OS Multi-Service Integrated Services Adapter Guide

Software Version: 7750 SR OS 8.0
February 2010
Document Part Number: 93-0262-01-01

Table of Contents

Preface 11

ISA-MS Hardware

ISA-MS Overview 16
Application Assurance Hardware Features 17
AA ISA Host System Support 17
IOM Support for AA ISA 18

Application Assurance

Application Assurance (AA) Overview 20
In-Line Deployment 21
Integration of AA in the Subscriber Edge and VPN PE 22
Fixed Residential Broadband On-Line Access 24
Application-Aware Business VPN Services 26
Multi-Appliance Off-line Content Processing 28
Application Assurance Software Features 30
Application Assurance System Architecture 30
Service Applicability 34
AA ISA Groups and Partitions 35
AA Group Partitions 36
Redundancy 38
ISA Load Balancing 39
Application Identification 41
AA Subscriber Application Service Definition 50
Application Assurance Policers 56
Application QoS Policy (AQP) 59
CLI Batch: Begin, Commit and Abort Commands 62
Per AA Subscriber Service Monitoring and Debugging 63
Statistics and Accounting 64
Cflowd 70
Configuring Application Assurance with CLI 71
Provisioning AA ISA 71
Configuring AA ISA 72
Configuring Watermark Parameters 74
Configuring a Group Policy 75
Beginning and Committing a Policy Configuration 75
Aborting a Policy Configuration 75
Configuring an Application Filter 76
Configuring an Application Group 77
Configuring an Application 78
Configuring an Application Profile 79
Configuring a Policer 80
Configuring an Application QoS Policy 81
Configuring Application Service Options 83
Configuring AA Volume Accounting and Statistics 84

Configuring Cflowd Collector 86
Application Assurance Command Reference 87

IP Security (IPSec)
IPSec Overview 180
Operational Conditions 183
QoS Interactions 184
OAM Interactions 184
Redundancy 184
Statistics Collection 185
Security 185
Remote Access VPN Concentrator Example 186
Video Wholesale Example 187
Configuring IPSec with CLI 189
Provisioning an IPSec ISA 189
Ports Used for IPSec 190
Configuring IPSec ISA 190
Configuring Router Interfaces for IPSec 191
Configuring IPSec Parameters 192
Configuring IPSec in Services 193
IP Security Command Reference 195

Video Services
Video Services 220
Video Groups 220
Video SAP 221
Video Interface 221
Multicast Information Policies 222
Retransmission and Fast Channel Change 224
RET and FCC Overview 224
Retransmission 224
Fast Channel Change (FCC) 225
RET and FCC Server Concurrency 233
Multi-Service ISA Support in the IOM-3 for Video Services 235
Prioritization Mechanism for RET vs. FCC 235
RET Features 236
FCC Features 238
Ad Insertion 239
Local/Zoned Ad Insertion 239
Transport Stream Ad Splicing 239
Ad Zones 242
Local/Zoned ADI Prerequisites and Restrictions 243
Configuring Video Service Components with CLI 245
Video Services Overview 245
Configuring an ISA-MS Module 247
Configuring a Video Group 248
Configuring a Video SAP and Video Interface in a Service 249
Basic Multicast Information Policy Configuration 251
Configuring RET/FCC Video Components with CLI 254

Configuring RET/FCC Video Features in the CLI 255
Configuring the RET Client 255
Configuring the RET Server 259
Configuring the FCC Server 263
Logging and Accounting Collection for Video Statistics 267
Configuring ADI Components with CLI 268
Configuring ADI in CLI 269
Configuring the RET Client 269
Configuring a Video Group 270
Configuring NTP 271
Configuring Channel Parameters 271
Configuring Service Entities 272
Video Command Reference 275
IP-TV Command Hierarchies 276
Show Commands 283
Clear Commands 283
Debug Commands 284
Video Services Commands 285
Generic Commands 285

Network Address Translation
Network Address Translation (NAT) Overview 334
Principles of NAT 334
Application Compatibility 335
Large Scale NAT 336
Layer-2 Aware NAT 337
Port Range Blocks 337
Reserved Ports and Priority Sessions 338
Timeouts 338
L2-Aware NAT 339
Watermarks 339
Configuring NAT 341
ISA Redundancy 341
NAT L2-Aware Configurations 344
Large Scale NAT Configuration 346
NAT Command Reference 349

Appendix A: Common CLI Command Descriptions
Common Service Commands 384

Glossary 387

Index 389

Table of Contents

List of Figures

ISA-MS Hardware

Figure 1: AA ISA on Host IOM 2-20G Example 18

Application Assurance

Figure 2: AA ISA In-Line Module 21
Figure 3: Business VPN Service 22
Figure 4: Application Assurance as DSL Residential Internet Market 25
Figure 5: Integration of AA in a Subscriber Edge 27
Figure 6: AA Filtering for Off-Line Specialized Appliance Processing 29
Figure 7: Application Assurance Functional Components 31
Figure 8: 7750 SR Application Assurance Ingress Datapath 33
Figure 9: Policy Structure 43
Figure 10: Determining the Subscriber Profile, SLA Profile and Application Profile of a Host 51
Figure 11: Configuration Example 52
Figure 12: AQP Definition Example 53
Figure 13: Single ASO Example 54
Figure 14: From-AA-Sub Application-Aware Bandwidth Policing 58
Figure 15: To-AA-Sub Application-Aware Bandwidth Policing 58

IP Security (IPSec)

Figure 16: 7750 IPSec Implementation Architecture 180
Figure 17: IPSec into VPRN Example 186
Figure 18: Video Wholesale Configuration 187

Video Services

Figure 19: RET Server Retransmission of a Missing Frame 224
Figure 20: FCC Client/Server Protocol 226
Figure 21: FCC Bursting Sent Faster Than Nominal Rate 227
Figure 22: FCC Denting Removing Less Important Frames 227
Figure 23: Ad Insertion Model 239
Figure 24: Transport Stream Ad Splicing 240
Figure 25: Splicer Model 240
Figure 26: Transport Stream Flow Example 241
Figure 27: Video Services Configuration Elements 246

Network Address Translation

Figure 28: L2-aware Tree 339

List of Tables

ISA-MS Hardware

Table 1: Application Assurance AA ISA System Support 17
Table 2: MS-ISA Host IOM Support Matrix 17

Application Assurance

Table 3: Traffic Diversion to the ISA 23
Table 4: AA Flows and Sessions 44
Table 5: Policer's Hardware Rate Steps for AA ISA 56
Table 6: Application Assurance Statistics Fields Generated per Record (Accounting File) 66

About This Guide

This guide discusses the video services supported on the Multiservice Integrated Services Adapter (ISA) on the 7750 SR and 7450 ESS. The video services are supported in conjunction with the Multi-Service Integrated Services Adapter (ISA-MS) which is a resource module within the router providing packet buffering and packet processing in support of the Internet Protocol Television (IPTV) video features.

The features covered in this document include:

- Application Assurance, coupled with subscriber and/or VPN access policy control points enables any broadband network to provide application-based services.
- Retransmission (RET) Client and Server — RET is supported for multicast video sent using Real-time Transport Protocol (RTP) where negative acknowledgments (NACKs) from the RTP receiver/client sent using Real-time Transport Control Protocol (RTCP) to a RET server will be responded to by the RET server with the missing RTP sequence numbers. Both a RET server, where the RET client is typically the IP-TV Set Top Box (STB), and a RET client, where the ISA will request any lost packets from an upstream RET server, are supported. RET client and server functionality are supported on the 7- and 12-slot 7750 SR and 7450 ESS chassis.
- Fast Channel Change (FCC) Server — FCC is an Alcatel-Lucent method for providing fast channel changes on multicast IPTV networks distributed over RTP. During a fast channel change, the FCC client initiates a unicast FCC session with the FCC server where the FCC server caches the video stream and sends the channel stream to the FCC client starting at the beginning of a Group of Pictures (GOP) to minimize the visual channel transition on the STB. The FCC unicast stream is sent at an accelerated rate in the time domain until the FCC client catches up with the main multicast stream and joins that RTP stream. FCC server functionality requires the Alcatel-Lucent 5910 Video Services Appliance (VSA) Re-Wrapper to encapsulate and condition the multicast channel streams into RTP, and a compatible FCC client on the STB based on the Alcatel-Lucent FCC/RET Client SDK. FCC server functionality is supported on the 7- and 12-slot 7750 SR and 7450 ESS chassis and can be combined with RET functionality on a single video ISA-MS.
- Local/Zoned Ad Insert (ADI) Splicer — Local/zoned ADI (ADI-LZ) splicing is a feature for Microsoft MediaRoom environments where the router acts as a post A Server transport

stream splicer for ADI. An incoming multicast stream is translated by configuration into multiple source-specific multicast (SSM) streams terminated at the router where each egress SSM stream represents a different “advertising zone”. The splicer inspects the stream for Society of Cable Telecommunications Engineers (SCTE) 35 “cue tones” in the stream and communicates with the ad server using SCTE 30 for instruction on when to insert a local/zoned advertisement which is streamed by the ad server to the splicer. The Alcatel-Lucent ADI splicer can splice into either encrypted or unencrypted transport streams. The spliced ads will always be unencrypted. Local/zoned ADI splicing is supported on the 7- and 12-slot 7750 SR chassis.

- Network Address Translation — The Alcatel-Lucent 7750 SR supports Network Address (and port) Translation (NAPT) to provide continuity of legacy IPv4 services during the migration to native IPv6. By equipping the Multiservice ISA (MS ISA) in an IOM3-XP, the 7750 SR can operate in two different modes, known as:

This document is organized into functional chapters and provides concepts and configuration sections, as well as Command Line Interface (CLI) syntax and command usage.

Audience

This manual is intended for network administrators who are responsible for configuring 7750 SR and 7450 ESS routers. It is assumed that the network administrators have an understanding of networking principles and configurations.

List of Technical Publications

The documentation set is composed of the following books:

- 7750 SR OS Basic System Configuration Guide
  7450 ESS OS Basic System Configuration Guide

  This guide describes basic system configurations and operations.
- 7750 SR OS System Management Guide
  7450 ESS OS System Management Guide

  This guide describes system security and access configurations as well as event logging and accounting logs.
- 7750 SR OS Interface Configuration Guide
  7450 ESS OS Interface Configuration Guide

  This guide describes card, Media Dependent Adapter (MDA), and port provisioning.
- 7750 SR OS Router Configuration Guide
  7450 ESS OS Router Configuration Guide

  This guide describes logical IP routing interfaces and associated attributes such as an IP address, port, link aggregation group (LAG) as well as IP and MAC-based filtering, and VRRP, and Cflowd.
- 7750 SR OS Routing Protocols Guide
  7450 ESS OS Routing Protocols Guide

  This guide provides an overview of routing concepts and provides configuration examples for RIP, OSPF, IS-IS, Multicast (7750-only), BGP (7750-only), and route policies.
- 7750 SR OS MPLS Guide
  7450 ESS OS MPLS Guide

  This guide describes how to configure Multiprotocol Label Switching (MPLS) and Label Distribution Protocol (LDP).
- 7750 SR OS Services Guide
  7450 ESS OS Services Guide

  This guide describes how to configure service parameters such as service distribution points (SDPs), customer information, and user services.
- 7750 SR OS OAM and Diagnostic Guide
  7450 ESS OS OAM and Diagnostic Guide

  This guide describes how to configure features such as service mirroring and Operations, Administration and Management (OAM) tools.
- 7750 SR OS Triple Play Guide
  7450 ESS OS Triple Play Guide

This guide describes Triple Play services and support provided by the 7750 SR and 7450 ESS and presents examples to configure and implement various protocols and services.

- 7750 SR OS Quality of Service Guide
  7450 ESS OS Quality of Service Guide

  This guide describes how to configure Quality of Service (QoS) policy management.

- OS Multi-Service ISA Guide

  This guide describes services provided by integrated service adapters such as Application Assurance, IPSec, ad insertion (ADI) and Network Address Translation (NAT).

Technical Support

If you purchased a service agreement for your router and related products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased an Alcatel-Lucent service agreement, contact your welcome center.

Web: http://www1.alcatel-lucent.com/comps/pages/carrier_support.jhtml

ISA-MS Hardware

In This Section

This section provides an overview of Alcatel-Lucent's implementation of the ISA MS hardware.

Topics include:

- ISA-MS Overview on page 16
- Application Assurance Hardware Features on page 17

ISA-MS Overview

The ISA-MS is a resource module within the router providing packet buffering and packet processing in support of IPTV video features.

ISA-MS fits in an MDA/ISA slot on an IOM and has no external ports, so all communication passes through the IOM, making use of the network processor complex on the carrier IOM for queuing and filtering functions like other MDAs and ISAs.

The actual ingress and egress throughput will vary depending on the buffering and processing demands of a given video application, but the ISA hardware connector can support slightly more than 10 Gbps of throughput ingress and egress.

Application Assurance Hardware Features

AA ISA Host System Support

The 7750 SR Application Assurance Integrated Services Adapter (AA ISA) is a resource adapter, which means that there are no external interface ports on the AA ISA itself. Instead, any other Input Output Modules on a system in which the AA ISA is installed are used to switch traffic internally MS ISA to the AA ISA. Table 1 describes Application Assurance ISA support on 7750 SR and products. Table 2 shows platform, IOM model, and feature matrix.

Table 1: Application Assurance AA ISA System Support

System	AA ISA Supported
7750 SR-12	Yes
7750 SR-7	Yes
7750 SR-c12	No
7750 SR-1	No
7710 SR	No

A key strength of Application Assurance features is the complete integration into the 7750 SR family of products. Common interfaces and operational familiarity reduce the effort to integrate the Application Assurance into existing networks.

Table 2: MS-ISA Host IOM Support Matrix

	7450 ESS: ESS-6, ESS-6v, ESS-7, ESS-12	7750 SR: SR-7, SR-12
Application Assurance	IOM-20G-B, IOM3-XP	IOM-20G-B, IOM2-20G, IOM3-XP
Video: FCC/RET	IOM-20G-B, IOM3-XP	IOM-20G-B, IOM2-20G, IOM3-XP
Video: Ad Insertion	n/a	IOM-20G-B, IOM2-20G, IOM3-XP
NAT	n/a	IOM3-XP

IOM Support for AA ISA

The AA ISA is supported on IOM-20G-B, IOM2-20G and IOM3-XP. Each IOM can support a maximum of two AA ISA modules. To maximize AA ISA redundancy, deployment of AA ISAs on separate host IOMs is recommended as it provides IOM resilience. Traffic from any supported IOM (for example IOM-20G-B, IOM2-20G and IOM3-XP, fixed port IOMs (IMMs)) can be diverted to AA ISA hosted by either an IOM-20G-B, IOM2-20G and IOM3-XP. The AA ISA is field replaceable and supports hot insertion and removal. See Figure 1. A system can support up to 7 active AA ISA cards providing up to 70 G of processing capacity.

AA ISA software upgrades are part of the ISSU functionality. Upgrades to AA ISA software, for example to activate new protocol signatures, do not impact the second MDA slot for the IOM carrying the AA ISA, nor do upgrades impact the router itself (for example. a new AA ISA software image can be downloaded without a need to upgrade other software images).

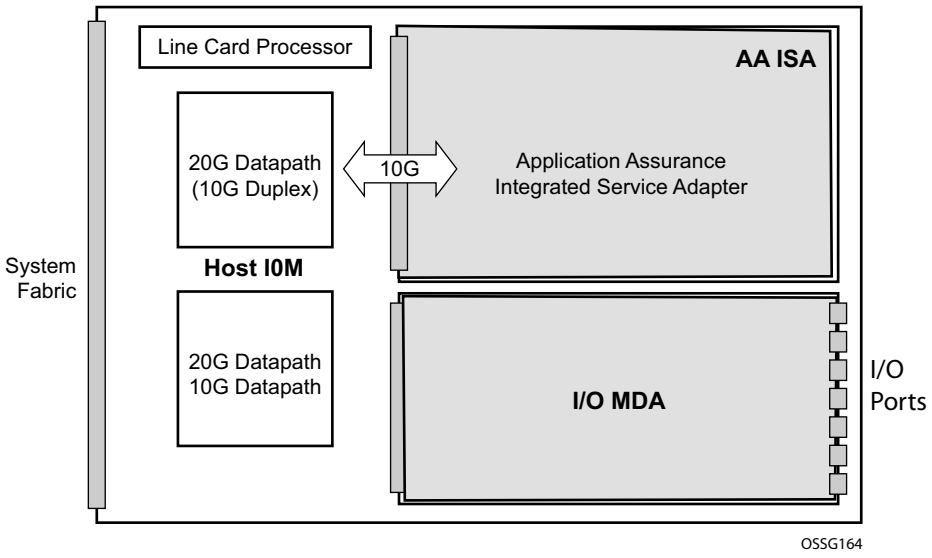

Figure 1: AA ISA on Host IOM 2-20G Example

Application Assurance

In This Section

This section provides an overview of Alcatel-Lucent's implementation of the Application Assurance service model.

Topics include:

- Application Assurance (AA) Overview on page 20
  - → In-Line Deployment on page 21
  - → Multi-Appliance Off-line Content Processing on page 28
  - → Application Assurance Software Features on page 30
  - → Configuring Application Assurance with CLI on page 71
  - → Application Assurance Command Reference on page 87

Application Assurance (AA) Overview

Network operators are transforming broadband network infrastructures to accommodate unified architecture for IPTV, fixed and mobile voice services, business services, and High Speed Internet (HSI), all with a consistent, integrated awareness and policy capability for the applications using these services.

As bandwidth demand grows and application usage shifts, the network must provide consistent application performance that satisfies the end customer requirements for deterministic, managed quality of experience (QoE), according to the business objectives for each service and application. Application Assurance (AA) is the enabling network technology for this evolution in the service router operating system.

Application Assurance, coupled with subscriber and/or VPN access policy control points enables any broadband network to provide application-based services. For service providers, the results unlocks:

- The opportunity for new revenue sources.
- Content control varieties of service.
- Control over network costs incurred by various uses of HSI.
- Complementary security aspects to the existing network security.
- Improved quality of service (QoS) sophistication and granularity of the network.
- The ability to understand and apply policy control on the transactions traversing the network.

In-Line Deployment

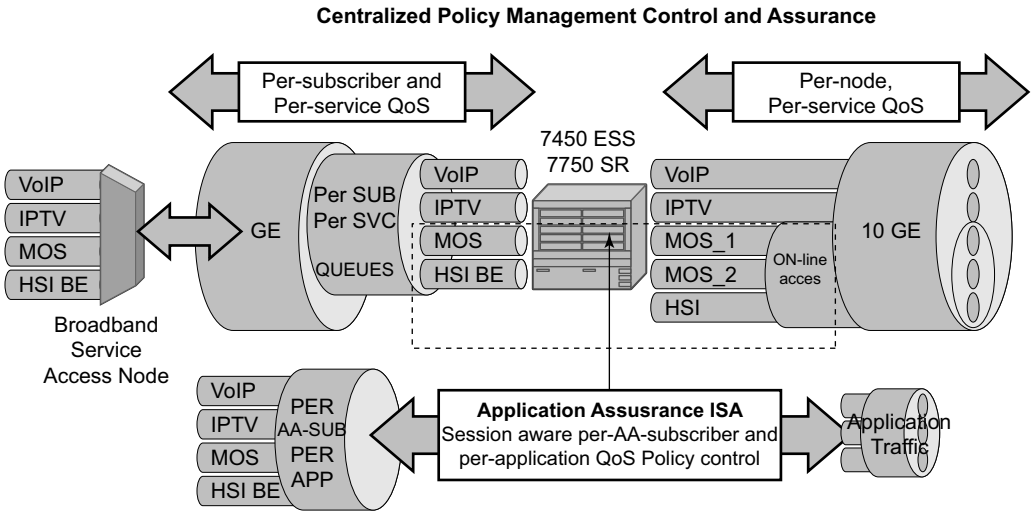

Figure 2: AA ISA In-Line Module

The integrated solution approach for Application Assurance recognizes that a per-AA-subscriber and per-service capable QoS infrastructure is a pre-condition for delivering application-aware QoS capabilities. Enabling per-application QoS in the context of individual subscriber's VPN access points maximizes the ability to monetize the application service, because a direct correlation can be made between customers paying for the service and the performance improvements obtained from it. By using an integrated solution there is no additional cost related to router port consumption, interconnect overhead or resilience to implement in-line application-aware policy enforcement.

Integration of AA in the Subscriber Edge and VPN PE

When a carrier decides that application policy management should form part of subscriber VPN access site management, integrating application assurance in the subscriber edge and VPN PE is the most attractive approach from an operational point of view. It is easier to introduce application assurance field upgrade to the installed base of equipment rather than integrate a whole new set of equipment and vendors into the network for Layer 4-7 awareness.

Integrating Layer 4-7 application policy with the 7750 SR or 7450 ESS is therefore the optimal solution to address markets like the residential broadband access or Layer 2/Layer 3 application aware business VPN. Placement of Layer 4-7 analysis at the distributed subscriber edge simplifies the problem in two significant ways:

- For residential markets, CO-based deployment allows deployment-driven scaling of resources to the amount of bandwidth needed and the amount of subscribers requiring application-aware functionality.
- For AA-aware business VPNs, a network deployment allows large scale application functionality at a VPN access point, vastly reducing complexity, cost, and time to market required to bring application-aware VPN service
- Traffic asymmetry is avoided. Any subscriber traffic usually passes through one CO subscriber edge element so there is no need for flow paths to be recombined for stateful analysis.

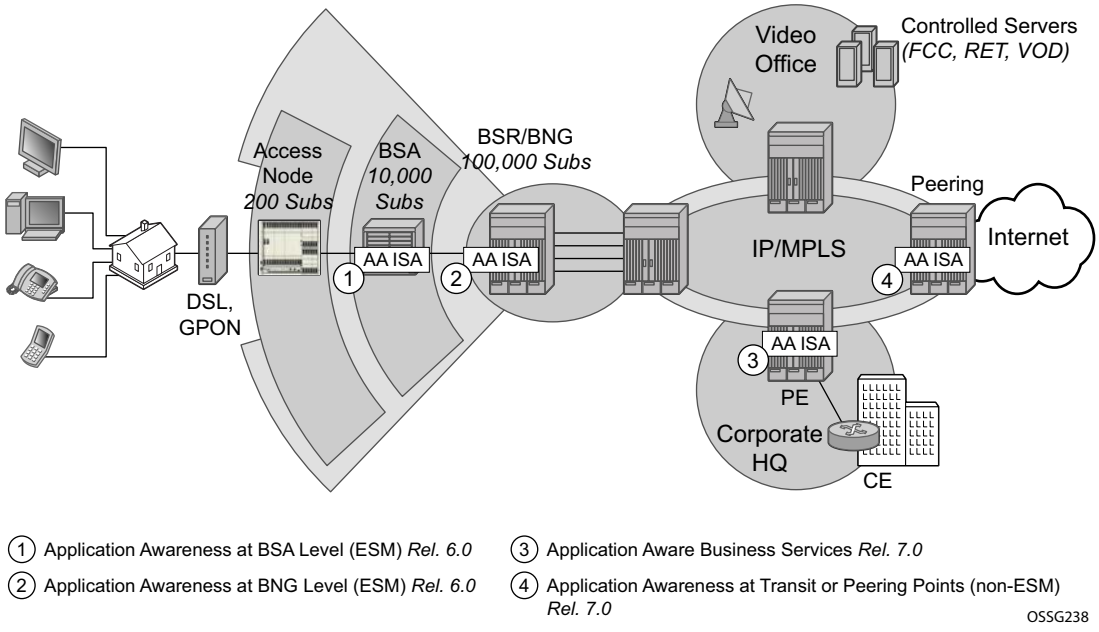

Figure 3: Business VPN Service

Application Assurance enables per AA-subscriber (a residential subscriber, a Layer 2/Layer 3 SAP or spoke SDP), per application policy for all or a subset of AA subscriber's applications. This facilitates the ability to:

- Provide Layer 4-7 identification of applications using a multitude of techniques from a simple port-based/IP address based identification to behavioral techniques used to identify, for example, encrypted applications.
- Once identified, to apply QoS policy on either an aggregate or a per-AA-subscriber, per-application basis.
- Provide reports on both the identification made and policies implemented.

An integrated AA module allows the SR/ESS product families to provide application-aware functions that previously required standalone devices (either in residential or business environment) at a fraction of cost and operational complexity that additional devices in a network required.

Table 3: Traffic Diversion to the ISA

Deployment Case	System Divert ID	AA-Sub Type	App-Profile on:
Residential Edge	ESM Sub-ID	Subscriber (ESM)	Sub (prefix, not hosts)
Business Edge	L2/L3 SAP	SAP	SAP (Aggregate)
Transparent Mode Peering	L2/L3 SAP	SAP	SAP (Aggregate)
Transparent Mode Wire Transit	L2/L3 SAP (any SAPs within a port)	SAP	SAP (Aggregate)
Spoke attached edge	Spoke SDP	Spoke SDP	Spoke SDP (Aggregate)

Fixed Residential Broadband On-Line Access

Fixed residential HSI services as a single edge Broadband Network Gateway (BNG) or as part of the Triple Play Service Delivery Architecture (TPSDA) are a primary focus of Application Assurance performance, subscriber and traffic scale.

To the service provider, application-based service management offers:

- New revenue opportunities to increase ARPU (average revenue per user) (for gaming, peer-to-peer, iVoIP, iVideo, etc.).
- Fairness: Aligns usage of HSI network resources with revenue on a per-subscriber basis.
- OTT IASP eco-system permits competing IASPs to differentiate themselves through delivery of new MOS offerings.

To the C/ASP, service offerings can be differentiated by improving the customer's on-line access experience. The subscriber can benefit from this by gaining a better application experience, while paying only for the value (applications) that they need and want.

Figure 4 shows an example of Application Assurance as deployed within TPSDA, enabling the architectural role of Broadband Service Expansion which complements the BSA and BSR roles. As OTT (over the top inside or complimentary to HSI) services evolve, wider scale deployment for both OTT service control as well as incremental revenue from premium MOS services will expand.

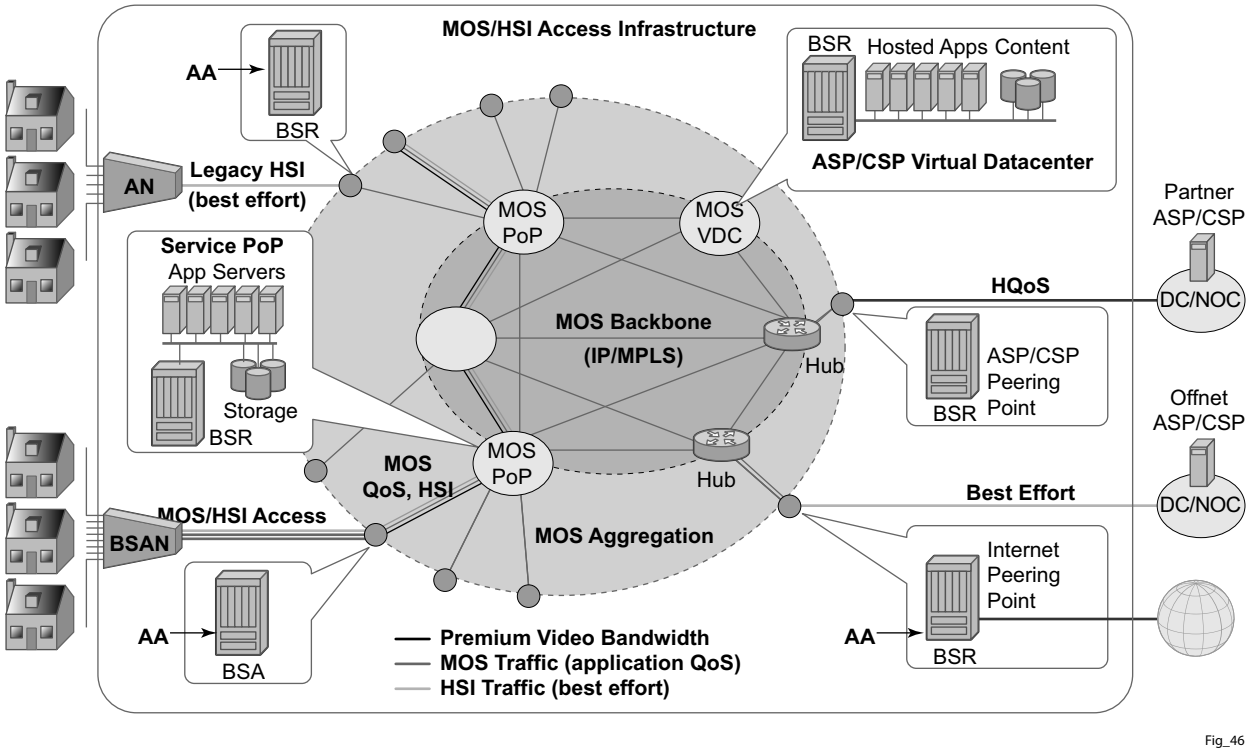

Figure 4: Application Assurance as DSL Residential Internet Market

Application-Aware Business VPN Services

AA for business services can be deployed at the Layer 2 or Layer 3 network provider edge (PE) policy enforcement point for the service or at Layer 2 aggregation policy enforcement point complimentary to the existing Layer 3 IP VPN PE. In a business environment, an AA-subscriber represents a VPN access point. A typical business service can have a much larger average bandwidth rate then the residential service and is likely to have a smaller AA-subscriber count than a residential deployment.

Up to seven active ISAs can be deployed per PE, each incrementally processing up to 10Gbps. The in-network scalability is a key capability that allows a carrier to be able to grow the service bandwidth without AA throughput affecting the network architecture (more edge nodes, application-aware devices).

Application-aware Layer 2 and Layer 3 VPNs implemented using AA ISA equipped 7750 SR/ 7450 ESS together with rich network management (5620 SAM, 5750 RAM, end customer application service portals) give operators a highly scalable, flexible, and cost effective integrated solution for application-based services to end customers. These services may include:

- Rich application reporting with VPN, access site visibility.
- Right-sizing access pipes into a VPN service to improve/ensure application performance.
- Application-level QoS (policing, session admission, remarking, etc.) to ensure application-level performance, end-customer QoE objectives are met.
- Value-added services such as application verification, new application detection, application mirroring.

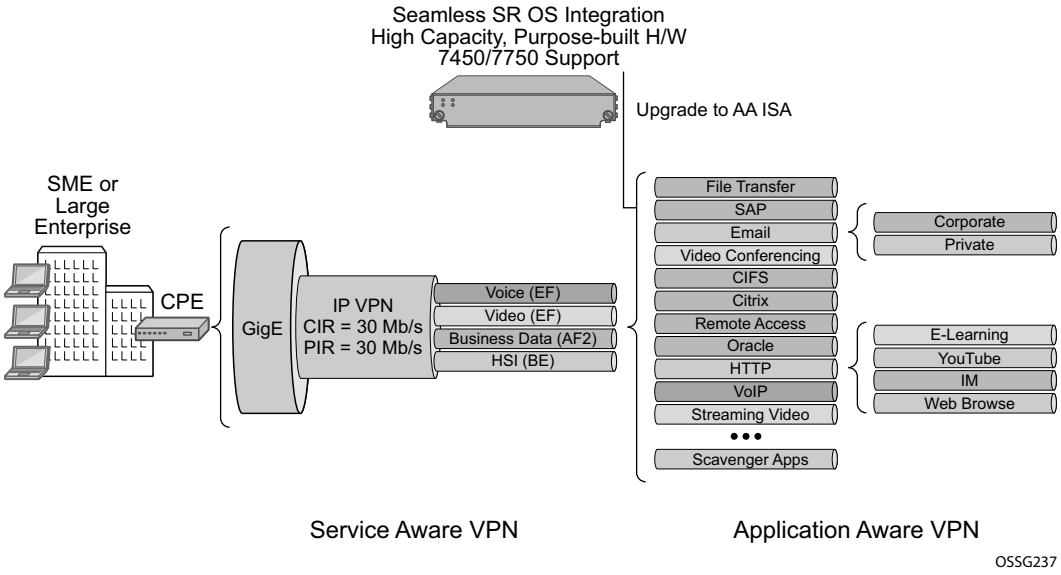

Figure 5: Integration of AA in a Subscriber Edge

Multi-Appliance Off-line Content Processing

Some deployments require specialized off-line processing not provided by 7750 SR AA. An example of such processing is Lawful Intercept (LI) traffic content processing or DRM right violation detection using an off-line appliance. To enable such capabilities in a highly-scalable fashion that minimizes traffic seen by the off-line device, the 7750 SR AA allows operators to use an AQP action to mirror traffic with both application and AA subscriber context, so detail content processing can be performed but only for AA subscribers and applications of choice. The content processing equipment can see the entire traffic stream for a given application. Therefore the entire application's traffic is mirrored including packets that have not yet been identified. Optionally, only traffic positively identified can be mirrored as well.

Although similar functionality could be achieved by mirroring service or a SAP for example, the total bandwidth and added complexity that an off-line appliance would need to handle extra bandwidth makes such a solution more costly and harder to scale.

Since the application mirroring is an additional function atop of all other AA functions provided on the ESS/SR, the in-line deployed AA ISA modules not only reduces the amount of traffic the off-line device must see, but also allows in-line policy enforcement actions with application awareness once the off-line devices triggers such a policy change. For example, AA subscriber traffic for an application or applications being mirrored can be quarantined while the remaining traffic remains unaffected.

Figure 6 depicts an example of application mirroring to a specialized off-line appliance for further processing. The model can be used among others to mirror P2P traffic suspected for DRM violation to specialized equipment detecting such a violation.

1. AA subscriber traffic contains applications requiring specialized off-line appliance processing that requires Layer 2 — Layer 7 application identification.

2 AA ISA with AQP configured:

Match:

→ Application for off-line processing for selected subscribers (downstream only, upstream only, or both).

Action:

→ Mirror source for application's IP packets into a mirror service configured on a router.

3 Specialized appliance sees only the required traffic and performs the desired off-line processing.

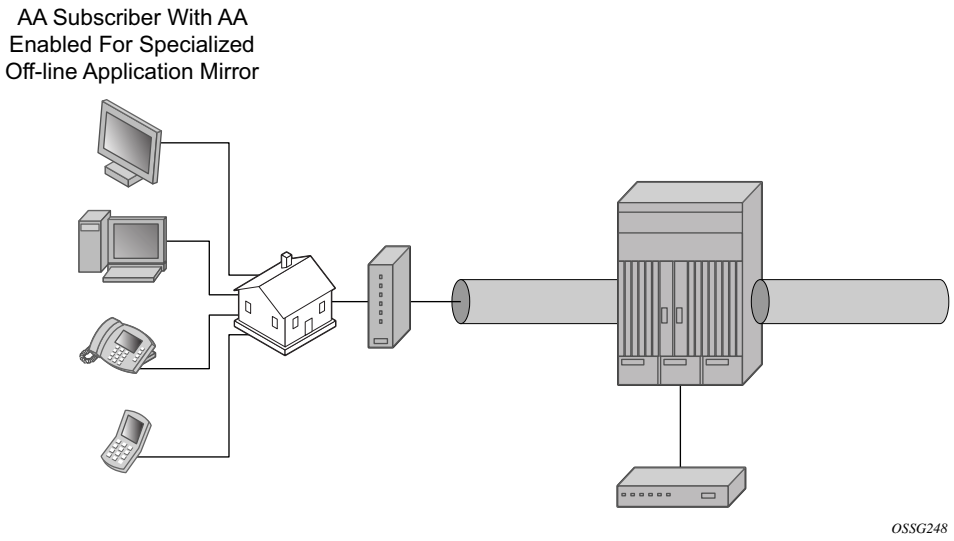

Figure 6: AA Filtering for Off-Line Specialized Appliance Processing

Application Assurance Software Features

- Application Assurance System Architecture on page 30
- Service Applicability on page 34
- AA ISA Groups and Partitions on page 35
- Redundancy on page 38
- Application Identification on page 41
- AA Subscriber Application Service Definition on page 50
  - → Application Profile on page 50
  - → Application Profile Map on page 51
  - → Application Service Options (ASOs) on page 52
- Application Assurance Policers on page 56
- Application QoS Policy (AQP) on page 59
  - → CLI Batch: Begin, Commit and Abort Commands on page 62
- Per AA Subscriber Service Monitoring and Debugging on page 63
  - → AQP Match Criteria on page 60
  - → AQP Actions on page 60
  - → Time of Day Policing Adjustments on page 61
- Statistics and Accounting on page 64
  - → Per-AA-Subscriber Special Study on page 64
  - → System Aspects on page 65
  - → Application Assurance Volume Statistics and Accounting on page 66

Application Assurance System Architecture

Traffic in the 7750 SR is selected to be processed by Application Assurance, which then undergoes packet analysis on the AA ISA. There are two elements of Application Assurance processing:

- Identification of the traffic on a per flow (session) basis.
- Policy treatment of the identified traffic.

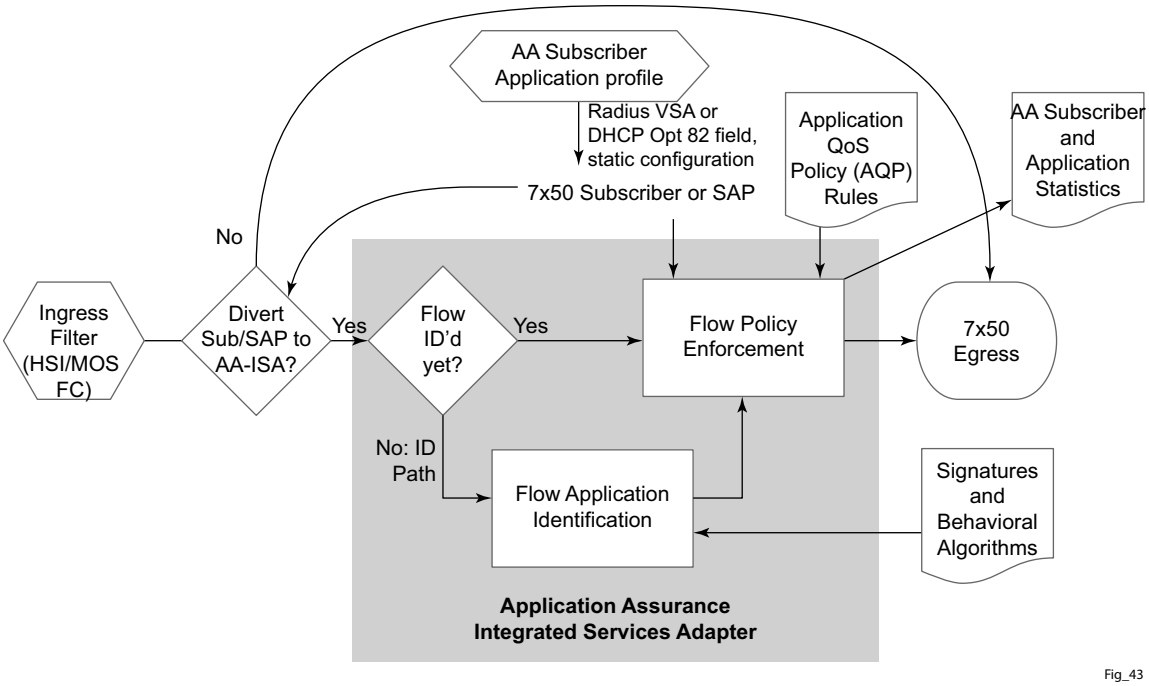

Figure 7: Application Assurance Functional Components

Any traffic can be diverted for application-aware processing. Application Assurance is enabled through the assignment of an application profile as part of either an enhanced subscriber management or static configuration. This process enables the AA functionality for all traffic of interest to and from a given subscriber/SAP/spoke SDP. Which traffic is deemed of interest, is configured through an AA ISA group-specific configuration of forwarding classes (FCs) to be diverted to AA and enabled on a per subscriber/SAP/spoke SDP using application profiles.

Application profiles typically contain one or more characteristics defined as Application Service Options (ASOs). The ASO's characteristics can comprise a menu of customer or/and operator visible network functionality available for AA subscribers, for example, service tier: Bronze, Silver, or Gold, partner's premium content such as real-time live video streaming, or VPN customer or application QoS policy identifier for example: AA QoS template 1, Customer X QoS template 1, etc. This optional inclusion of ASO characteristics, which are then later referenced by the application QoS policy (AQP) rules, allows flexible function-based application service offerings.

AQP defines the application policy rules when actions requiring application-awareness are to be performed against the traffic. Application QoS policy would typically use ASO characteristics assigned to the AA subscriber together with other methods to match flows to actions to be performed. Those methods include, among others, application groups, DSCP values, or server IP address.

AQP rules consist of match and action criteria:

- Match: Refers to application identification determined by application and application group configuration using protocol signatures and user-configurable application filters that allow customers to create a wide range of identifiable applications. To further enhance system-wide per subscriber/service management user configurable application groups are provided.
- Actions: Defines AA actions to be applied to traffic, a set of actions to apply to the flows like bandwidth policing, packet discards, QoS remarking and flow count or/and rate limiting.

Application Assurance System Datapath Overview

Figure 8 shows the general mechanism for filtering traffic of interest and diverting this traffic to the appropriate AA ISA module residing on an IOM (referred as the host IOM). This traffic management divert method applies to both bridged and routed 7750 SR configurations.

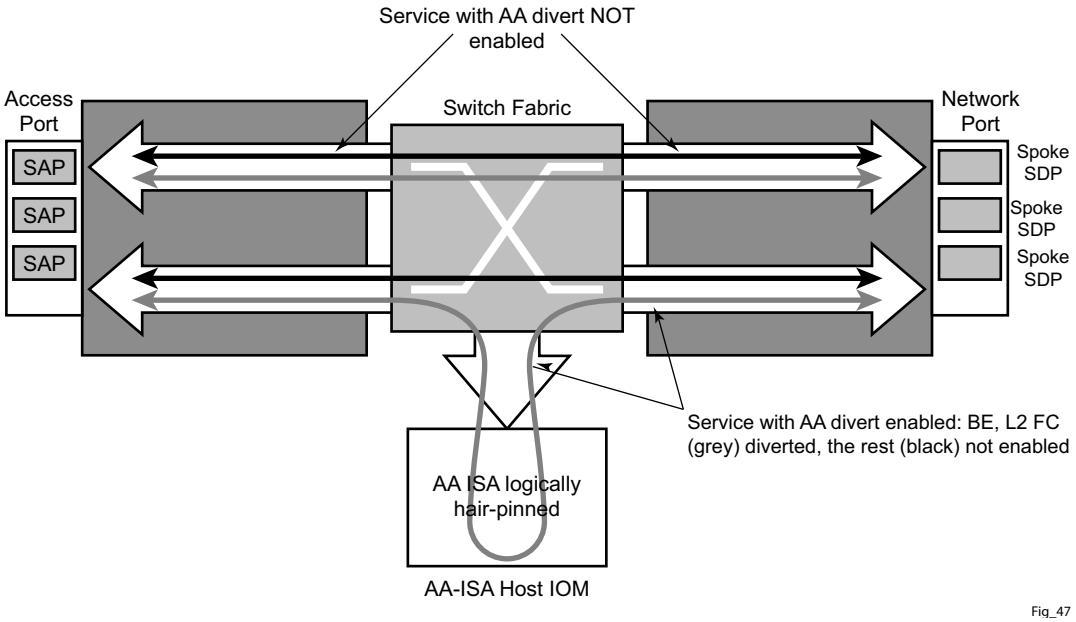

Figure 8: 7750 SR Application Assurance Ingress Datapath

For a SAP, subscribers with application profiles enabling AA, the traffic is diverted to the active AA ISA using ingress QoS policy filters, identifying forwarding and sub-forwarding classes that could be diverted to the Application Assurance. Only single point (SAP, ESM subscriber, spoke SDP) configuration is required to achieve divert for both traffic originated by and destined to a given AA subscriber. Diversion (divert) to the AA ISA is conditional based on the AA ISA status (enabled, failed, bypassed, etc.).

Unless the AA subscriber's application profile is configured as "divert" using Application Profiles and the FC is selected to be diverted as well, the normal ingress forwarding occurs. Traffic that is filtered for divert to AA ISAs is placed in the appropriate location for that system's AA ISA destination.

Users can leverage the extensive QoS capabilities of the router when deciding what IP traffic is diverted to the Application Assurance system for inspection. Through AA ISA group-wide configuration, at least one or more QoS forwarding classes with the "divert" option can be identified. The forwarding classes can be used for any AA subscriber traffic the service provider wants to inspect with Application Assurance.

Service Applicability

The 7750 SR AA ISA provides the Layer 3-7 packet processing used by the Application Assurance feature set. Application Assurance is applied to IPv4 traffic on a per ESM subscriber/ SAP/spoke SDP (AA subscriber) basis (non-IPv4 traffic is not diverted to AA and forwarded as if AA was not configured) where an AA subscriber may be contained in the following services:

- IES
- VPLS
- VLL
- VPRN

Application Assurance is supported with:

- Bridged CO
- Routed CO
- Multi-homed COs
- Layer 2/Layer 3 VPN service access points and spoke SDPs

The AA ISA feature set uses existing 7750 SR QoS capabilities and further enhances them to provide application-aware traffic reporting and management on per individual AA subscriber, AA subscriber-type or group. A few examples of per-application capabilities within the above AA subscriber contexts include:

- Per AA subscriber, application traffic monitoring and reporting.
- Per application bandwidth shaping/policing/prioritization.
- Throttling of flow establishment rate.
- Limiting the number of active flows per application (such as BitTorrent, video or teleconference sessions, etc.).
- Application-level classification to provide higher or lower (including drop) level traffic management in the system (for example, IOM QoS) and network.

The following restrictions are noted:

- Application Assurance is not supported for tunneled transit traffic (using PPP or DHCP) destined for a remote BRAS.
- Residential AA relies on ESM for subscriber context. Therefore any layer 3 edge / aggegation in front of a layer 2 edge (bridged CO) will not be able to use AA, particularly if there is a single MAC for the downstream device.

AA ISA Groups and Partitions

An AA ISA group allows operators to group multiple AA ISAs into a single logical group for consistent management of AA resources and policies across multiple AA ISA cards configured for that group.

Multiple AA ISA Groups

An AA ISA group allows operators to group multiple AA ISAs into one of several logical groups for consistent management of AA resources and policies across multiple AA ISA cards configured for that group. The following operations can be performed at the group level:

- Define one or multiple AA ISA groups to allow AA resource partitioning/reservation for different types of AA service.
- Assign physical AA ISAs to a group.
- Select forwarding classes to be diverted for inspection by the AA subscribers belonging to the group and select the AA policy to be applied to the group.
- Configure redundancy and bypass mode features to protect against equipment failure.
- Configure QoS on IOMs which host AA ISAs for traffic towards AA ISAs and from AA ISAs.
- Configure ISA capacity planning using low and high thresholds.
- Enable partitions of a group.

Residential services is an example where all AA services might be configured as part of a single group encompassing all AA ISAs, for operator-defined AA service. This provides management of common applications and reporting for all subscribers & services, with common or per customer AQP (using ASOs characteristics to divide AA Group’s AQP into per app-profile QoS policies).

Multiple groups can be further used to create separate services based on different sets of common applications, different traffic divert needs (such as for capacity planning) or different redundancy models. Cases where multiple groups might be used can include:

- For mix of residential and business customers.
- Among different business VPN verticals.
- For business services with a common template base but for different levels of redundancy, different FC divert, or scaling over what is supported per single group.

System level status statistics have AA ISA group/partition scope of visibility.

AA Group Partitions

VPN-specific AA services are enabled using operator defined partitions of an AA Group into AA policy partitions, typically with one partition for each VPN-specific AA Service. The partition allows VPN specific custom protocols/application/application group definition, VPN specific policy definition and VPN specific reporting (e.g. some VPNs with Volume only reports, while others with Volume and Performance reports). Each partition's policy can be again divided into multiple application QoS policies using ASOs.

Use of ISA Groups and partitions also improves scaling of policies, as needed with VPN-specific AA policies.

If partitions are not defined, all of the AA Group acts as a single partition. When partitions are configured, application identification, policy and statistics configuration applies only to the given partition and not any other partitions configured under the same AA Group.

Definition of Application profiles (and related ASO characteristics/values) are within the context of a given partition (however, App profiles names must have node-wide uniqueness)

Definition of applications, application groups and AQP are also specific to a given partition. This allows:

- Definition of unique applications and app-groups per partition.
- Definition of AQP policy per partition.
- Definition of common applications and app-groups per partition with per partition processing and accounting.

Partitions also enable accounting/reporting customization for every AA subscriber associated with a partition, for example:

- Ability to define different types of reporting/accounting policies for different partitions in a single AA group, such as uniquely define which application, protocols, app groups are being reported on for every AA subscriber that uses a given partition.
- AA group level protocol statistics with partition visibility (for example, protocol counts reported for each partition of the group separately).

The system provides independent editing and committing of each partition config (separate begin/commit/abort).

Policer templates allow group-wide policing, and can be referenced by partition policies.

Bypass Modes

If no active AA ISA is available (for example, due to an operational failure, misconfiguration) the default behavior is to forward traffic as if no AA was configured, the system does not send traffic to the AA ISA (equivalent to fail to closed). Alarms are raised to flag this state externally. There is an optional “fail to open” feature where AA ISA service traffic is dropped if no active AA ISA is present (such as no AA ISA is present and operationally up).

Redundancy

AA ISA group redundancy is supported, to protect against card failure and to minimize service interruption during maintenance or protocol signature upgrades.

No AA ISA Group Redundancy

AA can be configured with no ISA redundancy within the AA group. All AA ISAs are configured as primary with no backup (up to the limit of active AA ISAs per node). There is no fault state indicating that a spare AA ISA is missing. If a primary is configured but not active, there will be a "**no aa-isa**" fault.

N+1 AA ISA Card Warm Redundancy

The system supports N+1 AA ISA equipment warm redundancy (N primary and 1 backup). If a backup is configured and there is no ISA available (a primary and backup failed), there will be a "**no aa-isa**" fault. The backup AA ISA is pre-configured with isa-aa.tim and the group policies. Datapath traffic is only sent to active AA ISAs, so the backup has no flow state. If a backup ISA is unavailable, there will be a "backup missing" fault.

An AA subscriber is created and assigned to a primary AA ISA when an application profile is assigned to a subscriber, SAP, or spoke SDP. By default, AA subscribers are balanced across all configured primary AA ISAs.

Upon failure of a primary AA ISA, all of its AA subscribers and their traffic are operationally moved to the newly active backup AA ISA but the current flow states are lost (warm redundancy). The new AA ISA will identify any session-based active flows at a time of switchover as an **existing** protocol, while the other flows will be re-identified. The **existing** protocol-based application filters can be defined to ensure service hot redundancy for a subset of applications. Once the backup AA ISA has taken control, it will wait for operator control to revert activity to the failed primary AA ISA module.

The user can disable a primary AA ISA for maintenance by triggering a controlled AA ISA activity switch to do the AA ISA software field upgrade (a shutdown of an active AA ISA is recommended to trigger an activity switch).

The activity switch experiences the following AA service impact:

- All flow states for the primary ISA are lost, but existing flows can be handled with special AQP rules for the existing flows by the newly active backup AA ISA until sessions end.

- All statistics gathered on the active AA ISA since the last interval information that was sent to the CPM will be lost.

ISA Load Balancing

Capacity-cost based load balancing allows a cost to be assigned to diverted AA subscribers (by the app-profile). Load Balancing uses the total allocated costs on a per-ISA basis to assign the subscriber to the lowest sum cost ISA resource. Each ISA supports a threshold os the summed cost value that notifies the operator if or when capacity planning has been exceeded.

The load balancing decision is made based on the AA capacity cost of an AA subscriber. The capacity cost is configured against the app-profile. When assigning a new diverted aa-sub to an ISA, the ISA with the lowest summed cost (that also has sufficient resources) is chosen. Examples of different load-balancing approaches that may be implemented using this flexible model include:

- aa-sub count balancing — Configure the capacity cost for each app-profile to the same number (for example, 1).
- aa-sub stats resource balancing — Configure the capacity cost to the number of stats collected for AA subscribers using the app-profile. This might be used if different partitions have significantly different stats requirements.
- Bandwidth balancing — Configure the capacity cost to the total bandwidth in both directions (in kbps) expected for those AA subscribers. This might be used if different AA subscribers have highly varying bandwidth needs.

Load Balancing operates across ISAs withuin an AA Group, and will not balance across groups. The system will ensure that app-profiles assigned to AA subscribers (ESM subscribers, SAPs and spoke-sdps) that are within a single VPLS/Epipe/IES/VPRN service are all part of the same AA group (partitions within an AA group are not checked/ relevant).

Users can replace the app-profile assigned to an AA subscriber with another app-profile (from the same group/partition) that has a different capacity cost.

Regardless of the preferred choice of ISA, the system takes into account:

- Per previous releases, resource counts have per-ISA limits. If exceeded on the ISA of choice, that ISA cannot be used and the next best is chosen.
- Divert IOM service queuing resources may limit load-balancing. If queuing resources are exhausted, the system attempts to assign the aa-sub to the ISA where the first AA subscriber within that service (VPLS/Epipe) or service type (IES/VPRN) was allocated.

Capacity cost resource counting does not have a hard per-ISA limit, since the cost values are decoupled from actual ISA resources. However, the value of the total summed cost per-ISA can be reported, and a threshold value can be set which will raise an event when exceeded.

ISA overload (if actually overbooked to the level of congestion) will be seen using existing AA ISA congestion/backpressure stats.

While an app-profile is assigned to AA subscribers, the capacity-cost for that app-profile can be modified. The system makes updates in terms of the load balancing summary, but this does not trigger a re-balance.

In the absence of user configuration, the App-profile default capacity cost is 1. The range for capacity cost is 1 — 65535 (for example, for bandwidth based balancing the value 100 could represent 100kbps). Note that 0 is an invalid value.

Application Identification

Application identification means there is sufficient flow information to provide the network operator with a view to the underlying nature and value of the content. Application ID does not include:

- Anti-virus signatures per IPS/UTM.
- Content inspection (e-mail, text, picture, or video images). The payload data content of flows is typically not examined as part of the application identification.

Application Assurance can identify and measure non-encrypted IP traffic flows using any available information from Layer 2-Layer 7, and encrypted IP traffic flows using heuristic techniques.

Application Assurance attempts to positively identify the protocols and applications for flows based on a pattern signature observation of the setup and initial packets in a flow. The system correlates control and data flows belonging to the same application. In parallel, statistical and behavioral techniques are also used to identify the application. Until identified, the flow will not have a known application and will be treated according to the default policies (AQP policies defined using all or any ASO characteristics, subscriber Id and traffic direction as match criteria) for traffic for that AA subscriber, app-profile and direction (packets will be forwarded unless an action is configured otherwise). If the identification beyond OSI Layer 2is not successful, the flow will be flagged as an unknown protocol type, (for example unknown_tcp or unknown_udp). The unknown traffic is handled as part of all application statistics and policy, including generation of stats on the volume of unknown traffic.

Application Assurance allows operators to optionally define port-based applications for “trusted” TCP or UDP ports. Operators must explicitly identify a TCP/UDP port(s) in an application filter used for “trusted” port application definition and specify whether a protocol signature-based application identification is to be performed on a flow or not. Two options are available:

- If no protocol signature processing is required (expected to be used only when (A) AQP policy must be performed from the first packet seen, (B) the protocol signature processing requires more than 1 packet to positively identify a protocol/application, and (C) no other application traffic runs over a given TCP/UDP port), the first packet seen by AA ISA for a given flow on that TCP/UDP port will allow application identification. The traffic for a given flow will be identified as “trusted tcp/trusted_udp” protocols.
- If protocol signature verification of an application is required (expected to be used only when (a) AQP policy must be performed from the first packet seen, (b) the protocol signature processing requires more than 1 packet to positively identify a protocol/application, but (c) other application traffic may run over a given TCP/UDP port, for example TCP port 80), the first packet seen will identify the application but protocol signature-based analysis continues. Once the identification completes, the application is

re-evaluated against the remaining application filters allowing detection and policy control of unexpected applications on a “trusted” port.

At Application Assurance system startup or after an AA ISA activity switch, all open flows are marked with the “existing” protocol signature and have a policy applied according to an application based on the “existing” protocol until they end or the identification of an in-progress flow is possible. Statistics are generated.

From the first packet of a flow, a default per AA subscriber AQP policy is applied to every packet. Once an application is identified, subsequent packets for a flow will have AA subscriber and application-specific AQP applied. The AA-generated statistics for the flow with AA subscriber and application context are collected based on the final determination of the flow's application. A subset of the applications may be monitored on an ongoing basis to further refine the identification of applications carried with the traffic flow and to identify applications using an external application wrapper to evade detection.

Application Assurance Identification Components

Figure 9 shows the relationship between the Application Assurance system components used to identify applications and configure Application Assurance related capabilities. Each ID-related component is defined as follows:

- Protocol signatures
- Application filters
- Applications
- Application groups

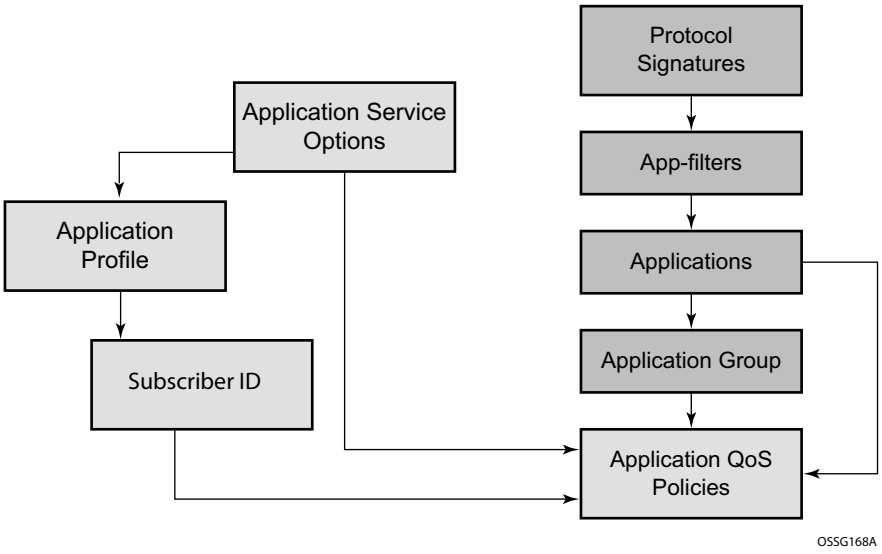

Figure 9: Policy Structure

Table 4 provides an overview of how those various components used in Application Assurance to recognize types of flows/sessions.

Table 4: AA Flows and Sessions

Term	Definition	Examples
Protocol Signature	Alcatel-Lucent's proprietary component of AA flow identification provided as part of AA S/W load to identify protocols used by clients. Where a protocol is defined as an agreed upon format for transmitting data between two devices.	Tftp, iMap, msn-msgr, RTP, emule, http_video, bittorrent, SIP **Note**: Alcatel-Lucent's protocol signatures do not rely on IP port numbers to identify a TCP/UDP port based protocols / applications in order to avoid eliminate false-positives but allow operators to define application filters if a port-based identification is deemed adequate (see an example below).
Application Filter	Operator configurable, optional component of AA flow identification that uses any combination of protocol signatures, server IP address and port, flow set-up direction, configurable expressions (for example an HTTP string match) to identify user's traffic.	http_video + IP address of partner's video server or http_video + an HTTP string to identify partner's video content TCP or UDP + TCP/UDP port number to identify a TCP or UDP based protocol or application.
Application	Operator configurable, optional component of AA flow identification that allows defining any specific forms of traffic to and from end user clients by combining application filter entries	Google Talk, POP3, YouTube, iTunes, Shoutcast
Application Group	Operator configurable, optional component of AA flow identification that allows grouping of similar end use applications using operator defined names and groups.	IM, Mail, Multimedia, P2P, Tunneling, Web, Other
Clients	End user programs that generate user traffic for applications and protocols, and that are used in a process of AA flow identification verification.	The list of clients is constantly evolving as new clients or versions are introduced in the marketplace. The following example illustrates clients that may be used to generate Application traffic matching BitTorrent application defined using BitTorrent and DHT protocol signatures: Limewire, BitTorrent, Azureus, Ktorrent, Transmission, Utorrent

Protocol Signatures

The set of signatures used to identify protocols is generated by Alcatel-Lucent and included with the Application Assurance software load. The signature set includes:

- The protocols that can be identified with this load, using a combination of pattern and behavioral techniques. The protocols are used in generating statistics by protocol, and are used as input in combination with other information to identify applications.
- Pattern signatures are the set of pattern-match signatures used in analysis.
- Behavior signatures are the set of diagnostic techniques used in analysis.

Dynamic upgrades of the signatures in the system are implemented by invoking an **admin application-assurance upgrade** command and then performing AA ISA activity switches.

The protocol signatures are included in aa-isa.tim software load which is not tightly coupled with software releases allowing for protocol signature updates without upgrading and impacting of routing/forwarding engines as part of an ISSU upgrade that updates only the AA ISA software. Refer to upgrade procedures described in the 7750 SR and/or 7450 ESS Release Notes for detailed information.

Since protocol signatures are intended to be the most basic block of Application Identification, other AA components like Application Filters are provided to further customize Protocol Signatures allowing operators to customize their applications and to reduce a need for a new Protocol Signature load when a new Application may need to be identified. This architecture gives operators more flexibility in responding to ever changing needs in application identifications.

Signature upgrade without a router upgrade is allowed within a major router release independently of system ISSU limits. An AA ISA signature upgrade is supported before the first ISSU router release (for example, operators can upgrade signatures for pre-ISSU minor releases).

In addition, any router release from ISSU introduction release can run any newer aa-isa.tim image within the same major release by performing an aa-isa.tim single step upgrade. For example, release 8.4 may be upgraded in a single step to run release 8.14 of isa-aa.tim.

Each protocol, except internal protocols used for special-case processing statistic gathering (like “cut-though”, for example), can be referenced in the definition of one or multiple applications (through the App-Filter definition). Assignment of a supported protocol to an app-filter or application is not mandatory. Protocols not assigned to an application are automatically mapped by the system to the default “Unknown” application.

Custom Protocols

Custom protocols are supported using configurable strings (up to 16 hex octets) for pattern-matched application identification in the payload of TCP or UDP based applications (mutually exclusive to other string matches in an app-filter).

The match is specified for the “client-to-server”, “server-to-client”, or “any” direction for TCP based applications, and in the “any” direction for UDP based applications.

There is a configurable description and custom protocol id for a protocol, with configurable shutdown. When disabled, traffic is identified as if the protocol was not configured.

Custom protocols and ALU-provided protocols are functionally equivalent. Custom protocols are used in application definition without limitations (all app-filter entries except strings are supported). Collection of custom protocol statistics on a partition/ISA group/special study sub level is supported.

Protocol Shutdown

The protocol **shutdown** feature provides the ability for signature upgrades without automatically affecting policy behavior, especially if some or even all new signatures are not required for a service. All new signatures are disabled on upgrade by default to ensure no policy/service impact because of the signature update.

All protocols introduced at the R1 stage of a given release are designated as “Parent” signatures for a given release and cannot be disabled.

Within a major release, all protocols introduced post-R1 of a major release as part of any isa-aa.tim ISSU upgrade are by default **shutdown**. They must be enabled on a per-protocol basis (system-wide) to take effect.

When shutdown, post R1-introduced protocols do not change AA behavior (app-id, policy, statistics are as before the protocol introduction), for example, traffic maps to the parent protocol on which the new signature is based. In cases where there is more than one parent protocol, all traffic is mapped to a single, most-likely, parent protocol. For example if 80% of a new protocol has traffic mapping to unknown_tcp, and 20% mapping to another protocol(s), unknown_tcp would be used as parent.

Enabling/disabling of a new protocol takes affect for new flows only. The current status (enabled/shutdown) of a signature and the parent protocol is visible to an operator as part of retrieving protocol information through CLI/SNMP.

Supported Protocol Signatures

Protocol signatures are release independent and can be upgraded independently from the router's software and without impacting router's operations as part of an ISSU upgrade. A separate document outlines signatures supported for each signature software load (isa-aa.tim). New signature loads are distributed as part of the SR/ESS maintenance cycle. Traffic identified by new signatures will be mapped to an "Unknown" application until the AA policy configuration changes to make use of the newly introduced protocol signatures.

Application Groups

Application groups are defined as a container for multiple applications. The only application group created by default is **Unknown**. Any applications not assigned to a group are automatically assigned to the default **Unknown** group. Application groups are expected to be defined when a common policy on a set of applications is expected, yet per each application visibility in accounting is required. The application group name is a key match criteria within application QoS policy rules.

Applications

The application context defines and assigns a description to the application names supported by the application filter entries, and assigns applications to application groups.

- Application name is a key match criteria within application QoS policy rules, which are applied to a subscribers IP traffic.
- Each application can be associated with one of the application groups provided by Application Assurance.

The Application Assurance system provides no pre-defined applications other than **Unknown**. Applications must be explicitely configured. Any protocols not assigned to an application are automatically assigned to the default **Unknown** application.

The applications are used by Application Assurance to identify the type of IP traffic within the subscriber traffic.

The network operator can:

- Define unique applications.
- Associate applications with an application group. The application group must already be configured.

Application Filters

Application filters (app-filter) are provided as an indirection between protocols and applications to allow the addition of variable parameters (port number, IP addresses, etc.) into an application definition. An application filter is a numbered rule entry that defines the use of protocol signatures and other criteria to define an application. Multiple rules can be used to define what constitutes an application but each rule will map to only one application definition.

The system concept of application filters is analogous to IP filters. Match of a flow to multiple rules is possible and is resolved by picking the rule with the lowest entry number that matches. A flow will only ever be assigned to one application.

The following criteria can be assigned to an application filter rule entry:

- Unique entry ID number
- Application name
- Flow setup direction
- Server IP address
- Server port
- Protocol signature
- IP protocol number
- String matches against Layer 5+ protocol header fields (for example, a string expression against HTTP header fields)

The application must be pre-configured prior to using it in an app-filter. Once defined, the new application names can be referenced.

AA Subscriber Application Service Definition

- Application Profile on page 50
- Application Profile Map on page 51
- Application Service Options (ASOs) on page 52

Application Profile

Application profiles enable application assurance service for a given ESM subscriber, Service Access Point or spoke SDP (AA subscriber). Each application profile is unique in the system and defines the AA service that the AA subscriber will receive. An ESM subscriber can be assigned to an application profile which affects every host of the particular subscriber. For SAP or spoke SDP AA subscribers, an application profile can be assigned which affects all traffic originated/destined over that SAP or spoke SDP. By default, ESM subscribers, SAPs or spoke SDPs are not assigned an application profile.

The following are main properties of application profiles:

- One or more application profiles can be configured in the system.
- Application profiles specify whether or not AA subscriber's traffic is to be diverted to Application Assurance.
- Application profiles are defined by an operator can reference the configured application service options (ASO) characteristics (see Application Service Options (ASOs) on page 52.
- Application profiles must only be assigned once AA resources (AA ISA cards) are configured.
- App-profiles can be assigned a capacity cost used for subscriber load balancing among ISAs within the AA group. (See ISA Load Balancing on page 39.)

ESM includes an application profile string. The string points to an application profile pre-provisioned within the router and is derived by:

- Parsing the DHCP Option 82 sub-option 1 circuit ID payload, vendor specific sub-option 9, or customer-defined option different from option 82, during authentication and the DHCPDISCOVER, as well as re-authentication and the subscriber’s DHCPREQUEST.
- RADIUS using a new VSA. [26-6527-xx] alc-application-profile-string
- Inherited by defaults in the **sap>sub-sla-mgmt** context, to allow default application profile assignment if no application profile was provided.
- Static configuration.

Mid-session (PPP/DHCP) changes to the application profile string allows:

- Modification of the application profile a subscriber is mapped to and pushes the change into the network as opposed to waiting for the subscriber to re-authenticate to the network.
- Change to the subscribers application profile inline, without a need for the subscriber to re-authenticate to RADIUS or perform any DHCP message exchange (renew or discover) to modify their IP information.

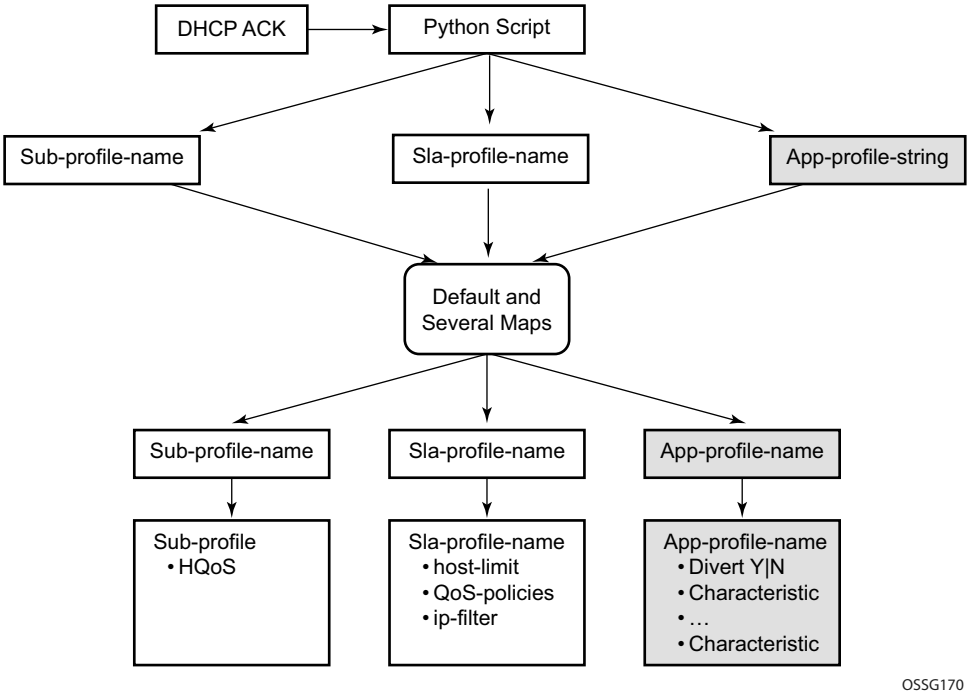

Figure 10: Determining the Subscriber Profile, SLA Profile and Application Profile of a Host

Application Profile Map

Application Assurance adds new map (app-profile-map) application profile command to associate an *app-profile-string* from dynamic subscriber management to a specific application profile using its app-profile-name that has been pre-provisioned. The application profile map is configured in the **config>subscr-mgmt>sub-ident-pol** context.

The pre-defined subscriber identification policy has to be assigned to a SAP, which determines the sub-id, sub, sla, and app-profiles.

Application Service Options (ASOs)

ASOs are used to define service provider and/or customer visible network control (policy) that is common between sets of AA subscribers (for example, upstream/downstream bandwidth for a tier of AA service). ASO definition decouples every AA subscriber from needing subscriber-specific entries in the AQP for standard network services.

As an example, an operator can define an ASO called “ServiceTier” to define various HSI services (Super, Lite, etc.) (Figure 11-A). The operator can then reference these defined ASOs when creating the App Profiles that are assigned to AA-subscribers (Figure 11-B).

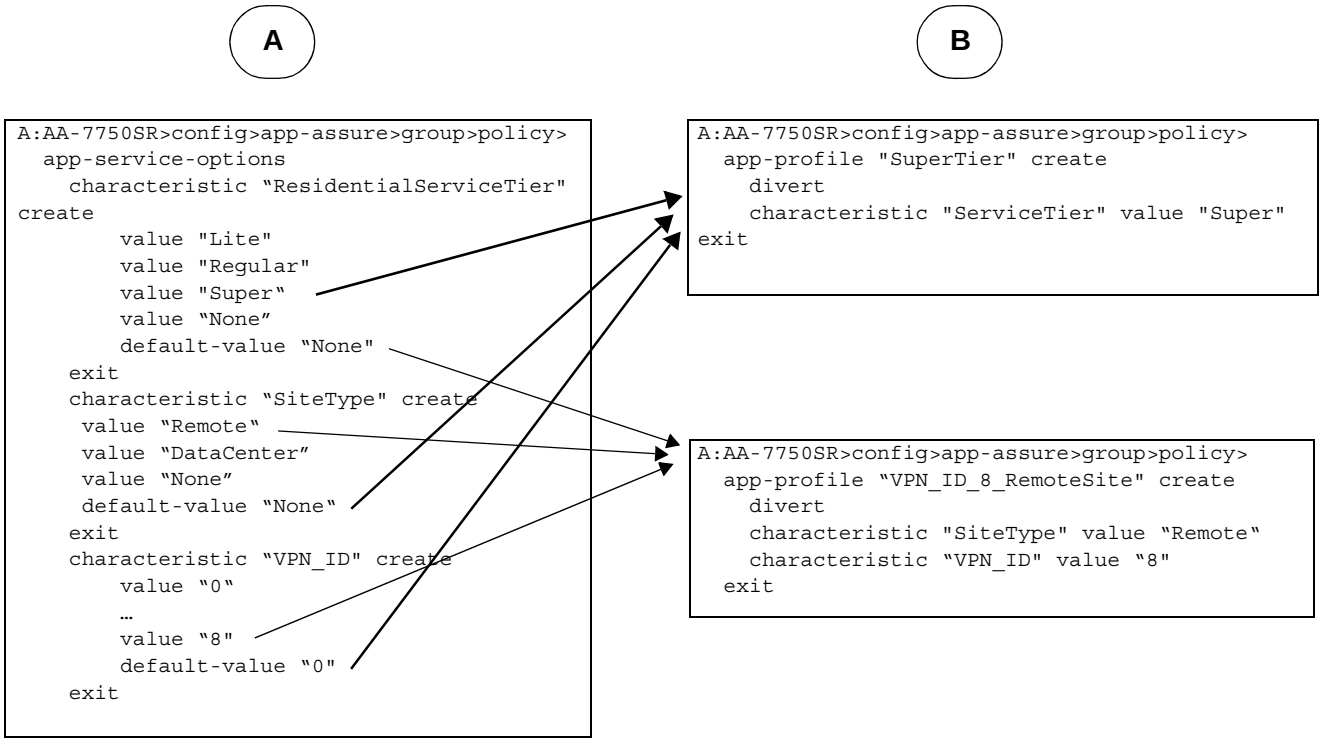

Figure 11: Configuration Example

Then, the defined ASOs are used in the AQP definition to determine the desired treatment / policy (Figure 12).

```
app-qos-policy
    entry 50 create
        description "Limit downstream b/w for Super sub-
scribers"
        match
            traffic-direction network-to-subscriber
            characteristic "ServiceTier" eq "Super"
        exit
        action
            bandwidth-policer "SuperDown"
        exit
        no shutdown
    exit
    entry 110 create
        match
            application-group eq "Tunneling"
            characteristic "SiteType" eq "Remote"
        exit
        action
            remark fc af
        exit
        no shutdown
    exit
```

Figure 12: AQP Definition Example

Alternatively, if ASOs were not used in the previous example, then the operator would have to define a unique AQP entry for every subscriber. Each of these AQPs will have its “match” criteria setup to point to the subscriber ID, while the action for all of these unique AQPs will be the same for the same service (for Tier 1 service, the policer bandwidth will be the same for all Tier 1 AA subscribers) (Figure 13).

```
7750SR>config>aa>group>policy>aqp>
  entry 100 create
    match
      aa-sub eq " sub_1"
    exit
    action
      bandwidth-policer "superDown"
    exit
    no shutdown
  exit

  entry 101 create
    match
      aa-sub eq " sub_2"
    exit
    action
      bandwidth-policer "superDown"
    exit
    no shutdown
  exit

  entry 102 create
    match
      aa-sub eq " sub_3"
    exit
    action
      bandwidth-policer "superDown"
    exit
    no shutdown
```

Figure 13: Single ASO Example

The example in Figure 13, shows how the use of just a single ASO can save the user from having to provision an AQP entry every time a subscriber is created.

Other example uses of ASO entries include:

- Entry per application group that is to be managed, such as VoIP, P2P, HTTP.
- Several entries where specific applications within an application group can individually be managed as service parameters, for example, HTTP content from a specific content provider, or streaming video from network television or games.
- HSI tiers (for example, Gold, Silver, and Bronze for specifying bandwidth levels).
- VPN customer ID.

Application characteristics are defined as specific to the services offered within the operator? network. The operator defines ASO characteristics and assigns to each ASO one or more values to define service offering to the customers.

The following are the main elements of an ASO:

- A unique name is applied to each characteristic.
- The name is unique to the group-partition-policy, but the expectation is that characteristics will be consistent network wide.
- Operator-defined values (variables) are defined for each characteristic and are unique to each characteristic. A default value must be specified from the set of the values configured.

The following lists how ASO characteristics are used:

- Application service options are used as input to application profiles.
- AQP rule sets also use the ASO characteristics to influence how specific traffic is inspected and policies applied.
- Multiple ASO characteristic values are allowed in a single rule.

Syntax checking is performed when defining application profiles and AQPs that include application characteristics. This ensures:

- The characteristic is correctly identified.
- In an app-profile and app-qos-policy when specifying a characteristic, the value must be specified. The “default-value” applies if a characteristic is not specified within an app-profile.

Application Assurance Policers

The rate limit (policer) policy actions provide the flow control mechanisms that enable rate limiting by application and/or AA subscriber(s).

There are four types of policers:

- Flow rate policer monitors a flow setup rate.
- Flow count limits control the number of concurrent active flows
- Single-rate bandwidth policers monitor bandwidth using a single rate and burst size parameters.
- Dual-rate bandwidth rate policers monitor bandwidth using CIR/PIR and CBS/MBS. These can only be used at the per-subscriber granularity.

  Once a policer is referred to by an AQP action for one traffic direction, the same policer cannot be referred to in the other direction. This also implies that AQP rules with policer actions must specify a traffic direction other than the “both” direction.

Table 5 illustrates a policer's hardware rate steps for AA ISA:

Table 5: Policer's Hardware Rate Steps for AA ISA

Hardware Rate Steps	Rate Range (Rate Step x 0 to Rate Step x 127 and max)
0.5Gb/sec	0 to 64Gb/sec
100Mb/sec	0 to 12.7Gb/sec
50Mb/sec	0 to 6.4Gb/sec
10Mb/sec	0 to 1.3Gb/sec
5Mb/sec	0 to 635Mb/sec
1Mb/sec	0 to 127Mb/sec
500Kb/sec	0 to 64Mb/sec
100Kb/sec	0 to 12.7Mb/sec
50Kb/sec	0 to 6.4Mb/sec
10Kb/sec	0 to 1.2Mb/sec
8Kb/sec	0 to 1Mb/sec
1Kb/sec	0 to 127Kb/sec

Policers are unidirectional and are named with these attributes:

- Policer name
- Policer type: single or dual bucket bandwidth, flow rate limit, flow count limit.
- Granularity: select per-subscriber or system-wide
- Parameters for flow setup rate (flows per second rate)
- Parameters for flow count (maximum number of flows)
- Rate parameters for single-rate bandwidth policer (PIR)
- Parameters for two-rate bandwidth policer (CIR, PIR)
- PIR and CIR adaptation rules (min, max, closest)
- Burst size (CBS and MBS)
- Conformant action: allow (mark as in-profile)
- Non-conformant action: discard, or mark with options being in profile and out of profile

Policers allow temporary oversubscription of rates to enable new sessions to be added to traffic that may already be running at peak rate. Existing flows are impacted with discards to allow TCP backoff of existing flows, while preventing full capacity from blocking new flows.

Policers can be based on an AQP rule configuration to allow per-app-group, per-AA-sub total, per AA profile policy per application, and per system per app-group enforcement.

Policers are applied with two levels of hierarchy (granularity):

- Per individual AA subscriber
  - → Per-AA-sub per app group/application or protocol rate
  - → Per-AA-sub per application rate limit for a small selection of applications
  - → Per-AA-sub PIR/CIR. This allows the AA ISAAA ISA to emulate IOM ingress policers in from-sub direction.
- Per system (AA ISA or a group of AA subscribers)
  - → Total protocol/application rate
  - → Total app group rate

Flows may be subject to multiple policers in each direction (from-subscriber-to-network or from -network-to-subscriber).

In Figure 14, Application Assurance policers are applied after ingress SAP policers. Configuration of the SAP ingress policers can be set to disable ingress policing or to set PIR/CIR values such that AA ISA ingress PIR/CIR will be invoked first. This enables application aware discard decisions, ingress policing at SAP ingress is application blind. However, this is a design / implementation guideline that is not enforced by the node.

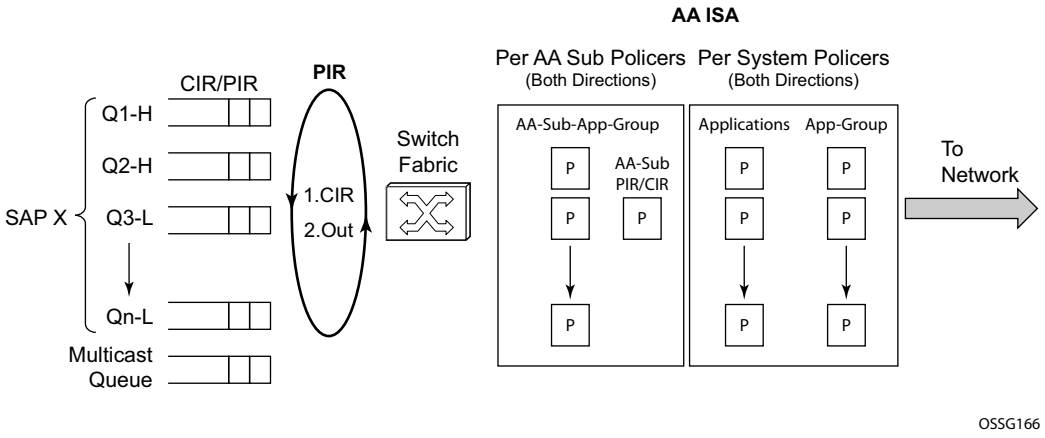

Figure 14: From-AA-Sub Application-Aware Bandwidth Policing

In the to-aa-sub direction (Figure 15), traffic hits the AA ISA policers before the SAP egress queuing and scheduling. This allows application aware flow, AA subscriber and node traffic policies to be implemented before the internet traffic is mixed with the other services at node egress. Note that AA ISA policers may remark out-of-profile traffic which allows preferential discard at an IOM egress congestion point only upon congestion.

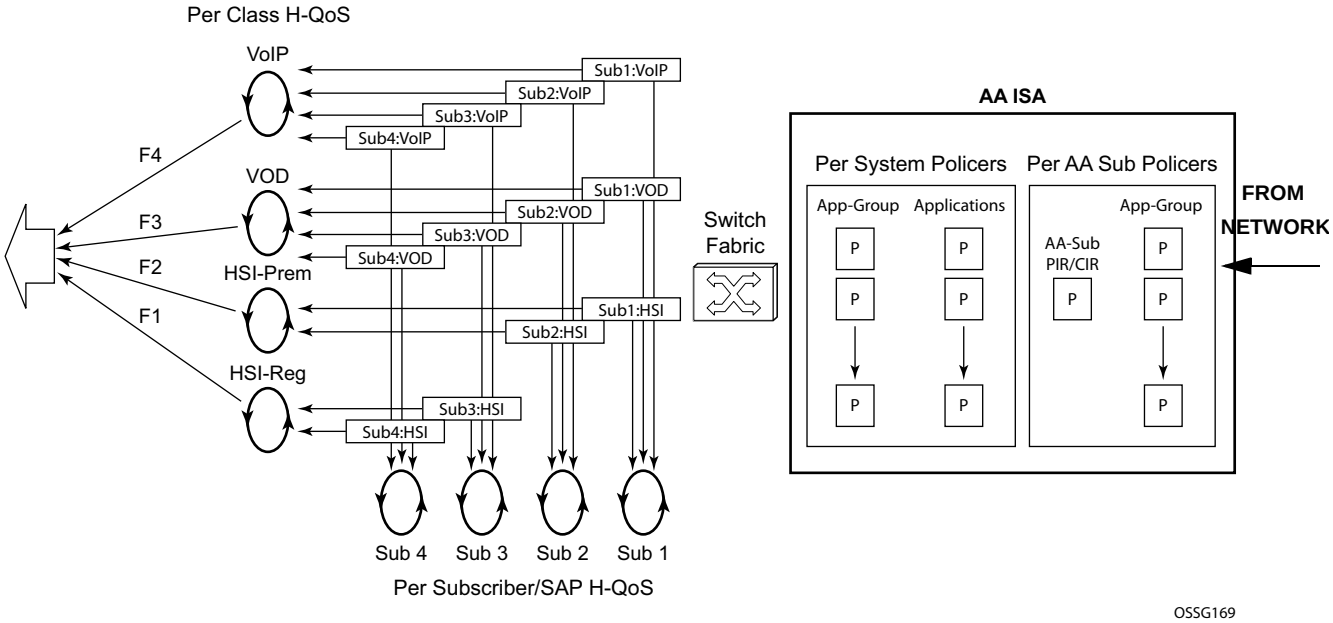

Figure 15: To-AA-Sub Application-Aware Bandwidth Policing

Application QoS Policy (AQP)

An AQP is an ordered set of entries defining application-aware policy (actions) for IP flows diverted to a given AA ISA group. The IP flow match criteria are based on application identification (application or application group name) but are expected to use additional match criteria such as ASO characteristic value, IP header information or AA subscriber ID, for example.

When application service option characteristic values are used in application profiles, the characteristics values can be further used to subdivide an AQP into policy subsets applicable only to a subset of AA subscribers with a given value of an ASO characteristic in their profile. This allows to, for example, subdivide AQP into policies applicable to a specific service option (MOS iVideo Service), specific subscriber class (Broadband service tier, VPN, Customer X), or a combination of both.

A system without AQP defined will have statistics generated but will not impact the traffic that is flowing through the system. However, it is recommended that an AQP policy is configured with at least default bandwidth and flow policing entries to ensure a fair access to AA ISA bandwidth/ flow resources for all AA subscribers serviced by a given AA ISA.

An AQP consists of a numbered and ordered set of entries each defining match criteria including AND, NOT and wildcard conditions followed by a set of actions.

```
AQP Entry <#> = <Match Criteria> AND <Match Criteria> <action> <action>
```

OR match conditions are supported in AQP through defining multiple entries. Multiple match criteria of a single AQP entry form an implicit AND function. An AQP can be defined for both recognized and unrecognized traffic. IP traffic flows that are in the process of being identified have a default policy applied (AQP entries that do not include application identification or IP header information). Flows that do not match any signatures are identified as unknown-tcp or unknown-udp and can have specific policies applied (as with any other protocol).

AQP Match Criteria

Match criteria consists of any combination of the following parameters:

- The source/destination IP address and port
- Application name
- Application group name
- One or more application service option characteristic and value pairs
- Direction of traffic (subscriber to network, network to subscriber, or both, or spoke SDP)
- DSCP name
- AA subscriber (ESM subscriber, SAP or spoke SDP)

  AQP entries with match criteria that exclusively use any combination of ASO characteristic and values, direction of traffic, and AA subscriber define default policies. All other AQP entries define application aware policies. Both default and application aware policies. Until a flow's application is identified only default policies can be applied.

AQP Actions

An AQP action consists of the following action types. Multiple actions are supported for each rule entry (unlike ip-filters):

- Dual or single-bucket bandwidth rate limit policer
- Flow setup rate limit policer
- Total active flow count limit policer
- Remark QoS (one or a combination of discard priority, forwarding class name, DSCP). When applied, ingress marked FC and discard priority is overwritten by AA ISA and the new values are used during egress processing (for example, egress queueing or egress policy DSCP remarking). For MPLS class-based forwarding, ingress-marked FC is still used to select an egress tunnel.
- Drop (discard)
- None (monitor and report only)
- Source mirror for an existing mirror service

Any flow diverted to an ISA group is evaluated against all entries of an AQP defined for that group at flow creation (default policy entries), application identification completion (all entries), and an AA policy change (all flows against all entries as a background task). Any given flow can match multiple entries, in which case multiple actions will be selected based on the AQP entry’s order (lowest number entry, highest priority) up to a limit of:

- 1 drop action
- Any combination of (applied only if no drop action is selected):
  - → Up to 1 mirror action;
  - → up to 1 FC, 1 priority and 1 DSCP remark action;
  - → up to 4 BW policers;
  - → up to 12 flow policers.

AQP entries the IP flow matched, that would cause the above per-IP-flow limits to be exceeded are ignored (no actions from that rule are selected).

Examples of some policy entries may be:

- Limit the subscriber to 20 concurrent Peer To Peer (P2P) flows max.
- Rate limit upstream total P2P application group to 400kbps.

Remark the voice application group to EF.

Time of Day Policing Adjustments

Time-of-day changes to Application Assurance policing rates can be implemented through the system's existing **cron** command. Typically, an operator may write scripts that can be executed at specific times of day that adjust policing rates. The adjusted policing limits are applied immediately to any pre-existing or new flows.

CLI Batch: Begin, Commit and Abort Commands

The Application Assurance uses CLI batches capability in policy definition. To start editing a policy, a begin command must be executed. To finish editing either abort (discard all changes) or commit (accept all changes) needs to be executed. CLI batch commands/state are preserved on HA activity switch.

To enter the mode to create or edit policies, the **begin** keyword must be entered at the prompt. Other editing commands include:

- The **commit** command saves changes made to policies during a session. The newly committed policy takes affect immediately for all new flows. Existing flows will transition onto the new policy shortly after the commit.
- The **abort** command discards changes that have been made to policies during a session.

To allow flexible order for policy editing, the **policy>commit** function cross references policy components to verify, among others:

- Whether all ASO characteristics have a default value and are defined in the app-profile.
- Limits checking.

Per AA Subscriber Service Monitoring and Debugging

Operators can use AA-specific tools in addition to system tools that allow them to monitor, adjust, debug AA services.

The following are examples of some of the available functions:

1. Display and monitor AA ISA group status and statistics (AA ISA status and capacity planning/monitoring).
2. Clear AA ISA group statistics (clears all system and per-AA-subscriber statistics).
3. Special study mode for real-time monitoring of AA-subscriber traffic (ESM subscriber, SAP or spoke SDP).
4. Per AQP entry statistics for number of hits (flow matching the entry) and conflicts (actions ignored due to per flow action limit exceeded).
5. Mirror (all or any subset of traffic seen by an AA ISA group).

Statistics and Accounting

Application Assurance statistics provide the operator with information to understand application usage within a network node. Application Assurance accounting aggregates the flow information into per application group, per application, per protocol reports on volume usage during the last accounting interval. This information is then sent to a statistics collector element for network wide correlation and aggregation into customized graphical usage reports. Application Assurance uses and benefits from the rich 7750 SR accounting infrastructure and the functionality it provides to control accounting policy details.

The following types of accounting volume records are generated and can be collected:

- Per ISA group and partition record for each configured application group
- Per ISA group and partition record for each configured application
- Per ISA group and partition record for each configured protocol
- Per each AA subscriber record with operator-configurable field content using custom AA records for operator-selected subset of protocols, applications and application groups.
- Per AA subscriber per each configured application record (special study mode)
- Per AA subscriber per each supported protocol record (special study mode)

Per AA flow statistics are provided as described in the cflowd section.

Refer to the 7750 SR OS System Management Guide for information on general accounting functionality.

Per-AA-Subscriber Special Study

The system can be configured to generate statistical records for each application and protocol that the system identifies for specific AA subscribers. These capabilities are disabled by default but can be enabled for a subset of AA subscribers to allow detailed monitoring of those AA subscriber's traffic.

Per-aa-sub per-application and per-aa-sub per-protocol records are enabled by assigning individual AA subscribers to "special study" service lists. The system and ISA group limit the number of AA subscribers in this mode to constrain the volume of stats generated. When an AA subscriber is in a special study mode, one record for every application and/or one record for every protocol that are configured in the system are generated for that subscriber. For example, if 500 applications are configured and 200 protocols are identified, 700 records per AA subscriber will be generated, if the AA subscriber is listed in both the per-aa-sub-application and per-aa-sub protocol lists.

System Aspects

Application Assurance uses the existing redundant accounting and logging capability of the 7750 SR for sending application and subscriber usage information, in-band or out-of-band. Application Assurance statistics are stored using compressed XML format with other system and subscriber statistics in compact flash modules on the redundant SF/CPMs. A large volume of statistics can be expected under scaled scenarios when per-AA-subscriber statistics/accounting is enabled.

AA accounting and statistics can be deployed as part of other system functionality as long as the system's function is compatible with AA accounting or as long as the system-level statistics can become application-aware due to, for example, AA ISA-based classification. An example of this feature interaction includes volume and time-based accounting where AA-based classification into IOM queues with volume and time accounting enabled can, for instance, provide different quota/credit management for off-net and on-net traffic or white/grey applications.

Application Assurance Volume Statistics and Accounting

Application Assurance is configured to collect and report on the following statistics when at least one AA ISA is active. The default Application Assurance statistics interval is 15 minutes.

Statistics to be exported from the node are aggregated into accounting records, which must be enabled in order to be sent. By default, no records are sent until enabled. Each record template type is enabled individually to control volume of statistics to the desired level of interest. Only non-zero records are written to the accounting files for all AA subscriber based statistics to reduce the volume of data.

The operator can further select a subset of the fields to be included in per-AA-subscriber records and whether to send records if no traffic was present for a given protocol or application, for example, sending only changed records.

Each record generated contains the record fields as described in Table 6. The header row represents the record type.

Table 6: Application Assurance Statistics Fields Generated per Record (Accounting File)

Record Fields	Description	Group/Partition App Group	Group/Partition Application	Group/Partition Protocol	AA-Sub Custom	AA-Sub Special Study per App	AA-Sub Special Study Protocol	XML Name
Application Group	Name	X						data name
Application	Name		X			X		data name
Protocol	Name			X			X	data name
Aggregation Type ID	ID (can be protocol, application or application group record)				X			agg-type-name
# Active Subscribers	# of subscribers who had a flow of this category during this interval	X	X	X				nsub
# allowed flows from-sub	# of new flows that were identified and allowed	X	X	X	X	X	X	sfa
# allowed flows to-sub	As above in opposite direction	X	X	X	X	X	X	nfa

Table 6: Application Assurance Statistics Fields Generated per Record (Accounting File)

Record Fields	Description	Group/Partition App Group	Group/Partition Application	Group/Partition Protocol	AA-Sub Custom	AA-Sub Special Study per App	AA-Sub Special Study Protocol	XML Name
# denied flows from-sub	the # of new flows that were identified and denied	X	X	X	X	X	X	sfd
# denied flows to-sub	As above in opposite direction	X	X	X	X	X	X	nfd
# Active flows from-sub	# of flows that were either: closed, opened & closed, opened, or continued during this interval	X	X	X	X	X	X	saf
# active flows to-sub	As above, in opposite direction	X	X	X	X	X	X	naf
Total packets from-sub		X	X	X	X	X	X	spa
Total packets to-sub		X	X	X	X	X	X	npa
Total bytes from-sub		X	X	X	X	X	X	sba
Total bytes to-sub		X	X	X	X	X	X	nba
Total discard packets from-sub		X	X	X	X	X	X	spd
Total short flows	Number of flows with duration <= 30 seconds that completed up to the end of this interval	X	X	X	X	X	X	sdf
Total medium flows	Number of flows with duration <= 180 seconds that completed up to the end of this interval	X	X	X	X	X	X	mdf
Total long flows	Number of flows with duration > 180 seconds that completed up to the end of this interval	X	X	X	X	X	X	ldf
Total discard packets to-sub		X	X	X	X	X	X	npd
Total discard bytes from-sub		X	X	X	X	X	X	sbd

Table 6: Application Assurance Statistics Fields Generated per Record (Accounting File)

Record Fields	Description	Group/Partition App Group	Group/Partition Application	Group/Partition Protocol	AA-Sub Custom	AA-Sub Special Study per App	AA-Sub Special Study Protocol	XML Name
Total discard bytes to-sub		X	X	X	X	X	X	nbd
Total flows completed	# of to- and from-subscriber flows that have been completed up to the reported interval.	X	X	X	X	X	X	tfc
Total flow duration	Duration, in seconds, of all flows that have been completed up to the reported interval.	X	X	X	X	X	X	tfd

The records are generated per ISA group and partition, with an ISA group identified by the group ID (XML field name “aaGroup”) , partition identified by the partition ID (XML field name “aaPart name” and per AA subscriber (if applicable) with the AA subscriber identified by the ESM subscriber name, SAP ID (XML field name “subscriber name”, “sap name” or “spoke SDP ID” respectively).

The date, time, and system ID for the records will be visible as part of the existing accounting log capability, thus does not need to be contained inside the Application Assurance records themselves.

Configurable AA-Subscriber Stats Collection

For AA subscriber accounting, an operator may select for which protocols, applications, or application groups that accounting records are to be generated up to a maximum of 512 records per subscriber. Each AA ISA card can generate up to 2048K per AA subscriber records (for example, 64K AA subscriber with 32 records).

By default no records are generated, unless upgrading from a release prior to Software Version 7750 SR/7450 OS 7.0 Rev. 01, in which case records for every application group will be generated if the per-application-group AA subscriber accounting was enabled. Per-AA-subscriber custom records are used for configurable AA-subscriber statistics collection.

Cflowd

Cflowd Export of AA Records

AA ISA allows cflowd records to be exported to an external cflowd collector. The cflowd collector parameters (such as IP address and port number) are configured per application assurance group. All cflowd records collected for both volume and per-flow TCP performance are exported to the configured collector(s). AA ISA supports cflowd Version 10/ IPFIX.

A cflowd record is only exported to the collector once the flow is closed/terminated.

TCP Application Performance

AA ISA allows an operator to collect per flow TCP performance statistics to be exported through cflowd v10/IPFIX.

The operator can decide to collect TCP performance for sampled flows within a TCP enabled group-partition-application/application-group. The flow sampling rate is configurable on per ISA-group level. For example a flow sample rate of 10 means that every 10th TCP flow is selected for TCP performance statistics collection. Anytime a flow is sampled (selected for TCP performance statistics collection) its mate flow in reverse direction is also selected. This allows collectors to correlate the results from the two flows and provide additional statistics (such as round-trip delay). Per-flow cflowd TCP performance records are exported to the configured collector(s) upon flow closure. The system can gather per flow TCP performance statistics for up to 307,200 concurrent flows.

Per-flow TCP performance can be enabled (or disabled) per application/app-group per partition per AA ISA-group.

Volume Statistics

AA ISA allows an operator to collect per flow volume statistics to be exported for any group partition. The packet sampling rate is configurable per AA- ISA-group level. For example, a packet sample rate of 10 means that one of every 10 packets is selected for volume statistics collection. If a flow has at least a single packet sampled for cflowd volume statistics, its per-flow cflowd volume record is exported to the configured collector upon flow closure.

Configuring Application Assurance with CLI

This section provides information to configure Application Assurance entities using the command line interface. It is assumed that the user is familiar with basic configuration of policies.

Provisioning AA ISA

The following illustrates syntax to provision AA ISA and configure ingress IOM QoS parameters. (The egress IOM QoS is configured in the **config>isa>application-assurance-grp>qos** context.)

CLI Syntax:
```
configure> card> mda mda-slot
    mda-type isa-aa
        network
            ingress
                pool
                    slope-policy slope-policy-name
                    resv-cbs percent-or-default
                queue-policy network-queue-policy-name
```

The following output displays AA ISA configuration example.

```
*A:cpm-a>config>app-assure# show mda 1/1
===============================================================================
MDA 1/1
===============================================================================
Slot  Mda   Provisioned           Equipped              Admin     Operational
            Mda-type              Mda-type              State     State
-------------------------------------------------------------------------------
1     1     isa-aa                isa-ms                up        up
===============================================================================
*A:cpm-a>config>app-assure#


*A:cpm-a>config>card# info
----------------------------------------------
        card-type iom-20g-b
        mda 1
            mda-type isa-aa
        exit
----------------------------------------------
*A:cpm-a>config>card#
```

Configuring AA ISA

To enable AA on the router:

- Create an AA ISA group.
- Assign AA ISA(s) to an AA ISA group.
- Select one or more FC to be diverted to AA.
- Enable the group.

The following example illustrates AA ISA group configuration with:

- Primary AA ISA and warm redundancy provided by the backup AA ISA.
- “fail-to-wire” behavior configured on group failure.
- BE forwarding class selected for divert.
- Default IOM QoS for logical ISA egress ports. The ISA ingress QoS is configured as part of ISA provisioning (**config>card>mda>network>ingress>qos**).

The following commands illustrate AA ISA group configuration context.

CLI Syntax:

```
config>>isa>application-assurance-group isa-aa-group-id
 backup mda-id
 description description
 divert-fc fc-name
 fail-to-open
 isa-capacity-cost-high-threshold threshold
 isa-capacity-cost-low-threshold threshold
 partitions
 primary mda-id
 qos
    egress
       from-subscriber
          pool [pool-name]
          resv-cbs percent-or-default
          slope-policy slope-policy-name
       port-scheduler-policy port-scheduler-policy-name
       queue-policy network-queue-policy-name
       to-subscriber
          pool [pool-name]
             resv-cbs percent-or-default
             slope-policy slope-policy-name
          port-scheduler-policy port-scheduler-policy-name
          queue-policy network-queue-policy-name
 [no] shutdown
```

The following output displays an AA ISA group configuration example.

```
A:ALU-A>config>isa>aa-grp# info detail
 ----------------------------------------------
     no description
     primary 1/2
     backup  2/2
     no fail-to-open
     isa-capacity-cost-high-threshold 4294967295
     isa-capacity-cost-low-threshold 0
     no partitions
     divert-fc be
     qos
        egress
          from-subscriber
               pool
                    slope-policy "default"
                    resv-cbs default
               exit
               queue-policy "default"
               no port-scheduler-policy
          exit
          to-subscriber
               pool
                    slope-policy "default"
                    resv-cbs default
               exit
               queue-policy "default"
               no port-scheduler-policy
          exit
        exit
     exit
     no shutdown
----------------------------------------------
A:ALU-A>config>isa>aa-grp#
```

Configuring Watermark Parameters

Use the following CLI syntax to configure thresholds for logs and traps when under high consumption of the flow table. The flow table has a limited size and these thresholds can be established to alert the user that the table is approaching capacity.

The low threshold is used while the high threshold is used as an alarm.

CLI Syntax:
```
config>application-assurance
 flow-table-high-wmark high-watermark
 flow-table-low-wmark low-watermark
```

Configuring a Group Policy

Beginning and Committing a Policy Configuration

To enter the mode to create or edit Application Assurance policies, you must enter the **begin** keyword at the **config>app-assure>group>policy** prompt. The **commit** command saves changes made to policies during a session. Changes do not take affect in the system until they have performed the commit function. The **abort** command discards changes that have been made to policies during a session.

The following error message displays when creating or modifying a policy without entering **begin** first.

```
A:ALA-B>config>app-assure>group>policy#
MINOR: AA #1005 Invalid Set - Cannot proceed with changes when in non-
edit mode
```

There are no default policy options. All parameters must be explicitly configured.

Use the following CLI syntax to begin a policy configuration.

CLI Syntax:
```
config>app-assure# group group-id
 policy
    begin
```

Use the following CLI syntax to commit a policy configuration.

CLI Syntax:
```
config>app-assure# group group-id
 policy
    commit
```

Aborting a Policy Configuration

Use the following CLI syntax to abort a policy configuration.

CLI Syntax:
```
config>app-assure# group group-id
 policy
    abort
```

Configuring an Application Filter

An operator can use an application filter to define applications based on ALU protocol signatures and a set of configurable parameters like IP flow setup direction, IP protocol number, server IP address and server TCP/UDP port. An application filter references an application configured as previously shown.

Use the following CLI syntax to configure an application filter entry.

CLI Syntax:

```
config>app-assure>group>policy# app-filter
 entry entry-id [create]
    application application-name
    description description-string
    expression expr-index expr-type {eq | neq} expr-string
    flow-setup-direction {subscriber-to-network | network-to-
       subscriber | both}
    ip-protocol-num {eq | neq} protocol-id
    protocol {eq | neq} protocol-signature-name
    server-address {eq | neq} ip-address[/mask]
    server-port {eq | neq | gt | lt} server-port-number
    server-port {eq|neq} range start-port-num end-port-num
    server-port {eq} {port-num | range start-port-num end-
       port-num} first-packet-trusted|first-packet-validate}
    no shutdown
```

The following example displays an application filter configuration.

```
*A:ALA-48>config>app-assure>group>policy>app-filter# entry 30 create
*A:ALA-48>config>app-assure>group>policy>app-filter>entry# info
----------------------------------------------
                      description "DNS traffic to local server on expected port #53"
                      protocol eq "dns"
                      flow-setup-direction subscriber-to-network
                      ip-protocol-num eq *
                      server-address eq 192.0.2.0/32
                      server-port eq 53
                      application "DNS_Local"
                      no shutdown
----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>app-filter>entry#
```

Configuring an Application Group

An operator can configure an application group to group multiple application into a single application assurance entity by referencing those applications to the group created.

Use the following CLI syntax to configure an application group.

CLI Syntax: config>app-assure>group>policy# app-group *application-group-name* [create]
description *description*

The following example displays an application group configuration.

```
*A:ALA-48>config>app-assure>group>policy# app-group "Peer to Peer" create
*A:ALA-48>config>app-assure>group>policy>app-grp# info
----------------------------------------------
                  description "Peer to Peer file sharing applications"
----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>app-grp#
```

Configuring an Application

An operator can configure an application to group multiple protocols, clients or network applications into a single Application Assurance application by referencing it later in the created application filters as display in other sections of this guide.

Use the following CLI syntax to configure an application.

CLI Syntax: config>app-assure>group>policy# application *application-name* [create]
app-group *app-group-name*
description *description*

The following example displays an application configuration.

```
*A:ALA-48>config>app-assure>group>policy# application "SQL" create
*A:ALA-48>config>app-assure>group>policy>app# info
----------------------------------------------
                    description "SQL protocols"
                    app-group "Business Critical Applications"
----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>app#
```

Configuring an Application Profile

Use the following CLI syntax to configure an application profile.

CLI Syntax: config>app-assure>group>policy# app-profile *app-profile-name* [create]
characteristic *characteristic-name* value *value-name*
description *description-string*
divert

The following example displays an application profile configuration.

```
*A:ALA-48>config>app-assure>group>policy# app-profile "Super" create
*A:ALA-48>config>app-assure>group>policy>app-prof# info
----------------------------------------------
                  description "Super User Application Profile"
                  divert
                  characteristic "Server" value "Prioritize"
                  characteristic "ServiceBw" value "SuperUser"
                  characteristic "Teleworker" value "Yes"
                  characteristic "VideoBoost" value "Priority"
----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>app-prof#
```

Configuring a Policer

Use the following CLI syntax to configure a policer.

CLI Syntax: config>app-assure>group>policy# policer *policer-name* type *type* granularity *granularity* create
action {priority-mark | permit-deny}
adaptation-rule pir {max | min | closest} [cir {max | min | closest}]
cbs *committed burst size*
description *description-string*
flow-count *flow-count*
mbs *maximum burst size*
rate *pir-rate* [cir *cir-rate*]

The following example displays an Application Assurance policer configuration.

```
*A:ALA-48>config>app-assure>group# policer "RegDown_Policer" type dual-bucket-bandwidth
granularity subscriber create

*A:ALA-48>config>app-assure>group>policer# info
----------------------------------------------
                description "Control the downstream aggregate bandwidth for Regular 1Mbps
subscribers"
                rate 1000 cir 500
                mbs 100
                cbs 50
----------------------------------------------
*A:ALA-48>config>app-assure>group>policer#
```

Configuring an Application QoS Policy

Use the following CLI syntax to configure an application QoS policy.

CLI Syntax:

```
config>app-assure>group>policy# app-qos-policy
        entry entry-id [create]
            action
                bandwidth-policer policer-name
                drop
                flow-count-limit policer-name
                flow-rate-limit policer-name
                mirror-source [all-inclusive] mirror-service-id
                remark
                    dscp in-profile dscp-name out-profile dscp-name
                    fc fc-name
                    priority priority-level
            description description-string
            match
                aa-sub sap {eq | neq} sap-id
                aa-sub esm {eq | neq} sub-ident-string
                aa-sub spoke-sdp {eq | neq} sdp-id:vc-id
                app-group {eq | neq} application-group-name
                application {eq | neq} application-name
                characteristic characteristic-name {eq} value-name
                dscp {eq | neq} dscp-name
                dst-ip {eq | neq} ip-address[/mask]
                dst-port {eq | neq} port-num
                dst-port {eq | neq} range start-port-num end-port-num
                src-ip {eq | neq} ip-address[/mask]
                src-port {eq | neq} port-num
                src-port {eq | neq} range start-port-num end-port-num
                traffic-direction {subscriber-to-network | network-to-
                  subscriber | both}
            no shutdown
```

The following example displays an application QoS policy configuration.

```
*A:ALA-48>config>app-assure>group>policy>aqp# entry 20 create
-----------------------------------------------
                        description "Limit downstream bandwidth to Reg_1M subscribers"
                        match
                            traffic-direction network-to-subscriber
                            characteristic "ServiceBw" eq "Reg_1M"
                        exit
                        action
                            bandwidth-policer "RegDown_Policer"
                        exit
                        no shutdown
-----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>aqp#
```

The following example display an AQP entry configuration to mirror all positively identified only P2P traffic (AppGroup P2P) for a subset of subscribers with ASO characteristic **aa-sub-mirror** enabled.

```
A:ALA-48>config>app-assure>group>policy>aqp#
------------------------------------------------------------------------------
   entry 100 create
     match
          app-group eq P2P
          characteristic aa-sub-mirror eq enabled
     exit
     action                      # mirror to an existing mirror service id
          mirror-source 100
     exit
   no shutdown
   exit
------------------------------------------------------------------------------
A:ALA-48>config>app-assure>group>policy>aqp#
```

The following example display AQP entries to mirror all P2P traffic (all positively identified P2P traffic and any unidentified traffic that may or may not be P2P - AppGroup P2P) for a subset of subscribers with ASO characteristic **aa-sub-mirror** enabled (the order is significant):

```
A:ALA-48>config>app-assure>group>policy>aqp>entry#
------------------------------------------------------------------------------
   entry 100 create
     match
          app-group eq P2P
          characteristic aa-sub-mirror value enabled
     exit
     action
          mirror-source all-inclusive 100
     exit
   no shutdown
   exit
------------------------------------------------------------------------------
A:ALA-48>config>app-assure>group>policy>aqp#
```

Configuring Application Service Options

Use the following CLI syntax to configure application service options.

CLI Syntax:
```
config>app-assure>group>policy# app-service-options
            characteristic characteristic-name [create]
               default-value value-name
               value value-name
```

The following example displays an application service options configuration.

```
*A:ALA-48>config>app-assure>group>policy>aso# info
----------------------------------------------
                    characteristic "Server" create
                        value "Block"
                        value "Permit"
                        value "Prioritize"
                        default-value "Block"
                    exit
                    characteristic "ServiceBw" create
                        value "Lite_128k"
                        value "Power_5M"
                        value "Reg_1M"
                        value "SuperUser"
                        default-value "Reg_1M"
                    exit
                    characteristic "Teleworker" create
                        value "No"
                        value "Yes"
                        default-value "No"
                    exit
                    characteristic "VideoBoost" create
                        value "No"
                        value "Priority"
                        default-value "No"
                    exit
----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>aso#
```

Configuring AA Volume Accounting and Statistics

A network operator can configure AA volume statistic collection and accounting on both AA ISA system and subscriber levels.

The following commands illustrate the configuration of statistics collection and accounting policy on an AA group/partition aggregate level (without subscriber context).

CLI Syntax: config>app-assure>group>statistics>app-group
accounting-policy *act-policy-id*
collect-stats

CLI Syntax: config>app-assure>group>statistics>application
accounting-policy *act-policy-id*
collect-stats

CLI Syntax: config>app-assure>group>statistics>protocol
accounting-policy *act-policy-id*
collect-stats

These commands illustrate the configuration of statistics collection and accounting policy for each AA subscriber in the system.

CLI Syntax: config>app-assure>group>statistics>aa-sub
accounting-policy *act-policy-id*
app-group *app-group-name*
application *application-name*
collect-stats
protocol *protocol-signature-name*

These commands illustrate configuration of special study mode for a subset of AA subscribers (configured) to collect all protocol and/or application statistics with an AA subscriber context.

CLI Syntax: config>app-assure>group>statistics# aa-sub-study {application|protocol}
accounting-policy *acct-policy-id*
collect-stats

For details on accounting policy configuration (including among others AA record type selection and customized AA subscriber record configuration) refer to the 7750 SR OS System Management Guide.

The following output illustrates per AA-subscriber statistics configuration that elects statistic collection for a small subset of all application groups, applications, protocols:

```
*A:ALU-40>config>app-assure>group>statistics>aa-sub# info
----------------------------------------------
                    accounting-policy 4
                    collect-stats
                    app-group "File Transfer"
                    app-group "Infrastructure"
                    app-group "Instant Messaging"
                    app-group "Local Content"
                    app-group "Mail"
                    app-group "MultiMedia"
                    app-group "Business_Critical
                    app-group "Peer to Peer"
                    app-group "Premium Partner"
                    app-group "Remote Connectivity"
                    app-group "Tunneling"
                    app-group "Unknown"
                    app-group "VoIP"
                    app-group "Web"
                    app-group "Intranet"
                    application "BitTorrent"
                    application "eLearning"
                    application "GRE"
                    application "H323"
                    application "TLS"
                    application "HTTP"
                    application "HTTPS"
                    application "HTTPS_Server"
                    application "HTTP_Audio"
                    application "HTTP_Video"
                    application "eMail_Business"
                    application "eMail_Other"
                    application "Oracle"
                    application "Skype"
                    application "SAP"
                    application "SIP"
                    application "SMTP"
                    application "SQL_Alltypes"
                    application "TFTP"
                    protocol "bittorrent"
                    protocol "dns"
                    protocol "sap"
                    protocol "skype"
----------------------------------------------
*A:ALU-40>config>app-assure>group>statistics>aa-sub#
```

Configuring Cflowd Collector

The following output displays an Application Assurance cflowd collector configuration example:

Example:
```
*A:ALA-48# configure application-assurance group 1 cflowd
collector 138.120.131.149:55000 create
*A:ALA-48>config>app-assure>group>cflowd>collector$ description
"cflowd_collector_NewYork"
*A:ALA-48>config>app-assure>group>cflowd>collector# no shutdown
*A:ALA-48>config>app-assure>group>cflowd>collector# exit


*A:ALA-48>config>app-assure>group>cflowd# info
----------------------------------------------
    collector 138.120.131.149:55000 create
         description "cflowd_collector_NewYork"
    no shutdown
----------------------------------------------
*A:ALA-48>config>app-assure>group>cflowd#
```

Application Assurance Command Reference

- Hardware Commands on page 87
- Admin Commands on page 88
- ISA Commands on page 88
- ISA Application Assurance Group on page 88
- Application Assurance Commands on page 90
- AA Group Commands on page 90
- Group Policy Commands on page 90
- Application Filter Commands on page 90
- Application Group Commands on page 91
- Application Profile Commands on page 91
- AQP Commands on page 91
- Application Service Options Commands on page 92
- Statistics Commands on page 92
- Show Commands on page 94
- Tools Commands on page 95
- Clear Commands on page 95
- Debug Commands on page 95
- Admin Commands on page 88

Hardware Commands

config
- **card** *slot-number*
  - **mda** *mda-slot*
    - **mda-type** *mda-type*
      - **network**
        - **ingress**
          - **pool** [*pool-name*]
          - **no pool**
            - **resv-cbs** *percent-or-default*
            - **no resv-cbs**
            - **slope-policy** *slope-policy-name*
            - **no slope-policy**
          - **queue-policy** ***network-queue-policy-name***
          - **no queue-policy**

Admin Commands

admin
- **application-assurance**
  - **upgrade**

ISA Commands

- **application-assurance-group** *application-assurance-group-index* [**create**]
- **no application-assurance-group** *application-assurance-group-index*
  - [**no**] **backup** *mda-id*
  - **description** *description-string*
  - **no description**
  - [**no**] **divert-fc** *fc-name*
  - **fail-to-open**
  - **no fail-to-open**
  - **isa-capacity-cost-high-threshold** *threshold*
  - **no isa-capacity-cost-high-threshold**
  - **isa-capacity-cost-low-threshold** *threshold*
  - **no isa-capacity-cost-low-threshold**
  - [**no**] **partitions**
  - [**no**] **primary** *mda-id*
  - **qos**
    - **egress**
      - **from-subscriber**
        - **pool** [*pool-name*]
        - **no pool**
          - **resv-cbs** *percent-or-default*
          - **no resv-cbs**
          - **slope-policy** *slope-policy-name*
          - **no slope-policy**
        - **port-scheduler-policy** *port-scheduler-policy-name*
        - **no port-scheduler-policy**
        - **queue-policy** ***network-queue-policy-name***
        - **no queue-policy**
      - **to-subscriber**
        - **pool** [*pool-name*]
        - **no pool**
          - **resv-cbs** *percent-or-default*
          - **no resv-cbs**
          - **slope-policy** *slope-policy-name*
          - **no slope-policy**
        - **port-scheduler-policy** *port-scheduler-policy-name*
        - **no port-scheduler-policy**
        - **queue-policy** ***network-queue-policy-name***
        - **no queue-policy**
  - [**no**] **shutdown**

LNS and NAT Group Commands

```
config
    — isa
        — lns-group lns-group-id [create]
        — no lns-group lns-group-id
            — description description-string
            — no description
            — mda mda-id [drain]
            — no mda mda-id
            — [no] shutdown
        — nat-group nat-group-id [create]
        — no nat-group nat-group-id
            — active-mda-limit number
            — no active-mda-limit
            — description description-string
            — no description
            — [no] mda mda-id
            — session-limits
                — reserved num-sessions
                — no reserved
                — watermarks high percentage low percentage
                — no watermarks
            — [no] shutdown
```

Application Assurance Commands

```
config
    — application-assurance
        — flow-table-high-wmark high-watermark
        — no flow-table-high-wmark
        — flow-table-low-wmark low-watermark
        — no flow-table-low-wmark
        — protocol protocol-name
            — [no] shutdown
        — group aa-group-id[:partition-id [create]
        — no group aa-group-id:partition-id
            — cflowd
                — collector ip-address[:port] [create]
                — no collector ip-address[:port]
                    — description description-string
                    — no description
                    — [no] shutdown
                — performance
                    — [no] app-group app-group-name perf-meas-type
                    — [no] application application-name perf-meas-type
                    — flow-rate perf-meas-type sample-rate
                    — no flow-rate perf-meas-type
                    — [no] shutdown
                — [no] shutdown
                — template-retransmit seconds
                — no template-retransmit
                — volume
                    — rate sample-rate
                    — no rate
                    — [no] shutdown
            — description description-string
            — no description
            — policer policer-name type type granularity granularity [create]
            — policer policer-name
            — no policer policer-name
                — action {priority-mark | permit-deny}
                — adaptation-rule pir {max | min | closest} [cir {max | min | closest}]
                — no adaptation-rule
                — cbs committed burst size
                — no cbs
                — description description-string
                — no description
                — flow-count flow-count
                — no flow-count
                — mbs maximum burst size
                — no mbs
                — rate pir-rate [cir cir-rate]
                — no rate
            — policy
                — abort
                — begin
                — commit
                — app-filter
                    — entry entry-id [create]
                    — no entry entry-id
```

- **application** *application-name*
- **description** *description-string*
- **no description**
- **expression** *expr-index expr-type* {**eq** | **neq**} *expr-string*
- **no expression** *expr-index*
- **flow-setup-direction** {**subscriber-to-network** | **network-to-subscriber** | **both**}
- **ip-protocol-num** {**eq** | **neq**} *protocol-id*
- **no ip-protocol-num**
- **protocol** {**eq** | **neq**} *protocol-signature-name*
- **no protocol**
- **server-address** {**eq**|**neq**} *ip-address*[/*mask*]
- **no server-address**
- **server-port** {**eq** | **neq** | **gt** | **lt**} *server-port-number*
- **server-port** {**eq**} *server-port-number* [**first-packet-trusted** | **first-packet-validate**]
- **no server-port**
- [**no**] **shutdown**

- **app-group** *application-group-name* [**create**]
- **no app-group** *application-group-name*
  - **description** *description-string*
  - **no description**
- **app-profile** *app-profile-name* [**create**]
- **no app-profile** *app-profile-name*
  - **capacity-cost cost**
  - **no capacity-cost**
  - **characteristic** *characteristic-name* **value** *value-name*
  - **no characteristic** *characteristic-name*
  - **description** *description-string*
  - **no description**
  - [**no**] **divert**
- **app-service-options** *characteristic-name* **value** *value-name*
- **no app-service-options** *characteristic-name*
- **app-qos-policy**
  - **entry** *entry-id* [**create**]
  - **no entry** *entry-id*
    - **action**
      - **bandwidth-policer** *policer-name*
      - **no bandwidth-policer**
      - [**no**] **drop**
      - **flow-count-limit** *policer-name*
      - **no flow-count-limit**
      - **flow-rate-limit** *policer-name*
      - **no flow-rate-limit**
      - **mirror-source** [**all-inclusive**] *mirror-service-id*
      - **no mirror-source**
      - **remark**
        - **dscp in-profile** *dscp-name* **out-profile** *dscp-name*
        - **no dscp**
        - **fc** *fc-name*
        - **no fc**

- priority *priority-level*
- no priority
- description *description-string*
- no description
- match
- aa-sub esm {eq | neq} *sub-ident-string*
- aa-sub sap {eq | neq} *sap-id*
- aa-sub spoke-sdp {eq | neq} *sdp-id:vc-id*
- no aa-sub
- app-group {eq | neq} *application-group-name*
- no app-group
- application {eq | neq} *application-group-name*
- no application
- characteristic *characteristic-name* eq *value-name*
- no characteristic
- dscp {eq | neq} *dscp-name*
- no dscp
- dst-ip {eq | neq} *ip-address*[/*mask*]
- no dst-ip
- dst-port {eq | neq} *port-num*
- dst-port {eq | neq} range *start-port-num end-port-num*
- no dst-port
- src-ip {eq | neq} *ip-address*[/*mask*]
- no src-ip
- src-port {eq | neq} *port-num*
- src-port {eq | neq}} range *start-port-num end-port-num*
- no src-port
- traffic-direction {subscriber-to-network | network-to-subscriber | both}
- [no] shutdown
- app-service-options
- characteristic *characteristic-name* [create]
- no characteristic *characteristic-name*
- default-value *value-name*
- no default-value
- [no] value *value-name*
- application *application-name* [create]
- no application *application-name*
- app-group *app-group-name*
- description *description-string*
- no description
- custom-protocol *custom-protocol-id* ip-protocol-num *protocol-id* [create]
- custom-protocol *custom-protocol-id*
- no custom-protocol *custom-protocol-id*
- description *description-string*
- no description
- expression *expr-index* eq *expr-string* offset *payload-octet-offset* direction *direction*
- no expression *expr-index*
- [no] shutdown
- diff
- statistics

- **aa-sub**
  - **accounting-policy** *acct-policy-id*
  - **no accounting-policy**
  - [**no**] **app-group** *app-group-name*
  - [**no**] **application** *application-name*
  - [**no**] **collect-stats**
  - [**no**] **protocol** *protocol-name*
- **aa-sub-study** *study-type*
  - [**no**] **aa-sub** {**esm** *sub-ident-string* | **sap** *sap-id* | **spoke-sdp** *sdp-id:vc-id*}
  - **accounting-policy** *acct-policy-id*
  - **no accounting-policy**
  - [**no**] **collect-stats**
- **app-group**
  - **accounting-policy** *acct-policy-id*
  - **no accounting-policy**
  - [**no**] **collect-stats**
- **application**
  - **accounting-policy** *acct-policy-id*
  - **no accounting-policy**
  - [**no**] **collect-stats**
- **protocol**
  - **accounting-policy** *acct-policy-id*
  - **no accounting-policy**
  - [**no**] **collect-stats**

Show Commands

```
show
  — isa
      — application-assurance-group [aa-group-id [load-balance [unassigned]]]
  — application-assurance
      — group aa-group-id
          — aa-sub esm sub-ident-string [snapshot]
          — aa-sub sap sap-id
          — aa-sub spoke-sdp sdp-id:vc-id [snapshot]
              — app-group [app-group-name] count [detail]
              — application [application-name] count [detail]
              — count [detail]
              — protocol [protocol-name] count [detail]
              — summary
          — aa-sub-list [isa mda-id]
          — aa-sub-study esm sub-ident-string [snapshot]
          — aa-sub-study sap sap-id
          — aa-sub-study spoke-sdp sdp-id:vc-id [snapshot]
              — application [application-name] count [detail]
              — protocol [protocol-name] count [detail]
          — app-group [app-group-name] count [detail]
          — application [application-name] count [detail]
          — cflowd
              — collector [detail]
              — status
          — partition summary
          — policer [policer-name]
          — policer summary
          — policy
              — admin
              — app-filter [entry-id]
              — app-group [app-group-name]
              — app-profile [app-prof-name]
              — app-profile app-prof-name associations
              — app-qos-policy [entry-id]
              — app-service-option [characteristic-name]
              — application [app-name]
              —
          — protocol [protocol-name] count [detail]
          — status [isa mda-id] cflowd
          — status [isa mda-id]
          — status [isa mda-id] detail
          — status {isa mda-id} qos count
          — status {isa mda-id} qos pools
      — protocol [protocol-name]
      — protocol [protocol-name] detail
      — version
  — service
      — aa-sub-using
      — aa-sub-using app-profile app-profile-name
      — sap-using
          — app-profile app-profile-name
      — sap-using
          — sdp-using [sdp-id[:vc-id]|far-end ip-address]
          — sdp-using app-profile app-profile-name
```

Tools Commands

tools
- **dump**
  - **application-assurance**
    - **group** *aa-group-id*>[:<*partition-id*]
      - **flow-record-search** **aa-sub** {esm *sub-ident-string* | **sap** *sap-id* | **spoke-sdp** *sdp-id:vc-id*} [**protocol** *protocol-name*] [**application** *app-name*] [**app-group** *app-group-name*] [**flow-status** *flow-status*] [**start-flowid** *start-flowid*] [**max-count** *max-count*] [**search-type** *search-type*] [**url** *file-url*]
      - **flow-record-search** **isa** *mda-id* [**protocol** *protocol-name*] [**application** *app-name*] [**app-group** *app-group-name*] [**flow-status** *flow-status*] [**start-flowid** *start-flowid*] [**max-count** *max-count*] [**search-type** *search-type*] [**url** *file-url*

Clear Commands

clear
- **application-assurance**
  - **group** *aa-group-id* **cflowd**
  - **group** *aa-group-id* **statistics**
  - **group** *aa-group-id* **status**

Debug Commands

debug
- [**no**] **mirror-source** *service-id*
  - **isa-aa-group** *aa-group-id* {**all** | **unknown**}
  - **no isa-aa-group** *aa-group-id*

Application Assurance Commands

- Application Assurance Commands on page 97
  - → Generic Commands on page 98
  - → Hardware Commands on page 99
  - → Application Assurance Commands on page 101
  - → Group Commands on page 106
    - – Policer Commands on page 106
    - – Policy Commands on page 110
      - – Application Filter Commands on page 114
      - – Application Profile Commands on page 119
      - – Application QoS Policy Commands on page 121
      - – Application Service Options Commands on page 130
    - – Statistics Commands on page 134
- ISA Commands on page 138

Application Assurance uses system components for some of its functionality. Refer to the following for details on:

- Configuration of Application Assurance Accounting policy including per accounting type record selection and customization of AA subscriber records.
- Configuration of AA ISA IOM QoS.

Generic Commands

description

Syntax **description** *description-string*
no description

Context config>app-assure>protocol
config>app-assure>group>policer
config>app-assure>group>policy>app-filter>entry
config>app-assure>group>policy>app-group
config>app-assure>group>policy>app-profile
config>app-assure>group>policy>aqp>entry
config>app-assure>group>policy>application
config>app-assure>group>cflowd>collector
config>app-assure>group>cflowd>group>cflowd
config>app-assure>group>cflowd>group>cflowd>collector
config>app-assure>group>cflowd>group>cflowd>volume
config>app-assure>group>policy>custom-protocol

Description This command creates a text description which is stored in the configuration file to help identify the content of the entity.

The **no** form of the command removes the string from the configuration.

Default **none**

Parameters *string* — The description character string. Allowed values are any string composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

shutdown

Syntax [**no**] **shutdown**

Context config>app-assure>group
config>app-assure>group>policy>app-filter>entry
config>app-assure>group>policy>aqp>entry
config>app-assure>group>cflowd>collector
config>app-assure>group>cflowd>group>cflowd>performance
config>isa>lns-group

Description This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

The **shutdown** command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Hardware Commands

isa-aa (mda-type)

Syntax **mda-type** *isa-aa*
no mda-type

Context config>card>mda

Description This command provisions an adaptor into an MDA position on an IOM slot. The AA ISA is provisioned into the system in the same manner as all other MDA type. Once an AA ISA is provisioned, independent of it actually existing in the system or the specified slot and MDA position, the AA ISA can be defined as a member of an application assurance group.

The **no** form of this command removes the module from the configuration. The module must be administratively shut down before it can be deleted from the configuration.

Refer to the 7750 SR OS Interface Guide for further information on command usage and syntax for the AA ISA and other MDA and ISA types.

Default No ISA types are configured for any slots by default.

Parameters *isa-aa* — Specifies the Application Assurance Integrated Services Adapter for the slot postion.

Admin Commands

application-assurance

Syntax **application-assurance**

Context admin

Description This command enables the context to perform Application Assurance (AA) configuration operations.

upgrade

Syntax **upgrade**

Context admin>app-assure

Description Use this command to load a new isa-aa.tim file as part of a router-independent signature upgrade. An AA ISA reboot is required.

Application Assurance Commands

application-assurance

Syntax **application-assurance**

Context config

Description This command enables the context to perform Application Assurance (AA) configuration operations.

flow-table-high-wmark

Syntax **flow-table-high-wmark** *high-watermark*
no flow-table-high-wmark

Context config>app-assure

Description The command configures the utilization of the flow records on the AA ISA group when a full alarm will be raised by the agent. The value must be larger than or equal to the **flow-table-low-wmark** *low-watermark* parameter.

Parameters *high-watermark* — Specifies the high watermark for flow table full alarms.

Values 0 — 100

flow-table-low-wmark

Syntax **flow-table-low-wmark** *low-watermark*
no flow-table-low-wmark

Context config>app-assure

Description The command configures the utilization of the flow records on the AA ISA group when the full alarm will be cleared by the agent. The value must be lower than or equal to the **flow-table-high-wmark** *high-watermark* parameter.

Parameters *low-watermark* — Specifies the low watermark for flow table full alarms.

Values 0 — 100

protocol

Syntax **protocol** *protocol-name*

Context config>app-assure

Description This command configures the shutdown of protocols system-wide.

Parameters *protocol-name* — A string of up to 32 characters identifying a predefined protocol.

group

Syntax **group** *aa-group-id*[:*partition-id* [**create**]
no group *aa-group-id*:*partition-id*

Context config>app-assure

Description This command configures and enables the context to configure an application assurance group and partition parameters.

Parameters *aa-group-id* — Represents a group of ISA MDAs.

Values 1 — 255

partition-id — Specifies a partition within a group,

Values 1 — 65535

create — Keyword used to create the partition in the group.

cflowd

Syntax **cflowd**

Context config>app-assure>group

Description This command enables the context to configure cflowd parameters for the application assurance group.

collector

Syntax **collector** *ip-address*[:*port*] [**create**]
no collector *ip-address*[:*port*]

Context config>app-assure>group>cflowd

Description This command defines a flow data collector for cflowd data. The IP address of the flow collector must be specified. The UDP port number is an optional parameter. If it is not set, the default of 2055 is used.

Parameters *ip-address* — The IP address of the flow data collector in dotted decimal notation.

:*port* **—** The UDP port of flow data collector.

Default 4739

Values 1— 65535

performance

Syntax **performance**

Context config>app-assure>group>cflowd

Description This command configures the cflowd performance export.

app-group

Syntax [**no**] **app-group** *app-group-name perf-meas-type*

Context config>app-assure>group>cflowd>performance

Description This command configures application groups to export performance records with cflowd.

The no form of the command removes the parameters from the configuration.

Parameters *app-group-name* — Specifies the application group name.

perf-meas-type — Specifies the kinds of performance measurement types which can be exported using cflowd in Application Assurance.

Values tcp

application

Syntax [**no**] **application** *application-name perf-meas-type*

Context config>app-assure>group>cflowd>performance

Description This command configures applications to export performance records with cflowd.

The **no** form of the command removes the parameters from the configuration.

Parameters *application-name* — Specifies the name defined for the application.

perf-meas-type — Specifies the kinds of performance measurement types which can be exported using cflowd in Application Assurance.

Values tcp

flow-rate

Syntax **flow-rate** *perf-meas-type sample-rate*
no flow-rate *perf-meas-type*

Context config>app-assure>group>cflowd>performance

Description This command configures specifies the per-flow sampling rate for the cflowd export of Application Assurance performance statistics.

The **no** form of the command reverts to the default.

Default no flow-rate

Parameters *perf-meas-type* — This is the type of traffic to perform performance measurement against.

Values tcp

sample-rate — This is the rate at which to sample flows that are eligible for TCP performance measurement.

Values 1 — 1000

template-retransmit

Syntax **template-retransmit** *seconds*
no template-retransmit

Context config>app-assure>group>cflowd

Description This command configures the period of time, in seconds, for the template to be retransmitted.

Parameters *seconds* — Specifies the time period for the template to be retransmitted.

Values 10 — 600

Default 600

volume

Syntax **volume**

Context config>app-assure>group>cflowd

Description This command configures the cflowd volume export.

rate

Syntax **rate** *sample-rate*
no rate

Context config>app-assure>group>cflowd>volume

Description This command configures the sampling rate of packets for the cflowd export of application assurance volume statistics.

The **no** form of the command reverts to the default value.

Parameters *sample-rate* — This is the rate at which to sample flows that are eligible for TCP performance measurement.

Values 1 — 10000

Group Commands

Policer Commands

policer

Syntax **policer** *policer-name* **type** *type* **granularity** *granularity* [**create**]
policer *policer-name*
no policer *policer-name*

Context config>app-assure>group

Description This command creates application assurance policer profile of a specified type. Policers can be bandwidth or flow limiting and can have a system scope (limits traffic entering AA ISA for all or a subset of AA subscribers), subscriber scope or granularity (limits apply to each AA subscriber traffic).

The policer type and granularity can only be configured during creation. They cannot be modified. The policer profile must be removed from all AQPs in order to be removed. Changes to policer profile parameters take effect immediately for policers instantiated as result of AQP actions using this profile..

The **no** form of the command deletes the specified policer from the configuration.

Parameters *type* — Specifies the policer type.

Values **single-bucket-bandwidth** — Creates a profile for a single bucket (PIR) bandwidth limiting policer.
dual-bucket-bandwidth — Creates profile for a dual backet (PIR, CIR) bandwidth limiting policer.
flow-rate-limit — Creates profile for a policer limiting rate of flow set-ups.
flow-count-limit — Creates profile for a policer limiting total flow count.

granularity — Specifies the granularity type.

Values **system** — Creates a system policer provile for a policer that limits the traffic in the scope of all or a subset of AA subscribers on a given AA ISA.
subscriber — Creates a policer profile for a policer for each AA subscriber that limits the traffic in the scope of that subscriber.

create — Keyword used to create the policer name and parameters.

Default none

Parameters *policer-name* — A string of up to 32 characters that identifies policer.

action

Syntax **action** {**priority-mark** | **permit-deny**}

Context config>app-assure>group>policer

Description This command configures the action to be performed by single-bucket bandwidth policers for non-conformant traffic.

Dual bucket bandwidth policers cannot have their action configured and always mark traffic below CIR in profile, between CIR and PIR out of profile, and drop traffic above PIR.
Flow policers always discard non-conformant traffic.
When multiple application assurance policers are configured against a single flow (including policers at both subscriber and system), the final action done to the flow/packet will be a logical OR of all policersí actions. For example, if only of the policers requires the packet to be discarded, the packet will be dropped regardless of the action of the other policers.

Default permit-deny

Parameters **priority-mark** — Non-conformant traffic will be marked out of profile and the conformant traffic will be marked in profile. The new marking will overwrite any previous IOM QoS marking done to a packet.

permit-deny — Non-conformant traffic will be dropped.

adaptation-rule

Syntax **adaptation-rule pir** {**max** | **min** | **closest**} [**cir** {**max** | **min** | **closest**}]
no adaptation-rule

Context config>app-assure>group>policer

Description This command defines the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined option. To change the CIR adaptation rule only, the current PIR rule must be part of the command executed.

The **no** form of the command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific adaptation-rule is removed, the default constraints for rate and cir apply.

Default closest

Parameters **max** — The operational PIR or CIR for the queue will be equal to or less than the administrative rate specified using the **rate** command.

min — The operational PIR or CIR for the queue will be equal to or greater than the administrative rate specified using the **rate** command.

closest — The operational PIR or CIR for the queue will be the rate closest to the rate specified using the **rate** command.

flow-count

Syntax **flow-count** *flow-count*
no flow-count

Context config>app-assure>group>policer

Description This command configures the flow count for the flow-count-limit policer. It is recommended to configure flow count subscriber-level policer for AA subscribers to ensure fair usage of flow resources between AA subscribers.

Parameters *flow-count* — Specifies the flow count for the flow-count-limit policer.

cbs

Syntax **cbs** *committed-burst-size*
no cbs

Context config>app-assure>group>policer

Description This command provides a mechanism to configure the committed burst size for the policer. It is recommended that CBS is configured larger than twice the maximum MTU for the traffic handled by the policer to allow for some burstiness of the traffic. CBS is configurable for dual-bucket bandwidth policers only.

The **no** form of the command resets the cbs value to its default.

Default 0

Parameters *committed-burst-size* — An integer value defining size, in kbytes, for the CBS of the policer.

Values 0 — 131071

mbs

Syntax **mbs** *maximum-burst-size*
no mbs

Context config>app-assure>group>policer

Description This command provides a mechanism to configure the maximum burst size for the policer. It is recommended that MBS is configured larger than twice the MTU for the traffic handled by the policer to allow for some burstiness of the traffic. MBS is configurable for single-bucket, dual-bucket bandwidth and flow setup rate policers only.

The **no** form of the command resets the MBS value to its default.

Default 0

Parameters *maximum-burst-size* — An integer value defining either size, in kbytes, for the MBS of the bandwidth policer, or flow count for the MBS of the flow setup rate policers.

Values 0 — 131071

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context config>app-assure>group>policer

Description This command configures the administrative PIR and CIR for bandwidth policers and flow setup rate limits for flow policers. The actual rate sustained by the flow can be limited by other policers that may be applied to that flow's traffic. This command does not apply to flow-count-limit policers. The **cir** option is applicable only to dual-bucket bandwidth policers. It is recommended to configure flow setup rate subscriber-level policer for AA subscribers to ensure fair usage of flow resources between AA subscribers.

The **no** form of the command resets the values to defaults.

Default 0

Parameters *pir-rate* — An integer specifying either the PIR rate in Kbps for bandwidth policers.

Values 1 — 100000000, max or flows

cir-rate **—** An integer specifying the CIR rate in Kbps.

Values 0 — 100000000, max

Policy Commands

policy

Syntax **policy**

Context config>app-assure>group>policy

Description This command enables the context to configure parameters for application assurance policy. To edit any policy content begin command must be executed first to enter editing mode. The editing mode is left when the abort or commit commands are issued.

abort

Syntax **abort**

Context config>app-assure>group>policy

Description This command ends the current editing session and aborts any changes entered during this policy editing session.

begin

Syntax **begin**

Context config>app-assure>group>policy

Description This command begins a policy editing session.

The editing session continues until one of the following conditions takes place:

- Abort or commit is issued.
- Control complex resets.

The editing session is not interrupted by:

- HA activity switch.
- CLI session termination (for example, as result of closing a Telnet session).

commit

Syntax **commit**

Context config>app-assure>group>policy

Description This command commits changes made during the current editing session. None of the policy changes done will take effect until commit command is issued. If the changes can be successfully committed,

no errors detected during the commit during cross-reference verification against exiting application assurance configuration, the editing session will also be closed.

The newly committed policy takes affect immediately for all new flows, existing flows will transition onto the new policy shortly after the commit.

app-group

Syntax **app-group** *application-group-name* [**create**]
no app-group *application-group-name*

Context config>app-assure>group>policy

Description This command creates an application group for an application assurance policy.

The **no** form of the command deletes the application group from the configuration. All associations must be removed in order to delete a group.

Default no app-group

Parameters *application-group-name* — A string of up to 32 characters uniquely identifying this application group in the system.

create — Mandatory keywork used when creating an application group. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

app-filter

Syntax **app-filter**

Context config>app-assure>group>policy

Description This command enables the context to configure an application filter for application assurance.

app-profile

Syntax **app-profile** *app-profile-name* [**create**]
no app-profile *app-profile-name*

Context config>app-assure>group>policy

Description This command creates an application profile and enables the context to configure the profile parameters.

The **no** form of the command removes the application profile from the configuration.

Default none

Parameters *app-profile-name* — Specifies the name of the application profile up to 32 characters in length.

create — Mandatory keywork used when creating an application profile. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

app-qos-policy

Syntax **app-qos-policy**

Context config>app-assure>group>policy

Description This command enables the context to configure an application QoS policy.

app-service-options

Syntax **app-service-options**

Context config>app-assure>group>policy

Description This command enables the context to configure application service option characteristics.

diff

Syntax **diff**

Context config>app-assure>group>policy

Description This command compares the newly configured policy against the operational policy.

application

Syntax **application** *application-name* [**create**]
no application *application-name*

Context config>app-assure>group>policy

Description This command creates an application of an application assurance policy.

The **no** form of the command deletes the application. To delete an application, all associations to the application must be removed.

Default none

Parameters *application-name* — Specifies a string of up to 32 characters uniquely identifying this application in the system.

create — Mandatory keyword used when creating an application. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

app-group

Syntax **app-group** *application-group-name*

Context config>app-assure>group>policy>application

Description This command associates an application with an application group of an application assurance policy.

Default none

Parameters *application-name* — A string of up to 32 characters uniquely identifying an existing application in the system.

APPLICATION FILTER COMMANDS

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context config>app-assure>group>policy>app-filter

Description This command creates an application filter entry.

App filter entries are an ordered list, the lowest numerical entry that matches the flow defines the application for that flow.

An application filter entry or entries configures match attributes of an application.

The **no** form of this command deletes the specified application filter entry.

Default none

Parameters *entry-id* — An integer that identifies an app-filter entry.

Values 1 — 65535

create — Keyword used to create the entry.

application

Syntax **application** *application-name*

Context config>app-assure>group>policy>app-filter>entry

Description This command assigns this application filter entry to an existing application. Assigning the entry to **Unknown** application restores the default configuration.

Default unknown application

Parameters *application-name* — Specifies an existing application name.

expression

Syntax **expression** *expr-index expr-type* {**eq** | **neq**} *expr-string*
no expression *expr-index*

Context config>app-assure>group>policy>app-filter>entry

Description This command configures string values to use in the application definition.

Parameters *expr-index* — Specifies an index value which represents .expression substrings.

Values 1 — 3

expr-type — Represents a type (and thereby the expression substring).

http-host, http-uri, http-referer, sip-ua, sip-uri
http-host — Matches the string against the HTTP Host field.
http-uri — Matches the string against the HTTP URI field.
http-referer — Matches the string against the HTTP Referer field.
sip-ua — Matches the string against the SIP UA field.
sip-uri — Matches the string against the SIP URI field.
sip-mt — Matches the string against the SIP MT field.
citrix-app — Matches the string against the Citrix app field.
h323-product-id — Matches the string against the h323-product-id field.
* - udp/tcp wildcard

eq — Specifies the equal to comparison operator to match the specified HTTP string.

neq — Specifies the not equal to comparison operator to match the specified HTTP string.

expr-string — Specifies an expression string, up to 64 characters, used to define a pattern match. Denotes a printable ASCII substring used as input to an application assurance filter match criteria object.

- The following syntax is permitted within the substring to define the pattern match criteria:

  ^<substring>* - matches when <substring> is at the beginning of the object.

  <substring> - matches when <substring> is at any place within the object.

  *<substring>$ - matches when <substring> is at the end of the object.

  ^<substring>$ - matches when <substring> is the entire object.

- Rules for <substring> characters:

  <substring> must contain printable ASCII characters.

  <substring> must not contain the “double quote” character or the “ ” (space) character on its own.

  <substring> match is case sensitive.

  <substring> must not include any regular expression meta-characters.

- The “\” (slash) character is used as an ESCAPE sequence. The following ESCAPE sequences are permitted within the <substring>:

  Character to match <substring> input

  Hexidecimal Octet YY \xYY

  Note: A <substring> that uses the '\' (backslash) ESCAPE character which is not followed by a “\” or “\x” and a 2-digit hex octet is not valid.

Operational notes:

1. When matching a TCP flow against HTTP-string based applications, the HTTP header fields are collected from the first HTTP request (for example a GET or a POST) for a given TCP flow. The collected strings are then evaluated against each HTTP flow created within the given TCP flow to determine whether a given HTTP flow matches the application. By not specifying a protocol, the HTTP expressions are matched against all protocols in the HTTP family. By specifying a specific HTTP protocol (for example, http_video) the expression match can be constrained to a subset of the HTTP protocols.

2. To uniquely identify a SIP-based application a protocol match is not required in the app-filter entry with the SIP expression. The SIP expression match is performed against any protocol in the SIP family (such as sip and rtp_sip). By specifying a specific SIP protocol (like rtp_sip) the expression match can be constrained to a subset of the SIP protocols.

flow-setup-direction

Syntax **flow-setup-direction** {**subscriber-to-network** | **network-to-subscriber** | **both**}

Context config>app-assure>group>policy>app-filter>entry

Description This command configures the direction of flow setup to which the application filter entry is to be applied.

Parameters **subscriber-to-network —** Specifies that the app-filter entry will be applied to flows initiated by a local subscriber.

network-to-subscriber — Specifies that the app-filter entry will be applied to flows initiated from a remote destination towards a local subscriber.

both — Specifies that the app filter entry will be applied for subscriber-to-network and network-to-subscriber traffic.

Default both

ip-protocol-num

Syntax **ip-protocol-num** {**eq** | **neq**} *protocol-id*
no ip-protocol-num

Context config>app-assure>group>policy>app-filter>entry

Description This command configures the IP protocol to use in the application definition.

The **no** form of the command restores the default (removes IP protocol number from application criteria defined by this app-filter entry).

Default none

Parameters **eq —** Specifies that the value configured and the value in the flow must be equal.

neq — Specifies that the value configured differs from the value in the flow.

protocol-id — Specifies the decimal value representing the IP protocol to be used as an IP filter match criterion. Well known protocol numbers include ICMP (1), TCP (6), UDP (17).

The **no** form the command removes the protocol from the match criteria.

Values 0 — 255 (values can be expressed in decimal, hexidecimal, or binary - DHB)
keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp
* — udp/tcp wildcard

server-address

Syntax **server-address** {**eq** | **neq**} *ip-address*[/*mask*]
no server-address

Context config>app-assure>group>policy>app-filter>entry

Description This command configures the server address to use in application definition. The server IP address may be the source or destination, network or subscriber IP address.

The **no** form of the command restores the default (removes the server address from application criteria defined by this entry).

Default no net-address

Parameters **eq —** Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

ip-address — Specifies a valid IPv4 unicast address.

mask — The mask associated with the IP address as a mask length, for example /16 for a sixteen-bit mask.

Values 1 — 32

server-port

Syntax **server-port** {**eq** | **neq** | **gt** | **lt**} *server-port-number*
server-port {**eq** | **neq**} range *start-port-num end-port-num*
server-port {**eq**} {*port-num* | range*start-port-num end-port-num*} {**first-packet-trusted** | **first-packet-validate**}
no server-port

Context config>app-assure>group>policy>app-filter>entry

Description This command specifies the server TCP or UDP port number to use in the application definition.

The **no** form of the command restores the default (removes server port number from application criteria defined by this app-filter entry).

Default no server-port (the server port is not used in the application definition)

Parameters **eq —** Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

gt — Specifies all port numbers greater than server-port-number match.

lt — Specifies all port numbers less than server-port-number match.

server-port-num — Specifies a valid server port number.

Values 0 — 65535

start-port-num, end-port-num — Specifies the starting or ending port number.

Values 0 — 65535

Server Port Options:

- **No option specified:** TCP/UDP port applications with full signature verification:
  - AA ensures that other applications that can be identified do not run over a well-known port.
  - Application-aware policy applied once sugnature-based identification completes (likely requiring several packets).
- **first-packet-validate:** TCP/UDP trusted port applications with signature verification:
  - Application identified using well known TCP/UDP port based filters and re-identified once signature identification completes.
  - AA policy applied from the first packet of a flow while continuing signature-based application identification. Policy re-evaluated once the signature identification completes, allowing to detect improper/unexpected applications on a well-known port.
- **first-packet-trusted:** TCP/UDP trusted port applications - no signature verification:
  - Application identified using well known TCP/UDP port based filters only.
  - Application Aware policy applied from the first packet of a flow.
  - No signature processing assumes operator/customer trusts that no other applications can run on the well-known TCP/UDP port (statistics collected against trusted_tcp or trusted_udp protocol).

protocol

Syntax **protocol** {**eq** | **neq**} *protocol-name*
no protocol

Context config>app-assure>group>policy>app-filter>entry

Description This command configures protocol signature in the application definition.

The **no** form of the command restores the default (removes protocol from match application defined by this app-filter entry).

Default no protocol

Parameters **eq —** Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

protocol-name — A string of up to 32 characters identifying a predefined protocol.

APPLICATION PROFILE COMMANDS

capacity-cost

Syntax **capacity-cost** *cost*
nocapacity-cost

Context config>app-assure>group>policy>app-profile

Description This command configures an application profile capacity cost. Capacity-Cost based load balancing allows a cost to be assigned to diverted SAPs (with the app-profile) and this is then used for load-balancing SAPs between ISAs as well as for a threshold that notifies the operator if/when capacity planning has been exceeded.

Parameters *cost* — Specifies the profile capacity cost.

Values 1 — 65535

characteristic

Syntax **characteristic** *characteristic-name* **value** *value-name*
no characteristic *characteristic-name*

Context config>app-assure>group>policy>app-profile

Description This command assigns one of the existing values of an existing application service option characteristic to the application profile.

The **no** form of the command removes the characteristic from the application profile.

Default none

Parameters *characteristic-name* — Specifies the name of an existing ASO characteristic.

value *value-name* **—** Specifies the name for the application profile characteristic up to 32 characters in length.

divert

Syntax [**no**] **divert**

Context config>app-assure>group>policy>app-profile

Description This command enables the redirection of traffic to AA ISA for the system-wide forwarding classes diverted to application assurance (**divert-fc**) for AA subscribers using this application profile.

The **no** form of the command stops redirect of traffic to AA ISAs for the AA subscribers using this application profile.

Default no divert

APPLICATION QOS POLICY COMMANDS

entry

Syntax [**no**] **entry** *entry-id* [**create**]

Context config>app-assure>group>policy>aqp

Description This command creates an application QoS policy entry. A flow that matches multiple Application QoS policies (AQP) entries will have multiple AQP entries actions applied. When a conflict occurs for two or more actions, the action from the AQP entry with the lowest numerical value takes precedence.

The **no** form of this command deletes the specified application QoS policy entry.

Default none

Parameters *entry-id* — An integer identifying the AQP entry.

Values 1 — 65535

create — Mandatory keyword creates the entry. The **create** keyword requirement can be enabled/ disabled in the **environment**>**create** context.

action

Syntax **action**

Context config>app-assure>group>policy>aqp>entry

Description This command enables the context to configure AQP actions to be performed on flows that match the AQP entry's match criteria.

bandwidth-policer

Syntax **bandwidth-policer** *policer-name*
no bandwidth-policer

Context config>app-assure>group>policy>aqp>entry>action

Description This command assigns an existing bandwidth policer as an action on flows matching this AQP entry. The match criteria for the AQP entry must specify a uni-directional traffic direction before a policer

action can be configured. If a policer is used in one direction in an AQP match entry the same policer name cannot be used by another AQP entry which uses a different traffic direction match criteria.

When multiple policers apply to a single flow, the final action on a packet is the worse case of all policer outcome (for example, if one of the policers marks packet out of profile, the final marking will reflect that).

The **no** form of the command removes bandwidth policer from actions on flows matching this AQP entry.

Default no bandwidth-policer

Parameters *policer-name* — Specifies the name of the existing bandwidth policer for this application assurance profile. The *policer-name* is configured in the **config**>**app-assure**>**profile**>**policer** context.

drop

Syntax [**no**] **drop**

Context config>app-assure>group>policy>aqp>entry>action

Description This command configures the drop action on flows matching this AQP entry. When enabled, all flow traffic matching this AQP entry will be dropped. When drop action is part of a set of multiple actions to be applied to a single flow as result of one or more AQP entry match, drop action will be performed first and no other action will be invoked on that flow.

The **no** form of the command disables the drop action on flows matching this AQP entry.

Default no drop

flow-count-limit

Syntax **flow-count-limit** *policer-name*
no flow-count-limit

Context config>app-assure>group>policy>aqp>entry>action

Description This command assigns an existing flow count limit policer as an action on flows matching this AQP entry.

The match criteria for the AQP entry must specify a uni-directional traffic direction before a policer action can be configured. If a policer is used in one direction in an AQP match entry the same policer name cannot be used by another AQP entry which uses a different traffic direction match criteria.

When multiple policers apply to a single flow, the final action on a packet is the worse case of all policer outcome (for example, if one of the policers marks packet out of profile, the final marking will reflect that).

The **no** form of the command removes this flow policer from actions on flows matching this AQP entry.

Default no flow-count-limit

Parameters *policer-name* — The name of an existing flow count limit policer for this application assurance profile. The *policer-name* is configured in the **config**>**app-assure**>**profile**>**policer** context.

flow-rate-limit

Syntax **flow-rate-limit** *policer-name*
no flow-rate-limit

Context config>app-assure>group>policy>aqp>entry>action

Description This command assigns an existing flow setup rate limit policer as an action on flows matching this AQP entry.

The match criteria for the AQP entry must specify a uni-directional traffic direction before a policer action can be configured. If a policer is used in one direction in an AQP match entry the same policer name cannot be used by another AQP entry which uses a different traffic direction match criteria.

When multiple policers apply to a single flow, the final action on a packet is the worse case of all policer outcome (for example, if one of the policers marks packet out of profile, the final marking will reflect that).

The **no** form of the command removes this flow policer from actions on flows matching this AQP entry.

Default no flow-rate-limit

Parameters *policer-name* — The name of the existing flow setup rate policer for this application assurance profile. The *policer-name* is configured in the **config**>**app-assure**>**profile**>**policer** context.

mirror-source

Syntax **mirror-source** [**all-inclusive**] *mirror-service-id*
no mirror-source

Context config>app-assure>group>policy>aqp>entry>action

Description This command configures an application-based policy mirroring service that uses this AA ISA group's AQP entry as a mirror source. When configured, AQP entry becomes a mirror source for IP packets seen by the AA (note that the mirrored packet is an IP packet analyzed by AA and does not include encapsulations present on the incoming interfaces).

Default no mirror-source

Parameters **all-inclusive —** Specifies that all packets during identification phase that could match a given AQP rule are mirrored in addition to packets after an application identification completes that match the AQP rule. This ensures all packets of a given flow are mirrored at a cost of sending unidentified packets that once the application is identified will no longer match this AQP entry.

mirror-service-id — Specifies the mirror source service ID to use for flows that match this policy.

Values 1 — 214748364
svc-name: 64 char max

remark

Syntax **remark**

Context config>app-assure>group>policy>aqp>entry>action

Description This command configures remark action on flows matching this AQP entry.

dscp

Syntax **dscp in-profile** *dscp-name* **out-profile** *dscp-name*
no dscp

Context config>app-assure>group>policy>aqp>entry>action>remark

Description This command enables the context to configure DSCP remark action or actions on flows matching this AQP entry. When enabled, all packets for all flows matching this AQP entry will be remarked to the configured DSCP name.

DSCP remark can only be applied when the entry remarks forwarding class or forwarding class and priority. In-profile and out-of profile of a given packet for DSCP remark is assessed after all AQP policing and priority remarking actions took place.

The **no** form of the command stops DSCP remarking action on flows matching this AQP entry.

Parameters **in-profile** *dscp-name* — Specifies the DSCP name to use to remark in-profile flows that match this policy.

out-profile *dscp-name* — Specifies the DSCP name to use to remark out-of-profile flows that match this policy.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

fc

Syntax **fc** *fc-name*
no fc

Context config>app-assure>group>policy>aqp>entry>action>remark

Description This command configures remark FC action on flows matching this AQP entry. When enabled, all packets for all flows matching this AQP entry will be remarked to the configured forwarding class.

The **no** form of the command stops FC remarking action on packets belonging to flows matching this AQP entry

Parameters *fc-name* — Configure the FC remark action for flows matching this entry.

Values be, l2, af, l1, h2, ef, h1, nc

priority

Syntax **priority** *priority-level*
no priority

Context config>app-assure>group>policy>aqp>entry>action>remark

Description This command configures remark discard priority action on flows matching this AQP entry. When enabled, all packets for all flows matching this AQP entry will be remarked to the configured discard priority.

Default no priority

Parameters *priority-level* — Specifies the priority to apply to a packet.

Values high, low

match

Syntax **match**

Context config>app-assure>group>policy>aqp>entry

Description This command enables the context to configure flow match rules for this AQP entry. A flow matches this AQP entry only if it matches all the match rules defined (logical and of all rules). If no match rule is specified, the entry will match all flows.

aa-sub

Syntax **aa-sub esm** {**eq | neq**} *sub-ident-string*
aa-sub sap {**eq | neq**} *sap-id*
aa-sub spoke-sdp {**eq | neq**} *sdp-id:vc-id*
no aa-sub

Context config>app-assure>group>policy>aqp>entry>match

Description This command specifies a Service Access Point (SAP) or an ESM subscriber as matching criteria.

The **no** form of the command removes the SAP or ESM matching criteria.

Parameters **eq —** Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

sub-ident-string — Specifies the name of an existing application assurance subscriber.

sap-id — Specifies the SAP ID.

sap *sap-id* **—** Specifies the physical port identifier portion of the SAP definition. Refer to Appendix A: Common CLI Command Descriptions on page 383 for syntax.

sdp-id:vc-id — Specifies the spoke SDP ID and VC ID.

Values 1 — 17407
1 — 4294967295

app-group

Syntax **app-group** {**eq** | **neq**} *application-group-name*
no app-group

Context config>app-assure>group>policy>aqp>entry>match

Description This command adds app-group to match criteria used by this AQP entry.

The **no** form of the command removes the app-group from match criteria for this AQP entry.

Default no app-group

Parameters **eq —** Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

application-group-name — The name of the existing application group entry. The application-group-name is configured in the **config**>**app-assure**>**group**>**policy**>**aqp**>**entry**>**match** context.

application

Syntax **application** {**eq** | **neq**} *application-name*
no application

Context config>app-assure>group>policy>aqp>entry>match

Description This command adds an application to match criteria used by this AQP entry.

The **no** form of the command removes the application from match criteria for this AQP entry.

Default no application

Parameters **eq —** Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

application-name — The name of name existing application name. The application-group-name is configured in the **config**>**app-assure**>**group**>**policy**>**aqp**>**entry**>**match** context.

characteristic

Syntax **characteristic** *characteristic-name* **eq** *value-name*
no characteristic

Context config>app-assure>group>policy>aqp>entry>match

Description This command adds an existing characteristic and its value to the match criteria used by this AQP entry.

The **no** form of the command removes the characteristic from match criteria for this AQP entry.

Default no characteristic

Parameters **eq —** Specifies that the value configured and the value in the flow are equal.

characteristic-name — The name of the existing ASO characteristic up to 32 characters in length.

value-name — The name of an existing value for the characteristic up to 32 characters in length.

dscp

Syntax **dscp** {**eq** | **neq**} **dscp-name**
no dscp

Context config>app-assure>group>policy>aqp>entry>match

Description This command adds a DSCP name to the match criteria used by this AQP entry.

The no form of the command removes dscp from match criteria for this AQP entry.

Default no dscp

Parameters **eq —** Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

dscp-name — The DSCP name to be used in match.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

dst-ip

Syntax **dst-ip** {**eq | neq**} *ip-address*[/*mask*]
no dst-ip

Context config>app-assure>group>policy>aqp>entry>match

Description This command specifies a destination IP address to use as match criteria.

Parameters **eq —** Specifies that a successful match occurs when the flow matches the specified address or prefix.

neq — Specifies that a successful match occurs when the flow does not match the specified address or prefix.

ip-address — Specifies a valid IPv4 unicast address.

mask — Specifies the length of the IP address prefix.

dst-port

Syntax **dst-port** {**eq | neq**} *port-num*
dst-port {**eq | neq**} **range** *start-port-num end-port-num*
no dst-port

Context config>app-assure>group>policy>aqp>entry>match

Description This command specifies a destination TCP/UDP port or destination range to use as match criteria.

The **no** form of the command removes the parameters from the configuration.

Parameters **eq —** Specifies that a successful match occurs when the flow matches the specified port.

neq — Specifies that a successful match occurs when the flow does not match the specified port.

port-num — Specifies the destination port number.

Values 0 — 65535

start-port-num end-port-num — Specifies the start or end destination port number.

Values 0 — 65535

src-ip

Syntax **src-ip** {**eq | neq**} *ip-address*[/*mask*]
no src-ip

Context config>app-assure>group>policy>aqp>entry>match

Description This command specifies a source TCP/UDP address to use as match criteria.

Parameters **eq —** Specifies that a successful match occurs when the flow matches the specified address or prefix.

neq — Specifies that a successful match occurs when the flow does not match the specified address or prefix.

ip-address — Specifies a valid IPv4 unicast address.

mask — Specifies the length of the IP address prefix.

src-port

Syntax **src-port** {**eq | neq**} *port-num*
src-port {**eq | neq**} **range** *start-port-num end-port-num*
no src-port

Context config>app-assure>group>policy>aqp>entry>match

Description This command specifies a source IP port or source range to use as match criteria.

The **no** form of the command removes the parameters from the configuration.

Parameters **eq —** Specifies that a successful match occurs when the flow matches the specified port.

neq — Specifies that a successful match occurs when the flow does not match the specified port.

port-num — Specifies the source port number.

Values 0 — 65535

start-port-num end-port-num — Specifies the start or end source port number.

Values 0 — 65535

traffic-direction

Syntax **traffic-direction** {**subscriber-to-network** | **network-to-subscriber** | **both**}

Context config>app-assure>group>policy>aqp>entry>match

Description This command specifies the direction of traffic where the AQP match entry will be applied.

To use a policer action with the AQP entry the match criteria must specify a traffic-direction of either subscriber-to-network or network-to-subscriber.

Default both

Parameters **subscriber-to-network —** Traffic from a local subscriber will macth this AQP entry.

network-to-subscriber — Traffic to a local subscriber will match this AQP entry.

both — Combines subscriber-to-network and network-to-subscriber.

APPLICATION SERVICE OPTIONS COMMANDS

characteristic

Syntax **characteristic** *characteristic-name* [**create**]
no characteristic *characteristic-name*

Context config>app-assure>group>policy>aso

Description This command creates the characteristic of the application service options.

The **no** form of the command deletes characteristic option. To delete a characteristic, it must not be referenced by other components of application assurance.

Default none

Parameters *characteristic-name* — Specifies a string of up to 32 characters uniquely identifying this characteristic.

create — Mandatory keywork used to create when creating a characteristic. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

default-value

Syntax **default-value** *value-name*
no default-value

Context config>app-assure>group>policy>aso>char

Description This command assigns one of the characteristic values as default.

When a default value is specified, app-profile entries that do not explicitly include this characteristic inherit the default value and use it as part of the AQP match criteria based on that app-profile.

A default-value is required for each characteristic. This is evaluated at commit time.

The **no** form of the command removes the default value for the characteristic.

Default none

Parameters *value-name* — Specifies the name of an existing characteristic value.

value

Syntax [**no**] **value** *value-name*

Context config>app-assure>group>policy>aso>char

Description This command configures a characteristic value.

The **no** form of the command removes the value for the characteristic.

Default none

Parameters *value-name* — Specifies a string of up to 32 characters uniquely identifying this characteristic value.

CUSTOM PROTOCOL COMMANDS

custom-protocol

Syntax **custom-protocol** *custom-protocol-id* **ip-protocol-num** *protocol-id* [**create**]
custom-protocol *custom-protocol-id*
no custom-protocol *custom-protocol-id*

Context config>app-assure>group>policy

Description This command creates and enters configuration context for custom protocols. Custom protocols allow the creation of TCP and UDP-based custom protocols (based on the *ip-protocol-num* option) that employ pattern-match at offset in protocol signature definition.

Operator-configurable custom-protocols are evaluated ahead of any Alcatel-Lucent provided protocol signature in order of **custom-protocol-id** (the lower ID is matched first in case of flow matching multiple custom-protocols) within the context the protocol is defined.

Custom protocols must be created before they can be used in application definition but do not have to be enabled. To reference a custom protocol in application definition, or any other CLI configuration one must use protocol name that is a concatenation of “custom_” and <custom-protocol-id>, (for example custom_01, custom_02 ... custom_10, etc.). This concatenation is also used when reporting custom protocol statistics.

Parameters *custom-protocol-id* — Specifies the index into the protocol list that defines a custom protocol for application assurance.

Values 1 — 10

protocol-id — Specifies the IP protocol number to match against for the custom protocol.

Values 0 — 255, Protocol numbers accepted in DHB,
keywords:none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp
* - udp/tcp wildcard

create — Mandatory keyword used when creating custom protocol. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

expression

Syntax **expression** *expr-index* **eq** *expr-string* **offset** *payload-octet-offset* **direction** direction
no expression expr-index

Context config>app-assure>group>policy>custom-protocol

Description This command configures an expression string value for pattern-based custom protocols match. A flow matches a custom protocol if the specified string is found at an offset of a TCP/UDP of the first payload packet.

Options:

client-to-server — A pattern will be matched against a flow from a TCP client.

server-to-client — A pattern will be matched against a flow from a TCP server.

any – A pattern will be matched against a TCP/UDP flow in any direction (towards or from AA subscriber)

The **no** form of this command deletes a specified string expression from the definition.

Parameters *expr-index* — Specifies the expression substring index.

Values 1

expr-string — Denotes a printable ASCII string, up to 16 characters, used to define a custom protocol match. Rules for expr-string characters:

- Must contain printable ASCII characters.
- Must not contain the “double quote” character or the “ ” (space) character on its own.
- Match is case sensitive.
- Must not include any regular expression meta-characters.

The “\” (slash) character is used as an ESCAPE sequence. The following ESCAPE sequences are permitted within the expr-string:

Character to match	expr-string input
Hexidecimal Octet YY	\xYY

Note: An expr-string that uses the '\' (backslash) ESCAPE character which is not followed by a “\” or “\x” and a 2-digit hex octet is not valid.

offset *payload-octet-offset* **—** specifies the offset (in octets) into the protocol payload, where the expr-string match criteria will start.

Values 0 — 127

direction *direction* **—** Specifies the protocol direction to match against to resolve to a custom protocol.

Values client-to-server, server-to-client, any

Statistics Commands

statistics

Syntax **statistics**

Context config>app-assure>group

Description This command enables the context to configure accounting and billing statistics for this AA ISA group.

app-group

Syntax [**no**] **app-group** *app-group-name*

Context config>app-assure>group>statistics

Description This command enables the context to configure accounting and statistics collection parameters per system for application groups of application assurance for a given AA ISA group/partition.

The **no** form of the command removes the application group name.

Default none

Parameters *app-group-name* — Specifies an existing application group name up to 32 characters in length.

aa-sub

Syntax **aa-sub**

Context config>app-assure>group>statistics

Description This command enables the context to configure accounting and statistics collection parameters per application assurance subscribers.

aa-sub-study

Syntax **aa-sub-study** *study-type*

Context config>app-assure>group>statistics

Description This command enables the context to configure accounting and statistics collection parameters per application assurance special study subscribers.

Parameters *study-type* — Specifies special study protocol subscriber stats.

Values application, protocol

application

Syntax [**no**] **application** *application-name*

Context config>app-assure>group>statistics

Description This command enables the context to configure accounting and statistics collection parameters per system for application groups of application assurance for a given AA ISA group/partition.

The **no** form of the command removes the application name.

Default none

Parameters *applicaiton-name* — Specifies an existing application name up to 32 characters in length.

accounting-policy

Syntax **accounting-policy** *acct-policy-id*

Context config>app-assure>group>statistics>app-grp
config>app-assure>group>statistics>app
config>app-assure>group>statistics>protocol
config>app-assure>group>statistics>aa-sub
config>app-assure>group>statistics>aa-sub-study

Description This command specifies the exisiting accounting policy to use for AA. Accounting policies are configured in the **config**>**log**>**accounting-policy** context.

Parameters *acct-policy-id* — Specifies the exisiting accounting policy to use for applications.

Values 1 — 99

protocol

Syntax **protocol**

Context config>app-assure>group>statistics

Description This command enables the context to configure accounting and statistics collection parameters per-system for protocols of application assurance for a given AA ISA group/partition.

aa-sub

Syntax [**no**] **aa-sub** {**esm** *sub-ident-string* | **sap** *sap-id*} | **spoke-sdp** *sdp-id:vc-id*}

Context config>app-assure>group>statistics>aa-sub-study

Description This command adds an existing subscriber identification to a group of special study subscribers (for example, subscribers for which per subscriber statistics and accounting records can be collected for protocols and applications of application assurance).

The **no** form of the command removes the subscriber from the special study subscribers.

Up to 100 subscribers can be configured into the special study group for protocols and up to a 100 potentially different subscribers can be configured into the special study group for applications.

When adding a subscriber to the special study group, accounting records and statistics generation will commence immediately. When removing a subscriber from the group, special study statistics and accounting records for that subscriber in the current interval will be lost.

Default none

Parameters *sub-ident-string* — The name of a subscriber ID. Note that the subscriber does not need to be currently active. Any sub-ident-string will be accepted. When the subscriber becomes active, statistics generation will start automatically at that time.

esm *sub-ident-string* **—** Specifies an existing subscriber identification policy name.

sap *sap-id* **—** Specifies the physical port identifier portion of the SAP definition. Refer to Appendix A: Common CLI Command Descriptions on page 383 for syntax.

spoke-id *sdp-id:vc-id* — Specifies the spoke SDP ID and VC ID.

Values 1 — 17407
1 — 4294967295

collect-stats

Syntax [**no**] **collect-stats**

Context config>app-assure>group>statistics>app-grp
config>app-assure>group>statistics>application
config>app-assure>group>statistics>protocol
config>app-assure>group>statistics>aa-sub
config>app-assure>group>statistics>aa-sub-study

Description This command enables statistic collection within the applicable context.

Default disabled

protocol

Syntax **protocol** *protocol-name*
no protocol

Context config>app-assure>group>statistics>app-sub

Description This command configures protocol signature in the application definition.

The **no** form of the command restores the default (removes protocol from match application defined by this app-filter entry).

Default no protocol

Parameters *protocol-name* — A string of up to 32 characters identifying a predefined protocol signature.

Values Use the **show>application-assurance>protocols** command to display a full list of protocols available based on isa-aa.tim image used with the given release software.

ISA Commands

Application Assurance Group Commands

application-assurance-group

Syntax **application-assurance-group** *application-assurance-group-index* [**create**]
no application-assurance-group *application-assurance-group-index*

Context config>isa

Description This command enables the context to create an application assurance group with the specified system-unique index and enables the context to configure that group's parameters.

The **no** form of the command deletes the specified application assurance group from the system. The group must be shutdown first.

Default none

Parameters *application-assurance-group-index* — Specifies an integer to identify the AA group

Values 1

create — Mandatory keyword used when creating an application assurance group in the ISA context. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

backup

Syntax [**no**] **backup** *mda-id*

Context config>isa>aa-grp

Description This command assigns an AA ISA configured in the specified slot to this application assurance group. The backup module provides the application assurance group with warm redundancy when the primary module in the group is configured. Primary and backup modules have equal operational status and when both module are coming up, the ones that becomes operational first becomes the active module. A module can serve as a backup for multiple AA ISA cards but only one can fail to it at one time.

On an activity switch from the primary module, configurations are already on the backup MDA but flow state information must be re-learned. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is not supported.

Operator is notified through SNMP events when:

- When the AA service goes down (all modules in the group are down) or comes back up (a module in the group becomes active).
- When AA redundancy fails (one of the modules in the group is down) or recovers (the failed module comes back up).

- When an AA activity switch occurred.

The **no** form of the command removes the specified module from the application assurance group.

Default no backup

Parameters *mda-id* — Specifies the card/slot identifying a provisioned module to be used as a backup module.

Values

mda-id:	*slot*/*mda*	
	slot	1 — up to 10 depending on chassis model
	mda	1 — 2

divert-fc

Syntax [**no**] **divert-fc** *fc-name*

Context config>isa>aa-grp

Description This command selects a forwarding class in the system to be diverted to an application assurance engine for this application assurance group. Only traffic to/from subscribers with application assurance enabled is diverted.

To divert multiple forwarding classes, the command needs to be executed multiple times specifying each forwarding class to be diverted at a time.

The **no** form of the command stops diverting of the traffic to an application assurance engine for this application assurance group.

Default no divert-fc

Parameters *fc-name* — Creates a class instance of the forwarding class fc-name.

Values be, l2, af, l1, h2, ef, h1, nc

fail-to-open

Syntax [**no**] **fail-to-open**

Context config>isa>aa-grp

Description This command configures mode of operation during an operational failure of this application assurance group when no application assurance engines are available to service traffic. When enabled, all traffic that was to be inspected will be dropped. When disabled, all traffic that was to be inspected will be forwarded without any inspection as if the group was not configured at all.

Default no fail-to-open

isa-capacity-cost-high-threshold

Syntax **isa-capacity-cost-high-threshold** *threshold*
no isa-capacity-cost-high-threshold

Context config>isa>aa-grp

Description This command configures the ISA-AA capacity cost high threshold.

The **no** form of the command reverts the threshold to the default value.

Default 4294967295

Parameters *threshold* — Specifies the capacity cost high threshold for the ISA-AA group.

Values 0 — 4294967295

isa-capacity-cost-low-threshold

Syntax **isa-capacity-cost-low-threshold** *threshold*
no isa-capacity-cost-low-threshold

Context config>isa>aa-grp

Description This command configures the ISA-AA capacity cost low threshold.

The **no** form of the command reverts the threshold to the default value.

Default 0

Parameters *threshold* — Specifies the capacity cost low threshold for the ISA-AA group.

Values 0 — 4294967295

partitions

Syntax [**no**] **partitions**

Context config>isa>aa-grp

Description This command enables partitions within an ISA-AA group. When enabled, partitions can be created

The **no** form of the command disables partitions within an ISA-AA group.

Default disabled

primary

Syntax [**no**] **primary** *mda-id*

Context config>isa>aa-grp

Description This command assigns an AA ISA module configured in the specified slot to this application assurance group. Primary and backup ISAs have equal operational status and when both ISAs are coming up, the one that becomes operational first becomes the active ISA.

On an activity switch from the primary ISA, all configurations are already on the backup ISA but flow state information must be re-learned. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is not supported.

Operator is notified through SNMP events when:

- When AA service goes down (all ISAs in the group are down) or comes back up (an ISA in the group becomes active)
- When AA redundancy fails (one of the ISAs in the group is down) or recovers (the failed MDA comes back up)
- When an AA activity switch occurred.

The **no** form of the command removes the specified ISA from the application assurance group.

Default no primary

Parameters *mda-id* — Specifies the slot/mda identifying a provisioned AA ISA.

Values mda-id: *slot*/*mda*
slot 1 — up to 10 depending on chassis model
mda 1 — 2

qos

Syntax **qos**

Context config>isa>aa-grp

Description This command enables the context for Quality of Service configuration for this application assurance group.

egress

Syntax **egress**

Context config>isa>aa-grp>qos

Description This command enables the context for IOM port-level Quality of Service configuration for this application assurance group in the egress direction (traffic entering an application assurance engine).

from-subscriber

Syntax **from-subscriber**

Context config>isa>aa-grp>qos>egress

Description This command enables the context for Quality of Service configuration for this application assurance group form-subscriber logical port, traffic entering the system from AA subscribers and entering an application assurance engine.

pool

Syntax **pool** [*pool-name*]
no pool

Context config>isa>aa-grp>qos>egress>from-subscriber
config>isa>aa-grp>qos>egress>to-subscriber
config>isa>aa-grp>qos>ingress

Description This command enables the context to configure an IOM pool as applicable to the specific application assurance group traffic. The user can configure resv-cbs (as percentage) values and slope-policy similarly to other IOM pool commands.

Default default

Parameters *pool-name* — The name of the pool.

Values default

resv-cbs

Syntax **resv-cbs** *percent-or-default*
no resv-cbs

Context config>isa>aa-grp>qos>egress>from-subscriber>pool
config>isa>aa-grp>qos>egress>to-subscriber>pool
config>isa>aa-grp>qos>ingress>pool

Description This command defines the percentage or specifies the sum of the pool buffers that are used as a guideline for CBS calculations for access and network ingress and egress queues. Two actions are accomplished by this command.

- A reference point is established to compare the currently assigned (provisioned) total CBS with the amount the buffer pool considers to be reserved. Based on the percentage of the pool reserved that has been provisioned, the over provisioning factor can be calculated.
- The size of the shared portion of the buffer pool is indirectly established. The shared size is important to the calculation of the instantaneous-shared-buffer-utilization and the average-shared-buffer-utilization variables used in Random Early Detection (RED) per packet slope plotting.

Note that this command does not actually set aside buffers within the buffer pool for CBS reservation. The CBS value per queue only determines the point at which enqueuing packets are subject to a RED slope. Oversubscription of CBS could result in a queue operating within its CBS size and still not able to enqueue a packet due to unavailable buffers. The resv-cbs parameter can be changed at any time.

If the total pool size is 10 MB and the resv-cbs set to 5, the ‘reserved size’ is 500 KB.

The **no** form of this command restores the default value.

Default default (30%)

Parameters *percent-or-default* — Specifies the pool buffer size percentage.

Values 0 — 100, default

slope-policy

Syntax **slope-policy** *name*
no slope-policy

Context config>isa>aa-grp>qos>egress>from-subscriber>pool
config>isa>aa-grp>qos>egress>to-subscriber>pool
config>isa>aa-grp>qos>ingress>pool

Description This command specifies an existing slope policy which defines high and low priority RED slope parameters and the time average factor. The slope policy is defined in the **config**>**qos**>**slope-policy** context.

queue-policy

Syntax **queue-policy** *network-queue-policy-name*
no queue-policy

Context config>isa>aa-grp>qos>egress>from-subscriber
config>isa>aa-grp>qos>egress>to-subscriber
config>isa>aa-grp>qos>ingress

Description This command assigns an IOM network queue policy as applicable to specific application assurance group traffic.

Default default

Parameters *network-queue-policy-name* — The name of the network queue policy defined in the system.

port-scheduler-policy

Syntax **port-scheduler-policy** *port-scheduler-policy-name*
no port-scheduler-policy

Context config>isa>aa-grp>qos>egress>from-subscriber
config>isa>aa-grp>qos>egress>to-subscriber

Description This command assigns an existing port scheduler policy as applicable to the specific application assurance group traffic.

Default default

Parameters *port-scheduler-policy-name* — specifies the name of an existing port scheduler policy.

to-subscriber

Syntax **to-subscriber**

Context config>isa>aa-grp>qos>egress

Description This command enables the context for Quality of Service configuration for this application assurance group to-subscriber logical port, traffic destined to AA subscribers and entering an application assurance engine.

ingress

Syntax **ingress**

Context config>card>mda>network>ingress

Description This command enables the context for MDA-level IOM Quality of Service configuration.

L2TP Network Server (LNS) Commands

lns-group

Syntax **lns-group** *lns-group-id* [**create**]
no lns-group *lns-group-id*

Context config>isa

Description This command configures an LNS group.

mda

Syntax **mda** *mda-id* [**drain**]
no mda *mda-id*

Context config>isa>lns-group

Description This command configures an ISA LNS group MDA.

The no form of the command removes the MDA ID from the LNS group configuration.

Parameters *mda-id* —

Values mda-id: *slot*/*mda*
slot: 1 — 10
mda: 1, 2

drain — Prevents new L2TP sessions being associated with the ISA. If an ISA is removed from the lns-group or if the lns-group be shutdown all associated L2TP sessions will be immediately terminated (and L2TP CDN messages sent to the L2TP peer). View show commands to determine which ISA is terminating which session (**show router l2tp session**).

Network Address Translation (NAT) Commands

nat-group

Syntax **nat-group** *nat-group-id* [**create**]
no nat-group *nat-group-id*

Context config>isa

Description This command configures an ISA NAT group.

The **no** form of the command removes the ID from the configuration.

Default none

Parameters *nat-group* — Specifies the ISA NAT group ID.

Values 1 — 4

active-mda-limit

Syntax **active-mda-limit** *number*
no active-mda-limit

Context config>isa

Description This command configures the ISA NAT group maximum number of MDA.

The **no** form of the command removes the number from the configuration.

Default none

Parameters *number* — Specifies the active MDA limit.

Values 1 — 6

mda

Syntax [**no**] **mda** *mda-id*

Context config>isa>nat-group

Description This command configures an ISA NAT group MDA.

Parameters *mda-id* — Specifies the MDA ID in the *slot/mda* format.

Values slot: 1 — 10

mda: 1 — 2

session-limits

Syntax **session-limits**

Context config>isa>nat-group

Description This command configures the ISA NAT group session limits.

reserved

Syntax **reserved** *num-sessions*
no reserved

Context config>isa>nat-group>session-limits

Description This command configures the number of sessions rper block that will be reserved for prioritized sessions.

Parameters *num-sessions* — Specifies the number of sessions reserved for prioritized sessions.

Values 0 — 4194303

watermarks

Syntax **watermarks high** *percentage* **low** *percentage*
no watermarks

Context config>isa>nat-group>session-limits

Description This command configures the ISA NAT group watermarks.

high *percentage* **—** Specifies the high watermark of the number of sessions for each MDA in this NAT ISA group.

Values 2 — 100

low *percentage* — Specifies the low watermark of the number of sessions for each MDA in this NAT ISA group.

Values 1 — 99

Show Commands

application-assurance-group

Syntax **application-assurance-group** [*aa-group-id* [**load-balance** [**unassigned**]]]

Context show>isa

Description This command displays ISA group information.

Parameters *aa-group-id* — Specifies the AA ISA group ID.

load-balance — Specifies load balancing information.

unassigned — Specifies load balancing unassigned aa-sub information.

Sample Output

```
A:ALU>show>isa# application-assurance-group 1
===============================================================================
ISA Application-assurance-groups
===============================================================================
ISA-AA Group Index   : 1
Description          : Test
Primary ISA-AA       : 2/1 up/active                          (7 subs, 9 saps)
                     : 3/2 up/active                          (6 subs, 8 saps)
Backup ISA-AA        : 1/1 up/standby
Last Active change   : 01/30/2009 20:14:37
Admin State          : Up
Oper State           : Up
Diverted FCs         : be l2
Fail to mode         : fail-to-wire                Partitions     : disabled
QoS
  Egress from subscriber
    Pool             : default
      Reserved Cbs   : 50 percent

      Slope Policy   : aa_spol1
    Queue Policy     : aa_nqpolEgr
    Scheduler Policy : aa_pspFrmSub
  Egress to subscriber
    Pool             : default
      Reserved Cbs   : 50 percent

      Slope Policy   : aa_spol1
    Queue Policy     : aa_nqpolEgr
    Scheduler Policy : aa_pspToSub
===============================================================================
A:ALU>show>isa#


*A:Dut-C# show isa application-assurance-group 84 load-balance
===============================================================================
ISA Application-assurance-group 84
===============================================================================
```

```
load-balance status         : Complete
isa-capacity-cost-threshold : low  0
                            : high 4294967295
-------------------------------------------------------------------------------
                 capacity-cost  aa-sub      aa-sub stats
                                count       count
-------------------------------------------------------------------------------
 3/1             1024           1024        1024
 Mda Limit       NA             65535       2097120
===============================================================================
aa-sub type count for group 84
===============================================================================
                 all         esm         sap         spoke-sdp
-------------------------------------------------------------------------------
 3/1             1024        20          1000        4
 Unassigned      14          2           8           4
===============================================================================
*A:Dut-C#


*A:Dut-C# show isa application-assurance-group 84 load-balance unassigned
===============================================================================
ISA Application-assurance-group 84 unassigned
===============================================================================
type      SvcId      aa-sub                        App-Profile
-------------------------------------------------------------------------------
esm       2          Sub1                          Cost30
esm       50         Sub2                          Cost31
sap       29         2/1/10:527                    Cost29
sap       30         2/1/10:528                    Cost29
sap       31         2/1/10:529                    Cost29
sap       31         2/1/10:530                    Cost29
sap       31         2/1/10:531                    Cost29
sap       32         2/1/10:546                    Cost29
sap       32         2/1/10:547                    Cost29
sap       33         2/1/10:548                    Cost29
spoke     201        199:10                        Cost27
spoke     202        199:17                        Cost10
spoke     202        199:18                        Cost10
spoke     202        199:19                        Cost10
===============================================================================
*A:Dut-C#
```

group

Syntax **group** *aa-group-id* [:*partition-id*]

Context show>app-assure

Description This command enables the context to display application-assurance group information.

Parameters *aa-group-id* — Specifies an AA ISA group ID.

Values 1

partition-id — Specifies a partition within a group.

Values 1 — 65535

aa-sub

Syntax **aa-sub esm** *sub-ident-string* [**snapshot**]
aa-sub sap *sap-id*
aa-sub spoke-id *sdp-id:vc-id* [**snapshot**]

Context show>app-assure>group

Description This command displays per-subscriber statistics.

Parameters **esm** *sub-ident-string* **—** Specifies an existing subscriber identification string.

sap *sap-id* **—** Specifies the physical port identifier portion of the SAP definition. Refer to Appendix A: Common CLI Command Descriptions on page 383 for syntax.

spoke-id *sdp-id:vc-id* — Specifies the spoke SDP ID and VC ID.

Values 1 — 17407
1 — 4294967295

snapshot — Specifies that the statistics retrieved include the sum of the statistics from the previous collection windows, and the statistics for any closed flows since the last collection window.

Sample Output

```
*A:Dut-C#  show application-assurance group 1 aa-sub spoke-sdp 1:1 snapshot applica-
tion count
===============================================================================
Application-Assurance Subscriber 1:1 (spoke-sdp)
Application Statistics (snapshot)
===============================================================================
Application                      Disc Octets          Packets       Flows
-------------------------------------------------------------------------------
Unknown                            0% 0               0             0
===============================================================================
*A:Dut-C#


*A:Dut-C# show application-assurance group 1 aa-sub spoke-sdp 1:1 summary
===============================================================================
Application-Assurance Subscriber Summary (realtime)
===============================================================================
AA-Subscriber       : 1:1 (spoke-sdp)
ISA assigned        : 3/1
App-Profile         : app_prof_D_4
App-Profile divert  : Yes
Capacity cost       : 1
-------------------------------------------------------------------------------
Traffic                  Octets            Packets         Flows
-------------------------------------------------------------------------------
Admitted from subscriber: 0                0               0
Denied from subscriber:   0                0               0
Active flows from subscriber:                              0
Admitted to subscriber:   0                0               0
Denied to subscriber:     0                0               0
Active flows to subscriber:                                0
Total flow duration:      0 seconds
Terminated flows:                                          0
```

```
Short Duration flows:                                        0
Medium Duration flows:                                       0
Long Duration flows:                                         0
-------------------------------------------------------------------------------
Top App-Groups                  Octets            Packets         Flows
-------------------------------------------------------------------------------
None
===============================================================================
*A:Dut-C#
```

aa-sub-list

Syntax **aa-sub-list** [**isa** *mda-id*]

Context show>app-assure>group

Description This command displays aa-subscriber lists.

Parameters **isa** *mda-id* **—** Displays the slot and MDA ID.

Values 1 — 10 (depending on chassis model)
1, 2

Sample Output

```
*A:Dut-C# show application-assurance group 224:10559 aa-sub-list
===============================================================================
Application-Assurance Subscriber List for Group 224:10559
===============================================================================
type      aa-sub                  ISA      App-Profile              divert
                                  assigned
-------------------------------------------------------------------------------
sap       1/1/1:113               3/2      prof_224_10559_1         Yes
sap       1/1/1:241               3/2      prof_224_10559_1         Yes
sap       1/1/1:369               3/2      prof_224_10559_1         Yes
sap       1/1/1:497               3/2      prof_224_10559_1         Yes
sap       1/1/4:113               3/2      prof_224_10559_2         Yes
sap       1/1/4:241               3/2      prof_224_10559_2         Yes
sap       1/1/4:369               3/2      prof_224_10559_2         Yes
sap       1/1/4:497               3/2      prof_224_10559_2         Yes
-------------------------------------------------------------------------------
Total number of aa-subs found               : 8
===============================================================================
*A:Dut-C#
```

```
*A:Dut-C# show application-assurance group 224:10559 aa-sub-list isa 3/2
===============================================================================
Application-Assurance Subscriber List for Group 224:10559, isa 3/2
===============================================================================
type      aa-sub                  ISA      App-Profile              divert
                                  assigned
-------------------------------------------------------------------------------
sap       1/1/1:113               3/2      prof_224_10559_1         Yes
sap       1/1/1:241               3/2      prof_224_10559_1         Yes
sap       1/1/1:369               3/2      prof_224_10559_1         Yes
sap       1/1/1:497               3/2      prof_224_10559_1         Yes
```

```
sap       1/1/4:113                3/2      prof_224_10559_2         Yes
sap       1/1/4:241                3/2      prof_224_10559_2         Yes
sap       1/1/4:369                3/2      prof_224_10559_2         Yes
sap       1/1/4:497                3/2      prof_224_10559_2         Yes
-------------------------------------------------------------------------------
Total number of aa-subs found              : 8
===============================================================================
*A:Dut-C#
```

aa-sub-study

Syntax **aa-sub-study esm** *sub-ident-string* [**snapshot**]
aa-sub-study sap *sap-id*
aa-sub-study spoke-sdp *sdp-id:vc-id* [**snapshot**]

Context show>app-assure>group

Description This command display per-subscriber special study statistics.

Parameters **esm** *sub-ident-string* **—** Specifies an existing subscriber identification string.

sap *sap-id* **—** Specifies the physical port identifier portion of the SAP definition. Refer to Appendix A: Common CLI Command Descriptions on page 383 for syntax.

spoke-id *sdp-id:vc-id* — Specifies the spoke SDP ID and VC ID.

Values 1 — 17407
1 — 4294967295

snapshot — Specifies that the statistics retrieved include the sum of the statistics from the previous collection windows, and the statistics for any closed flows since the last collection window.

app-group

Syntax **app-group** [*app-group-name*] **count** [**detail**]

Context show>app-assure>group>aa-sub
show>app-assure>group

Description This command displays per-application-group statistics. System-wide statistics displayed account for all flows completed and the last internal snapshot of the active flows.

Parameters *app-group-name* — Displays information about the specified application group name.

count — Displays the counters for the application group.

detail — Displays detailed information.

Sample Output

```
A:ALU>show>app-assure>group# app-group count
===============================================================================
App-group Statistics
===============================================================================
```

```
Application Group                Disc Octets          Packets       Flows
-------------------------------------------------------------------------------
File Transfer                     0% 0                0             0
Games                             0% 3865532          4952          144
Infrastructure                    0% 174524           1217          1177
Instant Messaging                 0% 2979117          9930          97
Local Content                     0% 10581539         10942         74
Mail                              0% 57940            346           24
MultiMedia                        0% 76911464         79417         198
NNTP                              0% 0                0             0
Peer to Peer                      0% 10903442         13901         485
Premium Partner                   0% 0                0             0
Remote Connectivity               0% 0                0             0
Server                            0% 1097             8             2
Suspect                          72% 1012             11            11
Tunneling                         0% 19872617         33989         204
Unknown                           0% 5243395          27510         2648
Web                               0% 82135303         91828         2152
-------------------------------------------------------------------------------
A:ALU>show>app-assure>group#


A:ALU>show>app-assure>group# app-group "MultiMedia" count detail
===============================================================================
App-group "MultiMedia" Statistics
===============================================================================
Application Group:
Type                       Octets            Packets         Flows
-------------------------------------------------------------------------------
MultiMedia:
Admitted from subscriber: 193605             1797            23
Denied from subscriber:   0                  0               0
Active flows from subscriber:                                0
Admitted to subscriber:   4835822            3366            23
Denied to subscriber:     0                  0               0
Active flows to subscriber:                                  0
Total flow duration:      433 seconds
Terminated flows:                                            46
Short Duration flows:                                        36
Medium Duration flows:                                       10
Long Duration flows:                                         0
Active subscribers:       0
===============================================================================
A:ALU>show>app-assure>group#
```

application

Syntax **application** [*application-name*] **count** [**detail**]

Context show>app-assure>group>aa-sub
show>app-assure>group
show>app-assure>group>aa-sub-study

Description This command displays per-application statistics. The system-wide statistics displayed account for all flows completed and the last internal snapshot of the active flows.

Subscriber statistics are available for special-study subscribers and account for all completed and active flows at the moment of this statistics request.

Parameters *application-name* — Displays information about the specified application name.

count — Displays counter information.

detail — Displays detailed information.

Sample Output

```
A:ALU-ABC>show>app-assure>group# application count
===============================================================================
Application Statistics
===============================================================================
Application                      Disc Octets          Packets       Flows
-------------------------------------------------------------------------------
...
DHT                                0% 0               0             0
DNS_53                             0% 96781           627           627
DNS_Local                          0% 0               0             0
DNS_Server                         0% 276             3             3
DNS_Suspect                      100% 736             8             8
FTP                                0% 0               0             0
...
-------------------------------------------------------------------------------
A:ALU-ABC>show>app-assure>group#


A:ALU-ABC>show>app-assure>group# application "POP3" count detail
===============================================================================
Application "POP3" Statistics
===============================================================================
    Application:
Type                      Octets            Packets         Flows
-------------------------------------------------------------------------------
    POP3:
Admitted from subscriber: 14095             149             10
Denied from subscriber:   0                 0               0
Active flows from subscriber:                               0
Admitted to subscriber:   30707             128             10
Denied to subscriber:     0                 0               0
Active flows to subscriber:                                 0
Total flow duration:      7 seconds
Terminated flows:                                           20
Active subscribers:       0
A:ALU-ABC>show>app-assure>group#


A:ALU>show>app-assure>group# application "HTTP_Video" count detail
===============================================================================
Application "HTTP_Video" Statistics
===============================================================================
    Application:
Type                      Octets            Packets         Flows
-------------------------------------------------------------------------------
    HTTP_Video:
```

```
Admitted from subscriber: 369528            5404            36
Denied from subscriber:   0                 0               0
Active flows from subscriber:                               1
Admitted to subscriber:   15387734          10629           36
Denied to subscriber:     0                 0               0
Active flows to subscriber:                                 1
Total flow duration:      463 seconds
Terminated flows:                                           72
Short Duration flows:                                       66
Medium Duration flows:                                      6
Long Duration flows:                                        0
Active subscribers:       1
===============================================================================
A:ALU>show>app-assure>group#
```

cflowd

Syntax **cflowd**

Context show>app-assure>group

Description This command enables the context to display cflowd output.

collector

Syntax **collector** [**detail**]

Context show>app-assure>group>cflowd

Description This command enables the context to display cflowd output.

Sample Output

```
A:ALU-A# show application-assurance group 1 cflowd collector
===============================================================================
Application Assurance Cflowd Collectors for group 1
===============================================================================
Host Address        Port  Version   Admin     Oper      Recs Sent
-------------------------------------------------------------------------------
192.168.7.7         2055    10       up        up        0
192.168.7.8         2055    10       up        up        0
-------------------------------------------------------------------------------
Collectors : 2
-------------------------------------------------------------------------------
A:ALU-A#

A:ALU-A# show application-assurance group 1 cflowd collector detail
===============================================================================
Application Assurance Cflowd Collectors for group 1
===============================================================================
Address                     : 192.168.7.7
Port                        : 2055
Description                 : AA Collector 1
Version                     : 10
```

```
Admin State                 : up
Oper State                  : up
Records Sent                : 0
Last Changed                : 07/27/2009 13:36:50

Address                     : 192.168.7.8
Port                        : 2055
Description                 : AA Collector 2
Version                     : 10
Admin State                 : up
Oper State                  : up
Records Sent                : 0
Last Changed                : 07/27/2009 13:37:10
===============================================================================
A:ALU-A#
```

status

Syntax **status**

Context show>app-assure>group>cflowd

Description This command display status information.

Sample Output

```
A:ALU-A# show application-assurance group 1 status [isa 1/2] cflowd
===============================================================================
Application-Assurance Group Cflowd Status
===============================================================================
Cflowd Admin Status  : Enabled
Cflowd Oper Status   : Enabled
-------------------------------------------------------------------------------
Volume :
-------------------------------------------------------------------------------
 Sample Rate          : <Disabled> or <1 in 500 packets>
 Active Flows         : 23102
 Records Reported     : 12345
 Records Dropped      : 10
 Records Per Second   : 45
 Packets Sent         : 1763
 Packets Sent Per Sec : 7
-------------------------------------------------------------------------------
TCP Performance :
-------------------------------------------------------------------------------
 Sample Rate          : <Disabled> or <1 in 1000 flows>
 Active Flows         : 32103
 Flows Not Allocated  : 33
 Records Reported     : 12345678
 Records Dropped      : 100
 Records Per Second   : 456
 Packets Sent         : 2057613
 Packets Sent Per Sec : 76
===============================================================================
A:ALU-A#
```

```
A:ALU-A#show application-assurance group <aa-group-id:[partition]> cflowd status
===============================================================================
Application-Assurance Group:Partition Cflowd Status
===============================================================================
-------------------------------------------------------------------------------
Volume :
-------------------------------------------------------------------------------
 Admin State          : Up
 Records Reported     : 12345
 Records Dropped      : 10
-------------------------------------------------------------------------------
TCP Performance :
-------------------------------------------------------------------------------
 Admin State          : Up
 Flows Not Allocated  : 33
 Records Reported     : 12345678
 Records Dropped      : 100

===============================================================================
A:ALU-A#
```

count

Syntax **count** [**detail**]

Context show>app-assure>group>aa-sub

Description This command displays per-subscriber app-group application and protocol statistics.

Parameters **detail —** Displays detailed information.

Sample Output

```
A:ALU>show>app-assure>group>aa-sub# count
===============================================================================
Application-Assurance Subscriber TestSubscriberName
Application Group, Application and Protocol Statistics
===============================================================================
Application Group                Disc Octets          Packets       Flows
-------------------------------------------------------------------------------
Database                           0% 0               0             0
File Transfer                      0% 27243           169           22
Games                              0% 0               0             0
Infrastructure                     0% 71494           555           515
Instant Messaging                  0% 4947792         25587         411
Local Content                      0% 923             8             2
Mail                               0% 53729           318           22
Mail Server                        0% 0               0             0
MultiMedia                         0% 31670667        33087         142
NNTP                               0% 0               0             0
Peer to Peer                      .45% 11096224       16339         2431
Premium Partner                    0% 0               0             0
Remote Connectivity                0% 15321           171           2
Server                             0% 0               0             0
Suspect                           72% 1012            11            11
Tunneling                          0% 19659289        33535         164
```

```
Unknown                              0% 1945164         6317          287
Web                                  0% 29538078        34873         1022
Web Server                           0% 0               0             0
===============================================================================
Application                      Disc Octets          Packets       Flows
-------------------------------------------------------------------------------
HTTP_Local                           0% 923             8             2
===============================================================================
Protocol                         Disc Octets          Packets       Flows
-------------------------------------------------------------------------------
dns                                  1.8% 40010         277           277
===============================================================================
A:ALU>show>app-assure>group>aa-sub#


A:ALU>show>app-assure>group>aa-sub# count detail
===============================================================================
Application-Assurance Subscriber TestSubscriberName
Application Group, Application and Protocol Statistics
===============================================================================
    Subscriber                       Application Group:
Type                     Octets            Packets         Flows
-------------------------------------------------------------------------------
    TestSubscriberName               Instant Messaging:
Admitted from subscriber: 2558576          12720           229
Denied from subscriber:   0                0               0
Active flows from subscriber:                              0
Admitted to subscriber:   2389216          12867           182
Denied to subscriber:     0                0               0
Active flows to subscriber:                                0
Total flow duration:      2912 seconds
Terminated flows:                                          411
Short Duration flows:                                      387
Medium Duration flows:                                     22
Long Duration flows:                                       2
 ...
    TestSubscriberName               Web:
Admitted from subscriber: 2343429          22806           511
Denied from subscriber:   0                0               0
Active flows from subscriber:                              1
Admitted to subscriber:   56359191         40528           511
Denied to subscriber:     0                0               0
Active flows to subscriber:                                1
Total flow duration:      4783 seconds
Terminated flows:                                          1020
Short Duration flows:                                      989
Medium Duration flows:                                     31
Long Duration flows:                                       0
===============================================================================
    Subscriber                       Application:
Type                     Octets            Packets         Flows
-------------------------------------------------------------------------------
    TestSubscriberName               HTTP_Local:
Admitted from subscriber: 0                0               0
Denied from subscriber:   0                0               0
Active flows from subscriber:                              0
Admitted to subscriber:   0                0               0
Denied to subscriber:     0                0               0
Active flows to subscriber:                                0
Total flow duration:      0 seconds
Terminated flows:                                          0
```

```
Short Duration flows:                                       0
Medium Duration flows:                                      0
Long Duration flows:                                        0
===============================================================================
    Subscriber                          Protocol:
Type                      Octets              Packets          Flows
-------------------------------------------------------------------------------
    TestSubscriberName                  dns:
Admitted from subscriber: 0                   0                0
Denied from subscriber:   0                   0                0
Active flows from subscriber:                                  0
Admitted to subscriber:   0                   0                0
Denied to subscriber:     0                   0                0
Active flows to subscriber:                                    0
Total flow duration:      0 seconds
Terminated flows:                                              0
Short Duration flows:                                          0
Medium Duration flows:                                         0
Long Duration flows:                                           0
===============================================================================
A:ALU>show>app-assure>group>aa-sub#
```

admin

Syntax **admin**

Context show>app-assure>group>policy

Description This command displays the application-assurance policy uncommitted changes.

Sample Output

```
*A:ALA-48>show>app-assure>group>policy# admin
                begin
                app-filter
                    entry 10 create
                        shutdown
                    exit
                exit
                app-qos-policy
                    entry 10 create
                        shutdown
                    exit
                exit
                commit
*A:ALA-48>show>app-assure>group>policy#
```

app-filter

Syntax **app-filter** [*entry-id*]

Context show>app-assure>group>policy

Description This command displays application-assurance policy filter information.

Parameters *entry-id* — Specifies an existing application filter entry.

Values 1 — 65535

app-group

Syntax **app-group** [*app-group-name*]

Context show>app-assure>group>policy

Description This command displays application-assurance policy application group information.

app-profile

Syntax **app-profile** [*app-prof-name*]
app-profile *app-prof-name* **associations**

Context show>app-assure>group>policy

Description This command displays application-assurance policy application profile information.

Parameters *app-prof-name* — Specifies an existing application profile name.

associations — Displays subscriber management associations.

app-qos-policy

Syntax **app-qos-policy** [*entry-id*]

Context show>app-assure>group>policy

Description This command displays application-assurance policy application QoS policy information.

Parameters *entry-id* — Specifies an existing applicatin QoS policy entry id.

Values 1 — 65535

app-service-option

Syntax **app-service-option** [*characteristic-name*]

Context show>app-assure>group>policy

Description This command displays application-assurance policy application service option information.

application

Syntax **application** [*app-name*]

Context show>app-assure>group>policy

Description This command displays application-assurance policy application information.

summary

Syntax **summary**

Context show>app-assure>group>policy

Description This command displays application-assurance policy summary information.

protocol

Syntax **protocol** [*protocol-name*] **count** [**detail**]

Context show>app-assure>group>aa-sub
show>app-assure>group

Description This command displays per-protocol statistics. The system-wide statistics displayed account for all flows completed and the last internal snapshot of the active flows.

Subscriber statistics are available for special study subscribers and account for all completed and active flows at the moment of this statistics request.

Parameters *protocol-name* — Displays information about the specified protocol name.

count — Displays protocol counters.

detail — Displays detailed information.

Sample Output

```
A:ALU>show>app-assure>group# protocol count
===============================================================================
Protocol Statistics
===============================================================================
Protocol                          Disc Octets          Packets       Flows
-------------------------------------------------------------------------------
aim_oscar                           0% 0               0             0
aim_oscar_file_xfer                 0% 0               0             0
aim_oscar_video_voice               0% 0               0             0
aim_toc                             0% 0               0             0
bittorrent                          0% 0               0             0
...


A:ALU>show>app-assure>group# protocol "http_audio" count detail
```

```
===============================================================================
Protocol "http_audio" Statistics
===============================================================================
    Protocol:
Type                      Octets            Packets         Flows
-------------------------------------------------------------------------------
    http_audio:
Admitted from subscriber: 14958             201             2
Denied from subscriber:   0                 0               0
Active flows from subscriber:                               0
Admitted to subscriber:   587590            396             2
Denied to subscriber:     0                 0               0
Active flows to subscriber:                                 0
Total flow duration:      21 seconds
Terminated flows:                                           4
Short Duration flows:                                       4
Medium Duration flows:                                      0
Long Duration flows:                                        0
Active subscribers:       1
===============================================================================
A:ALU>show>app-assure>group#
```

summary

Syntax **summary**

Context show>app-assure>group>aa-sub

Description This command displays a summary of statistics for a specific aa-sub.

Sample Output

```
A:ALU>show>app-assure>group>aa-sub# summary
===============================================================================
Application-Assurance Subscriber Summary
===============================================================================
AA-Subscriber       : TestSubscriberName
ISA assigned        : 3/2
App-Profile         : Power_Profile
App-Profile divert  : Yes

-------------------------------------------------------------------------------
Traffic                   Octets            Packets         Flows
-------------------------------------------------------------------------------
Admitted from subscriber: 7092548           52935           2843
Denied from subscriber:   51160             617             374
Active flows from subscriber:                               12
Admitted to subscriber:   73705675          73538           1453
Denied to subscriber:     0                 0               0
Active flows to subscriber:                                 12
Total flow duration:      12750 seconds
Terminated flows:                                           4646
Short Duration flows:                                       4516
Medium Duration flows:                                      130
Long Duration flows:                                        0
```

```
-------------------------------------------------------------------------------
Top App-Groups                  Octets          Packets         Flows
-------------------------------------------------------------------------------
MultiMedia                      29060053        29961           138
Tunneling                       19659289        33535           164
Web                             14856331        19829           932
===============================================================================
A:ALU>show>app-assure>group>aa-sub#
```

status

Syntax **status** [**isa** *mda-id*] **cflowd**
status [**isa** *mda-id*]
status [**isa** *mda-id*] **detail**
status {**isa** *mda-id*} **qos count**
status {**isa** *mda-id*} **qos pools**

Context show>app-assure>group

Description This command displays system statistics.

Parameters **isa —** Displays information about the specified AA ISA.

cflowd — Displays cflowd status information.

detail — Displays detailed status information.

qos count — Displays information about queue statistics. The **isa** *mda-id* must be specified.

qos pools — Displays information about pool utilization. The **isa** *mda-id* must be specified.

Sample Output

```
A:ALU>show>app-assure>group# status
===============================================================================
Application-assurance Status
===============================================================================
Last time change affecting status: 01/30/2009 20:14:37
Active Subs                     : 1
-------------------------------------------------------------------------------
                        Packets             Octets
-------------------------------------------------------------------------------
Diverted traffic       : 58783              46140537
Diverted discards      : 4                  0
Entered ISA-AAs        : 58784              46140614
Discarded in ISA-AAs   : 60                 4620
Exited ISA-AAs         : 58724              46135994
Returned discards      : 0                  0
Returned traffic       : 58724              46135994
===============================================================================
A:ALU>show>app-assure>group#


A:ALU>show>app-assure>group# status detail
```

```
===============================================================================
Application-assurance Status
===============================================================================
Last time change affecting status: 01/30/2009 20:14:37
Number of Active ISAs            : 2
Flows                            : 2364
Active Flows                     : 41
Flow Setup Rate                  : 2 per second
Traffic Rate                     : 1 Mbps
AA-Subs Downloaded               : 30
Active Subs                      : 1
-------------------------------------------------------------------------------
                         Packets              Octets
-------------------------------------------------------------------------------
Diverted traffic       : 60744                47206604
Diverted discards      : 4                    0
    Congestion         : 0                    0
    Errors             : 4                    N/A
Entered ISA-AAs        : 60745                47206968
Buffered in ISA-AAs    : 0                    0
Discarded in ISA-AAs   : 164                  12759
    Policy             : 164                  12759
    Congestion         : 0                    0
    Errors             : 0                    0
Errors (policy bypass) : 1                    60
Exited ISA-AAs         : 60581                47194209
Returned discards      : 0                    0
    Congestion         : 0                    0
    Errors             : 0                    N/A
Returned traffic       : 60580                47193845
===============================================================================
A:ALU>show>app-assure>group#


A:ALU>show>app-assure>group# status isa 3/2 qos count
===============================================================================
Application-assurance Queue Statistics for ISA-AA Group: 1, isa 3/2
===============================================================================

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

Egress From-Subscriber
     Queue  1               Packets                Octets
     In Profile  forwarded :    0                      0
     In Profile  dropped   :    0                      0
     Out Profile forwarded :    28940                  3767233
     Out Profile dropped   :    0                      0
     Queue  2               Packets                Octets
     In Profile  forwarded :    0                      0
     In Profile  dropped   :    0                      0
     Out Profile forwarded :    0                      0
     Out Profile dropped   :    0                      0

Egress To-Subscriber
     Queue  1               Packets                Octets
     In Profile  forwarded :    0                      0
     In Profile  dropped   :    0                      0
     Out Profile forwarded :    44499                  53066848
     Out Profile dropped   :    0                      0
     Queue  2               Packets                Octets
```

```
     In Profile  forwarded :    0                       0
     In Profile  dropped   :    0                       0
     Out Profile forwarded :    0                       0
     Out Profile dropped   :    0                       0


Ingress From-Subscriber
     Queue  1                 Packets                 Octets
     In Profile  forwarded :    25548                   3361023
     In Profile  dropped   :    0                       0
     Out Profile forwarded :    1                       60
     Out Profile dropped   :    0                       0
     Queue  2                 Packets                 Octets
     In Profile  forwarded :    2921                    365606
     In Profile  dropped   :    0                       0
     Out Profile forwarded :    0                       0
     Out Profile dropped   :    0                       0
     Queue  9                 Packets                 Octets
     In Profile  forwarded :    0                       0
     In Profile  dropped   :    0                       0
     Out Profile forwarded :    0                       0
     Out Profile dropped   :    0                       0
     Queue 10                 Packets                 Octets
     In Profile  forwarded :    0                       0
     In Profile  dropped   :    0                       0
     Out Profile forwarded :    0                       0
     Out Profile dropped   :    0                       0

Ingress To-Subscriber
     Queue  1                 Packets                 Octets
     In Profile  forwarded :    39541                   46899769
     In Profile  dropped   :    0                       0
     Out Profile forwarded :    1                       92
     Out Profile dropped   :    0                       0
     Queue  2                 Packets                 Octets
     In Profile  forwarded :    5050                    6291204
     In Profile  dropped   :    0                       0
     Out Profile forwarded :    0                       0
     Out Profile dropped   :    0                       0
     Queue  9                 Packets                 Octets
     In Profile  forwarded :    0                       0
     In Profile  dropped   :    0                       0
     Out Profile forwarded :    0                       0
     Out Profile dropped   :    0                       0
     Queue 10                 Packets                 Octets
     In Profile  forwarded :    0                       0
     In Profile  dropped   :    0                       0
     Out Profile forwarded :    0                       0
     Out Profile dropped   :    0                       0
===============================================================================
A:ALU>show>app-assure>group#
                                          ^


A:ALU>show>app-assure>group# status isa 3/2 qos pools
===============================================================================
Pool Information
===============================================================================
MDA                 : 3/2
Application         : Net-Ing           Pool Name          : default
Resv CBS            : 50%
```

```
-------------------------------------------------------------------------------
Utilization                   State       Start-Avg    Max-Avg    Max-Prob
-------------------------------------------------------------------------------
High-Slope                    Up                70%        90%         80%
Low-Slope                     Up                50%        75%         80%

Time Avg Factor      : 7
Pool Total           : 40960 KB
Pool Shared          : 20480 KB          Pool Resv          : 20480 KB

High Slope Start Avg : 12288 KB          High slope Max Avg : 16384 KB
Low Slope Start Avg  : 10240 KB          Low slope Max Avg  : 14336 KB

Pool Total In Use    : 0 KB
Pool Shared In Use   : 0 KB              Pool Resv In Use   : 0 KB
WA Shared In Use     : 0 KB

Hi-Slope Drop Prob   : 0                 Lo-Slope Drop Prob : 0
-------------------------------------------------------------------------------
FC-Maps                         Dest     MBS         Depth  A.CIR     A.PIR
 Q-Grp                          Q-Id     CBS                O.CIR     O.PIR
-------------------------------------------------------------------------------
be af l1 h2 ef h1 nc            5/*      20480       0      8000000   20000000
                                1        1280               8000000   Max
be af l1 h2 ef h1 nc            4/*      20480       0      8000000   20000000
                                1        1280               8000000   Max
be af l1 h2 ef h1 nc            3/1      20480       0      8000000   20000000
                                1        1280               8000000   Max
be af l1 h2 ef h1 nc            2/1      20480       0      8000000   20000000
                                1        1280               8000000   Max
be af l1 h2 ef h1 nc            1/1      20480       0      8000000   20000000
                                1        1280               8000000   Max
be af l1 h2 ef h1 nc            5/*      20480       0      8000000   20000000
                                1        1280               8000000   Max
be af l1 h2 ef h1 nc            4/*      20480       0      8000000   20000000
                                1        1280               8000000   Max
...
===============================================================================
Pool Information
===============================================================================
Port                 : 3/2/fm-sub
Application          : Net-Egr           Pool Name          : default
Resv CBS             : 50%
-------------------------------------------------------------------------------
Queue-Groups
-------------------------------------------------------------------------------
Utilization                   State       Start-Avg    Max-Avg    Max-Prob
-------------------------------------------------------------------------------
High-Slope                    Up                70%        90%         80%
Low-Slope                     Up                50%        75%         80%

Time Avg Factor      : 7
Pool Total           : 12288 KB
Pool Shared          : 6144 KB           Pool Resv          : 6144 KB

High Slope Start Avg : 4096 KB           High slope Max Avg : 5120 KB
Low Slope Start Avg  : 3072 KB           Low slope Max Avg  : 4096 KB

Pool Total In Use    : 0 KB
Pool Shared In Use   : 0 KB              Pool Resv In Use   : 0 KB
WA Shared In Use     : 0 KB
```

```
Hi-Slope Drop Prob   : 0                Lo-Slope Drop Prob : 0
-------------------------------------------------------------------------------
FC-Maps                         ID       MBS         Depth  A.CIR     A.PIR
 Q-Grp                          Q-Id     CBS                O.CIR     O.PIR
-------------------------------------------------------------------------------
be af l1 h2 ef h1 nc            3/2/fm-* 8192        0      4000000   10000000
                                1        5120               4000000   5000000
l2                              3/2/fm-* 6144        0      6000000   10000000
                                2        3584               5000000   5000000
===============================================================================
Pool Information
===============================================================================
Port                : 3/2/to-sub
Application         : Net-Egr           Pool Name          : default
Resv CBS            : 50%
-------------------------------------------------------------------------------
Queue-Groups
-------------------------------------------------------------------------------
Utilization                   State       Start-Avg    Max-Avg    Max-Prob
-------------------------------------------------------------------------------
High-Slope                    Up                70%        90%         80%
Low-Slope                     Up                50%        75%         80%

Time Avg Factor     : 7
Pool Total          : 24576 KB
Pool Shared         : 12288 KB          Pool Resv          : 12288 KB

High Slope Start Avg : 8192 KB          High slope Max Avg : 10240 KB
Low Slope Start Avg  : 6144 KB          Low slope Max Avg  : 8192 KB

Pool Total In Use    : 0 KB
Pool Shared In Use   : 0 KB             Pool Resv In Use   : 0 KB
WA Shared In Use     : 0 KB

Hi-Slope Drop Prob   : 0                Lo-Slope Drop Prob : 0
-------------------------------------------------------------------------------
FC-Maps                         ID       MBS         Depth  A.CIR     A.PIR
 Q-Grp                          Q-Id     CBS                O.CIR     O.PIR
-------------------------------------------------------------------------------
be af l1 h2 ef h1 nc            3/2/to-* 16384       0      4000000   10000000
                                1        10240              4000000   Max
l2                              3/2/to-* 12288       0      6000000   10000000
                                2        7168               6000000   Max
===============================================================================
A:ALU>show>app-assure>group#
```

partition

Syntax **partition summary**

Context show>app-assure>group

Description This command displays partition information.

Parameters **summary —** Displays partition summary information.

policer

Syntax **policer** [*policer-name*]
policer summary

Context show>app-assure>group

Description This command displays application-assurance policer information.

Parameters *policer-name* — Displays information about the specified policer.

summary — Displays summarized information about policers on this node.

Sample Output

```
A:ALU-ABC>show>app-assure>group# policer
          policer "100k_policer" type single-bucket-bandwidth granularity subscriber
create
                rate 100
                mbs 10
            exit
            policer "200FlowsDown_Policer" type flow-count-limit granularity sub-
scriber create
                flow-count 200
            exit
           policer "ServerDown_policer" type single-bucket-bandwidth granularity sub-
scriber create
                action priority-mark
                rate 500
                mbs 50
            exit
            policer "ServerUp_policer" type single-bucket-bandwidth granularity sub-
scriber create
                action priority-mark
                rate 500
                mbs 50
            exit
...
           policer "SuspectUp_policer" type single-bucket-bandwidth granularity sub-
scriber create
                rate 100
                mbs 10
            exit
           policer "Video_channel_policer" type single-bucket-bandwidth granularity
subscriber create
                action priority-mark
                rate 2000
                mbs 200
            exit

Number of policers         : 26
A:ALU-ABC>show>app-assure>group#


A:ALU-ABC>show>app-assure>group# policer "P2PAggrBwDown"
            policer "P2PAggrBwDown" type single-bucket-bandwidth granularity system
create
                rate 1000000
                mbs 100000
```

```
            exit
A:ALU-ABC>show>app-assure>group#


A:ALU-ABC>show>app-assure>group# policer summary
System-level single-bucket-bandwidth policers : 3 out of 64
System-level flow-count-limit policers        : 1 out of 64
System-level flow-rate-limit policers         : 1 out of 64
Subscriber-level single-bucket-bandwidth to-subscriber policers
    Base non-subscriber-specific entries      : 1 out of 32
    Worst case                                : 3 out of 32
        occurs with app-profile "Super"
Subscriber-level single-bucket-bandwidth from-subscriber policers
    Base non-subscriber-specific entries      : 1 out of 32
    Worst case                                : 2 out of 32
        occurs with app-profile "Lite"
Subscriber-level flow-count-limit policers
    Base non-subscriber-specific entries      : 0 out of 8
    Worst case                                : 2 out of 8
        occurs with app-profile "Lite"
Subscriber-level flow-rate-limit policers
    Base non-subscriber-specific entries      : 0 out of 8
    Worst case                                : 0 out of 8
A:ALU-ABC>show>app-assure>group#
```

policy

Syntax **policy**

Context show>app-assure>group

Description This command enables the context to display application-assurance policy configuration information.

protocol

Syntax **protocol** [*protocol-name*]
protocol [*protocol-name*] **detail**

Context show>app-assure

Description This command displays application-assurance policy protocols loaded from the isa-aa.tim file.

Parameters *protocol-name* — Displays all protocols from the isa-aa.tim file.

detail — Displays detailed information about the specified protocol name.

Sample Output

```
A:ALU-ABC>show>app-assure# protocol
===============================================================================
Application Assurance Protocols
===============================================================================
                        Protocol : Description
-------------------------------------------------------------------------------
```

```
                        aim_oscar : America Online Oscar Instant Messaging.
                aim_oscar_file_xfer : America Online Oscar File Transfer.
              aim_oscar_video_voice : America Online Oscar Video and Voice
                                      Traffic.
                           aim_toc : America Online Talk to Oscar Instant
                                      Messaging.
                        bittorrent : BitTorrent peer to peer protocol.
...
A:ALU-ABC>show>app-assure#


A:ALU-ABC>show>app-assure# protocol tftp
===============================================================================
Application Assurance Protocols
===============================================================================
                          Protocol : Description
-------------------------------------------------------------------------------
                              tftp : IETF RFC 1350: Trivial File Transfer
                                     Protocol.
===============================================================================
A:ALU-ABC>show>app-assure#
```

version

Syntax **version**

Context show>app-assure

Description This command displays the versions of the isa-aa.tim used by the CPM and the AA ISAs.

Sample Output

```
A:ALU>show>app-assure# version
===============================================================================
Versions of isa-aa.tim in use
===============================================================================
CPM           : TiMOS-M-7.0.R4
1/1           : TiMOS-I-7.0.R1
2/1           : TiMOS-I-7.0.R1
3/2           : TiMOS-I-7.0.R1
===============================================================================
A:ALU>show>app-assure#
```

aa-sub-using

Syntax **aa-sub-using**
aa-sub-using app-profile *app-profile-name*

Context show>service

Description This command displays application subscriber information.

Parameters *app-profile-name* — Specifies the application profile name.

app-profile

Syntax **app-profile** *app-profile-name*

Context show>service>sap-using

Description This command displays information about SAPs using the specified application profile.

Parameters *app-profile-name* — Specifies an existing application profile name created in the **config>app-assure>group>policy** context.

Sample Output

```
*A:ALA-48# show service sap-using app-profile test
===============================================================================
Service Access Point Using Application Profile 'test'
===============================================================================
PortId                          SvcId      Ing.  Ing.    Egr.  Egr.   Adm  Opr
                                           QoS   Fltr    QoS   Fltr
-------------------------------------------------------------------------------
1/1/18:0                        89         1     none    1     none   Up   Down
-------------------------------------------------------------------------------
Number of SAPs : 1
-------------------------------------------------------------------------------
===============================================================================
*A:ALA-48#
```

sdp-using

Syntax **sdp-using** [*sdp-id*[:*vc-id*]|**far-end** *ip-address*]
sdp-using app-profile *app-profile-name*

Context show>service

Description This command displays services using SDP or far-end address options.

Parameters *sdp-id* — Displays only services bound to the specified SDP ID.

Values 1 — 17407

vc-id — The virtual circuit identifier.

Values 1 — 4294967295

far-end *ip-address* **—** Displays only services matching with the specified far-end IP address.

Default Services with any far-end IP address.

app-profile *app-profile-name* **—** Specifies the application profile name.

Tools Commands

group

Syntax **group** *aa-group-id*[:*partition-id*]

Context tools>dump>application-assurance

Description This command dumps application-assurance information within a group/partition.

Parameters **Values** aa-group-id: partion:aa-group-id[:partition-id]
aa-group-id 1 — 255
partition-id 1 — 65535

flow-record-search

Syntax **flow-record-search aa-sub** {**esm** *sub-ident-string* | **sap** *sap-id* | **spoke-sdp** *sdp-id:vc-id*} [**protocol** *protocol-name*] [**application** *app-name*] [**app-group** *app-group-name*] [**flow-status** *flow-status*] [**start-flowid** *start-flowid*] [**max-count** *max-count*] [**search-type** *search-type*] [**url** *file-url*]

Context tools>dump>app-assure>group

Description This command dumps application-assurance flow-records matching the specified criteria for a specific AA subscriber.

Parameters **esm *sub-ident-string* —** Displays flows for the specified subscriber.

sap *sap-id* — Displays flows for the specified SAP.

spoke-sdp *sdp-id:vc-id* — Displays flows for the specified spoke SDP.

protocol *protocol-name* — Displays flows for the specified protocol.

application *app-name* — Displays flows for the specified application name.

app-group *app-group-name* — Displays flows for the specified application group,

flow-status *flow-status* — Displays only flows that are active or closed.

Values active, closed

start-flowid *start-flowid* — Specifies the starting flow ID.

Values 0 — 4294967295

max-count *max-count* — Specifies the maximum count of flows to display.

Values 1— 4294967295

search-type *search-type* — Specifies the level of detail displayed for flows that match the search criteria.

Values default — Displays some per flow information.
count — Displays the number of matching flows.
detail — Displays all per flow information available.

url *file-url* — Specifies the URL for the file to direct the search output to. The file may be local or remote.

Values local-url | remote-url

local-url	[<cflash-id>/][<file-path>]	
	200 chars max, including cflash-id	
	directory length 99 chars max each	
remote-url	[{ftp://|tftp://}<login>:<pswd>@<remote-locn>/][<file-path>]	
	255 chars max	
	directory length 99 chars max each	
remote-locn	[<hostname> | <ipv4-address> | <ipv6-address>]	
	ipv4-address	a.b.c.d
	ipv6-address	x:x:x:x:x:x:x:x[-interface]
		x:x:x:x:x:x:d.d.d.d[-interface]
		x - [0..FFFF]H
		d - [0..255]D
		interface - 32 chars max, for link local addresses
	cflash-id	flash slot ID

flow-record-search

Syntax **flow-record-search isa** *mda-id* [**protocol** *protocol-name*] [**application** *app-name*] [**app-group** *app-group-name*] [**flow-status** *flow-status*] [**start-flowid** *start-flowid*] [**max-count** *max-count*] [**search-type** *search-type*] [**url** *file-url*]

Context tools>dump>app-assure>group

Description This command dumps application-assurance flow-records matching the specified criteria for an ISA.

Parameters ***mda-id*** **—** Displays flows for the specified AA ISA.

protocol *protocol-name* **—** Displays flows for the specified protocol.

application *app-name* **—** Displays flows for the specified application name.

app-group *app-group-name* **—** Displays flows for the specified application group.

flow-status *flow-status* **—** Displays flows for flows that are active or closed.

Values active, closed

start-flowid *start-flowid* **—** Specifies the starting flow ID.

Values 0 — 4294967295

max-count *max-count* **—** Specifies the maximum count of flows to display.

Values 1— 4294967295

search-type *search-type* **—** Specifies the level of detail displayed for flows that match the search criteria.

Values default — Displays some per flow information.
count — Displays the number of matching flows.
detail — Displays all per flow information available.

url *file-url* — Specifies the URL for the file to direct the search output to. The file may be local or remote.

Values local-url | remote-url

local-url	[<cflash-id>/][<file-path>]	
	200 chars max, including cflash-id	
	directory length 99 chars max each	
remote-url	[{ftp://|tftp://}<login>:<pswd>@<remote-locn>/][<file-path>]	
	255 chars max	
	directory length 99 chars max each	
remote-locn	[<hostname> | <ipv4-address> | <ipv6-address>]	
	ipv4-address	a.b.c.d
	ipv6-address	x:x:x:x:x:x:x:x[-interface]
		x:x:x:x:x:x:d.d.d.d[-interface]
		x - [0..FFFF]H
		d - [0..255]D
		interface - 32 chars max, for link local addresses
	cflash-id	flash slot ID

Clear Commands

group

Syntax **group** *aa-group-id* **cflowd**
group *aa-group-id* **statistics**
group *aa-group-id* **status**

Context clear>app-assure

Description This command clears application assurance group statistics or status.

Parameters *aa-group-id* — Clears data for the specified AA ISA group.

cflowd — Clears application assurance cflowd statistics.

statistics — Clears application assurance system and subscriber statistics.

status — Clears application assurance status statistics.

Debug Commands

isa-aa-group

Syntax **isa-aa-group** *aa-group-id* {**all** | **unknown**}
no isa-aa-group *aa-group-id*

Context debug>mirror-source

Description This command configures AA ISAgroup as a mirror source for this mirror service. Traffic is mirrored after AA processing takes place on AA ISAs of the group, therefore, any packets dropped as part of that AA processing are not mirrored.

Parameters **all —** Specifies that all traffic after AA processing will be mirrored.

unknown — Specifies that all traffic during the identification phase (may match policy entry or entries that have mirror action configured) and traffic that had been identified as unknown_tcp or unknown_udp after AA processing will be mirrored

IP Security (IPSec)

In This Section

This section provides an overview of IP Security (IPSec) software features for the IPSec ISA.

Topics in this section include:

- IPSec Overview on page 180
  - → Operational Conditions on page 183
  - → OAM Interactions on page 184
  - → Redundancy on page 184
  - → Statistics Collection on page 185
  - → Security on page 185
  - → Remote Access VPN Concentrator Example on page 186
  - → Video Wholesale Example on page 187

IPSec Overview

This section discusses IP Security (IPSec) features for an IPSec ISA. This ISA is supported on all IOM-2 and IOM-3 cards. This ISA functions as a resource module for the system, providing IPSec tunnelingand encryption functions. The encryption functions provided by this module are applicable for many applications including: encrypted SDPs, video wholesale,site-to-site encrypted tunnel, and remote access VPN concentration.

Following is the architecture of 7750 IPsec implementation example:

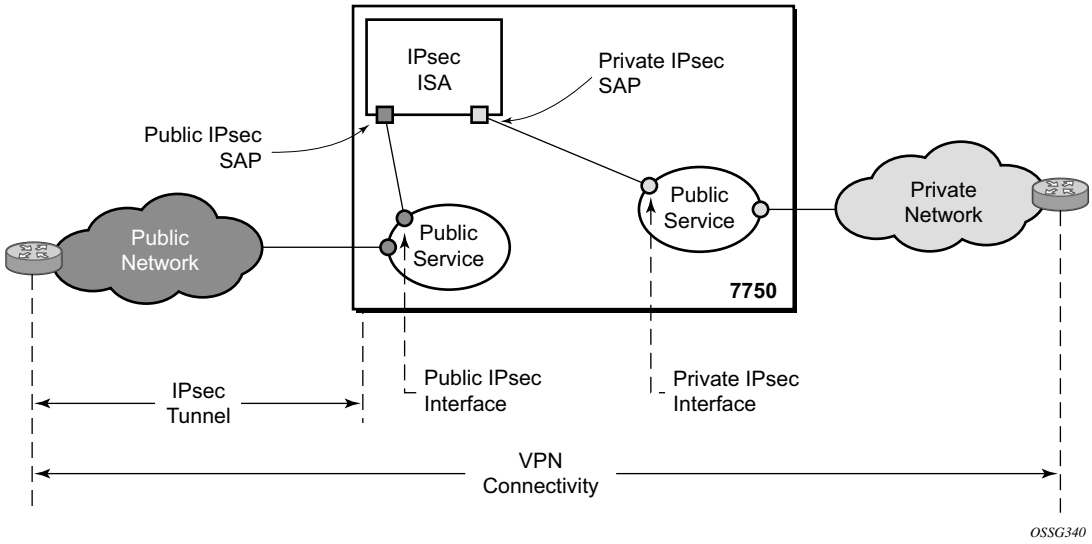

Figure 16: 7750 IPSec Implementation Architecture

In Figure 16, public network represents the “insecure network”, for example, Internet, public network connect to a public service(another name is “front-door service”) inside 7750, which could be an IES or VPRN service; while the private network represent the “secure network”, such as a company’s intranet. Private network connect to a private service, which can only be a VPRN service.

Public and private service are two separated services, the only “bridge” between these two services is the IPsec function. Traffic from public network has to be authenticated and encrypted inside IPsec tunnel to reach private network. In this way, the authenticity/confidentiality/integrity of accessing private network can be enforced.

The IPSec ISA provides a variety of encryption features required to establish bi-directional IPSec tunnels include:

Control Plane:

- Manual Keying
- Dynamic Keying: IKEv1
- IKEv1 Mode :Main and Aggressive
- Authentication: Pre-Shared-Key / xauth with Radius support
- Perfect Forward Secrecy(PFS)
- DPD
- NAT-Traveral
- Security Policy

Data Plane:

- ESP(with authentication) Tunnel mode
- Authentication Algorithm: MD5/SHA1
- Encryption Algorithm: DES/3DES/AES128/AES192/AES256
- DH-Group :1/2/5
- Replay Protection
- N :1 IPsec ISA card redundancy

There are two types of IPsec interfaces and SAPs:

- Public IPsec interface(another name is “front-door interface”): configured in the public service, use to define the subnet for IPsec tunnel local peer/gateway address.
- Public IPsec SAP: configured under public IPsec interface, a logic access point of IPsec ISA card in the public service
- Private IPsec interface: configured in the private service, can be used to define the subnet for the remote access IPsec clients.
- Private IPsec SAP: configured under private IPsec interface, a logic access point of IPsec ISA card in the private service

7750 use normal IP routing to forward IP packet into IPsec ISA card:

- For upstream encrypted traffic: 7750 will forward it to public IPsec interface based on the destination address which is the local address or gateway address of IPsec tunnel. the encrypted traffic will be decrypted inside IPsec ISA card, the tunnel header will be removed, the payload IP packet will be forwarded to the private vrf, and then will be forwarded again based on the destination address of payload IP packet.
- For downstream clear traffic: to route downstream traffic into IPsec tunnel correctly, routes with IPsec tunnel as the next-hop need to be created, these routes can be configured

as static route or be learned via BGP over IPsec tunnel or can be created dynamically during IKEv1 negotiation. After clear traffic is routed into IPsec ISA card, it will be encrypted, a ESP tunnel header will be added, then it will be forward into public vrf, and the will be forwarded again based on the destination of the tunnel header.

7750 IPsec ISA card support N:1 redundancy, up to rout IPsec groups can be configured in the system, each group contain a primary card and a backup card.

Operational Conditions

An IPSec group that is in use cannot be deleted. Changes to the primary ISA are allowed only in when the IPSec group is in a shutdown state. Change to the backup ISA (or the addition of a backup ISA) is allowed at any time unless the ISA is currently active for this IPSec group. When the backup module is active, changing the primary module is allowed without shutting down the IPSec group.

A change to the IPSec transform policy is allowed at any time. The change will not impact tunnels that have been established until they are renegotiated. If the change is required immediately the tunnel must be cleared (reset) for force renegotiation.

A change to the **ike-policy** is allowed at any time. The change will not impact tunnels that have been established until they are renegotiated. If the change is required immediately the tunnel must be cleared (reset) for force renegotiation.

The front-door interface address can be changed at any time (current behavior). If changed, tunnels that were configured to use it will require a configuration change. If the subnet changed the tunnels will be in an operationally down state until their configuration is corrected. The front-door service cannot be deleted while tunnels are configured to use it. A front-door service is the IES or VPRN service that hold the regular interface that connects the node to the public network. A back-door service connects to the private protected service.

IPSec group ID or tag cannot be changed. To remove an IPSec group instance, it must be in a shutdown state (both front-door and back-door).

A change to the security policy is not allowed while a tunnel is active and using the policy.

The tunnel local-gateway-address, peer address, or delivery router parameters cannot be changed while the tunnel is operationally up (shutdown will make it both admin down and operationally down).

A tunnel security policy cannot be changed while the tunnel is operationally up. An IPSec transform policy or ike-policy assignments to a tunnel requires the tunnel to be shutdown.

QoS Interactions

The ISA IPSec can interact with the queuing functions on the IOM through the ingress/egress QoS provisioning in the IES or IP VPN service where the IPSec session is bound. Multiple IPSec sessions can be assigned into a single IES or VPRN service. In this case, QoS defined at the IES or VPRN service level, is applied to the aggregate traffic coming out of or going into the set of sessions assigned to that service.

In order to keep marking relevant in the overall networking design, the ability to translate DSCP bit marking on packets into DSCP bit markings on the IPSec tunneled packets coming out of the tunnel is supported.

OAM Interactions

The ISA IPSec is IP-addressed by an operator-controlled IP on the public side. That IP address can be used in Ping and Traceroute commands and the ISA can either respond or forward the packets to the CPM.

The private side IP address is visible. The status of the interfaces and the tunnels can be viewed using show commands.

Traffic that ingresses or egresses an IES or VPRN service associated with certain IPSec tunnels can be mirrored like other traffic.

Mirroring is allowed per interface (public) or IPSec interface (private) side. A filter mirror is allowed for more specific mirroring.

Redundancy

Every IPSec group can be configured with primary and standby ISAs. An ISA can be used as a standby for multiple IPSec groups. The ISAs are warm standby such that upon failure of the primary the standby resumes operation after the tunnels re-negotiate state. While the standby ISA can be shared by multiple IPSec groups only one IPSec group can fail to a single ISA at one time (no double failure support).

IPSec also supports dead peer detection (DPD).

Statistics Collection

Input and output octets and packets per service queue are used for billing end customers who are on a metered service plan. Since multiple tunnels can be configured per interface the statistics can include multiple tunnels. These can be viewed in the CLI and SNMP.

Reporting (syslog, traps) for authentication failures and other IPSec errors are supported, including errors during IKE processing for session setup and errors during encryption or decryption.

A session log indicates the sort of SA setup when there is a possible negotiation. This includes the setup time, teardown time, and negotiated parameters (such as encryption algorithm) as well as identifying the service a particular session is mapped to, and the user associated with the session.

Security

The ISA IPSec module provides security utilities for IPSec-related service entities that are assigned to interfaces and SAPs. These entities (such as card, isa-ipsec module, and IES or VPRN services) must be enabled in order for the security services to process. The module only listens to requests for security services from configured remote endpoints. In the case of a VPN concentrator application, these remote endpoints could come from anywhere on the Internet. In the cases where a point-to-point tunnel is configured, the module listens only to messages from that endpoint.

Remote Access VPN Concentrator Example

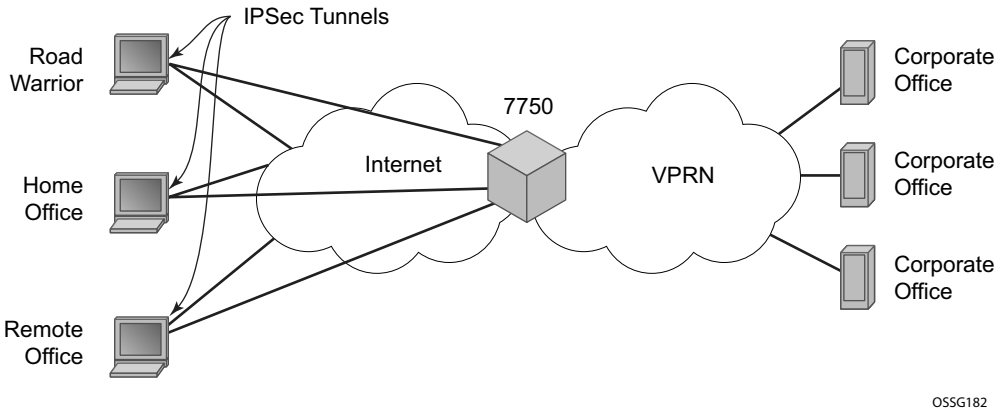

Figure 17: IPSec into VPRN Example

In this application (Figure 17), an IPSec client sets up encrypted tunnel across public network. The 7750 IPSec ISA acts as a concentrator gathering, and terminating these IPSec tunnels into an IES or VPRN service. This mechanism allows as service provider to offer a global VPRN service even if node of the VPRN are on an uncontrolled or insecure portion of the network.

Video Wholesale Example

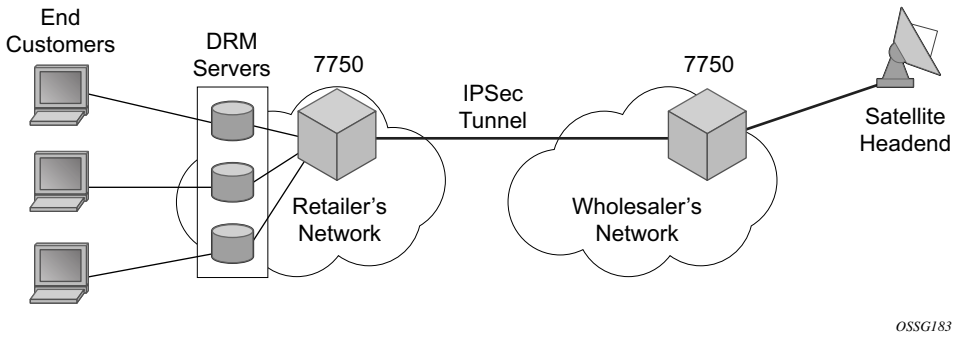

Figure 18: Video Wholesale Configuration

As satellite headend locations can be costly, many municipal and second tier operators cannot justify the investment in their own ground station in order to offer triple play features. However, it is possible for a larger provider or a cooperative of smaller providers to unite and provide a video headend. Each retail subscriber can purchase content from this single station, and receive it over IP. However, encryption is required so the signal cannot be understood if intercepted. A high speed encrypted tunnel is preferred over running two layers of double video protection which is cumbersome and computationally intensive.

Configuring IPSec with CLI

This section provides information to configure IPSec using the command line interface.

Topics in this section include:

- Provisioning an IPSec ISA on page 189
- Ports Used for IPSec on page 190
- Configuring IPSec ISA on page 190
- Configuring Router Interfaces for IPSec on page 191
- Configuring IPSec Parameters on page 192
- Configuring IPSec in Services on page 193

Provisioning an IPSec ISA

An IPSec ISA can only be provisioned on an IOM2. The following output displays a card and ISA configuration.

```
*A:ALA-49>config# info
----------------------------------------------
...
    card 1
        card-type iom2-20g
        mda 1
            mda-type m10-1gb-sfp
        exit
        mda 2
            mda-type isa-ipsec
        exit
    exit
...
----------------------------------------------
*A:ALA-49>config#
```

Ports Used for IPSec

The following output displays a network port and access port configuration for the IPSec ISA.

```
*A:ALA-49>config# info
----------------------------------------------
...
    port 1/1/1
        ethernet
        exit
        no shutdown
    exit
    port 1/1/2
        ethernet
            mode access
            encap-type null
        exit
        no shutdown
    exit
...
----------------------------------------------
*A:ALA-49>config#
```

Configuring IPSec ISA

The following output displays an IPSec group configuration in the ISA context. The **primary** command identifies the card/slot number where the IPSec ISA is the primary module for the IPSec group.

```
*A:ALA-49>config# info
----------------------------------------------
...
    isa
        ipsec-group 1 create
            primary 1/2
            no shutdown
        exit
    exit
...
----------------------------------------------
*A:ALA-49>config#
```

Configuring Router Interfaces for IPSec

The following output displays an interface “internet” configured using the network port (1/1/1).

```
*A:ALA-49>config# info
----------------------------------------------
...
    router
        interface "internet"
            address 10.10.7.118/24
            port 1/1/1
        exit
        interface "system"
            address 10.20.1.118/32
        exit
        autonomous-system 123
    exit
...
----------------------------------------------
*A:ALA-49>config#
```

Configuring IPSec Parameters

The following output displays an IPSec configuration example.

```
*A:ALA-49>config# info
----------------------------------------------
...
    ipsec
        ike-policy 1 create
            ipsec-lifetime 300
            isakmp-lifetime 600
            pfs
            auth-algorithm md5
            dpd interval 10 max-retries 5
        exit
        ipsec-transform 1 create
            esp-auth-algorithm sha1
            esp-encryption-algorithm aes128
        exit
    exit
...
----------------------------------------------
*A:ALA-49>config#
```

Configuring IPSec in Services

The following output displays an IES and VPRN service with IPSec parameters configured.

```
*A:ALA-49>config# info
----------------------------------------------
...
    service
        ies 100 customer 1 create
            interface "ipsec-public" create
                address 10.10.10.1/24
                sap ipsec-1.public:1 create
                exit
            exit
            no shutdown
        exit
       vprn 200 customer 1 create
            ipsec
                security-policy 1 create
                    entry 1 create
                        local-ip 172.17.118.0/24
                        remote-ip 172.16.91.0/24
                    exit
                exit
            exit
           route-distinguisher 1:1
            ipsec-interface "ipsec-private" create
                sap ipsec-1.private:1 create
                tunnel "remote-office" create
                    security-policy 1
                  local-gateway-address 10.10.10.118 peer 10.10.7.91 delivery-service
100
                    dynamic-keying
                        ike-policy 1
                        pre-shared-key "humptydumpty"
                        transform 1
                    exit
                    no shutdown
                exit
            exit
            interface "corporate-network" create
                address 172.17.118.118/24
                sap 1/1/2 create
                exit
            exit
          static-route 172.16.91.0/24 ipsec-tunnel "remote-office"
            no shutdown
        exit
    exit
...
----------------------------------------------
*A:ALA-49>config#
```

IP Security Command Reference

- Hardware Commands on page 195
- IPSec Commands on page 195
- Show Commands on page 198

Configuration Commands

Hardware Commands

config
- — **card** *slot-number*
  - — **mda** *mda-slot*
    - — **isa-ipsec** *mda-type*

IPSec Commands

config
- — **isa**
  - — **ipsec-group** *ipsec-group-id* [**create**]
  - — **no ipsec-group** *ipsec-group-id*
    - — **backup** *mda-id*
    - — **no backup**
    - — **description** *description-string*
    - — **no description**
    - — **primary** *mda-id*
    - — **no primary**
    - — [**no**] **shutdown**

config
- — **ipsec**
  - — **ike-policy** *ike-policy-id* [**create**]
  - — **no ike-policy** *ike-policy-id*
    - — **auth-algorithm** {**md5** | **sha1**}
    - — **no auth-algorithm**
    - — **auth-method** {**psk** | **plain-psk-xauth**}
    - — **no auth-method**
    - — **description** *description-string*
    - — **no description**
    - — **dh-group** {**1** | **2** | **5** | **14** | **15**}
    - — **no dh-group**
    - — **dpd** [**interval** *interval*] [**max-retries** *max-retries*] [**reply-only**]

— **no dpd**
— **encryption-algorithm** {**des** | **3des** | **aes128** | **aes192** | **aes256**}
— **no encryption-algorithm**
— **ike-mode** {**main** | **aggressive**}
— **no ike-mode**
— **ipsec-lifetime** *ipsec-lifetime*
— **no ipsec-lifetime**
— **isakmp-lifetime** *isakmp-lifetime*
— **no isakmp-lifetime**
— **nat-traversal** [**force**] [**keep-alive-interval** *keep-alive-interval*] [**force-keep-alive**]
— **no nat-traversal**
— **pfs** [**dh-group** {**1** | **2** | **5**}]
— **no pfs**

config
— **ipsec**
— **ipsec-transform** *transform-id* [**create**]
— **no ipsec-transform** *transform-id*
— **esp-auth-algorithm** {**null** | **md5** | **sha1**}
— **no esp-auth-algorithm**
— **esp-encryption-algorithm** {**null** | **des** | **3des** | **aes128** | **aes192** | **aes256**}
— **no esp-encryption-algorithm**

config
— **ipsec**
— **tunnel-template** *ipsec template identifier* [**create**]
— **no tunnel-template***ipsec template identifier*
— **description** *description-string*
— **no description**
— **replay-window** {**32** | **64** | **128** | **256** | **512**}
— **no replay-window**
— [**no**] **sp-reverse-route**
— **transform** *transform-id* [*transform-id*...(up to 4 max)]
— **no transform**

config
— **ipsec**
— [**no**] **static-sa** *sa-name*
— **authentication** *md5* | *sha1* {**ascii-key** *ascii-key* **| hex-key** *hex-key*}
— **no authentication**
— **description** *description-string*
— **no description**
— **direction** *inbound* | *outbound* | *bidirectional*
— **no direction**
— **protocol** *ah* | *esp*
— **no protocol**
— **spi** *spi-key*
— **no spi**

config
— **ipsec**
— **lns-group** *lns-group-id* [**create**]
— **no lns-group** *lns-group-id*
— **description** *description-string*
— **no description**
— **mda** *mda-id* [**drain**]

— **no mda** *mda-id*
— [**no**] **shutdown**

Show Commands

show

- **ipsec**
  - **gateway name** *name*
  - **gateway** [**service** *service-id*]
  - **gateway tunnel** [*ip-address:port*]
  - **gateway name** *name* **tunnel** *ip-address:port*
  - **gateway name** *name* **tunnel**
  - **gateway tunnel count**
  - **ike-policy** *ike-policy-id*
  - **ike-policy**
  - **security-policy** *service-id* [*security-policy-id*]
  - **security-policy**
  - **static-sa**
  - **static-sa name** *sa-name*
  - **static-sa spi** *spi*
  - **transform** [*transform-id*]
  - **tunnel** *ipsec-tunnel-name*
  - **tunnel**
  - **tunnel-template** [*ipsec template identifier*]

IPSec Configuration Commands

Generic Commands

description

Syntax **description** *description-string*

Context config>isa>ipsec-group
config>isa

Description This command creates a text description which is stored in the configuration file to help identify the content of the entity.

The **no** form of the command removes the string from the configuration.

Default **none**

Parameters *string* — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

shutdown

Syntax [**no**] **shutdown**

Context config>isa>aa-group
config>isa

Description This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

The **shutdown** command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Hardware Commands

isa-ipsec

Syntax **mda-type** *isa-ipsec*
no mda-type

Context config>card>mda

Description This command provisions an adaptor into an MDA position on an IOM slot. The ISA IPSec module is provisioned into the system in the same manner as all other MDA types. Once an ISA IPSec module is provisioned, independent of it actually existing in the system or the specified slot and ISA position, the ISA IPSec module can be defined as a member of an IPSec module group. These module groups can then be used to assign hardware resources to particular services.

The **no** form of this command removes the module from the configuration. The module must be administratively shut down before it can be deleted from the configuration.

Refer to the 7750 SR OS Interface Guide for further information on command usage and syntax for the ISA IPSec module and other MDA types.

Default No ISA types are configured for any slots by default.

Parameters *isa-ipsec* — Specifies the IPSec module for the slot postion.

ISA Commands

isa

Syntax **isa**

Context config

Description This command enables the context to configure Integrated Services Adapter (ISA) parameters.

ipsec-group

Syntax **ipsec-group** *ipsec-group-id* [**create**]
no ipsec-group *ipsec-group-id*

Context config>isa

Description This command enables the context to create an IPSec group and parameters.

The **no** form of the command deletes the specified IPSec group from the configuration.

Default none

Parameters *ipsec-group-id* — Specifies an integer to identify the IPSec group.

Values 1 — 4

create — Mandatory keyword used when creating an IPSec group in the ISA context. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

backup

Syntax **backup** *mda-id*
no backup

Context config>isa>ipsec-grp

Description This command assigns an ISA IPSec module configured in the specified slot to this IPSec group. The backup module provides the IPSec group with warm redundancy when the primary module in the group is configured. An IPSec group must always have a primary configured.

Primary and backup modules have equal operational status and when both modules are coming up, the one that becomes operational first becomes the active module. An IPSec module can serve as a backup for multiple IPSec groups but the backup can become active for only one ISA IPSec group at a time.

All configuration information is pushed down to the backup MDA from the CPM once the CPM gets notice that the primary module has gone down. This allows multiple IPSec groups to use the same backup module. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is supported.

The operator is notified through SNMP events when:

- When the ISA IPSec service goes down (all modules in the group are down) or comes back up (a module in the group becomes active).
- When ISA IPSec redundancy fails (one of the modules in the group is down) or recovers (the failed module comes back up).
- When an ISA IPSec activity switch took place.

The **no** form of the command removes the specified module from the IPSec group.

Default no backup

Parameters *mda-id* — Specifies the card/slot identifying a provisioned module to be used as a backup module.

Values

mda-id:	*slot*/*mda*	
	slot	1 — up to 10 depending on chassis model
	mda	1 — 2

primary

Syntax **primary** *mda-id*
no primary

Context config>isa>ipsec-grp

Description This command assigns an ISA IPSec module configured in the specified slot to this IPSec group. The backup ISA IPSec provides the IPSec group with warm redundancy when the primary ISA IPSec in the group is configured. Primary and backup ISA IPSec have equal operational status and when both MDAs are coming up, the one that becomes operational first becomes the active ISA IPSec.

All configuration information is pushed down to the backup MDA from the CPM once the CPM gets notice that the primary module has gone down. This allows multiple IPSec groups to use the same

backup module. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is supported.

The operator is notified through SNMP events when:

- When the ISA IPSec service goes down (all modules in the group are down) or comes back up (a module in the group becomes active).
- When ISA IPSec redundancy fails (one of the modules in the group is down) or recovers (the failed module comes back up).
- When an ISA IPSec activity switch took place.

The **no** form of the command removes the specified primary ID from the group's configuration.

Default no primary

Parameters *mda-id* — Specifies the card/slot identifying a provisioned IPSec ISAA.

Internet Key Exchange (IKE) Commands

ipsec

Syntax **ipsec**

Context config

Description This command enables the context to configure Internet Protocol security (IPSec) parameters. IPSec is a structure of open standards to ensure private, secure communications over Internet Protocol (IP) networks by using cryptographic security services.

ike-policy

Syntax **ike-policy** *ike-policy-id* [**create**]
no ike-policy *ike-policy-id*

Context config>ipsec

Description This command enables the context to configured an IKE policy.

The **no** form of the command

Parameters *ike-policy-id* — Specifies a policy ID value to identify the IKE policy.

Values 1 — 2048

auth-algorithm

Syntax **auth-algorithm** {**md5** | **sha1**}
no auth-algorithm

Context config>ipsec>ike-policy

Description The command specifies which hashing algorithm to use for the IKE authentication function.

The **no** form of the command removes the h

Parameters **md5 —** Specifies the hmac-md5 algorithm for authentication.

sha1 — Specifies the hmac-sha1 algorithm for authentication.

auth-method

Syntax **auth-method** {**psk** | **plain-psk-xauth**}
no auth-method

Context config>ipsec>ike-policy

Description This command specifies the authentication method used with this IKE policy.

The **no** form of the command removes the parameter from the configuration.

Default no auth-method

Parameters **psk —** Both client and gateway authenticate each other by a hash derived from a pre-shared secret. Both client and gateway must have the PSK.

plain-psk-xauth — Both client and gateway authenticate each other by pre-shared key and RADIUS.

dh-group

Syntax **dh-group** {**1** | **2** | **5 | 14 | 15**}
no dh-group

Context config>ipsec>ike-policy

Description This command specifies which Diffie-Hellman group to calculate session keys. Three groups are supported with IKE-v1:

- Group 1: 768 bits
- Group 2: 1024 bits
- Group 5: 1536 bits
- Group 14: 2048 bits
- Group 15: 3072 bits

More bits provide a higher level of security, but require more processing.

Default 5

The **no** form of the command removes the Diffie-Hellman group specification.

dpd

Syntax **dpd** [**interval** *interval*] [**max-retries** *max-retries*] [**reply-only**]
no dpd

Context config>ipsec>ike-policy

Description This command controls the dead peer detection mechanism.

The **no** form of the command removes the parameters from the configuration.

Parameters **interval** *interval* **—** Specifies the interval that will be used to test connectivity to the tunnel peer. If the peer initiates the connectivity check before the interval timer it will be reset.

Values 30 seconds

max-retries *max-retries* **—** Specifies the maximum number of retries before the tunnel is removed.

Values 5

reply-only — Specifies to only reply to DPD keepalives. Issuing the command without the reply-only keyword disables the behavior.

Values reply-only

encryption-algorithm

Syntax **encryption-algorithm** {**des | 3des | aes128 | aes192 | aes256**}
no encryption-algorithm

Context config>ipsec>ike-policy

Description This command specifies the encryption algorithm to use for the IKE session.

The **no** form of the command removes the encryption algorithm from the configuration.

Default aes128

Parameters **des —** This parameter configures the 56-bit **des** algorithm for encryption. This is an older algorithm, with relatively weak security. While better than nothing, it should only be used where a strong algorithm is not available on both ends at an acceptable performance level.

3des — This parameter configures the **3-des** algorithm for encryption. This is a modified application of the **des** algorithm which uses multiple **des** operations for more security.

aes128 — This parameter configures the **aes** algorithm with a block size of 128 bits. This is the mandatory impelmentation size for **aes**.

aes192 — This parameter configures the **aes** algorithm with a block size of 192 bits. This is a stronger version of **aes**.

aes256 — This parameter configures the **aes** algorithm with a block size of 256 bits. This is the strongest available version of **aes**.

ike-mode

Syntax **ike-mode** {**main | aggressive** }
no ike-mode

Context config>ipsec>ike-policy

Description This command specifies one of either two modes of operation. IKE version 1 can support main mode and aggressive mode. The difference lies in the number of messages used to establish the session.

The **no** form of the command removes the mode of operation from the configuration.

Default main

Parameters **main —** Specifies identity protection for the hosts initiating the IPSec session. This mode takes slightly longer to complete.

aggresive — Aggressive mode provides no identity protection but is faster.

ipsec-lifetime

Syntax **ipsec-lifetime** *ipsec-lifetime*
no ipsec-lifetime

Context config>ipsec>ike-policy

Description This parameter specifies the lifetime of a phase two SA.

The **no** form of the command reverts the *ipsec-lifetime* value to the default.

Default 3600 (1 hour)

Parameters *ipsec-lifetime* — specifies the lifetime of the phase two IKE key in seconds.

Values 60 — 4294967295

isakmp-lifetime

Syntax **isakmp-lifetime** *isakmp-lifetime*
no isakmp-lifetime

Context config>ipsec>ike-policy

Description This command specifies the lifetime of a phase one SA. ISAKMP stands for Internet Security Association and Key Management Protocol

The **no** form of the command reverts the *isakmp-lifetime* value to the default.

Default 28800

Parameters — Specifies the lifetime of the phase one IKE key in seconds.

Values 60 — 4294967295

nat-traversal

Syntax **nat-traversal** [**force**] [**keep-alive-interval** *keep-alive-interval*] [**force-keep-alive]**
no nat-traversal

Context config>ipsec>ike-policy

Description This command specifies whether NAT-T (Network Address Translation Traversal) is enabled, disabled or in forced mode.

The **no** form of the command reverts the parameters to the default.

Default none

Parameters **force —** Forces to enable NAT-T.

keep-alive-interval *keep-alive-interval* **—** Specifies the keep-alive interval.

Values 10 — 3600 seconds

force-keep-alive — When specified, the keep-alive does not expire.

pfs

Syntax **pfs** [**dh-group** {**1** | **2** | **5**}]
no pfs

Context config>ipsec>ike-policy

Description This command enables perfect forward secrecy on the IPSec tunnel using this policy. PFS provides for a new Diffie-hellman key exchange each time the SA key is renegotiated. After that SA expires, the key is forgotten and another key is generated (if the SA remains up). This means that an attacker who cracks part of the exchange can only read the part that used the key before the key changed. There is no advantage in cracking the other parts if they attacker has already cracked one.

The **no** form of the command disables PFS. If this it turned off during an active SA, when the SA expires and it is time to re-key the session, the original Diffie-hellman primes will be used to generate the new keys.

Default 5

Parameters **dh-group** {**1** | **2** | **5**} **—** Specifies which Diffie-hellman group to use for calculating session keys. More bits provide a higher level of security, but require more processing. Three groups are supported with IKE-v1:

Group 1: 768 bits
Group 2: 1024 bits
Group 5: 1536 bits

static-sa

Syntax [**no**] **static-sa** *sa-name*

Context config>ipsec

Description This command configures an IPsec static SA.

direction

Syntax **direction** *inbound* | *outbound* | *bidirectional*
no direction

Context config>ipsec>static-sa

Description This command configures the direction for an IPsec manual SA. The **no** statement resets to the default value.

Default bidirectional

protocol

Syntax **protocol** *ah* | *esp*
no protocol

Context config>ipsec>static-sa

Description This command configures the security protocol to use for an IPsec manual SA. The **no** statement resets to the default value.

Parameters *ah* — Specifies the Authentication Header protocol.

esp — Specifies the Encapsulation Security Payload protocol.

Default esp

authentication

Syntax **authentication** *md5* | *sha1* {**ascii-key** *ascii-key* **| hex-key** *hex-key*}
no authentication

Context config>ipsec>static-sa

Description This command configures the authentication algorithm to use for an IPsec manual SA. The **no** statement resets to the default value.

Default sha1

Parameters *ascii-key* — Specifies an ASCII key.

hex-key — Specifies a HEX key.

spi

Syntax **spi** *spi-key*
no spi

Context config>ipsec>static-sa

Description This command configures the SPI key value for an IPsec manual SA. The **no** statement resets to the default value.

lns-group

Syntax **lns-group lns-group-id [create]**
no lns-group lns-group-id

Context config>isa

Description This command configures an ISA LNS group.

Parameters *lns-group-id* — Specifies the LNS group ID.

Values 1..4

create — Keyword; specifies the creation of a new LNS group.

mda

Syntax **mda** *mda-id* [**drain**]
no mda *mda-id*

Context config>isa>lns-group

Description This command configures an ISA LNS group MDA.

ipsec-transform

Syntax **ipsec-transform** *transform-id* [**create**]

Context config>ipsec

Description This command enables the context to create an ipsec-transform policy. IPSec transforms policies can be shared. A change to the ipsec-transform is allowed at any time. The change will not impact tunnels that have been established until they are renegotiated. If the change is required immediately the tunnel must be cleared (reset) for force renegotiation.

IPSec transform policy assignments to a tunnel require the tunnel to be shutdown.

The **no** form of the command

Parameters *transform-id* — Specifies a policy ID value to identify the IPSec transform policy.

Values 1 — 2048

create —

esp-auth-algorithm

Syntax **esp-auth-algorithm** {**null** | **md5** | **sha1**}
no esp-auth-algorithm

Context config>ipsec>transform

Description The command specifies which hashing algorithm should be used for the authentication function Encapsulating Security Payload (ESP). Both ends of a manually configured tunnel must share the same configuration parameters for the IPSec tunnel to enter the operational state.

The **no** form of the command disables the authentication.

Parameters **null —** This is a very fast algorithm specified in RFC 2410, which provides no authentication.

md5 — This parameter configures ESP to use the **hmac-md5** algorithm for authentication.

sha1 — This parameter configures ESP to use the **hmac-sha1** algorithm for authentication.

esp-encryption-algorithm

Syntax **esp-encryption-algorithm** {**null** | **des** | **3des** | **aes128** | **aes192** | **aes256**}
no esp-encryption-algorithm

Context config>ipsec>transform

Description This command specifies the encryption algorithm to use for the IPSec session. Encryption only applies to esp configurations. If encryption is not defined esp will not be used.

For IPSec tunnels to come up, both ends need to be configured with the same encryption algorithm.

The **no** form of the command removes the

Default aes128

Parameters **null —** This parameter configures the high-speed null algorithm, which does nothing. This is the same as not having encryption turned on.

des — This parameter configures the 56-bit des algorithm for encryption. This is an older algorithm, with relatively weak security. Although slightly better than no encryption, it should only be used where a strong algorithm is not available on both ends at an acceptable performance level.

3des — This parameter configures the 3-des algorithm for encryption. This is a modified application of the des algorithm which uses multiple des operations to make things more secure.

aes128 — This parameter configures the aes algorithm with a block size of 128 bits. This is the mandatory impelmentation size for aes. As of today, this is a very strong algorithm choice.

aes192 — This parameter configures the aes algorithm with a block size of 192 bits. This is a stronger version of aes.

aes256 — This parameter configures the aes algorithm with a block size of 256 bits. This is the strongest available version of aes.

tunnel-template

Syntax **tunnel-template** *ipsec template identifier* [**create**]
no tunnel-template *ipsec template identifier*

Context config>ipsec

Description This command creates a tunnel template. Up to 2,000 templates are allowed.

Default none

Parameters *ipsec template identifier* — Specifies the template identifier.

Values 1 — 2048

create — Mandatory keyword used when creating a tunnel-template in the IPSec context. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

replay-window

Syntax **replay-window** {**32** | **64** | **128** | **256** | **512**}
no replay-window

Context config>ipsec>tnl-temp

Description This command sets the anti-replay window.

The **no** form of the command removes the parameter from the configuration.

Default no replay-window

Parameters **{32 | 64 | 128 | 256 | 512} —** Specifies the size of the anti-replay window.

sp-reverse-route

Syntax [**no**] **sp-reverse-route**

Context config>ipsec>tnl-temp

Description This command specifies whether the node using this template will accept framed-routes sent by the RADIUS server and install them for the lifetime of the tunnel as managed routes.

The no form of the command disables sp-reverse-route.

Default no sp-reverse-route

transform

Syntax **transform** *transform-id* [*transform-id*...(up to 4 max)]
no transform

Context config>ipsec>tnl-temp

Description This command configures IPSec transform

IPSec Show Commands

gateway

Syntax **gateway name** *name*
gateway [**service** *service-id*]
gateway tunnel [*ip-address:port*]
gateway name *name* **tunnel** *ip-address:port*
gateway name *name* **tunnel**
gateway tunnel count

Context show>ipsec

Description This command displays IPSec gateway information.

Parameters **name** *name* **—** Specifies an IPSec gateway name.

service *service-id* **—** specifies the service ID of the default security service used by the IPSec gateway.

Values 1 — 214748364
svc-name: 64 char max

tunnel *ip-address:port* **—** Specifies to display the IP address and UDP port of the SAP IPSec gateway to the tunnel.

Values port: 0— 65535

count — Specifies to display the number of IPSec gateway tunnels with the **ike-policy>auth-method** command set to **psk**.

ike-policy

Syntax **ike-policy** *ike-policy-id*
ike-policy

Context show>ipsec

Description This command displays

Parameters *ike-policy-id* — Specifies the ID of an IKE policy entry.

Values 1 — 2048

Sample Output

```
*A:ALA-48# show ipsec ike-policy 10
===============================================================================
IPsec IKE policy Configuration Detail
===============================================================================
Policy Id        : 10                  IKE Mode         : main
```

```
DH Group         : Group2               Auth Method      : psk
PFS              : False                PFS DH Group     : Group2
Auth Algorithm   : Sha1                 Encr Algorithm   : Aes128
ISAKMP Lifetime  : 86400                IPsec Lifetime   : 3600
NAT Traversal    : Disabled
NAT-T Keep Alive : 0                    Behind NAT Only  : True
DPD              : Disabled
DPD Interval     : 30                   DPD Max Retries  : 3
Description      : (Not Specified)
===============================================================================
*A:ALA-48#
```

security-policy

Syntax **security-policy** *service-id* [*security-policy-id*]
security-policy

Context show>ipsec

Description This command displays

Parameters *service-id* — Specifies the service-id of the tunnel delivery service.

Values 1 — 214748364
svc-name: 64 char max

security-policy-id — Specifies the IPSec security policy entry that this tunnel will use.

Values 1 — 8192

Sample Output

```
*A:ALA-48>show>ipsec# security-policy 1
===============================================================================
Security Policy Param Entries
===============================================================================
SvcId      Security   Policy     LocalIp             RemoteIp
           PlcyId     ParamsId
-------------------------------------------------------------------------------
1          1          1          0.0.0.0/0           0.0.0.0/0
-------------------------------------------------------------------------------
No. of IPsec Security Policy Param Entries: 1
===============================================================================
*A:ALA-48>show>ipsec#
```

static-sa

Syntax **static-sa**
static-sa name *sa-name*
static-sa spi *spi*

Context show>ipsec

Description This command displays IPsec static-SA information.

Parameters *sa-name* — Specifies the SA name.

Values 32 chars max

spi — Specifies the spi.

Values 256..16383

transform

Syntax **transform** [*transform-id*]

Context show>ipsec

Description This command displays IPSec transforms.

Parameters *transform-id* — Specifies an IPsec transform entry.

Values 1 — 2048

Sample Output

```
*A:ALA-48>config>ipsec# show ipsec transform 1
===============================================================
IPsec Transforms
===============================================================
TransformId    EspAuthAlgorithm    EspEncryptionAlgorithm
---------------------------------------------------------------
1              Sha1                Aes128
---------------------------------------------------------------
No. of IPsec Transforms: 1
===============================================================
*A:ALA-48>config>ipsec#
```

tunnel

Syntax **tunnel** *ipsec-tunnel-name*
tunnel

Context show>ipsec

Description This command displays

Parameters *ipsec-tunnel-name* — Specifies the name of the tunnel up to 32 characters in length.

tunnel-template

Syntax **tunnel-template** *[ipsec template identifier]*

Context show>ipsec

Description This command displays

Parameters *ipsec template identifier* — Displays an existing IPSec tunnel template ID.

Values 1 — 2048

Sample Output

```
*A:ALA-48>config>ipsec# show ipsec tunnel-template 1
===============================================================================
IPSec Tunnel Template
===============================================================================
Id      Trnsfrm1  Trnsfrm2  Trnsfrm3  Trnsfrm4  ReverseRoute      ReplayWnd
-------------------------------------------------------------------------------
1       1         none      none      none      useSecurityPolicy 128
-------------------------------------------------------------------------------
Number of templates: 1
===============================================================================
*A:ALA-48>config>ipsec#
```

Video Services

In This Section

This section describes how to configure the hardware for video services and some basic video services configuration concepts in support of the IPTV video applications.

Topics include:

- Video Services on page 220
  - → Video Groups on page 220
  - → Video SAP on page 221
  - → Video Interface on page 221
  - → Multicast Information Policies on page 222
- Retransmission and Fast Channel Change on page 224
  - → RET and FCC Overview on page 224
  - → Multi-Service ISA Support in the IOM-3 for Video Services on page 235
- Ad Insertion on page 239
  - → Local/Zoned Ad Insertion on page 239

Video Services

Video Groups

When configured in the router, ISA-MS are logically grouped into video groups for video services. A video group allows more than one video ISA to be treated as a single logical entity for a given application where the system performs a load balancing function when assigning tasks to a member of the group. All video group members are “active” members, so there is no concept of a “standby” ISA as in other ISA groups in the 7750 SR and 7450 ESS.

Video groups provide a redundancy mechanism to guard against hardware failure within a group where the system will automatically rebalance tasks to the group excluding the failed ISA. Video groups also pool the processing capacity of all the group members and will increase the application throughput because of the increased packet processing capability of the group. The buffer usage is typically identical for all members of the video group, so increasing the number of members in a group will not increase the scaling numbers for parameters bounded by available buffering, but there will still be the increase in performance gained from the pooled packet processor capacity. A video service must be enabled at the video group level before that service can be used.

A maximum of four ISA-MSs can be supported in a single video group. Note that a given video application may restrict the number of members supported in a video group to a smaller number. Refer to specific sections in this guide for video application additional information.

A maximum of four video groups are supported in a router. There is a chassis limit of eight ISA-MSs per router which constrains the number and members of video groups.

Note: ISA-MS in a single video group cannot be on the same IOM. An IOM can accomodate two ISA-MS modules provided that the ISA-MS are members of different video groups.

Video SAP

The video group logically interfaces to a service instance with a video Service Access Point (SAP). Like a SAP for connectivity services, the video SAP allows the assignment of an ingress and egress filter policy and QoS policy.

Note: Ingress and egress directions for the filter and QoS policy are named based on the perspective of the router which is the opposite perspective of the ISA. An “egress” policy is one that applies to traffic egressing the router and ingressing the ISA. An “ingress” policy is one that applies to traffic ingressing the router and egressing the video. Although potentially confusing, the labeling of ingress and egress for the ISA policies was chosen so that existing policies for connectivity services can be reused on the ISA unchanged.

If no filter or QoS policy is configured, the default policies are used.

One of the key attributes of a video SAP is a video group association. The video SAP’s video group assignment is what determines which video group will service on that video SAP. The video groups configuration determines what video services are available.

Video Interface

A video interface is a logical IP interface associated with a video SAP and provide the IP addressing for a video SAP.

A video interface can have up to 16 IP addresses assigned in a Layer 3 service instance. A video interface can have only one IP address assigned in a Layer 2 service instance.

Multicast Information Policies

Multicast information policies on the 7750 SR and 7450 ESS serve multiple purposes. In the context of a service with video services, the multicast information policy assigned to the service provides configuration information for the multicast channels and defines video policy elements for a video interface.

Note: This section describes the base elements of a multicast information policy in support of a video service. Specific video service features will require additional configuration in the multicast information policy which are described in the sections dedicated to the video feature.

Multicast information policies are named hierarchically structured policies composed of channel bundles which contain channels which contain source-overrides.

- Bundles are assigned a name and contain a collection of channels. Attributes not defined for a named bundle are inherited from the special default bundle named “default”.

```
*A:ALA-48configmcast-mgmtmcast-info-plcy# info
----------------------------------------------
            bundle "default" create
            exit
----------------------------------------------
*A:ALA-48configmcast-mgmtmcast-info-plcy#
```

- Channels are ranges of IP multicast address identified by a start IP multicast address (GG_{start}) and optional end IP multicast address (G_{end}), so the channels encompasses (*,G_{start}) through (*,G_{end}). A channel attribute is inherited from its bundle unless the attribute is explicitly assigned in which case the channel attribute takes precedence.
- A source-override within a channel are IP multicast addresses within the channel with a specific source IP address ($S_{override}$), so the source-override encompass ($S_{override}$,G_{start}) through ($S_{override}$,G_{end}). A source-override attribute is inherited from its channel unless the attribute is explicitly assigned in the source-override channel in which case the source-override channel attribute takes precedence.

For a given IP multicast channel (*,G) or (S,G), the most specific policy element in the hierarchy that matches applies to that channel.

A multicast information policy is assigned to a service instance. For video services, the multicast information policy assigned to the service determines the video group for a given IP multicast channel. When a channel is assigned to a video group, the channel is sent to the video group for buffering and/or processing as appropriate depending on the video services enabled on the video group. If no video group is assigned to a given channel, the channel will still be distributed within the service instance, but no video services will be available for that channel.

In addition to bundles, channels and source-overrides, multicast information policies also include video policies. Video policies define attributes for the video interfaces within the service instance.

Note: Video policy attributes are specific to the video feature and will be covered in detail in the applicable video feature section. Video policies are mentioned here because they are an element of the multicast information policy and provide the link to configuration for a video interface.

Retransmission and Fast Channel Change

RET and FCC Overview

The following sections provide an overview of RET and FCC.

Retransmission

RETransmission (RET) for RTP (RFC3550) is based on a client/server model where the client sends negative acknowledgments (NACKs) using Real-time Transport Control Protocol (RTCP) (RFC4585) to a RET server when the client detects missing sequence numbers n the RTP stream. The RET server which caches the RTP stream, for example in a circular buffer, detects missing sequence numbers in the replies to the NACKs by resending the missing RTP packets as illustrated in Figure 19.

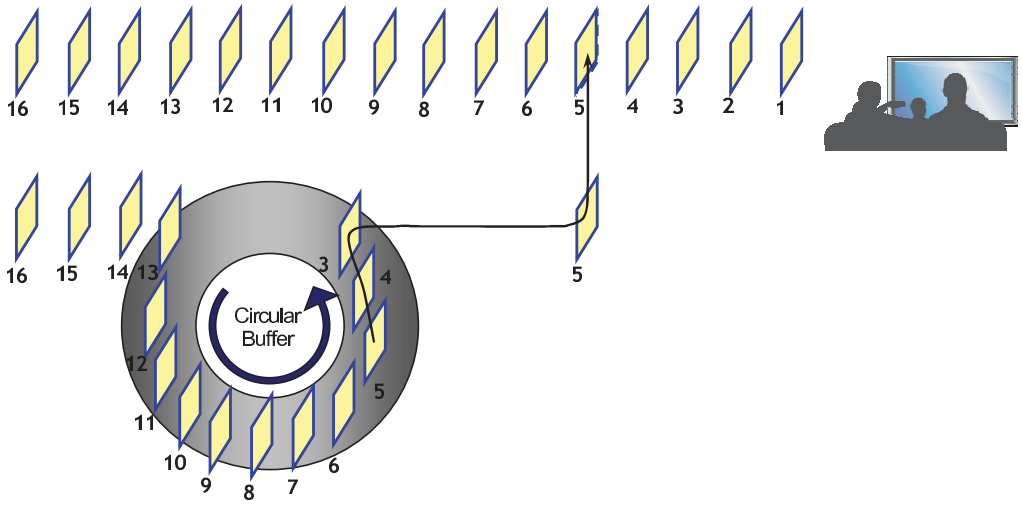

Figure 19: RET Server Retransmission of a Missing Frame

The format of the reply must be agreed upon by the RET client and server and can be an exact copy (Payload Type 33 as defined in RFC 3551, *RTP Profile for Audio and Video Conferences with Minimal Control*) or sent with a different Payload Type using an encapsulating RET header format (RFC 4588, *RTP Retransmission Payload Format*).

RET has been defined in standards organizations by the IETF in the above-noted RFCs and Digital Video Broadcasting (DVB) in “Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks (DVB-IPTV Phase 1.4)” which describes the STB standards.

STBs that have a port of the Alcatel-Lucent RET/FCC Client SDK are an example of a standards-compliant RET Client implementation.

Fast Channel Change (FCC)

FCC is an Alcatel-Lucent method based on a client/server model for providing fast channel changes on multicast IPTV networks distributed over RTP. During a fast channel change, the FCC client initiates a unicast FCC session with the FCC server where the FCC server caches the video stream and sends the channel stream to the FCC client starting at the beginning of a Group of Pictures (GOP). Beginning at a GOP in the past minimizes the visual channel transition on the client/STB, but the FCC unicast stream must be sent at an accelerated rate in the time domain to allow the unicast stream to catch up to the main multicast stream, at which point, the FCC server signals to the client to join the main RTP stream.

Figure 20 illustrates the FCC client and server communication.

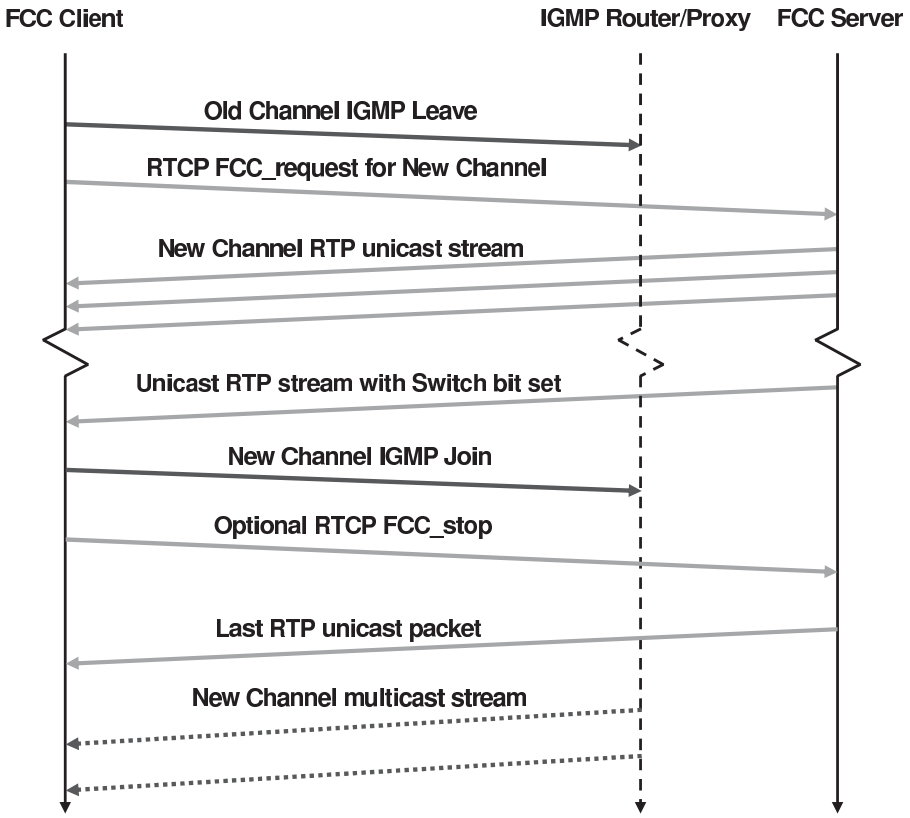

Figure 20: FCC Client/Server Protocol

There are two techniques for compressing the FCC unicast stream in time to allow the unicast session to catch up to the multicast stream: bursting and denting. When bursting, the stream is sent at a rate faster than multicast stream, for example, the stream can be “bursted” at 130% (or 30% over the nominal) multicast rate. “Denting” is a technique where less important video frames are dropped by the FCC server and not sent to the FCC client. Hybrid mode combines bursting and denting.

Bursting is illustrated in Figure 21 and denting is illustrated in Figure 22.

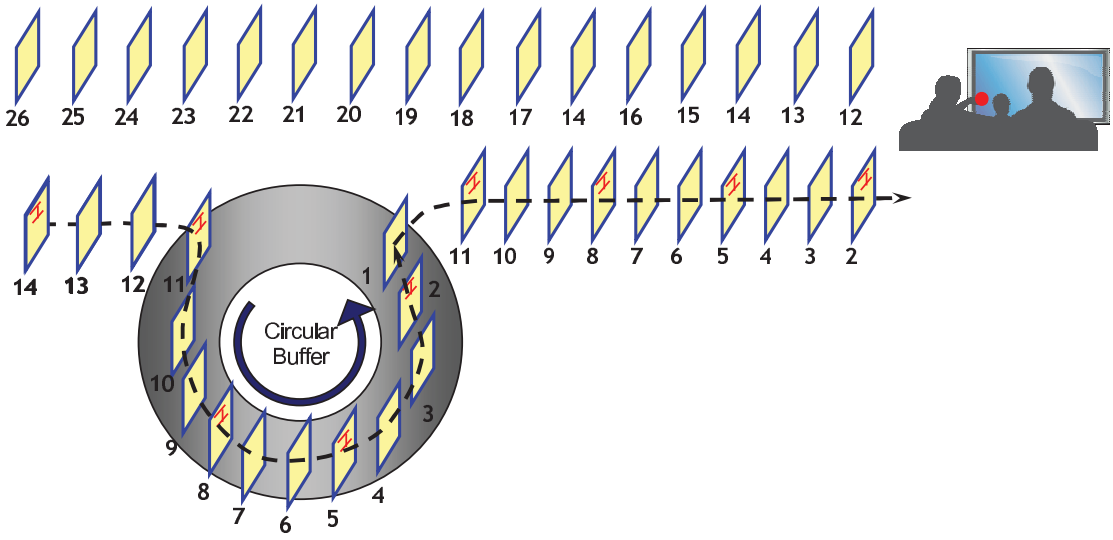

Figure 21: FCC Bursting Sent Faster Than Nominal Rate

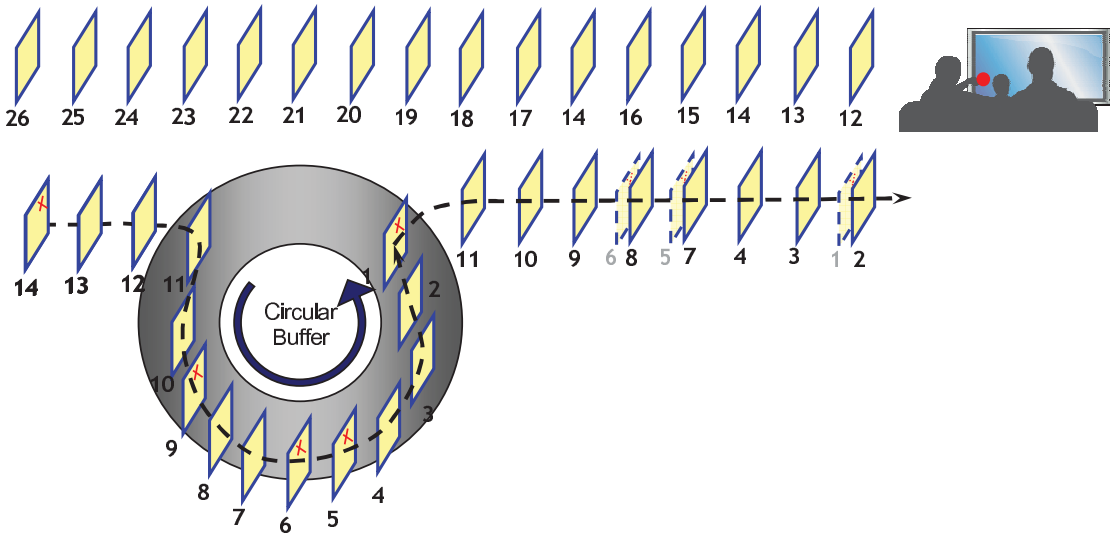

Figure 22: FCC Denting Removing Less Important Frames

When the unicast session has caught up to the multicast session, the FCC server signals to the FCC client to join the main multicast stream. The FCC server will then send the unicast session at a lower rate called the “handover” rate until the unicast session is terminated.

Note: FCC server functionality requires the Alcatel-Lucent 5910 Video Services Appliance (VSA) Re-Wrapper which is used to encapsulate and condition the multicast channel streams into RTP, adding important information in the RTP extension header. Also, the ISA FCC server requires an STB FCC client based on the Alcatel-Lucent FCC/RET Client SDK.

Retransmission Client

The ISA RET client is used in hierarchical RET deployments and performs upstream corrections for missing packets in the RTP multicast stream to ensure that the RET server has all the packets for the stream.

The RET client is supported within a VPLS, IES or VPRN service context as applicable to the platform. The RET client source address is explicitly assigned. In a VPLS, the RET client IP appears to be an IP host within the service, and like a host, the RET client is also configured with a gateway IP address to provide a default route to reach the upstream RET server.

Whenever the RET client receives a retransmission from an upstream RET server, the replies are sent downstream as multicast in the multicast service using Payload Type 33 which is the Payload Type for an original stream.

Whether the RET client is active for a given multicast channel is defined in the multicast information policy where channels are defined. The channel configuration for the RET client within the policy is an explicit enable/disable of the RET client and the IP address and UDP port for the upstream RET server for the channel.

The ISA RET server supports the network model where there are separate service instances for unicast and multicast traffic that are cross-connected and multicast replicated downstream in the network, for example, where an access node provides the multicast service cross connect and replication at the last mile. If there are separate multicast and unicast service instances, the multicast service instance must be configured in the unicast service, and the unicast and multicast services must use the same multicast information policy.

Retransmission Server

The ISA RET server is supported within a VPLS, IES or VPRN service context as applicable to the platform.

Whether the RET server is active for a given multicast channel is defined in the multicast information policy where channels are defined. The channel configuration for the RET server within the policy is an explicit enable/disable of the local RET server (that is, whether the channel should be buffered), the RET buffer size for the channel in the ISA and a channel type (Picture-in-Picture (PIP), Standard Definition (SD) or High Definition (HD)). The RET buffer should be large enough to account for the round trip delay in the network; typically, a few hundred milliseconds is sufficient.

In a VPLS service, a single IP address is assigned to the RET server, and it acts like an IP host within the service.

In an IES or VPRN service, up to 16 IP addresses can be assigned to a video interface.

The video policy within the multicast information policy defines the characteristics for the how the RET server should respond to NACKs received on an IP address. The different characteristics defined in a RET server “profile” are for each channel type (PIP, SD and HD):

- Enable/disable for the RET server (that is, whether requests should be serviced or dropped).
- The RET rate (as a percentage of the nominal channel rate).

Typically, RET replies are sent below line rate because most dropped packets occur in the last mile and sending RET replies at a high rate may compound any last mile drop issues.

The IP address(es) of the RET server is(are) defined in the unicast service instance, whereas the UDP port for the RET server is defined in the “default” bundle in the multicast information policy. The same UDP port is used for all RET server IP addresses that use the particular multicast information policy.

The ISA RET server supports the network model where there are separate service instances for unicast and multicast traffic that are cross-connected and multicast replicated downstream in the network. If there are separate multicast and unicast service instances, the unicast and multicast services must use the same multicast information policy.

Fast Channel Change Server

The ISA FCC server is supported within a VPLS, IES or VPRN service context as applicable to the platform. VPRN services are not supported on the 7450 ESS.

Whether the FCC server is active for a given multicast channel is defined in the multicast information policy where channels are defined. The channel configuration for the FCC server within the policy is an explicit enable/disable of the local FCC server (that is, whether the channel should be buffered) and a channel type PIP, SD or HD. When FCC is enabled, three (3) GOPs are stored in the buffer. the channel also defines an optional fcc tuning parameter called the fcc Minimum Duration which is used by the FCC server to determine which GOP to start the FCC unicast session. If there are too few frames of the current GOP stored in the fcc server buffer (based on number of milliseconds of buffering), the FCC server will start the FCC session from the previous GOP.

In a VPLS service, a single IP address is assigned to the FCC server, and it acts like a IP host within the service.

In an IES or VPRN service, up to 16 IP addresses can be assigned to a video interface.

The Video Policy within the multicast information policy defines the characteristics for the how the FCC server should respond to FCC requests received on an IP address. The different characteristics defined in an FCC server “profile” are for each channel type (PIP, SD and HD):

- Enable/disable for the FCC server (for example, should the requests be serviced or dropped).
- The FCC mode: burst, dent or hybrid.
- The burst rate (as a percentage above the nominal channel rate) for PIP, SD and HD channel types.
- The multicast handover rate (as a percentage of the nominal channel rate) used by the server after it has signaled the client to join the main multicast channel.

Different FCC rates are allowed for each of the channel types because the channel types have different nominal bandwidths. For example, the last mile may only be able to reliably send a 25% burst (above nominal) for HD whereas the equivalent bit rate for SD is a 75% burst. The profiles are designed to provide flexibility.

The IP address of the FCC server is defined in the unicast service instance, whereas the UDP port for the FCC server is defined in the “default” bundle in the multicast information policy. The same UDP port is used for all FCC server IP addresses that use the particular multicast information policy.

The ISA FCC server supports the network model where there are separate service instances for unicast and multicast traffic that are cross-connected and multicast replicated downstream in the

network. If there are separate multicast and unicast service instances, the unicast and multicast services must use the same multicast information policy.

Logging and Accounting for RET and FCC

In previous releases, logging and statistics were maintained for active sessions (RET and FCC).

This feature now provides more permanent logging, statistics and accounting for:

- RET Server sessions stats
- FCC session stats
- ADI events

RET Server Session Stats

For RET Server Stats, the RET session table entries will be sampled and periodically written to XML accounting records.

The basic framework is (requiring a CLI and perhaps some additional tuning) is:

- Session statistics will be written to a record in an XML file on a periodic basis with the sample period being 5 minutes or longer.
- Session statistics are written to a record when a) the session is removed from the session table, b) if the session is exists for more than two write periods.
- All statistics will be the total values (that is, not incremental values across sampling periods).

RET and FCC Server Concurrency

Even though the previous sections discussed the RET server and FCC server as separate entities, the ISA can support RET and FCC servers at the same service at the same time. As such, the configuration commands and operational commands for the services are intermingled. If both the RET server and FCC server are enabled for a given channel, a single buffer is used for caching of the channel.

A maximum bandwidth limit for all server requests can be defined for a given “subscriber” which is equated with the source IP address. Before an ISA server processes a request, the ISA calculates the bandwidth to the subscriber required, and will drop the request if the subscriber bandwidth limit will be exceeded.

The ISA services RET and FCC requests on a first in, first out (FIFO) basis. Before servicing any request, the ISA calculates whether its egress bandwidth can handle the request. If there is insufficient egress bandwidth to handle the service request, the request is dropped. Near the ISA’s egress limits, RET requests will generally continue to be serviced whereas FCC requests will be dropped because RET sessions are generally a fairly small percentage of the nominal rate and FCC sessions are slightly below to above the nominal channel rate.

Prerequisites and Restrictions

This section summarizes some key prerequisites and restrictions for the RET client, RET server and FCC server.

- Both RET and FCC require RTP as the transport stream protocol.
- FCC requires the Alcatel-Lucent 5910 VSA Re-Wrapper.
- FCC requires an implementation of the Alcatel-Lucent 5910 STB Client.
- The multicast information policies must be the same on multicast and unicast services which are cross connected downstream.
- Support for up to four ISA-MSs in a video group
- Only a single IP address and profile are supported within a VPLS service for RET or FCC, so only a single Profile can be supported in a VPLS service.
- Up to 16 IP addresses can be configured for a Layer 3 service video interface (IES or VPRN) with each supporting a distinct profile.
- There can be a maximum of 32 IP addresses across all Layer 3 service video interfaces per chassis.

Multi-Service ISA Support in the IOM-3 for Video Services

In previous releases, the Multi-Service ISA was supported in the iom-20g-b and the iom2-20g for video services. Now, this feature provides support for the Multi-Service ISA when installed in an iom3-xp card on both the 7450 ESS and the 7750 SR.

Prioritization Mechanism for RET vs. FCC

In previous releases, RET and FCC requests are processed with the same priority. Since RET generally has a more direct impact on a subscriber's "quality of experience", service providers are prioritizing RET as a feature over FCC, and for those that want to implement both, the preference is to have a mechanism to prioritize RET over FCC when there is contention for resources.

Now, this feature provides a mechanism to reserve an explicit amount of egress bandwidth for RET for all the ISAs within an video group. If the amount of egress bandwidth is less than the reserved amount, FCC requests are discarded and only RET requests processed. The bandwidth will need to be dynamically adjusted per ISA within the video group if ISAs become operational/non-operational within the group.

RET Features

Statistics ALU SQM MIB Additions

Alcatel-Lucent in Portugal has developed a network management application that does a statistical analysis of retransmissions to analyze the video quality. The following are existing MIB entries.

- TmnxVdoSessionEntry ::= SEQUENCE {
- tmnxVdoSessionSourceAddrType InetAddressType,
- tmnxVdoSessionSourceAddr InetAddress
- tmnxVdoSessionSourcePort InetPortNumber,
- tmnxVdoSessionSSRCId Counter32,
- tmnxVdoSessionUpTime Unsigned32,
- tmnxVdoSessionExpireTime Unsigned32,
- tmnxVdoSessionCName TNamedItem,
- tmnxVdoSessionDestAddrType InetAddressType,
- tmnxVdoSessionDestAddr InetAddress,
- tmnxVdoSessionRxFCCRequests Counter32,
- tmnxVdoSessionTxFCCReplies Counter32,
- tmnxVdoSessionTxFCCPackets Counter32,
- tmnxVdoSessionTxFCCOctets Counter32,
- tmnxVdoSessionRxRTRequests Counter32,
- tmnxVdoSessionTxRTReplies Counter32,
- tmnxVdoSessionTxRTPackets Counter32,
- tmnxVdoSessionTxRTOctets Counter32

The following are new entries:

- Total number of sequences of 10 — total sequences of 2 to 10 lost packets
- Total number of sequences of 20 — total sequences of 11 to 20 lost packets
- Total number of sequences of 30 — total sequences of 21 to 30 lost packets
- Total number of sequences of 40 — total sequences of 31 to 40 lost packets
- Total number of sequences of more ?total sequences of 41 or more lost packets}

RET Server Multicast Tuning Parameters

Downstream RET requests are responded to using multicast when there are a number of identical RET requests with the assumption that there was a loss in the network that affected a number of clients. In this instance, the retransmitted frames will be sent as Payload Type 33 as original packets and not in the RFC 4588, *RTP Retransmission Payload Format*, retransmission format.

The **rt-mcast-reply** command can tune the RET server as to when to use multicast to reply to RET requests have the option to disable multicast responses.

FCC Features

FCC Hybrid Mode Support

There are three modes of operation supported for FCC:

- In burst mode, the unicast FCC traffic is sent faster than nominal rate (bursted above nominal).
- In dent mode, packets are dropped from the unicast FCC stream based on a defined threshold for markings added to the packet that indicate the importance of the packet to the audio/video stream added by the rewrapper.
- Hybrid mode combines both bursting and denting.

Ad Insertion

Local/Zoned Ad Insertion

Transport Stream Ad Splicing

Alcatel-Lucent's Local/Zoned ADI feature allows a 7750 SR with the ISA-MS (the "splicer") to perform ad splicing in an MSTV environment. The splicer is a post-A server transport stream (TS) splicer and can splice into encrypted or unencrypted transport streams. The splicer is positioned between the A-server and the D-server. Figure 23 shows an ad insertion model displaying components.

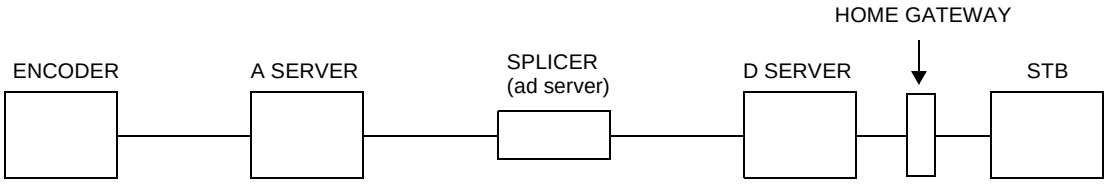

Figure 23: Ad Insertion Model

The ad insertion process is initiated when the splicer detects the SCTE 35 cue signal that identifies the upcoming start and end of the advertising time slot. The splicer communicates with the ad server using SCTE 30 standard messaging and will be instructed by the ad server:

- To take advantage of an ad insertion opportunity or avail and
- Determine the ad to be spliced into the main stream, if applicable.

The ad servers must be configured for ad content to match encoder configurations for video/audio streams. The ad server sends the ad stream to the ad splicer and the ad splicer will switch it into the main stream as dictated by the digital splice points (Figure 24). The ad splicer can splice multiple ads into multiple channels simultaneously.

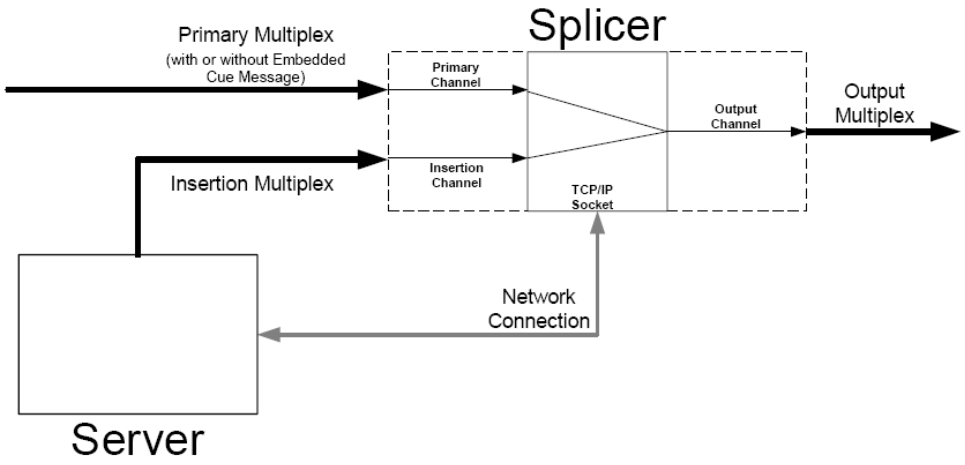

Figure 24: Transport Stream Ad Splicing

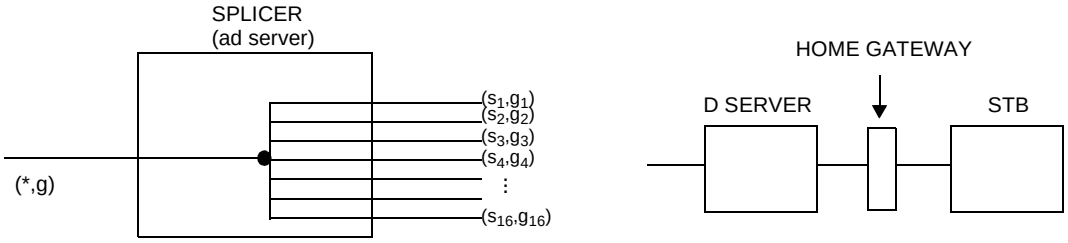

Figure 25: Splicer Model

Note that IPTV encryption and Digital Rights Management (DRM) can be applied to the transport stream payload but not to the transport stream (TS) header which allows a TS splicer to splice into encrypted streams, although the spliced ad content will in all cases be unencrypted. TS splicing does not put any requirements on the middleware platform as ad insertion will be outside the middleware's knowledge and control.

The Figure 26 depicts a TS flow with various MUXed elementary streams (ES) identified by a unique Packet Identifier (PID). The Program Map Table (PMT) is used as the legend to map PID to elementary streams. The digital cue points are also identified by separate unique PID also defined in the PMT that is used by the TS splicer to know when to splice-in and splice-out of the stream. It is important to note that the only important thing that a TS splicer needs are the headers of the TS packets, and the underlying payload of each ES is not needed. This gives the splicer flexibility and makes it agnostic to the ES payload types.

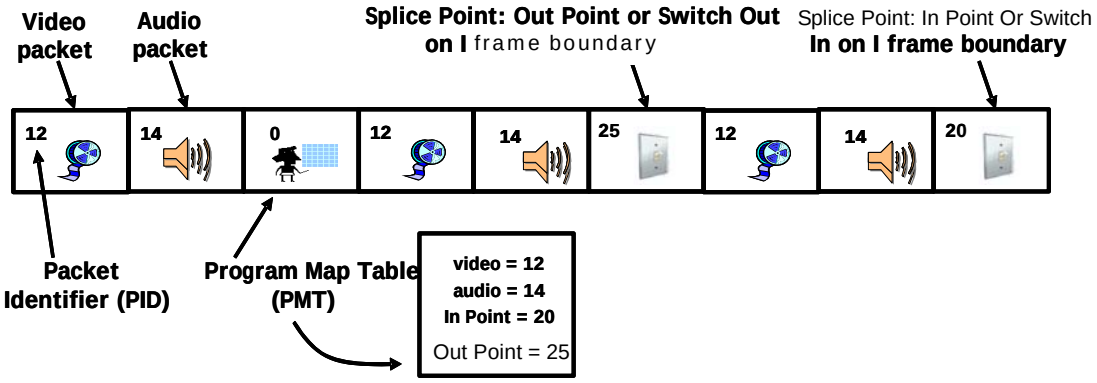

Figure 26: Transport Stream Flow Example

Ad Zones

Within the splicer, zones are created by taking an ingress main channel multicast group, for example (*,G) or (S,G), and creating one or more egress “zone channels” on distinct source-specific multicast (SSM) groups (S1,G1), (S2,G2), etc. Up to 16 zones can be configured for each ingress multicast channel. The group multicast address for the zone channels need not be unique and can actually be the same as the ingress channel, but the SSM sources for the zone channels must be distinct.

Within SCTE 30, the main channel and zone channel are identified by an ASCII string name. These names must all be unique and will be used when the splicer communicates with the ad server.

The input stream can be depicted through the following semantics diagram.

CHANNEL1	→	CHANNEL1_North (S1, G1)
(S, G)	→	CHANNEL1_South (S2, G2)
	→	CHANNEL1_East (S3, G3)
	→	CHANNEL1_West (S4, G4)
	→	CHANNEL1_Central (S5, G5)

where (S,G) is the input main channel stream mapping into five (5) (Sx, Gx) which are zone channel streams.

S1..S16 must be IP addresses in the video interface subnet but not the video interface address itself. This implies that traffic for the zones will be sourced from the ISA-MS.

To facilitate traffic from (S,G) to go to the ISA-MS, a static IGMP (S,G) must be configured on the video interface.

Local/Zoned ADI Prerequisites and Restrictions

This section describes prerequisites and restrictions for the local/zoned ADI feature:

- Network Time Protocol (NTP) is required to keep time synchronized between the ad server and the splicer. The time synchronization system helps keep the splicer and the server within +/-15 ms of each other.
- ADI is only supported within a Layer 3 IES or VPRN service.
- Splicing an SD advertisement into an HD main stream is supported, but splicing of an HD advertisement into an SD is not supported.
- The SCTE 30 connection between the ad server and the splicer must be maintained on separate IP addresses on the splicer within the video service.
- Up to 2 ad servers can be configured for redundancy.
- ADI only supports a single ISA-MS member in a video group.
- Up to 16 zone channels can be configured for a main channel.
- The audio re-ordering value in the multicast information policy must match the audio re-ordering configured on the A Server for reliable audio splicing.
- For best results, the ad should start/end with few frames of muted audio.
- The frequency of IDR frames in the network and ad streams must be less than one IDR frame every 1.3 seconds.
- Only the **splice_insert** command of SCTE-35 cue message is supported. The **splice_immediate** command is not supported.

Configuring Video Service Components with CLI

This section provides information to configure RET/FCC using the command line interface.

Topics in this section include:

- Video Services Overview on page 245
- Configuring RET/FCC Video Features in the CLI on page 255
- Configuring ADI Components with CLI on page 268

Video Services Overview

There can be a maximum of eight ISA-MSs in a given system. The main entities of video configurations are:

- Video group
- Multicast information policy
  - → A video policy to configure video interface properties
  - → Multicast bundles and channels to associate bundles/channels with video groups
- Within a service, configuring a video interfaces and their associations with video groups.

Figure 27 shows various configuration elements and how they are associated by configuration.

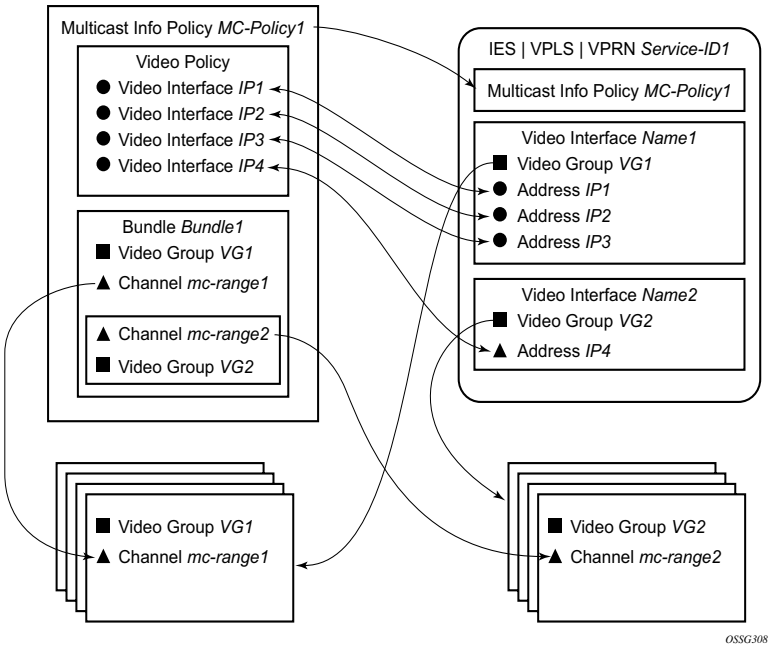

Figure 27: Video Services Configuration Elements

Note that a video interface within a service can have multiple IP address, and their association with the video interfaces within the video policy are based on IP addresses. Support for multiple video interface IP addresses for a given video interface allows video characteristics (burst rate, retransmission format, etc.) for the channels associated with the video interface to be based on the IP address on which the request is received.

Both the bundle/channel configuration and the video interface configuration within the service are associated with a specific video group. If the request is received on a video interface for a channel not serviced by the video group associated with the video interface, the request is invalid and is dropped. Figure 27 displays an example of this is a request for mc-range2 received on IP1, IP2 or IP3. A request for mc-range2 would only be valid on IP4.

As with other multicast information policies, the bundle name default is a special bundle and is reserved for setting of default values. If a video parameter is not explicitly set in a bundle/channel, the value set in the default bundle is used.

Configuring an ISA-MS Module

The ISA-MS hardware has an MDA form factor and is provisioned in the same manner as other MDAs in the **config>card>mda>mda-type** context.

Use the following commands to configure a ISA-MS module.

CLI Syntax:
```
config
    card slot-number
       mda slot-number
          mda-type isa-ms
```

The following output displays an ISA-MS configuration example:

```
*A:Dut-C>config>card# info
----------------------------------------------
        card-type iom2-20g
        mda 1
            mda-type isa-ms
        exit
        mda 2
            mda-type isa-ms
        exit
----------------------------------------------
*A:Dut-C>config>card#
```

Configuring a Video Group

When used for video services, ISA-MSes are logically grouped into video groups that pool the ISA buffering and processing resources into a single logical entity.

Use the following commands to configure a video group.

CLI Syntax:
```
config
    isa
        video-group video-group-id [create]
            description description-string
            primary mda-id
            [no] shutdown
```

The example shown below shows video-group 1 with a single ISA configured in slot 2/MDA 1.

```
*A:Dut-C>config>isa# info
----------------------------------------------------------------------------
        video-group 1 create
            description "Video Group 1"
            primary 7/2
            no shutdown
        exit
----------------------------------------------------------------------------
*A:Dut-C>config>isa#
```

Within the video group configuration, there are specific video application commands to enable features. These commands are described in the configuration examples for the application. Depending on the video application, more than one primary ISA-MS is allowed increasing the egress capacity of the video group.

Note: ISA-MS in a single video group cannot be on the same IOM. An IOM can accommodate two ISA-MS modules provided that the ISA-MS are members of different video groups.

Configuring a Video SAP and Video Interface in a Service

Video features in a VPLS service require the creation of a video SAP and a video interface. A video SAP is similar to other SAPs in the system in that QoS and filter policies can be associated with the SAP on ingress (traffic leaving the ISA and ingressing the system) and egress (traffic leaving system and entering the ISA).

Note that the video SAP is associated with a video group. Channels are also associated with a video group which is what establishes the link between what channels can be referenced through the video SAP. The multicast information policy associated with the service is where the channel to video group association is defined.

For unicast VPLS services that have an associated multicast service that is cross connected downstream of the router, the multicast service needs to be identified by the service ID in the unicast VPLS service.

The video commands for are identical in the IES and VPRN service contexts. The basic IES and VPRN commands are similar to the video commands in the VPLS context and follow the same logic of associating the video SAP with a video group and the multicast information policy defining the channel to video group association.

Another parameter defined for a channel in the multicast information policy that is important for video services is the administrative bandwidth defined for the channel. Many video applications use the bandwidth to determine if sufficient ISA egress bandwidth exists to service or drop a service request.

Use the following commands to configure video service SAP and interface entities.

CLI Syntax:

```
config>service# vpls service-id | vprn service-id
             multicast-info-policy policy-name
                video-interface ip-int-name [create]
                   address <ip-address/mask>
                   description description-string
                   multicast-service service-id
                   [no] shutdown
                   video-sap video-group-id
                      egress
                        filter ip ip-filter-id
                        filter mac mac-filter-id
                        qos egress-qos-policy-id
                      ingress
                        filter ip ip-filter-id
                        filter mac mac-filter-id
                        qos ingress-qos-policy-id
```

```
A:IPTV-SR7>config>service>ies# info
----------------------------------------------
            video-interface "video-100" create
                video-sap 4
                exit
                address 1.1.1.254/8
                address 100.100.0.254/8
                address 101.1.1.254/24
                adi
                    channel 234.4.5.228 source 195.168.9.10 channel-name "228"
                        scte35-action drop
                      zone-channel 234.4.5.228 source 100.100.100.1 adi-channel-name "228-
1"
                    exit
                    scte30
                       ad-server 10.200.14.2
                       local-address control 100.1.1.2 data 100.1.1.3
                    exit
                exit
----------------------------------------------
A:IPTV-SR7>config>service>ies#
```

Basic Multicast Information Policy Configuration

Multicast information policies are used by the video applications to define multicast channel attributes and video policies which contains application-specific configuration for a video interface IP address.

Note that it is within the multicast information policy bundles, channels and source-overrides that a video group is assigned to a channel. The video group association is inherited from the more general construct unless it is explicitly disabled.

The administrative bandwidth for channels at the bundle, channel or source-override level is also defined in the multicast information policy. Video applications use the administrative bandwidth here when a channel rate estimate is needed.

A video policy is defined within the multicast information policy for a specific video interface IP address. The IP address for the video policy is the key value that associates it with a specific video interface IP address within a service associated with overall multicast information policy.

Use the following commands to configure a multicast information policy.

CLI Syntax:

```
config>mcast-management
      multicast-info-policy policy-name [create]
         video-policy
            video-interface ip-address [create]
               hd
                  dent-threshold threshold
                  fcc-burst burst-percentage
                  fcc-server [mode {burst | dent | hybrid}]
                  local-rt-server
                  mc-handover percentage
                  rt-rate rt-burst-percentage
               pip
                  dent-threshold threshold
                  fcc-burst burst-percentage
                  fcc-server [mode {burst | dent | hybrid}]
                  local-rt-server
                  mc-handover percentage
                  rt-rate rt-burst-percentage
               sd
                  dent-threshold threshold
                  fcc-burst burst-percentage
                  fcc-server [mode {burst | dent | hybrid}]
                  local-rt-server
                  mc-handover percentage
                  rt-rate rt-burst-percentage
               subscriber-bw-limit bandwidth
```

Use the following commands to configure a multicast information policy bundle and channel parameters.

CLI Syntax:

```
config>mcast-management
        multicast-info-policy policy-name [create]
           bundle bundle-name [create]
              admin-bw kbps
              bw-activity {use-admin-bw|dynamic [falling-delay sec-
              onds]} [black-hole-rate kbps]
              channel ip-address [ip-address] [create]
                 admin-bw kbps
                 source-override ip-address [create]
                    admin-bw kbps
                    bw-activity {use-admin-bw|dynamic [falling-delay
                    seconds]} [black-hole-rate kbps]
                    video
                       fcc-channel-type {hd | sd | pip}
                       fcc-min-duration time
                       fcc-server [disable]
                       local-fcc-port port
                       local-rt-port port
                       local-rt-server [disable]
                       reorder-audio time
                       rt-buffer-size rt-buffer-size
                       rt-server disable
                       rt-server ip-address port port-num
                       video-group video-group-id
                       video-group disable
                 video
                    fcc-channel-type {hd | sd | pip}
                    fcc-min-duration time
                    fcc-server [disable]
                    local-fcc-port port
                    local-rt-port port
                    local-rt-server [disable]
                    reorder-audio time
                    rt-buffer-size rt-buffer-size
                    rt-server disable
                    rt-server ip-address port port-num
                    video-group video-group-id
                    video-group disable

              video
                 fcc-channel-type {hd|sd|pip}
                 fcc-min-duration time
                 fcc-server
                 local-fcc-port port-num
                 local-rt-port port-num
                 local-rt-server
```

```
                    max-sessions sessions
                    reorder-audio time
                    rt-buffer-size rt-buffer-size
                    rt-server ip-address port port-num
                    video-group video-group-id
```

The following output displays a policy example.

```
A:IPTV-SR7>config>mcast-mgmt># info
----------------------------------------------
            multicast-info-policy "ies100" create
                bundle "5.6.140" create
                    admin-bw 8000
                    video
                        video-group 1
                        local-rt-server
                        rt-buffer-size 3000
                    exit
                    channel "234.5.6.140" "234.5.6.140" create
                    exit
                exit
                bundle "default" create
                exit
                bundle "5.6.241-5.6.243" create
                    admin-bw 12000
                    video
                        video-group 1
                        rt-buffer-size 4000
                    exit
                    channel "234.5.6.241" "234.5.6.243" create
                    exit
                exit
            exit
----------------------------------------------
A:IPTV-SR7>config>router#
```

Configuring RET/FCC Video Components with CLI

This section provides information to configure RET/FCC using the command line interface.

Topics in this section include:

- Configuring RET/FCC Video Features in the CLI on page 255
  - → Configuring the RET Client on page 255
  - → Configuring the RET Server on page 259
  - → Configuring the FCC Server on page 263

Configuring RET/FCC Video Features in the CLI

The following sections provide configuration examples for the RET client, RET server and FCC server.

Configuring the RET Client

This section provides an example configuration for the RET client. The configuration example has the following assumptions:

- A single ISA-MS in slot 2/1 in video group 1
- A single channel 234.0.0.1 within multicast bundle “b1” with an administrative bandwidth of 2700 Kbps defined in **multicast-info-policy** *multicastinfopolicyname*.
- The upstream RET server for the channel is 4.4.4.4 on UDP port 4096
- A single video interface named “v1” in the service with IP address 3.3.3.3/24
- A RET client address of 3.3.3.4 for a VPLS and 3.3.3.3 for IES and VPRN case.

The first step in the configuration is to configure video group 1 and the ISA-MS hardware.

CLI Syntax: config>isa
video-group *video-group-id* [create]
primary *mda-id*
no shutdown

```
*A:ALA-48config>isa# info
----------------------------------------------
        video-group 1 create
            primary 2/1
            no shutdown
        exit
----------------------------------------------
*A:ALA-48config>isa#
```

CLI Syntax: config# card *slot-number*
mda *mda-slot*
mda-type *mda-type*

```
*A:ALA-48config>card>mda#  info
----------------------------------------------
            mda-type isa-ms
----------------------------------------------
*A:ALA-48config>card>mda#
```

The channel parameters for 234.0.0.1 are configured in **multicast-info-policy** *multicastinfopolicyname*. The channel configuration includes the administrative bandwidth, the channel's association with video group 1 and the upstream RET server configuration for the channel (4.4.4.4 UDP port 4096). The following output displays the configuration. Refer to the CLI tree for a complete list of CLI commands.

```
*A:ALA-48config>mcast-mgmt>mcast-info-plcy# info
----------------------------------------------
            bundle "b1" create
                admin-bw 2700
                video
                    video-group 1
                    rt-server 4.4.4.4 port 4096
                exit
                channel "234.0.0.1" "234.0.0.1" create
                exit
            exit
            bundle "default" create
            exit
            video-policy
                video-interface 3.3.3.3 create
                exit
            exit
----------------------------------------------
*A:ALA-48configmcast-mgmtmcast-info-plcy#
```

Note that the channel parameters are actually defined for the channel bundle "b1" and the channel inherits those values based on the multicast information policy inheritance rules.

For the RET client in a VPLS, the following commands within the service instance perform the following tasks to complete the RET client configuration:

- Associate the VPLS with **multicast-info-policy** *multicastinfopolicyname.*
- Create the video interface “vi”.
- Create video SAP and associate it with video group 1.
- Assigns a RET client address and gateway.
- Create a static IGMP join on SAP 3/2/13:21 for the channel 234.0.0.1.

  Note that SAP 3/2/13:21 is a dummy SAP with the only purpose of attracting multicast traffic to the node to enable the caching. No subscribers are connected to it.

```
*A:ALA-48config>service>vpls# info
----------------------------------------------
            igmp-snooping
                no shutdown
            exit
            video-interface "vi" create
                video-sap 1
                exit
                address 3.3.3.3/24
                gateway-ip 3.3.3.253
                rt-client-src-address 3.3.3.4
                no shutdown
            exit
----------------------------------------------
*A:ALA-48config>service>vpls#



*A:ALA-48config>router# info
----------------------------------------------
...
            multicast-info-policy multicastinfopolicyname
            sap 3/2/13:21 create
                igmp-snooping
                    static
                        group 234.0.0.1
                            starg
                        exit
                    exit
                exit
            exit
...
----------------------------------------------
*A:ALA-48config>router#
```

Note that the RET client address is 3.3.3.4 which must be within the IP subnet assigned to the video interface (3.3.3.3/24).

For the RET client in an IES or VPRN, the following commands within the service instance perform these tasks to complete the RET client configuration:

- Associate the service with **multicast-info-policy** *multicastinfopolicyname.*
- Create the video interface “vi” and assign IP address 3.3.3.3.
- Create video SAP and associate it with video group 1.
- Creates a static IGMP join on the video interface for the channel 234.0.0.1. (7750 only)

```
*A:ALA-48config>service>ies# info
----------------------------------------------
            video-interface "vi" create
                video-sap 1
                exit
                address 3.3.3.3/32
                no shutdown
            exit
...
----------------------------------------------
*A:ALA-48config>service>ies#


*A:ALA-48config>router# info
----------------------------------------------
...
    multicast-info-policy multicastinfopolicyname
    pim (7750 only)
        interface "vi"
        exit
    exit
    igmp (7750 only)
        interface "vi"
            static
                group 234.0.0.1
                    starg
                exit
            exit
        exit
----------------------------------------------
*A:ALA-48config>router#
```

The RET client address is 3.3.3.3 which is the address assigned to the video interface in the video policy portion of the multicast information policy.

Configuring the RET Server

This section provides an example configuration for the RET server. The configuration example has the following assumptions:

- A single ISA-MS in slot 2/1 in video group 1
- A single channel 234.0.0.1 within multicast bundle “b1” with an administrative bandwidth of 2700 Kbps defined in **multicast-info-policy** *multicastinfopolicyname.*
- A retransmission buffer for the channel set to 300 milliseconds.
- The RET rate is 5% of nominal.
- Local RET server address is 3.3.3.3 with destination port is UDP 4096.

The first step in the configuration is to configure video group 1 enabling the RET server and the ISA-MS hardware.

CLI Syntax: `config>isa`
`video-group` *`video-group-id`* `[create]`
`local-rt-server`
`no shutdown`

```
*A:ALA-48config>isa# info
----------------------------------------------
        video-group 1 create
            local-rt-server
            primary 2/1
            no shutdown
        exit
----------------------------------------------
*A:ALA-48config>isa#



*A:ALA-48config>card 2>mda 1# info
----------------------------------------------
            mda-type isa-ms
----------------------------------------------
*A:ALA-48config>card>mda#
```

Note the **local-rt-server** command in the above output enables the local RET server on the video group.

The channel parameters for 234.0.0.1 are configured in **multicast-info-policy** *multicastinfopolicyname.* The channel configuration includes the administrative bandwidth and the channel's association with video group 1.

```
*A:ALA-48config>mcast-mgmt>mcast-info-plcy# info
----------------------------------------------
            bundle "default" create
                local-rt-port 4096
            exit
            bundle "b1" create
                admin-bw 2700
                video
                    video-group 1
                    local-rt-server
                    rt-buffer-size 300
                exit
                channel "234.0.0.1" "234.0.0.1" create
                exit
            exit
            video-policy
                video-interface 3.3.3.3 create
                    rt-rate 5
                    hd
                        local-rt-server
                    exit
                    sd
                        local-rt-server
                    exit
                    pip
                        local-rt-server
                    exit
                exit
            exit
----------------------------------------------
*A:ALA-48config>mcast-mgmt>mcast-info-plcy#
```

Note the **local-rt-port** command in the bundle "default" defines the destination UDP port used to reach the local RET server on the service where the multicast information policy is applied. The RET server port can only be defined in the bundle "default" and applies for all bundles in the policy. If no value is specified, the default is used.

In the bundle "b1" the **local-rt-server** command enables the RET server for all channels in the bundle, and the **rt-buffer-size** *rt-buffer-size* command sets the retransmission buffer for all channels in the bundle to 300 milliseconds.

In the video policy above, the **local-rt-server** commands for the video interface 3.3.3.3 enables the RET server on that interface for all channel types "hd" (High Definition), "sd" (Standard Definition) and "pip" (Picture-in-Picture). The **rt-rate** *rt-burst-percentage* command in the policy indicates that the retransmission rate will be 5% of the nominal rate for all channel types; individual rates can be defined if desired.

For the RET server in a VPLS, these commands within the service instance perform the following tasks to complete the RET server configuration:

- Associate the VPLS with **multicast-info-policy** *multicastinfopolicyname.*
- Create the video interface “vi”.
- Create video SAP and associate it with video group 1.
- Assigns an IP address 3.3.3.3 to the video interface.
- Create a static IGMP join on SAP 3/2/13:21 for the channel 234.0.0.1.

  Note that SAP 3/2/13:21 is a dummy SAP with the only purpose of attracting multicast traffic to the node to enable the caching. No subscribers are connected to it.

```
*A:ALA-48config>service>vpls# info
----------------------------------------------
            igmp-snooping
                no shutdown
            exit
            video-interface "vi" create
                video-sap 1
                exit
                address 3.3.3.3/32
                no shutdown
            exit
            multicast-info-policy multicastinfopolicyname
            sap 3/2/13:21 create
                igmp-snooping
                    static
                        group 234.0.0.1
                            starg
                        exit
                    exit
                exit
            exit
----------------------------------------------
*A:ALA-48config>service>vpls#
```

The services available on the video interface address 3.3.3.3 are defined in the video policy in which the RET server was enabled.

For the RET server in an IES or VPRN, these commands within the service instance perform the following tasks to complete the RET server configuration:

- Associate the service with **multicast-info-policy** *multicastinfopolicyname.*
- Create the video interface “vi” and assign IP address 3.3.3.3.
- Create video SAP and associate it with video group 1.
- Creates a static IGMP join on video-interface “vi” for the channel 234.0.0.1.

```
*A:ALA-48config>service>ies# info
----------------------------------------------
            video-interface "vi" create
                video-sap 1
                exit
                address 3.3.3.3/32
                no shutdown
            exit
    multicast-info-policy multicastinfopolicyname
    pim
        interface "vi"
        exit
    exit
    igmp
        interface "vi"
            static
                group 234.0.0.1
                    starg
                exit
            exit
        exit
----------------------------------------------
*A:ALA-48config>service>ies#
```

The services available on the video interface address 3.3.3.3 are defined in the video policy in which the RET server was enabled.

Configuring the FCC Server

This section provides an example configuration for the FCC server. The configuration example has the following assumptions:

- A single ISA-MS in slot 2/1 in video group 1.
- A single channel 234.0.0.1 within multicast bundle “b1” with an administrative bandwidth of 8000 Kbps defined in **multicast-info-policy** *multicastinfopolicyname*.
- The FCC mode is burst with a rate 130% of nominal for HD, 200% for SD, and disabled for PIP.
- Local FCC server address is 3.3.3.3 with destination port is UDP 4098.

CLI Syntax:

```
config>isa
          video-group video-group-id [create]
             fcc-server
             no shutdown
```

The first step in the configuration is to configure video group 1 enabling the RET server and the ISA-MS hardware.

```
*A:ALA-48config>isa# info
----------------------------------------------
        video-group 1 create
            fcc-server
            primary 2/1
            no shutdown
        exit
----------------------------------------------
*A:ALA-48config>isa#


*A:ALA-48config>card>mda# info
----------------------------------------------
            mda-type isa-ms
----------------------------------------------
*A:ALA-48config>card>mda#
```

Note the **fcc-server** command in the above output enables the FCC server on the video group.

The channel parameters for 234.0.0.1 are configured in **multicast-info-policy** *multicastinfopolicyname.* The channel configuration includes the administrative bandwidth and the channel's association with video group 1.

```
*A:ALA-48configmcast-mgmtmcast-info-plcy# info
----------------------------------------------
            bundle "default" create
                local-fcc-port 4098
            exit
            bundle "b1" create
                admin-bw 8000
                video
                    video-group 1
                    fcc-server
                    fcc-channel-type hd
                exit
                channel "234.0.0.1" "234.0.0.1" create
                exit
            exit
            video-policy
                video-interface 3.3.3.3 create
                    rt-rate 5
                    hd
                        fcc-server mode burst
                        fcc-burst 30
                    exit
                    sd
                        fcc-server mode burst
                        fcc-burst 100
                    exit
                    pip
                        no fcc-server
                    exit
                exit
            exit
----------------------------------------------
*A:ALA-48configmcast-mgmtmcast-info-plcy#
```

Note the **local-fcc-port** command in the bundle "default" defines the destination UDP port used to reach the FCC server on the service where the multicast information policy is applied. The FCC server port can only be defined in the bundle "default" and applies for all bundles in the policy. If no value is specified, the default is used.

In the bundle "b1", the **fcc-server** command enables the FCC server for all channels in the bundle, and the **fcc-channel-type hd** command sets the channel type for all channels in the bundle to "hd" (High Definition).

In the video policy context above, the **fcc-server** commands for the video interface 3.3.3.3 enables the FCC server on that interface for all channel types "hd" (High Definition), "sd" (Standard Definition) whereas the **no fcc-server** command disables the FCC for "pip" (Picture-in-Picture) channels on the video interface. The **fcc-burst** command in the policy indicates that the burst rate over the nominal rate for the channel type; HD at 130% (30% over nominal) and SD at 200% (100% over nominal).

For the FCC server in a VPLS, the following commands within the service instance perform the following tasks to complete the FCC server configuration:

- Associate the VPLS with **multicast-info-policy** *multicastinfopolicyname.*
- Create the video interface “vi”.
- Create video SAP and associate it with video group 1.
- Assigns an IP address 3.3.3.3 to the video interface.
- Create a static IGMP join on SAP 3/2/13:21 for the channel 234.0.0.1.

  Note that SAP 3/2/13:21 is a dummy SAP with the only purpose of attracting multicast traffic to the node to enable the caching. No subscribers are connected to it.

```
*A:ALA-48configservicevpls# info
----------------------------------------------
            igmp-snooping
                no shutdown
            exit
            video-interface "vi" create
                video-sap 1
                exit
                address 3.3.3.3/32
                no shutdown
            exit
            multicast-info-policy multicastinfopolicyname
            sap 3/2/13:21 create
                igmp-snooping
                    static
                        group 234.0.0.1
                            starg
                        exit
                    exit
                exit
            exit
----------------------------------------------
*A:ALA-48configservicevpls#
```

The services available on the video interface address 3.3.3.3 are defined in the video policy in which the FCC server was enabled.

For the FCC server in an IES or VPRN, the following commands within the service instance perform the following tasks to complete the FCC server configuration:

- Associate the service with **multicast-info-policy** *multicastinfopolicyname.*
- Create the video interface “vi” and assign IP address 3.3.3.3.
- Create video SAP and associate it with video group 1.
- Creates a static IGMP join on video-interface “vi” for the channel 234.0.0.1.

```
*A:ALA-49configserviceies# info
----------------------------------------------
            video-interface "vi" create
                video-sap 1
                exit
                address 4.4.4.4/32
                no shutdown
            exit
----------------------------------------------
*A:ALA-49configserviceies#


*A:ALA-48configrouter# info
----------------------------------------------
...
    multicast-info-policy multicastinfopolicyname
    pim
        interface "vi"
        exit
    exit
    igmp
        interface "vi"
            static
                group 234.0.0.1
                    starg
                exit
            exit
        exit
----------------------------------------------
*A:ALA-48configrouter#
```

The services available on the video interface address 3.3.3.3 are defined in the video policy in which the FCC server was enabled.

Logging and Accounting Collection for Video Statistics

The following output displays a configuration example used in logging and accounting for video.

```
*A:SR-7/Dut-C>config>log# info
----------------------------------------------
        file-id 1
            location cf3:
        exit
        accounting-policy 1
            shutdown
            record video
            collection-interval 5
            to file 1
        exit
...
----------------------------------------------
*A:SR-7/Dut-C>config>log#
```

Use the following CLI to enable logging and accounting to a service to collect stats for that particular service.

Example:

```
*A:SR-7/Dut-C>config>service>ies# video-interface "vi" accounting-policy 1
*A:SR-7/Dut-C>config>service>ies# info
  video-interface "vi" create
        accounting-policy "1"
  exit
```

Start ing stats collection can be enabled by executing a **no shutdown** command on the accounting policy. This starts the recording of stats and the stats will be written in an act-collect directory and a **shutdown** command on the accounting policy will move the recorded file to act directory.

Configuring ADI Components with CLI

This section provides information to configure ADI using the command line interface.

Topics in this section include:

- Configuring the RET Client on page 269
- Configuring a Video Group on page 270
- Configuring NTP on page 271
- Configuring Channel Parameters on page 271
- Configuring Service Entities on page 272

Configuring ADI in CLI

Configuring the RET Client

This section provides an example configuration for the ADI splicer. The configuration example makes the following assumptions:

- A single ISA-MS is configured in slot 2/1 in video group 1.
- The NTP server for the router is 192.168.15.221.
- A single channel main 234.5.6.140 within multicast bundle “b1” is defined in the **multicast-info-policy** *multicastinfopolicyname* context.
- IES service 100 is a Layer 3 service in which ADI will be performed.
- The video interface in IES 100 is 100.100.0.254/8
- The ad server address is 10.200.14.2
- The splicer’s local addresses used to communicate with the ad server are 100.1.1.2 for control traffic and 100.1.1.3 for data traffic.
- For the SCTE 30 communication in the example, the main channel is named 228 with (S,G) = (195.168.9.10,234.4.5.228) and the zone channel is named 228-1with (S,G) = (100.100.100.1,234.4.5.228).
- Must have an IGMP static entry for the network channel (S,G) on the video-interface to attract the network traffic to the video interface.
- Must have the video-interface enabled in PIM.

Configuring a Video Group

The first step in the configuration is to configure a video group (*video-group-id* = 1) and enabling ad insertion and the ISA-MS hardware. Note the **ad-insert** command enables the ADI splicer on the video group.

```
A:ALA-49>config>isa# info
----------------------------------------------
...
        video-group 1 create
            description "Video Group 1"
            ad-insert
            primary 7/2
            no shutdown
        exit
...
----------------------------------------------
A:ALA-49>config>isa#
```

The following output shows the card and MDA configuration.

```
A:ALA-49>config>card# info
----------------------------------------------
        card-type iom2-20g
        mda 1
            shutdown
            mda-type isa-ms
        exit
        mda 2
            mda-type isa-ms
        exit
----------------------------------------------
A:ALA-49>config>card#
```

Configuring NTP

NTP is required on the splicer to ensure that time is synchronized between it and the ad server.

```
A:ALA-49>config>system>time# info
----------------------------------------------
            ntp
                no authentication-check
                ntp-server
                server 192.168.15.221
                no shutdown
            exit
...
----------------------------------------------
A:ALA-49>config>system>time#
```

Configuring Channel Parameters

The channel parameters for 234.4.5.228 are configured in the **multicast-info-policy** *multicastinfopolicyname* context. For ADI, the channel configuration required is the channel's association with video group 1.

```
*A:ALA-49>config>mcast-mgmt# info
----------------------------------------------
...
            multicast-info-policy "multicastinfopolicyname" create
                bundle "b1" create
                    video
                        video-group 1
                    exit
                    channel "234.4.5.228" "234.4.5.228" create
                    exit
                exit
                bundle "default" create
                exit
            exit
...
----------------------------------------------
*A:ALA-49>config>mcast-mgmt#
```

Configuring Service Entities

In addition to the commands needed to configure a service, the following commands within the service instance are used to perform the following ADI configuration steps. This example uses an IES service context.

- Associate IES 100 with **multicast-info-policy** *multicastinfopolicyname.*
- Create the video interface video-100.
- Create a video SAP and associate it with video group 1.
- Assigns an IP address 100.100.0.254 to the video interface and subnet 100.0.0.0/8.
- Name the main channel (S,G) = (195.168.9.10,234.4.5.228) “228” and the zone channel (S,G) = (100.100.100.1,234.4.5.228) “228-1”.
- Configure the ad server (address = 10.200.14.2) and create IP addresses within the video interface subnet for SCTE 30 control traffic (100.1.1.2) and data traffic (100.1.1.3).
- The control and data addresses must be in the video interface subnet.

```
*A:ALA-49>config>service>ies# info
----------------------------------------------
...
            video-interface "video-100" create
                video-sap 1
                exit
                address 100.100.0.254/8
                adi
                    channel 234.4.5.228 source 195.168.9.10 channel-name "228"
                        scte35-action drop
                      zone-channel 234.4.5.228 source 100.100.100.1 adi-channel-name "228-
1"
                    exit
                    scte30
                        ad-server 10.200.14.2
                        local-address control 100.1.1.2 data 100.1.1.3
                    exit
                exit
                no shutdown
            exit
            no shutdown
----------------------------------------------
*A:ALA-49>config>service>ies#
```

Note that the source address (100.100.100.1) for the zone channel (S,G) and the local addresses (100.1.1.2 and 100.1.1.3) used for SCTE 30 communication must all be within the video interface subnet (100.0.0.0/8).

Connections are accepted from multiple ad-servers. This can be used for ad server redundancy.

If the main channel were a (*,G), the source address of 0.0.0.0 would have been specified.

Additional zone channels with distinct names could be configured within the service instance. In a practical configuration, the G for the main channel (234.4.5.228) will be the same for G in the zone channel (S,G) because the STBs will join the (*,G) at the A-server and D-server.

Configuring ADI for a VPRN service instance uses the same commands within the VPRN service context.

Video Command Reference

This section provides a command reference for the CLI commands for IP-TV video applications

Topics include:

- IP-TV Command Hierarchies on page 276
  - → Hardware Commands on page 276
  - → Video Group Commands on page 276
  - → Video Policy Video Commands on page 276
  - → Bundle and Channel Commands on page 278
  - → Service Video Interface Commands on page 280
  - → Show Commands on page 283
  - → Clear Commands on page 283
  - → Debug Commands on page 284
- Video Services Commands on page 285

IP-TV Command Hierarchies

Hardware Commands

```
config
    — [no] card slot-number
        — card-type card-type
        — no card-type
        — [no] mda mda-slot
            — mda-type mda-type
            — no mda-type
```

Video Group Commands

```
config
    — isa
        — lns-group lns-group-id [create]
        — no lns-group lns-group-id
            — description description-string
            — no description
            — mda mda-id [drain]
            — no mda mda-id
            — [no] shutdown
        — video-group video-group-id [create]
        — no video-group video-group-id
            — [no] ad-insert
            — description description-string
            — no description
            — [no] fcc-server
            — [no] local-rt-server
            — [no] primary mda-id
            — resv-ret resv-ret
            — [no] shutdown
```

Video Policy Video Commands

```
config
    — mcast-management
        — multicast-info-policy policy-name [create]
        — no multicast-info-policy policy-name
            — video-policy
                — video-interface ip-address [create]
                — no video-interface ip-address
                    — hd
                        — dent-threshold threshold
                        — no dent-threshold
                        — fcc-burst burst-percentage
                        — no fcc-burst
                        — fcc-server [mode {burst | dent | hybrid}]
                        — no fcc-server
                        — local-rt-server
```

- — **no local-rt-server**
- — **mc-handover** *percentage*
- — **no mc-handover**
- — **rt-rate** *rt-burst-percentage*
- — **no rt-rate**

— **max-sessions** *sessions*
— **no max-sessions**
— **pip**

- — **dent-threshold** *threshold*
- — **no dent-threshold**
- — **fcc-burst** *burst-percentage*
- — **no fcc-burst**
- — **fcc-server** [**mode** {**burst** | **dent** | **hybrid**}]
- — **no fcc-server**
- — **local-rt-server**
- — **no local-rt-server**
- — **mc-handover** *percentage*
- — **no mc-handover**
- — **rt-rate** *rt-burst-percentage*
- — **no rt-rate**

— **rt-mcast-reply** [**count** *count*] [**interval** *milliseconds*] [**hold-time** *milliseconds*]
— **no rt-mcast-reply**
— **rt-payload-type** *payload-type*
— **no rt-payload-type**
— **rt-rate** *rt-burst-percentage*
— **no rt-rate**
— **sd**

- — **dent-threshold** *threshold*
- — **no dent-threshold**
- — **fcc-burst** *burst-percentage*
- — **no fcc-burst**
- — **fcc-server** [**mode** {**burst** | **dent** | **hybrid**}]
- — **no fcc-server**
- — **local-rt-server**
- — **no local-rt-server**
- — **mc-handover** *percentage*
- — **no mc-handover**
- — **rt-rate** *rt-burst-percentage*
- — **no rt-rate**

— **subscriber-bw-limit** *bandwidth*
— **no subscriber-bw-limit**

Bundle and Channel Commands

```
config
    — mcast-management
        — multicast-info-policy policy-name [create]
        — no multicast-info-policy policy-name
            — bundle bundle-name [create]
            — no bundle bundle-name
                — admin-bw kbps
                — no admin-bw
                — bw-activity {use-admin-bw | dynamic [falling-delay seconds]} [black-hole-rate kbps]
                — no bw-activity
                — channel ip-address [ip-address] [create]
                — no channel ip-address [ip-address]
                    — admin-bw kbps
                    — no admin-bw
                    — video
                        — fcc-channel-type {hd | sd | pip}
                        — no fcc-channel-type
                        — fcc-min-duration time
                        — no fcc-min-duration
                        — fcc-server [disable]
                        — no fcc-server
                        — local-fcc-port port
                        — no local-fcc-port
                        — local-rt-port port
                        — no local-rt-port
                        — local-rt-server [disable]
                        — no local-rt-server
                        — reorder-audio time
                        — no reorder-audio
                        — rt-buffer-size rt-buffer-size
                        — no rt-buffer-size
                        — rt-server disable
                        — rt-server ip-address port port-num
                        — no rt-server
                        — video-group video-group-id
                        — video-group disable
                        — no video-group
                    — source-override ip-address [create]
                    — no source-override ip-address
                        — admin-bw kbps
                        — no admin-bw
                        — video
                            — fcc-channel-type {hd | sd | pip}
                            — no fcc-channel-type
                            — fcc-min-duration time
                            — no fcc-min-duration
                            — fcc-server [disable]
                            — no fcc-server
                            — local-fcc-port port
                            — no local-fcc-port
```

- **local-rt-port** *port*
- **no local-rt-port**
- **local-rt-server** [**disable**]
- **no local-rt-server**
- **reorder-audio** *time*
- **no reorder-audio**
- **rt-buffer-size** *rt-buffer-size*
- **no rt-buffer-size**
- **rt-server disable**
- **rt-server** *ip-address* **port** *port-num*
- **no rt-server**
- **video-group** *video-group-id*
- **no video-group**

— **video**

- **fcc-channel-type** {**hd** | **sd** | **pip**}
- **no fcc-channel-type**
- **fcc-min-duration** *time*
- **no fcc-min-duration**
- **fcc-server** [**disable**]
- **no fcc-server**
- **local-fcc-port** *port*
- **no local-fcc-port**
- **local-rt-port** *port*
- **no local-rt-port**
- **local-rt-server** [**disable**]
- **no local-rt-server**
- **reorder-audio** *time*
- **no reorder-audio**
- **rt-buffer-size** *rt-buffer-size*
- **no rt-buffer-size**
- **rt-server disable**
- **rt-server** *ip-address* **port** *port-num*
- **no rt-server**
- **source-port** *port-num*
- **no source-port**
- **video-group** *video-group-id*
- **video-group disable**
- **no video-group**

Service Video Interface Commands

VPLS Commands

config>service>vpls *service-id*
- — **multicast-info-policy** *policy-name*
- — **no multicast-info-policy**
- — **video-interface** *ip-int-name* [**create**]
- — **no video-interface** ***ip-int-name***
  - — [**no**] **address** *ip-address/mask*
  - — **cpu-protection** *policy-id*
  - — **no cpu-protection**
  - — **description** *description-string*
  - — **no description**
  - — **gateway-ip** *ip-address*
  - — **no gateway-ip**
  - — **multicast-service** *service-id*
  - — **no multicast-service**
  - — **rt-client-src-address** *ip-address*
  - — **no rt-client-src-address**
  - — [**no**] **shutdown**
  - — **video-sap** *video-group-id*
  - — **no video-sap**
    - — **egress**
      - — **filter ip** *ip-filter-id*
      - — **no filter**
      - — **qos** *egress-qos-policy-id*
      - — **no qos**
    - — **ingress**
      - — **filter ip** *ip-filter-id*
      - — **no filter**
      - — **qos** *ingress-qos-policy-id*
      - — **no qos**

IES Commands

config>service>ies *service-id*
- **video-interface** *ip-int-name* [**create**]
- **no video-interface** ***ip-int-name***
  - [**no**] **address** *ip-address/mask*
  - **adi**
    - **channel** *mcast-address* **source** *ip-address* [**channel-name** *channel-name*]
    - **no channel** *mcast-address* **source** *ip-address*
      - **description** *description-string*
      - **no description**
      - **scte35-action** {**forward** | **drop**}
      - **zone-channel** *mcast-address* **source** *ip-address* **adi-channel-name** *channel-name*
      - **no zone-channel** *mcast-address* **source** *ip-address*
    - **scte30**
      - [**no**] **ad-server** *ip-address*
      - **local-address control** *ip-address* **data** *ip-address*
      - **no local-address**
    - [**no**] **shutdown**
  - **description** *description-string*
  - **no description**
  - **multicast-service** *service-id*
  - **no multicast-service**
  - **rt-client-src-address** *ip-address*
  - **no rt-client-src-address**
  - [**no**] **shutdown**
  - **video-sap** *video-group-id*
  - **no video-sap**
    - **egress**
      - **filter ip** *ip-filter-id*
      - **no filter**
      - **qos** *egress-qos-policy-id*
      - **no qos**
    - **ingress**
      - **filter ip** *ip-filter-id*
      - **no filter**
      - **qos** *ingress-qos-policy-id*
      - **no qos**

VPRN Commands

Note that VPRN service commands are only applicable to the 7750 SR-Series platforms.

config>service>vprn *service-id*
- **video-interface** *ip-int-name* [**create**]
- **no video-interface** ***ip-int-name***
  - [**no**] **address** *ip-address/mask*
  - **adi**
    - **channel** *mcast-address* **source** *ip-address* [**channel-name** *channel-name*]
    - **no channel** *mcast-address* **source** *ip-address*
      - **description** *description-string*
      - **no description**
      - **scte35-action** {**forward** | **drop**}
      - **zone-channel** *mcast-address* **source** *ip-address* **adi-channel-name** *channel-name*
      - **no zone-channel** *mcast-address* **source** *ip-address*
    - **scte30**
      - [**no**] **ad-server** *ip-address*
      - **local-address control** *ip-address* **data** *ip-address*
      - **no local-address**
    - [**no**] **shutdown**
  - **description** *description-string*
  - **no description**
  - **multicast-service** *service-id*
  - **no multicast-service**
  - **rt-client-src-address** *ip-address*
  - **no rt-client-src-address**
  - [**no**] **shutdown**
  - **video-sap** *video-group-id*
  - **no video-sap**
    - **egress**
      - **filter ip** *ip-filter-id*
      - **no filter**
      - **qos** *egress-qos-policy-id*
      - **no qos**
    - **ingress**
      - **filter ip** *ip-filter-id*
      - **no filter**
      - **qos** *ingress-qos-policy-id*
      - **no qos**

Show Commands

show
- **isa**
  - **video-group** [*video-group-id*]

show
- **video**
  - **adi** [**service** *service-id*] [**interface** ip-*int-name*] [**address** *mcast-address*] [**source** *ip-address*] [**detail**]
    - **channel** [**service** *service-id*] [**interface** *ip-int-name*] [**address** *mcast-address*] [**source** *ip-address*] [**detail**]
    - **session** [**service** *service-id*] [**interface** *ip-int-name*] [**address** *mcast-address*] [**source** *ip-address*]
    - **splice-status** [**service** *service-id*] [**interface** *ip-int-name*][**address** *mcast-address*] [**source** *ip-address*] [**start-time** *start-time* [**interval** *time-interval*]]
  - **channel** [**service** *service-id*] [**interface** *ip-int-name*] [**address** *mcast-address*] [**source** *ip-address*] [**summary** | **detail**]
  - **interface** [**service** *service-id*] [**interface** *ip-int-name*] [**stats** {**rt-server**| **fcc-server**}]
  - **interface** [**service** *service-id*] [**interface** *ip-int-name*] **summary**
  - **rtp-session** [**service** *service-id*] [**source** *ip-address*] [**detail** [**stats** {**rt-server** | **fcc-server**}]]
  - **rtp-session** [**service** *service-id*] **summary**

Clear Commands

clear
- **video**
  - **id** *service-id*
    - **session all**
    - **session client** *srcAddr*
  - **statistics**
    - **id** *service-id*
      - **adi-session**
      - **channel all** [**rt-client**] [**rt-server**] [**fcc-server**] [**ad-insert**]
      - **channel** *grp-address* [**source** *srcAddr*] [**rt-client**] [**rt-server**] [**fcc-server**] [**ad-insert**]
      - **interface** *ip-int-name* [**address** *ip-address*] **rt-client**] [**rt-server**] [**fcc-server**] [**ad-insert**]
      - **session all** [**rt-server**] [**fcc-server**]
      - **session client** *srcAddr* [**rt-server**] [**fcc-server**]
    - **isa** *video-group-id* [*mda-id*]

Debug Commands

debug
- **—** [**no**] **service**
  - **—** **id** *service-id*
    - **—** [**no**] **video-interface** *video-ip-int-name*
    - **—** **adi** [*zone-channel-name*]
    - **—** **no adi**
    - **—** **adi-packet** [*zone-channel-name*] [**type** {*type-name* [*type-name*]|**all**}]
    - **—** **no adi-packet**
    - **—** **fcc-server** [**client** *client-ip* [**source-port** *src-port*]]
    - **—** **no fcc-server**
    - **—** **packet-rx** [**client** *client-ip* [**source-port** *src-port*]] [**fcc-join**] [**fcc-leave**] [**ret-nack**]
    - **—** **no packet-rx**
    - **—** **packet-tx** [**group** *grp-addr* [**source** *srcAddr*]] [**ret-nack**]
    - **—** **no packet-tx**
    - **—** **rt-client** [**group** *group-addr*]
    - **—** **no rt-client**
    - **—** **rt-server** [**client** *client-ip* [**source-port** *src-port*]]
    - **—** **no rt-server**
    - **—** **sg** [**group** *grp-addr* [**source** *src-addr*]]
    - **—** **no sg**

Video Services Commands

- Generic Commands on page 285
- Hardware Commands on page 287
- lns-group ins-group-id [create] on page 290
- Multicast Info Policy Commands on page 293
- Video Policy Commands on page 300
- Bundle and Channel Commands on page 307
- Service Video Interface Commands on page 312
- Show Commands on page 319
- Clear Commands on page 327
- Debug Commands on page 330

GENERIC COMMANDS

description

Syntax **description** *description-string*
no description

Context config>isa>video-group
config>service>ies>video-interface
config>service>vpls>video-interface
config>service>vprn>video-interface
config>service>ies>video-interface>adi>channel
config>service>vpls>video-interface>adi>channel
config>service>vprn>video-interface>adi>channel

Description This command creates a text description stored in the configuration file for a configuration context.

The **description** command associates a text string with a configuration context to help identify the context in the configuration file.

The **no** form of this command removes any description string from the context.

Default No description is associated with the configuration context.

Parameters *description-string* — A text string describing the entity. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

shutdown

Syntax [**no**] **shutdown**

Context config>isa>video-group
config>service>ies>video-interface
config>service>vpls>video-interface
config>service>vprn>video-interface
config>service>ies>video-interface>adi
config>service>vpls>video-interface>adi
config>service>vprn>video-interface>adi

Description The **shutdown** command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

The **shutdown** command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they can be deleted.

Unlike other commands and parameters where the default state is not indicated in the configuration file, **shutdown** and **no shutdown** are always indicated in system generated configuration files.

Default no shutdown

HARDWARE COMMANDS

card

Syntax **card** *slot-number*
no card *slot-number*

Context config

Description This mandatory command enables access to the chassis card Input/Output Module (IOM), slot, and MDA CLI context.

The **no** form of this command removes the card from the configuration. All associated ports, services, and MDAs must be shutdown

Default No cards are configured.

Parameters *slot-number* — The slot number of the card in the chassis.

Values 1 — 10 depending on chassis model.

SR-1: *slot-number* = 1
SR-7: *slot-number* = 1 — 5
SR-12: *slot-number* = 1 — 10

ESS-1: *slot-number* = 1
ESS-6: *slot-number* = 1 — 4
ESS-7: *slot-number* = 1 — 5
ESS-12: *slot-number* = 1 — 10

card-type

Syntax **card-type** *card-type*
no card-type

Context config>card

Description This mandatory command adds an IOMto the device configuration for the slot. The card type can be preprovisioned, meaning that the card does not need to be installed in the chassis.

A card must be provisioned before an MDA or port can be configured.

A card can only be provisioned in a slot that is vacant, meaning no other card can be provisioned (configured) for that particular slot. To reconfigure a slot position, use the **no** form of this command to remove the current information.

A card can only be provisioned in a slot if the card type is allowed in the slot. An error message is generated if an attempt is made to provision a card type that is not allowed.

If a card is inserted that does not match the configured card type for the slot, then a medium severity alarm is raised. The alarm is cleared when the correct card type is installed or the configuration is modified.

A high severity alarm is raised if an administratively enabled card is removed from the chassis. The alarm is cleared when the correct card type is installed or the configuration is modified. A low severity trap is issued when a card is removed that is administratively disabled.

Because the IOM-3 integrated card does not have the capability in install separate MDAs, the configuration of the MDA is automatic. This configuration only includes the default parameters such as default buffer policies. Commands to manage the MDA such as **shutdown**, named buffer pool etc will remain in the MDA configuration context.

An appropriate alarm is raised if a partial or complete card failure is detected. The alarm is cleared when the error condition ceases.

The **no** form of this command removes the card from the configuration

Default No cards are preconfigured for any slots.

Parameters *card-type* — The type of card to be configured and installed in that slot.

Values
7750 SR: iom-20g, iom2-20g, iom-20g-b, iom3-xp
7450 ESS: iom-20g, iom-20g-b, iom3-xp

mda

Syntax **mda** *mda-slot*
no mda *mda-slot*

Context config>card

Description This mandatory command enables access to a card's MDA CLI context to configure MDAs.

Default No MDA slots are configured by default.

Parameters *mda-slot* — The MDA slot number to be configured. Slots are numbered 1 and 2. On vertically oriented slots, the top MDA slot is number 1, and the bottom MDA slot is number 2. On horizontally oriented slots, the left MDA is number 1, and the right MDA slot is number 2.

Values 1, 2

mda-type

Syntax **mda-type** *mda-type*
no mda-type

Context config>card>mda

Description This mandatory command provisions a specific MDA type to the device configuration for the slot. The MDA can be preprovisioned but an MDA must be provisioned before ports can be configured. Ports can be configured once the MDA is properly provisioned.

A maximum of two MDAs can be provisioned on an IOM. Only one MDA can be provisioned per IOM MDA slot. To modify an MDA slot, shut down all port associations.

An MDA can only be provisioned in a slot if the MDA type is allowed in the MDA slot. An error message is generated when an MDA is provisioned in a slot where it is not allowed.

A medium severity alarm is generated if an MDA is inserted that does not match the MDA type configured for the slot. This alarm is cleared when the correct MDA is inserted or the configuration is modified.

A high severity alarm is raised when an administratively enabled MDA is removed from the chassis. This alarm is cleared if the either the correct MDA type is inserted or the configuration is modified. A low severity trap is issued if an MDA is removed that is administratively disabled.

An alarm is raised if partial or complete MDA failure is detected. The alarm is cleared when the error condition ceases.

All parameters in the MDA context remain and if non-default values are required then their configuration remains as it is on all existing MDAs.

The **no** form of this command deletes the MDA from the configuration. The MDA must be administratively shut down before it can be deleted from the configuration.

Default No MD types are configured for any slots by default.

Parameters *mda-type* — The type of MDA selected for the slot postion.

7750: m60-10/100eth-tx, m10-1gb-sfp, m16-oc12/3-sfp, m8-oc12/3-sfp, m16-oc3-sfp, m8-oc3-sfp, m4-oc48-sfp, m1-oc192, m5-1gb-sfp, m12-chds3, m1-choc12-sfp, m1-10gb, m4-choc3-sfp, m2-oc48-sfp, m20-100eth-sfp, m20-1gb-tx, m2-10gb-xfp, m4-atmoc12/3-sfp, m16-atmoc3-sfp, m20-1gb-sfp, m4-chds3, m1-10gb-xfp, vsm-cca, 5-1gb-sfp-b, m10-1gb-sfp-b, m4-choc3-as-sfp, m10-1gb+1-10gb, isa-ipsec, m1-choc12-as-sfp, m12-chds3-as, m4-chds3-as, m10-1gb-hs-sfp, m1-10gb-hs-xfp, m4-choc3-ces-sfp, m1-choc3-ces-sfp, m4-10gb-xp-xfp, m2-10gb-xp-xfp, m1-10gb-xp-xfp, m10-1gb-xp-sfp, m20-1gb-xp-sfp, m20-1gb-xp-tx, m1-choc12-ces-sfp, imm24-1gb-xp-sfp, imm24-1gb-xp-tx, imm4-10gb-xp-xfp, imm2-10gb-xp-xfp, isa-ms

7450: m60-10/100eth-tx, m10-1gb-sfp, m16-oc12/3-sfp, m8-oc12/3-sfp, m16-oc3-sfp, m4-oc48-sfp, m1-10gb, m2-oc48-sfp, m20-100eth-sfp, m20-1gb-tx, m2-10gb-xfp, m20-1gb-sfp, m1-10gb-xfp, vsm-cca, m5-1gb-sfp-b, m10-1gb-sfp-b, m10-1gb+1-10gb, m10-1gb-hs-sfp, m1-10gb-hs-xfp, m4-10gb-xp-xfp, m2-10gb-xp-xfp, m1-10gb-xp-xfp, m10-1gb-xp-sfp, m20-1gb-xp-sfp, m20-1gb-xp-tx, isa-ms

LNS GROUP COMMANDS

lns-group

Syntax **lns-group** *ins-group-id* [**create**]
no lns-group *lns-group-id*

Context config>isa

Description This command configures the ISA LNS group.

Parameters *lns-group-id* — Specified the LNS group ID.

Values 1 — 4

create — Keyword required when first creating the configuration context. Once the context is created, one can navigate into the context without the **create** keyword.

mda

Syntax **mda** *mda-id* [**drain**]
no mda *mda-id*

Context config>isa>lns-group

Description This command configures an ISA LNS group MDA.

Parameters *mda-id* — Specifies the slot and MDA number for the primary video group ISA.

Values slot/mda
slot 1 — 10 (depending on the chassis model)
mda 1 — 2

VIDEO GROUP COMMANDS

video-group

Syntax **video-group** *video-group-id* [**create**]
no video-group *video-group-id*

Context config>isa

Description This command configures an ISA video group.

Parameters *video-group-id* — Specifies a video group ID.

Values 1 — 4

create — Keyword required when first creating the configuration context. Once the context is created, one can navigate into the context without the **create** keyword.

ad-insert

Syntax [**no**] **ad-insert**

Context config>isa>video-group

Description This command enables the ad insert server for the group. Ad insertion cannot be enabled if an FCC server or local RT server is enabled.

The **no** form of the command disables the server.

fcc-server

Syntax [**no**] **fcc-server**

Context config>isa>video-group

Description This command enables the FCC server capability for the ISA video group. FCC server cannot be enabled if ad insertion or the local RET server is enabled.

FCC Server parameters can be configured in a multicast information policy or a service, but the parameters will have no effect if the FCC server is disabled or if the video group is administratively disabled (shutdown).

The **no** form of the command disables the FCC server.

Default no fcc-server

local-rt-server

Syntax [**no**] **local-rt-server**

Context config>isa>video-group

Description This command enables the local RET server for the group. A local RET server cannot be enabled if an FCC server or ad insertion is enabled.

The **no** form of the command disables the server.

primary

Syntax [**no**] **primary** *mda-id*

Context config>isa>video-group

Description This command configures the primary video group ISA. Only one primary can be configured per video group when ad insertion is enabled. The maximum number of primaries per video-group for FCC and RD is 4.

Parameters *mda-id* — Specifies the slot and MDA number for the primary video group ISA.

Values slot/mda

slot	1 — 10 (depending on the chassis model)
mda	1 — 2

resv-ret

Syntax **resv-ret** *resv-ret*

Context config>isa>video-group

Description This command provides a mechanism to reserve an explicit amount of egress bandwidth for RET for all the ISAs within a video group. If the amount of egress bandwidth is less than the reserved amount, FCC requests are discarded and only RET requests processed. The bandwidth is dynamically adjusted per ISA within the video group if an ISA becomes operational/non-operational within the group.

MULTICAST INFO POLICY COMMANDS

multicast-info-policy

Syntax **multicast-info-policy** *policy-name* [**create**]
no multicast-info-policy *policy-name*

Context config>mcast-management

Description This command configures a multicast information policy. Multicast information policies are used to manage parameters associated with Layer 2 and Layer 3 multicast records. Multiple features use the configured information within the policy. The multicast ingress path manager uses the policy to decide the inactive and active state behavior for each multicast record using the ingress paths to the switch fabric. The egress multicast CAC function may use the policy information as a basis for allowing or disallowing downstream nodes to join multicast streams. The system's multicast ECMP join decisions are influenced by the channel information contained within the policy.

Multicast Bundles:

A multicast information policy consists of one or multiple named bundles. Multicast streams are mapped to a bundle based on matching the destination address of the multicast stream to configured channel ranges defined within the bundles. Each policy has a bundle named 'default' that is used when a destination address does not fall within any of the configured channel ranges.

Each bundle has a set of default parameters used as the starting point for multicast channels matching the bundle. The default parameters may be overridden by optional exception parameters defined under each channel range. Further optional parameter overrides are possible under explicit source address contexts within each channel range.

Default Multicast Information Policy

A multicast information policy always exists with the name 'default' and cannot be edited or deleted. The following parameters are contained in the default multicast information policy:

Policy Description: Default policy, cannot be edited or deleted.
Bundle: default
Bundle Description: Default Bundle, cannot be edited or deleted.
Congestion-Priority-Threshold: 4
ECMP-Optimization-Limit-Threshold: 7

Bundle Defaults:
Administrative Bandwidth:0 (undefined)
Preference: 0
CAC-Type: Optional
Bandwidth Activity: Dynamic with no black-hole rate
Explicit Ingress SF Path: None (undefined)
Configured Channel Ranges: None

The default multicast information policy is applied to all VPLS and VPRN services and all routing contexts until an explicitly defined multicast information policy has been mapped.

Explicit Multicast Information Policy Associations

Each VPLS service and each routing context (including VPRN routing contexts) supports an explicit association with an pre-existing multicast information policy. The policy may need to be

unique per service or routing context due to the fact that each context has its own multicast address space. The same multicast channels may be and most likely will be used for completely different multicast streams and applications in each forwarding context.

Interaction with Ingress Multicast Path Management

When ingress multicast path management is enabled on an MDA, the system automatically creates a bandwidth manager context that manages the multicast path bandwidth into the switch fabric used by the ingress ports on the MDA. As routing or snooping protocols generate L2 or L3 multicast FIB records that will be populated on the MDA's forwarding plane, they are processed though the multicast information policy that is associated with the service or routing context associated with the record. The policy will return the following information for the record to be used by the ingress bandwidth manager:

- The records administrative bandwidth ('0' if undefined)
- Preference level (0 to 7 with 7 being highest)
- Bandwidth activity monitoring setting (use admin bw or dynamic monitoring)
  If admin bw is indicated, will also return active and inactive thresholds
- Initial switch fabric multicast path (primary, secondary or ancillary)
  If ancillary path is indicated, will also return an SF destination threshold
- Explicit switch fabric multicast path (primary, secondary, ancillary or none)

Interaction with Egress Multicast CAC

The egress multicast CAC feature has its own multicast CAC policy that is applied to egress IP interfaces or egress VPLS interfaces. The policy contains bundles, each with their own sets of channel ranges defined. When a multicast joint event occurs on the interface, the system searches the multicast CAC policy to determine how that join event should be processed. The information returned from the CAC lookup provides the bundles allowed bandwidth and the channels administrative bandwidth. Since the allowed bundle bandwidth may change between differing egress interfaces, multiple policies with the same channel information may be needed.

With the addition of the multicast information policy, managing the CAC feature is simplified. The CAC monitor for the egress interface first searches the multicast CAC policy to determine if the multicast join event matches a configured channel range. If a match is found, it simply uses the local policy information. If a match is not found, it then searches the multicast information policy associated with the service or routing context to which the join event is associated. The multicast information policy returns the following information to the interfaces CAC manager:

- Bundle name
- Administrative bandwidth ('0' if undefined)
- Congestion Priority Threshold (high or low)
- CAC Type (mandatory or optional)

The CAC manager evaluates the returned results according to the following rules:

- If the returned administrative bandwidth = '0', all results are ignored
- If the returned bundle name is not found in the local multicast CAC policy, all results are ignored
- The administrative bandwidth is interpreted as channel 'bw'
- A value of 'high' for congestion priority threshold is interpreted as 'class high'
- A value of 'low' for congestion priority threshold is interpreted as 'class low'
- A value of 'mandatory' for CAC type is interpreted as 'type mandatory'

- A value of ‘optional’ for CAC type is interpreted as ‘type optional’
- Bundle bandwidth is always derived from the local multicast CAC policy

Using the multicast information policy to store the CAC information allows a single centralized managed policy for all channel information, allowing the multicast CAC policies to only have bundle defined with the appropriate bundle bandwidth. The multicast CAC policy still may be for channel information in exception cases.

Interaction with Multicast ECMP Optimization

The multicast information policy is used by the multicast ECMP optimization function to derive each channels administrative bandwidth. The ECMP function tallies all bandwidth information for channels joined and attempts to equalize the load between the various paths to the sender. The multicast information policy returns the following information to the ECMP path manager:

1. Administrative bandwidth (‘0’ if undefined)
2. Preference (0 to 7 with 7 the highest preference value)

Parameters *policy-name* — Iidentifies the name of the policy to be either created or edited. Each multicast information policy must be uniquely named within the system. Names of up to 32 ASCII characters are supported with the normal character restrictions.

create — The create keyword is required if creating a new multicast information policy when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the multicast information policy name already exists.

multicast-info-policy

Syntax **multicast-info-policy** *policy-name*
no multicast-info-policy

Context config>service>ies
config>service>vpls
config>service>vprn
config>router

Description This command overrides the default multicast information policy on a service or routing context. When the policy association is changed, all multicast channels in the service or routing context must be reevaluated.

If a multicast information policy is not explicitly associated with the service or routing context, the default multicast information policy is used when ingress multicast path management is enabled.

While a multicast information policy is associated with a service or routing context, the policy cannot be deleted from the system.

The **no** form of the command removes an explicit multicast information policy from the service or routing context and restores the default multicast information policy.

Parameters *policy-name* — The policy-name parameter is required and specifies an existing multicast information policy that should be associated with the service or routing context.

Default default

bundle

Syntax **bundle** *bundle-name* [**create**]
no bundle *bundle-name*

Context config>mcast-mgmt>mcast-info-plcy

Description The bundle command is used to create or edit channel bundles within a multicast information policy. Bundles are used for two main purposes. First, bundles are used by the multicast CAC function to group multicast channels into a common bandwidth context. The CAC function limits the ability for downstream nodes to join multicast channels based on the egress interfaces ability to handle the multicast traffic. Bundling allows multicast channels with common preference or application to be managed into a certain percentage of the available bandwidth.

The second function of bundles is to provide a simple provisioning mechanism. Each bundle within a multicast information policy has a set of default channel parameters. If each channel provisioned in to the bundle is able to use the default parameters for the bundle, the provisioning and configuration storage requirements are minimized.

Up to 31 explicit bundles may be defined within a multicast information policy (32 including the default bundle).

Once a bundle is created, the default channel parameters should be configured and the individual channel ranges should be defined. Within each channel range, override parameters may be defined that override the default channel parameters. Further overrides are supported within the channel range based on explicit source overrides.

A bundle may be deleted at anytime (except for the default bundle). When a bundle is deleted, all configuration information within the bundle is removed including multicast channel ranges. Any multicast records using the bundle should be reevaluated. Multicast CAC and ECMP managers should also be updated.

Default Bundle

Each multicast information policy contains a bundle named **default**. The default bundle cannot be deleted. Any multicast channel that fails to match a channel range within an explicit bundle is automatically associated with the default bundle.

The **no** form of the command removes a bundle from the multicast information policy. The default bundle cannot be removed from the policy.

Default default

bundle-name — Specifies bundle expressed as an ASCII string with up to 16 characters and must follow normal naming conventions. If bundle-name already exists, the system will enter the bundle context for editing purposes. If bundle-name does not exist, the system will create the defined bundle in the policy and enter the bundle context for editing purposes.

create — The create keyword is required if creating a new multicast information policy bundle when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the bundle name already exists.

admin-bw

Syntax **admin-bw** *kbps*
no admin-bw

Context config>mcast-mgmt>mcast-info-plcy
config>mcast-mgmt>mcast-info-plcy>channel

Description This command configures the administrative bandwidth.

Parameters *kbps* — Specifies the administrative bandwidth in Kbps.

Values 1 — 40000000

bw-activity

Syntax **bw-activity** {**use-admin-bw** | **dynamic** [**falling-delay** *seconds*]} [**black-hole-rate** *kbps*]
no bw-activity

Context config>mcast-mgmt>mcast-info-plcy>bundle
config>mcast-mgmt>mcast-info-plcy>channel

Description This command defines how the multicast ingress path manager determines the amount of bandwidth required by a multicast channel. The default setting is dynamic which causes the bandwidth manager to adjust the path bandwidth based on the current ingress multicast bandwidth. The alternative setting is use-admin-bw which causes the bandwidth manager to use the configured admin-bw associated with the channel. The use-admin-bw setting is enabled once the channels ingress bandwidth reaches the bandwidth-policy admin-bw-threshold value. The bandwidth manager uses the dynamic method until the threshold has been reached. If the ingress bandwidth falls below the threshold, the bandwidth manager reverts back to the dynamic method.

While operating in dynamic bandwidth mode, the bandwidth manager uses the falling-delay threshold to hold on to the previous highest bandwidth until the delay time has expired. This allows the bandwidth manager ignore momentary drops in channel bandwidth.

The bw-activity command in the bundle context defines how the current bandwidth is derived for all channels associated with the bundle unless the channel has an overriding bw-activity defined in the channel context. The channel context may also be overridden by the bw-activity command in the source-override context for a specific channel or channel range. The channel and source-override bw-activity settings default to ‘null’ (undefined) and have no effect unless explicitly set. The default-channel-info bw-activity default value is set to dynamic.

The use-admin-bw setting requires that the channel be configured with an admin-bw value that is not equal to ‘0’ in the same context as the bw-activity command using the setting. If use-admin-bw is defined in the default-channel-info context, then the default-channel-info admin-bw setting must not be set to ‘0’. A similar rule applies for channel and source-override bw-activity and admin-bw settings. Once a context has use-admin-bw configured, the context’s admin-bw value cannot be set to ‘0’ and the no admin-bw command will fail for that context.

The bw-activity command also supports an optional black-hole-rate kilobits-per-second keyword and parameter that defines at which current rate a channel should be placed in the black-hole state. This is intended to provide a protection mechanism against multicast channels that exceed a reasonable rate and cause outages in other channels.

The **no** form of the command reverts to the default parameters.

channel

Syntax **channel** *ip-address* [*ip-address*] [**create**]
no channel *ip-address* [*ip-address*]

Context config>mcast-mgmt>mcast-info-plcy>bundle

Description This command defines explicit channels or channel ranges that are associated with the containing bundle. A channel or channel range is defined by their destination IP addresses. A channel may be defined using either IPv4 or IPv6 addresses. If a channel range is being defined, both the start and ending addresses must be the same type.

A specific channel may only be defined within a single channel or channel range within the multicast information policy. A defined channel range cannot overlap with an existing channel range.

If a channel range is to be shortened, extended, split or moved to another bundle, it must first be removed from its existing bundle.

Each specified channel range creates a containing context for any override parameters for the channel range. By default, no override parameters exist.

The **no** form of the command removes the specified multicast channel from the containing bundle.

Parameters **start-channel-ip-address** [*end-channel-ip-address*] **—** The start-channel-ip-address parameter and optional end-channel-ip-address parameters define the starting and ending destination IP addresses for a channel range.

If only the start-channel-ip-address is given, the channel ranges comprises of a single multicast channel.

If both the starting and ending address are specified, all addresses within the range including the specified address are part of the channel range.

IPv4 or IPv6 addresses may be defined. All specified addresses must be valid multicast destination addresses. The starting IP address must be numerically lower then the ending IP address. [What do we do with 224.0.0.x addresses?]

Values Any valid IP multicast destination address

Default None

create — The create keyword is required if creating a new multicast channel range when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the specified channel range already exists.

source-override

Syntax **source-override** *ip-address* [**create**]
no source-override *ip-address*

Context config>mcast-mgmt>mcast-info-plcy>bundle>channel

Description This command defines a multicast channel parameter override context for a specific multicast sender within the channel range. The specified senders IP address must be of the same type (IPv4 or IPv6) as the containing channel range.

The **no** form of the command removes the specifed sender override context from the channel range.

Default none

Parameters *ip-address* — Specifies either am IPv4 or IPv6 address and it must be the same type as the containing channel range.

Values

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D

create — The create keyword is required if creating a new source override when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the specified source override IP address already exists.

VIDEO POLICY COMMANDS

video-policy

Syntax **video-policy**

Context config>mcast-mgmt>mcast-info-plcy

Description This command enables the context to configure video interfaces and video services.

video-interface

Syntax **video-interface** *ip-address* [**create**]
no video-interface *ip-address*

Context config>mcast-mgmt>mcast-info-plcy>video-policy

Description This command creates a video interface policy context that correlates to the IP address assigned for a video interface. This interface is created in a subscriber service to which the multicast information policy is assigned. If the specified IP address does not correlate to a video interface ip address, the parameters defined within this context have no effect.

The **no** form of the command deletes the video interface policy context.

Parameters *ip-address* — The IP address of a video interface provisioned within the context of a service to which the Multicast Information Policy is assigned. If the IP address does not match the IP address assigned to a video interface, the parameters defined within this context have no effect.

create — Mandatory keyword needed when creating a new video interface within the video policy.

hd

Syntax **hd**

Context config>mcast-mgmt>mcast-info-plcy>video-policy>video-if

Description This command configures properties relating to requests received by the video interface for High Definition (HD) channel requests.

Default none

dent-threshold

Syntax **dent-threshold** *threshold*
no dent-threshold

Context config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd

config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd

Description This command sets the threshold value below which the FCC server will dent/drop unicast data sent to the FCC client during a fast channel change. Within the RTP extension header, the packet priority (PRI) (2 bits) and the fine-grained priority (FPRI) (3 bits) indicate the "importance" of the frame as to how essential it is to the video stream.

This parameter is only applicable if the FCC server mode is **dent**.

The **no** form of the command returns the parameter to the default value.

Default 16 (only B frames are dropped)

Parameters *threshold* — The threshold value is used by the FCC server to compare with the concatenation of the PRI and FPRI to determine whether to send the packet to the FCC client. If the PRI and FPRI expressed as a decimal integer is greater than or equal to the threshold value, the packet will be sent.

Values 1 — 31

fcc-burst

Syntax **fcc-burst** *burst-percentage*
no fcc-burst

Context config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd

Description This command sets the burst rate at which the Fast Channel Change (FCC) server will send unicast data to the FCC client above the received rate to allow the client to catchup to the multicast stream.

This parameter is only applicable if the FCC server mode is **burst**.

The **no** form of the command returns the parameter to the default value.

Default 25

Parameters *burst-percentage* — Specifies the percentage of nominal bandwidth used to catch up to the multicast stream.

Values

HD:	0 — 100
SD and PIP:	0 — 600

Default 25

fcc-server

Syntax **fcc-server** [**mode** {**burst | dent | hybrid**}]
no fcc-server

Context config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip

config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd

Description This command enables the Fast Channel Change (FCC) server and sets the mode to send the FCC unicast stream.

The mode indicates how the FCC server will send information to the client. When **burst** is specified, the FCC server will send the channel at a nominally faster rate than the channel was received based on the applicable fcc-burst setting. When **dent** is specified, the FCC server will selectively discard frames from the original stream based on the applicable dent-threshold setting. If no mode is specified, burst is the default mode.

The **no** form of the command disables the FCC server at that context and subordinate contexts.

Default no fcc-server

Parameters **mode burst —** Sets the mode of the FCC server to burst when sending the channel to the FCC client.

mode dent — Sets the mode of the FCC server to dent when sending the channel to the FCC client.

mode hybrid — Combines the burst and dent modes.

local-rt-server

Syntax [**no**] **local-rt-server**

Context config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd

Description This command enables the local retransmission server function for requests directed to the IP address.

The **no** form of the command disables the retransmission server.

Default no local-rt-server

mc-handover

Syntax **mc-handover** *percentage*
no mc-handover

Context config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd

Description This command sets the rate at which the Fast Channel Change (FCC) server will send unicast data to the FCC client during the handover to the multicast stream.

The **no** form of the command returns the parameter to the default value.

Parameters *percentage* — Specifies the percentage of nominal bandwidth.

Values

HD:	0 — 100
SD and PIP:	0 — 600

Default 25

rt-mcast-reply

Syntax **rt-mcast-reply** [**count** *count*] [**interval** *milliseconds*] [**hold-time** *milliseconds*]
no rt-mcast-reply

Context config>mcast-mgmt>mcast-info-plcy>video-policy>video-if

Description This command enables the use of multicast retransmission packets by the retransmission server in response to a number of identical retransmission requests.

By default, the retransmission server replies to all retransmission requests with a unicast stream directed to the client requesting retransmission. Enabling multicast retransmission on the retransmission server is an optimization where a number of identical retransmission requests received will trigger the retransmission server to service the retransmission request with a single multicast reply stream with packets of Payload Type 33. An example of where multiple clients will request retransmission for identical packets is if there is a packet loss in the Access Network which affects multiple clients.

For clients that received the original packets or requested retransmission and had the retransmission serviced in unicast, the multicast retransmission will look like duplicate packets and discard the multicast retransmitted packets. For other clients, the multicast retransmission will look like out-of-sequence multicast packets, so the client must support reception of out of sequence multicast for multicast retransmission for multicast retransmission to be used.

The threshold value for identical retransmission requested received by the retransmission server is configured when enabling multicast retransmission along with a sample interval and a hold time. The sample interval is the elapsed time over which the retransmission requests are counted. The hold time is a quiet period after a multicast retransmission is triggered on the retransmission server where an identical retransmission request will be ignored. After the hold time expires, a new sampling interval is started. Sampling intervals will be restarted until the packets for the multicast request are cleared from the retransmission buffer.

To illustrate the threshold count, sample interval and hold time, suppose the values are 5, 100 ms and 50 ms, respectively. The first retransmission request arrives at time = 0. In one scenario, assume the fifth identical retransmission request arrives at the server at time = 60 ms. In this case, the first four retransmission requests are serviced as unicast and the arrival of the fifth retransmission request triggers a multicast retransmission. All identical retransmission requests received between time = 60 and 110 ms are ignored. At time = 110 ms, a new sampling period is started and retransmission requests are serviced in unicast unless the threshold is passed again in the new sampling period. For a second scenario, assume the fifth identical retransmission request arrives at time = 25 ms. In this scenario, the behavior is the same except the new sampling period starts at time = 75 ms even though this is before the original sampling period was set to expire.

The **no** form of the command disables retransmissions using multicast, so all retransmissions will be sent as unicast.

Default no rt-mcast-reply – Retransmission requests will only be serviced with unicast retransmission replies.

Parameters **count** *count* — Specifies the number of identical retransmission requests received for a packet in a sampling interval after which a reply will be sent as multicast Payload Type 33.

Values 2 – 1024

Default 5

interval *milliseconds* — Specifies the number of milliseconds for a sampling interval .

Values 100 – 8000 ms

Default 100 ms

hold-time *milliseconds* **—** Specifies the number of milliseconds after a multicast reply is sent that the retransmission server will wait before starting a new sampling period

rt-payload-type

Syntax **rt-payload-type** *payload-type*
no rt-payload-type

Context config>mcast-mgmt>mcast-info-plcy>video-policy>video-if

Description This command describes the format to be used by Retransmission (RT) server to send retransmission packets. The RET server interface allows the payload type within the retransmission packets to be configured.

Default 99 — Indicates that the frames will be sent in the RFC 4588, *RTP Retransmission Payload Format*, format.

Parameters *payload-type* — Indicates the format expected for received retransmission packets. The value 33 indicates that the frames will be received as originally sent. A value between 96 and 127 indicates the dynamic payload type value (per RFC 3551) to be used for RFC 4588 formatted retransmission packets.

Values 33, 96 – 127

rt-rate

Syntax **rt-rate** *rt-burst-percentage*
no rt-rate

Context config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd

Description This command sets the rate of nominal bandwidth at which retransmission packets are sent to the retransmission client for requests directed to the IP address.

The **no** form of the command returns the parameter to the default value.

Default 5

Parameters *rt-burst-percentage* — Specifies the percentage of nominal bandwidth to send retransmission packets.

Values 1— 100

Default 5

max-sessions

Syntax **max-sessions** *sessions*
no max-sessions

Context config>mcast-mgmt>mcast-info-plcy>video-policy>video-if

Description This command configures the per-client maximum number of sessions.

The **no** form of the command reverts to the default value.

Parameters *sessions* — Specifies the per-client maximum number of sessions.

Values 1 — 65536

Default 256

pip

Syntax **pip**

Context config>mcast-mgmt>mcast-info-plcy>video-policy>video-if

Description This command enables the context within a video interface policy to configure properties relating to requests received by the video interface for Picture-in-Picture (PIP) channel requests.

Default none

sd

Syntax **sd**

Context config>mcast-mgmt>mcast-info-plcy>video-policy>video-if

Description This command enables the context within a video interface policy to configure properties relating to requests received by the video interface for Standard Definition (SD) channel requests.

subscriber-bw-limit

Syntax **subscriber-bw-limit** *bandwidth*
no subscriber-bw-limit

Default config>mcast-mgmt>mcast-info-plcy>video-policy>video-if

Description This command configures of an egress per-subscriber bandwidth limit for the combined retransmission and Fast Channel Change (FCC) replies for requests received directed to the IP address. If the bandwidth for a request will exceed the bandwidth limit, the request is logged and dropped.

The **no** form of the command disables enforcement of an egress bandwidth limit.

Default 4294967295

Parameters *bandwidth* — The per-subscriber egress bandwidth limit for retransmission and FCC packets in kilobits per second expressed as an integer indicates infinity or no limit.

Values 1 — 4294967295 kbps

BUNDLE AND CHANNEL COMMANDS

video

Syntax **video**

Context config>mcast-mgmt>mcast-info-plcy>bundle
config>mcast-mgmt>mcast-info-plcy>bundle>channel
config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override

Description This command enables the context to configure video parameters.

fcc-channel-type

Syntax **fcc-channel-type** {**hd** | **sd** | **pip**}
no fcc-channel-type

Context config>mcast-mgmt>mcast-info-plcy>bundle>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video

Description This command configures the channel type for the bundle/channel. The channel type is used in the video policy to set various Fast Channel Change (FCC) parameters including the type of FCC and various FCC rates.

The no form of the command returns the parameter to the default value.

Default no fcc-channel

Parameters **hd** — The channel type is High-Definition (HD) (Default).

sd — The channel type is Standard Definition (SD).

pip — The channel type is Picture in Picture (PIP).

fcc-min-duration

Syntax **fcc-min-duration** *time*
no fcc-min-duration

Context config>mcast-mgmt>mcast-info-plcy>bundle>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>video

Description This command configures the minimum time duration, in milliseconds, of the Fast Channel Change (FCC) burst. The value of this object determines the starting point of the FCC burst. If the current Group of Pictures (GOP) has less than the minimum duration worth of data, FCC burst begins from the previous GOP.

The **no** form of the command reverts to the default value.

Default 300

Parameters *time* — Specifies the FCC burst minimum duration, in milliseconds.

Values 300 — 8000

fcc-server

Syntax **fcc-server** [**disable**]
no fcc-server

Context config>mcast-mgmt>mcast-info-plcy>bundle>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video

Description This command enables Fast Channel Change (FCC) for a multicast bundle or channel. Note that additional parameters such as **fcc-channel-type** should also be configured to match the characteristics of the bundle/channel.

The **no** form of the command disables removes the FCC configuration for the bundle/channelcontext and implies the setting is inherited from a higher context or the default policy.

Default no fcc

Parameters **disable —** Explicitly disables the FCC server within the policy. For the default bundle within the default multicast information policy, the **no** form of the command and the **disable** keyword have the same meaning and imply that the server is disabled.

local-fcc-port

Syntax **local-fcc-port** *port*
no local-fcc-port

Context config>mcast-mgmt>mcast-info-plcy>bundle>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video

Description This command configures the local port on which Fast Channel Change (FCC) requests are received. The value of this object can only be set for the default bundle and will be used by all bundles and channels.

The **local-fcc-port** *port* value is the only configuration parameter in the bundle “default” context.

The **no** form of the command removes the port from the video configuration.

Parameters *port* — Specifies a local port for FCC requests.

Values 1024 — 65535

local-rt-port

Syntax **local-rt-port** *port*
no local-rt-port

Context config>mcast-mgmt>mcast-info-plcy>bundle>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video

Description This command configures the local port on which retransmission (RET) requests are received. The value of this object can only be set for the default bundle and will be used by all channels.

The **local-rt-port** *port* value is the only configuration parameter in the bundle "default" context.

The **no** form of the command removes the port from the video configuration.

Parameters *port* — Specifies a local port for RT requests.

Values 1024 — 65535

local-rt-server

Syntax **local-rt-server** [**disable**]
no local-rt-server

Context config>mcast-mgmt>mcast-info-plcy>bundle>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video

Description This command enables the local retransmission server capability on the ISA video group.

RET server parameters can be configured in a multicast information policy or a service, but the parameters will have no effect if the RET server is disabled or if the video group is administratively disabled (shutdown).

The **no** form of the command returns the parameter to the default value where the RET server is disabled on the video group.

Default no local-rt-server

Parameters **disable —** Specifies to disable the RET server.

reorder-audio

Syntax **reorder-audio** *time*
no reorder-audio

Context config>mcast-mgmt>mcast-info-plcy>bundle>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>video

Description This command configures the time, in milliseconds, by which the audio packets are reordered in the ad stream.

Configuring this parameter depends on what is configured on the A Server and the GOP sizes of the network stream. Typically, this configuration should match the A Server configuration.

The **no** form of the command removes the time value from the configuration.

Default no redorder-audio

Parameters *time* — Specifies the audio reorder time, in milliseconds.

Values 100 — 1000

rt-buffer-size

Syntax **rt-buffer-size** *rt-buffer-size*
no rt-buffer-size

Context config>mcast-mgmt>mcast-info-plcy>bundle>channel>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video

Description This command configures the retransmission buffer for channels within the bundle or channel range.

The **no** form of the command returns the parameter to the default value.

Default 300

Parameters *rt-buffer-size* — Specifies the buffer size, in milliseconds, to store channel packets.

Values 300 — 8000

rt-server

Syntax **rt-server disable**
rt-server *ip-address* **port** *port-num*
no rt-server

Context config>mcast-mgmt>mcast-info-plcy>bundle>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video

Description This command enables and configures the upstream retransmission server configuration parameters.

The **no** form of the command removes the upstream retransmission server configuration and implies the configuration is inherited from a higher context or from the default policy.

Default no rt-server – The upstream retransmission server settings are inherited.

Parameters **disable —** This keyword explicitly disables the upstream retransmission server within the policy. For the default bundle within the default Multicast Information Policy, the **no** form of the command and the disable keyword have the same meaning and imply the server is disabled.

ip-address — The IP address of the upstream retransmission server.

port *num* **—** The UDP port to use to send RET requests to the upstream RET server.

Values 1024 — 65535

source-port

Syntax **source-port** *port-num*
no source-port

Context config>mcast-mgmt>mcast-info-plcy>bundle>video

Description This command configures the source port for upstream RET requests.

The **source-port** *port-num* value is the only configuration parameter in the bundle "default" context.

The **no** form of the command removes the value from the configuration.

Parameters *port-num* — Specifies the source port in the received RTP multicast stream.

Values 1024 — 65535

video-group

Syntax **video-group** *video-group-id*
video-group disable
no video-group

Context config>mcast-mgmt>mcast-info-plcy>bundle>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video

Description This command assigns a video group ID to the channel.

Parameters *video-group-id* — specifies the identifier for this video group. The video group must have been configured in the **config>isa** context.

Values 1 — 4

disable — Explicitly disables the video group within the policy.

SERVICE VIDEO INTERFACE COMMANDS

video-interface

Syntax **video-interface** *ip-int-name* [**create**]
no video-interface *ip-int-name*

Context config>service>ies
config>service>vpls
config>service>vprn

Description This command creates a video interface within the service. The video interface and associated IP addresses are the addresses to which clients within the service will send requests.

The video interface must be associated with an ISA group using the video-sap command and have IP addresses for it to be functional.

The no form of the command deletes the video interface. The video interface must be administratively shut down before issuing the **no video-interface** command.

Default none

Parameters *ip-int-name* — Specifies the name of the video interface up to 32 characters in length. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

create — This keyword is mandatory when creating a video interface.

address

Syntax [**no**] **address** *ip-address/mask*

Context config>service>ies>video-interface
config>service>vpls>video-interface
config>service>vprn>video-interface

Description This command assigns an IP address to the video interface within the service. Video interface IP addresses are used by video service clients to direct requests for video server services. Up to 16 IP address/subnets can be defined. Note that the addresses defined must all be distinct and cannot be contained within a previously defined address.

In the VPLS context, only one IP address can be defined for a video interface.

The **no** form of the command deletes the IP address/subnet from the video interface.

Default none

Parameters *ip-address* — The IP address/subnet of the video interface in dotted decimal notation.

mask — The subnet mask length for the IP address expressed as an integer.

adi

Syntax **adi**

Context config>service>ies>video-interface
config>service>vprn>video-interface

Description This command enables the context to configure ad insertion (ADI) for the video interafce.

channel

Syntax **channel** *mcast-address* **source** *ip-address* [**channel-name** *channel-name*]
no channel *mcast-address* **source** *ip-address*

Context config>service>ies>video-interface>adi
config>service>vprn>video-interface>adi

Description This command configures channel parameters for ad insertion.

Parameters *mcast-address* — Specifies the multicast addres.

source *ip-address* **—** Specifies the source IP address.

channel-name *channel-name* **—** Specifies the channel name up to 32 characters in length.

cpu-protection

Syntax **cpu-protection** *policy-id*
no cpu-protection

Context config>service>vpls>video-if
config>service>ies>video-if
config>service>vprn>video-if

Description This command assigns an existing CPU protection policy to the associated service video interface. The CPU protection policies are configured in the **config>sys>security>cpu-protection>policy** *cpu-protection-policy-id* context. The number of RTCP messages per client will be limited to the number as configured under the policy.

Default none

Parameters *policy-id* — Specifies a CPU protection policy.

Values 1 — 255

scte35-action

Syntax **scte35-action** {**forward** | **drop**}

Context config>service>ies>video-interface>adi>channel

config>service>vprn>video-interface>adi>channel

Description This command specifies whether the Society of Cable Telecommunications Engineers 35 (SCTE 35) cue avails in the stream need to be forwarded or not. When specified to forward, SCTE 35 messages will be forwarded downstream. When specified to drop, SCTE 35 messages will not be forwarded downstream. They will be still be processed for local splicing decisions.

Parameters **forward —** Forwards SCTE 35 messages downstream.

drop — Drops SCTE 35 messages.

zone-channel

Syntax **zone-channel** *mcast-address* **source** *ip-address* **adi-channel-name** *channel-name*
no zone-channel *mcast-address* **source** *ip-address*

Context config>service>ies>video-interface>adi>channel
config>service>vprn>video-interface>adi>channel

Description This command configures zone-channel parameters or ad insertion. The channel configuration along with the zone-channel configuration associates a network channel to a zone-channel and builds the store and forward relationship.

Parameters *mcast-address* — Specifies the IP multicast group address for which this entry contains information.

source *ip-address* **—** Specifies the type of address to be used for a source address/

adi-channel-name *channel-name* **—** Specifies the name for this zone channel.

scte30

Syntax **scte30**

Context config>service>ies>video-interface>adi
config>service>vprn>video-interface>adi

Description This command enables the context to configure SCTE 30 parameters.

ad-server

Syntax [**no**] **ad-server** *ip-address*

Context config>service>ies>video-interface>adi>scte30
config>service>vprn>video-interface>adi>scte30

Description This command configures the ad server address. A TCP session will be accepted for SCTE 30 messaging only for IP addresses that appear in this configuration.

The **no** form of the command removes the address from the ad server configuration.

Parameters *ip-address* — Specifies the IP address of the ad server.

local-address

Syntax **local-address control** *ip-address* **data** *ip-address*
no local-address

Context config>service>ies>video-interface>adi>scte30
config>service>vprn>video-interface>adi>scte30

Description SCTE 30 requires a TCP session per zone-channel between the ad server and splicer for control communication and it requires UDP sessions on which the video ad stream is sent. This command specifies the splicer's control IP address to which the ad-server(s) should setup TCP connections and the data IP address to which the video ad streams should be sent.

The no form of the command removes the address information from the local address configuration.

Parameters **control** *ip-address* **—** Specifies the local IP address to which ad servers send Society of Cable Telecommunications Engineers 30 (SCTE 30) ad control streams. This address should be in the same subnet as the ip address assigned to the video interface.

The values of **control** *ip-address* and the **data** *ip-address* specify the local IP address to which ad servers send SCTE 30 ad data streams, must be set together in the same SNMP request PDU or else the set request will fail with an inconsistent value error.

data *ip-address* **—** Specifies the local IP address to which ad servers send Society of Cable Telecommunications Engineers 30 (SCTE 30) ad data streams. This address should be in the same subnet as the ip address assigned to the video interface.

The values of the **control** *ip-address* and the **data** *ip-address* specifiy the local IP address to which ad servers send SCTE 30 ad control streams, must be set together in the same SNMP request PDU or else the set request will fail with an inconsistent value error.

multicast-service

Syntax **multicast-service** *service-id*
no multicast-service

Context config>service>ies>video-interface
config>service>vpls>video-interface
config>service>vprn>video-interface

Description This command adds a multicast service association to the video interface. This parameter is not required on the video interface when the service carries both unicast and multicast traffic.

When multicast and unicast are carried in separate service instances, the operator can set this parameter on the unicast video interface to form an association with the multicast service when replies need to be sent in the multicast service instance.

When multicast and unicast are carried in separate services when a downstream device (such as a DSLAM) can perform a service cross connect between the services and performs multicast replication.

The **no** form of the command removes the multicast service association.

Default none

Parameters *service-id* — The service ID of the associated multicast service.

Values *service-id*: 1 — 2147483647
svc-name: 64 characters maximum

rt-client-src-address

Syntax **rt-client-src-address** *ip-address*
no rt-client-src-address

Context config>service>ies>video-interface
config>service>vpls>video-interface
config>service>vprn>video-interface

Description This command assigns the IP address for the retransmission client on the video interface within the service. The RET client IP address is the originating address used for communication with upstream RET servers. If no RET client address is assigned, the RT client is operationally down as the RET client configuration is incomplete.

For a VPLS service, the RET client address cannot be the same as an existing address for the video interface, but it must be an address within a video interface subnet.

For IES and VPRN, the RET client address can be the same as an existing address for the video interface or an address within a video interface subnet.

The **no** form of the command deletes the RT client address from the video interface.

Default none

Parameters *ip-address* — Specifies the IP address for the retransmission client on the video interface within the service.

video-sap

Syntax **video-sap** *video-group-id*
no video-sap

Context config>service>ies>video-interface
config>service>vpls>video-interface
config>service>vprn>video-interface

Description This command configures a service video interface association with a video group.

The **no** form of the command removes the video group association.

Parameters none

Parameters *video-group-id* — Specifies the video group ID number.

Values 1 — 4

egress

Syntax **egress**

Context config>service>ies>video-interface>video-sap
config>service>vpls>video-interface>video-sap
config>service>vprn>video-interface>video-sap

Description This command enables the context to configure egress parameters for the service's video SAP.

ingress

Syntax **ingress**

Context config>service>ies>video-interface>video-sap
config>service>vpls>video-interface>video-sap
config>service>vprn>video-interface>video-sap

Description This command enables the context to configure in parameters for the service's video SAP.

qos

Syntax **qos** *policy-id*
no qos

Context config>service>ies>video-interface>video-sap>egress
config>service>vpls>video-interface>video-sap>egress
config>service>vprn>video-interface>video-sap>egress
config>service>ies>video-interface>video-sap>ingress
config>service>vpls>video-interface>video-sap>ingress
config>service>vprn>video-interface>video-sap>ingress

Description This command associates an existing egress or ingress QoS policy to a video interface. If the policy-id does not exist, an error will be returned. Attempts to associate a QoS policy of the wrong type returns an error.

Only one QoS policy can be associated with a video interface at one time in the ingress and egress contexts. Attempts to associate a second QoS policy of a given type will return an error.

The **no** form of the command removes the QoS policy association from the video interface, and the QoS policy reverts to the default.

Default default QoS policy

Parameters *policy-id* — The sap-egress or sap-ingress policy ID to associate with the video interface on ingress/egress. The policy ID must already exist.

Values 1 — 65535

filter

Syntax **filter ip** *ip-filter-id*
no filter

Context config>service>ies>video-interface>video-sap>egress
config>service>vpls>video-interface>video-sap>egress
config>service>vprn>video-interface>video-sap>egress
config>service>ies>video-interface>video-sap>ingress
config>service>vpls>video-interface>video-sap>ingress
config>service>vprn>video-interface>video-sap>ingress

Description This command associates an existing IP filter policy with an ingress or egress video SAP. Filter policies control the forwarding and dropping of packets based on the matching criteria.

Filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to the match criteria, so the default action in the filter policy applies to these packets.

The **no** form of this command removes any configured filter ID association with the SAP. The filter ID itself is not removed from the system.

Parameters **ip** *ip-filter-id* — Specifies the ID for the IP filter policy.

Values 1 — 65535

gateway-ip

Syntax [**no**] **gateway-ip** *ip-address*

Context config>service>vpls>video-interface

Description This command assigns a gateway IP address for the video interface within the VPLS service. Because VPLS is a Layer 2 service and the video interface is modeled like a host within the service, the video interface needs a gateway IP to send requests to devices outside of the VPLS subnet.

The **no** form of the command deletes the gateway IP address from the VPLS video interface.

Default none

Parameters *ip-address* — Specifies the gateway IP address of the VPLS video interface.

Show Commands

video-group

Syntax **video-group** [*video-group-id*]

Context show>isa

Description This command displays ISA IPsec group information

Parameters *ipsec-aa-group-id* — Specifies the ISA video group ID.

Sample Output

```
A:SR-7/Dut-C# show isa video-group
===============================================================================
ISA Video Group
===============================================================================
Video Group Id         : 1              Admin State            :  Up
Oper State             : Up             RT Server State        :  Enabled
FCC Server State       : Disabled       ADI State              :  Disabled
RT Resv Bandwidth(Mbps): 0              ADI State              :  Disabled

MDA                    : 2/1            Channels               :  2
Admin State            : Up             Oper State             :  Up
Used Cache (bytes)     : 586622         Available Cache (bytes): 1869186816
Mem alloc failures     : 0              Dropped pkts (denting) : 0
Failed Chnl Allocs     : 0              Egress Bandwidth excee*:  0
Bandwidth in use(kbps) : 0              Peak Bandwidth(kbps)   : 200
Egress stream resets   : 0              Ingress stream resets  : 53
Ad stream resets       : 0              Ad stream aborts       :  0
SSRC collisions        : 0              Received data packets  : 4521
Received data octets   : 6284714        Rx data packet errors  : 0
Transmitted data packts: 1183           Transmitted data octets:  1646212
Tx data packet errors  : 0              Tx lost data packets   : 47
Active RTCP sessions   : 1              Requested RTP Packets  : 968
RTCP Parse Errors      : 0              RTCP Config Errors     : 0
RTCP IPC Errors        : 0              RTCP SG Errors         :  0
RTCP Subscriber Errors : 0              RTCP Interface Errors  : 0
Total RET BW (Kbps)    : 0              Max. RET BW (Kbps)     : 100
Total FCC BW (Kbps)    : 0              Drop Count for FCC     : 0
Mcast RET Req for RTCP : 0              Mcast RET Req for RUDP : 0
Mcast RET Created      : 0              Mcast RET Req Quenched : 0
HighPkt pool limit hit : 0
Pkts Lost (2-10)       : 24             Pkts Lost (11-20)      : 48
Pkts Lost (21-30)      : 0              Pkts Lost (31-40)      : 0
Pkts Lost ( >40)       : 0
-------------------------------------------------------------------------------
Video-groups : 1
===============================================================================
* indicates that the corresponding row element may have been truncated.
A:SR-7/Dut-C#
```

adi

Syntax **adi** [**service** *service-id*] [**interface** ip-*int-name*] [**address** *mcast-address*] [**source** *ip-address*] [**detail**]

Context show>video

Description This command displays ad insertion channel information.

Parameters **service** *service-id* **—** Displays information pertaining to the specified service ID.

Values 1 — 2147483648
svc-name — a string up to 64 characters in length.

interface *ip-int-name* **—** Displays information pertaining to the specified interface.

address *mcast-address* **—** Displays information pertaining to the specified multicast channel address.

source *ip-address* **—** Displays information pertaining to the source IP address.

detail — The output displays detailed information.

channel

Syntax **channel** [**service** *service-id*] [**interface** *ip-int-name*] [**address** *mcast-address*] [**source** *ip-address*] [**summary** | **detail**]

Context show>video
show>video>adi

Description This command displays video channel information.

Parameters **service** *service-id* **—** Displays video channel information pertaining to the specified service ID.

Values service-id: 1 — 214748364
svc-name: A string up to 64 characters in length.
router-name: Base, management, vpls-management

Default Base

interface *ip-int-name* **—** Displays video channel information pertaining to the specified interface.

address *mcast-address* **—** Displays video channel information pertaining to the specified multicast channel address.

source *ip-address* **—** Displays video channel information pertaining to the source IP address.

summary — The output displays summarized video channel information.

detail — The output displays detailed video channel information.

Sample Output

```
*B:IPTV-SR7# show video adi channel
===============================================================================
Adi Channel Info
===============================================================================
```

```
SvcId       Interface Name   Group Address    Source Address   Channel Name
-------------------------------------------------------------------------------
100         video-100        234.4.5.228      195.168.9.10     228
100         video-100        234.4.5.240      195.168.9.10     240
100         video-100        234.4.5.241      195.168.9.10     241
...
===============================================================================
*B:IPTV-SR7#


*A:Dut-C# show video channel
===============================================================================
Video channel
===============================================================================
Service Id     Group Address        Stream   SSRCId       RxPackets  TxPackets
 Interface      Source Address       GrpId    Src/DstPrt   RxBytes    TxBytes
-------------------------------------------------------------------------------
1              234.0.0.1            Network  0            0          0
 vi             1.0.102.102          1        33333/40005  0          0
1              234.0.0.2            Network  0            0          0
 vi             1.0.102.102          1        33333/40005  0          0
1              234.0.0.3            Network  0            0          0
 vi             1.0.102.102          1        33333/40005  0          0
1              234.0.0.4            Network  0            0          0
 vi             1.0.102.102          1        33333/40005  0          0
1              234.0.0.5            Network  0            0          0
 vi             1.0.102.102          1        33333/40005  0          0
1              234.0.0.6            Network  0            0          0
 vi             1.0.102.102          1        33333/40005  0          0
1              234.0.0.7            Network  0            0          0
 vi             1.0.102.102          1        33333/40005  0          0
1              234.0.0.8            Network  0            0          0
...
1              234.0.0.249          Network  0            0          0
 vi             1.0.102.102          1        33333/40005  0          0
1              234.0.0.250          Network  0            0          0
 vi             1.0.102.102          1        33333/40005  0          0
-------------------------------------------------------------------------------
Number of channels : 250
===============================================================================
*A:Dut-C#


*A:Dut-C# show video  channel detail
===============================================================================
Video channel detail
===============================================================================
Service Id       : 1
Interface Name   : vi
Group Address    : 234.0.0.1
Source Address   : 1.0.102.102
SSRC Id (hex)    : ea000001             Group Id         : 1
UDP Source Port  : 33333                UDP Dest Port    : 40005
Stream Type      : Network              Up Time          : 0d 00:01:54
Admin Buffer     : 1000                 Oper Buffer      : 0
Admin Bandwidth  : 3300                 Received Bytes   : 44107480
Received Pkts    : 31732                Rx Invalid Pkts  : 0
Tx Bytes         : 0                    Tx Packets       : 0
Tx Failed Pkts   : 0

RTClnt AdmState  : Up                   RT Server Port   : 4098
```

```
RT Server Address: 4.4.4.4
Received Bytes   : 0                    Received Pkts    : 0
Tx RT Req        : 0                    Tx Repeat RTReq  : 0
Gaps detected    : 0                    Failed RT Req    : 0

Local RT Server Admin State : Up
RTP Pkts Req     : 0                    Rcvd RT Req      : 0
Failed RT Req    : 0                    Trans RT Replies : 0
Transmittd Bytes : 0                    Tx Packets       : 0

FCC Svr AdmState : Up                   FCC Svr Chl Type : HD
Rx FCC Requests  : 449                  Failed FCC Req   : 0
Tx FCC Replies   : 449                  Tx Bytes         : 17054546
Tx Packets       : 295583
-------------------------------------------------------------------------------
*A:Dut-C#
```

interface

Syntax **interface** [**service** *service-id*] [**interface** *ip-int-name*] [**stats** {**rt-server** | **fcc-server**}]

Context show>video

Description This command displays video interface information.

Parameters **service** *service-id* **—** Displays video interface information pertaining to the specified service ID.

Values 1 — 2147483648
svc-name — a string up to 64 characters in length.

interface *ip-int-name* **—** Displays video interface information pertaining to the specified interface.

stats — Displays video interface statistics.

Values **rt-server** — Displays video interface statistics for the RET server.
fcc-server — Displays video interface statistics for the FCC server.

Sample Output

```
*A:Dut-C# show video  interface
===============================================================================
Video interface
===============================================================================
Service Id       : 1
Name             : vi
Admin/Oper State : Up/Up                If Index         : 0
Video Group Id   : 1                    Sap Id           : lag-201:5
Sessions         : 2000                 Mcast Protocol   : PIM

Address          : 3.3.3.3/32
Tx Failed Pkts   : 0
SCTE30 TCP sess  : 0                    SCTE30 INIT sess : 0
SD RT Srvr State : Enabled
SD RT Requests   : 0                    SD Failed Req    : 0
SD RTP Pkts Req  : 0                    SD RT Replies    : 0
Tx SD Bytes      : 0                    Tx SD Packets    : 0
HD RT Srvr State : Enabled
```

```
HD RT Requests   : 0                    HD Failed Req    : 0
HD RTP Pkts Req  : 0                    HD RT Replies    : 0
Tx HD Bytes      : 0                    Tx HD Packets    : 0
PIP RT Svr State : Enabled
PIP RT Requests  : 0                    PIP Failed Req   : 0
PIP RTP Pkts Req : 0                    PIP RT Replies   : 0
Tx PIP Bytes     : 0                    Tx PIP Packets   : 0
SD FCC Svr State : Enabled              SD FCC Svr Mode  : Burst
SD FCC Requests  : 0                    SD Failed Req    : 0
Tx SD Bytes      : 0                    Tx SD Packets    : 0
SD FCC Replies   : 0
HD FCC Svr State : Enabled              HD FCC Svr Mode  : Burst
HD FCC Requests  : 448820               HD Failed Req    : 0
Tx HD Bytes      : 17150845788          Tx HD Packets    : 293148098
HD FCC Replies   : 448820
PIP FCCSvr State : Enabled              PIP FCC Svr Mode : Burst
PIP FCC Requests : 0                    PIP Failed Req   : 0
Tx PIP Bytes     : 0                    Tx PIP Pkts      : 0
PIP FCC Replies  : 0
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
*A:Dut-C#
```

session

Syntax **session** [**service** *service-id*] [**interface** *ip-int-name*] [**address** *mcast-address*] [**source** *ip-address*]

Context show>video>adi

Description This command displays ADI video session information.

Parameters **service** *service-id* **—** Displays video session information pertaining to the specified service ID.

Values 1 — 2147483648
svc-name — a string up to 64 characters in length.

interface *ip-int-name* **—** Displays session information for the specified interface.

address *mcast-addres***s —** Displays session information for the specified multicast address.

source *ip-address* **—** Displays session information for the specified IP address.

Sample Output

```
*B:IPTV-SR7# show video adi session
===============================================================================
Adi Session
===============================================================================
Service Id       : 100                  Interface Name   : video-100
Group Address    : 234.4.5.241          Source Address   : 100.100.100.1
Ad Server Addr   : 10.200.14.2          Up Time          : 0d 13:30:02
Init Requests    : 1                    Succ/Unsucc Resp : 1/0
Alive Requests   : 0                    Succ/Unsucc Resp : 0/0
Cue Requests     : 0                    Succ/Unsucc Resp : 0/0
Abort Requests   : 0                    Succ/Unsucc Resp : 0/0
```

```
Splice Requests  : 910                  Succ/Unsucc Resp : 906/4
Successful splice-in complete responses     : 902
Successful splice-out complete responses    : 894
Unsuccessful splice-out complete responses  : 11
Invalid SCTE30 R*: 0
-------------------------------------------------------------------------------
Number of adi sessions : 1
===============================================================================
*B:IPTV-SR7#
```

splice-status

Syntax **splice-status** [**service** *service-id*] [**interface** *ip-int-name*][**address** *mcast-address*] [**source** *ip-address*] [**start-time** *start-time* [**interval** *time-interval*]]

Context show>video>adi

Description This command displays ADI slice information.

service *service-id* **—** Displays splice status information pertaining to the specified service ID.

Values 1 — 2147483648
svc-name — a string up to 64 characters in length.

interface *ip-int-name* **—** Displays splice status information for the specified interface.

address *mcast-addres***s —** Displays splice status information for the specified multicast address.

source *ip-address* **—** Displays splice status information for the specified IP address.

start-time *start-time* **—** Enter the start time.

Values 1 — 4294967295 minutes earlier

interval *time-interval* **—** Enter the interval time.

Values 1 — 4294967295 minutes

Sample Output

```
*B:IPTV-SR7# show video adi splice-status
===============================================================================
Adi Splice Status
===============================================================================
Service Id       : 100                  Interface Name   : video-100
Group Address    : 234.4.5.241          Source Address   : 100.100.100.1
Start Time       : 07/17/2009 10:19:14  Ad Server Addr   : 10.200.14.2
Status           : Complete             Rate             : 8936 kbps
Duration Req     : 30 sec               Duration Played  : 29 sec
Session Id       : 1                    Prior Session Id : 4294967295
SpliceIn SeqNum  : 378                  SpliceOut SeqNum : 29727
Abort Reason     : None                 Black Frames     : 0
First black frame PTS  : 1530
Max Ad Stream PTS  : 0
Min Network Stream PTS  : 0
-------------------------------------------------------------------------------
Service Id       : 100                  Interface Name   : video-100
Group Address    : 234.4.5.241          Source Address   : 100.100.100.1
```

```
Start Time       : 07/17/2009 10:19:44  Ad Server Addr   : 10.200.14.2
Status           : Complete             Rate             : 0 kbps
Duration Req     : 30 sec               Duration Played  : 0 sec
Session Id       : 2                    Prior Session Id : 1
SpliceIn SeqNum  : 29727                SpliceOut SeqNum : 0
Abort Reason     : Session incomplete   Black Frames     : 0
First black frame PTS  : 1530
Max Ad Stream PTS  : 0
Min Network Stream PTS  : 0
-------------------------------------------------------------------------------
*B:IPTV-SR7#
```

rtp-session

Syntax **rtp-session** [**service** *service-id*] [**source** *ip-address*] [**detail** [**stats** {**rt-server** | **fcc-server**}]]
rtp-session [**service** *service-id*] **summary**

Context show>video

Description This command displays video session information.

Parameters **service** *service-id* **—** Displays video session information pertaining to the specified service ID.

Values 1 — 2147483648
svc-name — a string up to 64 characters in length.

source *ip-address* **—** Displays session informationfor the specified IP address.

detail — The output displays detailed video session information.

stats — Displays video session statistics.

Values **rt-server** — Displays video session statistics for the RT server.
fcc-server — Displays video session statistics for the FCC server.

summary — The output displays summarized video session information.

Sample Output

```
*A:Dut-C# show video  rtp-session
===============================================================================
Video RTP session
===============================================================================
Service Id        Source address      SSRC Id (hex)   RT reqs      FCC reqs
 Interface         Source Port         Time to expire  RT replies   FCC replies
-------------------------------------------------------------------------------
1                 1.0.103.103         1               0            226
 vi                1000                0d 00:03:24     0            225
1                 1.0.103.103         1               0            226
 vi                1001                0d 00:03:24     0            225
1                 1.0.103.103         1               0            226
 vi                1002                0d 00:03:24     0            225
1                 1.0.103.103         1               0            226
 vi                1003                0d 00:03:24     0            225
1                 1.0.103.103         1               0            226
 vi                1004                0d 00:03:24     0            225
1                 1.0.103.103         1               0            226
 vi                1005                0d 00:03:24     0            225
```

```
1                 1.0.103.103         1               0            226
 vi                1006                0d 00:03:24     0            225
1                 1.0.103.103         1               0            226
 vi                1007                0d 00:03:24     0            225
1                 1.0.103.103         1               0            226
 vi                1008                0d 00:03:24     0            225
1                 1.0.103.103         1               0            226
 vi                1009                0d 00:03:24     0            225
-------------------------------------------------------------------------------
Number of RTP sessions : 10
===============================================================================
*A:Dut-C#


*A:Dut-C# show video  rtp-session summary
===============================================================================
Video RTP session summary
===============================================================================
Num Sessions     : 2000
Rx RT Requests   : 0                    Tx RT Packets    : 0
Tx RT Replies    : 0                    Tx RT Octets     : 0
Rx FCC Requests  : 371068               Tx FCC Packets   : 243011904
Tx FCC Replies   : 368259               Tx FCC Octets    : 14152149376
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
*A:Dut-C#

*A:Dut-C# show video  rtp-session detail
===============================================================================
Video RTP session detail
===============================================================================
Service Id       : 1
Interface        : vi
Source Address   : 1.0.103.103          Source Port      : 1000

Destination Addr : 3.3.3.3              SSRC Id (hex)    : 1
CName            : ixiaPort
Up Time          : 0d 00:07:08          Time to Expire   : 0d 00:04:59

Num RT Requests  : 0                    Num RT Replies   : 0
RT Packets Sent  : 0                    RT Octets Sent   : 0
RT Failed Pkts   : 0                    Req RTP Packets  : 0

Num FCC Requests : 212                  Num FCC Replies  : 211
FCC Packets Sent : 138582               FCC Octets Sent  : 8145140
FCC Failed Pkts  : 1
-------------------------------------------------------------------------------
*A:Dut-C#
```

Clear Commands

id

Syntax **id** *service-id*

Context clear>video

Description This command clears video information pertaining to the specified service ID.

Parameters **service** *service-id* **—** Specifies the service ID to clear.

Values 1 — 2147483648
svc-name — a string up to 64 characters in length.

session

Syntax **session all**
session client *srcAddr*

Context clear>videoid

Description This command clears session information.

Parameters **all —** Clears all sessions.

client *srcAddr* **—** Clears information for the client source address.

statistics

Syntax **statistics**

Context clear>video

Description This command clears video related statistics.

id

Syntax **id** *service-id*

Context clear>video>statistics

Description This command clears video statistics for a particular service.

Parameters **service** *service-id* **—** Specifies the service ID to clear statistics.

Values 1 — 2147483648
svc-name — a string up to 64 characters in length.

adi-session

Syntax **adi-session**

Context clear>video>statistics>id

Description This command clears video statistics for an ADI session.

channel

Syntax **channel all** [**rt-client**] [**rt-server**] [**fcc-server**] [**ad-insert**]
channel *grp-address* [**source** *srcAddr*] [**rt-client**] [**rt-server**] [**fcc-server**] [**ad-insert**]

Context clear>video>statistics>id

Description This command clears video statistics for a particular channel.

Parameters **all —** Clears statistics for all channels.

rt-client — Clears all RET client related statistics.

rt-server — Clears all RET server related statistics.

fcc-server — Clears all FCC server related statistics.

ad-insert — Clears all ad insert related statistics.

grp-address — Clears statistics for the specified channel group address.

source *srcAddr* **—** Clears statistics for the specified source address.

interface

Syntax **interface** *ip-int-name* [**address** *ip-address*] **rt-client**] [**rt-server**] [**fcc-server**] [**ad-insert**]

Context clear>video>statistics>id

Description This command clears video statistics for a particular channel.

Parameters *ip-int-name* — Clears statistics for the specified interface.

address *ip-address* **—** Clears statistics for the specified IP address.

rt-client — Clears all RET client related statistics.

rt-server — Clears all RET server related statistics.

fcc-server — Clears all FCC server related statistics.

ad-insert — Clears all ad insert related statistics.

grp-address — Clears statistics for the specified channel group address.

source *srcAddr* **—** Clears statistics for the specified source address.

session

Syntax **session all** [**rt-server**] [**fcc-server**]
session client *srcAddr* [**rt-server**] [**fcc-server**]

Context clear>video>statistics>id

Description This command clears video statistics for a particular channel.

Parameters **all —** Clears statistics for all sessions.

rt-server — Clears all RET server related statistics.

fcc-server — Clears all FCC server related statistics.

client *srcAddr* **—** Clears statistics for the specified source address.

isa

Syntax **isa** *video-group-id* [*mda-id*]

Context clear>video>statistics

Description .This command clears statistics for a particular ISA video group.

Parameters *video-group-id* — statistics for a particular ISA video group a video group ID.

Values 1 — 4

mda-id — Specifies the card/slot identifying a provisioned ISA.

Values mda-id: slot/mda
slot: 1 — 10 (depending on the chassis model)
mda: 1 — 2

Debug Commands

video-interface

Syntax [**no**] **video-interface** *video-ip-int-name*

Context debug>service>id

Description This command enables debugging for video interfaces.

The **no** form of the command disables the video interface debugging.

Parameters *video-ip-int-name* — Specifies the video interface name.

adi

Syntax **adi** [*zone-channel-name*]
no adi

Context debug>service>id>video-interface

Description This command enables debugging for the ad insert server.

Parameters *zone-channel-name* — Specifies the channel name up to 32 characters in length.

adi-packet

Syntax **adi-packet** [*zone-channel-name*] [**type** {*type-name* [*type-name*]|**all**}]
no adi-packet

Context debug>service>id>video-interface

Description This command enables debugging for ADI packets exchanged between the splicer and the ad-server over scte30 session(s)

Parameters *zone-channel-name* — Specifies the channel name up to 32 characters in length.

type *type-name* **—** Specifies the ADI packet type.

Values alive, abort, init, splice, cue, all

Sample Output

```
A:IPTV-SR7# debug service id 100 video-interface video-100 adi-packet 240-1 type init
A:IPTV-SR7# show debug
debug
    service id 100
        video-interface video-100
            adi-packet 240-1 type init
```

```
        exit
    exit
exit
A:IPTV-SR7# debug service id 100 video-interface video-100 adi-packet 240-1 type
alive
A:IPTV-SR7# show debug
debug
    service id 100
        video-interface video-100
            adi-packet 240-1 type alive
        exit
    exit
exit
```

fcc-server

Syntax **fcc-server** [**client** *client-ip* [**source-port** *src-port*]]
no fcc-server

Context debug>service>id>video-interface

Description This command enables debugging the FCC server.

Parameters **client** *client-ip* **—** Specifies the client IP address.

source-port *src-port* **—** Specifies the source port's IP address.

packet-rx

Syntax **packet-rx** [**client** *client-ip* [**source-port** *src-port*]] [**fcc-join**] [**fcc-leave**] [**ret-nack**]
no packet-rx

Context debug>service>id>video-interface

Description This command enables debugging of received RTCP messages. The options for this command allow the user to filter only certain types of messages to appear in the debug traces.

Parameters **client** *client-ip* **—** Specifies the client IP address.

source-port *src-port* **—** Specifies the source port's IP address.

fcc-join — Enables debugging for FCC joins.

fcc-leave — Enables debugging for FCC leaves.

ret-nack — Enables debugging for retransmission nack packets.

packet-tx

Syntax **packet-tx** [**group** *grp-addr* [**source** *srcAddr*]] [**ret-nack**]
no packet-tx

Context debug>service>id>video-interface

Description This command enables debugging transmitted RTCP packets.

Parameters **client** *client-ip* **—** Specifies the client IP address.

source *src-srcAddr* **—** Specifies the source port.

Values 1 — 65535

rt-client

Syntax **rt-client** [**group** *group-addr*]
no rt-client

Context debug>service>id>video-interface

Description This command enables debugging the RET client.

Parameters **group** *group-addr* **—** Specifies the multicast group address.

rt-server

Syntax **rt-server** [**client** *client-ip* [**source-port** *src-port*]]
no rt-server

Context debug>service>id>video-interface

Description This command enables debugging for the RET server.

Parameters **client** *client-ip* **—** Specifies the client IP address.

source *src-srcAddr* **—** Specifies the source port.

Values 1 — 65535

sg

Syntax **sg** [**group** *grp-addr* [**source** *src-addr*]]
no sg

Context debug>service>id>video-interface

Description This command enables channel debugging.

Parameters **group** *grp-addr* **—** Specifies the multicast channel address.

source *src-addr* **—** Specifies the source address.

Network Address Translation

In This Chapter

This chapter provides information about Network Address Translation (NAT) and implementation notes.

Topics in this chapter include:

- Network Address Translation (NAT) Overview on page 334
  - → Principles of NAT on page 334
  - → Application Compatibility on page 335
  - → Large Scale NAT on page 336
  - → Layer-2 Aware NAT on page 337
  - → Port Range Blocks on page 337
    - – Reserved Ports and Priority Sessions on page 338
    - – Timeouts on page 338
    - – L2-Aware NAT on page 339
    - – Watermarks on page 339

Network Address Translation (NAT) Overview

The Alcatel-Lucent 7750 SR supports Network Address (and port) Translation (NAPT) to provide continuity of legacy IPv4 services during the migration to native IPv6. By equipping the Multiservice ISA (MS ISA) in an IOM3-XP, the 7750 SR can operate in two different modes, known as:

- Large Scale NAT, and;
- Layer 2-Aware NAT

These two modes both perform source address and port translation as commonly deployed for shared Internet access. The 7750 SR with NAT is used to provide consumer broadband or business Internet customers access to IPv4 internet resources with a shared pool of IPv4 addresses, such as may occur around the forecast IPv4 exhaustion. During this time it, is expected that native IPv6 services will still be growing and a significant amount of Internet content will remain IPv4.

Principles of NAT

Network Address Translation devices modify the IP headers of packets between a host and server, changing some or all of the source address, destination address, source port (TCP/UDP), destination port (TCP/UDP), or ICMP query ID (for ping). The 7750 SR in both NAT modes performs Source Network Address and Port Translation (S-NAPT). S-NAPT devices are commonly deployed in residential gateways and enterprise firewalls to allow multiple hosts to share one or more public IPv4 addresses to access the Internet. The common terms of inside and outside in the context of NAT refer to devices inside the NAT (that is behind or masqueraded by the NAT) and outside the NAT, on the public Internet.

TCP/UDP connections use ports for multiplexing, with 65536 ports available for every IP address. Whenever many hosts are trying to share a single public IP address there is a chance of port collision where two different hosts may use the same source port for a connection. The resultant collision is avoided in S-NAPT devices by translating the source port and tracking this in a stateful manner. All S-NAPT devices are stateful in nature and must monitor connection establishment and traffic to maintain translation mappings. The 7750 SR NAT implementation does not use the well-known port range (1..1023).

In most circumstances, S-NAPT requires the inside host to establish a connection to the public Internet host or server before a mapping and translation will occur. With the initial outbound IP packet, the S-NAPT knows the inside IP, inside port, remote IP, remote port and protocol. With this information the S-NAPT device can select an IP and port combination (referred to as outside IP and outside port) from its pool of addresses and create a unique mapping for this flow of data.

Any traffic returned from the server will use the outside IP and outside port in the destination IP/port fields – matching the unique NAT mapping. The mapping then provides the inside IP and inside port for translation.

The requirement to create a mapping with inside port and IP, outside port and IP and protocol will generally prevent new connections to be established from the outside to the inside as may occur when an inside host wishes to be a server.

Application Compatibility

Applications which operate as servers (such as HTTP, SMTP, etc) or peer-to-peer applications can have difficulty when operating behind an S-NAPT because traffic from the Internet can reach the NAT without a mapping in place.

Different methods can be employed to overcome this, including:

- Port Forwarding;
- STUN support; and,
- Application Layer Gateways (ALG)

The 7750 SR supports all three methods following the best-practice RFC for TCP (RFC 5382) and UDP (RFC 4787). Port Forwarding is supported on the 7750 SR to allow servers which operate on well-known ports <1024 (such as HTTP and SMTP) to request the appropriate outside port for permanent allocation.

STUN is facilitated by the support of Endpoint-Independent Filtering and Endpoint-Independent Mapping (RFC 4787) in the NAT device, allowing STUN-capable applications to detect the NAT and allow inbound P2P connections for that specific application. Many new SIP clients and IM chat applications are STUN capable.

Application Layer Gateways (ALG) allows the NAT to monitor the application running over TCP or UDP and make appropriate changes in the NAT translations to suit. The 7750 SR has an FTP ALG enabled following the recommendation of the IETF BEHAVE RFC for NAT (RFC 5382).

Even with these three mechanisms some applications will still experience difficulty operating behind a NAT. As an industry-wide issue, forums like UPnP the IETF, operator and vendor communities are seeking technical alternatives for application developers to traverse NAT (including STUN support). In many cases the alternative of an IPv6-capable application will give better long-term support without the cost or complexity associated with NAT.

Large Scale NAT

Large Scale NAT represents the most common deployment of S-NAPT in carrier networks today, it is already employed by mobile operators around the world for handset access to the Internet.

A Large Scale NAT is typically deployed in a central network location with two interfaces, the inside towards the customers, and the outside towards the Internet. A Large Scale NAT functions as an IP router and is located between two routed network segments (the ISP network and the Internet).

Traffic can be sent to the Large Scale NAT function on the 7750 SR using IP filters (ACL) applied to SAPs or by installing static routes with a next-hop of the NAT application. These two methods allow for increased flexibility in deploying the Large Scale NAT, especially those environments where IP MPLS VPN are being used in which case the NAT function can be deployed on a single PE and perform NAT for any number of other PE by simply exporting the default route.

The 7750 SR NAT implementation supports NAT in the base routing instance and VPRN, and through NAT traffic may originate in one VPRN (the inside) and leave through another VPRN or the base routing instance (the outside). This technique can be employed to provide customer's of IP MPLS VPN with Internet access by introducing a default static route in the customer VPRN, and NATing it into the Internet routing instance.

As Large Scale NAT is deployed between two routed segments, the IP addresses allocated to hosts on the inside must be unique to each host within the VPRN. While RFC1918 private addresses have typically been used for this in enterprise or mobile environments, challenges can occur in fixed residential environments where a subscriber has existing S-NAPT in their residential gateway. In these cases the RFC 1918 private address in the home network may conflict with the address space assigned to the residential gateway WAN interface. Some of these issues are documented in *draft-shirasaki-nat444-isp-shared-addr-02*. Should a conflict occur, many residential gateways will fail to forward IP traffic.

Layer-2 Aware NAT

In an effort to address issues of conflicting address space raised in *draft-shirasaki-nat444-isp-shared-addr-02* Alcatel-Lucent co-developed an enhancement to Large Scale NAT to give every broadband subscriber their own NAT mapping table, yet still share a common outside pool of IPs.

Layer-2 Aware (or subscriber aware) NAT is combined with Enhanced Subscriber Management on the 7750 BNG to overcome the issues of colliding address space between home networks and the inside routed network between the customer and Large Scale NAT.

Layer-2 Aware NAT permits every broadband subscriber to be allocated the exact same IPv4 address on their residential gateway WAN link and then proceeds to translate this into a public IP through the NAT application. In doing so, L2-Aware NAT avoids the issues of colliding address space raised in draft-shirasaki without any change to the customer gateway or CPE.

L2-Aware NAT is supported on any of the ESM access technologies, including PPPoE, IPoE (DHCP) and L2TP LNS. For IPoE both n:1 (VLAN per service) and 1:1 (VLAN per subscriber) models are supported. A subscriber device operating with L2-Aware NAT needs no modification or enhancement – existing address mechanisms (DHCP or PPP/IPCP) are identical to a public IP service, the 7750 BNG simply translates all IPv4 traffic into a pool of IPv4 addresses, allowing many L2-Aware NAT subscribers to share the same IPv4 address.

More information on L2-Aware NAT can be found in draft-miles-behave-l2nat-00.

Port Range Blocks

The S-NAPT service on the 7750 BNG incorporates a port range block feature to address scalability of a NAT mapping solution. With a single BNG capable of hundreds of thousands of NAT mappings every second, logging each mapping as it is created and destroyed logs for later retrieval (as may be required by law enforcement) could quickly overwhelm the fastest of databases and messaging protocols. Port range blocks address the issue of logging and customer location functions by allocating a block of contiguous outside ports to a single subscriber. Rather than log each NAT mapping, a single log entry is created when the first mapping is created for a subscriber and a final log entry when the last mapping is destroyed. This can reduce the number of log entries by 5000x or more. An added benefit is that as the range is allocated on the first mapping, external applications or customer location functions may be populated with this data to make real-time subscriber identification, rather than having to query the NAT as to the subscriber identity in real-time and possibly delay applications.

Port range blocks are configurable as part of outside pool configuration, allowing the operator to specify the number of ports allocated to each subscriber when a mapping is created. Once a range is allocated to the subscriber, these ports are used for all outbound dynamic mappings and are

assigned in a random manner to minimise the predictability of port allocations (*draft-ietf-tsvwg-port-randomization-05*).

Port range blocks also serve another useful function in a Large Scale NAT environment, and that is to manage the fair allocation of the shared IP resources among different subscribers.

When a subscriber exhausts all ports in their block, further mappings will be prohibited. As with any enforcement system, some exceptions are allowed and the NAT application can be configured for reserved ports to allow high-priority applications access to outside port resources while exhausted by lowpriority applications.

Reserved Ports and Priority Sessions

Reserved ports allows an operator to configure a small number of ports to be reserved for designated applications should a port range block be exhausted. Such a scenario may occur when a subscriber is unwittingly subjected to a virus or engaged in extreme cases of P2P file transfers. In these situations, rather than block all new mappings indiscriminately the 7750 NAT application allows operators to nominate a number of reserved ports and then assign a 7750 forwarding class as containing high priority traffic for the NAT application. Whenever traffic reaches the NAT application which matches a priority session forwarding class, reserved ports will be consumed to improve the chances of success. Priority sessions could be used by the operator for services such as DNS, web portal, email, VoIP, etc to permit these applications even when a subscriber exhausted their ports.

Timeouts

Creating a NAT mapping is only one half of the problem – removing a NAT mapping at the appropriate time maximises the shared port resource. Having ports mapped when an application is no longer active reduces solution scale and may impact the customer experience should they exhaust their port range block. The NAT application provides timeout configuration for TCP, UDP and ICMP.

TCP state is tracked for all TCP connections, supporting both 3-way handshake and simultaneous TCP SYN connections. Separate and configurable timeouts exist for TCP SYN, TCP transition (between SYN and Open), established and time-wait state. Time-wait assassination is supported and enabled by default to quickly remove TCP mappings in the TIME WAIT state.

UDP does not have the concept of connection state and is subject to a simple inactivity timer. Alcatel-Lucent-sponsored research into applications and NAT behaviour suggested some applications, like the Bittorrent Distributed Hash Protocol (DHT) can make a large number of outbound UDP connections that are unsuccessful. Rather than wait the default five (5) minutes to time these out, the 7750 NAT application supports an udp-initial timeout which defaults to 15 seconds. When the first outbound UDP packet is sent, the 15 second time starts – it is only after

subsequent packets (inbound or outbound) that the default UDP timer will become active, greatly reducing the number of UDP mappings.

L2-Aware NAT

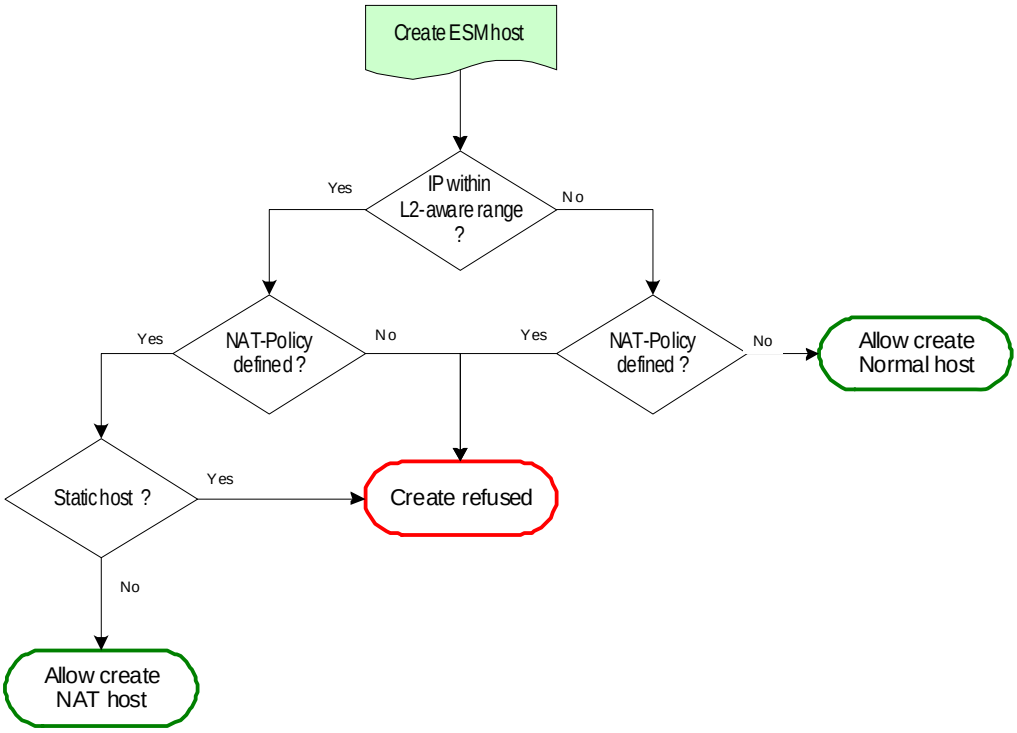

Figure 28: L2-aware Tree

Nat is supported on DHCP, PPPoE and L2TP, there is not support for static and arp hosts.

Watermarks

It is possible to define watermarks to monitor the actual usage of sessions and/or ports.

For each watermark, a high and a low value has to be set. Once the high value is reached, a notification will be send. As soon as the usage drops below the low watermark, another notification will be send.

Watermarks can be defined on nat-group, pool and policy level.

- **Nat-group** : Watermarks can be placed to monitor the total number of sessions on an MDA.
- **Pool** : Watermarks can be placed to monitor the total number of blocks in use in a pool.
- **Policy** : In the policy it is possible to define watermarks on session and port usage. In both cases, it is the usage per subscriber (for l2-aware nat) or per host (for large-scale nat) that will be monitored.

Configuring NAT

This section provides information to configure NAT using the command line interface.

Topics in this section include:

- ISA Redundancy on page 341
- NAT L2-Aware Configurations on page 344
- Large Scale NAT Configuration on page 346

ISA Redundancy

The 7750 SR supports ISA redundancy to provide reliable NAT even when an MDA fails. The active-mda-limit allows an operator to specify how many MDAs will be active in a given NAT group. Any number of MDAs configured above the active-mda-limit will be spare MDAs; they take over the NAT function if one of the current active MDAs fail.

A sample configuration is as follows:

```
Configure
    isa
        nat-group 1 create
            active-mda-limit 1
            mda 1/2
            mda 2/2
            no shutdown
        exit
    exit
exit
```

Show commands are available to display the actual state of a natgroup and its corresponding MDAs:

```
show isa nat-group 1
===============================================================================
ISA NAT Group 1
===============================================================================
Admin state       : inService           Operational state : inService
Active MDA limit  : 1                   Reserved sessions : 0
High Watermark (%): (Not Specified)     Low Watermark (%) : (Not Specified)
Last Mgmt Change  : 01/11/2010 15:05:36
===============================================================================
===============================================================================
ISA NAT Group 1 members
===============================================================================
Group Member     State          Mda  Addresses  Blocks     Se-% Hi Se-Prio
-------------------------------------------------------------------------------
1     1          active         1/2  0          0          0    N  0
-------------------------------------------------------------------------------
No. of members: 1
===============================================================================
```

A maximum of four (4) nat-groups can be configured. This gives the operator the ability to differentiate between different traffic types. Normal traffic could be routed to nat-group one (1), where a limited number of MDA without spare MDAs are available, while high priority traffic could make use of nat-group two (2), where several active MDAs and a spare MDA are configured. A maximum of six (6) MDAs per nat-group can be configured.

A nat-group cannot become active (no shutdown) if the number of configured MDAs is lower that the active-mda-limit.

A given MDA can be configured in several nat-groups but it can only be active in a single nat-group at any moment in time. Spare MDAs can be shared in several nat-groups, but a spare can only become active in one (1) nat-group at a time. Changing the active-mda-limit, adding or removing MDAs can only be done when the nat-group is shutdown.

Nat-groups that share spare MDAs must be configured with the same list of MDAs. It is possible to remove/add spare MDAs to a nat-group while the nat-group is admin enabled.

```
Configure
    isa
        nat-group 1 create
            active-mda-limit 1
            mda 1/2
            mda 2/2
            mda 3/1
            no shutdown
        exit
        nat-group 2 create
            active-mda-limit 1
            mda 1/2
            mda 2/2
            mda 3/1
            no shutdown
        exit
    exit
exit
```

Via show commands it is possible to display an overview of all the natgroups and MDAs.

```
show isa nat-group
===============================================================================
ISA NAT Group Summary
===============================================================================
Mda  Group 1            Group 2
-------------------------------------------------------------------------------
1/1  active             busy
2/2  busy               active
3/1  standby            standby
===============================================================================
```

If an MDA fails, the spare (if available) will take over. All active sessions will be lost, but new incoming sessions will make use of the spare MDA.

In case of an MDA failure in a nat-group without any spare MDA, all traffic towards that MDA will be black-holed.

For l2-aware NAT, the operator has the possibility to clear all the subscribers on the affected MDA (clear nat isa), terminating all the subscriber leases. New incoming subscribers will make use of the MDAs that are still available in the nat-group.

NAT L2-Aware Configurations

The following sections provide NAT L2-Aware configurations.

```
#--------------------------------------------------
echo "Card Configuration"
#--------------------------------------------------
    card 1
        card-type iom3-xp
        mda 1
            mda-type m60-10/100eth-tx
        exit
        mda 2
            mda-type isa-bb
        exit
    exit
    card 2
        card-type iom3-xp
        mda 1
            mda-type m60-10/100eth-tx
        exit
        mda 2
            mda-type isa-bb
        exit
    exit

#--------------------------------------------------
echo "ISA Configuration"
#--------------------------------------------------
    isa
        nat-group 1 create
            description "1 active + 1 spare"
            active-mda-limit 1
            mda 1/2
            mda 2/2
            no shutdown
        exit
    exit
#--------------------------------------------------
echo "Router (Network Side) Configuration"
#--------------------------------------------------
    router
        ...
#--------------------------------------------------
echo "NAT (Network Side) Configuration"
#--------------------------------------------------
        nat
            outside
                pool "pool1" nat-group 1 type l2-aware create
                    address-range 81.81.0.0 81.81.0.200 create
                    exit
                    no shutdown
                exit
            exit
        exit
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
```

```
    service
        customer 1 create
            description "Default customer"
        exit
        ...
        vprn 100 customer 1 create
            ...
            nat
                outside
                    pool "pool2" nat-group 1 type l2-aware create
                        address-range 82.0.0.0 82.0.0.200 create
                        exit
                        no shutdown
                    exit
                exit
            exit
        exit

        vprn 101 customer 1 create
            ...
            nat
                inside
                    l2-aware
                        # Hosts in this service with IP addresses in these ranges
                        # will be subject to l2-aware NAT.
                        address 10.0.0.1/29
                        address 10.1.0.1/29
                    exit
                exit
            exit
        exit
        ...
        nat
            nat-policy "l2-aware-nat-policy1" create
                pool "pool1" router Base
            exit
            nat-policy "l2-aware-nat-policy2" create
                pool "pool2" router 100
            exit
        exit
        ...
    exit
#--------------------------------------------------
echo "Subscriber-mgmt Configuration"
#--------------------------------------------------
    subscriber-mgmt
        # Subscribers using these sub-profiles will be subject to l2-aware NAT.
        # The configured nat-policies will determine which IP pool will be used.
        sub-profile "l2-aware-profile1" create
            nat-policy "l2-aware-nat-policy1"
        exit
        sub-profile "l2-aware-profile2" create
            nat-policy "l2-aware-nat-policy2"
        exit
        ...
    exit
```

Large Scale NAT Configuration

The following sections provide Large Scale NAT configuration examples.

```
configure
#--------------------------------------------------
echo "Card Configuration"
#--------------------------------------------------
    card 3
        card-type iom3-xp
        mda 1
            mda-type isa-bb
        exit
        mda 2
            mda-type isa-bb
        exit
    exit
#--------------------------------------------------
echo "ISA Configuration"
#--------------------------------------------------
    isa
        nat-group 1 create
            active-mda-limit 2
            mda 3/1
            mda 3/2
            no shutdown
        exit
    exit
#--------------------------------------------------
echo "Filter Configuration"
#--------------------------------------------------
    filter
        ip-filter 123 create
            entry 10 create
                match
                    src-ip 13.0.0.1/8
                exit
                action nat
            exit
        exit
    exit
#--------------------------------------------------
echo "NAT (Declarations) Configuration"
#--------------------------------------------------
    service
        nat
            nat-policy "ls-outPolicy" create
            exit
        exit
    exit
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        customer 1 create
            description "Default customer"
        exit
        vprn 500 customer 1 create
```

```
            interface "ip-113.0.0.1" create
            exit
            nat
                outside
                    pool "nat1-pool" nat-group 1 type large-scale create
                        port-reservation ports 200
                        address-range 81.81.0.0 81.81.6.0 create
                        exit
                        no shutdown
                    exit
                exit
            exit
        exit
        vprn 550 customer 1 create
            interface "ip-13.0.0.1" create
            exit
        exit
        nat
            nat-policy "ls-outPolicy" create
                pool "nat1-pool" router 500
                timeouts
                    udp hrs 5
                    udp-initial min 4
                exit
            exit
        exit
        vprn 500 customer 1 create
            router-id 10.21.1.2
            route-distinguisher 500:10
            vrf-target export target:500:1 import target:500:1
            interface "ip-113.0.0.1" create
                address 113.0.0.1/24
                static-arp 113.0.0.5 14:99:01:01:00:01
                sap 1/1/1:200 create
                exit
            exit
            no shutdown
        exit
        vprn 550 customer 1 create
            router-id 10.21.1.2
            route-distinguisher 550:10
            vrf-target export target:550:1 import target:550:1
            interface "ip-13.0.0.1" create
                address 13.0.0.1/8
                sap 1/2/1:900 create
                    ingress
                        filter ip 123
                    exit
                exit
            exit
            nat
                inside
                    nat-policy "ls-outPolicy"
                exit
            exit
            no shutdown
        exit
    exit
exit all
```

NAT Command Reference

Command Hierarchies

- NAT Service Configuration Commands on page 349
- NAT Subscriber Management Commands on page 352
- NAT Router Configuration Commands on page 352
- NAT Show Commands on page 353
- NAT Filter Commands on page 354

NAT ISA Configuration Commands

config
- **isa**
  - **nat-group** *nat-group-id* [**create**]
  - **no nat-group**
    - **active-mda-limit** *number*
    - **no active-mda-limit**
    - **description** *description-string*
    - **no description**
    - [**no**] **mda** *mda-id*
    - **session-limits**
      - **reserved num-sessions**
      - **no reserved**
      - **watermarks high** *percentage* **low** *percentage*
      - **no watermarks**
    - [**no**] **shutdown**

NAT Service Configuration Commands

configure
- **service**
  - **nat**
    - **nat-policy** *nat-policy-name* [**create**]
    - **no nat-policy** *nat-policy-name*
      - **description** *description-string*
      - **no description**
      - **filtering** *filtering-mode*
      - **no filtering**
      - **pool** *nat-pool-name* **service-name** *service-name*
      - **pool** *nat-pool-name* **router** *router-instance*
      - **no pool**
      - **port-limits**
        - **reserved *num-ports***

```
                                    — no reserved
                                    — watermarks high percentage-high low percentage-low
                                    — no watermarks
                                — [no] priority-sessions
                                    — [no] fc fc-name
                                — session-limits
                                    — max num-sesesions
                                    — no max
                                    — reserved num-sessions
                                    — no reserved
                                    — watermarks high percentage-high low percentage-low
                                    — no watermarks
                                — [no] timeouts
                                    — timeouts [min minutes] [sec seconds]
                                    — no timeouts
                                    — tcp-established [hrs hours] [min minutes] [sec seconds]
                                    — no tcp-established
                                    — tcp-syn [hrs hours] [min minutes] [sec seconds]
                                    — no tcp-syn
                                    — tcp-time-wait [min minutes] [sec seconds]
                                    — no tcp-time-wait
                                    — tcp-transitory [hrs hours] [min minutes] [sec seconds]
                                    — no tcp-transitory
                                    — udp [hrs hours] [min minutes] [sec seconds]
                                    — no udp
                                    — udp-dns [hrs hours] [min minutes] [sec seconds]
                                    — no udp-dns
                                    — udp-initial [min minutes] [sec seconds]
                                    — no udp-initial

config
    — service
        — vprn service-id customer cust-id create
            — nat
                — inside
                    — [no] destination-prefix ip-prefix/length
                    — l2-aware
                        — [no] address ip-address/mask
                    — nat-policy nat-policy-name
                    — no nat-policy
                — outside
                    — pool nat-pool-name [nat-group nat-group-id type pool-type
                      create]
                    — no pool nat-pool-name
                        — address-range start-ip-address end-ip-address
                          [create]
                        — no address-range start-ip-address end-ip-address
                            — description description-string
                            — no description
                            — [no] drain
                        — description description-string
                        — no description
                        — port-reservation blocks num-blocks
                        — port-reservation ports num-ports
                        — no port-reservation
```

- [**no**] **shutdown**
- **watermarks high** *percentage-high* **low** *percentage-low*
- **no watermarks**

NAT Subscriber Management Commands

configure
- **subscriber-mgmt**
  - **sub-profile**
    - **watermarks** *policy-name*
    - **no nat-policy**

NAT Router Configuration Commands

config
- **router**
  - **nat**
    - **inside**
      - [**no**] **destination-prefix** *ip-prefix/length*
      - **nat-policy** *nat-policy-name*
      - **no nat-policy**
    - **outside**
      - **pool** *nat-pool-name* [**nat-group** *nat-group-id* **type** *pool-type* **create**]
      - **no pool** *nat-pool-name*
        - **address-range** *start-ip-address end-ip-address* [**create**]
        - **no address-range** *start-ip-address end-ip-address*
          - **description** *description-string*
          - **no description**
          - [**no**] **drain**
        - **description** *description-string*
        - **no description**
        - **port-reservation blocks** *num-blocks*
        - **port-reservation ports** *num-ports*
        - **no port-reservation**
        - [**no**] **shutdown**
        - **watermarks high** *percentage-high* **low** *percentage-low*
        - **no watermarks**

NAT Show Commands

show
- **isa**
  - **nat-group**
  - **nat-group** *nat-group-id* [**associations**]
  - **nat-group** *nat-group-id* **member** *[1..255]* [**statistics**]
  - **nat-group** [*nat-group-id*] **members**
- **service**
  - **nat**
    - **l2-aware-hosts** [**outside-router** *router-instance*] [**outside-ip** *outside-ip-address*] [**inside-ip-prefix** *ip-prefix/mask*]
    - **l2-aware-subscribers** [**nat-policy** *nat-policy-name*] [**nat-group** *nat-group-id*] [**member** *[1..255]*] [**outside-router** *router-instance*] [**outside-ip** *outside-ip-address*]
    - **l2-aware-subscribers subscriber** *sub-ident*
    - **nat-policy** *nat-policy-name* **associations**
    - **nat-policy** *nat-policy-name* **statistics**
    - **nat-policy** *nat-policy-name*
    - **nat-policy**

show
- **router**
  - **nat**
    - **l2-aware-blocks** [**outside-ip-prefix** *ip-prefix/length*] [**outside-port** *[1..65535]*] [**pool** *pool-name*]
    - **lsn-blocks** [**inside-router** *router-instance*] [**inside-ip** *ip-address*] [**outside-ip-prefix** *ip-prefix/length*] [**outside-port** *[1..65535]*] [**pool** *pool-name*]
    - **lsn-hosts host** *ip-address*
    - **lsn-hosts** [**outside-router** *router-instance*] [**outside-ip** *ip-address*] [**inside-ip-prefix** *ip-prefix/mask*]
    - **pool** *pool-name*
    - **pool**
    - **summary**

Clear Commands

clear
- **nat**
  - **isa**
    - **nat-group** *nat-group-id* **member** *[1..255]* **l2-aware-subscribers**
    - **nat-group** *nat-group-id* **member** *[1..255]* **statistics**

Tools Commands

tools
- **dump**
  - **nat**

— **isa**

— **resources mda** *mda-id*

— **sessions** [**nat-group** *nat-group-id*] [**mda** *mda-id*] [**protocol** {**icmp**|**tcp**|**udp**}] [**inside-ip** *ip-address*] [**inside-router** *router-instance*] [**inside-port** *port-number*] [**outside-ip** *ip-address*] [**outside-port** *port-number*] [**foreign-ip** *ip-address*] [**foreign-port** *port-number*]

NAT Filter Commands

configure

— **filter**

— **ip-filter** *filter-id*

— **entry** *entry-id*

— **action nat**

— **no action**

Network Address Translation Configuration Commands

Generic Commands

nat

Syntax [**no**] **nat**

Context config>service>vprn
config>router

Description This command configures, creates or deletes a NAT instance.

inside

Syntax **inside**

Context config>service>vprn>nat
config>router>nat

Description This command enters the “inside” contex to configure the inside NAT instance.

outside

Syntax **outside**

Context config>service>vprn>nat
config>router>nat

Description This command enters the “outside” context to configure the outside NAT instance.

destination-prefix

Syntax [**no**] **destination-prefix** *ip-prefix/length*

Context config>service>vprn>nat>inside
config>router>nat>inside

Description This command configures a destination prefix. An (internal) static route will be created for this prefix. All traffic that hits this route will be subject to NAT. The system will not allow a destination-prefix to be configured if the configured nat-policy refers to an IP pool that resides in the same service (as this would result in a routing loop).

Parameters *ip-prefix* — Specifies the IP prefix; host bits must be zero (0).

Values a.b.c.d

length — Specifies the prefix length.

Values 0..32

l2-aware

Syntax **l2-aware**

Context config>services>vprn>nat>inside

Description This command enters the "l2-aware" context for configuration specific to layer-2 aware NAT.

address

Syntax [**no**] **address** *ip-address/mask*

Context config>services>vprn>nat>inside>l2-aware

Description This command configures a layer-2-aware NAT address. This address will act as a local address of the system. Hosts connected to the inside service will be able to ARP for this address. To verify connectivity, a host can also ping the address. This address is typically used as next hop of the default route of an l2-aware host. The given mask defines an l2-aware subnet. The (inside) IP address used by an l2-aware host must match one of the subnets defined here or it will be rejected.

Parameters *ip-address* — Specifies the IP address in a.b.c.d format.

mask — Specifies the mask.

Values 16..32

nat-policy

Syntax **nat-policy** *nat-policy-name*
no nat-policy

Context config>services>vprn>nat>inside
config>router>nat>inside

Description This command configures the NAT policy that will be used for large-scale NAT in this service.

Parameters *nat-policy-name* — Specifies the NAT policy name.

Values 32 chars max

pool

Syntax **pool** *nat-pool-name* [**nat-group** *nat-group-id* **type** *pool-type* **create**]
no pool *nat-pool-name*

Context config>service>vprn>nat>outside
config>router>nat>outside

Description This command configures a NAT pool.

Parameters *nat-pool-name* — Specifies the NAT pool name.

Values 32 chars max

nat-group-id — Specifies the NAT group ID.

Values 1..4

create — Keyword; must be specified to create a new NAT pool.

pool-type — Species the pool type, either large-scale or l2-aware.

address-range

Syntax **address-range** *start-ip-address end-ip-address* [**create**]
no address-range *start-ip-address end-ip-address*

Context config>service>vprn>nat>outside>pool
config>router>nat>outside>pool

Description This command configures a NAT address range.

Parameters *start-ip-address* — Specifies the beginning IP address in a.b.c.d form.

end-ip-address — Specifies the ending IP address in a.b.c.d. form.

create — Keyword; must be specified for new address ranges.

description

Syntax **description** *description-string*
no description

Context config>srevice>vprn>nat>outside>pool>address-range
config>service>vprn>nat>outside>pool
config>router>nat>outside>pool>address-range
config>router>nat>outside>pool

Description This command configures the description for the NAT address range.

Parameters *description-string* — Specifies the NAT address range description.

Values 80 chars max

drain

Syntax [**no**] **drain**

Context config>service>vprn>nat>outside>pool>address-range
config>router>nat>outside>pool>address-range

Description This command starts or stops draining this NAT address range. When an address-range is being drained, it will not be used to serve new hosts. Existing hosts, however, will still be able to use the address that was assigned to them even if it is being drained.An address-range can only be deleted if the parent pool is shut down or if the range itself is effectively drained (no hosts are using the addresses anymore).

port-reservation

Syntax **port-reservation blocks** *num-blocks*
port-reservation ports *num-ports*
no port-reservation

Context config>service>vprn>nat>outside>pool
config>router>nat>outside>pool

Description This command configures the size of the port-block that will be assigned to a host that is served by this pool. The number of ports configured here will be available to UDP, TCP and ICMP (as identifiers).

Parameters *num-blocks* — Specifies the number of port-blocks per IP address. Setting num-blocks to one (1) for large scale NAT will enable 1:1 NAT for IP addresses in this pool.

Values 1..64512

num-ports — Specifies the number of ports per block.

Values 1..32256

shutdown

Syntax [**no**] **shutdown**

Context config>service>vprn>nat>outside>pool

Description This command administratively enables or disables the NAT pool.

watermarks

Syntax **watermarks high** *percentage-high* **low** *percentage-low*
no watermarks

Context config>service>vprn>nat>outside>pool
config>router>nat>outside>pool

Description This command configures the watermarks for this NAT pool.

Parameters *percentage-high* — Specifies the high percentage.

Values 2..100

percentage-low — Specifies the low percentage.

Values 1..99

filtering

Syntax **filtering** *filtering-mode*
no filtering

Context config>service>nat>nat-policy

Description This command configures the filtering of the NAT policy.

Parameters *filtering-mode* — Specifies the way that inbound traffic is filtered.

Values address-and-port-dependent | endpoint-independent

pool

Syntax **pool** *nat-pool-name* **service-name** *service-name*
pool *nat-pool-name* **router** *router-instance*
no pool

Context config>service>nat>nat-policy

Description This command configures the NAT pool of this policy.

Parameters *nat-pool-name* — Specifies the name of the NAT pool.

Values 32 chars max

router-instance — Specifies the router instance the pool belongs to, either by router name or service ID.

Values *router-name*: “Base” | “management”

Default Base

Values 1 — 2147483648
svc-name — a string up to 64 characters in length.

service-name — Specifies the name of the service.

Values 64 chars max

port-limits

Syntax **port-limits**

Context config>service>nat>nat-policy

Description This command configures the port limits of this policy.

reserved

Syntax **reserved num-ports**
no reserved

Context config>service>nat>nat-policy>port-limits

Description This command configures the number of ports per block that will be reserved for prioritized sessions.

Parameters *num-ports* — Specifies the number of ports to reserve for prioritized sessions.

Values 1..65534

watermarks

Syntax **watermarks high** *percentage-high* **low** *percentage-low*
no watermarks

Context config>service>nat>nat-policy port-limits

Description This command configures the port usage watermarks for the NAT policy.

Parameters *percentage-high* — Specifies the high percentage.

Values 1..100

percentage-low — Specifies the low percentage.

Values 0..99

priority-sessions

Syntax [**no**] **priority-sessions**

Context config>service>nat>nat-policy

Description This command configures the prioritized sessions of this NAT policy.

fc

Syntax [**no**] **fc** *fc-name*

Context config>service>nat>nat-policy>priority-sessions

Description This command configures the forwarding classes that have their sessions prioritized.

Parameters *fc-name* — Specifies the forwarding class.

Values be | l2 | af | l1 | h2 | ef | h1 | nc

max

Syntax **max** *num-sessions*
no max

Context config>service>nat>nat-policy>session-limits

Description This command configures the session limit of this policy. The session limit is the maximum number of sessions allowed for a subscriber associated with this policy

Parameters *num-sessions* — Specifies the session limit.

Values 1..65535

timeouts

Syntax [**no**] **timeouts**

Context config>service>nat>nat-policy

Description This command configures the timeouts.

icmp-query

Syntax **icmp-query** [**min** *minutes*] [**sec** *seconds*]
no icmp

Context config>service>nat>nat-policy>timeouts

Description This command configures the timeout applied to an ICMP query session.

Parameters *minutes* — Specifies the timeout in minutes.

Values 1..4

seconds — Specifies the timeout in seconds.

Values 1..59

tcp-established

Syntax **tcp-established** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no tcp-established

Context config>service>nat>nat-policy>timeouts

Description This command configures the idle timeout applied to a TCP session in the established state.

Parameters *hours* — Specifies the timeout hours field.

Values 1..24

minutes — Specifies the timeout minutes field.

Values 1..59

seconds — Specifies the timeout seconds field.

Values 1..59

tcp-syn

Syntax **tcp-syn** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no tcp-syn

Context config>service>nat>nat-policy>timeouts

Description This command configures the timeout applied to a TCP session in the SYN state.

Parameters *hours* — Specifies the timeout hours field.

Values 1..24

minutes — Specifies the timeout minutes field.

Values 1..59

seconds — Specifies the timeout seconds field.

Values 1..59

tcp-time-wait

Syntax **tcp-time-wait** [**min** *minutes*] [**sec** *seconds*]
no tcp-time-wait

Context config>service>nat>nat-policy>timeouts

Description This command configures the timeout applied to a TCP session in a time-wait state.

Parameters *minutes* — Specifies the timeout minutes field.

Values 1..4

seconds — Specifies the timeout seconds field.

Values 1..59

tcp-transitory

Syntax **tcp-transitory** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no tcp-transitory

Context config>service>nat>nat-policy>timeouts

Description This command configures the idle timeout applied to a TCP session in a transitory state.

Parameters *hours* — Specifies the timeout hours field.

Values 1..24

minutes — Specifies the timeout minutes field.

Values 1..59

seconds — Specifies the timeout seconds field.

Values 1..59

udp

Syntax **udp** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no udp

Context config>service>nat>nat-policy>timeouts

Description This command configures the UDP mapping timeout.

Parameters *hours* — Specifies the timeout hours field.

Values 1..24

minutes — Specifies the timeout minutes field.

Values 1..59

seconds — Specifies the timeout seconds field.

Values 1..59

udp-dns

Syntax **udp-dns** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no udp-dns

Context config>service>nat>nat-policy>timeouts

Description This command configures the timeout applied to a UDP session with destination port 53.

Parameters *hours* — Specifies the timeout hours field.

Values 1..24

minutes — Specifies the timeout minutes field.

Values 1..59

seconds — Specifies the timeout seconds field.

Values 1..59

udp-initial

Syntax **udp-initial** [**min** *minutes*] [**sec** *seconds*]
no udp-initial

Context config>service>nat>nat-policy>timeouts

Description This command configures the UDP mapping timeout applied to new sessions.

Parameters *minutes* — Specifies the timeout minutes field.

Values 1..4

seconds — Specifies the timeout seconds field.

Values 1..59

nat-policy

Syntax **nat-policy** *nat-policy-name* [**create**]
no nat-policy *nat-policy-name*

Context config>service>nat

Description This commmand configures a NAT policy.

Parameters *nat-policy-name* — Specifies the NAT policy name.

Values 32 chars max

nat-policy

Syntax **nat-policy policy-name**
no nat-policy

Context config>subscriber-mgmt>sub-profile

Description This command configures the NAT policy to be used for subscribers associated with this subscriber profile.

Parameters *policy-name* — Specifies the policy name.

Values 32 chars max

nat-group

Syntax **nat-group** *nat-group-id* [**create**]
no nat-group *nat-group-id*

Context config>isa

Description This command configures an ISA NAT group.

active-mda-limit

Syntax **active-mda-limit** *number*
no active-mda-limit

Context config>isa>nat-group

Description This command configures the number of MDAs in this NAT ISA group that are intended for active use.

Parameters *number* — Specifies the active MDA limit.

mda

Syntax [**no**] **mda** *mda-id*

Context config>isa>nat-group

Description This command configures an ISA NAT group MDA.

Parameters *mda-id* — Specifies the MDA ID in the *slot/mda* format.

Values slot: 1 — 10

mda: 1 — 2

session-limits

Syntax **session-limits**

Context config>isa>nat-group

Description This command configures the ISA NAT group session limits.

reserved

Syntax **reserved** *num-sessions*
no reserved

Context config>isa>nat-group>session-limits

Description This command configures the number of sessions per block that will be reserved for prioritized sessions.

Parameters *num-sessions* — Specifies the number of sessions reserved for prioritized sessions.

Values 0 — 4194303

watermarks

Syntax **watermarks high** *percentage* **low** *percentage*
no watermarks

Context config>isa>nat-group>session-limits

Description This command configures the ISA NAT group watermarks.

high *percentage* **—** Specifies the high watermark of the number of sessions for each MDA in this NAT ISA group.

Values 2 — 100

low *percentage* — Specifies the low watermark of the number of sessions for each MDA in this NAT ISA group.

Values 1 — 99

NAT Show Commands

nat-group

Syntax **nat-group**
nat-group *nat-group-id* [**associations**]
nat-group *nat-group-id* **member** *[1..255]* [**statistics**]
nat-group [*nat-group-id*] **members**

Context show>isa

Description This command displays ISA NAT group information.

Parameters *nat-group-id* — Specifies the NAT group ID.

Values 1..4

statistics — Keyword; displays NAT group statistics.

Sample Output

```
show isa nat-group
===============================================================================
ISA NAT Group Summary
===============================================================================
Mda Group 1 Group 2 Group 3
-------------------------------------------------------------------------------
3/1 active - -
3/2 - active busy
4/1 - busy active
4/2 - standby standby
===============================================================================


show isa nat-group 1
===============================================================================
ISA NAT Group 1
===============================================================================
Admin state : inService Operational state : inService
Active MDA limit : 1 Reserved sessions : 0
High Watermark (%): (Not Specified) Low Watermark (%) : (Not Specified)
Last Mgmt Change : 02/04/2010 16:24:33
===============================================================================
===============================================================================
ISA NAT Group 1 members
===============================================================================
Group Member State Mda Addresses Blocks Se-% Hi Se-Prio
-------------------------------------------------------------------------------
1 1 active 3/1 2 3 0 N 0
-------------------------------------------------------------------------------
No. of members: 1
===============================================================================
```

```
show isa nat-group members
===============================================================================
ISA NAT group members
===============================================================================
Group Member State Mda Addresses Blocks Se-% Hi Se-Prio
-------------------------------------------------------------------------------
1 1 active 3/1 2 3 0 N 0
2 1 active 3/2 0 0 0 N 0
3 1 active 4/1 0 0 0 N 0
-------------------------------------------------------------------------------
No. of members: 3
===============================================================================

show isa nat-group 1 members
===============================================================================
ISA NAT Group 1 members
===============================================================================
Group Member State Mda Addresses Blocks Se-% Hi Se-Prio
-------------------------------------------------------------------------------
1 1 active 3/1 2 3 0 N 0
-------------------------------------------------------------------------------
No. of members: 1
===============================================================================


show isa nat-group 1 member 1 statistics
===============================================================================
ISA NAT Group 1 Member 1
===============================================================================
no resource : 0
pkt rx on wrong port : 0
unsupported protocol : 0
no host : 0
no ip or port : 0
no matching flow : 0
max flow exceeded : 0
TCP no flow for RST : 0
TCP no flow for FIN : 0
TCP no flow : 0
addr. dep. filtering : 0
unsupported ICMP : 0
unsupported local ICMP : 0
ICMP checksum error : 0
ICMP embedded checksum error : 0
ICMP unsupported L4 : 0
pkt length error : 0
ICMP length error : 0
FTP ALG host refused : 0
FTP ALG no resource : 0
Pkt not ip : 7
Pkt rcv error : 0
Pkt ip exception : 8
Pkt fragmented : 0
Pkt not TCP or UDP : 0
Pkt error : 0
Pkt send error : 0
no policy : 0
locked by mgmt core : 0
```

```
log failed : 0
new flow : 0
TCP closed : 0
TCP expired : 0
UDP expired : 0
ICMP expired : 0
ICMP local : 0
found flow : 0
===============================================================================


show isa nat-group 1 associations
===============================================================================
ISA NAT Group 1 pool associations
===============================================================================
Pool Router
-------------------------------------------------------------------------------
MyPool Base
MyPool2 Base
-------------------------------------------------------------------------------
No. of pools: 2
===============================================================================
```

l2-aware-hosts

Syntax **l2-aware-hosts** [**outside-router** *router-instance*] [**outside-ip** *outside-ip-address*] [**inside-ip-prefix** *ip-prefix/mask*]

Context show>service>nat

Description This command displays layer-2 aware NAT hosts.

Parameters *nat-policy-name* — Specifies the NAT policy name.

Values 32 chars max

nat-group-id — Specifies the NAT group ID.

Values 1..4

router-instance — Specifies the router instance.

Values

router-name:	Base , management
service-id:	1 — 2147483647
svc-name:	A string up to 64 characters in length.

outside-ip-address — Specifies the outside IP address.

Values a.b.c.d

sub-ident — Specifies the identifier.

Values 32 chars max

Sample Output

```
show service nat l2-aware-hosts
===============================================================================
Layer-2-Aware NAT hosts
===============================================================================
Inside IP Out-Router Outside IP Subscriber
-------------------------------------------------------------------------------
13.0.0.100 Base 81.81.0.0 Sub001
13.0.0.102 Base 81.81.0.0 Sub001
13.0.0.101 Base 81.81.0.203 Sub002
13.0.0.103 Base 81.81.0.0 Sub003
-------------------------------------------------------------------------------
No. of hosts: 4
===============================================================================
```

l2-aware-subscribers

Syntax **l2-aware-subscribers** [**nat-policy** *nat-policy-name*] [**nat-group** *nat-group-id*] [**member** ***[****1..255****]***] [**outside-router** *router-instance*] [**outside-ip** *outside-ip-address*]
l2-aware-subscribers *subscriber sub-ident*

Context show>service>nat

Description This command displays layer-2 aware NAT subscribers.

Parameters *nat-policy-name* — Specifies the NAT policy name.

Values 32 chars max

nat-group-id — Specifies the NAT group ID.

Values 1..4

router-instance — Specifies the router instance.

Values

router-name:	Base , management
service-id:	1 — 2147483647
svc-name:	A string up to 64 characters in length.

outside-ip-address — Specifies the outside IP address.

Values a.b.c.d

sub-ident — Specifies the identifier.

Values 32 chars max

Sample Output

```
show service nat l2-aware-subscribers
===============================================================================
Layer-2-Aware NAT subscribers
===============================================================================
Subscriber Policy Group/Member
Outside IP Router Ports
```

```
-------------------------------------------------------------------------------
Sub001 outPolicy 1/1
81.81.0.0 Base 32-33
Sub002 outPolicy2 1/1
81.81.0.203 Base 32-41
Sub003 outPolicy 1/1
81.81.0.0 Base 34-35
-------------------------------------------------------------------------------
No. of subscribers: 3
===============================================================================


show service nat l2-aware-subscribers subscriber "Sub881"
===============================================================================
Layer-2-Aware NAT subscriber Sub001
===============================================================================
Policy : outPolicy
ISA NAT group : 1
ISA NAT group member : 1
Outside router : Base
Outside IP : 81.81.0.0
ICMP Port usage (%) : < 1
ICMP Port usage high : false
UDP Port usage (%) : < 1
UDP Port usage high : false
TCP Port usage (%) : < 1
TCP Port usage high : false
Session usage (%) : < 1
Session usage high : false
Number of sessions : 0
Number of reserved sessions : 0
Ports : 32-33
===============================================================================
```

nat-policy

Syntax **nat-policy** *nat-policy-name* **associations**
nat-policy *nat-policy-name*
nat-policy *nat-policy-name* **statistics**
nat-policy

Context show>service>nat

Description This command displays NAT policy information.

Parameters *nat-policy-name* — Specifies the NAT Policy name.

Values 32 chars max

associations — Keyword; displays the router instances and/or subscriber profiles associated with the NAT policy.

statistics — Keyword; displays statistics of the specified NAT policy.

Sample Output

```
show service nat nat-policy
===============================================================================
NAT policies
===============================================================================
Policy Description
-------------------------------------------------------------------------------
outPolicy
outPolicy2
outPolicy3
-------------------------------------------------------------------------------
No. of NAT policies: 3
===============================================================================


show service nat nat-policy "outPolicy2"
===============================================================================
NAT Policy outPolicy2
===============================================================================
Pool : MyPool2
Router : Base
Filtering : endpointIndependent
Reserved ports : 0
Port usage High Watermark (%) : (Not Specified)
Port usage Low Watermark (%) : (Not Specified)
Session limit : 65535
Reserved sessions : 0
Session usage High Watermark (%) : (Not Specified)
Session usage Low Watermark (%) : (Not Specified)
Prioritized forwarding classes : (Not Specified)
Timeout TCP established (s) : 7440
Timeout TCP transitory (s) : 240
Timeout TCP SYN (s) : 15
Timeout TCP TIME-WAIT (s) : 0
Timeout UDP mapping (s) : 300
Timeout UDP initial (s) : 15
Timeout UDP DNS (s) : 15
Timeout ICMP Query (s) : 60
Last Mgmt Change : 02/04/2010 15:33:05
===============================================================================


show service nat nat-policy "outPolicy2" associations
===============================================================================
NAT Policy outPolicy2 Subscriber Profile Associations
===============================================================================
sub_prof_B_3
-------------------------------------------------------------------------------
No. of subscriber profiles: 1
===============================================================================

show service nat nat-policy "outPolicy2" statistics
===============================================================================
NAT Policy outPolicy2 Statistics
===============================================================================
mda 3/1
-------------------------------------------------------------------------------
hostsActive : 1
```

```
hostsPeak : 1
sessionsTcpCreated : 0
sessionsTcpDestroyed : 0
sessionsUdpCreated : 0
sessionsUdpDestroyed : 0
sessionsIcmpQueryCreated : 0
sessionsIcmpQueryDestroyed : 0
===============================================================================
```

l2-aware-blocks

Syntax **l2-aware-blocks** [**outside-ip-prefix** *ip-prefix/length*] [**outside-port** *[1..65535]*] [**pool** *pool-name*]

Context show>router>nat

Description This command displays Layer 2 aware NAT blocks.

Parameters *ip-prefix* — Specifies the IP prefix.

Values a.b.c.d (host bits must be 0)

length — Specifies the IP prefix length.

Values 1..32

pool-name — Specifies the pool name.

Values 32 chars max

Sample Output

```
show router nat l2-aware-blocks
===============================================================================
Layer-2-Aware NAT blocks for Base
===============================================================================
81.81.0.0 [32..33]
Pool : MyPool
Policy : outPolicy
Started : 2010/02/04 16:24:55
Subscriber ID : Sub001
81.81.0.0 [34..35]
Pool : MyPool
Policy : outPolicy
Started : 2010/02/04 16:25:24
Subscriber ID : Sub003
81.81.0.203 [32..41]
Pool : MyPool2
Policy : outPolicy2
Started : 2010/02/04 16:25:21
Subscriber ID : Sub002
-------------------------------------------------------------------------------
Number of blocks: 3
===============================================================================
```

lsn-blocks

Syntax **lsn-blocks** [**inside-router** *router-instance*] [**inside-ip** *ip-address*] [**outside-ip-prefix** *ip-prefix/length*] [**outside-port** *[1..65535]*] [**pool** *pool-name*]

Context show>router>nat

Description This command displays large scale NAT blocks.

Parameters *router-instance* — Specifies the router instance name and service ID.

Values
router-name: Base , management
service-id: 1 — 2147483647
svc-name: A string up to 64 characters in length.

ip-address — Specifies the IP address in a.b.c.d format.

ip-prefix — Specifies the IP prefix.

Values a.b.c.d (host bits must be 0)

length — Specifies the IP prefix length.

Values 1..32

pool-name — Specifies the pool name.

Values 32 chars max

Sample Output

```
show router 588 nat lsn-blocks
===============================================================================
Large-Scale NAT blocks for vprn500
===============================================================================
81.81.0.0 [1232..1431]
Pool : nat1-pool
Policy : ls-outPolicy
Started : 2010/02/04 19:43:01
Inside router : vprn550
Inside IP address : 13.0.0.7
81.81.0.0 [1432..1631]
Pool : nat1-pool
Policy : ls-outPolicy
Started : 2010/02/04 19:43:00
Inside router : vprn550
Inside IP address : 13.0.0.5
..
-------------------------------------------------------------------------------
Number of blocks: 6
===============================================================================
```

lsn-hosts

Syntax **lsn-hosts host** *ip-address*
lsn-hosts [**outside-router** *router-instance*] [**outside-ip** *ip-address*] [**inside-ip-prefix** *ip-prefix/mask*]

Context show>router

Description This command displays large scale NAT hosts.

Parameters *router-instance* — Specifies the router instance name and service ID.

Values
router-name: Base , management
service-id: 1 — 2147483647
svc-name: A string up to 64 characters in length.

ip-address — Specifies the IP address in a.b.c.d format.

ip-prefix — Specifies the IP prefix.

Values a.b.c.d (host bits must be 0)

length — Specifies the IP prefix length.

Values 1..32

pool-name — Specifies the pool name.

Values 32 chars max

Sample Output

```
show router 588 nat lsn-hosts
===============================================================================
Large-Scale NAT hosts for router 550
===============================================================================
Inside IP Out-Router Outside IP
-------------------------------------------------------------------------------
13.0.0.5 500 81.81.0.0
13.0.0.6 500 81.81.3.1
13.0.0.7 500 81.81.0.0
13.0.0.8 500 81.81.0.0
13.0.0.9 500 81.81.3.1
13.0.0.10 500 81.81.0.0
-------------------------------------------------------------------------------
No. of hosts: 6
===============================================================================

show router 558 nat lsn-hosts host 13.8.8.5
===============================================================================
Large-Scale NAT host details
===============================================================================
Policy : ls-outPolicy
ISA NAT group : 1
ISA NAT group member : 1
Outside router : vprn500
Outside IP : 81.81.0.0
ICMP Port usage (%) : < 1
```

```
ICMP Port usage high : false
UDP Port usage (%) : 2
UDP Port usage high : false
TCP Port usage (%) : < 1
TCP Port usage high : false
Session usage (%) : < 1
Session usage high : false
Number of sessions : 5
Number of reserved sessions : 0
Ports : 1432-1631
===============================================================================
```

pool

Syntax **pool** *pool-name*
pool

Context show>router>nat

Description This command displays NAT pool information.

Parameters *pool-name* — Specifies the pool name.

Values 32 chars max

Sample Output

```
show router nat pool
===============================================================================
NAT pools
===============================================================================
Pool NAT-group Type Admin-state
-------------------------------------------------------------------------------
MyPool 1 l2Aware inService
MyPool2 1 l2Aware inService
-------------------------------------------------------------------------------
No. of pools: 2
===============================================================================

show router nat pool "MyPool"
===============================================================================
NAT Pool MyPool
===============================================================================
ISA NAT Group : 1
Pool type : l2Aware
Admin state : inService
Port reservation : 2 ports
Block usage High Watermark (%) : (Not Specified)
Block usage Low Watermark (%) : (Not Specified)
Block usage (%) : < 1
Last Mgmt Change : 02/04/2010 16:24:33
===============================================================================
===============================================================================
NAT address ranges of pool MyPool
===============================================================================
```

```
Range Drain Num-blk
-------------------------------------------------------------------------------
81.81.0.0 - 81.81.0.200 2
-------------------------------------------------------------------------------
No. of ranges: 1
===============================================================================
```

summary

Syntax **summary**

Context show>router>nat

Description This command displays the NAT information summary.

Sample Output

```
show router nat summary
===============================================================================
NAT Layer-2-Aware addresses
===============================================================================
Layer-2-Aware address subnet
-------------------------------------------------------------------------------
13.0.0.1/16
-------------------------------------------------------------------------------
No. of subnets: 1
===============================================================================
===============================================================================
NAT pools
===============================================================================
Pool NAT-group Type Admin-state
-------------------------------------------------------------------------------
MyPool 1 l2Aware inService
MyPool2 1 l2Aware inService
-------------------------------------------------------------------------------
No. of pools: 2
===============================================================================
```

NAT Tools Commands

nat-group

Syntax **nat-group** *nat-group-id* **member** [*1..255*] **l2-aware-subscribers**
nat-group *nat-group-id* **member** [*1..255*] **statistics**

Context clear>nat>isa

Description This command clears ISA nat-group commands related statistics or removes all the subscribers that are associated with a specific nat-group member

Parameters *nat-group-id* — Specifies the NAT group ID to clear.

Values 1..4

statistics — Keyword; specifies to clear the NAT group ID's statistics.

l2-aware-subscribers — Keyword; specifies to clear the NAT group ID's l2-aware subscribers.

NAT Tools Commands

nat

Syntax **nat**

Context tools>dump

Description This command enables the dump tools for NAT.

isa

Syntax **isa**

Context tools>dump>nat

Description This command enables the dump tools for NAT ISA.

resources

Syntax **resources mda** *mda-id*

Context tools>dump>nat>isa

Description This command enables dump ISA resources for an MDA.

sessions

Syntax **sessions** [**nat-group** *nat-group-id*] [**mda** *mda-id*] [**protocol** {**icmp|tcp|udp**}] [**inside-ip** *ip-address*] [**inside-router** *router-instance*] [**inside-port** *port-number*] [**outside-ip** *ip-address*] [**outside-port** *port-number*] [**foreign-ip** *ip-address*] [**foreign-port** *port-number*]

Context tools>dump>nat

Description This command dumps ISA sessions.

Sample Output

```
===============================================================================
*A:Dut-C# tools dump nat sessions

===============================================================================
Matched 3 sessions on Slot #3 MDA #2
===============================================================================
```

```
Owner               : LSN-Host@11.11.12.12
Router              : 10
Flow Type           : TCP               Timeout (sec)       : 11
Inside IP Addr      : 11.11.12.12       Inside Port         : 99
Outside IP Addr     : 101.0.0.1         Outside Port        : 1537
Foreign IP Addr     : 10.10.10.10       Foreign Port        : 5678
-------------------------------------------------------------------------------
Owner               : LSN-Host@11.11.12.12
Router              : 10
Flow Type           : ICMP              Timeout (sec)       : 59
Inside IP Addr      : 11.11.12.12       Inside Identifier   : 12345
Outside IP Addr     : 101.0.0.1         Outside Identifier  : 1535
Foreign IP Addr     : 10.10.10.10
-------------------------------------------------------------------------------
Owner               : LSN-Host@11.11.12.12
Router              : 10
Flow Type           : UDP               Timeout (sec)       : 109
Inside IP Addr      : 11.11.12.12       Inside Port         : 99
Outside IP Addr     : 101.0.0.1         Outside Port        : 1533
Foreign IP Addr     : 10.10.10.10       Foreign Port        : 5678
-------------------------------------------------------------------------------
===============================================================================
*A:Dut-C# tools
```

NAT Filter Commands

action

Syntax **action nat**
no action

Context config>filter>ip-filter>entry

Description This command specifies packets matching the entry criteria will be subject to large-scale NAT.

Appendix A: Common CLI Command Descriptions

In This Chapter

This section provides information about common Command Line Interface (CLI) syntax and command usage.

Topics in this chapter include:

- SAP syntax on page 384

Common Service Commands

sap

Syntax [**no**] **sap** *sap-id*

Description This command specifies the physical port identifier portion of the SAP definition.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

The *sap-id* can be configured in one of the following formats:

Type	Syntax	Example
port-id	*slot*/*mda*/*port*[.*channel*]	1/1/5
null	[*port-id* | *bundle-id*| *bpgrp-id* | *lag-id* | *aps-id*]	*port-id*: 1/1/3 *bundle-id*: bundle-ppp-1/1.1 *bpgrp-id*: bpgrp-ima-1 *lag-id*: lag-3 *aps-id*: aps-1
dot1q	[*port-id* | *bundle-id*| *bpgrp-id* | *lag-id* | *aps-id*]:qtag1	*port-id*:qtag1: 1/1/3:100 *bundle-id*: bundle-ppp-1/1.1 *bpgrp-id*: bpgrp-ima-1 *lag-id*:qtag1:lag-3:102 *aps-id*:qtag1: aps-1:27
qinq	[*port-id* | *bpgrp-id* | *lag-id*]:*qtag1.qtag2*	*port-id*:qtag1.qtag2: 1/1/3:100.10 *bpgrp-id*: bpgrp-ima-1 *lag-id*:qtag1.qtag2: lag-10:
atm	[*port-id* | *aps-id* | *bundle-id* | *bpgrp-id*][:vpi/vci |vpi |vpi1.vpi2]	port-id: 1/1/1 aps-id: aps-1 *bundle-id*: bundle-ima-1/1.1 bundle-ppp-1/1.1 *bpgrp-id*: bpgrp-ima-1 vpi/vci: 16/26 vpi: 16 vpi1.vpi2: 16.200
frame-relay	[*port-id* | *aps-id*]:*dlci*	*port-id*: 1/1/1:100 *bundle-id*: bundle-fr-3/1.1:100 *aps-id*: aps-1 *dlci*: 16
cisco-hdlc	*slot/mda/port.channel*	*port-id*: 1/1/3.1

7750 SR:

Values: *sap-id*

null	[*port-id* | *bundle-id* | *bpgrp-id* | *lag-id* | *aps-id*]	
dot1q	[*port-id* | *bundle-id* | *bpgrp-id* | *lag-id* | *aps-id*]:*qtag1*	
qinq	[*port-id* | *bundle-id* | *bpgrp-id* | *lag-id*]:*qtag1.qtag2*	
atm	[*port-id* | *aps-id*][:*vpi/vci*|*vpi*| *vpi1.vpi2*]	
frame	[*port-id* | *aps-id*]:*dlci*	
cisco-hdlc	*slot/mda/port.channel*	
cem	*slot/mda/port.channel*	
ima-grp	[*bundle-id*[:vpi/vci|vpi|*vpi1.vpi2*]	
port-id	*slot/mda/port*[.*channel*]	
bundle-id	bundle-*type-slot/mda.bundle-num*	
	bundle	keyword
	type	ima, fr, ppp
	bundle-num	1 — 336
bpgrp-id	bpgrp-*type-bpgrp-num*	
	bpgrp	keyword
	type	ima, ppp
	bpgrp-num	1 — 2000
aps-id	aps-*group-id*[.*channel*]	
	aps	keyword
	group-id	1 — 64
ccag-id	ccag-*id.path-id*[*cc-type*]:*cc-id*	
	ccag	keyword
	id	1 — 8
	path-id	a, b
	cc-type	.sap-net, .net-sap
	cc-id	0 — 4094
eth-tunnel	eth-tunnel-*id*[:*eth-tun-sap-id*]	
	id	1— 1024
	eth-tun-sap-id	0 — 4094
lag-id	lag-id	
	lag	keyword
	id	1 — 200
qtag1	0 — 4094	
qtag2	*, 0 — 4094	
vpi	NNI: 0 — 4095	
	UNI: 0 — 255	
vci	1, 2, 5 — 65535	
dlci	16 — 1022	
ipsec-id	ipsec-*id*.[private | public]:*tag*	
	ipsec	keyword
	id	1 — 4
	tag	0 — 4094

7450 ESS:

Values: *sap-id*	null	[*port-id* | *bundle-id* | *bpgrp-id* | *lag-id* | *aps-id*]	
	dot1q	[*port-id* | *bundle-id* | *bpgrp-id* | *lag-id* | *aps-id*]:*qtag1*	
	qinq	[*port-id* | *bundle-id* | *bpgrp-id* | *lag-id*]:*qtag1.qtag2*	
	atm	[*port-id* | *aps-id*][:*vpi/vci*|*vpi*| *vpi1.vpi2*]	
	frame	[*port-id* | *aps-id*]:*dlci*	
	cisco-hdlc	*slot/mda/port.channel*	
	ima-grp	[*bundle-id*[:vpi/vci|vpi|*vpi1.vpi2*]	
	port-id	*slot/mda/port*[*.channel*]	
	bundle-id	bundle-*type-slot/mda.bundle-num*	
		bundle	keyword
		type	ima, fr, ppp
		bundle-num	1 — 336
	bpgrp-id	bpgrp-*type-bpgrp-num*	
		bpgrp	keyword
		type	ima, ppp
		bpgrp-num	1 — 2000
	aps-id	aps-*group-id*[*.channel*]	
		aps	keyword
		group-id	1 — 64
	ccag-id	ccag-*id.path-id*[*cc-type*]:*cc-id*	
		ccag	keyword
		id	1 — 8
		path-id	a, b
		cc-type	.sap-net, .net-sap
		cc-id	0 — 4094
	eth-tunnel	eth-tunnel-*id*[:*eth-tun-sap-id*]	
		id	1— 1024
		eth-tun-sap-id	0 — 4094
	lag-id	lag-id	
		lag	keyword
		id	1 — 200
	qtag1	0 — 4094	
	qtag2	*, 0 — 4094	
	vpi	NNI: 0 — 4095	
		UNI: 0 — 255	
	vci	1, 2, 5 — 65535	
	dlci	16 — 1022	

Glossary

The following terms and acronyms describe the operation and maintenance of RET/ FCC and ad insertion configurations are presented for reference purposes.

ADI Ad Insertion

ADI-LZ Ad Insertion Local and Zoned

Avail An “available” part of the program stream where an authorized operator is allowed to replace the stream.

A time space offered to cable operators by cable programming services during a program for use by the CATV operator; the time can be sold to local advertisers or used for channel self promotion.

BTV Broadcast Television

DPI Digital Program Insertion

DRM Digital Rights Management

DSLAM Digital Subscriber Line Access Multiplexer

ES Elementary Stream

FCC Fast Channel Change

GOP Group of Pictures

HD High Definition

HGW Home Gateway

IPTV Internet Protocol Television

ISA	Integrated Services Adapter
MSTV	Microsoft Television
NTP	Network Time Protocol
PID	Packet Identifier
PMT	Program Map Table
PON	Passive Optical Network
RG	Routed Gateway
RET	Retransmission
RTCP	RTP Control Protocol
RTP	Real-Time Transport Protocol
STB	Set Top Box
TS	Transport Stream
VoD	Video-on-Demand

Index

A

AA accounting files 66

AA-ISA groups 35
- bypass modes 37
- redundancy 38

accounting
- special study 64
- statistics and accounting 64

ad zones 242

adi
- local/zoned 239
- splicing 239

application assurance
- fixed residential broadband 24
- in-line deployment 21
- overview 20
- subscriber edge 22

application filters 49

application groups 48

application profiles 50

application QoS policies 59

application service options 52

applications 48

AQP 31

ASO 31

B

bursting 227

business VPN services 26

C

Card, MDA, Port
- configuring
  - command reference
    - card commands 276

command reference 87
- AA commands 90
  - admin 88
  - clear 95
  - debug commands 95
  - show commands 94
- clear commands 327
- debug commands 330
- IPSec commands 195
  - configuration 195
  - hardware 195
  - show 198
- IPSec configuration commands 195
- show commands 319

configuration tasks
- configuring
  - accounting and billing statistics 84
  - application filters 76
  - application groups 77
  - application profile 79
  - application QoS policies 81
  - application service options 83
  - policers 80
- policies
  - aborting 75
  - beginning and committing 75
- profile policies 75
- watermark 74

configuring 245, 254
- bundle parameters 252
- channel parameters 271
- FCC server 263
- NTP 271
- RET client 255, 269
- RET server 259
- service entities 249, 272
- video group 248, 270
- video ISA module 247
- video policy 251

D

denting 227

F
FCC 225
FCC server 231

G
glossary 387
group of pictures (GOP) 225

H
hardware
IOM support 18
MDA support 17
hardware features 17

I
IPSec 180

M
multicast information policies 222

N
NAT 334
334
overview 334

O
overview
RET and FCC 224
video ISA 16

P
policers 56
profile policies
abort 75
begin 75
commit 75
protocol signatures 45

R
retransmission 224
client 229
server 230

S
server concurrency 233
Services command reference
Virtual Private Routed Network 349
software features 30
application ID 41
application QoS policies 59
CLI batch commands 62
datapath overview 33
identification components 43
services 34

T
ToD adjustments 61

V
video
groups 220
interface 221
saps 221