tip To select multiple ports, click the first port, hold the shift key down, and click the last port.

f. Confirm or enter the following:

Parameter	Setting
VPI	8
VCI	59
CoS	N/A[1]
Connection Type	PVC
PPPoA to PPPoE Conversion	Disabled
Multiplex Method	LLC

1. Not applicable to UTStarcom AN-2000 B820 (not ATM).

g. Click **Apply**.

Step 2 Create the data PVC and assign it to a DSL line.

a. Choose **Node > Shelf1 > Slot1 > ATM VC**.

The ATM VC window appears.

b. Click the **Add** button at the bottom of the window.

c. From the list, select the ports to which to assign the PVC.

d. Confirm or enter the following:

Parameter	Setting
VPI	8
VCI	35
CoS	N/A[1]
Connection Type	PVC
PPPoA to PPPoE Conversion	Disabled
Multiplex Method	LLC

1. Not applicable to UTStarcom AN-2000 B820 (not ATM).

e. Click **Apply**.

Step 3 Create the voice PVC and assign it to a DSL line.

a. Choose **Node > Shelf1 > Slot1 > ATM VC**.

The ATM VC window appears.

b. Click the **Add** button (bottom).

c. From the list, select the ports to which to assign the PVC.

d. Confirm or enter the following:

Parameter	Setting
VPI	0
VCI	51
CoS	N/A[1]
Connection Type	PVC
PPPoA to PPPoE Conversion	Disabled
Multiplex Method	LLC

1. Not applicable to UTStarcom AN-2000 B820 (not ATM).

e. Click **Apply**.

Step 4 Click the **Configuration** tab and choose **Save** from the drop-down menu.

Note CoS (UBR, CBR, VBR) does not apply to this DSLAM. Instead, Ethernet QoS must be used.

Note The PVCs created on the DSLAM match the PVCs created on the RGs (residential gateways, ADSL modems, or home access gateways). (For an RG configuration, see Configuring Ericsson DSL Equipment, page C-1.)

Tip In order to view the amount of data received by each PVC, and whether any data is being dropped, choose **Node > Shelf1 > Slot1** and click the **Performance** tab (bottom of screen). Then click the **Bridge** tab (top of screen).

Configuring the Number of MAC Addresses Supported per Port

Do the following to configure the number of MAC addresses that can be supported by a specific PVC on a line port.

Step 1 Click the **Provisioning** tab.

Step 2 Choose **Node > Shelf1 > Slot1 > ADSL Port**.

Step 3 Click the **MAC Address Per Port** tab.

Step 4 Choose the number of MAC addresses for each PVC/ADSL line port.

Step 5 Click the port to be configured.

Step 6 Click **Modify**.

Step 7 From the drop-down list, choose four MAC addresses per port.

Step 8 Click **Apply**.

Configuring the Port Label Used for DHCP Option 82

If DHCP Option 82 is used to add client information to the DHCP request, you must assign each port a port label that is a unique identifier.

Do the following to configure the port label used for DHCP Option 82.

Step 1 Click the **Provisioning** tab.

Step 2 Choose **Node > Shelf1 > Slot1 > ADSL Port**.

Step 3 Click the **Port Label** tab.

Step 4 Choose **Port 1**, then click **Modify**.

Step 5 Enter a label that identifies the DSLAM, Slot, and ADSL Port Number.

Note You can enter any string for the port label. The port label is used by the DHCP server to identify the port and user uniquely.

Step 6 Click **Apply**.

Step 7 Choose the next port, then proceed as in Step 2 through Step 6.

Step 8 Repeat Step 7 for each port.

Step 9 Click the **Configuration** tab and choose **Save** from the drop-down menu.

Creating VLAN-to-PVC Mappings for Voice, Video, and Data

Each VLAN that enters the DSLAM through the GE trunk ports must be mapped to a PVC in order for the data to be sent over the ADSL port to the RG. Conversely, PVCs that carry voice, video, and data traffic from the RG to the DSLAM must be mapped to VLANs before the data can be sent out the GE ports of the DSLAM to the AR.

Do the following to create VLAN-to-PVC mappings for voice, video, and data.

Step 1 Create the VLAN-to-PVC mapping for the video service.

a. Click the **Provisioning** tab.

b. Choose **Node > Shelf1 > Slot1 > VLANs**.

c. Click the **VLAN** tab.

d. Click **Add** and confirm or enter the following:

Parameter	Setting
VLAN ID	100
User Isolation	Disabled
VLAN Name	VideoVlan100
Tagged Ports	WAN Only
Untagged Ports	01:08:59, 02:08:59, 03:08:59, and so on[1]

1. Select the PVC port pairs that apply for that VLAN.

e. Click **Apply**.

Step 2 Create the VLAN-to-PVC mapping for the voice service.

a. Proceed as in Step 1a through Step 1c, but make the following changes:

Set **VLAN ID** to **200**.

Set **VLAN Name** to **VoiceVlan200**.

Set **Untagged Ports** to **01:00:51**. (Select the PVC port pairs that apply for that VLAN.)

Set **Tagged Ports** to **WAN**.

b. Click **Apply**.

Step 3 Create a VLAN-to-PVC mapping for the data service. In this case, a unique VLAN is assigned to each ADSL port (user) for the data PVC, which is 8:35.

a. Create a data VLAN for User 1. Proceed as in Step 1a through Step 1c, but make the following changes:

Set **VLAN ID** to **500**.

Set **VLAN Name** to **DataVlan500**.

Set **Untagged Ports** to **01:08:35**. (Select the PVC port pairs that apply for that VLAN.)

b. Click **Apply**.

c. Create a data VLAN for User 2. Proceed as in Step 3a through Step 3b, but make the following changes:

   Set **VLAN ID** to **501**.

   Set **VLAN Name** to **DataVlan501**.

   Set **Untagged Ports** to **02:08:35**.

d. Click **Apply**.

e. Create a data VLAN for User 3. Proceed as in Step 3a through Step 3b, but make the following changes:

   Set **VLAN ID** to **502**.

   Set **VLAN Name** to **DataVlan502**.

   Set **Untagged Ports** to **03:08:35**. (Select the PVC port pairs that apply for that VLAN.)

f. Click **Apply**.

Note The hub-and-spoke topology calls for a unique data VLAN per ADSL port line (user or subscriber). The valid VLAN range for the test bed was 500–1000. For the purpose of testing, a unique user VLAN was configured per user, as shown above. However, in an actual customer deployment, these configurations can be automated by means of a script.

Step 4 Check the ingress rules for the VLANs.

a. Choose **Node > Shelf1 > Slot1 > VLANs**.

b. Click the **Ingress Rule** tab.

c. Confirm that **Admit All VLANs** is shown for each port.

Note If **Admit All VLANs** is not selected, then the STB was unable to get a DHCP address. UTStarcom recommends that Select All VLANs be used, as this is the default.

Step 5 Check the VLAN untag settings.

a. Choose **Node > Shelf1 > Slot1 > VLANs**.

b. Click the **VLAN Untag** tab.

   All port VLAN pairs should be shown. This is because communication over the DSL line is VLAN untagged.

Caution Do not change the default configuration.

Note If VLAN tagging is enabled and an Ericsson HAG is being used with an Amino STB, the video service cannot initiate.

Verifying the Access List Configuration on the DSLAM

Do the following to verify the configuration of access lists on the DSLAM.

Step 1 Click the **Provisioning** tab.

Step 2 Choose **Node > Shelf1 > Slot1 > Access List**.

Step 3 Confirm that all line card DSL ports and PVCs defined for those ports are shown. The Inbound and Outbound Rules column should be blank.

Note No inbound or outbound rules were defined for solution testing.

Configuring QoS for the IPADSL3A Line Cards

Do the following to configure QoS for the IPADSL3A line cards.

Step 1 Configure packet priority.

a. Click the **Provisioning** tab.

b. Choose **Node > Shelf1 > Slot1 > QoS**.

c. Click **Packet Priority** tab.

d. Confirm that all of the Port and PVCs numbers are shown on the left side of the screen, and that the Assigned rule Index field on the right side of the screen is blank.

Step 2 Configure port-based priority.

a. Choose **Node > Shelf1 > Slot1 > QoS**.

b. Click the **Port-Based Priority** tab.

c. Assign priority based on the service. Available priorities are 7–0, with 7 being the highest.

Step 3 Assign a priority to the voice service.

a. Click **1-0-51**. (This number translates to DSL line number 1, voice ADSL port/PVC pair.)

b. Click **Edit**.

c. From the drop-down menu, select priority **7**.

d. Click **OK**.

e. Repeat Step 3a through Step 3d for each voice ADSL port/ PVC pair, making changes as noted below.

Parameter	Setting
2-0-51[1]	Priority 7
3-0-51[2]	

1. DSL line 2 voice/PVC pair.
2. DSL line 3 voice/PVC pair.

Step 4 Assign a priority to the video service.

a. Repeat Step 3a through Step 3d for each video ADSL port/ PVC pair, making changes as noted below.

Parameter	Setting
1-8-59[1]	Priority 4
2-8-59[2]	
3-8-59[3]	

1. DSL line 1 video/PVC pair.
2. DSL line 2 video/PVC pair.
3. DSL line 3 video/PVC pair.

Step 5 Assign a priority to the data service.

a. Repeat Step 3a through Step 3d for each data ADSL port/ PVC pair, making changes as noted below.

Parameter	Setting
1-8-35[1]	Priority 0
2-8-35[2]	
3-8-35[3]	

1. DSL line 1 data/PVC pair.
2. DSL line 2 data/PVC pair.
3. DSL line 3 data/PVC pair.

Step 6 Click the **Configuration** tab and choose **Save** from the drop-down menu.

Step 7 Confirm that 802.1p tags are not regenerated (re-marked).

a. Choose **Node > Shelf1 > Slot1 > QoS**.

b. Click the **802.1p** tab.

c. Confirm that **Regenerate 802.1p Tag for WAN Port** is **Disabled**.

Note The aggregation router connects to the GE trunk ports from the DSLAM, and re-marks the 802.1p values for any data exiting the DSLAM. Therefore, it is not necessary for the DSLAM itself to re-mark 802.1p values.

Saving the Configuration

Do the following to save all configuration changes.

Step 1 Click the **Configuration** tab and choose **Save** from the drop-down menu.