



Alcatel-Lucent 7705

SERVICE AGGREGATION ROUTER OS | RELEASE 1.1
SERVICES GUIDE

Alcatel-Lucent assumes no responsibility for the accuracy of the information presented, which is subject to change without notice.

Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners.

Copyright 2008 Alcatel-Lucent.
All rights reserved.

Disclaimers

Alcatel-Lucent products are intended for commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The customer hereby agrees that the use, sale, license or other distribution of the products for any such application without the prior written consent of Alcatel-Lucent, shall be at the customer's sole risk. The customer hereby agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the products in such applications.

This document may contain information regarding the use and installation of non-Alcatel-Lucent products. Please note that this information is provided as a courtesy to assist you. While Alcatel-Lucent tries to ensure that this information accurately reflects information provided by the supplier, please refer to the materials provided with any non-Alcatel-Lucent product and contact the supplier for confirmation. Alcatel-Lucent assumes no responsibility or liability for incorrect or incomplete information provided about non-Alcatel-Lucent products.

However, this does not constitute a representation or warranty. The warranties provided for Alcatel-Lucent products, if any, are set forth in contractual documentation entered into by Alcatel-Lucent and its customers.

This document was originally written in English. If there is any conflict or inconsistency between the English version and any other version of a document, the English version shall prevail.

Table of Contents

Preface	19
Getting Started	21
Alcatel-Lucent 7705 SAR Services Configuration Process	21
Notes on 7705 SAR-F and 7705 SAR-8	22
Services Overview	25
Introduction to Services on the 7705 SAR	26
Service Types	27
Service Policies	28
Alcatel-Lucent Service Model	29
Service Entities	30
Customers	31
Service Types	31
Service Access Points (SAPs)	31
SAP Encapsulation Types and Identifiers	32
SAP Configuration Considerations	34
Service Destination Points (SDPs)	35
SDP Binding	36
Spoke SDPs	37
SDP Encapsulation Types	38
SDP Ping	42
SDP Keepalives	42
Mobile Solutions	44
HSDPA Offload	44
Failure Detection	46
Service Creation Overview	47
Subscriber Services Components	49
Port and SAP CLI Identifiers	50
Reference Sources	50
Configuring Global Service Entities with CLI	51
Service Model Entities	52
Service CLI Command Structure	53
List of Commands	55
Basic Configuration	57
Common Configuration Tasks	59
Configuring Customer Accounts	59
Configuring SDPs	60
SDP Configuration Considerations	60
Configuring an SDP	61
Service Management Tasks	63
Modifying Customer Accounts	63
Deleting Customers	64
Modifying SDPs	64
Deleting SDPs	65
Deleting LSP Associations	65

Table of Contents

Global Service Command Reference	67
Global Service Configuration Commands	70
Show Commands	84
VLL Services	93
ATM VLL (Apipe) Services	94
ATM VLL for End-to-End ATM Service	94
ATM SAP-to-SAP Service	95
ATM Traffic Management Support	96
Network Ingress Classification	96
ATM Access Egress Queuing and Shaping	96
Control Word	96
Circuit Emulation VLL (Cpipe) Services	97
Cpipe Service Overview	97
TDM SAP-to-SAP Service	98
Cpipe Service Modes	98
TDM PW Encapsulation	101
Circuit Emulation Parameters and Options	103
Error Situations	113
Ethernet VLL (Epipe) Services	114
Epipe Service Overview	114
Ethernet Access Egress Queuing and Scheduling	116
Control Word	116
MTU	116
Raw and Tagged Modes	117
VLL Service Considerations	121
Service Support	121
SDPs	121
SDP Statistics for VLL Services	122
SAP Encapsulations and Pseudowire Types	122
ATM PWE3 N-to-1 Cell Mode Encapsulation	123
QoS Policies	125
MTU Settings	126
Targeted LDP and MTU	129
Pseudowire Control Word	130
Configuring a VLL Service with CLI	131
List of Commands	132
Common Configuration Tasks	140
Configuring VLL Components	141
Creating an Apipe Service	141
Configuring Apipe SAP Parameters	143
Configuring Apipe SDP Bindings	145
Creating a Cpipe Service	146
Configuring Cpipe SAP parameters	146
Configuring Cpipe SDP bindings	149
Creating an Epipe Service	150
Configuring Epipe SAP Parameters	150
Configuring Epipe SDP Bindings	152
Configuring Ingress and Egress SAP Parameters	154

Using the Control Word	155
Service Management Tasks	157
Modifying Service Parameters	157
Disabling a Service	159
Re-enabling a Service	161
Deleting a Service	161
VLL Services Command Reference	163
VLL Service Configuration Commands	168
Show Commands	193
Clear Commands	234
Internet Enhanced Service	237
IES for In-band Management	238
Setting Up Connections Between the 5620 SAM and the 7705 SAR	239
Encapsulation	240
Layer 2 and Layer 3 Traffic Management	241
Troubleshooting and Fault Detection Services	242
Configuring an IES Management Service with CLI	243
List of Commands	244
Common Configuration Tasks	246
Configuring IES Components	247
Creating an IES Service	247
Configuring Interface Parameters	248
Configuring IES SAP Parameters	249
Service Management Tasks	251
Modifying IES Service Parameters	251
Disabling an IES Service	251
Re-enabling an IES Service	252
Deleting an IES Service	252
IES Management Command Reference	253
IES Management Configuration Commands	255
Show Commands	268
OAM and SAA	277
OAM Overview	278
LSP Diagnostics	278
LSP Ping	278
LSP Traceroute	278
SDP Diagnostics	279
SDP Ping	279
SDP MTU Path Discovery	280
Service Diagnostics	280
Service Ping	280
VLL Diagnostics	281
VCCV Ping	281
EFM OAM	283
Unidirectional OAM Operation	283
Remote Loopback	283
802.3ah OAMPDU Tunneling for Epipe Services	284

Table of Contents

OAM Propagation to Attachment Circuits	284
ATM Ports	284
T1/E1 TDM Ports	285
Ethernet Ports	285
LDP Status Signaling	285
LDP Status via Label Withdrawal	285
LDP Status via TLV	286
Service Assurance Agent Overview	287
SAA Application	287
Traceroute Implementation	287
OAM and SAA List of Commands	288
Configuring SAA Test Parameters	290
OAM and SAA Command Reference	293
OAM and SAA Commands	297
Show Commands	337
Clear Commands	339
Debug Commands	340
Tools	341
Tools Command Reference	341
Tools Configuration Commands	344
Tools Performance Commands	352
Standards and Protocol Support	357

List of Tables

Getting Started	21
Table 1: 7705 SAR Configuration Process	21
Table 2: 7705 SAR-8 and 7705 SAR-F Comparison	22
Services Overview	25
Table 3: Pseudowire Service Types	27
Table 4: Service Types and SAP Encapsulations	34
Table 5: GRE Header Descriptions	40
Table 6: GRE Pseudowire Payload Packet Descriptions	41
Table 7: CLI Commands to Configure Service Parameters	55
Table 8: SDP Echo Reply Response Conditions	80
Table 9: Show Customer Command Output Fields	84
Table 10: Show Service SDP Output Fields	86
Table 11: Show Service sdp-using Output Fields	89
Table 12: Show Service service-using Output Fields	91
VLL Services	93
Table 13: Unstructured Payload Defaults	104
Table 14: Default and Minimum Payload Size for CESoPSN without CAS	106
Table 15: Payload Size for E1 CESoPSN with CAS	108
Table 16: Control Word Bit Descriptions	112
Table 17: Ingress SAP Tagging Rules	118
Table 18: Egress SAP Tagging Rules	119
Table 19: Ethernet VLL Encapsulation Translation	120
Table 20: MTU Points and Descriptions	127
Table 21: MTU Values – Service Creation (Worst Case)	128
Table 22: Matching MTU or Payload Values for Signaled VLL Services	129
Table 23: CLI Commands to Configure VLL Service Parameters	133
Table 24: Maximum Transmission Unit Values	174
Table 25: SAP ID Configurations	176
Table 26: Port and Encapsulation Values	177
Table 27: Show Service-ID All Command Output Fields	193
Table 28: Show Service-ID Base Output Fields	213
Table 29: Show Service Egress Label Output Fields	215
Table 30: Show Service Ingress Label Output Fields	217
Table 31: Service-ID Labels Output Fields	218
Table 32: SAP Fields	219
Table 33: Show Service SAP Output Fields	227

List of Tables

Table 34:	SDP Output Fields	229
Internet Enhanced Service		237
Table 35:	CLI Commands to Configure IES Management Service Parameters	244
Table 36:	SAP ID Configurations	263
Table 37:	Show Service ID All Command Output Fields	268
OAM and SAA		277
Table 38:	Supported VCCV CC and CV Types	282
Table 39:	OAM Command Summary	288
Table 40:	SVC Ping Report Fields	307
Table 41:	Local SDP Message Results	313
Table 42:	Remote SDP Message Results	314
Table 43:	SDP Ping Response Messages	326
Table 44:	Single Response Connectivity	329
Table 45:	SAA Field Descriptions	337

List of Figures

Services Overview	25
Figure 1: Service Entities and the Service Model	30
Figure 2: Service Access Point (SAP)	32
Figure 3: Multiple SAPs on a Single Port/Channel	33
Figure 4: SDP Tunnel Pointing from ALU-A to ALU-B	37
Figure 5: GRE Header	39
Figure 6: GRE Pseudowire Payload Packet over Ethernet	41
Figure 7: HSDPA Offload Example	45
Figure 8: Service Creation and Implementation Flow Chart	48
Figure 9: Subscriber Service Components	49
Figure 10: Core and Customer Command Overview	53
Figure 11: Global Service CLI Command Overview	54
VLL Services	93
Figure 12: ATM VLL for End-to-End ATM Service	95
Figure 13: E1 Framing for CAS Support in a Multiframe	100
Figure 14: SAToP MPLS Encapsulation	101
Figure 15: CESoPSN MPLS Encapsulation	101
Figure 16: CESoPSN Packet Payload Format for Trunk-Specific n x 64 kb/s (with and without CAS transport)	102
Figure 17: Control Word Bit Structure	111
Figure 18: Ethernet VLL Frame with MPLS Encapsulation	115
Figure 19: Epipe Service	115
Figure 20: Ethernet Frame Representations	119
Figure 21: N-to-1 Cell Mode Encapsulation	123
Figure 22: MTU Points on the 7705 SAR	126
Figure 23: SDPs — Unidirectional Tunnels	152
OAM and SAA	277
Figure 24: VCCV Ping Application	281

List of Acronyms

Acronym	Expansion
2G	second generation wireless telephone technology
3G	third generation mobile telephone technology
5620 SAM	5620 Service Aware Manager
7705 SAR	7705 Service Aggregation Router
ABR	available bit rate
AC	alternating current attachment circuit
ACL	access control list
ACR	adaptive clock recovery
AIS	alarm indication signal
ANSI	American National Standards Institute
Apipe	ATM VLL
ARP	address resolution protocol
AS	autonomous system
ASAP	any service, any port
ATM	asynchronous transfer mode
ATM PVC	ATM permanent virtual circuit
B-bit	beginning bit (first packet of a fragment)
Batt A	battery A
Bellcore	Bell Communications Research
BFD	bidirectional forwarding detection
BITS	building integrated timing supply
BOF	boot options file

Acronym	Expansion
BRAS	Broadband Remote Access Server
BSC	Base Station Controller
BSTA	Broadband Service Termination Architecture
BTS	base transceiver station
CAS	channel associated signaling
CBN	common bonding networks
CBS	committed buffer space
CC	control channel
CE	customer edge circuit emulation
CEM	circuit emulation
CES	circuit emulation services
CESoPSN	circuit emulation services over packet switched network
CIDR	classless inter-domain routing
CIR	committed information rate
CLI	command line interface
CLP	cell loss priority
CoS	class of service
CPE	customer premises equipment
Cpipe	circuit emulation (or TDM) VLL
CPU	central processing unit
CRC	cyclic redundancy check
CRON	a time-based scheduling service (from chronos = time)
CSM	Control and Switching Module
CSPF	constrained shortest path first

Acronym	Expansion
CV	connection verification customer VLAN (tag)
CW	control word
DC	direct current
DC-C	DC return - common
DC-I	DC return - isolated
DCO	digitally controlled oscillator
DDoS	distributed DoS
DHCP	dynamic host configuration protocol
DNS	domain name server
DoS	denial of service
dot1q	IEEE 802.1q encapsulation for Ethernet interfaces
DPLL	digital phase locked loop
DSCP	differentiated services code point
DSL	digital subscriber line
DSLAM	digital subscriber line access multiplexer
DTE	data termination equipment
DU	downstream unsolicited
e911	enhanced 911 service
E-bit	ending bit (last packet of a fragment)
ECMP	equal cost multi-path
EFM	Ethernet in the first mile
ELER	egress label edge router
Epipe	Ethernet VLL
ESD	electrostatic discharge
ETE	end-to-end

Acronym	Expansion
EVDO	evolution - data optimized
EXP bits	experimental bits
FC	forwarding class
FCS	frame check sequence
FDB	forwarding database
FDL	facilities data link
FEC	forwarding equivalence class
FIB	forwarding information base
FTN	FEC-to-NHLFE
FTP	file transfer protocol
GigE	Gigabit Ethernet
GRE	generic routing encapsulation
GSM	Global System for Mobile Communications (2G)
HEC	header error control
HSDPA	high-speed downlink packet access
HSPA	high-speed packet access
IBN	isolated bonding networks
ICMP	Internet control message protocol
ICP	IMA control protocol cells
IEEE	Institute of Electrical and Electronics Engineers
IES	Internet Enhanced Service
IETF	Internet Engineering Task Force
ILER	ingress label edge router
ILM	incoming label map
IMA	inverse multiplexing over ATM
IOM	input/output module

Acronym	Expansion
IP	Internet Protocol
LCP	link control protocol
LDP	label distribution protocol
LER	label edge router
LLID	loopback location ID
LSP	label switched path
LSR	label switch router
LTN	LSP ID to NHLFE
MAC	media access control
MBB	make-before-break
MBS	maximum buffer space maximum burst size media buffer space
MD5	message digest version 5 algorithm
MDA	media dependent adapter
MEF	Metro Ethernet Forum
MFC	multi-field classification
MIB	management information base
MIR	minimum information rate
MLPPP	multilink point-to-point protocol
MP	multilink protocol
MPLS	multiprotocol label switching
MRRU	maximum received reconstructed unit
MRU	maximum receive unit
MTSO	mobile trunk switching office
MTU	maximum transmission unit multi-tenant unit

Acronym	Expansion
NHLFE	next hop label forwarding entry
NNI	network-to-network interface
Node B	similar to BTS but used in 3G networks — term is used in UMTS (3G systems) while BTS is used in GSM (2G systems)
OAM	operations, administration, and maintenance
OAMPDU	OAM protocol data units
OS	operating system
OSS	operations support system
PDU	protocol data units
PDV	packet delay variation
PDVT	packet delay variation tolerance
PE	provider edge router
PHB	per-hop behavior
PHY	physical layer
PID	protocol ID
PIR	peak information rate
POP	point of presence
PPP	point-to-point protocol
PSN	packet switched network
PVC	permanent virtual circuit
PVCC	permanent virtual channel connection
PW	pseudowire
PWE3	pseudowire emulation edge-to-edge
QoS	quality of service
RAN	Radio Access Network
RDI	remote defect indication

Acronym	Expansion
RED	random early discard
RNC	Radio Network Controller
RSVP-TE	resource reservation protocol - traffic engineering
R&TTE	Radio and Telecommunications Terminal Equipment
RT	receive/transmit
RTM	route table manager
RTN	battery return
RTP	real-time protocol
SAA	service assurance agent
SAP	service access point
SAR-8	7705 Service Aggregation Router - 8-slot chassis
SAR-F	7705 Service Aggregation Router - fixed form-factor chassis
SAToP	structure-agnostic TDM over packet
SDP	service destination point
SIR	sustained information rate
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNTP	simple network time protocol
SPE	source provider edge router
SPF	shortest path first
SR	service router (includes 7710 SR, 7750 SR)
SSH	secure shell
SSU	system synchronization unit
SVC	switched virtual circuit
TCP	transmission control protocol
TDM	time division multiplexing

Acronym	Expansion
TLDP	targeted LDP
TLV	type length value
ToS	type of service
TPE	target provider edge router
TPID	tag protocol identifier
TTL	time to live
TTM	tunnel table manager
UBR	unspecified bit rate
UDP	user datagram protocol
UMTS	Universal Mobile Telecommunications System (3G)
UNI	user-to-network interface
VC	virtual circuit
VCC	virtual channel connection
VCCV	virtual circuit connectivity verification
VCi	virtual circuit identifier
VLAN	virtual LAN
VLL	virtual leased line
VoIP	voice over IP
VP	virtual path
VPC	virtual path connection
VPI	virtual path identifier
VPN	virtual private network
VPRN	virtual private routed network
WCDMA	wideband code division multiple access (transmission protocol used in UMTS networks)
WRED	weighted random early discard

Preface

About This Guide

This guide describes subscriber services support provided by the 7705 Service Aggregation Router (7705 SAR) and presents examples to configure and implement various protocols and services.

This document is organized into functional chapters and provides concepts and descriptions of the implementation flow, as well as Command Line Interface (CLI) syntax and command usage.

Audience

This guide is intended for network administrators who are responsible for configuring the 7705 SAR routers. It is assumed that the network administrators have an understanding of networking principles and configurations. Protocols, standards, and services described in this guide include the following:

- CLI concepts
- subscriber services
- operations, administration and maintenance (OAM) operations

List of Technical Publications

The 7705 SAR OS documentation set is composed of the following guides:

- 7705 SAR OS Basic System Configuration Guide
This guide describes basic system configurations and operations.
- 7705 SAR OS System Management Guide
This guide describes system security and access configurations as well as event logging and accounting logs.
- 7705 SAR OS Interface Configuration Guide
This guide describes card and port provisioning.

- **7705 SAR OS Router Configuration Guide**
This guide describes logical IP routing interfaces, IP-based filtering, and routing policies.
- **7705 SAR OS MPLS Guide**
This guide describes how to configure Multiprotocol Label Switching (MPLS) and Label Distribution Protocol (LDP).
- **7705 SAR OS Services Guide**
This guide describes how to configure service parameters such as service access points (SAPs), service destination points (SDPs), customer information, user services, and Operations, Administration and Management (OAM) tools.
- **7705 SAR OS Quality of Service Guide**
This guide describes how to configure Quality of Service (QoS) policy management.

Technical Support

If you purchased a service agreement for your 7705 SAR 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 at:

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

Getting Started

In This Chapter

This chapter provides the process flow information required to configure services.

Alcatel-Lucent 7705 SAR Services Configuration Process

[Table 1](#) lists the tasks necessary to configure subscriber services. This guide is presented in an overall logical configuration flow. Each section describes a software area and provides CLI syntax and command usage to configure parameters for a functional area.

Table 1: 7705 SAR Configuration Process

Area	Task	Reference
Subscriber services	Configure subscriber services	
	Global entities	Configuring Global Service Entities with CLI on page 51
VLL services	Apipe service	ATM VLL (Apipe) Services on page 94
	Cpipe service	Circuit Emulation VLL (Cpipe) Services on page 97
	Epipe service	Ethernet VLL (Epipe) Services on page 114
Internet Enhanced Service	Configure in-band management of 7705 SAR over ATM links	Internet Enhanced Service on page 237
Diagnostics/Service verification	OAM	OAM and SAA on page 277
Reference	List of IEEE, IETF, and other proprietary entities	Standards and Protocol Support on page 357

Notes on 7705 SAR-F and 7705 SAR-8

The 7705 SAR-F and the 7705 SAR-8 run the same operating system software. The main difference between the products is their hardware configuration. The 7705 SAR-8 has an 8-slot chassis that supports two CSMs, six adapter cards, and a Fan module. The 7705 SAR-F chassis has a fixed hardware configuration, replacing the 7705 SAR-8 physical components (the CSM, Fan module, and adapter cards) with an all-in-one unit that provides comparable functional blocks, as detailed in [Table 2](#).

The fixed configuration of the 7705 SAR-F means that provisioning the router at the “card slot” and “type” levels is preset and is not user-configurable. Operators begin configurations at the port level.



Note: Unless stated otherwise, references to the terms "Adapter card" and "CSM" throughout the 7705 SAR OS documentation set include the equivalent functional blocks on the 7705 SAR-F.

Table 2: 7705 SAR-8 and 7705 SAR-F Comparison

7705 SAR-8	7705 SAR-F	Notes
CSM	Control and switching functions	The control and switching functions include the console and management interfaces, the alarm and fan functions, the synchronization interfaces, system LEDs, and so on.
Fan module	Integrated with the control and switching functions	
16-port T1/E1 ASAP Adapter card	16 individual T1/E1 ports on the faceplate	The T1/E1 ports on the 7705 SAR-F are equivalent to a 16-port T1/E1 ASAP Adapter card on the 7705 SAR-8 with additional support for multiple synchronization sources. The 7705 SAR-8 CLI indicates that the MDA type for the T1/E1 ASAP Adapter card is <code>a16-chds1</code> . The 7705 SAR-F supports MDA type <code>a16-chds1v2</code> .
8-port Ethernet Adapter card	8 individual Ethernet ports on the faceplate	The Ethernet ports on the 7705 SAR-F are equivalent to one 8-port Ethernet Adapter card (version 2) on the 7705 SAR-8 with additional support for multiple synchronization sources. The 7705 SAR-8 CLI indicates that the MDA type for the Ethernet Adapter card is <code>a8-eth</code> or <code>a8-ethv2</code> . The 7705 SAR-F supports MDA type <code>a8-ethv3</code> . Versions 2 and 3 support Synchronous Ethernet timing.

Table 2: 7705 SAR-8 and 7705 SAR-F Comparison (Continued)

7705 SAR-8	7705 SAR-F	Notes
Requires user configuration at card (IOM) and MDA (adapter card) levels	Configuration at card (IOM) and MDA (adapter card) levels is preset and users cannot change these types	

Services Overview

In This Chapter

This chapter provides an overview of the 7705 SAR subscriber services, service model, and service entities. Additional details on the individual subscriber services are found in subsequent chapters.

Topics in this chapter include:

- [Introduction to Services on the 7705 SAR on page 26](#)
 - [Service Types on page 27](#)
 - [Service Policies on page 28](#)
- [Alcatel-Lucent Service Model on page 29](#)
- [Service Entities on page 30](#)
 - [Customers on page 31](#)
 - [Service Types on page 31](#)
 - [Service Access Points \(SAPs\) on page 31](#)
 - [Service Destination Points \(SDPs\) on page 35](#)
- [Mobile Solutions on page 44](#)
 - [HSDPA Offload on page 44](#)
- [Service Creation Overview on page 47](#)
- [Port and SAP CLI Identifiers on page 50](#)
- [Configuring Global Service Entities with CLI on page 51](#)
- [Global Service Command Reference on page 67](#)

Introduction to Services on the 7705 SAR

A service is a type of telecommunications connection from one place to another. These telecommunications connections have the particular attributes and characteristics that are needed to provide a specific communications link through which an information flow or exchange can occur. The 7705 Service Access Router (7705 SAR) offers Layer 2 point-to-point VPN services.

The 7705 SAR service model uses (logical) service entities to construct a service. These logical entities provide a uniform, service-centric configuration, management, and billing model for service provisioning (see [Alcatel-Lucent Service Model on page 29](#) for more information). Many services can be created on the same 7705 SAR at the same time, and each service is uniquely identified by a service ID.

The 7705 SAR offers Virtual Leased Line (VLL) services (also referred to as pseudowire (PW) services or pipes), which emulate a Layer 1/2 entity, such as a wire or a leased line. These emulated services provide connectivity between a service access point (SAP) on one 7705 SAR and on another SAP on the same router, or on a remote 7705 SAR, 7710 SR, or 7750 SR. VLL services offer SAP logical entities — such as a VLAN or a virtual connection — Layer 2 visibility or processing (IMA termination). A SAP is the point where customer traffic enters and exits the service.

When the connection is between two SAPs on the same router, this is known as local service. When the connection is between SAPs on a local and a remote router, this is known as distributed service. In Release 1.1, SAP-to-SAP connections are supported for ATM and TDM VLLs.

Distributed services use service destination points (SDPs) to direct traffic from a local router to a remote router through a service tunnel. An SDP is created on the local router and identifies the endpoint of a logical unidirectional service tunnel. Traffic enters the tunnel at the SDP on the local router and exits the tunnel at the remote router. Hence, a service tunnel provides a path from a 7705 SAR to another service router, such as another 7705 SAR, a 7710 SR, or a 7750 SR. Because an SDP is unidirectional, two service tunnels are needed for bidirectional communication between two service routers (one SDP on each router).

SDPs are configured on each participating 7705 SAR or service router, specifying the address of the source router (the 7705 SAR participating in the service communication) and the address of the destination router, such as another 7705 SAR or service router. After SDPs are created, they are bound to a specific service. The binding process is needed to associate the far-end devices to the service; otherwise, far-end devices are not able to participate in the service.

Service Types

Services are commonly called customer or subscriber services. The 7705 SAR offers the following types of service, which are described in more detail in the referenced chapters:

- Virtual Leased Line (VLL) services
 - ATM VLL (Apipe) — a pseudowire emulation edge-to-edge (PWE3) ATM service over MPLS or GRE tunnels on 7705 SAR nodes. See [ATM VLL \(Apipe\) Services on page 94](#).
 - Circuit emulation VLL (Cpipe) — a PWE3 circuit emulation service over MPLS or GRE tunnels on 7705 SAR nodes. See [Circuit Emulation VLL \(Cpipe\) Services on page 97](#).
 - Ethernet VLL (Epipe) — a PWE3 Ethernet service over MPLS or GRE tunnels for Ethernet frames on 7705 SAR nodes. See [Ethernet VLL \(Epipe\) Services on page 114](#).
- Internet Enhanced Service (IES)
 - In Release 1.1, IES is used only for in-band management of the 7705 SAR and is not used as a routing service. See [Internet Enhanced Service on page 237](#).

[Table 3](#) lists the pseudowire (PW) service types supported in Release 1.1. The values are as defined in RFC 4446.

Table 3: Pseudowire Service Types

PW Service Type (EtherType)	Value
Ethernet tagged mode	0x0004
Ethernet raw	0x0005
ATM N-to-one VCC cell mode ⁽¹⁾	0x0009
ATM N-to-one VPC cell mode	0x000A
SAToP E1	0x0011
SAToP T1	0x0012
CESoPSN basic mode	0x0015
CESoPSN TDM with CAS	0x0017

Note 1: “N-to-one” is expressed as “N-to-1” throughout this guide.

Service Policies

Common to all 7705 SAR connectivity services are policies that are assigned to the service. Policies are defined at the global level and then applied to a service on the router. Policies are used to define 7705 SAR service enhancements.

The types of policies that are common to all 7705 SAR connectivity services are SAP Quality of Service (QoS) policies and accounting policies.

- SAP Quality of Service (QoS) policies allow for different classes of traffic within a service at SAP ingress and SAP egress.

QoS ingress and egress policies determine the QoS characteristics for a SAP. A QoS policy applied to a SAP specifies the number of queues, queue characteristics (such as forwarding class, committed and peak information rates) and the mapping of traffic to a forwarding class. A QoS policy must be created before it can be applied to a SAP. A single ingress and a single egress QoS policy can be associated with a SAP.

- Accounting policies define how to count the traffic usage for a service for billing purposes.

The 7705 SAR routers provide a comprehensive set of service-related counters. Accounting data can be collected on a per-service, per-forwarding class basis, which enables network operators to accurately measure network usage and bill each customer for each individual service using any of a number of different billing models.

For more information on provisioning QoS policies, including queuing behaviors, refer to the 7705 SAR OS Quality of Service Guide.

Alcatel-Lucent Service Model

The 7705 SAR routers are deployed at the provider edge (PE). Services are provisioned on the 7705 SAR and other network equipment in order to facilitate the transport of telecommunications data across an IP/MPLS provider's core network. The data is formatted so that it can be transported in encapsulation tunnels created using generic routing encapsulation (GRE) or MPLS label switched paths (LSPs).

The service model has four main logical components, referred to as (logical) service entities. The entities are: customers, service types, service access points (SAPs), and service destination points (SDPs) (see [Service Entities on page 30](#)). In accordance with the service model, the operator uses the (logical) service entities to construct an end-to-end service. The service entities are designed to provide a uniform, service-centric model for service provisioning. This service-centric design implies the following characteristics.

- Many services can be bound to a single customer.
- Many services can be bound to a single tunnel.
- Tunnel configurations are independent of the services they carry.
- Changes are made to a single service entity rather than to multiple ports on multiple devices. It is easier to change one tunnel rather than several services.
- The operational integrity of a service entity (such as a service tunnel or service endpoint) can be verified by one operation rather than through the verification of dozens of parameters, thereby simplifying management operations, network scalability, and performance.
- A failure in the network core can be correlated to specific subscribers and services.
- QoS policies and accounting policies are applied to each service.

Additional properties can be configured for bandwidth assignments, class of service, and accounting and billing on the appropriate entity.

Service Entities

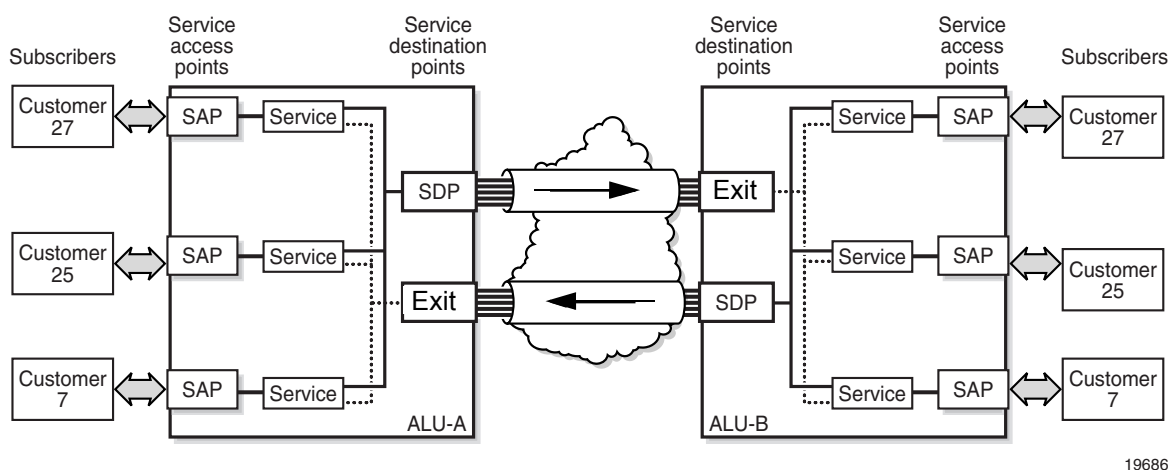
The basic (logical) service entities in the service model used to construct an end-to-end service are:

- [Customers](#)
- [Service Types](#)
- [Service Access Points \(SAPs\)](#)
- [Service Destination Points \(SDPs\)](#)

[Figure 1](#) shows an example of how the service entities relate to the service model. A subscriber (or customer) attachment circuit connects to a SAP. SDPs define the entrance and exit points of unidirectional service tunnels, which carry one-way traffic between the two routers (ALU-A and ALU-B). After SDPs have been configured, they are bound to a service, which is the final step in making the end-to-end service connection. In [Figure 1](#), the entrance point is labeled SDP and the exit point is labeled Exit.

Traffic encapsulation occurs at the SAP and SDP. The SAP encapsulation types are Ethernet and TDM. The SDP encapsulation types are MPLS and GRE. For information on SAP encapsulation types, see [SAP Encapsulation Types and Identifiers](#). For information on SDP encapsulation types, see [SDP Encapsulation Types](#).

Figure 1: Service Entities and the Service Model



19686

Customers

The terms customers and subscribers are used synonymously. Every customer account must have a customer ID, which is assigned when the customer account is created. To provision a service, a customer ID must be associated with the service at the time of service creation.

Service Types

Service types provide the traffic adaptation needed by customer attachment circuits (ACs). This (logical) service entity adapts customer traffic to service tunnel requirements. The 7705 SAR provides three types of VLL service: ATM VLL (Apipe), circuit emulation VLL (Cpipe), and Ethernet VLL (Epipe) service types.

Service Access Points (SAPs)

A service access point (SAP) is the point at which a service begins (ingress) or ends (egress) and represents the access point associated with a service. A SAP may be a physical port or a logical entity within a physical port. For example, a SAP may be a channel group within a DS1 or E1 frame, an ATM endpoint, an Ethernet port, or a VLAN that is identified by an Ethernet port and a VLAN tag. Each subscriber service connection on the 7705 SAR is configured to use only one SAP.

A SAP identifies the customer interface point for a service on an 7705 SAR router. [Figure 2](#) shows one customer connected to two services via two SAPs. The SAP identifiers are 1/1/5 and 1/1/6, which represent the physical ports associated with these SAPs. The physical port information should be configured prior to provisioning a service. Refer to the 7705 SAR OS Interface Configuration Guide for more information on configuring a port. See [Port and SAP CLI Identifiers on page 50](#) for more information on identifiers.

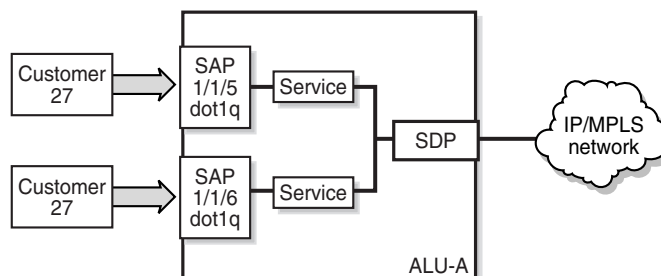
There are three VLL service types available on the 7705 SAR: Apipe, Cpipe, and Epipe. For each service type, the SAP has slightly different parameters. In general, SAPs are logical endpoints that are local to the 7705 SAR and are uniquely identified by:

- the physical Ethernet port or TDM channel group
- the encapsulation type for the service (for example, ATM)
- the encapsulation identifier (ID), which is, for example, the optional VLAN ID for Epipes, or the channel group ID for Cpipes

Depending on the encapsulation, a physical port or channel can have more than one SAP associated with it (for example, a port may have several circuit groups, where each group has an associated SAP). SAPs can only be created on ports or channels designated as “access” in the physical port configuration.

SAPs cannot be created on ports designated as core-facing “network” ports because these ports have a different set of features enabled in software.

Figure 2: Service Access Point (SAP)



19479

SAP Encapsulation Types and Identifiers

The SAP encapsulation type is an access property of the Ethernet port or TDM channel group used for the service. It identifies the protocol that is used to provide the service. The 7705 SAR supports two SAP encapsulation types: Ethernet and TDM. Encapsulation types may have more than one option to choose from. For example, the options for TDM encapsulation type are "cem" (for circuit emulation service) and "atm" (for ATM service).

The encapsulation ID is an optional suffix that is appended to a *port-id* to specify a logical sub-element for a SAP. For example, a port can be tagged to use IEEE 802.1Q encapsulation (referred to as dot1q), where each individual tag can identify with an individual service. The encapsulation ID for an ATM SAP is a special case because it requires that a channel group identifier (which always uses the value 1) precede the VPI/VCI value.



Note: Throughout this guide, the term “channel group” is often simplified to “channel”.

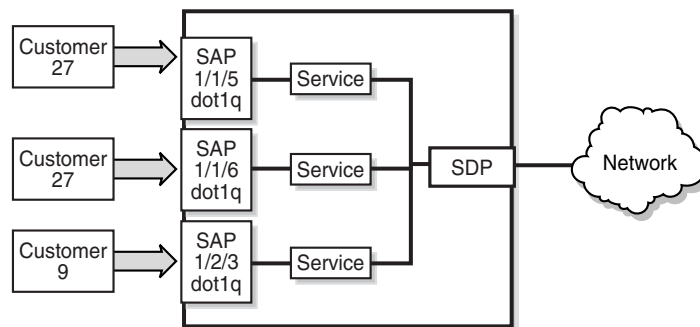
Note: Do not confuse the term “encapsulation ID” (described here) with the term “Encapsulation ID”, which is used with the SNMP and MIBs for the 7705 SAR.

Ethernet Encapsulations

The following encapsulation service options are available on Ethernet ports:

- Null — supports a single service on the port; for example, where a single customer with a single service customer edge (CE) device is attached to the port.
- Dot1q — supports multiple services for one customer or services for multiple customers (see [Figure 3](#)). An example of dot1q use might be the case where the Ethernet port is connected to a multi-tenant unit device with multiple downstream customers. The encapsulation ID used to distinguish an individual service is the VLAN ID in the IEEE 802.1Q header.

Figure 3: Multiple SAPs on a Single Port/Channel



19480

TDM Encapsulations

The following service encapsulation options are available on TDM ports:

- atm — supports multiple services for one customer
- cem — supports multiple services for one customer. Structured cem service (circuit emulation service over packet switched network (CESoPSN ($n \times DS0$))) and unstructured cem service (structure-agnostic TDM over packet (SAToP)) are supported.

Service Types and SAP Encapsulations — Summary

Table 4 lists the SAP encapsulations available to 7705 SAR service types. These encapsulations apply to access-facing ports. The service (port) type and encapsulations are configured at the port level.

Table 4: Service Types and SAP Encapsulations

Service (Port) Type	Encapsulation Option
Ethernet	null
Ethernet	dot1q
TDM	cem
TDM	atm

SAP Configuration Considerations

In addition to being an entry or exit point for a service traffic, a SAP has to be configured for a service and, therefore, has properties. When configuring a SAP, consider the following.

- A SAP is a local entity and is only locally unique to a given device. The same SAP ID value can be used on another 7705 SAR.
- There are no default SAPs. All subscriber service SAPs must be created.
- The default administrative state for a SAP at creation time is administratively enabled.
- When a SAP is deleted, all configuration parameters for the SAP are also deleted.
- A SAP is owned by and associated with the service in which it is created.
- An Ethernet port or channel with a dot1q encapsulation type means that the traffic for the SAP is identified based on a specific IEEE 802.1Q VLAN ID value. The VLAN ID is stripped off at SAP ingress and the appropriate VLAN ID is placed on at SAP egress. As a result, VLAN IDs only have local significance, so the VLAN IDs for the SAPs for a service need not be the same at each SAP.
- A TDM circuit emulation service (for example, CESoPSN) requires a channel group. The channel group must be created before it can be assigned to a SAP.
- An ATM service (for example, ATM N-to-1 VCC cell transport) requires a channel group. For this case, the channel group requires the assignment of all 24 timeslots (T1) or 30 timeslots (E1). The timeslot assignments are made automatically after a channel group is configured for ATM encapsulation.
- If a port or channel is administratively shut down, all SAPs on that port or channel will be operationally out of service.

- A SAP cannot be deleted until it has been administratively disabled (shut down).
- Each SAP can have one of the following policies assigned to it:
 - Ingress QoS policy
 - Egress QoS policy
 - Accounting policy

Service Destination Points (SDPs)

An SDP identifies the endpoint of a logical unidirectional service tunnel. The service tunnel provides a path from one 7705 SAR to another network device, such as another 7705 SAR, a 7710 SR, or a 7750 SR.

In more general terms, SDP refers to the service tunnel itself. The SDP terminates at the far-end router, which is responsible for directing the flow of packets to the correct service egress SAPs on that device.



Note: In this document and in command line interface (CLI) usage, SDP is defined as Service Destination Point. However, it is not uncommon to find the term SDP defined in several different ways, as listed below. In essence, all variations of SDP have the same meaning:

- Service Destination Point
- Service Distribution Point
- Service Destination Path
- Service Distribution Path
- Service Delivery Path

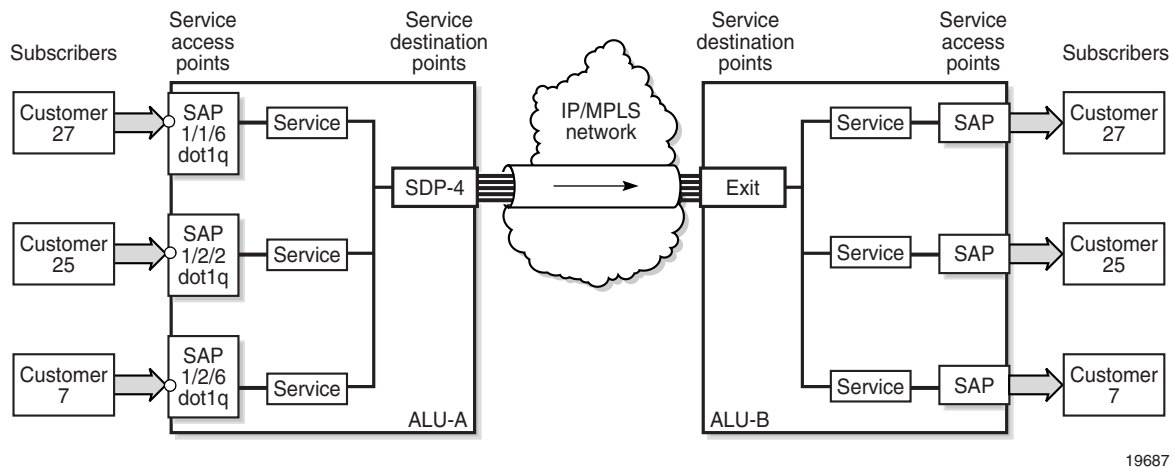
When an SDP is bound to a service, the service is referred to as a distributed service. A distributed service consists of a configuration with at least one SAP on a local node, one SAP on a remote node, and an SDP binding that binds the service to the service tunnel.

An SDP has the following characteristics.

- An SDP is locally unique to a participating 7705 SAR. The same SDP ID can appear on other 7705 SAR routers.
- An SDP uses the system IP address of the far-end edge router to locate its destination.
- An SDP is not specific to any one service or to any type of service. Once an SDP is created, services are bound to the SDP. An SDP can also have more than one service type associated with it.
- All services bound to an SDP use the same SDP (transport) encapsulation type defined for the SDP (GRE or MPLS).
- An SDP is a service entity used for service management. Even though the SDP configuration and the services carried within it are independent, they are related objects. Operations on the SDP affect all the services associated with the SDP. For example, the operational and administrative state of an SDP controls the state of services bound to the SDP.
- An SDP tunnel from the local device (typically, a 7705 SAR) to the far-end device (router) requires a return SDP tunnel from the far end back to the local device. Each device must have an SDP defined for every remote router to which it wants to provide service. The SDP must be created before a distributed service can be configured.

SDP Binding

To configure a distributed service pointing from ALU-A to ALU-B, the SDP ID on the ALU-A side (see [Figure 4](#)) must be specified during service creation in order to bind the service to the tunnel (the SDP). Otherwise, service traffic is not directed to a far-end point and the far-end 7705 SAR device(s) cannot participate in the service (there is no service). To configure a distributed service pointing from ALU-B to ALU-A, the SDP ID on the ALU-B side must be specified.

Figure 4: SDP Tunnel Pointing from ALU-A to ALU-B

19687

Spoke SDPs

There are two types of SDPs: spoke and mesh. The type of SDP defines how flooded traffic (or broadcast traffic, such as an ARP request) is transmitted. Since point-to-point PW/VLL Services are the only supported service type on the 7705 SAR, spoke SDPs are the only way to bind services to the far-end router.

A spoke SDP that is bound to a service operates like a traditional bridge port. Flooded traffic that is received on the spoke SDP is transmitted to all the spoke SDPs to which it is connected. Flooded traffic is not transmitted back toward the port from which it was received.



Note: In contrast, a mesh SDP that is bound to a service operates like a single bridge port. Flooded traffic received on a mesh SDP is transmitted to all spoke SDPs and SAPs to which it is connected. Flooded traffic is not transmitted to any other mesh SDPs or back toward the port from which it was received. This property of mesh SDPs is important for multi-node networks; mesh SDPs are used to prevent the creation of routing loops.

SDP Encapsulation Types

The Alcatel-Lucent service model uses encapsulation tunnels (also referred to as service tunnels) through the core to interconnect 7705 SAR and SR routers. An SDP is a logical way of referencing the entrance to an encapsulation tunnel.

In Release 1.1, the following encapsulation types are supported:

- Layer 2 within LDP signaled (see [MPLS Encapsulation](#))
- Layer 2 within generic routing encapsulation (GRE — [GRE Encapsulation](#))

Each SDP service tunnel has an entrance and an exit point for the pseudowires contained within it.

MPLS Encapsulation

Multiprotocol label switching (MPLS) encapsulation has the following characteristics.

- An MPLS 7705 SAR router supports both signaled and non-signaled LSPs through the network.
- Non-signaled paths are defined at each hop through the network.

An SDP has an implicit Maximum Transmission Unit (MTU) value because services are carried in encapsulation tunnels and an SDP is an entrance to the tunnel. The MTU is configurable (in octets), where the transmitted frame can be no larger than the MTU. With MPLS, the MTU for the network port permits the addition of labels for transmission across the MPLS network. Ethernet frames that are sent out of a network port toward the MPLS core network (or a P router) are allowed to be oversized in order to include the MPLS labels without the need to fragment large frames. See [MTU Settings on page 126](#) for more information.

The following ways of configuring an MPLS tunnel are supported:

- LDP signaled
- user-configured (static LSP)

GRE Encapsulation

Generic routing encapsulation (GRE) is one of the most common tunneling techniques in the industry. GRE tunnels are used to transport various network layer packets and are especially useful for facilitating pseudowires over IP networks. Since MPLS is a Layer 2.5 protocol, MPLS packets cannot be natively transported over a Layer 3 (IP) network. Therefore, GRE is the ideal alternative for applications where traffic must travel over a Layer 3 network; for example, in DSL applications.

For the HSDPA offload application (see [HSDPA Offload on page 44](#)), ATM pseudowires are transported over IP using GRE tunneling. For other applications, Ethernet and TDM pseudowires over GRE are also supported.

GRE SDPs are supported on any port of the 8-port Ethernet Adapter card (for the 7705 SAR-8) or any Ethernet port on the 7705 SAR-F.

GRE format

In accordance with RFC 2784, a GRE encapsulated packet has the following format:

- delivery header
- GRE header
- payload packet

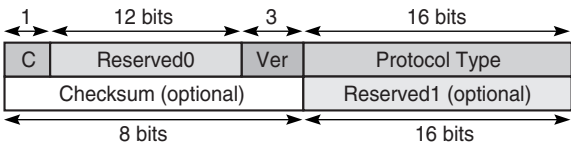
Delivery Header

The delivery header is always an IP header.

GRE Header

The GRE header format is shown in [Figure 5](#) and described in [Table 5](#).

Figure 5: GRE Header



19874

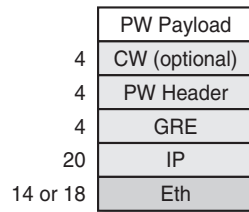
Table 5: GRE Header Descriptions

Field	Description
C	<p>Specifies whether there is a checksum in the header</p> <p>If set to 1, both the checksum and reserved1 fields must be present</p> <p>On the 7705 SAR, in the network egress (transmit) direction, the C bit is always set to 0; therefore, the checksum and reserved1 fields are omitted from the header. The GRE header is therefore always 4 bytes (32 bits) in the network egress direction.</p> <p>In the network ingress direction, the C bit validity is checked. If it is set to a non-zero value, the GRE packet is discarded and the IP discards counter is increased.</p>
Reserved0	<p>Indicates whether the header contains optional fields</p> <p>Not applicable to the 7705 SAR — first 5 bits of the field are always set to 0 and bits 6 to 12 are reserved for future use and also set to 0 by the 7705 SAR</p>
Ver	<p>Always set to 000 for GRE</p> <p>At network ingress, if a GRE packet is received with the version field set to any value other than 000, the packet is discarded and the IP discards counter is increased</p>
Protocol Type	Specifies the protocol type of the original payload packet — identical to Ethertype with the only supported option being MPLS unicast (0x8847)
Checksum (optional)	Not applicable
Reserved1 (optional)	Not applicable

Payload packet

The payload encapsulation format for pseudowires over GRE is shown in [Figure 6](#) and described in [Table 6](#).

Figure 6: GRE Pseudowire Payload Packet over Ethernet



19873

Table 6: GRE Pseudowire Payload Packet Descriptions

Field	Description
Eth	This field is the Layer 2 transport header In Release 1.1, the only Layer 2 protocol supported is Ethernet MTU size depends on the encapsulation type (14 bytes for null encapsulation and 18 bytes for dot1q encapsulation)
IP	Indicates the transport protocol The Ethertype is always set to IP (0x800), and in case of a mismatch, the unexpected or illegal Ethertype counters are increased ⁽¹⁾
GRE	Indicates the encapsulation protocol
PW header	The pseudowire header identifies a service within the GRE tunnel
CW (optional)	The pseudowire control word (CW) is a 32-bit (4-byte) field that is inserted between the VC label and the Layer 2 frame For more information on the control word, see Pseudowire Control Word on page 130
PW payload	The PW payload is the payload of the service being encapsulated (Ethernet, ATM, or TDM)

Note (1): The only exception to the Ethertype is if the packets are address resolution protocol (ARP) packets. For information on ARP, refer to the 7705 SAR OS Router Configuration Guide.

When using GRE, the service MTU might have to be set to a value smaller than 1514 octets. For more information on MTU, see [MTU Settings on page 126](#).

At the network egress of the 7705 SAR, the source address of the IP header is always set to the system IP address. The destination IP address is set to the system IP address of the service router on which the GRE SDP is configured. Using the system IP addresses to bring up the GRE session ensures that any IP link between the two routers can be used to transport GRE/IP packets. It might therefore be necessary to use static IP address configuration over DSL networks to ensure connectivity between the routers (especially if the DSL modem is in bridge mode).

SDP Ping

Ping is an application that allows a user to test whether a particular host is reachable. SDP Ping is an application that allows a user to test whether a particular SDP endpoint is reachable.

SDP ping uses the SDP identifier that is stored in the 7705 SAR that originates the ping request. SDP ping responses can be configured to return through the corresponding return tunnel as a round-trip ping, or out-of band when unidirectional pings are requested. See [SDP Ping on page 279](#) for more information.

SDP Keepalives

The SDP keepalive application allows a system operator to actively monitor the SDP operational state using periodic Alcatel-Lucent SDP Echo Request and Echo Reply messages. Automatic SDP keepalives work in a manner that is similar to a manual SDP ping command. The SDP Echo Request and Echo Reply messages provide a mechanism for exchanging far-end SDP statuses.

SDP keepalive Echo Request messages are only sent after the SDP has been completely configured and is administratively up and the SDP keepalives are administratively up. If the SDP is administratively down, keepalives for the SDP are disabled.

SDP keepalive Echo Request messages are sent out periodically based on the configured Hello Time. An optional message length for the Echo Request can be configured.

The SDP is immediately brought operationally down when:

- the Max Drop Count Echo Request messages do not receive an Echo Reply
- a keepalive response is received that indicates an error condition

After a response is received that indicates the error has cleared and the Hold Down Time interval has expired, the SDP is eligible to be put into the operationally up state. If no other condition prevents the operational change, the SDP enters the operational state.

Configuring SDP keepalives on a given SDP is optional. SDP keepalives have the following configurable keepalive parameters:

- Hello Time
- Message Length
- Max Drop Count
- Hold Down Time
- Timeout

For information about configuring keepalive parameters, refer to [Configuring an SDP on page 61](#).

Mobile Solutions

The Mobile Radio Access Network (RAN) is rapidly growing to meet the increased demand in mobile services. This in turn increases demands on carriers to provide high-bandwidth, mobile broadband services. Today, at a typical cell site, 2G and 3G base stations are connected to high-cost, T1/E1 leased lines that are used to backhaul both voice and data traffic to the MTSO. For mission-critical, delay-sensitive, and low-bandwidth traffic such as voice, signaling, and synchronization traffic, it is vital that the high availability of these leased lines is ensured. SLA agreements also promise a high level of availability for customers.

Currently, however, best-effort traffic such as high-speed downlink packet access (HSDPA) is also switched over these SLA-enabled leased lines. HSDPA is a 3G mobile telephony communications service that allows UMTS networks to have higher data transfer speeds and capacity, allowing the mobile customer (end user) to browse the Internet or to use the mobile device. The increasing use of HSDPA is having a dramatic impact on the ability of the T1/E1 leased lines to scale with the traffic growth as well as on the operating costs of these lines.

Similar issues confront CDMA EVDO networks today.

Alcatel-Lucent provides a solution that enables mobile operators to keep their existing infrastructure (circuit-based leased lines), while gradually migrating to a packet-based infrastructure that will allow scalability, decrease costs, and ease the transition to the next-generation, all-IP network solutions.

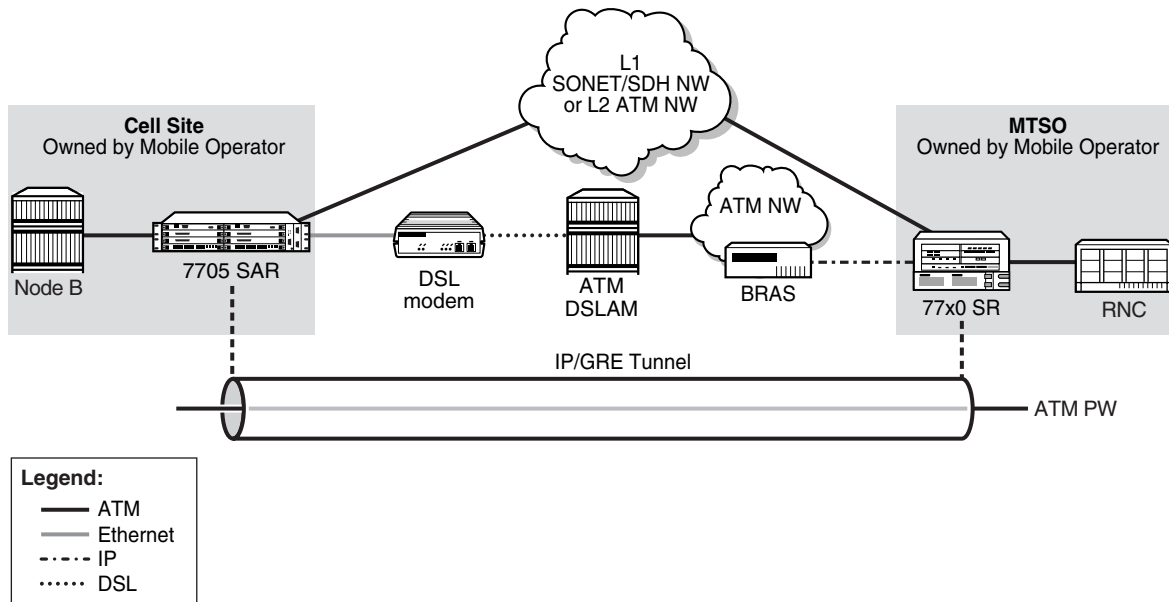
HSDPA Offload

The Alcatel-Lucent solution is to make use of widely available DSL networks and split the traffic being backhauled. Mission-critical traffic (voice, signaling, synchronization) remains on the T1/E1 leased line circuits, while the best-effort, bandwidth-hungry HSDPA traffic is offloaded to DSL networks.

The 7705 SAR-F, introduced in Release 1.1, is an ideal candidate for this scenario. The 7705 SAR-F is a small-scale, fixed version of the 7705 SAR product family. It is optimized for use in standalone small or mid-sized sites where traffic aggregation from multiple cell sites is not needed. For more information on the 7705 SAR-F, refer to the 7705 SAR-F Chassis Installation Guide.

Figure 7 shows a typical example of HSDPA offload.

Figure 7: HSDPA Offload Example



19872

A 3G Node B is connected to a 7705 SAR-F (or 7705 SAR-8) over an ATM/IMA access port (SAP endpoint). An ATM SAP-to-SAP connection is set up in the 7705 SAR and a pseudowire is configured between the two endpoints to emulate local ATM switching. Traffic from the Node B enters an ATM/IMA port, the VCs transporting mission-critical traffic are locally switched (SAP-to-SAP) to another ATM/IMA port (SAP endpoint), and then switched over the leased lines to the MTSO.



Note: ATM SAP-to-SAP connections are supported between any T1/E1 ASAP port that is in access mode with ATM/IMA encapsulation and another port with the same configuration. One endpoint of a SAP connection can be an IMA group, while the other endpoint can be on a single ATM port.

For non-mission-critical traffic, for example, HSDPA traffic, an Ethernet interface on the 7705 SAR is connected to an external DSL modem. HSDPA traffic is interworked to ATM pseudowires and transported over the DSL network to the BRAS, then forwarded to the service router at the MTSO.

Failure Detection

Failure of the GRE SDP or the IP network it rides over can be detected by OAM tools as well as by BFD. With SAA, OAM tools can be configured to run periodically in order to facilitate faster failure detection. If a failure occurs, the ATM SAPs must be rerouted by the 5620 SAM to the ATM ports used for backhauling the traffic. The mission-critical traffic is still serviced before the best-effort HSDPA traffic.

For information on OAM and SAA tools, see the chapter [OAM and SAA on page 277](#). For information on BFD, refer to the 7705 SAR OS Router Configuration Guide.

Service Creation Overview

[Figure 8](#) shows a flow chart that provides an overview of the process to create a service. Service creation can be separated into two main functional areas — core services tasks and subscriber services tasks. Core services tasks are performed prior to subscriber services tasks.

Before starting the process shown in [Figure 8](#), ensure that the 7705 SAR system has been configured with an IP address and (for the 7705 SAR-8) has the appropriate adapter cards installed and activated.

Core tasks include the following items:

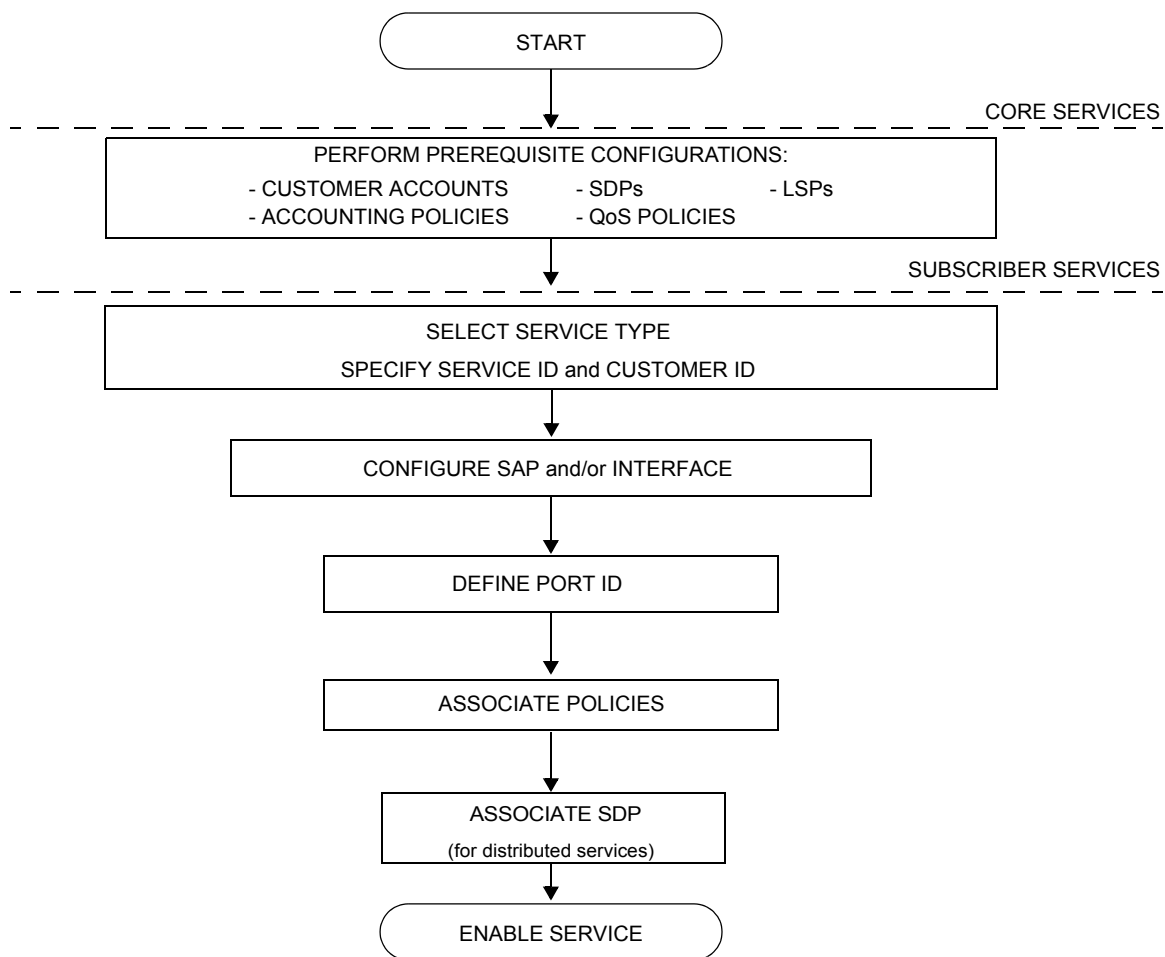
- create customer accounts
- create template QoS and accounting policies
- create LSPs
- create SDPs

Subscriber services tasks include the following items:

- create Apipe, Cpipe, or Epipe services or IES
- configure SAPs
- bind SDPs
- create exclusive QoS policies

See [Subscriber Services Components on page 49](#) for additional information on subscriber services.

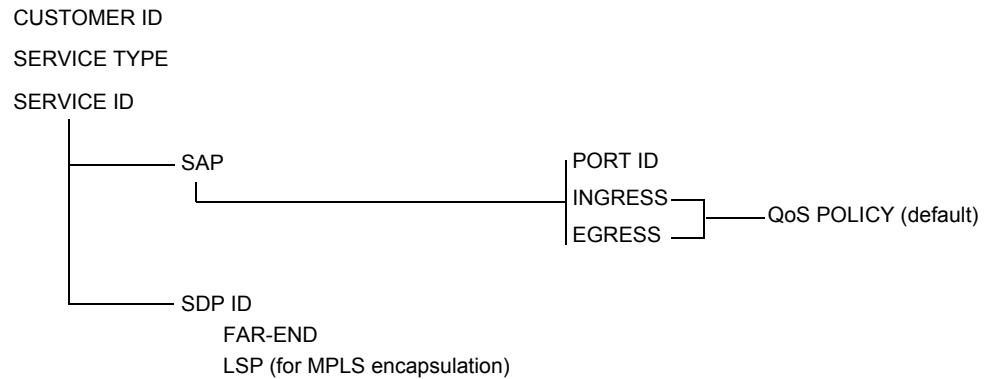
Figure 8: Service Creation and Implementation Flow Chart



Subscriber Services Components

Figure 9 shows the basic components of a subscriber service. The items in the figure are described in the list following Figure 9.

Figure 9: Subscriber Service Components



- Customer ID — associates information with a particular customer
- Service type — specifies the connectivity type, such as Apipe, Cpipe, or Epipe
- Service ID — identifies each service with a unique ID number
- SAP — the subscriber-side service entry (access) and exit point for a service
 - Port ID — identifies the physical port part of the SAP definition
 - QoS policy — identifies the QoS policy associated with an ingress or egress SAP or IP interface. QoS policy ID 1 is the default.
- SDP — the (logical) service entity that ties a far-end 7705 SAR to a specific service without having to specifically define the far-end SAPs. Each SDP, identified by a local SDP ID, represents a method for reaching a far-end 7705 SAR.

Port and SAP CLI Identifiers

When typing text in the command line interface (CLI), *port-id* is often displayed to indicate that a port identifier may need to be typed in the command line. Similarly, to identify a SAP, the *port-id* is used, but additional information may need to be appended to indicate a logical sub-element of the port.

On the CLI, a *port-id* is defined using the format *slot/mda/port*, where *slot* identifies the IOM card slot (always 1), *mda* identifies the physical slot in the chassis for the adapter card, and *port* identifies the physical port on the adapter card.

The value that can be appended to a SAP has the format *[:][ID]* or *[.][ID]*. The colon or dot and following ID identify a sub-element of the port (if applicable), such as a TDM channel group for a Cpipe or a VPI/VCI value for an Apipe.

For example, a SAP associated with a TDM channel group on port 12 of an ASAP card in MDA slot 3 is identified as <1/3/12.3>, where ".3" is the appended value and identifies that for this SAP the channel group begins in timeslot 3.

Reference Sources

For information on standards and supported MIBs, refer to [Standards and Protocol Support on page 357](#).

Configuring Global Service Entities with CLI

This section provides information to create subscriber (customer) accounts and to configure service destination points (SDPs) using the command line interface.

Topics in this section include:

- [Service Model Entities on page 52](#)
 - [Service CLI Command Structure on page 53](#)
 - [List of Commands on page 55](#)
 - [Basic Configuration on page 57](#)
 - [Common Configuration Tasks on page 59](#)
 - [Configuring Customer Accounts on page 59](#)
 - [Configuring SDPs on page 60](#)
 - [Service Management Tasks on page 63](#)
-

Service Model Entities

The Alcatel-Lucent service model uses (logical) service entities to construct a service. Each entity within the model has properties that describe it and influence its behavior. The service model has four main entities to configure a service. The entities are:

- Customers
 - [Configuring Customer Accounts on page 59](#)
 - Service Destination Points (SDPs)
 - [Configuring SDPs on page 60](#)
 - Service Types
 - [ATM VLL \(Apipe\) Services on page 94](#)
 - [Circuit Emulation VLL \(Cpipe\) Services on page 97](#)
 - [Ethernet VLL \(Epipe\) Services on page 114](#)
 - [Internet Enhanced Service on page 237](#)
 - Service Access Points (SAPs)
 - [Configuring Apipe SAP Parameters on page 143](#)
 - [Configuring Cpipe SAP parameters on page 146](#)
 - [Configuring Epipe SAP Parameters on page 150](#)
 - [Configuring IES SAP Parameters on page 249](#)
-

Service CLI Command Structure

There are two main areas that need to be configured in order to set up a service:

- core and customer configuration
- global service configuration

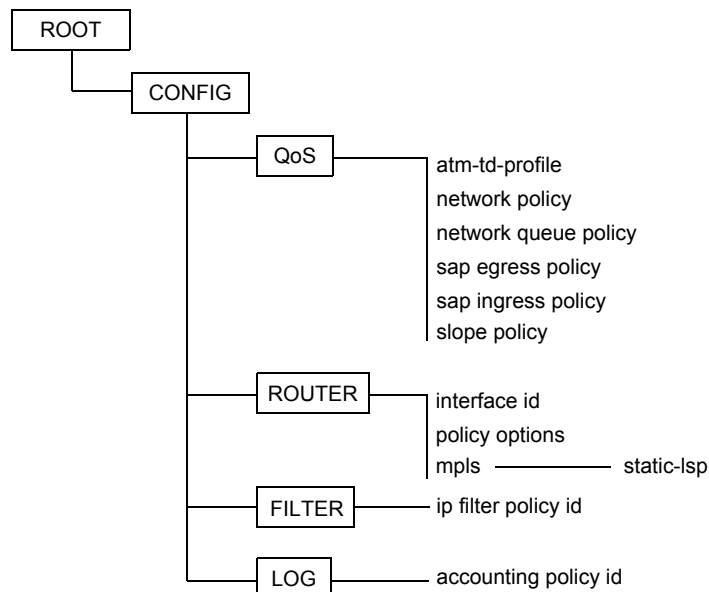
Core and Customer Configuration

Figure 10 displays the structural overview of the basic CLI commands used for core and customer configuration. These commands should be performed prior to provisioning a subscriber service.

For command and syntax information needed to use these commands, refer to the following guides:

- 7705 SAR OS Quality of Service Guide
- 7705 SAR OS Router Configuration Guide
- 7705 SAR OS System Management Guide
- 7705 SAR OS MPLS Guide

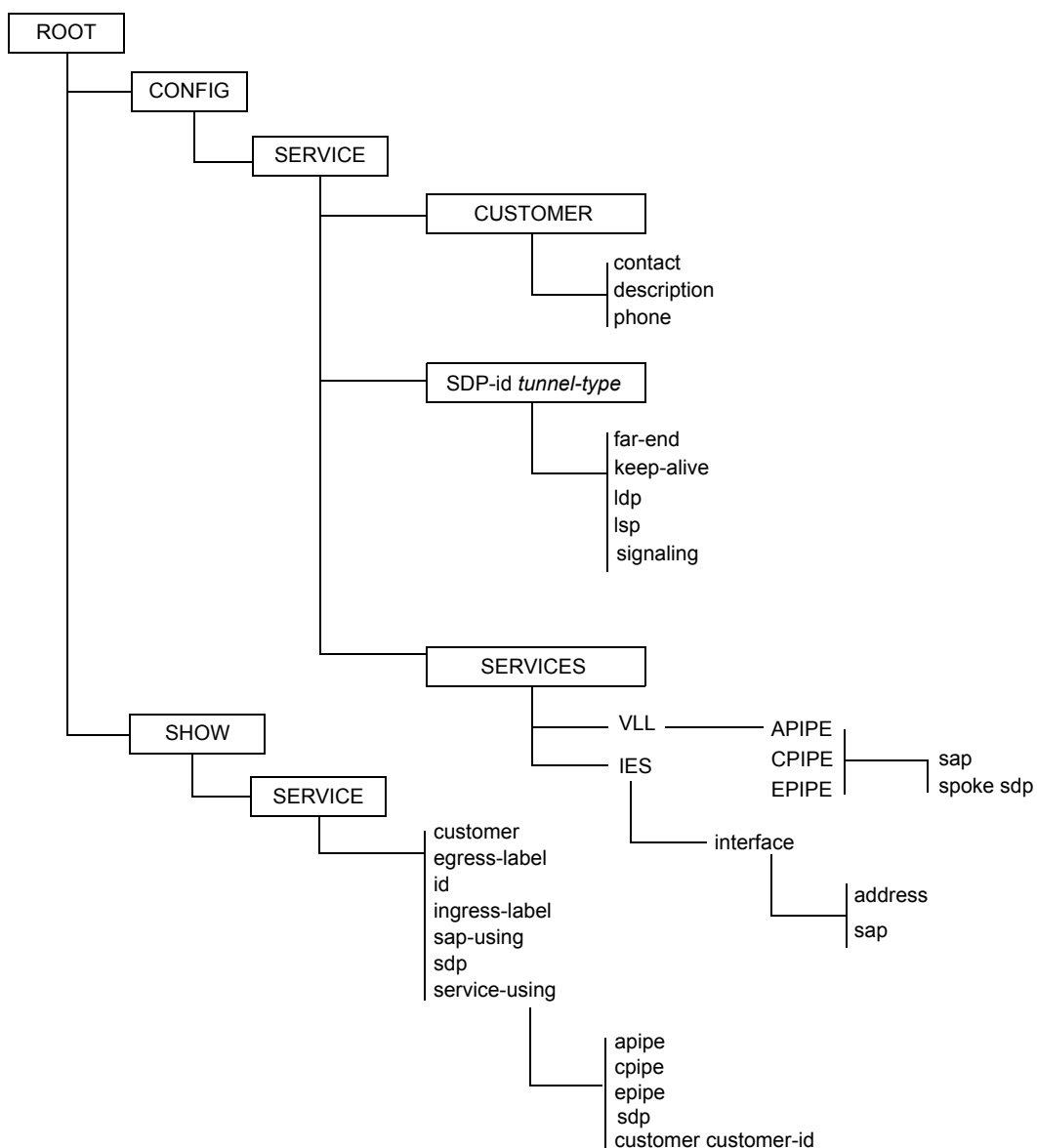
Figure 10: Core and Customer Command Overview



Global Service Configuration

Figure 11 displays the structural overview of the CLI commands used to configure a service. The service configuration commands are located under the `config>service` context and are described in this guide (7705 SAR OS Services Guide). Use the `show>service` context to view information about an aspect of the service.

Figure 11: Global Service CLI Command Overview



List of Commands

[Table 7](#) lists all the configuration commands required to configure subscriber accounts and SDPs, indicating the configuration level at which each command is implemented with a short command description.

The command list is organized in the following task-oriented manner:

- [Configure the customer account](#)
- [Configure an SDP](#)
- [Configure SDP keepalive parameters](#)

Table 7: CLI Commands to Configure Service Parameters

Command	Description	Page
Configure the customer account		
<code>config>service>customer</code>		59
<code>contact</code>	Creates a customer ID and the customer context used to associate information with a particular customer	73
<code>description</code>	Creates a text description of the customer that is stored in the configuration file	71
<code>phone</code>	Adds phone number information for a customer ID	74
Configure an SDP		
<code>config>service>sdp</code>		60
<code>adv-mtu-override</code>	Overrides the advertised VC MTU	76
<code>description</code>	Specifies a text string describing the SDP	71
<code>far-end</code>	Configures the system IP address of the far-end destination router for the SDP that is terminating services	76
<code>gre</code>	Specifies that the SDP uses GRE encapsulation	75
<code>keep-alive</code>	Configures SDP connectivity monitoring keepalive messages for the SDP ID	80
<code>ldp</code>	Enables LDP-signaled LSPs on MPLS-encapsulated SDPs	77
<code>lsp</code>	Creates associations between an LSP and an MPLS SDP	77

Table 7: CLI Commands to Configure Service Parameters (Continued)

Command	Description	Page
<code>mpls</code>	Specifies that the SDP uses MPLS encapsulation	75
<code>metric</code>	Specifies the metric to be used within the tunnel table manager for decision-making purposes	78
<code>path-mtu</code>	Configures the MTU in bytes that the SDP can transmit to the far-end router without packet dropping the SDP-type default path-mtu	78
<code>shutdown</code>	Administratively enables or disables the SDP	71
<code>signaling</code>	Enables the signaling protocol (targeted LDP) to obtain the ingress and egress labels in frames transmitted and received on the SDP	79
<code>vlan-vc-etype</code>	Specifies the VLAN VC EtherType	79
Configure SDP keepalive parameters		60
<code>config>service>sdp>keep-alive</code>		80
<code>hello-time</code>	Configures the time period between SDP keepalive messages on the SDP-ID for the SDP connectivity monitoring messages	81
<code>hold-down-time</code>	Configures the minimum time period the SDP will remain in the operationally down state in response to SDP keepalive monitoring	81
<code>max-drop-count</code>	Configures the number of consecutive SDP keepalive failed request attempts or remote replies that can be missed after which the SDP is operationally downed	82
<code>message-length</code>	Configures the size of SDP monitoring keepalive request messages	82
<code>shutdown</code>	Administratively enables or disables the keepalive messages	71
<code>timeout</code>	Configures the time interval that the SDP waits before tearing down the session	83

Basic Configuration

Before configuring a subscriber service, the QoS, logs, and MPLS LSPs (if applicable) must be configured. Refer to the following guides for more information:

- 7705 SAR OS Quality of Service Guide
- 7705 SAR OS Router Configuration Guide
- 7705 SAR OS System Management Guide
- 7705 SAR OS MPLS Guide

A basic service configuration must have the following items configured:

- a customer ID
- a service type
- a service ID
- a SAP identifying a port and encapsulation value
- an interface (where required) identifying an IP address, IP subnet, and broadcast address
- an associated SDP (for distributed services)

The following example shows an Epipe service configuration displaying the SDP and Epipe service entities. SDP ID 2 was created with the far-end node 10.10.10.104. Epipe ID 6000 was created for customer ID 6, which uses the SDP ID 2.

```
A:ALU-B>config>service# info detail
#-----
...
    sdp 2 mpls create
        description "MPLS-10.10.10.104"
        far-end 10.10.10.104
    ldp
        signaling tldp
        no vlan-vc-etype
        no path-mtu
        keep-alive
        shutdown
        hello-time 10
        hold-down-time 10
        max-drop-count 3
        timeout 5
        no message-length
    exit
    no shutdown
exit
...
epipe 6000 customer 6 vpn 6000 create
    service-mtu 1514
    sap 1/1/2:0 create
        no multi-service-site
```

```
        ingress
            qos 1
        exit
        egress
            qos 1
        exit
        no shutdown
    exit
    spoke-sdp 2:6111 create
        ingress
            no vc-label
        exit
        egress
            no vc-label
        exit
        no shutdown
    exit
    no shutdown
exit
...
#-----
A:ALU-B>config>service#
```

Common Configuration Tasks

This section provides a brief overview of the following common configuration tasks that must be performed to configure a customer account and an SDP:

- [Configuring Customer Accounts](#)
- [Configuring SDPs](#)

Configuring Customer Accounts

Use the `customer` command to configure customer information. Every customer account must have a customer ID. Optional parameters include:

- `description`
- `contact name`
- `telephone number`

If special characters are included in the customer description string, such as spaces, #, or ?, the entire string must be enclosed in double quotes.

Use the following CLI syntax to create and input customer information.

CLI Syntax:

```
config>service# customer customer-id create
                    contact contact-information
                    description description-string
                    phone phone-number
```

Example:

```
config>service# customer 5 create
config>service>cust# contact "Technical Support"
config>service>cust$ description "Alcatel-Lucent Customer"
config>service>cust# phone "650 555-5100"
config>service>cust# exit
```

The following example displays the customer account configuration output.

```
A:ALU-12>config>service# info
-----
..
    customer 5 create
        contact "Technical Support"
        description "Alcatel-Lucent Customer"
        phone "650 555-5100"
    exit
...
-----
A:A:ALU-12>config>service#
```

Configuring SDPs

Every service destination point (SDP) must have the following items configured:

- a locally unique SDP identification (ID) number
- the system IP address of the far-end router
- an SDP encapsulation type — either GRE or MPLS

SDP Configuration Considerations

Consider the following SDP characteristics when creating and configuring an SDP.

- SDPs can be configured as either GRE or MPLS.
- If an SDP configuration does not include the IP address of the associated far-end router, then VLL services to the far-end router cannot be provided.
- A service must be bound to an SDP.
- An SDP is only used when a service is bound to it.
By default, SDPs are not associated with services. Once an SDP is created, services can be associated with that SDP.
- An SDP can have more than one service bound to it. That is, an SDP is not specific or exclusive to any one service or any type of service.
- When configuring an SDP:
 - The far-end SDP IP address must be the system IP address of a 7705 SAR or an SR-series router.
 - For MPLS SDPs, the LSPs must be configured before the LSP-to-SDP associations can be assigned. The LSP-to-SDP associations must be created explicitly.
 - Automatic ingress and egress labeling (targeted LDP) is enabled by default. Ingress and egress VC labels are signaled over a targeted LDP connection between two 7705 SAR routers.



Note: If signaling is disabled for an SDP, then ingress and egress vc-labels for the services using that SDP must be configured manually.

Configuring an SDP

When configuring an SDP, consider the following points.

- If you do not specify an encapsulation type, the default is MPLS.
- When configuring a distributed service, you must identify an SDP ID and the far-end IP address. Use the `show>service>sdp` command to display a list of qualifying SDPs.
- When specifying MPLS SDP parameters, you can either specify an LSP or enable an LDP. There cannot be two methods of transport in a single SDP.
- LSPs are configured in the `config>router>mpls` context. See the 7705 SAR OS MPLS Guide for configuration and command information.

Use the following CLI syntax to create an SDP.

CLI Syntax:

```
config>service>sdp sdp-id [gre | mpls] create
adv-mtu-override
description description-string
far-end ip-addr
keep-alive
  hello-time seconds
  hold-down-time seconds
  max-drop-count count
  message-length octets
  timeout timeout
no shutdown
ldp                                     (for MPLS SDPs only)
lsp lsp-name [lsp-name] (for MPLS SDPs only)
path-mtu octets
signaling {off|tldp}
no shutdown
```

Example:

```
config>service# sdp 2 gre create
config>service>sdp# description "GRE-10.10.10.104"
config>service>sdp# far-end "10.10.10.104"
config>service>sdp# no shutdown
config>service>sdp# exit
config>service# sdp 4 mpls create
config>service>sdp# description "MPLS-10.10.10.104"
config>service>sdp# far-end "10.10.10.104"
config>service>sdp# ldp
config>service>sdp# no shutdown
config>service>sdp# exit
config>service# sdp 8 mpls create
config>service>sdp# description "MPLS-10.10.10.104"
config>service>sdp# far-end "10.10.10.104"
config>service>sdp# lsp "to-104"
```

```
config>service>sdp# no shutdown
config>service>sdp# exit
config>service# sdp 104 mpls create
config>service>sdp# description "MPLS-10.10.10.94"
config>service>sdp# far-end "10.10.10.94"
config>service>sdp# ldp
config>service>sdp# no shutdown
config>service>sdp# exit
```

The following example displays the SDP sample configuration output.

```
A:ALU-12>config>service# info
-----
...
    sdp 2 create
        description "GRE-10.10.10.104"
        far-end 10.10.10.104
        keep-alive
            shutdown
        exit
        no shutdown
    sdp 4 create
        description "MPLS-10.10.10.104"
        far-end 10.10.10.104
        ldp
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 8 mpls create
        description "MPLS-10.10.10.104"
        far-end 10.10.10.104
        lsp "to-104"
        keep-alive
            shutdown
        exit
        no shutdown
    exit
    sdp 104 mpls create
        description "MPLS-10.10.10.94"
        far-end 10.10.10.94
        ldp
        keep-alive
            shutdown
        exit
        no shutdown
    exit
...
-----
A:ALU-12>config>service#
```

Service Management Tasks

This section provides a brief overview of the following service management tasks:

- [Modifying Customer Accounts](#)
- [Deleting Customers](#)
- [Modifying SDPs](#)
- [Deleting SDPs](#)
- [Deleting LSP Associations](#)

Modifying Customer Accounts

Use the `show>service>customer` command to display a list of customer IDs.

To modify a customer account:

1. Access the specific account by specifying the customer ID.
2. Enter the parameter to modify (description, contact, phone) and then enter the new information.

CLI Syntax: `config>service# customer customer-id create`
`[no] contact contact-information`
`[no] description description-string`
`[no] phone phone-number`

Example: `config>service# customer 27 create`
`config>service>customer$ description "Western Division"`
`config>service>customer# contact "John Dough"`
`config>service>customer# no phone "(650) 237-5102"`

Deleting Customers

The `no` form of the `customer` command typically removes a customer ID and all associated information; however, all service references to the customer must be shut down and deleted before a customer account can be deleted.

CLI Syntax: `config>service# no customer customer-id`

Example:

```
config>service# epipe 5 customer 27 shutdown
config>service# epipe 9 customer 27 shutdown
config>service# no epipe 5
config>service# no epipe 9
config>service# no customer 27
```

Modifying SDPs

Use the `show>service>sdp` command to display a list of SDP IDs.

To modify an SDP:

1. Access the specific SDP by specifying the SDP ID.
2. Enter the parameter to modify, such as `description`, `far-end`, or `lsp`, and then enter the new information.



Note: Once the SDP is created, you cannot modify the SDP encapsulation type.

CLI Syntax: `config>service# sdp sdp-id`

Example:

```
config>service# sdp 79
config>service>sdp# description "Path-to-107"
config>service>sdp# shutdown
config>service>sdp# far-end "10.10.10.107"
config>service>sdp# path-mtu 1503
config>service>sdp# no shutdown
```


Deleting SDPs

The `no` form of the `sdp` command typically removes an SDP ID and all associated information; however, before an SDP can be deleted, the SDP must be shut down and removed (unbound) from all customer services where it is applied.

CLI Syntax: `config>service# no sdp 79`

Example:

```
config>service# epipe 5 spoke-sdp 79:5
config>service>epipe>spoke-sdp# shutdown
config>service>epipe>spoke-sdp# exit
config>service>epipe 5 no spoke-sdp 79:5
config>service>epipe# exit
config>service# no sdp 79
```

Deleting LSP Associations

The `no` form of the `lsp` command removes an LSP ID and all associated information; however, before an LSP can be deleted, it must be removed from all SDP associations.

CLI Syntax: `config>service# sdp sdp-id`
`[no] lsp lsp-name`

Example:

```
config>service# sdp 79
config>service>sdp# no lsp 123
config>service>sdp# exit all
```

Global Service Command Reference

Command Hierarchies

- [Global Service Configuration Commands](#)
 - [Customer Commands](#)
 - [SDP Commands](#)
 - [SAP Commands](#)
- [Show Commands](#)

Global Service Configuration Commands

Customer Commands

```

config
  — service
    — customer customer-id [create]
    — no customer customer-id
      — customer contact-information
      — no customer
      — description description-string
      — no description
      — phone phone-number
      — [no] phone

```

SDP Commands

```

config
  — service
    — sdp sdp-id [gre | mpls] [create]
    — no sdp sdp-id
      — [no] adv-mtu-override
      — description description-string
      — no description
      — far-end ip-address
      — no far-end
      — keep-alive
        — hello-time seconds
        — no hello-time
        — hold-down-time seconds
        — no hold-down-time
        — max-drop-count count
        — no max-drop-count
        — message-length octets
        — no message-length
        — [no] shutdown
        — timeout timeout
        — no timeout
      — [no] ldp
      — [no] lsp lsp-name
      — metric metric
      — no metric
      — path-mtu bytes
      — no path-mtu
      — signaling {off | tldp}
      — [no] shutdown
      — vlan-vc-etype 0x0600..0xffff
      — no vlan-vc-etype [x0600.0xffff]

```

SAP Commands

```

config
  — service
    — apipe
      — sap sap-id [create]
      — no sap sap-id
    — cpipe
      — sap sap-id [create]
      — no sap sap-id
    — epipe
      — sap sap-id [create]
      — no sap sap-id
    — ies
      — interface ip-int-name [create]
        — sap sap-id [create]
        — no sap sap-id

```

Show Commands

```

show
  — service
    — customer customer-id
    — sdp [sdp-id | far-end ip-addr] [detail | keep-alive-history]
    — sdp-using [sdp-id [.vc-id] | far-end ip-address]
    — service-using [epipe] [apipe] [cpipe] [sdp sdp-id] [customer customer-id]

```

Global Service Configuration Commands

- [Generic Commands on page 71](#)
- [Customer Commands on page 73](#)
- [SDP Commands on page 75](#)
- [SDP Keepalive Commands on page 80](#)

Generic Commands

description

Syntax	description <i>description-string</i> no description
Context	config>service>customer config>service>sdp
Description	This command creates a text description stored in the configuration file for a configuration context. The no form of this command removes the string from the context.
Default	No description is associated with the configuration context.
Parameters	<i>description-string</i> — 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>service>sdp config>service>sdp>keep-alive
Description	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. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many objects must be shut down before they may be deleted. Many entities must be explicitly enabled using the no shutdown command. The no form of this command places the entity into an administratively enabled state. Services are created in the administratively down state (shutdown). When a no shutdown command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities are described in the following Special Cases.

Special Cases

Service Admin State — bindings to an SDP within the service will be put into the out-of-service state when the service is shut down. While the service is shut down, all customer packets are dropped and counted as discards for billing and debugging purposes.

SDP (global) — when an SDP is shut down at the global service level, all bindings to that SDP are put into the out-of-service state and the SDP itself is put into the administratively and operationally

down states. Packets that would normally be transmitted using this SDP binding will be discarded and counted as dropped packets.

SDP (service level) — shutting down an SDP within a service only affects traffic on that service from entering or being received from the SDP. The SDP itself may still be operationally up for other services.

SDP Keepalives — enables SDP connectivity monitoring keepalive messages for the SDP ID. Default state is disabled (shutdown), in which case the operational state of the SDP-ID is not affected by the keepalive message state.

Customer Commands

customer

Syntax	customer <i>customer-id</i> [create] no customer <i>customer-id</i>
Context	config>service
Description	<p>This command creates a customer ID and customer context used to associate information with a particular customer. Services can later be associated with this customer at the service level.</p> <p>Each <i>customer-id</i> must be unique and the create keyword must follow each new customer <i>customer-id</i> entry.</p> <p>To edit a customer's parameters, enter the existing customer <i>customer-id</i> without the create keyword.</p> <p>Default customer 1 always exists on the system and cannot be deleted.</p> <p>The no form of this command removes a <i>customer-id</i> and all associated information. Before removing a <i>customer-id</i>, all references to that customer in all services must be deleted or changed to a different customer ID.</p>
Parameters	<i>customer-id</i> — specifies the ID number to be associated with the customer, expressed as an integer
Values	1 to 2147483647

contact

Syntax	contact <i>contact-information</i> no contact
Context	config>service>customer
Description	<p>This command allows you to configure contact information for a customer. Include any customer-related contact information such as a technician's name or account contract name.</p> <p>The no form of this command removes the contact information from the customer ID.</p>
Default	No contact information is associated with the <i>customer-id</i> .
Parameters	<p><i>contact-information</i> — the customer contact information entered as an ASCII 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.</p>

phone

Syntax	[no] phone <i>phone-number</i>
Context	config>service>customer
Description	<p>This command adds telephone number information for a customer ID.</p> <p>The no form of this command removes the phone number value from the customer ID.</p>
Default	No telephone number information is associated with a customer.
Parameters	<i>phone-number</i> — the customer phone number entered as an ASCII 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.

SDP Commands

sdp

Syntax	sdp <i>sdp-id</i> [gre mpls] [create] no sdp <i>sdp-id</i>
Context	config>service
Description	<p>This command creates or edits an SDP. SDPs must be explicitly configured.</p> <p>An SDP is a (logical) service entity that is created on the local router. An SDP identifies the endpoint of a logical, unidirectional service tunnel. Traffic enters the tunnel at the SDP on the local router and exits the tunnel at the remote router. Thus, it is not necessary to specifically define far-end SAPs.</p> <p>In Release 1.1, generic routing encapsulation (GRE) and multiprotocol label switching (MPLS) tunnels are supported. For MPLS, a 7705 SAR supports both signaled and non-signaled label switched paths (LSPs) through the network. Non-signaled paths are defined at each hop through the network. Signaled LSPs are established in LDP-DU (downstream unsolicited) mode.</p> <p>SDPs are created and then bound to services. Many services may be bound to a single SDP. The operational and administrative state of the SDP controls the state of the SDP binding to the service.</p> <p>If <i>sdp-id</i> does not exist, a new SDP is created. SDPs are created in the admin down state (shutdown). Once all relevant parameters are defined, the no shutdown command must be executed before the SDP can be used.</p> <p>If <i>sdp-id</i> exists, the current CLI context is changed to that SDP for editing and modification. If editing an existing SDP, the gre or mpls keyword is not specified. If a keyword is specified for an existing <i>sdp-id</i>, an error is generated and the context of the CLI is not changed to the specified <i>sdp-id</i>.</p> <p>The no form of this command deletes the specified SDP. Before an SDP can be deleted, it must be administratively down (shutdown) and not bound to any services. If the specified SDP is bound to a service, the no sdp command fails, generating an error message specifying the first bound service found during the deletion process. If the specified <i>sdp-id</i> does not exist, an error is generated.</p>
Default	none
Parameters	<p><i>sdp-id</i> — the SDP identifier</p> <p>Values 1 to 17407</p> <p>gre — specifies that the SDP will use GRE encapsulation tunnels. Only one GRE SDP is supported to a given destination 7705 SAR or 7710/7750 SR.</p> <p>mpls — specifies that the SDP will use MPLS encapsulation and one or more LSP tunnels to reach the far-end 7705 SAR or 7710/7750 SR. Multiple MPLS SDPs are supported to a given destination service router. Multiple MPLS SDPs to a single destination service router are helpful when they use divergent paths.</p>

adv-mtu-override

Syntax	[no] adv-mtu-override
Context	config>service>sdp
Description	<p>This command overrides the advertised VC-type MTU. When enabled, the 7705 SAR signals a VC MTU equal to the service MTU that includes the Layer 2 header. Under normal operations it will advertise the service MTU minus the Layer 2 header. In the receive direction, it will accept either one.</p> <p>The no form of this command disables the VC-type MTU override.</p>
Default	no adv-mtu-override

far-end

Syntax	far-end ip-address no far-end		
Context	config>service>sdp		
Description	<p>This command configures the system IP address of the far-end destination 7705 SAR, 7710 SR, 7750 SR, or other router ID platform for the SDP that is the termination point for a service.</p> <p>The far-end IP address must be explicitly configured. The destination IP address must be a 7705 SAR, 7710 SR, 7750 SR, or other router ID platform system IP address.</p> <p>If the SDP uses GRE for the destination encapsulation, the local 7705 SAR might not know whether the <i>ip-address</i> is actually a system IP interface address on the far-end service router.</p> <p>If the SDP uses MPLS encapsulation, the far-end ip-address is used to check LSP names when added to the SDP. If the “to IP address” defined within the LSP configuration does not exactly match the SDP far-end ip-address, the LSP will not be added to the SDP and an error message will be generated.</p> <p>An SDP cannot be administratively enabled until a far-end ip-address is defined. The SDP is operational when it is administratively enabled (no shutdown).</p> <p>The no form of this command removes the currently configured destination IP address for the SDP. The <i>ip-address</i> parameter is not specified and will generate an error message if used in the no far-end command. The SDP must be administratively disabled using the config>service>sdp>shutdown command before the no far-end command can be executed. Removing the far-end IP address will cause all <i>lsp-name</i> associations with the SDP to be removed.</p>		
Default	none		
Parameters	<p><i>ip-address</i> — the system address of the far-end 7705 SAR for the SDP</p> <table><tr><td>Values</td><td>a.b.c.d</td></tr></table>	Values	a.b.c.d
Values	a.b.c.d		

ldp

Syntax	[no] ldp
Context	config>service>sdp
Description	<p>This command enables LDP-signaled LSPs on MPLS-encapsulated SDPs.</p> <p>In MPLS SDP configurations, either one LSP can be specified or LDP can be enabled. The SDP ldp and lsp commands are mutually exclusive. If an LSP is specified on an MPLS SDP, then LDP cannot be enabled on the SDP. To enable LDP on the SDP when an LSP is already specified, the LSP must be removed from the configuration using the no lsp lsp-name command.</p> <p>Alternatively, if LDP is already enabled on an MPLS SDP, then an LSP cannot be specified on the SDP. To specify an LSP on the SDP, LDP must be disabled. The LSP must have already been created in the config>router>mpls context with a valid far-end IP address.</p>
Default	no ldp (disabled)

lsp

Syntax	[no] lsp lsp-name
Context	config>service>sdp
Description	<p>This command creates an association between an LSP and an MPLS SDP. This command is implemented only on MPLS-type encapsulated SDPs.</p> <p>In MPLS SDP configurations, either one LSP can be specified or LDP can be enabled. The SDP ldp and lsp commands are mutually exclusive. If an LSP is specified on an MPLS SDP, then LDP cannot be enabled on the SDP. To enable LDP on the SDP when an LSP is already specified, the LSP must be removed from the configuration using the no lsp lsp-name command.</p> <p>Alternatively, if LDP is already enabled on an MPLS SDP, then an LSP cannot be specified on the SDP. To specify an LSP on the SDP, LDP must be disabled. The LSP must have already been created in the config>router>mpls context with a valid far-end IP address. Refer to the 7705 SAR OS MPLS Guide for CLI syntax and command usage.</p> <p>If no LSP is associated with an MPLS SDP, the SDP cannot enter the operationally up state. The SDP can be administratively enabled (no shutdown) with no LSP associations. The <i>lsp-name</i> may be shut down, causing the association with the SDP to be operationally down (the LSP will not be used by the SDP).</p> <p>LSP SDPs also require that the TLDP signaling be specified and that the SDP keepalive parameter be enabled and not timed out.</p> <p>The no form of this command deletes an LSP association from an SDP. If the <i>lsp-name</i> does not exist as an association or as a configured LSP, no error is returned. An <i>lsp-name</i> must be removed from all SDP associations before the <i>lsp-name</i> can be deleted from the system. The SDP must be administratively disabled (shutdown) before the last <i>lsp-name</i> association with the SDP is deleted.</p>

Default	No LSP names are defined.
Parameters	<i>lsp-name</i> — the name of the LSP to associate with the SDP. An LSP name is case-sensitive and is limited to 32 ASCII 7-bit printable characters with no spaces. If an exact match of <i>lsp-name</i> does not already exist as a defined LSP, an error message is generated. If the <i>lsp-name</i> does exist and the LSP to IP address matches the SDP far-end IP address, the association is created.

metric

Syntax	metric <i>metric</i> no metric
Context	config>service>sdp
Description	This command specifies the metric to be used within the tunnel table manager for decision-making purposes. When multiple SDPs going to the same destination exist, this value is used as a tie-breaker by tunnel table manager users to select the route with the lower value.
Parameters	<i>metric</i> — specifies the SDP metric Values 1 to 17407

path-mtu

Syntax	path-mtu <i>bytes</i> no path-mtu
Context	config>service>sdp
Description	<p>This command configures the Maximum Transmission Unit (MTU) in bytes that the SDP can transmit to the far-end router without packet dropping.</p> <p>The default SDP-type path-mtu can be overridden on a per-SDP basis.</p> <p>Dynamic maintenance protocols on the SDP may override this setting.</p> <p>If the physical mtu on an egress interface indicates that the next hop on an SDP path cannot support the current path-mtu, the operational path-mtu on that SDP will be modified to a value that can be transmitted without fragmentation.</p> <p>The no form of this command removes any path-mtu defined on the SDP and the SDP will use the system default for the SDP type.</p>
Default	The default path-mtu defined on the system for the type of SDP is used.
Parameters	<i>bytes</i> — specifies the number of bytes in the path MTU Values 576 to 1554

signaling

Syntax	signaling {off tldp}
Context	config>service>sdp
Description	<p>This command specifies the signaling protocol used to obtain the ingress and egress labels in frames transmitted and received on the SDP. When signaling is off, then labels are manually configured when the SDP is bound to a service. The signaling value can only be changed while the administrative status of the SDP is down.</p> <p>The no form of this command is not applicable. To modify the signaling configuration, the SDP must be administratively shut down and then the signaling parameter can be modified and re-enabled.</p>
Default	tldp
Parameters	<p>off — ingress and egress signal auto-labeling is not enabled. If this parameter is selected, then each service using the specified SDP must manually configure VPN labels. This configuration is independent of the SDP's transport type, MPLS (LDP).</p> <p>tldp — ingress and egress signaling auto-labeling is enabled</p>

vlan-vc-etype

Syntax	vlan-vc-etype 0x0600..0xffff no vlan-vc-etype [0x0600..0xffff]
Context	config>service>sdp
Description	<p>This command configures the VLAN VC EtherType. The no form of this command returns the value to the default. The etype value populates the EtherType field in the Ethernet frame. It is used to indicate which protocol is being transported in the Ethernet frame. The default value indicates that the payload is an IEEE 802.1q-tagged frame.</p>
Default	no vlan-vc-etype (0x8100)
Parameters	<i>0x0600..0xffff</i> — specifies a valid VLAN etype identifier.

SDP Keepalive Commands

keep-alive

Syntax	keep-alive
Context	config>service>sdp
Description	This command is the context for configuring SDP connectivity monitoring keepalive messages for the SDP-ID.

SDP-ID keepalive messages use SDP Echo Request and Reply messages to monitor SDP connectivity. The operating state of the SDP is affected by the keepalive state on the SDP-ID. SDP Echo Request messages are only sent when the SDP-ID is completely configured and administratively up. If the SDP-ID is administratively down, keepalives for that SDP-ID are disabled. SDP Echo Requests, when sent for keepalive messages, are always sent with the *originator-sdp-id*. All SDP-ID keepalive SDP Echo Replies are sent using generic IP OAM encapsulation.

When a keepalive response is received that indicates an error condition, the SDP ID will immediately be brought operationally down. Once a response is received that indicates the error has cleared and the **hold-down-time** interval has expired, the SDP ID will be eligible to be put into the operationally up state. If no other condition prevents the operational change, the SDP ID will enter the operational state.

A set of event counters track the number of keepalive requests sent, the size of the message sent, non-error replies received and error replies received. A keepalive state value is kept, indicating the last response event. A keepalive state timestamp value is kept, indicating the time of the last event. With each keepalive event change, a log message is generated, indicating the event type and the timestamp value.

[Table 8](#) describes keepalive interpretation of SDP Echo Reply response conditions and the effect on the SDP ID operational status.

Table 8: SDP Echo Reply Response Conditions

Result of Request	Stored Response State	Operational State
keepalive request timeout without reply	Request Timeout	Down
keepalive request not sent due to non-existent <i>orig-sdp-id</i> ⁽¹⁾	Orig-SDP Non-Existent	Down
keepalive request not sent due to administratively down <i>orig-sdp-id</i>	Orig-SDP Admin-Down	Down
keepalive reply received, invalid origination-id	Far End: Originator-ID Invalid	Down

Table 8: SDP Echo Reply Response Conditions (Continued)

Result of Request	Stored Response State	Operational State
keepalive reply received, invalid responder-id	Far End: Responder-ID Error	Down
keepalive reply received, No Error	Success	Up (if no other condition prevents)

1. This condition should not occur.

hello-time

Syntax	hello-time <i>seconds</i> no hello-time				
Context	config>service>sdp>keep-alive				
Description	This command configures the time period between SDP keepalive messages on the SDP-ID for the SDP connectivity monitoring messages. The no form of this command reverts the hello-time <i>seconds</i> value to the default setting.				
Parameters	<i>seconds</i> — the time period in seconds between SDP keepalive messages, expressed as a decimal integer <table> <tr> <td>Default</td><td>10</td></tr> <tr> <td>Values</td><td>1 to 3600</td></tr> </table>	Default	10	Values	1 to 3600
Default	10				
Values	1 to 3600				

hold-down-time

Syntax	hold-down-time <i>seconds</i> no hold-down-time
Context	config>service>sdp>keep-alive
Description	This command configures the minimum time period the SDP will remain in the operationally down state in response to SDP keepalive monitoring. This parameter can be used to prevent the SDP operational state from “flapping” by rapidly transitioning between the operationally up and operationally down states based on keepalive messages. When an SDP keepalive response is received that indicates an error condition or the max-drop-count keepalive messages receive no reply, the <i>sdp-id</i> will immediately be brought operationally down. If a keepalive response is received that indicates the error has cleared, the <i>sdp-id</i> will be eligible to be put into the operationally up state only after the hold-down-time interval has expired.

The **no** form of this command reverts the **hold-down-time** *seconds* value to the default setting.

Parameters	<i>seconds</i> — the time in seconds, expressed as a decimal integer, the <i>sdp-id</i> will remain in the operationally down state after an SDP keepalive error before it is eligible to enter the operationally up state. A value of 0 indicates that no hold-down-time will be enforced for <i>sdp-id</i> .
Default	10
Values	0 to 3600

max-drop-count

Syntax	max-drop-count <i>count</i> no max-drop-count
Context	config>service>sdp>keep-alive
Description	<p>This command configures the number of consecutive SDP keepalive failed request attempts or remote replies that can be missed after which the SDP is operationally downed.</p> <p>If the max-drop-count consecutive keepalive request messages cannot be sent or no replies are received, the SDP-ID will be brought operationally down by the keepalive SDP monitoring.</p> <p>The no form of this command reverts the max-drop-count <i>count</i> value to the default settings.</p>
Parameters	<i>count</i> — the number of consecutive SDP keepalive requests that can fail to be sent or replies missed before the SDP is brought down, expressed as a decimal integer
Default	3
Values	1 to 5

message-length

Syntax	message-length <i>octets</i> no message-length
Context	config>service>sdp>keep-alive
Description	<p>This command configures the size of SDP monitoring keepalive request messages transmitted on the SDP.</p> <p>The no form of this command reverts the message-length <i>octets</i> value to the default setting.</p>
Parameters	<i>octets</i> — the size of keepalive request messages in octets, expressed as a decimal integer. The size keyword overrides the default keepalive message size.
	The message length should be equal to the SDP operating path MTU as configured in the path-mtu command.

If the default size is overridden, the actual size used will be the smaller of the operational SDP-ID path MTU and the size specified.

Default 0

Values 72 to 1500

timeout

Syntax **timeout** *timeout*
no timeout

Context config>service>sdp>keep-alive

Description This command configures the time interval that the SDP waits before tearing down the session.

Parameters *timeout* — the timeout in seconds, expressed as a decimal integer

Default 5

Values 1 to 10

Show Commands

customer

Syntax	customer <i>customer-id</i>
Context	show>service
Description	This command displays service customer information.
Parameters	<i>customer-id</i> — displays only information for the specified customer ID Default all customer IDs display Values 1 to 2147483647
Output	Show Customer Command Output — The following table describes show customer command output fields.

Table 9: Show Customer Command Output Fields

Label	Description
Customer-ID	Displays the unique customer identification number
Contact	Displays the name of the primary contact person
Description	Displays generic information about the customer
Phone	Displays the telephone or pager number used to reach the primary contact person
Total Customers	Displays the total number of customers configured

Sample Output

```
*A:ALU-12# show service customer
=====
Customers
=====
Customer-ID : 1
Contact : Manager
Description : Default customer
Phone : (123) 555-1212

Customer-ID : 2
Contact : Tech Support
Description : ABC Networks
Phone : (234) 555-1212

Customer-ID : 3
Contact : Fred
Description : ABC Networks
```

Phone : (345) 555-1212

Customer-ID : 6
 Contact : Ethel
 Description : Epipe Customer
 Phone : (456) 555-1212

Customer-ID : 7
 Contact : Lucy
 Description : VPLS Customer
 Phone : (567) 555-1212

Customer-ID : 8
 Contact : Customer Service
 Description : IES Customer
 Phone : (678) 555-1212

Customer-ID : 274
 Contact : Mssrs. Beaucoup
 Description : ABC Company
 Phone : 650 123-4567

Customer-ID : 94043
 Contact : Test Engineer on Duty
 Description : TEST Customer
 Phone : (789) 555-1212

 Total Customers : 8

*A:ALU-12#
 *A:ALU-12# show service customer 274

=====

Customer 274
 =====
 Customer-ID : 274
 Contact : Mssrs. Beaucoup
 Description : ABC Company
 Phone : 650 123-4567

 Total Customers : 1

*A:ALU-12#

sdp

Syntax	sdp [<i>sdp-id</i> far-end <i>ip-address</i>] [detail keep-alive-history]
Context	show>service
Description	This command displays SDP information. If no optional parameters are specified, a summary SDP output for all SDPs is displayed.
Parameters	<p><i>sdp-id</i> — the SDP ID for which to display information</p> <p>Default all SDPs</p> <p>Values 1 to 17407</p> <p>far-end <i>ip-address</i> — displays only SDPs matching with the specified far-end IP address</p> <p>Default SDPs with any far-end IP address</p> <p>detail — displays detailed SDP information</p> <p>Default SDP summary output</p> <p>keep-alive-history — displays the last fifty SDP keepalive events for the SDP</p> <p>Default SDP summary output</p>
Output	Show Service SDP — The following table describes show service SDP output fields.

Table 10: Show Service SDP Output Fields

Label	Description
SDP Id	Identifies the SDP
Description	Identifies the SDP by the text description stored its configuration file
SDP Source	Specifies the SDP source type
Adm MTU Adm Path MTU	Specifies the desired largest service frame size (in octets) that can be transmitted through this SDP to the far-end router
Opr MTU Opr Path MTU	Specifies the actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router
Far End	Specifies the IP address of the remote end of the GRE or MPLS tunnel defined by this SDP
Adm Admin State	Specifies the desired state of the SDP
Opr Oper State	Specifies the operating state of the SDP
Deliver Delivery	Specifies the type of delivery used by the SDP: GRE or MPLS

Table 10: Show Service SDP Output Fields (Continued)

Label	Description
Flags	Specifies all the conditions that affect the operating status of this SDP
Signal Signaling	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on the SDP
Metric	Specifies the value used as a tie-breaker by the tunnel table manager to select a route
Last Status Change	Specifies the time of the most recent operating status change to this SDP
Last Mgmt Change	Specifies the time of the most recent management-initiated change to this SDP
Adv. MTU Over	Specifies the state of the advertised VC-type MTU override command
VLAN VC Etype	Specifies the VLAN VC EtherType for the SDP
Number of SDPs	Specifies the total number of SDPs displayed according to the criteria specified
Keepalive Information:	
Hello Time	Specifies how often the SDP Echo Request messages are transmitted on this SDP
Hello Msg Len	Specifies the length of the SDP Echo Request messages transmitted on this SDP
Hello Timeout	Specifies the number of seconds to wait for an SDP echo response message before declaring a timeout
Unmatched Replies	Specifies the number of SDP unmatched message replies timer expired
Max Drop Count	Specifies the maximum number of consecutive SDP Echo Request messages that can be unacknowledged before the keepalive protocol reports a fault
Hold Down Time	Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state
TX Hello Msgs	Specifies the number of SDP echo request messages transmitted since the keepalive was administratively enabled or the counter was cleared
Rx Hello Msgs	Specifies the number of SDP echo request messages received since the keepalive was administratively enabled or the counter was cleared
Collect Stats.	Specifies that the collection of accounting and statistical data for the SDP is enabled or disabled

Table 10: Show Service SDP Output Fields (Continued)

Label	Description
Associated LSP LIST:	
Note: If the SDP type is GRE, the following message displays: SDP Delivery Mechanism is not MPLS	
Lsp Name	For MPLS: identifies the name of the static LSP
Time since Last Trans*	For MPLS: specifies the time that the associated static LSP has been in service

Sample Output

```
*A:ALU-12# show service sdp
```

```
=====
Services: Service Destination Points
=====
```

SdpId	Adm MTU	Opr MTU	IP address	Adm	Opr	Deliver	Signal
10	0	0	10.10.10.24	Up	Down	LDP	TLDP
20	0	0	10.10.10.24	Up	Down	MPLS	TLDP
30	4462	1514	10.20.1.21	Up	Up	GRE	TLDP

```
-----
Number of SDPs : 3
=====
```

```
*A:ALU-12#
```

```
*A:ALU-12# show service sdp 10
```

```
=====
Service Destination Point (Sdp Id : 10)
=====
```

SdpId	Adm MTU	Opr MTU	IP address	Adm	Opr	Deliver	Signal
10	0	0	10.10.10.24	Up	Down	LDP	TLDP

```
=====
*A:ALU-12#
```

```
*A:ALU-12# show service sdp 8 detail
```

```
=====
Service Destination Point (Sdp Id : 8) Details
=====
```

```
-----
Sdp Id 8 -(10.10.10.104)
=====
```

Description	: MPLS-10.10.10.104		
SDP Id	: 8	SDP-Source	: manual
Admin Path MTU	: 0	Oper Path MTU	: 1550
Far End	: 10.10.10.104	Delivery	: MPLS
Admin State	: Up	Oper State	: Down
Signaling	: TLDP	Metric	: 0
Last Status Change	: 02/01/2007 09:11:39	Adv. MTU Over.	: No


```

Last Mgmt Change      : 02/01/2007 09:11:46  VLAN VC Etype      : 0x8100
Flags                 : SignalingSessDown TransportTunnDown

KeepAlive Information :
Admin State           : Disabled              Oper State           : Disabled
Hello Time            : 10                   Hello Msg Len         : 0
Hello Timeout         : 5                   Unmatched Replies     : 0
Max Drop Count        : 3                   Hold Down Time        : 10
Tx Hello Msgs         : 0                   Rx Hello Msgs         : 0

Associated LSP LIST :
Lsp Name              : to-104
Admin State           : Up                   Oper State            : Down
Time Since Last Tran* : 01d07h36m
=====
* indicates that the corresponding row element may have been truncated.
*A:ALU-12#

```

sdp-using

- Syntax** `sdp-using [sdp-id[:vc-id] | far-end ip-address]`
- 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 to 17407
- vc-id* — the virtual circuit identifier
- Values** 1 to 4294967295
- far-end ip-address* — displays only services matching with the specified far-end IP address
- Default** services with any far-end IP address
- Output** **Show Service SDP Using** — The following table describes show service sdp-using output fields.

Table 11: Show Service sdp-using Output Fields

Label	Description
SvcID	Identifies the service
SdpID	Identifies the SDP
Type	Indicates the type of SDP (spoke)
Far End	Displays the far-end address of the SDP
Opr State	Displays the operational state of the service

Table 11: Show Service sdp-using Output Fields (Continued)

Label	Description
I. Label	Displays the ingress label used by the far-end device to send packets to this device in this service by this SDP
E. Label	Displays the egress label used by this device to send packets to the far-end device in this service by this SDP

Sample Output

```
*A:ALU-1# show service sdp-using 300
=====
Service Destination Point (Sdp Id : 300)
=====
```

SvcId	SdpId	Type	Far End	Opr State	I.Label	E.Label
1	300:1	Spok	10.0.0.13	Up	131071	131071
2	300:2	Spok	10.0.0.13	Up	131070	131070
100	300:100	Spok	10.0.0.13	Up	131069	131069
101	300:101	Spok	10.0.0.13	Up	131068	131068
102	300:102	Spok	10.0.0.13	Up	131067	131067

```
-----
Number of SDPs : 5
-----
=====
*A:ALU-1#
```

service-using

Syntax	service-using [epipe] [apipe] [cpipe] [sdp <i>sdp-id</i>] [customer <i>customer-id</i>]
Context	show>service
Description	<p>This command displays the services matching certain usage properties.</p> <p>If no optional parameters are specified, all services defined on the system are displayed.</p>
Parameters	<p>epipe — displays matching Epipe services</p> <p>apipe — displays matching Apipe services</p> <p>cpipe — displays matching Cpipe services</p> <p>sdp <i>sdp-id</i> — displays only services bound to the specified SDP ID</p> <p> Default services bound to any SDP ID</p> <p> Values 1 to 17407</p> <p>customer <i>customer-id</i> — displays services only associated with the specified customer ID</p> <p> Default services associated with a customer</p> <p> Values 1 to 2147483647</p>

Output **Show Service Service-Using** — The following table describes show service service-using output fields.

Table 12: Show Service service-using Output Fields

Label	Description
Service Id	Identifies the service
Type	Specifies the service type configured for the service ID
Adm	Displays the desired state of the service
Opr	Displays the operating state of the service
CustomerID	Displays the ID of the customer who owns this service
Last Mgmt Change	Displays the date and time of the most recent management-initiated change to this service

Sample Output all services used in system

Sample for service-using

=====

*A:ALU-12# show service service-using

=====

Services					
ServiceId	Type	Adm	Opr	CustomerId	Last Mgmt Change
1	Cpipe	Down	Down	1	10/10/2007 04:11:09
2	Apipe	Down	Down	1	10/10/2007 05:20:22
103	Epipe	Up	Up	104	10/10/2007 03:35:01
104	Epipe	Up	Up	104	10/10/2007 03:35:01
105	Epipe	Up	Up	104	10/10/2007 03:35:01
303	Cpipe	Up	Up	104	10/10/2007 03:35:01
304	Cpipe	Up	Up	104	10/10/2007 03:35:03
305	Cpipe	Up	Up	104	10/10/2007 03:35:06
701	Apipe	Up	Down	1	10/10/2007 03:35:10
702	Apipe	Up	Down	1	10/10/2007 03:35:10
703	Apipe	Up	Down	1	10/10/2007 03:35:10
704	Apipe	Up	Down	1	10/10/2007 03:35:10
705	Apipe	Up	Down	1	10/10/2007 03:35:10
706	Apipe	Up	Down	1	10/10/2007 03:35:10
806	Apipe	Up	Down	1	10/10/2007 03:35:10
807	Apipe	Up	Down	1	10/10/2007 03:35:11
808	Apipe	Up	Down	1	10/10/2007 03:35:11
903	Cpipe	Up	Up	1	10/10/2007 03:35:08
904	Cpipe	Up	Up	1	10/10/2007 03:35:08

=====

Matching Services : 19

Sample Output services used by customer

*A:ALU-12# show service service-using customer 1

```
=====
Services Customer 1
=====
ServiceId      Type      Adm      Opr      CustomerId      Last Mgmt Change
-----
1              Cpipe     Down     Down     1               10/10/2007 04:11:09
2              Apipe     Down     Down     1               10/10/2007 05:20:22
701            Apipe     Up       Down     1               10/10/2007 03:35:10
702            Apipe     Up       Down     1               10/10/2007 03:35:10
703            Apipe     Up       Down     1               10/10/2007 03:35:10
704            Apipe     Up       Down     1               10/10/2007 03:35:10
705            Apipe     Up       Down     1               10/10/2007 03:35:10
706            Apipe     Up       Down     1               10/10/2007 03:35:10
806            Apipe     Up       Down     1               10/10/2007 03:35:10
807            Apipe     Up       Down     1               10/10/2007 03:35:11
808            Apipe     Up       Down     1               10/10/2007 03:35:11
903            Cpipe     Up       Up       1               10/10/2007 03:35:08
904            Cpipe     Up       Up       1               10/10/2007 03:35:08
-----
Matching Services : 13
*A:ALU-12#
```

Sample Output by service type

*A:ALU-12# show service service-using epipe

```
=====
Services [epipe]
=====
ServiceId      Type      Adm      Opr      CustomerId      Last Mgmt Change
-----
103            Epipe     Up       Up       104             10/10/2007 03:35:01
104            Epipe     Up       Up       104             10/10/2007 03:35:01
105            Epipe     Up       Up       104             10/10/2007 03:35:01
-----
Matching Services : 3
*A:ALU-12#
```

VLL Services

In This Chapter

This chapter provides information about Virtual Leased Line (VLL) services and implementation notes.

Topics in this chapter include:

- [ATM VLL \(Apipe\) Services on page 94](#)
- [Circuit Emulation VLL \(Cpipe\) Services on page 97](#)
- [Ethernet VLL \(Epipe\) Services on page 114](#)
- [VLL Service Considerations on page 121](#)
- [Configuring a VLL Service with CLI on page 131](#)
- [VLL Services Command Reference on page 163](#)

ATM VLL (Apipe) Services

This section provides information about the Apipe service. Topics in this section include:

- [ATM VLL for End-to-End ATM Service](#)
- [ATM SAP-to-SAP Service](#)
- [ATM Traffic Management Support](#)
- [Control Word](#)

Apipe configuration information is found under the following topics:

- [List of Commands on page 132](#)
- [Common Configuration Tasks on page 140](#)
- [Configuring VLL Components on page 141](#)
 - [Creating an Apipe Service on page 141](#)
- [Service Management Tasks on page 157](#)

ATM VLL for End-to-End ATM Service

ATM VLLs (Apipe) provide a point-to-point ATM service between users connected to 7705 SAR nodes or other SR routers over an IP/MPLS network (see [Figure 12](#)). User ATM traffic is connected to a 7705 SAR either directly or through an ATM access network. In both cases, an ATM PVC—for example, a virtual channel (VC) or a virtual path (VP)—is configured on the 7705 SAR. VPI/VCI translation is supported in the ATM VLL.

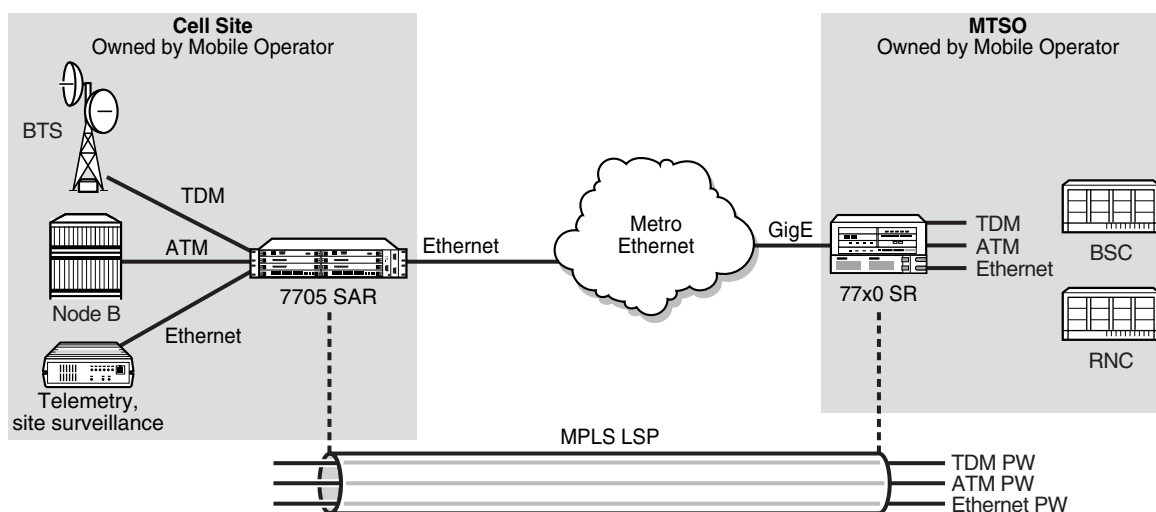
The 7705 SAR receives standard UNI/NNI cells on the ATM service access point (SAP), which are then encapsulated into a pseudowire packet using N-to-1 cell mode encapsulation in accordance with RFC 4717.

The ATM pseudowire (PW) is initiated using targeted LDP signaling as specified in RFC 4447, *Pseudowire Setup and Maintenance using LDP*; alternatively, it can be configured manually. The 7705 SAR supports MPLS and GRE as the tunneling technologies for transporting ATM PWs.

In addition to supporting N-to-1 cell mode encapsulation, ATM VLL service supports cell concatenation, control word (CW), SAP-to-SAP (local service), and SAP-to-SDP binding (distributed service). See [SAP Encapsulations and Pseudowire Types on page 122](#) for more information on N-to-1 cell mode encapsulation.

ATM VLL optimizes the ATM cell from a 53-byte cell to a 52-byte packet by removing the header error control (HEC) byte at the near end. The far end regenerates the HEC before switching ATM traffic to the attached circuit.

Figure 12: ATM VLL for End-to-End ATM Service



19482

ATM SAP-to-SAP Service

ATM VLLs can be configured with both endpoints (SAPs) on the same 7705 SAR. This is referred to as ATM SAP-to-SAP or local ATM service. ATM SAP-to-SAP emulates local ATM switching between two ATM endpoints on the 7705 SAR. Both ingress and egress traffic is legacy ATM traffic.

An ATM SAP-to-SAP connection is set up in the 7705 SAR and a pseudowire is configured between the two endpoints. One endpoint of the SAP connection can be an IMA group, while the other endpoint can be an unbundled port.



Note: ATM SAP-to-SAP connections are supported between any T1/E1 ASAP port that is in access mode with ATM/IMA encapsulation and another port with the same configuration. One endpoint of a SAP connection can be an IMA group, while the other endpoint can be on a single ATM port.

ATM Traffic Management Support

The 7705 SAR supports the ATM Forum Traffic Management Specification Version 4.1.

Network Ingress Classification

Classification is based on the EXP value of the pseudowire label and EXP-to-FC mapping is determined by the network ingress QoS policy.

The ingress MPLS packets are mapped to forwarding classes based on EXP bits that are part of the headers in the MPLS packets. The EXP bits are used to ensure an end-to-end QoS application. For PW services, there are two labels: one for the MPLS tunnel and one for the pseudowire itself. Mapping is done according to the outer tunnel EXP bit settings. This ensures that if the EXP bit settings are altered along the path by the intermediate LSR nodes, the newly requested FC selection is carried out properly.

Ingress GRE packets are mapped to forwarding classes based on DSCP bit settings of the IP header.

ATM Access Egress Queuing and Shaping

The 7705 SAR provides a per-SAP queuing architecture on the T1/E1 ASAP Adapter card. After the ATM pseudowire is terminated at the access egress point, all the ATM cells are mapped to default queue 1, and queuing is performed on a per-SAP basis.

Access ingress and access egress traffic management features are identical for SAP-to-SAP and SAP-to-SDP applications. For more information on ATM access egress queuing and scheduling, refer to the 7705 SAR OS Quality of Service Guide.

Control Word

ATM VLL supports an optional control word (CW). Refer to [Pseudowire Control Word on page 130](#) for more information.

Circuit Emulation VLL (Cpipe) Services

This section provides information about the Cpipe service.

Topics in this section include:

- [Cpipe Service Overview](#)
 - [TDM SAP-to-SAP Service](#)
 - [Cpipe Service Modes](#)
 - [TDM PW Encapsulation](#)
 - [Circuit Emulation Parameters and Options](#)
 - [Error Situations](#)

Cpipe configuration information is found under the following topics:

- [List of Commands on page 132](#)
- [Common Configuration Tasks on page 140](#)
- [Configuring VLL Components on page 141](#)
 - [Creating a Cpipe Service on page 146](#)
- [Service Management Tasks on page 157](#)

Cpipe Service Overview

Cpipe service is the Alcatel-Lucent implementation of TDM PW VLL as defined in the IETF PWE3 working group.

The 7705 SAR can support TDM circuit applications that are able to transport delay-sensitive TDM traffic over a packet network. For example, in the case of cell site aggregation, Cpipe services provide transport service for 2G connectivity between the base transceiver station and the base station controller, and for 3G backhaul applications (for example, EVDO traffic from T1/E1 ports with MLPPP). In Release 1.1, Cpipe services over MPLS or GRE tunnels are supported.

The 2G traffic is transported encapsulated in a TDM VLL over the packet switched network (PSN). The entire T1/E1 frame or part of a frame ($n \times 64$ kb/s) is carried as a TDM VLL over the PSN. At the far end, the transport layer frame structure is regenerated when structured circuit emulation is used, or simply forwarded as part of the payload when unstructured circuit emulation is used. The 3G UMTS R99 traffic uses ATM/IMA as the transport protocol. The IMA sessions are terminated at the site by the 7705 SAR and the 3G ATM traffic is transported across the PSN through the use of ATM VLLs (PWE3).

TDM SAP-to-SAP Service

TDM VLLs can be configured with both endpoints (SAPs) on the same 7705 SAR. This is referred to as TDM SAP-to-SAP or local TDM service. TDM SAP-to-SAP emulates a TDM multiplexing and switching function on the 7705 SAR.

A TDM SAP-to-SAP connection is set up in the 7705 SAR and a pseudowire is configured between the two endpoints.



Note: TDM SAP-to-SAP connections are supported between any T1/E1 ASAP port or channel that is configured for access mode and circuit emulation service and another port or channel with the same configuration.

Cpipe Service Modes

Cpipe services support unstructured circuit emulation mode (SAToP) as per RFC 4553 and structured circuit emulation mode (CESoPSN) for DS1, E1 and $n \times 64$ kb/s circuits as per RFC 5086.

Unstructured Mode (SAToP)

Structure-agnostic TDM over Packet (SAToP) is an unstructured circuit emulation mode used for the transport of unstructured TDM or structured TDM (where the structure is ignored).



Note: The word “agnostic” is used in RFC 4553, but it is not used in the literal sense. The meaning of agnostic in this case is “unaware or independent”; therefore, structure-agnostic is used to mean structure-unaware or structure-independent.

As a structure-unaware or structure-independent service, SAToP service does not align to any framing; the framing mode for the port is set to unframed. For structured TDM, SAToP disregards the bit sequence and TDM structure in order to transport the entire signal over a PSN as a pseudowire.

Structured Mode (CESoPSN)

Structure-aware circuit emulation is used for the transport of structured TDM, taking at least some level of the structure into account. By selecting only the necessary $n \times 64$ kb/s timeslots to transport, bandwidth utilization is reduced or optimized (compared to a full DS1 or E1). Full DS1s or E1s can be transported by selecting all the timeslots in the DS1 or E1 circuit. Framing bits (DS1) or FAS (E1) are terminated at the near end and reproduced at the far end.

The 7705 SAR supports CESoPSN without CAS for DS1 and E1, and CESoPSN with CAS for E1.

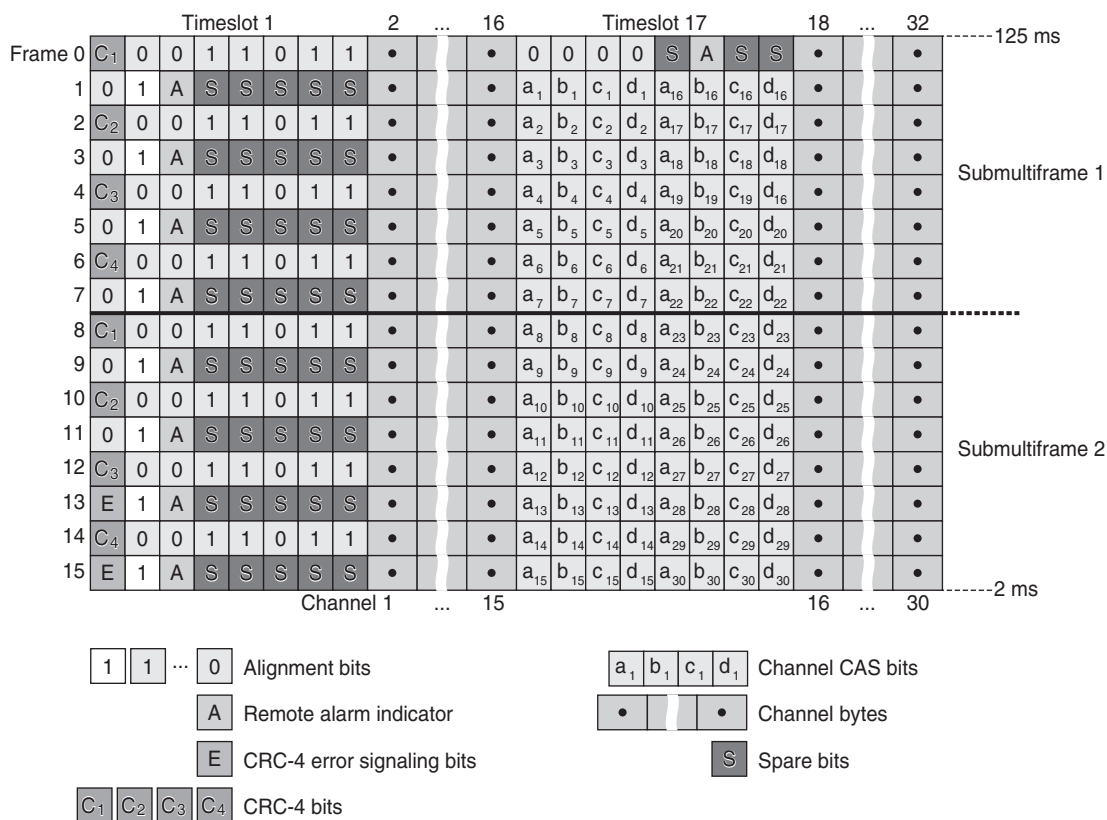
Channel Associated Signaling (CAS) includes four signaling bits (A, B, C, and D) in the messages sent over a voice trunk. These messages provide information such as the dialed digits and the call state (whether on-hook or off-hook).

The mechanism for E1 CAS is described in ITU-T G.732. When the vc-type is configured for E1 CAS, timeslot 17 carries the signaling information for the timeslots used for voice trunking. Each channel requires four signaling bits, so grouping 16 E1 frames into a multiframe allows the signaling bits for all 30 channels to be trunked.

As shown in [Figure 13](#), timeslot 1 of all frames within the E1 multiframe is reserved for alignment, alarm indication, and CRC. For Frame 0, timeslot 17 is reserved for multiframe alignment bits. For the remaining 15 frames, timeslot 17 contains ABCD bits for two channels.



Note: For E1 CAS, timeslots are numbered 1 to 32 on the 7705 SAR.

Figure 13: E1 Framing for CAS Support in a Multiframe

19966

When CESoPSN with CAS is selected, the ABCD bits are coded into the E1 multiframe, transported within the TDM PW, and reconstructed in the E1 multiframe at the far end for each timeslot.

TDM PW Encapsulation

TDM circuits are MPLS-encapsulated as per RFC 4533 (SAToP) and RFC 5086 (CESoPSN) (see [Figure 14](#) and [Figure 15](#)).

Figure 14: SAToP MPLS Encapsulation

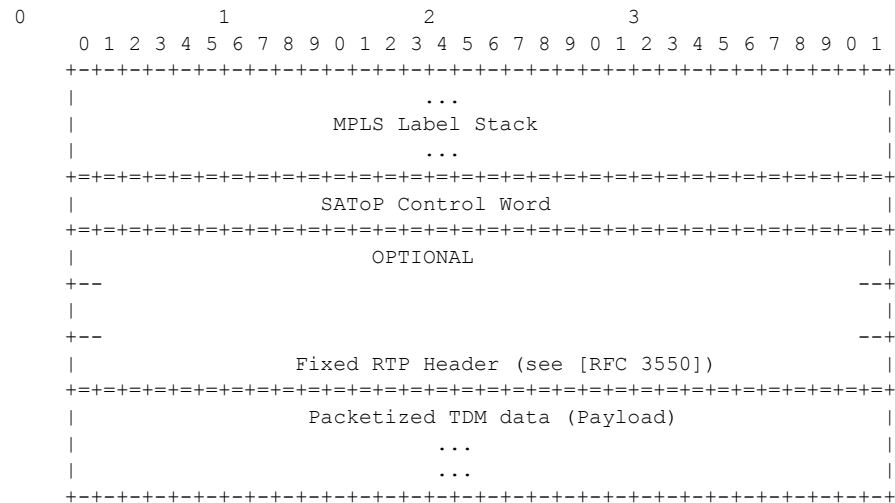


Figure 15: CESoPSN MPLS Encapsulation

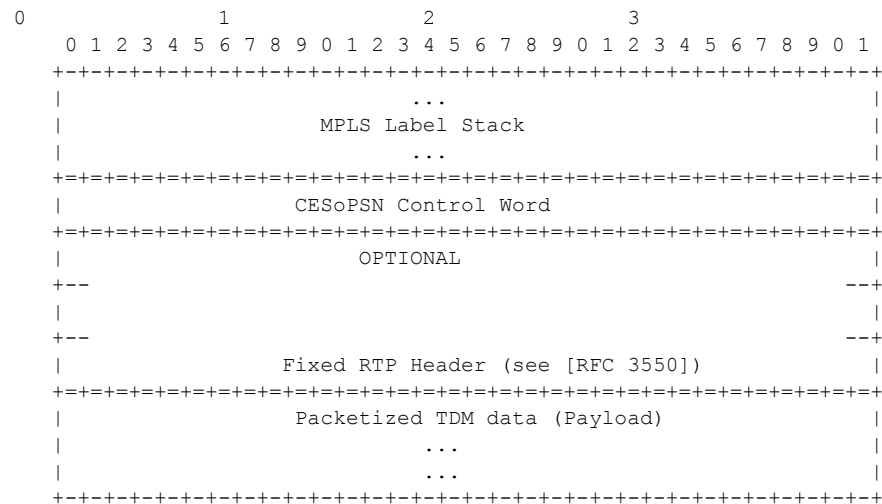
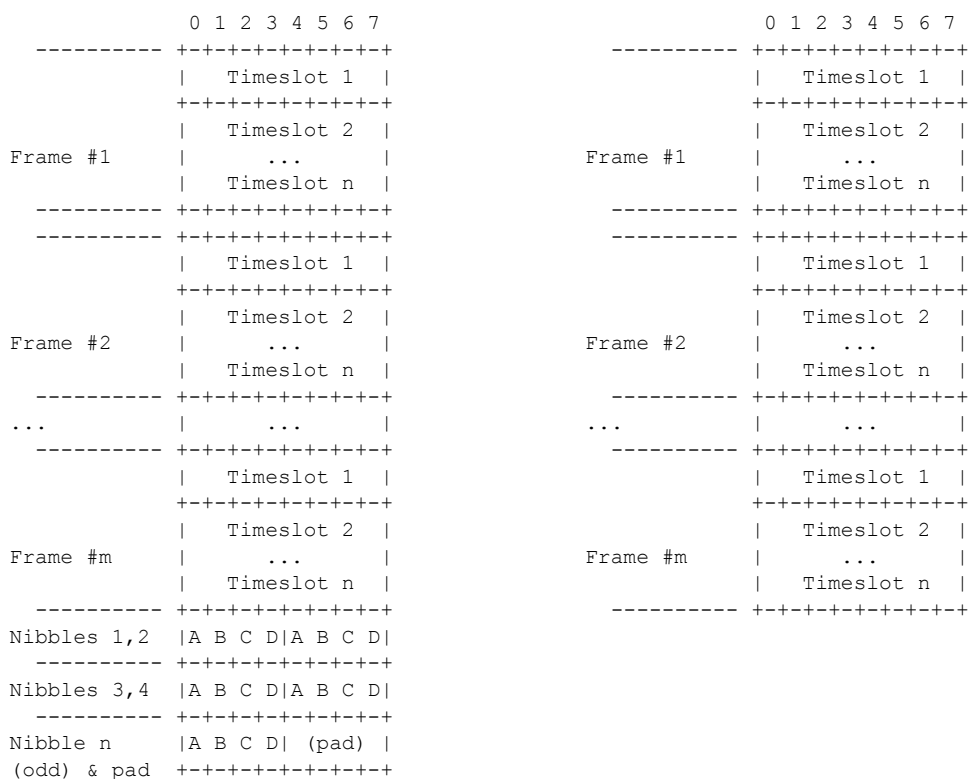


Figure 16 shows the format of the CESoPSN TDM payload (with and without CAS) for packets carrying trunk-specific $n \times 64$ kb/s service.

Figure 16: CESoPSN Packet Payload Format for Trunk-Specific $n \times 64$ kb/s (with and without CAS transport)



(a) Packet with CAS

(b) Packet without CAS

For CESoPSN without CAS, select the packet size so that an integer number of frames are transported. That is, if n timeslots per frame are to be encapsulated in a TDM PW, then the packet size must be a multiple of n (where n is not equal to 1). For example, if $n = 4$ timeslots, then the packet size can be 8, 12, 16 and so on.

For CESoPSN with CAS, the packet size is an integer number of frames, where the number of frames is a multiple of 16 for E1 and is not user-configurable. The extra bytes for ABCD (CAS) signaling bits are not included when setting the packet size.



Note: The extra bytes for CAS signaling bits must be included when setting the service-mtu size. See [Structured E1 CES with CAS on page 107](#) for more information.

Circuit Emulation Parameters and Options

All ports on a 16-port T1/E1 ASAP Adapter card can be configured independently to support TDM circuit emulation across the packet network. Structure-aware mode (CESoPSN) is supported for $n \times 64$ kb/s channel groups in DS1 and E1 circuits. Unstructured mode (SAToP) is supported for full DS1 and E1 circuits. The following parameters and options are described in this section:

- [Unstructured](#)
- [Structured DS1/E1 CES without CAS](#)
- [Structured E1 CES with CAS](#)
- [Packet Payload Size](#)
- [Jitter Buffer](#)
- [RTP Header](#)
- [Control Word](#)

Unstructured

Unstructured CES is configured by choosing `satop-t1` or `satop-e1` as the `vc-type` when creating a Cpipe service. For DS1 and E1 unstructured circuit emulation, the framing parameter of the port must be set to `ds1-unframed` and `e1-unframed` (respectively) because SAToP service ignores the underlying framing. Additionally, channel group 1 must contain all 24 or 32 timeslots, which is configured automatically when channel group 1 is created.

For DS1 and E1 circuit emulation, the payload packet size is configurable and must be an integer value between 2 and 1514 octets. The payload packet size affects the packet efficiency and packetization delay. [Table 13](#) shows the default values for packet size and packetization delay. See [Packet Payload Size on page 110](#) for more information.



Note: When using SAToP to transport DS1 traffic, the framing bit (bit 193) in the DS1 overhead is included and packed in the payload and sent over the PSN. If the underlying framing is ESF, then the Facility Data Link (FDL) channel is transported over the Cpipe as part of the SAToP service. No matter the case, the framing parameter of the port must be set to unframed.

Table 13: Unstructured Payload Defaults

Circuit	Payload Size (Octets)	Packetization Delay (ms)
DS1	192	1.00
E1	256	1.00

Structured DS1/E1 CES without CAS

Structured CES without CAS is configured by choosing `cesopsn` as the `vc-type` when creating a Cpipe service. For $n \times 64$ kb/s structured circuit emulation operation, the framing parameter of the port must be set to a framed setting (such as ESF for DS1). Each channel group contains n DS0s (timeslots), where n is between 1 and 24 timeslots for DS1 and between 1 and 31 timeslots for E1.

The packet payload size is configurable (in octets) and must be an integer multiple of the number of timeslots in the channel group. The minimum payload packet size is 2 octets (based on two frames per packet and one timeslot per frame). See [Table 14](#) for default and minimum payload size values. The maximum payload packet size is 1514 octets.

Each DS1 or E1 frame contributes a number of octets to the packet payload. That number is equal to the number of timeslots configured in the channel group. Thus, a channel group with four timeslots contributes 4 octets to the payload. The timeslots do not need to be contiguous.

Note that a smaller packet size results in a lower packetization delay; however, it increases the packet overhead (when expressed as a percentage of the traffic).

Calculation of Payload Size

The payload size (S), in octets, can be calculated using the following formula:

$$S = N \times F$$

where:

N = the number of octets (timeslots) collected per received frame (DS1 or E1)

F = the number of received frames (DS1 or E1) that are accumulated in each CESoPSN packet

For example, assume the packet collects 16 frames (F) and the channel group contains 4 octets (timeslots) (N). Then the packet payload size (S) is:

$$\begin{aligned} S &= 4 \text{ octets/frame} \times 16 \text{ frames} \\ &= 64 \text{ octets} \end{aligned}$$

Calculation of Packetization Delay

Packetization delay is the time needed to collect the payload for a CESoPSN packet. DS1 and E1 frames arrive at a rate of 8000 frames per second. Therefore, the received frame arrival period is 125 μ s.

In the previous example, 16 frames were accumulated in the CESoPSN packet. In this case, the packetization delay (D) can be calculated as follows:

$$\begin{aligned} D &= 125 \mu\text{s/frame} \times 16 \text{ frames} \\ &= 2.000 \text{ ms} \end{aligned}$$

Table 14 shows the default and minimum values for frames per packet, payload size, and packetization delay as they apply to the number of timeslots (N) that contribute to the packet payload. The default values are set by the operating system as follows:

- for $N = 1$, the default is 64 frames/packet
- for $2 \leq N \leq 4$, the default is 32 frames/packet
- for $5 \leq N \leq 15$, the default is 16 frames/packet
- for $N \geq 16$, the default is 8 frames/packet

Table 14: Default and Minimum Payload Size for CESoPSN without CAS

Number of Timeslots (N)	Default Values			Minimum Values		
	Frames per Packet (F)	Payload Size (Octets) (S)	Packetization Delay (ms) (D)	Frames per Packet (F)	Payload Size (Octets) (S)	Packetization Delay (ms) (D)
1	64	64	8.000	2	2	0.250
2	32	64	4.000	2	4	0.250
3	32	96	4.000	2	6	0.250
4	32	128	4.000	2	8	0.250
5	16	80	2.000	2	10	0.250
6	16	96	2.000	2	12	0.250
7	16	112	2.000	2	14	0.250
8	16	128	2.000	2	16	0.250
9	16	144	2.000	2	18	0.250
10	16	160	2.000	2	20	0.250
11	16	176	2.000	2	22	0.250
12	16	192	2.000	2	24	0.250
13	16	208	2.000	2	26	0.250
14	16	224	2.000	2	28	0.250
15	16	240	2.000	2	30	0.250
16	8	128	1.000	2	32	0.250
17	8	136	1.000	2	34	0.250
18	8	144	1.000	2	36	0.250
19	8	152	1.000	2	38	0.250
20	8	160	1.000	2	40	0.250
21	8	168	1.000	2	42	0.250
22	8	176	1.000	2	44	0.250
23	8	184	1.000	2	46	0.250

Table 14: Default and Minimum Payload Size for CESoPSN without CAS (Continued)

Number of Timeslots (N)	Default Values			Minimum Values		
	Frames per Packet (F)	Payload Size (Octets) (S)	Packetization Delay (ms) (D)	Frames per Packet (F)	Payload Size (Octets) (S)	Packetization Delay (ms) (D)
24	8	192	1.000	2	48	0.250
25	8	200	1.000	2	50	0.250
26	8	208	1.000	2	52	0.250
27	8	216	1.000	2	54	0.250
28	8	224	1.000	2	56	0.250
29	8	232	1.000	2	58	0.250
30	8	240	1.000	2	60	0.250
31	8	248	1.000	2	62	0.250

Structured E1 CES with CAS

In Release 1.1, structured circuit emulation with CAS is only supported for E1 circuits.

Structured CES with CAS service is configured by choosing `cesopsn-cas` as the `vc-type` when creating a Cpipe service. The E1 service on the port associated with the Cpipe SAP should be configured to support CAS (via the `signal-mode {cas}` command) before configuring the Cpipe service to support E1 with CAS. Refer to the 7705 SAR OS Interface Configuration Guide for information on configuring signal mode.

For $n \times 64$ kb/s structured circuit emulation with CAS, the implementation is almost identical to that of CES without CAS. When CAS operation is enabled, timeslot 16 cannot be included in the channel group on E1 carriers. The CAS option is enabled or disabled at the port level; therefore, it applies to all channel groups on that E1 port.

The packet size is based on 16 frames per packet for E1 when CAS is enabled and is not user-configurable. For example, if the number of timeslots is 4, then the payload size is 64 octets. This 16-frame fixed configuration is logical because an E1 multiframe contains 16 frames; therefore, proper bit positioning for the A, B, C, and D CAS signaling bits can be ensured at each end of the pseudowire. [Table 15](#) shows the payload sizes based on the number of timeslots.

For CAS, the signaling portion adds $(n/2)$ bytes (n is an even integer) or $((n+1)/2)$ bytes (n is odd) to the packet, where n is the number of timeslots in the channel group. Note that you do not include the additional signaling bytes in the configuration setting of the TDM payload size. However, the operating system includes the additional bytes in the total packet payload, and the total payload must be accounted for when setting the service-mtu size. Continuing the example above, since $n = 4$, the total payload is 64 octets plus $(4/2 = 2)$ CAS octets, or 66 octets. Refer to [Figure 16](#) to see the structure of the CES with CAS payload.



Note: If you configure the service-mtu size to be smaller than the total payload size (payload plus CAS bytes), then the Cpipe will not become operational. This must be considered if you change the service-mtu from its default value.

CES fragmentation is not supported.

Table 15: Payload Size for E1 CESoPSN with CAS

Number of Timeslots	Number of Frames per Packet	Payload Size (Octets)	Packetization Delay (ms)
1	16	16	2.00
2	16	32	2.00
3	16	48	2.00
4	16	64	2.00
5	16	80	2.00
6	16	96	2.00
7	16	112	2.00
8	16	128	2.00
9	16	144	2.00
10	16	160	2.00
11	16	176	2.00
12	16	192	2.00
13	16	208	2.00
14	16	224	2.00
15	16	240	2.00
16	16	256	2.00
17	16	272	2.00

Table 15: Payload Size for E1 CESoPSN with CAS (Continued)

Number of Timeslots	Number of Frames per Packet	Payload Size (Octets)	Packetization Delay (ms)
18	16	288	2.00
19	16	304	2.00
20	16	320	2.00
21	16	336	2.00
22	16	352	2.00
23	16	368	2.00
24	16	384	2.00
25	16	400	2.00
26	16	416	2.00
27	16	432	2.00
28	16	448	2.00
29	16	464	2.00
30	16	480	2.00

Packet Payload Size

The packet payload size defines the number of octets contained in the payload of a TDM PW packet when the packet is transmitted. Each DS0 (timeslot) in a DS1 or E1 frame contributes 1 octet to the payload, and the total number of octets contributed per frame depends on the number of timeslots in the channel group (for example, 10 timeslots contribute 10 octets per frame).

Jitter Buffer

A circuit emulation service uses a jitter buffer to ensure that received packets are tolerant to packet delay variation (PDV). The selection of jitter buffer size must take into account the size of the TDM-encapsulated packets (payload size). A properly configured jitter buffer provides continuous play-out, thereby avoiding discards due to overruns and underruns (packets arriving too early or too late). The maximum receive jitter buffer size is configurable for each SAP configured for circuit emulation. The range of values is from 3 to 250 ms in increments of 1 ms.

Configuration/design Considerations

Determining the best configuration value for the jitter buffer may require some adjustments to account for the requirements of your network, which can change PDV as nodes are added or removed.

The buffer size must be set to at least 3 times the packetization delay and no greater than 32 times the packetization delay. Use a buffer size (in ms) that is equal to or greater than the peak-to-peak packet delay variation (PDV) expected in the network used by circuit emulation service. For example, for a PDV of ± 5 ms, configure the jitter buffer to be at least 10 ms.



Note: The jitter buffer setting and payload size (packetization delay) interact such that it may be necessary for the operating system to adjust the jitter buffer setting in order to ensure no loss of packets. Thus, the configured jitter buffer value may not be the value used by the system. Use the `show>service>id service_id>all` command to show the effective PDVT (packet delay variation tolerance).

The following values are the default jitter buffer times for structured circuits, where N is the number of timeslots:

- for $N = 1$, the default is 32 ms
- for $2 \leq N \leq 4$, the default is 16 ms
- for $5 \leq N \leq 15$, the default is 8 ms
- for $N \geq 16$, the default is 5 ms

Jitter buffer overrun and underrun counters are available for statistics and can raise an alarm (optional) while the circuit is operational. For overruns, excess packets are discarded and counted. For underruns, an all-ones pattern is sent for unstructured circuits and an all-ones or a user-defined pattern is sent for structured circuits (based on configuration).

The circuit status and statistics can be displayed using the `show` command.

RTP Header

For all circuit emulation channels, the RTP in the header is optional (as per RFC 5086). When enabled for absolute mode operation, an RTP header is inserted in the MPLS frame upon transmit. Absolute mode is defined in RFC 5086 and means that the ingress PE will set timestamps using the clock recovered from the incoming TDM circuit. When an MPLS frame is received, the RTP header is ignored. The RTP header mode is for TDM PW interoperability purposes only and should be enabled when the other device requires an RTP header.

Control Word

The structure of the control word is mandatory for SAToP and CESoPSN and is shown in [Figure 17](#). [Table 16](#) describes the bit fields. Refer to [Pseudowire Control Word on page 130](#) for more information.

Figure 17: Control Word Bit Structure

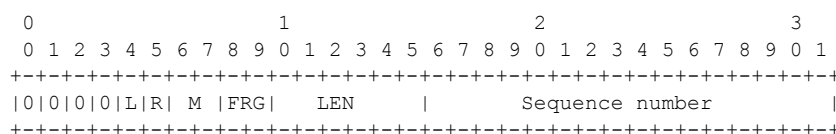


Table 16: Control Word Bit Descriptions

Bit(s)	Description
Bits 0 to 3	The use of bits 0 to 3 is described in RFC 4385. These bits are set to 0 unless they are being used to indicate the start of an Associated Channel Header (ACH) for the purposes of VCCV.
L (Local TDM Failure)	The L bit is set to 1 if an abnormal condition of the attachment circuit such as LOS, LOF, or AIS has been detected and the TDM data carried in the payload is invalid. The L bit is cleared (set back to 0) when fault is rectified.
R (Remote Loss of Frames indication)	The R bit is set to 1 if the local CE-bound interworking function (IWF) is in the packet loss state and cleared (reset to 0) after the local CE-bound IWF is no longer in the packet loss state.
M (Modifier)	<p>The M bits are a 2-bit modifier field. For SAToP, M is set to 00 as per RFC 4553. For CESoPSN, M is set according to RFC 5086, summarized as follows:</p> <ul style="list-style-type: none"> When L bit = 0, and <ul style="list-style-type: none"> M = 00 – Normal conditions M = 01 – Reserved for future use M = 10 – RDI condition for the attachment circuit (AC) M = 11 – Reserved for CESoPSN When L bit = 1, and <ul style="list-style-type: none"> M = 00 – TDM data is invalid M = 01 – Reserved for future use M = 10 – Reserved for future use M = 11 – Reserved for future use
FRG	The FRG bits in the CESoPSN control word are set to 00.
LEN	The LEN bits (bits 10 to 15) carry the length of the CESoPSN packet (defined as the size of the CESoPSN header plus the payload size) if it is less than 64 bytes, and set to 0 otherwise.
Sequence number	The sequence number is used to provide the common PW sequencing function as well as detection of lost packets.

Error Situations

The CE-bound interworking function (IWF) uses the sequence numbers in the control word to detect lost and incorrectly ordered packets. Incorrectly ordered packets that cannot be reordered are discarded.

For unstructured CES, the payload of received packets with the L bit set is replaced with an all-ones pattern. For structured CES, the payload of received packets with the L bit set is replaced with an all-ones or a user-configurable bit pattern. This is configured using the `idle-payload-fill` command. For structured CES with CAS (E1 only in Release 1.1), the signaling bits are replaced with an all-ones or a user-configurable bit pattern. This is configured using the `idle-signal-fill` command. Refer to the 7705 SAR OS Interface Configuration Guide for more information.

All circuit emulation services can have a status of up, loss of packets (LOP) or admin down, and any jitter buffer overruns or underruns are logged.

Ethernet VLL (Epipe) Services

This section provides information about the Epipe service.

Topics in this section include:

- [Epipe Service Overview](#)
 - [Ethernet Access Egress Queuing and Scheduling](#)
 - [Control Word](#)
 - [MTU](#)
 - [Raw and Tagged Modes](#)

Epipe configuration information is found under the following topics:

- [List of Commands on page 132](#)
- [Common Configuration Tasks on page 140](#)
- [Configuring VLL Components on page 141](#)
 - [Creating an Epipe Service on page 150](#)
- [Service Management Tasks on page 157](#)

Epipe Service Overview

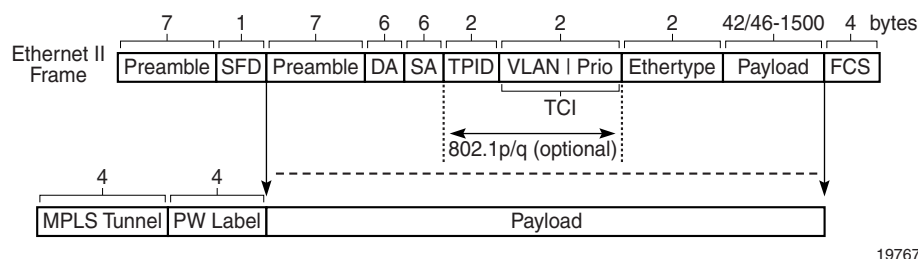
An Ethernet pseudowire (PW) is used to carry Ethernet/802.3 protocol data units (PDUs) over an MPLS or IP network, allowing service providers to offer emulated Ethernet services over existing MPLS or IP networks. For the 7705 SAR, Ethernet emulation is a point-to-point service.

The 7705 SAR uses Ethernet VLLs to carry Ethernet traffic from various sources at a site, including traffic such as e911 locators, power supply probes, and HSPA-dedicated interfaces. Native Ethernet bridging is not supported.

An MPLS Epipe service is the Alcatel-Lucent implementation of an Ethernet VLL based on the IETF RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*.

Figure 18 shows a typical Ethernet VLL frame together with its MPLS tunnel encapsulation:

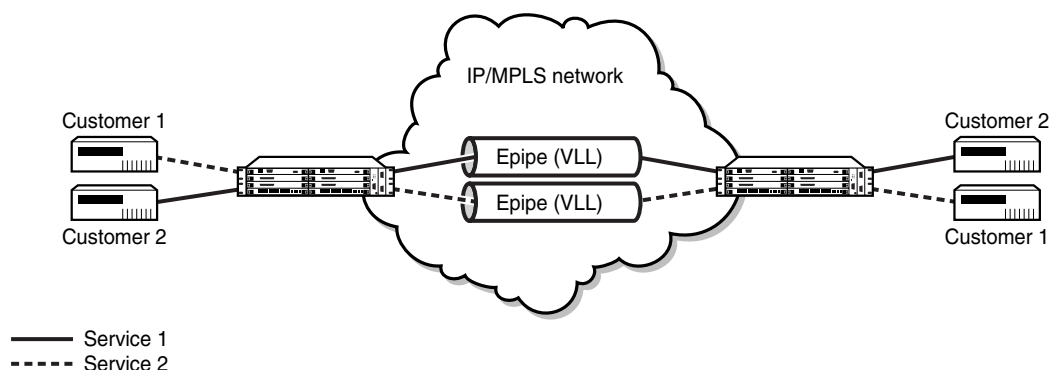
Figure 18: Ethernet VLL Frame with MPLS Encapsulation



An Epipe service is a Layer 2 point-to-point service where the customer data is encapsulated and transported across a service provider's MPLS or IP network. An Epipe service is completely transparent to the subscriber's data and protocols. Like other PW VLL services, Epipe service behaves like a non-learning Ethernet bridge. A distributed Epipe service consists of a SAP and an SDP pair, where one SDP is on same router as the SAP, and the second SDP is on the far-end router.

Each SAP configuration includes a specific port on which service traffic enters the 7705 SAR from the customer side (also called the access side). Each port is configured with an encapsulation type (SAP encapsulation). Thus, a whole Ethernet port can be bound to a single service (that is, the whole Ethernet port is configured as an SAP), or if a port is configured for IEEE 802.1Q encapsulation (referred to as dot1q), then a unique encapsulation value (ID) must be specified.

Figure 19: Epipe Service



Ethernet Access Egress Queuing and Scheduling

Ethernet access egress queuing and scheduling is very similar to the Ethernet access ingress behavior. Once the Ethernet pseudowire is terminated, traffic is mapped to up to eight different forwarding classes per SAP. Mapping traffic to different forwarding classes is performed based on the EXP bit settings of the received Ethernet pseudowire.

For more information on Ethernet access egress queuing and scheduling, refer to the 7705 SAR OS Quality of Service Guide.

Control Word

Ethernet VLL supports an optional control word (CW). Refer to [Pseudowire Control Word on page 130](#) for more information.

MTU

The largest maximum transmission unit (MTU) supported on an Ethernet port is 1572 bytes. The default MTU for a Gigabit Ethernet port is 1572 bytes; whereas, the default MTU for a 10/100 Ethernet port is 1514 or 1518 bytes, depending on the encapsulation type setting (null or dot1q).

Network-facing Ethernet ports must support a larger MTU than access-facing Ethernet ports in order to account for the pseudowire headers that are added to the access Ethernet frames.

The following list gives the worst-case MTU sizes for Ethernet VLLs over Ethernet port(s) under various configurations, where the worst case is the largest MTU size required in order to carry the payload:

- Access, null mode: 1514 bytes (1500 bytes payload)
- Access, dot1q mode: 1518 bytes (1500 bytes payload)
- Network, null mode: 1572 bytes (1514 bytes payload)
- Network, dot1q mode: 1572 bytes (1518 bytes payload)



Note: Since it is not practical to split a Layer 2 Ethernet frame into smaller frames, the access port (SAP) MTU must be smaller than the service and network port MTU. If the access port MTU is larger than the tunnel MTU, the Ethernet VLL does not come into service and remains in the inoperative state. See [MTU Settings on page 126](#) for information on MTU for VLL service.

Raw and Tagged Modes

An Ethernet PW operates in one of two modes: raw or tagged. Raw and tagged modes relate to the way the router handles VLAN tags embedded in the header of an Ethernet frame. Both modes are supported by the 7705 SAR.

Raw and tagged modes are configured using the `vc-type {ether|vlan}` parameter under the `spoke-sdp` command. To configure raw mode, choose the `ether` option; to configure tagged mode, choose `vlan`.

VLAN tags can provide service-affecting information about a frame. Service-affecting means that information in the tag affects the forwarding decisions that are made to route the packet. The port connected to the attachment circuit (AC) can be configured for `null` or `dot1q` operation. When the port is configured for `null`, the 7705 SAR treats any attached tag received at the SAP (from the AC) as not service affecting; when configured for `dot1q`, received tags are service affecting.

Raw Mode

In raw mode, VLAN tags are not service affecting (that is, the port is set to `null` and the tags do not affect frame forwarding decisions) and are forwarded over the Epipe as part of the payload.

If a service-affecting tag arrives from the ingress AC (that is, the port is set to `dot1q` and a tag is received), the tag is removed (popped) from the payload before the Ethernet frame gets switched over the PSN via the Epipe.

In raw mode, all traffic from the ingress port gets switched to the same endpoint. However, if the MTU (or configured size) of the tunnel is exceeded then service is affected because the frame is dropped.

In raw mode, when the 7705 SAR detects a failure on the Ethernet ingress port or the port is administratively disabled, the 7705 SAR sends a PW status notification message to the remote router.

Tagged Mode

In tagged mode, every frame sent on the Ethernet PW has a service-affecting VLAN tag. If the frame received by the 7705 SAR from the attachment circuit (AC) does not have a service-affecting VLAN tag, then the 7705 SAR inserts (pushes) a VLAN tag into the frame header before sending the frame to the SDP and the PW. If the frame received from the AC has a service-affecting VLAN tag, the tag is replaced.

In tagged mode, when the 7705 SAR detects a failure on the Ethernet physical port or the port is administratively disabled, the 7705 SAR sends a PW status notification message for all PWs associated with the port.

VLAN Translation

VLAN ID translation is supported, as appropriate. [Table 19](#) (see [Tagging Rules](#)) shows the VLAN ID translation operation for the various packet types. The payload part of the packet is shown in parentheses.

The operations to add, strip (remove), or forward the VLAN headers are performed based on the encapsulation type at the ingress of the attachment circuit (the SAP), in the network, and at the egress circuit.

Tagging Rules

[Table 17](#) and [Table 18](#) show the general tagging rules for combinations of interface port type (null or dot1q) and Epipe type (Ethernet or VLAN) for SAP ingress and SAP egress directions.

An attachment circuit (ingress or egress) can be configured for one of the following encapsulation types:

- null
- dot1q
- QinQ



Note: The QinQ mode is not supported in Release 1.1 of the 7705 SAR.

Table 17: Ingress SAP Tagging Rules

Ingress SAP Type ⁽¹⁾	VC Type (Epipe)	
	Raw (Ethernet)	Tagged (VLAN)
Null	No operation	Push (VC tag)
Dot1q	Pop (outer tag)	Pop (outer tag) Push (VC tag) ⁽²⁾

Notes:

1. Ingress SAP type is configured at the port level.
2. If the VC tag is not set, then the original tag is preserved.

Table 18: Egress SAP Tagging Rules

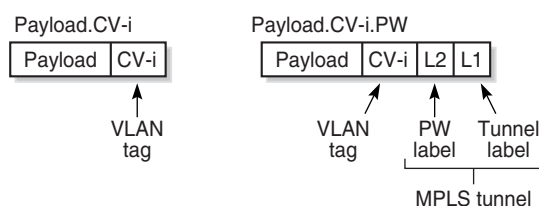
Egress SAP Type ⁽¹⁾	VC Type (Epipe)	
	Raw (Ethernet)	Tagged (VLAN)
Null	No operation	Pop (VC tag)
Dot1q	Push (SAP tag) ⁽²⁾	Pop (VC tag) Push (SAP tag) ⁽³⁾

Notes:

1. Ingress SAP type is configured at the port level.
2. If the SAP tag is 0, then no VLAN tag is pushed.
3. If the SAP tag is 0, then only the pop operation is performed.

Table 19 shows the VLAN ID translation operation (from ingress to egress) for the various packet types. In Table 19, the following abbreviations are used to simplify the operations shown in each cell, and the text in the cell represents the packet format.

- The packet payload at the service level is shown in parenthesis. It includes any SAP headers.
- CV represents the Customer VLAN tag, where CV-i and CV-x represent the ingress VLAN tag, and CV-e represents egress VLAN tag.
- PV represents the Provider VLAN tag, where PV can be either the customer-configured VLAN tag (that is, CV-x) or a provider-configured VLAN tag (that is, configured using the `spoke-sdp>vlan-vc-tag` CLI command)
- PW represents the MPLS label, which consists of a PW label and a tunnel label.
- Dots in packet formats represent the places in an Ethernet frame where labels or tags are added to a packet. Figure 20 shows two examples using the more familiar representation of a packet format, where the packet starts on the right-hand side.

Figure 20: Ethernet Frame Representations

19786



Note: When the SAP type is dot1q, the SAP VLAN tag always affects the ingress traffic, regardless of the Ethernet VLL type (raw or tagged). Similarly, when the SAP type is dot1q, untagged frames are dropped at the SAP ingress. That is, only the frames with an outer VLAN tag that matches the SAP VLAN tag are forwarded. The exception to this occurs when the VLAN tag = 0. When a SAP is configured with VLAN ID = 0, any untagged packets received are processed.

Table 19: Ethernet VLL Encapsulation Translation

Ingress / Attachment Circuit (Ethernet)	MPLS Network		Egress / Attachment Circuit (Ethernet)	
	Packet Format	VC Type	Encap	Packet Format
Null (untagged Ethernet)				
Payload	(Payload).PW	Raw	Null	Payload
	(Payload).PV.PW	Tag	Dot1q	Payload.CV-e
Payload.CV-i	(Payload.CV-i).PW	Raw	Null	Payload.CV-i
	(Payload.CV-i).PV.PW	Tag	Dot1q	Payload.CV-i.CV-e
Payload.CV-i.CV-x	(Payload.CV-i.CV-x).PW	Raw	Null	Payload.CV-i.CV-x
	(Payload.CV-i.CV-x).PV.PW	Tag	Dot1q	Payload.CV-i.CV-x.CV-e
Dot1q				
Payload	(Payload).PW	Raw	Null	Payload
	(Payload).PV.PW	Tag	Dot1q	Payload.CV-e
Payload.CV-i	(Payload).PW	Raw	Null	Payload
	(Payload).PV.PW	Tag	Dot1q	Payload.CV-e
Payload.CV-i.CV-x	(Payload.CV-i).PW	Raw	Null	Payload.CV-i
	(Payload.CV-i).PV.PW	Tag	Dot1q	Payload.CV-i.CV-e

VLL Service Considerations

This section describes the general 7705 SAR service features and any special capabilities or considerations as they relate to VLL services.

Topics in this section include:

- [Service Support](#)
- [SDPs](#)
- [SAP Encapsulations and Pseudowire Types](#)
- [QoS Policies](#)
- [MTU Settings](#)
- [Pseudowire Control Word](#)

Service Support

ATM VLL service is supported on any T1/E1 port on the 16-port T1/E1 ASAP Adapter card when the port is configured for ATM or IMA.

Ethernet VLL service is supported on any Ethernet port on the 8-port Ethernet Adapter card.

TDM VLL service is supported on any T1/E1 port on the 16-port T1/E1 ASAP Adapter card when the port is configured for circuit emulation encapsulation.

The 7705 SAR supports a combined total of 1024 VLLs for ATM, Ethernet, and TDM VLLs.



Note: MPLS and VLL service over MPLS is not supported on access ports.

SDPs

The most basic SDPs must have the following characteristics:

- a locally unique SDP identification (ID) number and a VC-ID
- the system IP address of the far-end 7705 SAR routers
- an SDP encapsulation type — GRE or MPLS

SDP Statistics for VLL Services

Release 1.1 supports local CLI-based and SNMP-based statistics collection for each VC used in the SDPs. This allows for traffic management of tunnel usage by the different services and, with aggregation, the total tunnel usage.

SAP Encapsulations and Pseudowire Types

The section describes encapsulations and PW types for the following VLL services:

- Apipe
- Cpipe
- Epipe

Apipe

ATM VLLs can be configured with both endpoints (SAPs) on the same router or with the two endpoints on different routers. In the latter case, Pseudowire Emulation Edge-to-Edge (PWE3) signaling can be used to establish a pseudowire between the devices, allowing ATM traffic to be tunneled through an MPLS or IP network.

As an alternative to signaled pseudowires, manual configuration of pseudowires is also supported.

The Apipe service supports both VP and VC connections, which are identified by specifying the `vc-type` when provisioning the Apipe. The N-to-1 VCC cell transport mode is supported (see [ATM PWE3 N-to-1 Cell Mode Encapsulation on page 123](#)). The value of N is always 1.

The PW service types supported in Release 1.1 are 0x0009 (for ATM N-to-1 VCC cell mode) and 0x000A (for ATM N-to-1 VPC cell mode), as defined in RFC 4446.

Cpipe

Cpipe service supports CESoPSN and SAToP encapsulation over MPLS or GRE tunnels to connect to the far-end circuit. In Release 1.1, Cpipes support SAP-to-SAP and SAP-to-spoke SDP binding with a default service MTU of 1514 bytes.

The PW service types supported in Release 1.1 are 0x0011 (SAToP E1), 0x0012 (SAToP T1), 0x0015 (CESoPSN basic mode), and 0x0017 (CESoPSN TDM with CAS).

Epipe

Epipe service is designed to carry Ethernet frame payloads, so it can provide connectivity between any two SAPs on different nodes that pass Ethernet frames. The following SAP encapsulations are supported on the 7705 SAR Epipe service:

- Ethernet null
- Ethernet dot1q

While different encapsulation types can be used at either end, encapsulation mismatching can occur if the encapsulation behavior is not understood by connecting devices and if those devices are unable to send and receive the expected traffic. For example, if the encapsulation type on one side of the Epipe is dot1q and the other is null, tagged traffic received on the null SAP will be double-tagged when it is transmitted out of the dot1q SAP.

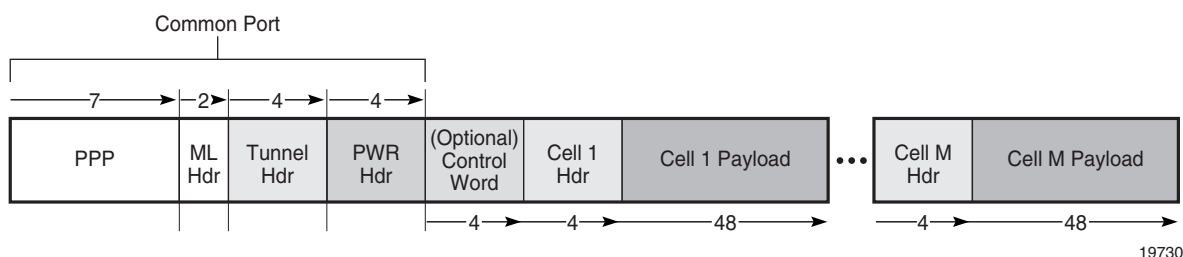
The PW service types supported in Release 1.1 are 0x0004 (Ethernet tagged mode), and 0x0005 (Ethernet raw).

ATM PWE3 N-to-1 Cell Mode Encapsulation

ATM PWE3 signaling over a PSN uses N-to-1 cell mode encapsulation (as per RFC 4717). For Release 1.1, N is not user-configurable and N = 1 is the only value supported. [Figure 21](#) shows the structure of an N-to-1 cell mode frame.

In N-to-1 mode, OAM cells are transported through the VLL in the same way as any other cell.

Figure 21: N-to-1 Cell Mode Encapsulation



VPI/VCI Translation

To simplify provisioning, the same VPI and VCI can be used at different sites. Before traffic from various sites can be switched to a Radio Network Controller (RNC), VPI and VCI translation must occur in order to uniquely identify the site and the far-end equipment.

The endpoints of a PWE3 N-to-1 cell mode ATM VLL can be:

- ATM VCs—VPI/VCI translation is supported (the VPI/VCI at each endpoint does not need to be the same)

In this case, when the VPI and VCI used at the endpoints are different, both the VPI and the VCI can be modified at the endpoint (VPI and/or VCI can only be changed by the far-end PE node, before the cells are switched to the ATM interface).

- ATM VPs—VPI translation is supported (the VPI at each endpoint need not be the same, but the original VCI will be maintained)

In this case, when the VPI and VCI used at the endpoints are different, only the VPI can be modified at the endpoint (VPI can only be changed by the far-end PE node, before the cells are switched to the ATM interface).

Control Word

An optional control word (CW) is supported for ATM VLLs. Refer to [Pseudowire Control Word on page 130](#) for more information.

Cell Concatenation

Cell concatenation (or packing) into a pseudowire packet payload at the VC and VP levels is supported. Cells are packed on ingress to the VLL and unpacked on egress.

Cell concatenation is supported only for N-to-1 cell mode, where $N = 1$.

The number of cells in the payload of a single VLL packet is user-configurable, which ensures proper transport of traffic sensitive to delay and jitter. (For example, for voice traffic in 3G/WCDMA, delay is a crucial factor and the time spent for concatenation should be minimized. The payload is extremely delay-sensitive and should be transported with only a small amount of bandwidth optimization.) In all cases, the number of cells in a VLL packet must be less than the MTU size, where the MTU maximum is 1514 bytes and the maximum N-to-1 mode payload is 29 cells (52 ATM bytes per cell (no HEC byte)).

While cells are being packed, the concatenation process may be terminated by any one of the following conditions. Each condition has a configurable attribute associated with it:

- reaching a maximum number of cells per packet
- expiring of a timer
- changing of the cell loss priority (CLP) bit

If none of the conditions are met, the packet is sent when the MTU is reached. The CLP bits are untouched, even if VPI/VCI translation occurs at egress.



Note: Configuring the attributes that provide the best compromise between minimizing delay (low number of cells concatenated) and maximizing bandwidth (high number of cells concatenated) requires careful planning.

QoS Policies

When applied to 7705 SAR Apipe, Cpipe, and Epipe services, service ingress QoS policies only create the unicast queues defined in the policy.

With Apipe, Cpipe, and Epipe services, egress QoS policies function as with other services where the class-based queues are created as defined in the policy.

Both Layer 2 and Layer 3 criteria can be used in the QoS policies for traffic classification in a Cpipe or Epipe service. QoS policies on Apipes cannot perform any classification.

MTU Settings

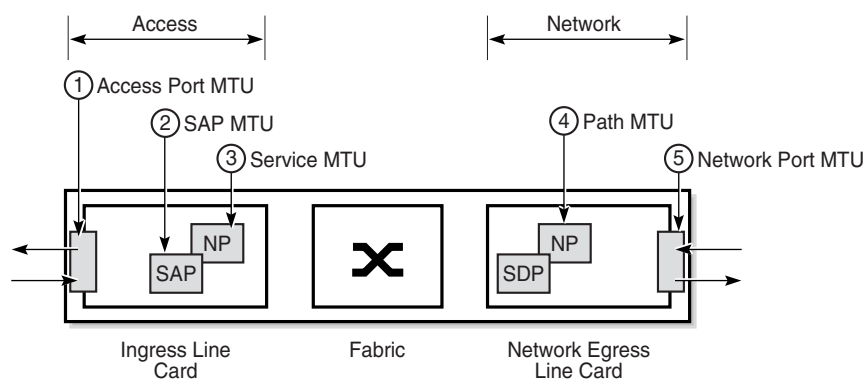
There are several MTU values that must be set properly for a VLL service (Apipe, Cpipe, or Epipe) to work from end to end. [Figure 22](#) locates the MTU point for each value. [Table 20](#) describes the MTU points. The MTU points are:

- access port MTU
- SAP MTU
- service MTU
- path MTU
- network port MTU

In order for a VLL service to be declared “up” without any MTU-related error messages, the following rule must be true:

$$\text{SAP MTU} \geq \text{Service MTU} \leq \text{Path MTU}$$

Figure 22: MTU Points on the 7705 SAR



1968

Table 20: MTU Points and Descriptions

Key	MTU Point	Description
1	Access port MTU	<p>The access port MTU value is a configurable value that accounts for the L2 header and the payload. The default access port MTU value for the following Fast Ethernet port SAP encapsulations is:</p> <ul style="list-style-type: none"> • Null: 1514 bytes (payload = 1500 bytes, L2 header = 14 bytes) • dot1q: 1518 bytes (payload = 1500 bytes, L2 header = 18 bytes)
2	SAP MTU	<p>The SAP MTU value is not a configurable value. It is set at the SAP by the 7705 SAR operating system. It defines the service payload capability of the service and is automatically set to be the same value as the access port MTU.</p>
3	Service MTU	<p>The service MTU value is a configurable value and is the same size as the VLL payload. The service MTU is sometimes called the VC-type MTU in the 7705 SAR documentation set. In Figure 22, NP stands for network processor.</p> <p>For CESoPSN with CAS service, ensure that the service MTU is set to a value large enough to account for the extra bytes appended to the packet payload for CAS bits. See Structured E1 CES with CAS on page 107 for more information.</p>
4	Path MTU	<p>The path MTU is configured at the SDP. It is the maximum that the SDP can transmit without rejecting and discarding the packet. The path MTU value is derived from the network port MTU value by subtracting the Layer 2 and Layer 2.5 overhead values (for MPLS) and the Layer 2 and Layer 3 overhead values (for GRE).</p> <p>If the network port SDP binding is Ethernet, then the following equations hold:</p> <ul style="list-style-type: none"> • For MPLS: Path MTU = Port MTU - (Ethernet header [14 bytes or 18 bytes] + Tunnel header + PW header) • For GRE: Path MTU = Port MTU - (Ethernet header [14 bytes or 18 bytes] + IP header [20 bytes] + Tunnel header [4 bytes] + PW header [4 bytes])
5	Network port MTU	<p>The network port MTU is a configurable value equal to the payload plus all headers (L2, IP (for GRE), tunnel and PW), up to the maximum supported value (hardware limit) of 1572 bytes.</p>

[Table 21](#) shows a breakdown of the various payload and overhead components that contribute to the MTU sizes of the VLL services at the MTU points shown in [Figure 22](#).

Table 21: MTU Values — Service Creation (Worst Case)

Packet Component	Access Port MTU		SAP MTU	Service MTU	Network Port MTU (for worst-case Service MTU ⁽¹⁾)					
	TDM/ ATM	Eth			PPP	ML-PPP	Eth-Null	Eth-dot1q	Eth-QinQ ⁽²⁾	IP
Eth-FCS										
Payload	1514	1500	1514	1514	1514	1514	1514	1514	1514	1510 or 1514
RTP Header				12	12	12	12	12	12	12
Ctrl Word				4	4	4	4	4	4	4
PW Header					4	4	4	4	4	4
MPLS Header					4	4	4	4	4	0
GRE Header										4
IP										20
QinQ ⁽²⁾									4	
VLAN								4	4	4 ⁽³⁾
Eth-Type		2					2	2	2	2
Eth-SA		6					6	6	6	6
Eth-DA		6					6	6	6	6
PPP-FCS										
ML-Sequence						3				
ML-Preamble						1				
PPP-Protocol					2	2				
PPP-Control					1	1				
PPP-Address					1	1				
PPP-Flag										
Total	1514	1514	1514	1530	1542	1546	1552	1556	1560	1572 ⁽⁴⁾

Notes:

1. The service MTU value for Cpipe represents the worst-case value for the Apipe, Cpipe, and Epipe services.
2. Ethernet QinQ is not supported in Release 1.1 and is shown here for reference purposes only.
3. Optional
4. The maximum MTU cannot exceed 1572 bytes (hardware limit); therefore, the payload value might have to be less than 1514 bytes.



Note: In order to accommodate current and future services (including overhead), the MTU value for Gigabit Ethernet and PPP/MLPPP ports have the default value set to 1572 bytes. For 10/100 Ethernet ports, the MTU value is set to 1514 or 1518 bytes, depending on the encapsulation setting (null or dot1q).

Note: The default service MTU value is 1514 bytes; the maximum value is 1522 bytes.

Targeted LDP and MTU

The extended discovery mechanism for Label Distribution Protocol (LDP) sends LDP Targeted Hello messages to a specific address. This is known as targeted LDP or TLDP. Refer to RFC 5036 for detailed information about the extended discovery mechanism.

During the VLL service creation process (that is, using targeted LDP signaling), the MTU or payload size of a service is signaled to the far-end peer. MTU settings at both ends (near and far peers) must match in order for the VLL service to operate. [Table 22](#) shows the values that are expected to match.

Table 22: Matching MTU or Payload Values for Signaled VLL Services

	Apipe	Cpipe	Epipe
Payload size (bytes)		Yes	
Bit rate		Yes	
Maximum number of ATM cells	Yes		
Service MTU			Yes
Must match at both ends	Yes	Yes	Yes

Pseudowire Control Word

The PW control word (CW) is a 32-bit field that is inserted between the VC label and the Layer 2 frame. The presence of the control word is indicated by the C bit of the FEC element used in LDP signaling. The PW control word is described in RFC 4385.

The PW control word is supported for all implemented PW types (ATM N-to-1 cell mode, Ethernet VLLs, SAToP, and CESoPSN PW) in Release 1.1 of the 7705 SAR.

The following points describe the behavior of the 7705 SAR when it receives a Label Mapping message for a PW. It is assumed that no Label Mapping message for the PW has been sent to the next PW router yet. The 7705 SAR operating system does the following.

- If the received Label Mapping message has $C = 0$ (where C refers to the C bit of the FEC element), a Label Mapping message with $C = 0$ is sent forward to the next router (or hop). In this case, the control word is not used.
 - If the received Label Mapping message has $C = 1$ and the PW is locally configured such that the use of the control word is mandatory, then the 7705 SAR sends a Label Mapping message with $C = 1$. In this case, the control word is used. (Note: SAToP and CESoPSN are the only services in Release 1.1 that require the control word.)
 - If the received Label Mapping message has $C = 1$ and the locally configured PW does not support use of an optional control word (that is, Ethernet or ATM N-to-1 cell mode PWs), then the 7705 SAR sends a new Label Mapping message in which the C bit is set to correspond to the locally configured preference for use of the control word (that is, $C = 0$).
-

Configuring a VLL Service with CLI

This section provides the information required to configure Virtual Leased Line (VLL) services using the command line interface.

Topics in this section include:

- [List of Commands on page 132](#)
- [Common Configuration Tasks on page 140](#)
- [Configuring VLL Components on page 141](#)
 - [Creating an Apipe Service on page 141](#)
 - [Creating a Cpipe Service on page 146](#)
 - [Creating an Epipe Service on page 150](#)
 - [Configuring Ingress and Egress SAP Parameters on page 154](#)
 - [Using the Control Word on page 155](#)
- [Service Management Tasks on page 157](#)
 - [Modifying Service Parameters on page 157](#)
 - [Disabling a Service on page 159](#)
 - [Re-enabling a Service on page 161](#)
 - [Deleting a Service on page 161](#)

List of Commands

[Table 23](#) lists all the service configuration commands, indicating the configuration level at which each command is implemented with a short command description. VLL services are configured in the `config>service` context. The command list is organized in the following task-oriented manner:

- Apipe
 - [Configure an Apipe service](#)
 - [Configure Apipe service parameters](#)
 - [Configure Apipe SAP parameters](#)
 - [Configure Apipe SAP egress and ingress parameters](#)
 - [Configure Apipe SAP ATM parameters](#)
 - [Configure Apipe SAP ATM egress and ingress parameters](#)
 - [Configure Apipe spoke SDP parameters](#)
 - [Configure Apipe spoke SDP cell concatenation parameters](#)
 - [Configure Apipe spoke SDP egress or ingress parameters](#)
- Cpipe
 - [Configure a Cpipe service](#)
 - [Configure Cpipe service parameters](#)
 - [Configure Cpipe SAP parameters](#)
 - [Configure Cpipe SAP egress and ingress parameters](#)
 - [Configure Cpipe SAP cem parameters](#)
 - [Configure Cpipe spoke SDP parameters](#)
 - [Configure Cpipe spoke SDP egress or ingress parameters](#)
- Epipe
 - [Configure an Epipe service](#)
 - [Configure Epipe service parameters](#)
 - [Configure Epipe SAP parameters](#)
 - [Configure Epipe SAP egress and ingress parameters](#)
 - [Configure Epipe spoke SDP parameters](#)
 - [Configure Epipe spoke SDP egress or ingress parameters](#)

Table 23: CLI Commands to Configure VLL Service Parameters

Command	Description	Page
Configure an Apipe service		
<code>config>service>apip</code>		
<code>config>service>apip service-id [customer customer-id] [vpn vpn-id] [vc-type {atm-vcc atm-vpc}]</code>		171
<code>service-id</code>	Specifies a unique service identification number identifying the service in the service domain	171
<code>customer-id</code>	Specifies the existing customer ID number associated with the service	171
<code>vpn-id</code>	Specifies the VPN ID number which allows you to identify VPNs	171
<code>vc-type</code>	Specifies a 15-bit value that defines the type of the VC signaled to the peer	171
Configure Apipe service parameters		
<code>config>service>apip</code>		
<code>description</code>	Specifies a text string describing the service	169
<code>sap</code>	Enables access to the context to configure SAP-related attributes	175
<code>service-mtu</code>	Configures the MTU to be used for this service	173
<code>shutdown</code>	Administratively enables or disables the Apipe service	169
<code>spoke-sdp</code>	Binds a service to an existing SDP (for distributed service)	184
Configure Apipe SAP parameters		
<code>config>service>apip>sap</code>		175
<code>accounting-policy</code>	Specifies the accounting policy to apply to the SAP	181
<code>atm</code>	Enables access to the context to configure ATM-related attributes	190
<code>collect-stats</code>	Enables the collection of accounting and statistical data for the SAP or network port	181
<code>description</code>	Specifies a text string describing the Apipe SAP	169
<code>egress</code>	Enables access to the context to configure egress SAP QoS policies	182
<code>ingress</code>	Enables access to the context to configure ingress SAP QoS policies	182

Table 23: CLI Commands to Configure VLL Service Parameters (Continued)

Command	Description	Page
shutdown	Administratively enables or disables the SAP	123
Configure Apipe SAP egress and ingress parameters		
config>service>apip		
config>service>apip		
qos	Associates a QoS policy with an ingress or egress SAP	182
Configure Apipe SAP ATM parameters		
config>service>apip		
egress	Configures egress ATM attributes for the SAP	190
ingress	Configures ingress ATM attributes for the SAP	190
oam	Enables access to the context to configure OAM functionality for a PVCC delimiting a SAP	192
Configure Apipe SAP ATM egress and ingress parameters		
config>service>apip		
config>service>apip		
traffic-desc	Assigns an ATM traffic descriptor profile to a given context, such as to a SAP	190
Configure Apipe spoke SDP parameters		
config>service>apip		184
cell-concatenation	Enables access to the context to configure the various options that control the termination of ATM cell concatenation into an MPLS frame. Several options can be configured simultaneously.	187
egress	Configures the egress spoke SDP context	188
ingress	Configures the ingress spoke SDP context	188
shutdown	Administratively enables or disables the spoke SDP binding	169

Table 23: CLI Commands to Configure VLL Service Parameters (Continued)

Command	Description	Page
Configure Apipe spoke SDP cell concatenation parameters		
<code>config>service>apipe>spoke-sdp>cell-concatenation</code>		
<code>clp-change</code>	Enables the CLP change to be an indication to complete the cell concatenation operation	187
<code>max-cells</code>	Configures the maximum number of ATM cells to accumulate in an MPLS packet	188
<code>max-delay</code>	Configures the maximum amount of time to wait while performing ATM cell concatenation into an MPLS packet before transmitting the MPLS packet	189
Configure Apipe spoke SDP egress or ingress parameters		
<code>config>service>apipe>spoke-sdp>egress</code> <code>config>service>apipe>spoke-sdp>ingress</code>		
<code>vc-label</code>	Configures the egress or ingress VC label	185
Configure a Cpipe service		
<code>config>service>cpipe <i>service-id</i> [customer <i>customer-id</i>] [vpn <i>vpn-id</i>] [vc-type {satop-el satop-tl cesopsn} cesopsn-cas}]</code>		
<code>customer-id</code>	Specifies the existing customer ID number associated with the service	172
<code>service-id</code>	Specifies a unique service identification number identifying the service in the service domain	172
<code>vpn-id</code>	Specifies the VPN ID number which allows you to identify VPNs	172
<code>vc-type</code>	Specifies a 15-bit value that defines the type of the VC signaled to the peer	172
Configure Cpipe service parameters		
<code>config>service>cpipe</code>		
<code>description</code>	Specifies a text string describing the service	169
<code>sap</code>	Enables access to the context to configure SAP-related attributes	175
<code>service-mtu</code>	Configures the MTU to be used for this service	173
<code>shutdown</code>	Administratively enables or disables the Cpipe service	169

Table 23: CLI Commands to Configure VLL Service Parameters (Continued)

Command	Description	Page
<code>spoke-sdp</code>	Binds a service to an existing SDP (for distributed service)	184
Configure Cpipe SAP parameters		
<code>config>service>cpipe>sap</code>		
<code>accounting-policy</code>	Specifies the accounting policy to apply to the SAP	181
<code>cem</code>	Enables access to the context to configure circuit emulation service parameters	178
<code>collect-stats</code>	Enables the collection of accounting and statistical data for the SAP or network port	181
<code>description</code>	Specifies a text string describing the Cpipe SAP	169
<code>egress</code>	Enables access to the context to configure egress SAP QoS policies	182
<code>ingress</code>	Enables access to the context to configure ingress SAP QoS policies	182
<code>shutdown</code>	Administratively enables or disables the SAP	169
Configure Cpipe SAP cem parameters		
<code>config>service>cpipe>sap>cem</code>		
<code>packet</code>	Enables access to the context to configure packet parameters	178
<code>report-alarm</code>	Enables or disables alarm reporting for CES circuit alarm conditions	179
<code>rtp-header</code>	Specifies the optional RTP header, if one has been inserted in the circuit emulation service packets	180
Configure Cpipe SAP cem packet parameters		
<code>config>service>cpipe>sap>cem>packet</code>		
<code>jitter-buffer</code>	Configures the size of the receive jitter buffer for the circuit emulation service SAP	178
<code>payload-size</code>	Configures the size of the payload for one circuit emulation service packet	179

Table 23: CLI Commands to Configure VLL Service Parameters (Continued)

Command	Description	Page
Configure Cpipe SAP egress and ingress parameters		
config>service>cpipe>sap>egress		
config>service>cpipe>sap>ingress		
qos	Associates a QoS policy with an ingress or egress SAP	182
Configure Cpipe spoke SDP parameters		
config>service>cpipe>spoke-sdp		
egress	Configures the egress spoke SDP context	188
ingress	Configures the ingress spoke SDP context	188
shutdown	Administratively enables or disables the SDP	169
Configure Cpipe spoke SDP egress or ingress parameters		
config>service>cpipe>spoke-sdp>egress		
config>service>cpipe>spoke-sdp>ingress		
vc-label	Configures the egress or ingress VC label	185
Configure an Epipe service		
config>service>epipe <i>service-id</i> [customer <i>customer-id</i>] [vpn <i>vpn-id</i>]		
customer-id	Specifies the customer ID number to be associated with the service	173
service-id	Specifies a unique service identification number identifying the service in the service domain	173
vpn-id	Specifies the VPN ID number which allows you to identify VPNs	173
Configure Epipe service parameters		
config>service>epipe		
description	Specifies a text string describing the Epipe service	169
sap	Enables access to the context to configure SAP-related attributes	175

Table 23: CLI Commands to Configure VLL Service Parameters (Continued)

Command	Description	Page
<code>service-mtu</code>	Configures the service payload MTU in bytes for the service ID overriding the service-type default MTU	173
<code>shutdown</code>	Administratively enables or disables the service	169
<code>spoke-sdp</code>	Binds a service to an existing SDP	184
Configure Epipe SAP parameters		
<code>config>service>epipe>sap</code>		
<code>accounting-policy</code>	Associates the accounting policy ID with the SAP. Accounting policies are configured in the <code>config>log</code> context.	181
<code>collect-stats</code>	Enables the collection of accounting and statistical data for the SAP, network port, or IP interface	181
<code>description</code>	Specifies a text string describing the Epipe SAP	169
<code>egress</code>	Enables access to the context to configure egress SAP QoS policies	182
<code>ingress</code>	Configures ingress SAP QoS policies	182
Configure Epipe SAP egress and ingress parameters		
<code>config>service>epipe>sap>egress</code> <code>config>service>epipe>sap>ingress</code>		
<code>qos</code>	Associates a QoS policy with an egress or ingress SAP or IP interface	182
Configure Epipe spoke SDP parameters		
<code>config>service>epipe>spoke-sdp</code>		
<code>egress</code>	Configures the egress spoke SDP context	188
<code>ingress</code>	Configures the ingress spoke SDP context	188
<code>shutdown</code>	Administratively enables the SDP	169
<code>vlan-vc-tag</code>	Specifies an explicit dot1q value used for encapsulation to the SDP far end	186

Table 23: CLI Commands to Configure VLL Service Parameters (Continued)

Command	Description	Page
Configure Epipe spoke SDP egress or ingress parameters		
config>service>epipe>spoke-sdp>egress		
config>service>epipe>spoke-sdp>ingress		
vc-label	Configures the egress or ingress VC label	185

Common Configuration Tasks

The list below provides a brief overview of the tasks that must be performed to configure a VLL service.

- Associate the service with a customer ID.
 - Define SAP parameters.
 - Optional – select egress and ingress QoS policies (configured in `config>qos` context)
 - Define spoke SDP parameters.
 - Optional – select egress and ingress vc label parameters
 - Enable the service.
-

Configuring VLL Components

This section provides configuration examples for components of VLL services. Each component includes some or all of the following: introductory information, CLI syntax, a specific CLI example, and a sample CLI display output. Included are the following VLL components:

- Apipe
 - [Creating an Apipe Service](#)
 - [Configuring Apipe SAP Parameters](#)
 - [Configuring Apipe SDP Bindings](#)
- Cpipe
 - [Creating a Cpipe Service](#)
 - [Configuring Cpipe SAP parameters](#)
 - [Configuring Cpipe SDP bindings](#)
- Epipe
 - [Creating an Epipe Service](#)
 - [Configuring Epipe SAP Parameters](#)
 - [Configuring Epipe SDP Bindings](#)
- [Configuring Ingress and Egress SAP Parameters](#)
- [Using the Control Word](#)

Creating an Apipe Service

Use the following CLI syntax to create an Apipe service.

CLI Syntax: `config>service# apipe service-id [customer customer-id]
[create] [vpn vpn-id] [vc-type {atm-vcc|atm-vpc}]
description description-string
service-mtu octets
no shutdown`

PE router 1 (A:ALU-41):

Example: `A:ALU-41>config>service# apipe 5 customer 1 create
A:ALU-41config>service>apip# description "apip test"
A:ALU-41config>service>apip# service-mtu 1400
A:ALU-41config>service>apip# no shutdown
A:ALU-41config>service>apip#`

PE router 2 (A:ALU-42):

Example: A:ALU-42>config>service# apipe 5 customer 1 create
 A:ALU-42>config>service>apipe# description "apipe test"
 A:ALU-42>config>service>apipe# service-mtu 1400
 A:ALU-42>config>service>apipe# no shutdown
 A:ALU-42>config>service>apipe#

The following example displays the Apipe service creation output.

PE Router 1 (ALU-41):

```
A:ALU-41>config>service# info
-----
...
      apipe 5 customer 1 create
        description "apipe test"
        service-mtu 1400
        no shutdown
      exit
...
-----
A:ALU-41>config>service#
```

PE Router 2 (ALU-42):

```
A:ALU-42>config>service# info
-----
...
      apipe 5 customer 1 create
        description "apipe test"
        service-mtu 1400
        no shutdown
      exit
...
-----
A:ALU-42>config>service#
```

Configuring Apipe SAP Parameters

Use the following CLI syntax to configure Apipe SAP parameters. For ingress and egress configuration information, see [Configuring Ingress and Egress SAP Parameters on page 154](#).

CLI Syntax: `config>service# apipe service-id [customer customer-id]
[create] [vpn vpn-id] [vc-type {atm-vcc|atm-vpc}]
sap sap-id [create]
accounting-policy acct-policy-id
atm
egress
traffic-desc traffic-desc-profile-id
ingress
traffic-desc traffic-desc-profile-id
oam
alarm-cells
collect-stats
description description-string
egress
qos policy-id
ingress
qos policy-id
no shutdown`

Example:

```
A:ALU-41>config>service# apipe 5
A:ALU-41>config>service>apip# sap 1/1/1.1:0/32 create
A:ALU-41>config>service>apip# ingress
A:ALU-41>config>service>apip>sap>ingress# qos 102
A:ALU-41>config>service>apip>sap>ingress# exit
A:ALU-41>config>service>apip>sap# egress
A:ALU-41>config>service>apip>sap>egress# qos 103
A:ALU-41>config>service>apip>sap>egress# exit
A:ALU-41>config>service>apip>sap# no shutdown
A:ALU-41>config>service>apip>sap# exit
A:ALU-41>config>service>apip#
```

The following example displays the Apipe SAP configuration output for PE Router 1 (ALU-41).

```
A:ALU-41>config>service# info
-----
...
    apipe 5 customer 1 create
        description "apipe test"
        service-mtu 1400
        sap 1/1/1.1:0/32 create
            ingress
                qos 102
            exit
            egress
                qos 103
            exit
        exit
        no shutdown
    exit
...
-----
```

To configure a basic local Apipe service (SAP-to-SAP), enter the `sap sap-id` command twice with different port IDs in the same service configuration.

The following example displays an ATM SAP-to-SAP configuration:

```
A:ALU-4>config>service# info
-----
...
    apipe 5 customer 1 create
        description "ATM sap2sap"
        service-mtu 1514
        sap 1/1/1.1:0/32
        sap 1/2/1.1:0/100
        no shutdown
    exit
...
-----
```


Configuring Apipe SDP Bindings

Use the following CLI syntax to create a spoke SDP binding with an Apipe service (for distributed service). For SDP configuration information, see [Configuring SDPs on page 60](#).

CLI Syntax: config>service# apipe *service-id* [customer *customer-id*] [create] [vpn *vpn-id*] [vc-type {atm-vcc|atm-vpc}] spoke-sdp *sdp-id:vc-id* [create] cell-concatenation clp-change max-cells *cell-count* max-delay *delay-time* egress vc-label *egress-vc-label* ingress vc-label *ingress-vc-label* no shutdown

Example: A:ALU-41>config>service# apipe 5
A:ALU-41>config>service>apipe# spoke-sdp 1:5 create
A:ALU-41>config>service>apipe>spoke-sdp# no shutdown
A:ALU-41>config>service>apipe>spoke-sdp# exit

The following example displays the Apipe spoke SDP configuration output for PE Router 1 (ALU-41).

```
A:ALU-41>config>service# info
-----
...
    apipe 5 customer 1 create
        description "apipe test"
        service-mtu 1400
        sap 1/1/1.1:0/32 create
            ingress
                qos 102
            exit
            egress
                qos 103
            exit
        exit
        spoke-sdp 1:5 create
        exit
        no shutdown
    exit
...
-----
A:ALU-41>config>service#
```

Creating a Cpipe Service

Use the following CLI syntax to create a Cpipe service.

CLI Syntax: config>service# cpipe *service-id* [customer *customer-id*] [create] [vpn *vpn-id*] [vc-type {satop-e1 | satop-t1 | cesopsn | cesopsn-cas}]

```

description description-string
service-mtu octets
no shutdown
```

Example:

```

config>service# cpipe 234 customer 123 create vc-type
cesopsn
config>service>cpipe# description "cpipe test"
config>service>cpipe# service-mtu 1400
config>service>cpipe# no shutdown
config>service>cpipe#
```

The following example displays the Cpipe service creation output for PE Router 1 (ALU-41).

```

A:ALU-41>config>service# info
-----
...
    cpipe 234 customer 123 create
        description "cpipe test"
        service-mtu 1400
        no shutdown
    exit
...
-----
A:ALU-41>config>service#
```

Configuring Cpipe SAP parameters

Use the following CLI syntax to configure Cpipe SAP parameters. For ingress and egress configuration information, see [Configuring Ingress and Egress SAP Parameters on page 154](#).

CLI Syntax: config>service# cpipe *service-id* [customer *customer-id*] [create] [vpn *vpn-id*] [vc-type {satop-e1 | satop-t1 | cesopsn | cesopsn-cas}]

```

sap sap-id [create]
    cem
        [no] packet
            jitter-buffer value | payload-size value
            payload-size value
        [no] report-alarm [stray] [malformed] [pktloss]
```

```

[overrun] [underrun] [rpktloss]
[rfault] [rrdi]
[no] rtp-header
[no] collect-stats
description description-string
no description
egress
    qos policy-id
    no qos
ingress
    qos policy-id
    no qos
[no] shutdown

```

Example:

```

A:ALU-41>config>service# cpipe 5 cesopsn
A:ALU-41>config>service>cpipe# sap 1/1/1.1 create
A:ALU-41>config>service>cpipe>sap# ingress
A:ALU-41>config>service>cpipe>sap>ingress# qos 102
A:ALU-41>config>service>cpipe>sap>ingress# exit
A:ALU-41>config>service>cpipe>sap# egress
A:ALU-41>config>service>cpipe>sap>egress# qos 103
A:ALU-41>config>service>cpipe>sap>egress# exit
A:ALU-41>config>service>cpipe>sap# no shutdown
A:ALU-41>config>service>cpipe>sap# exit
A:ALU-41>config>service>cpipe#

```

The following example displays the Cpipe SAP configuration output for PE Router 1 (ALU-41).

```

A:ALU-41>config>service# info
-----
...
    cpipe 5 customer 1 create
        description "cpipe test"
        service-mtu 1400
        sap 1/1/1.1 create
            ingress
                qos 102
            exit
            egress
                qos 103
            exit
        exit
        no shutdown
    exit
...
-----
A:ALU-41>config>service#

```

To configure a basic local Cpipe service (SAP-to-SAP), enter the `sap sap-id` command twice with different port IDs in the same service configuration.

The following example displays a TDM SAP-to-SAP configuration:

```
A:ALU-4>config>service# info
-----
...
      cpipe 5 customer 1 create
        description "TDM sap2sap"
        service-mtu 1400
        sap 1/1/1.1
        sap 1/2/1.1
        no shutdown
      exit
...
-----
```

Configuring Cpipe SDP bindings

Use the following CLI syntax to create a spoke SDP binding with a Cpipe service. For SDP configuration information, see [Configuring SDPs on page 60](#).

CLI Syntax: config>service# cpipe *service-id* [customer *customer-id*] [create] [vpn *vpn-id*] [vc-type {satop-e1 | satop-t1 | cesopsn | cesopsn-cas}]

```

    spoke-sdp sdp-id:vc-id [create]
    egress
        vc-label egress-vc-label
    ingress
        vc-label ingress-vc-label
    [no] shutdown

```

Example:

```

A:ALU-41>config>service# cpipe 5
A:ALU-41>config>service>cpipe# spoke-sdp 1:5 create
A:ALU-41>config>service>cpipe>spoke-sdp# no shutdown
A:ALU-41>config>service>cpipe>spoke-sdp# exit

```

The following example displays the Cpipe spoke SDP configuration output for PE Router 1 (ALU-41).

```

A:ALU-41>config>service# info
-----
...
    cpipe 5 customer 1 create
        description "cpipe test"
        service-mtu 1400
        sap 1/1/1.1 create
            ingress
                qos 102
            exit
            egress
                qos 103
            exit
        exit
        spoke-sdp 1:5 create
        exit
        no shutdown
    exit
...
-----
A:ALU-41>config>service#

```

Creating an Epipe Service

Use the following CLI syntax to create an Epipe service.

CLI Syntax: `config>service# epipe service-id [customer customer-id]
[create] [vpn vpn-id]
 description description-string
 no shutdown`

Example: `config>service# epipe 500 customer 5 create
config>service>epipe$ description "Local epipe service"
config>service>epipe# no shutdown`

The following example displays the Epipe service creation output.

```
ALU-1>config>service# info
-----
...
      epipe 500 customer 5 vpn 500 create
      description "Local epipe service"
      no shutdown
      exit
-----
ALU-1>config>service#
```

Configuring Epipe SAP Parameters

In Release 1.1, distributed Epipe service is supported. A distributed Epipe consists of two SAPs on different nodes. To configure a distributed Epipe service, you must configure service entities on the originating and far-end nodes.

Use the following CLI syntax to create distributed Epipe SAPs. For ingress and egress configuration information, see [Configuring Ingress and Egress SAP Parameters on page 154](#).

CLI Syntax: `config>service# epipe service-id [customer customer-id]
[create]`

```
      sap sap-id [create]
      accounting-policy policy-id
      collect-stats
      description description-string
      no shutdown
      egress
      qos policy-id
      ingress
      qos policy-id
```

Example:

```

ALU-1>epipe 5500 customer 5 create
config>service>epipe$ description "Distributed epipe
service to east coast"
config>service>epipe# sap 1/1/3.1:21 create
config>service>epipe>sap# ingress
config>service>epipe>sap>ingress# qos 555
config>service>epipe>sap>ingress# exit
config>service>epipe>sap# egress
config>service>epipe>sap>egress# qos 627
config>service>epipe>sap>egress# exit
config>service>epipe>sap# no shutdown
config>service>epipe>sap# exit
config>service>epipe#

ALU-2>config>service# epipe 5500 customer 5 create
config>service>epipe$ description "Distributed epipe
service to west coast"
config>service>epipe# sap 1/1/4.1:550 create
config>service>epipe>sap# ingress
config>service>epipe>sap>ingress# qos 654
config>service>epipe>sap>ingress# exit
config>service>epipe>sap# egress
config>service>epipe>sap>egress# qos 432
config>service>epipe>sap>egress# exit
config>service>epipe>sap# no shutdown
config>service>epipe#

```

The following example displays the SAP configuration output for ALU-1 and ALU-2.

```

ALU-1>config>service# info
-----
...
    epipe 5500 customer 5 vpn 5500 create
        description "Distributed epipe service to east coast"
        sap 1/1/3.1:21 create
            ingress
                qos 555
            exit
            egress
                qos 627
            exit
        exit
    exit
...
-----
ALU-1>config>service#

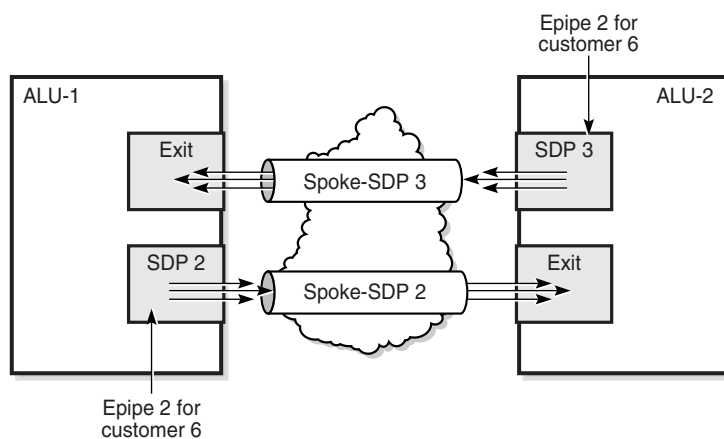
```

```
ALU-2>config>service# info
-----
...
    epipe 5500 customer 5 vpn 5500 create
        description "Distributed epipe service to west coast"
        sap 1/1/4.1:550 create
            ingress
                qos 654
            exit
            egress
                qos 432
            exit
        exit
    exit
ALU-2>config>service#
```

Configuring Epipe SDP Bindings

Figure 23 displays an example of a distributed Epipe service configuration between two routers, identifying the service and customer IDs and the unidirectional SDPs required to communicate to the far-end routers. The `spoke-sdp sdp-id:vc-id` must match on both sides.

Figure 23: SDPs — Unidirectional Tunnels



19484

Use the following CLI syntax to create a spoke SDP binding with an Epipe service. For SDP configuration information, see [Configuring SDPs on page 60](#).

CLI Syntax: config>service# epipe *service-id* [customer *customer-id*]
[create]

```

    spoke-sdp sdp-id:vc-id [vc-type {ether|vlan}]
    [create] vlan-vc-tag 0..4094
    egress
        vc-label egress-vc-label
    ingress
        vc-label ingress-vc-label
    no shutdown

```

Example: ALU-1>config>service# epipe 5500
 config>service>epipe# spoke-sdp 2:123
 config>service>epipe>spoke-sdp# egress
 config>service>epipe>spoke-sdp>egress# vc-label 5500
 config>service>epipe>spoke-sdp>egress# exit
 config>service>epipe>spoke-sdp# ingress
 config>service>epipe>spoke-sdp>ingress# vc-label 6600
 config>service>epipe>spoke-sdp>ingress# exit
 config>service>epipe>spoke-sdp# no shutdown

```

ALU-2>config>service# epipe 5500
config>service>epipe# spoke-sdp 2:123
config>service>epipe>spoke-sdp# egress
config>service>epipe>spoke-sdp>egress# vc-label 6600
config>service>epipe>spoke-sdp>egress# exit
config>service>epipe>spoke-sdp# ingress
config>service>epipe>spoke-sdp>ingress# vc-label 5500
config>service>epipe>spoke-sdp>ingress# exit
config>service>epipe>spoke-sdp# no shutdown

```

The following example displays the configuration output for binding an Epipe service between ALU-1 and ALU-2. This example assumes the SAPs have already been configured (see [Configuring Epipe SAP Parameters on page 150](#)).

```

ALU-1>config>service# info
-----
...
    epipe 5500 customer 5 vpn 5500 create
        description "Distributed epipe service to east coast"
        sap 1/1/3:21 create
            ingress
                qos 555
            exit
            egress
                qos 627
            exit
        exit
        spoke-sdp 2:123 create
            ingress
                vc-label 6600
            exit
            egress

```

```
vc-label 5500
exit
exit
no shutdown
exit
...
-----
ALU-1>config>service#

ALU-2>config>service# info
-----
...
exit
    epipe 5500 customer 5 vpn 5500 create
    description "Distributed epipe service to west coast"
    sap 1/1/4:550 create
    ingress
        qos 654
    exit
    egress
        qos 432
    exit
exit
spoke-sdp 2:123 create
    ingress
        vc-label 5500
    exit
    egress
        vc-label 6600
    exit
exit
no shutdown
exit
...
-----
```

Configuring Ingress and Egress SAP Parameters

By default, QoS policy ID 1 is applied to ingress and egress service SAPs. Existing QoS policies can be associated with service SAPs on ingress and egress ports.

Ingress and egress SAP parameters can be applied to distributed Epipe service SAPs, and to Apipe and Cpipe service SAPs.

Example:

```
ALU-1>config>service# epipe 5500
config>service>epipe# sap 1/1/3:21
config>service>epipe>sap# ingress
config>service>epipe>sap>ingress# qos 555
config>service>epipe>sap>ingress# exit
config>service>epipe>sap# egress
config>service>epipe>sap>egress# qos 627
config>service>epipe>sap>egress# exit
config>service>epipe>sap#
```

The following example displays the Epipe SAP ingress and egress configuration output.

```

ALU-1>config>service#
-----
...
    epipe 5500 customer 5 vpn 5500 create
        description "Distributed epipe service to east coast"
        sap 1/1/3:21 create
            ingress
                qos 555
            exit
            egress
                qos 627
            exit
        exit
    spoke-sdp 2:123 create
        ingress
            vc-label 6600
        exit
        egress
            vc-label 5500
        exit
    exit
    no shutdown
    exit
-----
ALU-1>config>service#

```

Using the Control Word

The control word is mandatory for Cpipe SAToP and CESoPSN configurations. It is optional for Apipe and Epipe configurations.

When the control word is enabled, the Admin Control Word is set to Preferred. Both sides of the VLL must be configured with a matching control word, either both enabled or both disabled, for the pipe to be up.

The control word state will be set to True or False depending on what is configured, either enabled (True) or disabled (False).

Example:

```

config>service# cpipe 2100 customer 1
config>service>cpipe$ description "Default cpipe
description for service id 2100"
config>service>cpipe$ sap 1/2/7.1:4 create
config>service>cpipe>sap$ description "Default sap
description for service id 2100"
config>service>cpipe>sap$ exit
config>service>cpipe# spoke-sdp 1:2001 create
config>service>cpipe>spoke-sdp$ control-word
config>service>cpipe>spoke-sdp$ exit
config>service>cpipe# no shutdown

```

The following example displays the control word configuration output for a Cpipe service.

```
*A:ALU-Dut-B>config>service>cpipe# info
-----
description "Default cpipe description for service id 2100"
sap 1/2/7.1:4 create
    description "Default sap description for service id 2100"
exit
spoke-sdp 1:2001 create
    control-word
exit
no shutdown
-----
*A:ALU-Dut-B>config>service>cpipe#
```

Control word cannot be disabled on Cpipe services. To disable the control word option on Apipe and Epipe services use the `no control-word` command.

Example: `config>service>apip# spoke-sdp 1:2001 no control-word`
 `config>service>apip>spoke-sdp$ exit`

Service Management Tasks

The service management tasks are similar for Apipe, Cpipe and Epipe services. This section discusses the following service management tasks:

- [Modifying Service Parameters](#)
- [Disabling a Service](#)
- [Re-enabling a Service](#)
- [Deleting a Service](#)

Modifying Service Parameters

Use the `show service service-using` command to display a list of configured VLL services.

To modify a VLL service:

1. Access the specific account by specifying the service ID.
2. Enter the service parameter to modify and then enter the new information.

PE router 1 (A:ALU-41):

Example:

```
A:ALU-41>config>service# apipe 5
A:ALU-41>config>service>apipe# sap 1/1/1.1:0/32 create
A:ALU-41>config>service>apipe>sap# accounting-policy 2
A:ALU-41>config>service>apipe>sap# exit
A:ALU-41>config>service>apipe# spoke-sdp 1:4
A:ALU-41>config>service>apipe>spoke-sdp# egress
A:ALU-41>config>service>apipe>spoke-sdp>egress# vc-label
2048
A:ALU-41>config>service>apipe>spoke-sdp>egress# exit
A:ALU-41>config>service>apipe>spoke-sdp# ingress
A:ALU-41>config>service>apipe>spoke-sdp>ingress# vc-label
18431
A:ALU-41>config>service>apipe>spoke-sdp>ingress# exit
A:ALU-41>config>service>apipe>spoke-sdp# exit
A:ALU-41>config>service>apipe#
```

PE router 2 (A:ALU-42):

Example:

```
A:ALU-42>config>service# apipe 5
A:ALU-42>config>service>apipe# sap 2/2/2.1:0/32 create
A:ALU-42>config>service>apipe>sap# accounting-policy 2
A:ALU-42>config>service>apipe>sap# exit
A:ALU-42>config>service>apipe# spoke-sdp 1:4
A:ALU-42>config>service>apipe>spoke-sdp# egress
A:ALU-42>config>service>apipe>spoke-sdp>egress# vc-label
18431
A:ALU-42>config>service>apipe>spoke-sdp>egress# exit
A:ALU-41>config>service>apipe>spoke-sdp# ingress
A:ALU-41>config>service>apipe>spoke-sdp>ingress# vc-label
2043
A:ALU-41>config>service>apipe>spoke-sdp>ingress# exit
A:ALU-42>config>service>apipe>spoke-sdp# exit
A:ALU-42>config>service>apipe#
```

The following example displays the configuration output when adding an accounting-policy to an existing SAP and modifying the spoke-sdp parameters on an existing Apipe service for PE Router 1 (ALU-41) and PE Router 2 (ALU-42).

Use a similar syntax to modify Cpipe and Epipe services.

```
A:ALU-41>config>service# info
-----
...
    apipe 5 customer 1 create
        description "apipe test"
        service-mtu 1400
        sap 1/1/1.1:0/32 create
            accounting-policy 2
            ingress
                qos 102
            exit
            egress
                qos 103
            exit
        exit
        spoke-sdp 1:4 create
            egress
                vc-label 2048
            ingress
                vc-label 18431
        exit
        no shutdown
    exit
...
-----
A:ALU-41>config>service#
```

```

A:ALU-42>config>service# info
-----
...
    apipe 5 customer 1 create
        description "apipe test"
        service-mtu 1400
        sap 2/2/2.1:0/32 create
            accounting-policy 2
            ingress
                qos 102
            exit
            egress
                qos 103
            exit
        exit
        spoke-sdp 1:4 create
            egress
                vc-label 18431
            ingress
                vc-label 2048
        exit
        no shutdown
    exit
...
-----
A:ALU-42>config>service#

```

Disabling a Service

A service can be shut down without deleting the service parameters.

Use the `shutdown` command to shut down a VLL service. The following CLI syntax displays the command to shut down an Apipe service. Use a similar syntax to shut down Cpipe and Epipe services.

CLI Syntax:

```

config>service#
    apipe service-id
        shutdown

```

PE router 1 (A:ALU-41):

Example:

```

A:ALU-41>config>service# apipe 5
A:ALU-41>config>service>apipe# shutdown
A:ALU-41>config>service>apipe# exit

```

PE router 2 (A:ALU-42):

Example:

```

A:ALU-42>config>service# apipe 5
A:ALU-42>config>service>apipe# shutdown
A:ALU-42>config>service>apipe# exit

```

The following example displays the configuration output for deleting an Apipe service on PE Router 1 (ALU-41) and PE Router 2 (ALU-42).

```
A:ALU-41>config>service# info
-----
...
    apipe 5 customer 1 create
        shutdown
        description "apipe test"
        service-mtu 1400
        sap 1/1/1.1:0/32 create
            accounting-policy 2
            ingress
                qos 102
            exit
            egress
                qos 103
            exit
        exit
        spoke-sdp 1:4 create
            egress
                vc-label 16
        exit
        no shutdown
    exit
...
-----
A:ALU-41>config>service#

A:ALU-42>config>service# info
-----
...
    apipe 5 customer 1 create
        shutdown
        description "apipe test"
        service-mtu 1400
        sap 2/2/2.1:0/32 create
            accounting-policy 2
            ingress
                qos 102
            exit
            egress
                qos 103
            exit
        exit
        spoke-sdp 1:4 create
            egress
                vc-label 16
        exit
    exit
...
-----
A:ALU-42>config>service#
```


Re-enabling a Service

Use the `no shutdown` command to re-enable a previously disabled VLL service. The following CLI syntax displays the command to re-enable an Apipe service. Use a similar syntax to re-enable Cpipe and Epipe services.

CLI Syntax: `config>service#
 apipe service-id
 no shutdown`

PE router 1 (A:ALU-41):

Example: `A:ALU-41>config>service# apipe 5
A:ALU-41>config>service>apipe# no shutdown
A:ALU-41>config>service>apipe# exit`

PE router 2 (A:ALU-42):

Example: `A:ALU-42>config>service# apipe 5
A:ALU-42>config>service>apipe# no shutdown
A:ALU-42>config>service>apipe# exit`

Deleting a Service

Use the `shutdown` command to delete a VLL service. The SAP, and any associated protocols and spoke-SDPs, must be deleted from the VLL service before the VLL service can be deleted.

Perform the following steps to delete a service:

1. Shut down the SAP and SDP.
2. Delete the SAP and SDP.
3. Shut down the service.

Use the following syntax to delete Apipe services. Use a similar syntax to delete Cpipe and Epipe services.

CLI Syntax:

```
config>service#
    apipe service-id
        sap sap-id
            shutdown
            exit
        no sap sap-id
        spoke-sdp [sdp-id:vc-id]
            shutdown
            exit
        no spoke-sdp [sdp-id:vc-id]
        shutdown
        exit
    no apipe service-id
```

Example:

```
A:ALU-41>config>service# apipe 5
A:ALU-41>config>service>apipe# sap 1/1/1.1:0/32
A:ALU-41>config>service>apipe>sap# shutdown
A:ALU-41>config>service>apipe>sap# exit
A:ALU-41>config>service>apipe# no sap 1/1/1.1:0/32
A:ALU-41>config>service>apipe# spoke-sdp 1:4
A:ALU-41>config>service>apipe>spoke-sdp# shutdown
A:ALU-41>config>service>apipe>spoke-sdp# exit
A:ALU-41>config>service>apipe# no spoke-sdp 1:4
A:ALU-41>config>service>apipe# shutdown
A:ALU-41>config>service>apipe# exit
A:ALU-41>config>service# no apipe 5
```

VLL Services Command Reference

Command Hierarchies

- [VLL Service Configuration Commands](#)
 - [Apipe Service Configuration Commands](#)
 - [Cpipe Service Configuration Commands](#)
 - [Epipe Service Configuration Commands](#)
- [Show Commands](#)
- [Clear Commands](#)

VLL Service Configuration Commands

Apipe Service Configuration Commands

```

config
  — service
    — apipe service-id [customer customer-id] [create] [vpn vpn-id] [vc-type {atm-vcc | atm-vpc}]
    — no apipe service-id
      — description description-string
      — no description
      — sap sap-id [create]
      — no sap sap-id
        — accounting-policy acct-policy-id
        — no accounting-policy
        — atm
          — egress
            — traffic-desc traffic-desc-profile-id
            — no traffic-desc
          — ingress
            — traffic-desc traffic-desc-profile-id
            — no traffic-desc
          — oam
            — [no] alarm-cells
        — [no] collect-stats
        — description description-string
        — no description
        — egress
          — qos policy-id
          — no qos
        — ingress
          — qos policy-id
          — no qos
        — [no] shutdown
      — service-mtu octets
      — no service-mtu
      — [no] shutdown

    — spoke-sdp sdp-id:vc-id [create] (see Note)
    — no spoke-sdp sdp-id:vc-id
      — cell-concatenation
        — [no] clp-change
        — max-cells cell-count
        — no max-cells [cell-count]
        — max-delay delay-time
        — no max-delay [delay-time]
      — [no] control-word
      — egress
        — vc-label egress-vc-label
        — no vc-label [egress-vc-label]
      — ingress
        — vc-label ingress-vc-label

```

- **no** **vc-label** *[ingress-vc-label]*
- **[no]** **shutdown**



Note: The spoke-sdp configuration does not apply to ATM SAP-to-SAP configuration (local service). It only applies to SAP-to-SDP configuration (distributed service).

Cpipe Service Configuration Commands

```

config
  — service
    — [no] cpipe service-id [customer customer-id] [create] [vpn vpn-id] [vc-type {satop-e1 | satop-t1 | cesopsn | cesopsn-cas}]
      — description description-string
      — no description
      — sap sap-id [create]
      — [no] sap sap-id
        — accounting-policy acct-policy-id
        — no accounting-policy
        — cem
        — [no] packet
          — [no] jitter-buffer jitter-buffer value | payload-size size
          — payload-size size
          — [no] report-alarm [stray] [malformed] [pktloss] [overrun] [underrun] [rpktloss] [rfault] [rrdi]
          — [no] rtp-header
        — [no] collect-stats
        — description description-string
        — no description
        — egress
          — qos policy-id
          — no qos
        — ingress
          — qos policy-id
          — no qos
        — [no] shutdown
      — service-mtu octets
      — no service-mtu
      — [no] shutdown

    — spoke-sdp sdp-id:vc-id [create] (see Note)
    — no spoke-sdp sdp-id:vc-id
      — control-word
      — [no] egress
        — [no] vc-label egress-vc-label
      — [no] ingress
        — [no] vc-label ingress-vc-label
      — [no] shutdown

```



Note: The spoke-sdp configuration does not apply to TDM SAP-to-SAP configuration (local service). It only applies to SAP-to-SDP configuration (distributed service).

Epipe Service Configuration Commands

```

config
  — service
    — [no] epipe service-id [customer customer-id] [create] [vpn vpn-id]
      — description description-string
      — no description
      — sap sap-id [create]
      — no sap sap-id
        — accounting-policy acct-policy-id
        — no accounting-policy
        — [no] collect-stats
        — description description-string
        — no description
        — egress
          — qos policy-id
          — no qos
        — ingress
          — qos policy-id
          — no qos
      — service-mtu octets
      — no service-mtu
      — [no] shutdown
      — spoke-sdp sdp-id:vc-id [vc-type {ether | vlan}] [create]
      — no spoke-sdp sdp-id:vc-id
        — [no] control-word
        — egress
          — vc-label egress-vc-label
          — no vc-label [egress-vc-label]
        — ingress
          — vc-label ingress-vc-label
          — no vc-label [ingress-vc-label]
      — vlan-vc-tag 0..4094
      — no vlan-vc-tag [0..4094]

```

Show Commands

```

show
  — service
    — egress-label start-label [end-label]
    — id service-id
      — all
      — base
      — labels
      — sap [sap-id] [detail]
      — sdp [sdp-id | far-end ip-address] [detail]
    — ingress-label start-label [end-label]
    — sap-using [sap sap-id]
    — sap-using [ingress | egress] atm-td-profile td-profile-id
    — sap-using [ingress | egress] qos-policy qos-policy-id

```

Clear Commands

```

clear
  — service
    — id service-id
      — spoke-sdp sdp-id:vc-id ingress-vc-label
    — statistics
      — id service-id
        — counters
        — spoke-sdp sdp-id:vc-id {all | counters}
      — sap sap-id {all | cem | counters}
      — sdp sdp-id keep-alive

```

VLL Service Configuration Commands

- [Generic Commands on page 169](#)
- [VLL Global Commands on page 171](#)
- [VLL SAP Commands on page 175](#)
- [SAP cem Commands on page 178](#)
- [Service Billing Commands on page 181](#)
- [SAP QoS Policy Commands on page 182](#)
- [VLL SDP Commands on page 184](#)
- [SDP Cell Concatenation Commands on page 187](#)
- [ATM Commands on page 190](#)
- [ATM OAM Commands on page 192](#)

Generic Commands

description

Syntax	description <i>description-string</i> no description
Context	config>service>apipe config>service>apipe>sap config>service>cpipe config>service>cpipe>sap config>service>epipe config>service>epipe>sap
Description	This command creates a text description stored in the configuration file for a configuration context. The no form of this command removes the string from the context.
Default	No description is associated with the configuration context.
Parameters	<i>description-string</i> — 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>service>apipe config>service>apipe>sap config>service>apipe>spoke-sdp config>service>cpipe config>service>cpipe>sap config>service>cpipe>spoke-sdp config>service>epipe

Description 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. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many objects must be shut down before they may be deleted. Many entities must be explicitly enabled using the **no shutdown** command.

The **no** form of this command places the entity into an administratively enabled state.

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities are described in the following Special Cases.

Special Cases

Service Admin State — bindings to an SDP within the service will be put into the out-of-service state when the service is shut down. While the service is shut down, all customer packets are dropped and counted as discards for billing and debugging purposes.

Service Operational State — a service is considered operational if at least one SAP and one SDP are operational.

SDP (global) — when an SDP is shut down at the global service level, all bindings to that SDP are put into the out-of-service state and the SDP itself is put into the administratively and operationally down states. Packets that would normally be transmitted using this SDP binding will be discarded and counted as dropped packets.

SDP (service level) — shutting down an SDP within a service only affects traffic on that service from entering or being received from the SDP. The SDP itself may still be operationally up for other services.

VLL Global Commands

apipe

Syntax	apipe <i>service-id</i> [customer <i>customer-id</i>] [create] [vpn <i>vpn-id</i>] [vc-type { <i>atm-vcc</i> <i>atm-vpc</i> }] no apipe <i>service-id</i>
Context	config>service
Description	This command configures a point-to-point ATM service. The Apipe service provides a point-to-point L2 VPN connection to a local or remote SAP. An Apipe can connect an ATM endpoint locally (in the same 7705 SAR) or over a PSN to a remote endpoint of the same type.
Parameters	<p><i>service-id</i> — uniquely identifies a service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The <i>service-id</i> must be the same number used for every 7705 SAR on which this service is defined.</p> <p>Values 1 to 2147483647</p> <p>customer <i>customer-id</i> — specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.</p> <p>Values 1 to 2147483647</p> <p>vpn <i>vpn-id</i> — specifies the VPN ID number which allows you to identify virtual private networks (VPNs) by a VPN identification number. If this parameter is not specified, the VPN ID uses the same service ID number.</p> <p>Values 1 to 2147483647</p> <p>Default null (0)</p> <p>vc-type — specifies a 15-bit value that defines the type of the VC signaled to the peer. Its values are defined in <i>draft-ietf-pwe3-iana-allocation</i> and it defines both the signaled VC type as well as the resulting datapath encapsulation over the Apipe.</p> <p>Values atm-vcc, atm-vpc</p> <p>Default atm-vcc</p>

cpipe

Syntax	[no] cpipe <i>service-id</i> [customer <i>customer-id</i>] [vpn <i>vpn-id</i>] [vc-type { <i>satop-e1</i> <i>satop-t1</i> <i>cesopsn</i> <i>cesopsn-cas</i> }]
Context	config>service
Description	This command configures a circuit emulation service utilizing MPLS or GRE encapsulation. The <i>vc-type</i> defines the type of unstructured or structured circuit emulation service to be configured. All other parameters (<i>service-id</i> , <i>customer</i>) have common usage with other service types.

Default	no cpipe
Parameters	<p><i>service-id</i> — uniquely identifies a service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The <i>service-id</i> must be the same number used for every 7705 SAR on which this service is defined.</p> <p>Values 1 to 2147483647</p> <p>customer <i>customer-id</i> — specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.</p> <p>Values 1 to 2147483647</p> <p>vpn <i>vpn-id</i> — specifies the VPN ID number which allows you to identify virtual private networks (VPNs) by a VPN identification number. If this parameter is not specified, the VPN ID uses the same service ID number.</p> <p>Values 1 to 2147483647</p> <p>Default null (0)</p> <p>vc-type — specifies a value that defines the type of the VC signaled to the peer. This optional parameter is included when the Cpipe service is created.</p> <p>Values satop-e1: unstructured E1 circuit emulation service satop-t1: unstructured DS1 circuit emulation service cesopsn: basic structured $n \times 64$ kb/s circuit emulation service cesopsn-cas: structured $n \times 64$ kb/s circuit emulation service with signaling</p> <p>Default cesopsn</p>

epipe

Syntax	[no] epipe <i>service-id</i> [customer <i>customer-id</i>] [vpn <i>vpn-id</i>]
Context	config>service
Description	<p>This command configures a point-to-point Ethernet service. An Epipe connects two endpoints defined as SAPs. Both SAPs are defined on separate routers (7705 SAR routers or other Alcatel-Lucent service routers) connected over the service provider network. When the endpoint SAPs are separated by the service provider network, the far-end SAP is generalized into an SDP. This SDP describes a destination 7705 SAR and the encapsulation method used to reach it.</p> <p>No MAC learning or filtering is provided (or needed) on an Epipe.</p> <p>When a service is created, the customer keyword and <i>customer-id</i> must be specified, which associates the service with a customer. The <i>customer-id</i> must already exist, having been created using the customer command in the service context. Once a service has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and recreated with a new customer association.</p>

Once a service is created, the use of the **customer** *customer-id* is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect *customer-id* specified will result in an error.

By default, Epipe services do not exist until they are explicitly created with this command.

The **no** form of this command deletes the Epipe service instance with the specified *service-id*. The service cannot be deleted until the service has been shut down.

Parameters	<i>service-id</i> — uniquely identifies a service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The <i>service-id</i> must be the same number used for every 7705 SAR on which this service is defined.
	Values 1 to 2147483647
	customer <i>customer-id</i> — specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.
	Values 1 to 2147483647
	vpn <i>vpn-id</i> — specifies the VPN ID number which allows you to identify virtual private networks (VPNs) by a VPN ID. If this parameter is not specified, the VPN ID uses the same service ID number.
	Values 1 to 2147483647
	Default null (0)

service-mtu

Syntax	service-mtu <i>octets</i> no service-mtu
Context	config>service>apipe config>service>cpipe config>service>epipe
Description	<p>This command configures the service payload (Maximum Transmission Unit – MTU), in octets, for the service. This MTU value overrides the service-type default MTU.</p> <p>The service-mtu defines the payload capabilities of the service. It is used by the system to validate the SAP and SDP binding's operational state within the service.</p> <p>The service MTU and a SAP's service delineation encapsulation overhead (4 bytes for a dot1q tag) is used to derive the required MTU of the physical port or channel on which the SAP was created. If the required payload is larger than the port or channel MTU, then the SAP will be placed in an inoperative state. If the required MTU is equal to or less than the port or channel MTU, the SAP will be able to transition to the operative state.</p>

When binding an SDP to a service, the service MTU is compared to the path MTU associated with the SDP. The path MTU can be administratively defined in the context of the SDP. The default or administrative path MTU can be dynamically reduced due to the MTU capabilities discovered by the tunneling mechanism of the SDP or the egress interface MTU capabilities based on the next hop in the tunnel path. If the service MTU is larger than the path MTU, the SDP binding for the service will be placed in an inoperative state. If the service MTU is equal to or less than the path MTU, then the SDP binding will be placed in an operational state.

In the event that a service MTU, port or channel MTU, or path MTU is dynamically or administratively modified, then all associated SAP and SDP binding operational states are automatically re-evaluated.

The **no** form of this command returns the default service-mtu for the indicated service type to the default value.

Parameters *octets* — specifies the size of the MTU, expressed as a decimal integer

Values 1 to 1514

Default apipe: 1508
cpipe: 1514
epipe: 1514

[Table 24](#) displays MTU values for specific VC types.

Table 24: Maximum Transmission Unit Values

VC-Type	Example of Service MTU	Advertised MTU
Ethernet	1514	1500
Ethernet (with preserved dot1q)	1518	1504
VLAN (dot1p transparent to MTU value)	1514	1500

VLL SAP Commands

sap

Syntax	sap <i>sap-id</i> [create] no sap <i>sap-id</i>
Context	config>service>apipe config>service>cpipe config>service>epipe
Description	<p>This command creates a SAP within a service. Each SAP must be unique.</p> <p>All SAPs must be explicitly created with the create keyword. If no SAPs are created within a service or on an IP interface, a SAP will not exist on that object.</p> <p>To edit SAP parameters, enter an existing SAP without the create keyword.</p> <p>A SAP can only be associated with a single service. The SAP is owned by the service in which it was created. A SAP can only be defined on a port that has been configured as an access port in the config>port <i>port-id</i> context using the mode access command. Fractional TDM ports are always access ports. Refer to the 7705 SAR OS Interface Configuration Guide.</p> <p>If a port is shut down, all SAPs on that port become operationally down. When a service is shut down, SAPs for the service are not displayed as operationally down although all traffic traversing the service will be discarded. The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.</p> <p>The following SAP types are supported:</p> <ul style="list-style-type: none"> • ATM VPI/VCI on an ATM port for vc-type atm-vcc • ATM VPI on an ATM port for vc-type atm-vpc • Ethernet-Ethernet • SAToP • CESoPSN (with and without CAS) <p>The no form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP will also be deleted.</p>
Default	No SAPs are defined.
Special Cases	<p>A default SAP has the following format: <i>port-id</i>:. This type of SAP is supported only on Ethernet Adapter cards and its creation is allowed only in the scope of Layer 2 Epipe services. This type of SAP is mutually exclusive with a SAP defined by explicit null encapsulation (m 1/1/1:0).</p>
Parameters	<i>sap-id</i> — specifies the physical port identifier portion of the SAP definition

The *sap-id* can be configured in one of the formats described in [Table 25](#).

Table 25: SAP ID Configurations

Type	Syntax	Example
port-id	<i>slot/mda/port[.channel]</i>	1/1/5
null	<i>[port-id bundle-id]</i>	<i>port-id</i> : 1/1/3 <i>bundle-id</i> : bundle-ppp-1/1.1
dot1q	<i>[port-id bundle-id]:qtag1</i>	<i>port-id</i> :qtag1: 1/1/3:100 <i>bundle-id</i> : bundle-ppp-1/1.1
atm	<i>[port-id bundle-id][:vpi/vci vpi]</i>	<i>port-id</i> : 1/1/1.1 <i>bundle-id</i> : bundle-ima-1/1.1 bundle-ppp-1/1.1 vpi/vci: 16/26 vpi: 16
cem	slot/mda/port.channel	1/1/1.3

Values	<i>sap-id</i> :	null	<i>[port-id bundle-id]</i>
		dot1q	<i>[port-id bundle-id]:qtag1</i>
		atm	<i>[port-id bundle-id][:vpi/vci vpi vpi1.vpi2]</i>
		port-id	<i>slot/mda/port[.channel]</i>
		bundle-type-slot/mda.bundle-num	
		bundle keyword	
		type ima, ppp	
		bundle-num 1 to 10	
		qtag1 0 to 4094	
		vpi NNI 0 to 4095	
		UNI 0 to 255	
		vci 1, 2, 5 to 65535	

port-id — specifies the physical port ID in the *slot/mda/port* format

If the card in the slot has an adapter card installed, the *port-id* must be in the slot_number/MDA_number/port_number format. For example 1/2/3 specifies port 3 on MDA 2 in slot 1.

The *port-id* must reference a valid port type. When the *port-id* parameter represents TDM channels, the port ID must include the channel ID. A period “.” separates the physical port from the *channel-id*. The port must be configured as an access port.

bundle-id — specifies the multilink bundle to be associated with this IP interface. The **bundle** keyword must be entered at the beginning of the parameter. The command syntax must be configured as follows:

bundle-id: **bundle-type-slot-id/mda-slot.bundle-num**
bundle-id value range: 1 to 10

For example:

```
*A:ALU-12>config# port bundle-ppp-5/1.1
*A:ALU-12>config>port# multilink-bundle
```

qtag1 — specifies the encapsulation value used to identify the SAP on the port or sub-port. If this parameter is not specifically defined, the default value is 0.

Values qtag1: 0 to 4094

The values depend on the encapsulation type configured for the interface. [Table 26](#) describes the allowed values for the port and encapsulation types.

Table 26: Port and Encapsulation Values

Port Type	Encap-Type	Allowed Values	Comments
Ethernet	Null	0	The SAP is identified by the port.
Ethernet	Dot1q	0 to 4094	The SAP is identified by the 802.1Q tag on the port. Note that a 0 qtag1 value also accepts untagged packets on the dot1q port.

create — keyword used to create a SAP instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

SAP cem Commands

cem

Syntax	cem
Context	config>service>cpipe>sap
Description	<p>This command configures the circuit emulation service parameters on a Cpipe.</p> <p>This command is blocked for all SAPs except for E1, DS1 and $n \times 64$ kb/s channels configured for encap-type cem.</p>

packet

Syntax	[no] packet
Context	config>service>cpipe>sap>cem
Description	This command enables the context to configure packet parameters on the SAP.

jitter-buffer

Syntax	[no] jitter-buffer <i>value</i> <i>payload-size size</i>
Context	config>service>cpipe>sap>cem>packet
Description	This command defines the size of the receive jitter buffer for the circuit emulation service SAP.
Default	<p>The default value varies depending on the SAP bandwidth, as follows:</p> <ul style="list-style-type: none"> • 5 ms, where SAP bandwidth ≥ 16 DS0s (1024 kb/s) • 8 ms, where SAP bandwidth is between 5 and 15 DS0s (between 320 and 960 kb/s) • 16 ms, where SAP bandwidth is between 2 and 4 DS0s (between 128 and 256 kb/s) • 32 ms, where SAP bandwidth = 1 DS0 (64 kb/s)
Parameters	<p><i>value</i> — This parameter describes the size of the receive jitter buffer, expressed in milliseconds. The range of supported values is 2 to 250 ms. The buffer size must be set to at least 2 times the value of the packetization delay and no greater than 32 times the value of the packetization delay.</p> <p>To calculate the size of the buffer (in bytes), multiply the value of the buffer size (in ms) by the SAP TDM bandwidth (in bits per second) and divide by 8. After the initialization of the circuit emulation service, transmission of TDM data begins when the buffer is half full (50%).</p>

size — For convenience, the payload size can be configured at the same time as the jitter buffer. This avoids any configuration errors due to interactions between the jitter buffer and payload size settings. See [payload-size](#).

payload-size

Syntax	payload-size size
Context	config>service>cpipe>sap>cem>packet
Description	This parameter defines the payload size for one circuit emulation service packet.
Default	For SAToP, see Table 13 . For CESoPSN without CAS, see Table 14 . For CESoPSN with CAS, see Table 15 .
Parameters	<p><i>size</i> — The bytes value defines the payload size (in octets) to be encapsulated in one circuit emulation service packet. The valid range of supported values is 2 to 1514 bytes. The packetization delay for the circuit emulation service can be calculated by multiplying the payload size (in octets) by 8 (bits/octet) and then dividing by the SAP TDM bandwidth (in bits per second).</p> <p>For CESoPSN with CAS, the configured value of the payload size does not need to include the extra bytes for the transport of CAS bits. The configured value of the service-mtu size must take the extra CAS bytes into account. See Structured E1 CES with CAS on page 107 for details.</p> <p>For CESoPSN, the payload size may be specified as the number of bytes to be included in the packet.</p> <p>For SAToP circuit emulation services, the payload size must be specified in multiples of 32 bytes. The minimum value is 64 bytes for both SAToP T1 and SAToP E1.</p> <p>Interactions — The jitter-buffer value must be greater than or equal to twice the payload size to ensure that a frame arrives prior to the start of play-out. Therefore, the payload size may have to be decreased prior to setting the jitter-buffer value. Alternatively, the jitter-buffer value may have to be increased prior to setting the payload-size.</p>

report-alarm

Syntax	[no] report-alarm [stray] [malformed] [pktloss] [overrun] [underrun] [rpktloss] [rfault] [rrdi]
Context	config>service>cpipe>sap>cem
Description	This command enables or disables alarm reporting for CES circuit alarm conditions.
Default	<p>On: stray, malformed, pktloss, overrun and underun</p> <p>Off: rpktloss, rfault, rrdi</p>
Parameters	<p>stray — reports the reception of packets not destined for this CES circuit</p> <p>malformed — reports the reception of packets not properly formatted as CES packets</p>

pktloss — reports the lack of reception of CES packets

overrun — reports the reception of too many CES packets resulting in an overrun of the receive jitter buffer

underrun — reports the reception of too few CES packets resulting in an underrun of the receive jitter buffer

rpktloss — reports that the remote peer is currently in packet loss status

rfault — reports that the remote TDM interface is currently not in service

rrdi — reports that the remote TDM interface is currently in RDI status

rtp-header

Syntax	[no] rtp-header
Context	config>service>cpipe>sap>cem
Description	This optional command inserts RTP headers operating in absolute mode in the CES packets. The no form of this command will not insert RTP headers into CES packets.
Default	no rtp-header

Service Billing Commands

accounting-policy

Syntax	accounting-policy <i>acct-policy-id</i> no accounting-policy
Context	config>service>apipe>sap config>service>cpipe>sap config>service>epipe>sap
Description	<p>This command creates the accounting policy context that can be applied to a SAP.</p> <p>An accounting policy must be defined before it can be associated with a SAP. If the <i>policy-id</i> does not exist, an error message is generated.</p> <p>A maximum of one accounting policy can be associated with a SAP at one time. Accounting policies are configured in the config>log context.</p> <p>The no form of this command removes the accounting policy association from the SAP, and the accounting policy reverts to the default.</p>
Default	no accounting-policy
Parameters	<i>acct-policy-id</i> — enter the accounting <i>policy-id</i> as configured in the config>log>accounting-policy context
Values	1 to 99

collect-stats

Syntax	[no] collect-stats
Context	config>service>apipe>sap config>service>cpipe>sap config>service>epipe>sap
Description	<p>This command enables accounting and statistical data collection for the SAP. When applying accounting policies, the data, by default, is collected in the appropriate records and written to the designated billing file.</p> <p>When the no collect-stats command is issued, the statistics are still accumulated by the CSM cards. However, the CPU will not obtain the results and write them to the billing file. If a subsequent collect-stats command is issued, then the counters written to the billing file include all the traffic while the no collect-stats command was in effect.</p>
Default	collect-stats

SAP QoS Policy Commands

egress

Syntax	egress
Context	config>service>apipe>sap config>service>cpipe>sap config>service>epipe>sap
Description	This command enables the context to configure egress SAP Quality of Service (QoS) policies. If no sap-egress QoS policy is defined, the system default sap-egress QoS policy is used for egress processing.

ingress

Syntax	ingress
Context	config>service>apipe>sap config>service>cpipe>sap config>service>epipe>sap
Description	This command enables the context to configure ingress SAP QoS policies. If no sap-ingress QoS policy is defined, the system default sap-ingress QoS policy is used for ingress processing.

qos

Syntax	qos <i>policy-id</i> no qos
Context	config>service>apipe>sap>egress config>service>apipe>sap>ingress config>service>cpipe>sap>egress config>service>cpipe>sap>ingress config>service>epipe>sap>egress config>service>epipe>sap>ingress
Description	This command associates a QoS policy with an ingress or egress SAP. QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP. If the <i>policy-id</i> does not exist, an error will be returned.

The **qos** command is used to associate both ingress and egress QoS policies. The **qos** command only allows ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP at one time. Attempts to associate a second QoS policy of a given type will return an error.

By default, no specific QoS policy is associated with the SAP for ingress or egress, so the default QoS policy is used.

The **no** form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

Parameters *policy-id* — Associates the ingress or egress policy ID with the SAP on ingress or egress. The policy ID must already exist.

Values 1 to 65535

VLL SDP Commands

spoke-sdp

Syntax	spoke-sdp <i>sdp-id[:vc-id]</i> [create] spoke-sdp <i>sdp-id[:vc-id]</i> [vc-type { ether vlan }] [create] no spoke-sdp <i>sdp-id[:vc-id]</i>
Context	config>service>apipe config>service>cpipe config>service>epipe
Description	<p>This command binds a service to an existing Service Destination Point (SDP).</p> <p>A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke SDPs or SAPs) and not transmitted on the port it was received.</p> <p>The SDP has an operational state that determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.</p> <p>The SDP must already be defined in the config>service>sdp context in order to associate an SDP with an Epipe service. If the sdp <i>sdp-id</i> is not already configured, an error message is generated. If the <i>sdp-id</i> does exist, a binding between that <i>sdp-id</i> and the service is created.</p> <p>SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end 7705 SAR devices can participate in the service.</p> <p>The no form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.</p>
Default	No <i>sdp-id</i> is bound to a service.
Parameters	<p><i>sdp-id</i> — uniquely identifies the SDP</p> <p>Values 1 to 17407</p> <p><i>vc-id</i> — identifies the virtual circuit</p> <p>Values 1 to 4294967295</p> <p>vc-type — for Epipe services, this command overrides the default VC type signaled for the spoke binding to the far end of the SDP. The VC type is a 15-bit quantity containing a value which represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the vc-type command can still be used to define the dot1q value expected by the far-end provider equipment. A change of the binding’s VC type causes the binding to signal the new VC type to the far end when signaling is enabled.</p>

VC types are derived according to IETF *draft-martini-l2circuit-trans-mpls*.

- The VC type value for Ethernet is 0x0005.
- The VC type value for an Ethernet VLAN is 0x0004.

Values ether | vlan

ether — for Epipe services, this parameter defines the VC type as Ethernet. The **ethernet** and **vlan** keywords are mutually exclusive. When the VC type is not defined, then the default is Ethernet for spoke SDP bindings. Defining Ethernet is the same as executing **no vc-type** and restores the default VC type for the spoke SDP binding.

vlan — for Epipe services, this parameter defines the VC type as VLAN. The **ethernet** and **vlan** keywords are mutually exclusive. When the VC type is not defined, then the default is Ethernet for spoke SDP bindings. The VLAN VC-type requires at least one dot1Q tag within each encapsulated Ethernet packet transmitted to the far end.

vc-label

Syntax	[no] vc-label egress-vc-label
Context	config>service>apipe>spoke-sdp>egress config>service>cpipe>spoke-sdp>egress config>service>epipe>spoke-sdp>egress
Description	This command configures the egress VC label.
Parameters	<i>egress-vc-label</i> — indicates a specific connection
Values	16 to 1048575

vc-label

Syntax	[no] vc-label ingress-vc-label
Context	config>service>apipe>spoke-sdp>ingress config>service>cpipe>spoke-sdp>ingress config>service>epipe>spoke-sdp>ingress
Description	This command configures the ingress VC label.
Parameters	<i>ingress-vc-label</i> — indicates a specific connection
Values	2048 to 18431

vlan-vc-tag

Syntax	vlan-vc-tag <i>0..4094</i> no vlan-vc-tag [<i>0..4094</i>]
Context	config>service>epipe>spoke-sdp
Description	<p>This command specifies an explicit dot1q value used when encapsulating to the SDP far end. When signaling is enabled between the near and far end, the configured dot1q tag can be overridden by a received TLV specifying the dot1q value expected by the far end. This signaled value must be stored as the remote signaled dot1q value for the binding. The provisioned local dot1q tag must be stored as the administrative dot1q value for the binding.</p> <p>When the dot1q tag is not defined, the default value of zero is stored as the administrative dot1q value. Setting the value to zero is equivalent to not specifying the value.</p> <p>The no form of this command disables the command</p>
Default	no vlan-vc-tag
Parameters	<i>0..4094</i> — specifies a valid VLAN identifier to bind an 802.1Q VLAN tag ID

SDP Cell Concatenation Commands

cell-concatenation

Syntax	cell-concatenation
Context	config>service>apipe>spoke-sdp
Description	This command enables the context to provide access to the various options that control the termination of ATM cell concatenation into an MPLS frame. Several options can be configured simultaneously. The concatenation process for a given MPLS packet ends when the first concatenation termination condition is met. The concatenation parameters apply only to ATM N-to-1 cell mode VLL.

In Release 1.1, frame boundaries are not configurable.

clp-change

Syntax	[no] clp-change
Context	config>service>apipe>spoke-sdp>cell-concatenation
Description	This command enables the configuration of CLP change to be an indication to complete the cell concatenation operation.

The **no** form of the command resets the configuration to ignore the CLP change as an indication to complete the cell concatenation.

control-word

Syntax	control-word no control-word
Context	config>service>apipe>spoke-sdp config>service>cpipe>spoke-sdp config>service>epipe>spoke-sdp
Description	This command indicates whether the control word is used or not. The value of the control word is negotiated with the peer.

This command is mandatory for SAToP and CESoPSN encapsulation.

egress

Syntax	[no] egress
Context	config>service>apipe>spoke-sdp config>service>cpipe>spoke-sdp config>service>epipe>spoke-sdp
Description	This command configures the egress SDP context.

ingress

Syntax	[no] ingress
Context	config>service>apipe>spoke-sdp config>service>cpipe>spoke-sdp config>service>epipe>spoke-sdp
Description	This command configures the ingress SDP context.

max-cells

Syntax	max-cells <i>cell-count</i> no max-cells [<i>cell-count</i>]
Context	config>service>apipe>spoke-sdp>cell-concatenation
Description	<p>This command enables the configuration of the maximum number of ATM cells to accumulate in an MPLS packet. The remote peer will also signal the maximum number of concatenated cells it is willing to accept in an MPLS packet. When the lesser of the configured value and the signaled value is reached, the MPLS packet is queued for transmission onto the pseudowire. It is ensured that the MPLS packet MTU conforms to the configured service MTU.</p> <p>If the max-delay and jitter buffer options are not configured, then the maximum number of cells allowed in a single VLL frame must be less than the configured service-mtu size.</p> <p>The no form of this command sets max-cells to the value “1”, indicating that no concatenation will be performed.</p>
Parameters	<i>cell-count</i> — specifies the maximum number of ATM cells to be accumulated in an MPLS packet before queuing the packet for transmission onto the pseudowire
Values	1 to 29
Default	29

max-delay

Syntax	max-delay <i>delay-time</i> no max-delay [<i>delay-time</i>]				
Context	config>service>apipe>spoke-sdp>cell-concatenation				
Description	<p>This command enables the configuration of the maximum amount of time to wait while performing ATM cell concatenation into an MPLS packet before transmitting the MPLS packet. This places an upper bound on the amount of delay introduced by the concatenation process. When this amount of time is reached from when the first ATM cell for this MPLS packet was received, the MPLS packet is queued for transmission onto the pseudowire.</p> <p>The no form of this command resets max-delay to its default value.</p>				
Parameters	<p><i>delay-time</i> — specifies the maximum amount of time, in hundreds of microseconds, to wait before transmitting the MPLS packet with whatever ATM cells have been received. For example, to bound the delay to 1 ms, the user would configure 10 (hundreds of microseconds). The delay-time is rounded up to one of the following values 1, 5, 10, 50, 100, 200, 300 and 400.</p> <table><tr><td>Values</td><td>1 to 400</td></tr><tr><td>Default</td><td>400, which represents 40 ms of delay time (400 units of hundreds of microseconds)</td></tr></table>	Values	1 to 400	Default	400, which represents 40 ms of delay time (400 units of hundreds of microseconds)
Values	1 to 400				
Default	400, which represents 40 ms of delay time (400 units of hundreds of microseconds)				

ATM Commands

atm

Syntax	atm
Context	config>service>apipe>sap
Description	<p>This command enables access to the context to configure ATM-related attributes. This command can only be used when a given context (for example, a channel or SAP) supports ATM functionality such as:</p> <ul style="list-style-type: none"> • configuring ATM port or ATM port-related functionality on T1/E1 ASAP Adapter cards • configuring ATM-related configuration for ATM-based SAPs that exist on T1/E1 ASAP Adapter cards <p>If ATM functionality is not supported for a given context, the command returns an error.</p>

egress

Syntax	egress
Context	config>service>apipe>sap>atm
	This command provides access to the context to configure egress ATM traffic policies for the SAP.

ingress

Syntax	ingress
Context	config>service>apipe>sap>atm
Description	This command provides access to the context to configure ingress ATM traffic policies for the SAP.

traffic-desc

Syntax	traffic-desc <i>traffic-desc-profile-id</i> no traffic-desc
Context	config>service>apipe>sap>atm>egress config>service>apipe>sap>atm>ingress
Description	This command assigns an ATM traffic descriptor profile to a given context (for example, a SAP).

When configured under the ingress context, the specified traffic descriptor profile defines the traffic contract in the forward direction.

When configured under the egress context, the specified traffic descriptor profile defines the traffic contract in the backward direction.

The **no** form of the command reverts the traffic descriptor to the default traffic descriptor profile.

Default The default traffic descriptor (trafficDescProfileId. = 1) is associated with newly created PVCC-delimited SAPs.

Parameters *traffic-desc-profile-id* — specifies a defined traffic descriptor profile (see the QoS **atm-td-profile** command)

ATM OAM Commands

oam

Syntax	oam
Context	config>service>apipe>sap>atm
Description	<p>This command enables the context to configure OAM functionality for a PVCC delimiting a SAP.</p> <p>The T1/E1 ASAP Adapter card supports the generation of F4 (VP) and F5 (VC) AIS cells when Apipe service is operationally down. When Apipe service is operationally up, OAM cells are transported over Apipe and transparent to the 7705 SAR. This capability is in accordance with ITU-T Recommendation I.610 - B-ISDN Operation and Maintenance.</p>

alarm-cells

Syntax	[no] alarm-cells
Context	config>service>apipe>sap>atm>oam
Description	<p>This command configures AIS/RDI fault management on a PVCC. Fault management allows PVCC terminations to monitor and report the status of their connection by propagating fault information through the network and by driving the PVCC's operational status.</p> <p>The 7705 SAR Apipe does not support PVCC terminations. Instead, it allows OAM cells to be transported transparently from end-to-end. When this command is enabled, AIS cells are generated when an Apipe or corresponding SAP is operationally down.</p> <p>The no command disables alarm-cells functionality for the Apipe. When alarm-cells functionality is disabled, AIS cells are not generated as result of the Apipe or corresponding SAP going into the operationally down state.</p>
Default	enabled

Show Commands

all

Syntax	all
Context	show>service>id
Description	This command displays detailed information for all aspects of the service.
Output	Show Service-ID All Output — The following table describes the show service-id all command output fields.

Table 27: Show Service-ID All Command Output Fields

Label	Description
Service Detailed Information	
Service Id	Identifies the service by its ID number
VPN Id	Identifies the VPN by its ID number
Service Type	Specifies the type of service
VLL Type	Specifies the VLL type
Description	Displays generic information about the service
Customer Id	Identifies the customer by its ID number
Last Status Change	Displays the date and time of the most recent status change to this service
Last Mgmt Change	Displays the date and time of the most recent management-initiated change to this service
Admin State	Specifies the desired state of the service
Oper State	Specifies the operating state of the service
MTU	Specifies the service MTU
SAP Count	Displays the number of SAPs specified for this service
SDP Bind Count	Displays the number of SDPs bound to this service

Table 27: Show Service-ID All Command Output Fields (Continued)

Label	Description
Service Destination Points (SDPs)	
Description	Displays generic information about the SDP
SDP Id	Identifies the SDP
Type	Identifies the service SDP binding type (for example, spoke)
VC Type	Displays the VC type for the SDP (for example, CESoPSN)
VC Tag	The explicit dot1Q value used when encapsulating to the SDP far end
Admin Path MTU	Specifies the desired largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented
Oper Path MTU	Specifies the actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented
Far End	Displays the IP address of the remote end of the MPLS or GRE tunnel defined by this SDP
Delivery	Specifies the type of delivery used by the SDP (MPLS or GRE)
Admin State	Specifies the administrative state of this SDP
Oper State	Specifies the operational state of this SDP
Acct. Pol	The accounting policy ID assigned to the SAP
Collect Stats	Specifies whether collect stats is enabled
Ingress Label	Displays the label used by the far-end device to send packets to this device in this service by this SDP
Egress Label	Displays the label used by this device to send packets to the far-end device in this service by this SDP
Admin ControlWord	Specifies the administrative state of the control word: Preferred (control word enabled) or Not Preferred (control word disabled)
Oper ControlWord	Specifies the operational state of the control word: True (control word enabled) or False (control word disabled)
Last Status Change	Specifies the time of the most recent operating status change to this spoke SDP

Table 27: Show Service-ID All Command Output Fields (Continued)

Label	Description
Signaling	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP
Last Mgmt Change	Specifies the time of the most recent management-initiated change to this spoke SDP
Flags	Displays the conditions that affect the operating status of this spoke SDP. Display output includes PathMTUtooSmall, SdpOperDown, NoIngVCLabel, NoEgrVCLabel, and so on
Mac Move	Indicates the administrative state of the MAC movement feature associated with the service
Peer Pw Bits	Displays the setting of the pseudowire peer bits. Display output includes pwNotforwarding, psnIngressFault, psnEgressFault, lacIngressFault, lacEgressFault
Peer Fault Ip	N/A
Peer Vccv CV Bits	Displays the setting of the pseudowire peer VCCV control verification bits (lspPing)
Peer Vccv CC Bits	Displays the setting of the pseudowire peer VCCV control channel bits (pwe3ControlWord and/or mplsRouterAlertLabel)
Keepalive Information	
Admin State	Specifies the administrative state of the keepalive protocol
Oper State	Specifies the operational state of the keepalive protocol
Hello Time	Specifies how often the SDP Echo Request messages are transmitted on this SDP
Hello Msg Len	Specifies the length of the SDP Echo Request messages transmitted on this SDP
Max Drop Count	Specifies the maximum number of consecutive SDP Echo Request messages that can be unacknowledged before the keepalive protocol reports a fault
Hold Down Time	Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state
Statistics	
I. Fwd. Pkts.	Specifies the number of forwarded ingress packets
I. Dro. Pkts.	Specifies the number of dropped ingress packets

Table 27: Show Service-ID All Command Output Fields (Continued)

Label	Description
I. Fwd. Octs.	Specifies the number of forwarded ingress octets
I. Dro. Octs.	Specifies the number of dropped ingress octets
E. Fwd. Pkts.	Specifies the number of forwarded egress packets
E. Fwd. Octets	Specifies the number of forwarded egress octets
Associated LSP LIST	
Lsp Name	Specifies the name of the static LSP
Admin State	Specifies the administrative state of the associated LSP
Oper State	Specifies the operational state of the associated LSP
Time Since Last Tr*	Specifies the time that the associated static LSP has been in-service
APIPE Service Destination Point specifics	
Admin Concat Limit	Specifies the administrative (configured) value for the maximum number of cells for cell concatenation, as defined via the <code>max-cells</code> command
Oper Concat Limit	Specifies the operational value for the maximum number of cells for cell concatenation
Peer Concat Limit	Specifies the far-end value for the maximum number of cells for cell concatenation
Max Concat Delay	Specifies the amount of time to wait while cell concatenation is occurring, as defined via the <code>max-delay</code> command
CPIPE Service Destination Point specifics	
Local Bit-rate	Specifies the number of DS0s used by the local SDP
Peer Bit-rate	Specifies the number of DS0s used by the far-end SDP
Local Payload Size	Specifies the local payload size, in bytes, used by the local SDP
Peer Payload Size	Specifies the peer payload size, in bytes, used by the far-end SDP
Local Sig Pkts	Specifies the type of signaling packets used by the local SDP
Peer Sig Pkts	Specifies the type of signaling packets used by the far-end SDP
Local CAS Framing	Specifies the type of CAS framing used by the local SDP
Peer CAS Framing	Specifies the type of CAS framing used by the far-end SDP

Table 27: Show Service-ID All Command Output Fields (Continued)

Label	Description
Local RTP Header	Specifies whether the local router inserts the RTP header
Peer RTP Header	Specifies whether the peer router inserts the RTP header
Number of SDPs	Specifies the number of SDPs bound to the service
Service Access Points	
Service Id	Identifies the service
SAP	Specifies the ID of the access port where this SAP is defined
Encap	Specifies the encapsulation type for this SAP on the access port
Admin State	Specifies the desired state of the SAP
Oper State	Specifies the operating state of the SAP
Flags	Specifies the conditions that affect the operating status of this SAP. Display output includes ServiceAdminDown, PortOperDown, and so on.
Last Status Change	Specifies the date and time of the most recent status change to this SAP
Last Mgmt Change	Specifies the date and time of the most recent management-initiated change to this SAP
Dot1Q Ethertype	Identifies the value of the dot1q Ethertype
LLF Admin State	Specifies the Link Loss Forwarding administrative state
LLF Oper State	Specifies the Link Loss Forwarding operational state
Admin MTU	Specifies the desired largest service frame size (in octets) that can be transmitted through this SAP to the far-end router, without requiring the packet to be fragmented
Oper MTU	Specifies the actual largest service frame size (in octets) that can be transmitted through this SAP to the far-end router, without requiring the packet to be fragmented
Ingr IP Fltr-ID	Specifies the ingress IP filter policy ID assigned to the SAP
Egr IP Fltr-Id	Specifies the egress IP filter policy ID assigned to the SAP
Ingr Mac Fltr-ID	Specifies the ingress MAC filter policy ID assigned to the SAP
Egr Mac Fltr-Id	Specifies the egress MAC filter policy ID assigned to the SAP
Acct. Pol	Specifies the accounting policy applied to the SAP

Table 27: Show Service-ID All Command Output Fields (Continued)

Label	Description
Collect Stats	Specifies whether accounting statistics are collected on the SAP
QoS	
Ingress qos-policy	Displays the SAP ingress QoS policy ID
Egress qos-policy	Displays the SAP egress QoS policy ID
SAP Statistics	
Last Cleared Time	Displays the date and time that a clear command was issued on statistics
Forwarding Engine Stats	
Dropped	Indicates the number of packets or octets dropped by the forwarding engine
Off. HiPrio	Indicates the number of high-priority packets or octets offered to the forwarding engine
Off. LowPrio	Indicates the number of low-priority packets offered to the forwarding engine
Queueing Stats (Ingress QoS Policy)	
Dro. HiPrio	Indicates the number of high-priority packets or octets discarded, as determined by the SAP ingress QoS policy
Dro. LowPrio	Indicates the number of low-priority packets discarded, as determined by the SAP ingress QoS policy
For. InProf	Indicates the number of in-profile packets or octets (rate below CIR) forwarded, as determined by the SAP ingress QoS policy
For. OutProf	Indicates the number of out-of-profile packets or octets (rate above CIR) forwarded, as determined by the SAP ingress QoS policy

Table 27: Show Service-ID All Command Output Fields (Continued)

Label	Description
Queueing Stats (Egress QoS Policy)	
Dro. InProf	Indicates the number of in-profile packets or octets discarded, as determined by the SAP egress QoS policy
Dro. OutProf	Indicates the number of out-of-profile packets or octets discarded, as determined by the SAP egress QoS policy
For. InProf	Indicates the number of in-profile packets or octets (rate below CIR) forwarded, as determined by the SAP egress QoS policy
For. OutProf	Indicates the number of out-of-profile packets or octets (rate above CIR) forwarded, as determined by the SAP egress QoS policy
Sap per Queue stats	
Ingress Queue <i>n</i>	Specifies the index of the ingress QoS queue of this SAP, where <i>n</i> is the index number
Off. HiPrio	Indicates the packets or octets count of the high-priority traffic for the SAP (offered)
Off. LoPrio	Indicates the packets or octets count of the low-priority traffic for the SAP (offered)
Dro. HiPrio	Indicates the number of high-priority traffic packets/octets dropped
Dro. LoPrio	Indicates the number of low-priority traffic packets/octets dropped
For. InProf	Indicates the number of in-profile packets or octets (rate below CIR) forwarded
For. OutPro	Indicates the number of out-of-profile octets (rate above CIR) forwarded
Egress Queue <i>n</i>	Specifies the index of the egress QoS queue of the SAP, where <i>n</i> is the index number
For. InProf	Indicates the number of in-profile packets or octets (rate below CIR) forwarded
For. OutProf	Indicates the number of out-of-profile packets or octets (rate above CIR) forwarded
Dro. InProf	Indicates the number of in-profile packets or octets dropped for the SAP

Table 27: Show Service-ID All Command Output Fields (Continued)

Label	Description
Dro. OutProf	Indicates the number of out-of-profile packets or octets discarded
ATM SAP Configuration Information	
Ingress TD Profile	The profile ID of the traffic descriptor applied to the ingress SAP
Egress TD Profile	The profile ID of the traffic descriptor applied to the egress SAP
Alarm Cell Handling	Indicates that OAM cells are being processed
OAM Termination	Indicates whether this SAP is an OAM termination point
CEM SAP Configuration Information	
Endpoint Type	Specifies the type of endpoint
Bit-rate	Specifies the number of DS0s or timeslots in the channel group
Payload Size	Specifies the number of octets contained in the payload of a TDM PW packet when the packet is transmitted
Jitter Buffer	Specifies the size of the receive jitter buffer, expressed in milliseconds
Use RTP Header	Specifies whether RTP headers are used in CES packets (Yes or No)
CAS Framing	Specifies the type of CAS framing
Effective PVDT	Displays the peak-to-peak packet delay variation (PDV) used by the circuit emulation service. Since the operating system may adjust the jitter buffer setting in order to ensure no packet loss, the configured jitter buffer value may not be the value used by the system. The effective PVDT provides an indication that the PVD has been adjusted by the operating system (see Jitter Buffer on page 110)
Cfg Alarm	Specifies the alarms that have alarm reporting enabled
Alarm Status	Indicates the current alarm state (for example, stray, malformed, packet loss, overrun, underrun, remote packet loss, remote fault, or remote RDI)

Table 27: Show Service-ID All Command Output Fields (Continued)

Label	Description
CEM SAP Statistics	
Packets	(Column heading) Displays the number of packets counted for the statistic since the last counter reset
Seconds	(Column heading) Displays the number of seconds elapsed for the statistic since the last counter reset
Events	(Column heading) Displays the number of events counted for the statistic since the last counter reset
Egress Stats	Indicates that the following statistics are egress statistics
Forwarded	Displays the number of forwarded packets
Missing	Displays the number of missing packets
Reordered and Forwarded	Displays the number of packets that have been reordered and forwarded
Underrun	Displays the accumulated number of underrun packets for the number of underrun events
Overrun	Displays the accumulated number of overrun packets for the number of overrun events
Misordered Dropped	Displays the number of misordered packets that have been dropped
Malformed Dropped	Displays the number of malformed packets that have been dropped
Error	Displays the accumulated number of seconds that have passed while any error has occurred
Severely Error	Displays the accumulated number of seconds that have passed while severe errors has occurred
Unavailable	Displays the accumulated number of seconds that have passed while the Cpipe is unavailable
Failure Count	Displays the accumulated number of failed events
Ingress Stats	Indicates that the following statistics are ingress statistics
Forwarded	Displays the number of forwarded packets
Dropped	Displays the number of dropped packets

The following CLI sample outputs are shown:

- [Sample Output \(Apipe ATMVcc service\)](#)
- [Sample Output \(Apipe ATMVpc service\)](#)
- [Sample Output \(Cpipe service\)](#)
- [Sample Output \(Epipe service\)](#)

Sample Output (Apipe ATMVcc service)

```
=====
*A:ALU-A>show>service# id 2 all
=====
Service Detailed Information
=====
Service Id      : 2                Vpn Id          : 0
Service Type    : Apipe            VLL Type        : ATMVCC
Customer Id     : 2
Last Status Change: 03/11/2008 19:58:19
Last Mgmt Change  : 03/28/2008 19:49:51
Admin State     : Down              Oper State       : Down
MTU              : 1508
Vc Switching    : False
SAP Count       : 1                SDP Bind Count   : 1
-----
Service Destination Points (SDPs)
-----
Sdp Id 2:2  -(138.120.38.1)
-----
SDP Id          : 2:2                Type            : Spoke
VC Type         : ATMVCC             VC Tag          : 0
Admin Path MTU  : 0                  Oper Path MTU    : 0
Far End         : 138.120.38.1       Delivery         : MPLS

Admin State     : Up                  Oper State       : Down
Acct. Pol       : None                Collect Stats    : Disabled
Ingress Label   : 0                  Egress Label     : 0
Ing mac Fltr    : n/a                Egr mac Fltr     : n/a
Ing ip Fltr     : n/a                Egr ip Fltr      : n/a
Admin ControlWord : Not Preferred    Oper ControlWord : False
Admin BW(Kbps)  : 0                  Oper BW(Kbps)    : 0
Last Status Change : 03/11/2008 19:58:19
Last Mgmt Change  : 03/28/2008 19:49:51
Signaling       : TLDP
Endpoint        : N/A                Precedence       : 4
Class Fwding State : Down
Flags           : SdpOperDown SdpOperDown
                  NoIngVCLabel NoEgrVCLabel
                  PathMTUTooSmall
Mac Move        : Ukwn                Blockable Level  : Unknown
Peer Pw Bits    : None
Peer Fault Ip   : None
Peer Vccv CV Bits : None
Peer Vccv CC Bits : None
```

```

KeepAlive Information :
Admin State           : Disabled           Oper State           : Disabled
Hello Time            : 10                 Hello Msg Len        : 0
Max Drop Count        : 3                 Hold Down Time       : 10

```

```

Statistics           :
I. Fwd. Pkts.        : 0                 I. Dro. Pkts.        : 0
I. Fwd. Octs.         : 0                 I. Dro. Octs.        : 0
E. Fwd. Pkts.        : 0                 E. Fwd. Octets       : 0

```

```

Associated LSP LIST :
No LSPs Associated

```

APIPE Service Destination Point specifics

```

Admin Concat Limit : 1                 Oper Concat Limit : 1
Peer Concat Limit  : n/a              Max Concat Delay  : 400

```

Number of SDPs : 1

Service Access Points

SAP 1/4/1.1:0/32

```

Service Id           : 2
SAP                  : 1/4/1.1:0/32      Encap                : atm
Admin State          : Up                Oper State            : Down
Flags                : ServiceAdminDown  PortOperDown L2OperDown
Multi Svc Site       : None
Last Status Change   : 03/11/2008 19:58:19
Last Mgmt Change     : 03/28/2008 19:35:51
Sub Type             : regular

Admin MTU            : 1572              Oper MTU              : 1572
Ingr IP Fltr-Id      : n/a              Egr IP Fltr-Id       : n/a
Ingr Mac Fltr-Id     : n/a              Egr Mac Fltr-Id      : n/a
tod-suite            : None              qinq-pbit-marking    : both
Egr Agg Rate Limit   : max
Endpoint             : N/A

Acct. Pol            : None              Collect Stats         : Disabled

```

QOS

```

Ingress qos-policy   : 1                 Egress qos-policy    : 1
Shared Q plcy        : n/a              Multipoint shared    : Disabled

```

Sap Statistics

```

Last Cleared Time     : N/A

```

Packets

Octets

Show Commands

```
Forwarding Engine Stats
Dropped          : 0                      n/a
Off. HiPrio      : 39192                  n/a
Off. LowPrio     : n/a                    n/a

Queueing Stats(Ingress QoS Policy 1)
Dro. HiPrio      : 0                      n/a
Dro. LowPrio     : n/a                    n/a
For. InProf      : 19596                  19596
For. OutProf     : 19596                  19596

Queueing Stats(Egress QoS Policy 1)
Dro. InProf      : 0                      n/a
Dro. OutProf     : n/a                    n/a
For. InProf      : 39192                  39192
For. OutProf     : n/a                    n/a
-----
Sap per Queue stats
-----
                                Packets      Octets

Ingress Queue 1 (Unicast) (Priority)
Off. HiPrio      : 39192                  n/a
Off. LoPrio      : n/a                    n/a
Dro. HiPrio      : 0                      n/a
Dro. LoPrio      : n/a                    n/a
For. InProf      : 19596                  19596
For. OutProf     : 19596                  19596

Egress Queue 1
For. InProf      : 39192                  39192
For. OutProf     : n/a                    n/a
Dro. InProf      : 0                      n/a
Dro. OutProf     : n/a                    n/a
-----
ATM SAP Configuration Information
-----
Ingress TD Profile : 1                      Egress TD Profile : 1
Alarm Cell Handling: Enabled                AAL-5 Encap       : n/a
OAM Termination   : Disabled                Periodic Loopback : Disabled
-----
Service Endpoints
-----
No Endpoints found.
=====
```

Sample Output (Apipe ATMVpc service)

```
=====
*A:ALU-A>show>service# id 5 all

Service Detailed Information
=====
Service Id      : 5                      Vpn Id          : 5
Service Type    : Apipe                  VLL Type        : ATMVPC
Customer Id     : 2
```

```

Last Status Change: 03/11/2008 19:58:19
Last Mgmt Change  : 04/01/2008 16:51:59
Admin State       : Down                Oper State       : Down
MTU               : 1508
Vc Switching     : False
SAP Count        : 1                    SDP Bind Count   : 1
-----
Service Destination Points (SDPs)
-----
Sdp Id 5:5  -(138.120.20.1)
-----
SDP Id           : 5:5                    Type            : Spoke
VC Type         : ATMVPC                  VC Tag          : 0
Admin Path MTU  : 0                      Oper Path MTU   : 0
Far End        : 138.120.20.1             Delivery        : MPLS

Admin State     : Up                      Oper State      : Down
Acct. Pol      : None                    Collect Stats   : Disabled
Ingress Label   : 0                      Egress Label    : 0
Ing mac Fltr    : n/a                    Egr mac Fltr   : n/a
Ing ip Fltr     : n/a                    Egr ip Fltr    : n/a
Admin ControlWord : Not Preferred        Oper ControlWord : False
Admin BW(Kbps)  : 0                      Oper BW(Kbps)   : 0
Last Status Change : 03/11/2008 19:58:19 Signaling       : TLDP
Last Mgmt Change  : 04/01/2008 16:51:59
Endpoint       : N/A                      Precedence      : 4
Class Fwding State : Down
Flags          : SdpOperDown SdpOperDown
                  NoIngVCLabel NoEgrVCLabel
                  PathMTUTooSmall

Mac Move       : Ukwn                    Blockable Level  : Unknown
Peer Pw Bits   : None
Peer Fault Ip  : None
Peer Vccv CV Bits : None
Peer Vccv CC Bits : None

KeepAlive Information :
Admin State     : Disabled                Oper State      : Disabled
Hello Time     : 10                      Hello Msg Len   : 0
Max Drop Count : 3                       Hold Down Time  : 10

Statistics      :
I. Fwd. Pkts.   : 0                      I. Dro. Pkts.   : 0
I. Fwd. Octs.   : 0                      I. Dro. Octs.   : 0
E. Fwd. Pkts.   : 0                      E. Fwd. Octets  : 0

Associated LSP LIST :
No LSPs Associated

-----
APIPE Service Destination Point specifics
-----
Admin Concat Limit : 1                    Oper Concat Limit : 1
Peer Concat Limit  : n/a                  Max Concat Delay  : 400
-----
Number of SDPs : 1
-----

```

Show Commands

----- Service Access Points -----

----- SAP 1/4/14.1:55 -----

Service Id	: 5		
SAP	: 1/4/14.1:55	Encap	: atm
Admin State	: Up	Oper State	: Down
Flags	: ServiceAdminDown PortOperDown L2OperDown		
Multi Svc Site	: None		
Last Status Change	: 03/11/2008 19:58:19		
Last Mgmt Change	: 04/01/2008 17:03:42		
Sub Type	: regular		
Admin MTU	: 1572	Oper MTU	: 1572
Ingr IP Fltr-Id	: n/a	Egr IP Fltr-Id	: n/a
Ingr Mac Fltr-Id	: n/a	Egr Mac Fltr-Id	: n/a
tod-suite	: None	qinq-pbit-marking	: both
Egr Agg Rate Limit	: max		
Endpoint	: N/A		
Acct. Pol	: None	Collect Stats	: Disabled

----- QoS -----

Ingress qos-policy	: 1	Egress qos-policy	: 1
Shared Q plcy	: n/a	Multipoint shared	: Disabled

----- Sap Statistics -----

Last Cleared Time : N/A

	Packets	Octets
Forwarding Engine Stats		
Dropped	: 0	n/a
Off. HiPrio	: 30	n/a
Off. LowPrio	: n/a	n/a

Queueing Stats(Ingress QoS Policy 1)

Dro. HiPrio	: 0	n/a
Dro. LowPrio	: n/a	n/a
For. InProf	: 15	15
For. OutProf	: 15	15

Queueing Stats(Egress QoS Policy 1)

Dro. InProf	: 0	n/a
Dro. OutProf	: n/a	n/a
For. InProf	: 30	30
For. OutProf	: n/a	n/a

----- Sap per Queue stats -----

	Packets	Octets
Ingress Queue 1 (Unicast) (Priority)		

```

Off. HiPrio      : 30          n/a
Off. LoPrio      : n/a         n/a
Dro. HiPrio      : 0           n/a
Dro. LoPrio      : n/a         n/a
For. InProf      : 15          15
For. OutProf     : 15          15

```

```

Egress Queue 1
For. InProf      : 30          30
For. OutProf     : n/a         n/a
Dro. InProf      : 0           n/a
Dro. OutProf     : n/a         n/a

```

ATM SAP Configuration Information

```

Ingress TD Profile : 1          Egress TD Profile : 1
Alarm Cell Handling: Enabled
OAM Termination    : Disabled   Periodic Loopback : Disabled

```

Service Endpoints

No Endpoints found.

```
*A:ALU-A>show>service#
```

Sample Output (Cpipe service)

```

=====
*A:ALU-A>show>service# id 51 all

```

Service Detailed Information

```

Service Id      : 51          Vpn Id      : 0
Service Type    : Cpipe       VLL Type    : CESoPSN
Description     : Henry Cpipe
Customer Id     : 2
Last Status Change: 03/11/2008 19:58:19
Last Mgmt Change  : 03/31/2008 20:41:13
Admin State     : Down        Oper State    : Down
MTU             : 1514
Vc Switching    : False
SAP Count       : 1          SDP Bind Count : 1

```

Service Destination Points (SDPs)

```
Sdp Id 51:51 - (138.120.38.1)
```

```

SDP Id      : 51:51          Type      : Spoke
VC Type     : CESoPSN       VC Tag    : 0
Admin Path MTU : 0          Oper Path MTU : 0
Far End      : 138.120.38.1 Delivery    : MPLS

Admin State  : Up           Oper State   : Down
Acct. Pol    : None        Collect Stats : Disabled

```

Show Commands

```
Ingress Label      : 0
Ing mac Fltr       : n/a
Ing ip Fltr        : n/a
Admin ControlWord  : Preferred
Admin BW(Kbps)     : 0
Last Status Change : 03/11/2008 19:58:19
Last Mgmt Change   : 03/31/2008 20:41:13
Endpoint           : N/A
Class Fwding State : Down
Flags              : SdpOperDown SdpOperDown
                   : NoIngVCLabel NoEgrVCLabel
                   : PathMTUTooSmall
Mac Move           : Ukwn
Peer Pw Bits       : None
Peer Fault Ip      : None
Peer Vccv CV Bits  : None
Peer Vccv CC Bits  : None

Egress Label       : 0
Egr mac Fltr       : n/a
Egr ip Fltr        : n/a
Oper ControlWord    : True
Oper BW(Kbps)       : 0
Signaling           : TLDP
Precedence          : 4
Blockable Level     : Unknown

KeepAlive Information :
Admin State          : Disabled
Hello Time           : 100
Max Drop Count       : 3
Oper State           : Disabled
Hello Msg Len        : 0
Hold Down Time       : 10

Statistics           :
I. Fwd. Pkts.        : 0
I. Fwd. Octs.         : 0
E. Fwd. Pkts.        : 0
I. Dro. Pkts.         : 0
I. Dro. Octs.         : 0
E. Fwd. Octets        : 0

Associated LSP LIST :
No LSPs Associated
```

----- CPIPE Service Destination Point specifics -----

```
Local Bit-rate      : 10
Local Payload Size   : 160
Local Sig Pkts       : No Sig.
Local CAS Framing    : No CAS
Local RTP Header     : Yes
Local Differential    : No
Local Timestamp      : 0
Peer Bit-rate        : n/a
Peer Payload Size    : n/a
Peer Sig Pkts        : No Sig.
Peer CAS Framing     : No CAS
Peer RTP Header      : No
Peer Differential     : No
Peer Timestamp       : 0
```

Number of SDPs : 1

----- Service Access Points -----

----- SAP 1/4/5.1 -----

```
Service Id          : 51
SAP                  : 1/4/5.1
Admin State          : Up
Flags                : ServiceAdminDown
                   : PortOperDown
Multi Svc Site       : None
Last Status Change   : 03/11/2008 19:58:19
Encap                 : cem
Oper State           : Down
```


Last Mgmt Change : 03/31/2008 21:38:50
 Sub Type : regular

Admin MTU	: 1572	Oper MTU	: 1572
Ingr IP Fltr-Id	: n/a	Egr IP Fltr-Id	: n/a
Ingr Mac Fltr-Id	: n/a	Egr Mac Fltr-Id	: n/a
tod-suite	: None	qinq-pbit-marking	: both
Egr Agg Rate Limit	: max		
Endpoint	: N/A		

Acct. Pol : Default Collect Stats : Enabled

 QOS

Ingress qos-policy	: 1	Egress qos-policy	: 1
Shared Q plcy	: n/a	Multipoint shared	: Disabled

 Sap Statistics

 Last Cleared Time : N/A

	Packets	Octets
Forwarding Engine Stats		
Dropped	: 0	0
Off. HiPrio	: 0	0
Off. LowPrio	: n/a	n/a

Queueing Stats(Ingress QoS Policy 1)

Dro. HiPrio	: 0	0
Dro. LowPrio	: n/a	n/a
For. InProf	: 0	0
For. OutProf	: 0	0

Queueing Stats(Egress QoS Policy 1)

Dro. InProf	: n/a	n/a
Dro. OutProf	: n/a	n/a
For. InProf	: n/a	n/a
For. OutProf	: n/a	n/a

 Sap per Queue stats

	Packets	Octets
Ingress Queue 1 (Unicast) (Priority)		
Off. HiPrio	: 0	0
Off. LoPrio	: n/a	n/a
Dro. HiPrio	: 0	0
Dro. LoPrio	: n/a	n/a
For. InProf	: 0	0
For. OutProf	: 0	0
Egress Queue 1		
For. InProf	: n/a	n/a
For. OutProf	: n/a	n/a
Dro. InProf	: n/a	n/a
Dro. OutProf	: n/a	n/a

 CEM SAP Configuration Information

Show Commands

```
-----
Endpoint Type   : NxDS0                      Bit-rate       : 10
Payload Size    : 160                        Jitter Buffer   : 8
Use RTP Header  : Yes                        Differential    : No
Timestamp Freq  : 0                          CAS Framing     : No CAS
Effective PDVT  : +/-4

Cfg Alarm       : stray malformed pktloss overrun underrun
Alarm Status    :
-----

CEM SAP Statistics
-----

                Packets          Seconds          Events
Egress Stats
Forwarded       : 0
Dropped         : 0
Missing         : 0
Reordered Forwarded : 0
Underrun        : 0                                0
Overrun         : 0                                0
Misordered Dropped : 0
Malformed Dropped : 0
LBit Dropped    : 0
Multiple Dropped : 0
Error           :                                0
Severely Error  :                                0
Unavailable     :                                0
Failure Count   :                                0

Ingress Stats
Forwarded       : 0
Dropped         : 0
-----

Service Endpoints
-----

No Endpoints found.
=====
```

Sample Output (Epipe service)

```
=====
*A:ALU-A>show>service# id 101 all

=====
Service Detailed Information
=====
Service Id      : 101                      Vpn Id         : 101
Service Type    : Epipe
Customer Id     : 2
Last Status Change: 03/11/2008 19:58:19
Last Mgmt Change : 03/31/2008 18:35:46
Admin State     : Down                      Oper State      : Down
MTU             : 1514
Vc Switching    : False
SAP Count       : 1                        SDP Bind Count  : 1
-----

Service Destination Points (SDPs)
```

```
-----
Sdp Id 99:99  -(138.120.38.1)
-----
```

```
SDP Id           : 99:99                      Type           : Spoke
VC Type          : Ether                      VC Tag          : n/a
Admin Path MTU   : 1512                      Oper Path MTU   : 1512
Far End          : 138.120.38.1              Delivery        : MPLS

Admin State      : Up                        Oper State       : Down
Acct. Pol        : None                     Collect Stats    : Disabled
Ingress Label    : 0                        Egress Label     : 0
Ing mac Fltr     : n/a                     Egr mac Fltr    : n/a
Ing ip Fltr      : n/a                     Egr ip Fltr     : n/a
Admin ControlWord : Not Preferred           Oper ControlWord : False
Admin BW(Kbps)   : 0                        Oper BW(Kbps)    : 0
Last Status Change : 03/11/2008 19:58:19    Signaling        : TLDP
Last Mgmt Change  : 03/31/2008 18:40:29    Force Vlan-Vc    : Disabled
Endpoint         : N/A                      Precedence       : 4
Class Fwding State : Down
Flags            : SdpOperDown SdpOperDown
                  NoIngVCLabel NoEgrVCLabel
                  PathMTUTooSmall

Mac Move         : Ukwn                      Blockable Level  : Unknown
Peer Pw Bits     : None
Peer Fault Ip    : None
Peer Vccv CV Bits : None
Peer Vccv CC Bits : None
```

```
KeepAlive Information :
Admin State           : Disabled              Oper State           : Disabled
Hello Time            : 10                    Hello Msg Len        : 0
Max Drop Count        : 3                     Hold Down Time       : 10
```

```
Statistics           :
I. Fwd. Pkts.        : 0                      I. Dro. Pkts.        : 0
I. Fwd. Octs.         : 0                      I. Dro. Octs.        : 0
E. Fwd. Pkts.        : 0                      E. Fwd. Octets       : 0
```

```
Associated LSP LIST :
No LSPs Associated
```

```
-----
Number of SDPs : 1
-----
```

```
-----
Service Access Points
-----
```

```
-----
SAP 1/3/1
-----
```

```
Service Id        : 101
SAP                : 1/3/1                      Encap              : null
Admin State       : Down                        Oper State         : Down
Flags             : ServiceAdminDown SapAdminDown
                  PortOperDown
Multi Svc Site    : None
Last Status Change : 03/11/2008 19:58:19
```

Show Commands

Last Mgmt Change : 03/31/2008 17:56:05
Sub Type : regular
Dot1Q Ethertype : 0x8100 QinQ Ethertype : 0x8100

LLF Admin State : Down LLF Oper State : Clear
Admin MTU : 1514 Oper MTU : 1514
Ingr IP Fltr-Id : n/a Egr IP Fltr-Id : n/a
Ingr Mac Fltr-Id : n/a Egr Mac Fltr-Id : n/a
tod-suite : None qinq-pbit-marking : both
Egr Agg Rate Limit : max
Endpoint : N/A
Q Frame-Based Acct : Disabled
Vlan-translation : None

Acct. Pol : Default Collect Stats : Enabled

----- QoS

Ingress qos-policy : 1 Egress qos-policy : 1
Shared Q plcy : n/a Multipoint shared : Disabled

Sap Statistics

Last Cleared Time : N/A

	Packets	Octets
Forwarding Engine Stats		
Dropped	: 0	0
Off. HiPrio	: 0	0
Off. LowPrio	: 0	0

Queueing Stats(Ingress QoS Policy 1)

Dro. HiPrio	: 0	0
Dro. LowPrio	: 0	0
For. InProf	: 0	0
For. OutProf	: 0	0

Queueing Stats(Egress QoS Policy 1)

Dro. InProf	: 0	0
Dro. OutProf	: 0	0
For. InProf	: 0	0
For. OutProf	: 0	0

----- Sap per Queue stats

	Packets	Octets
Ingress Queue 1 (Unicast) (Priority)		
Off. HiPrio	: 0	0
Off. LoPrio	: 0	0
Dro. HiPrio	: 0	0
Dro. LoPrio	: 0	0
For. InProf	: 0	0
For. OutProf	: 0	0
Egress Queue 1		
For. InProf	: 0	0
For. OutProf	: 0	0

```

Dro. InProf      : 0                      0
Dro. OutProf     : 0                      0

```

```

-----
Service Endpoints
-----

```

```

No Endpoints found.
=====

```

base

Syntax	base
Context	show>service>id
Description	This command displays basic information about the service specified by the ID, including service type, description, SAPs and SDPs.
Output	Show Service-ID Base — The following table describes show service-id base output fields.

Table 28: Show Service-ID Base Output Fields

Label	Description
Service Basic Information	
Service Id	Identifies the service by its ID number
VPN Id	Identifies the VPN by its ID number
Service Type	Specifies the type of service
VLL Type	Specifies the VLL type
Description	Displays generic information about the service
Customer Id	Identifies the customer by its ID number
Last Status Change	Displays the date and time of the most recent status change to this service
Last Mgmt Change	Displays the date and time of the most recent management-initiated change to this service
Admin State	Specifies the desired state of the service
Oper State	Specifies the operating state of the service
MTU	Specifies the service MTU
SAP Count	Displays the number of SAPs specified for this service
SDP Bind Count	Displays the number of SDPs bound to this service

Table 28: Show Service-ID Base Output Fields (Continued)

Label	Description
Service Access and Destination Points	
Identifier	Lists the SAP and SDP
Type	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on the SDP
AdmMTU	Specifies the desired largest service frame size (in octets) that can be transmitted through this SDP to the far-end edge services router (ESR), without requiring the packet to be fragmented
OprMTU	Specifies the actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end ESR, without requiring the packet to be fragmented
Adm	Indicates the operating state of the SAP or SDP
Opr	Indicates the operating state of the SAP or SDP

Sample Output (Apipe ATMVcc base)

```

=====
*A:ALU-12# show service id 701 base

=====
Service Basic Information
=====
Service Id       : 701                Vpn Id           : 701
Service Type     : Apipe              VLL Type          : ATMVCC
Description      : Default apipe description for service id 701
Customer Id      : 1
Last Status Change: 02/10/2008 03:30:03
Last Mgmt Change  : 02/10/2008 03:35:10
Admin State      : Up                  Oper State         : Down
MTU              : 1508
Vc Switching     : False
SAP Count        : 1                  SDP Bind Count     : 1

-----
Service Access & Destination Points
-----
Identifier                Type      AdmMTU  OprMTU  Adm    Opr
-----
sap:1/1/9.1:10/50         atm       1572   1572    Up     Down
sdp:101:701 S(10.20.1.3)  n/a       0      1514    Up     Up
-----
[<sap-id>] indicates a Managed SAP
=====

```

egress-label

Syntax	egress-label <i>start-label</i> [<i>end-label</i>]
Context	show>service
Description	<p>This command displays services using the range of egress labels.</p> <p>If only the mandatory <i>start-label</i> parameter is specified, only services using the specified label are displayed.</p> <p>If both <i>start-label</i> and <i>end-label</i> parameters are specified, the services using this range of labels are displayed.</p> <p>Use the show router ldp bindings command to display dynamic labels.</p>
Parameters	<p><i>start-label</i> — indicates the starting egress label value for which to display services using the label range. If only <i>start-label</i> is specified, services only using <i>start-label</i> are displayed.</p> <p>Values 0, 2048 to 131071</p> <p><i>end-label</i> — indicates the ending egress label value for which to display services using the label range</p> <p>Default the <i>start-label</i> value</p> <p>Values 2049 to 131071</p>
Output	Show Service Egress Command Output — The following table describes show service egress label output fields.

Table 29: Show Service Egress Label Output Fields

Label	Description
Svc Id	Identifies the service
Sdp Binding	Identifies the SDP
Type	Specifies the SDP binding type (for example, spoke)
I. Lbl	Displays the VC label used by the far-end device to send packets to this device in this service by the SDP
E. Lbl	Displays the VC label used by this device to send packets to the far-end device in this service by the SDP
Number of bindings found	Indicates the total number of SDP bindings that exist within the specified egress label range

Sample Output

```

=====
*A:ALU-12# show service egress-label 0 131071
=====
Martini Service Labels
=====

```

Svc Id	Sdp Binding	Type	I.Lbl	E.Lbl
1	101:1	Spok	131049	0
103	101:103	Spok	131067	131067
104	301:104	Spok	131066	131067
105	501:105	Spok	131065	131068
303	101:303	Spok	131064	131066
304	301:304	Spok	131063	131064
305	501:305	Spok	131062	131065
701	101:701	Spok	131059	131064
702	101:702	Spok	131058	131063
703	501:703	Spok	131057	131064
704	501:704	Spok	131056	131063
705	301:705	Spok	131055	131062
706	301:706	Spok	131054	131061
805	201:805	Spok	131053	131062
806	201:806	Spok	131052	131061
807	401:807	Spok	131051	131060
808	401:808	Spok	131050	131059
903	201:903	Spok	131061	131065
904	401:904	Spok	131060	131063

```

-----
Number of Bindings Found : 19
-----

```

id

Syntax `id service-id`

Context `show>service`

Description This command displays information for a particular service-id.

Parameters *service-id* — identifies the service in the domain

ingress-label

Syntax `ingress-label start-label [end-label]`

Context `show>service`

Description This command displays services using the range of ingress labels.

If only the mandatory *start-label* parameter is specified, only services using the specified label are displayed.

If both *start-label* and *end-label* parameters are specified, the services using this range of labels are displayed.

Use the **show router vprn-service-id ldp bindings** command to display dynamic labels.

Parameters *start-label* — indicates the starting ingress label value for which to display services using the label range. If only *start-label* is specified, services only using *start-label* are displayed.

Values 0, 2048 to 131071

end-label — indicates the ending ingress label value for which to display services using the label range

Default the *start-label* value

Values 2049 to 131071

Output **Show Service Ingress-Label** — The following table describes show service ingress-label output fields:

Table 30: Show Service Ingress Label Output Fields

Label	Description
Svc ID	Identifies the service
SDP Binding	Identifies the SDP
Type	Specifies the SDP binding type (for example, spoke)
I.Lbl	Displays the ingress label used by the far-end device to send packets to this device in this service by the SDP
E.Lbl	Displays the egress label used by this device to send packets to the far-end device in this service by the SDP
Number of Bindings Found	Indicates the number of SDP bindings within specified the label range

Sample Output

```
*A:ALU-12# show service ingress-label 0
=====
Martini Service Labels
=====
Svc Id      Sdp Binding      Type  I.Lbl      E.Lbl
-----
100         300:100          Spok  0           0
200         301:200          Spok  0           0
300         302:300          Spok  0           0
400         400:400          Spok  0           0
-----
Number of Bindings Found : 4
-----
*A:ALU-12#
```

labels

Syntax	labels
Context	show>service>id
Description	This command displays the labels being used by the service.
Output	Show Service-ID Labels — The following table describes show service-id labels output fields:

Table 31: Service-ID Labels Output Fields

Label	Description
Svc Id	Identifies the service
Sdp Binding	Identifies the SDP bound to the service
Type	Indicates the SDP binding type (for example, spoke)
I. Lbl	Displays the VC label used by the far-end device to send packets to this device in this service by the SDP
E. Lbl	Displays the VC label used by this device to send packets to the far-end device in this service by the SDP

Sample Output

```
*A:ALU-12# show service id 1 labels
=====
Martini Service Labels
=====
Svc Id      Sdp Binding      Type      I.Lbl      E.Lbl
-----
1           10:1             Spok      0           0
-----
Number of Bound SDPs : 1
-----
*A:ALU-12#
```

sap

Syntax	sap sap-id [detail]
Context	show>service>id
Description	This command displays information for the SAPs associated with the service. If no optional parameters are specified, a summary of all associated SAPs is displayed.
Parameters	<i>sap-id</i> — identifies the SAPs for the service in the form <i>slot/mda/port[.channel]</i> detail — displays detailed information for the SAP

Output **Show Service-ID SAP** — The following table describes show service SAP fields:

Table 32: SAP Fields

Label	Description
Service Access Points	
Service Id	Identifies the service
SAP	Specifies the ID of the access port where this SAP is defined
Encap	Specifies the encapsulation type for this SAP on the access port
Admin State	Specifies the desired state of the SAP
Oper State	Specifies the operating state of the SAP
Flags	Specifies the conditions that affect the operating status of this SAP. Display output includes ServiceAdminDown, PortOperDown, and so on
Last Status Change	Specifies the date and time of the most recent status change to this SAP
Last Mgmt Change	Specifies the date and time of the most recent management-initiated change to this SAP
Dot1Q Ethertype	Identifies the value of the dot1q Ethertype
LLF Admin State	Specifies the Link Loss Forwarding administrative state
LLF Oper State	Specifies the Link Loss Forwarding operational state
Admin MTU	Specifies the desired largest service frame size (in octets) that can be transmitted through this SAP to the far-end router, without requiring the packet to be fragmented
Oper MTU	Specifies the actual largest service frame size (in octets) that can be transmitted through this SAP to the far-end router, without requiring the packet to be fragmented
Ingr IP Fltr-Id	Specifies the ingress IP filter policy ID assigned to the SAP
Egr IP Fltr-Id	Specifies the egress IP filter policy ID assigned to the SAP
Ingr Mac Fltr-Id	Specifies the ingress MAC filter policy ID assigned to the SAP
Egr Mac Fltr-Id	Specifies the egress MAC filter policy ID assigned to the SAP
Acct. Pol	Specifies the accounting policy applied to the SAP
Collect Stats	Specifies whether accounting statistics are collected on the SAP

Table 32: SAP Fields (Continued)

Label	Description
QoS	
Ingress qos-policy	Displays the SAP ingress QoS policy ID
Egress qos-policy	Displays the SAP egress QoS policy ID
SAP Statistics	
Last Cleared Time	Displays the date and time that a clear command was issued on statistics
Forwarding Engine Stats	
Dropped	Indicates the number of packets or octets dropped by the forwarding engine
Off. HiPrio	Indicates the number of high-priority packets or octets offered to the forwarding engine
Off. LowPrio	Indicates the number of low-priority packets offered to the forwarding engine
Queueing Stats (Ingress QoS Policy)	
Dro. HiPrio	Indicates the number of high-priority packets or octets discarded, as determined by the SAP ingress QoS policy
Dro. LowPrio	Indicates the number of low-priority packets discarded, as determined by the SAP ingress QoS policy
For. InProf	Indicates the number of in-profile packets or octets (rate below CIR) forwarded, as determined by the SAP ingress QoS policy
For. OutProf	Indicates the number of out-of-profile packets or octets (rate above CIR) forwarded, as determined by the SAP ingress QoS policy
Queueing Stats (Egress QoS Policy)	
Dro. InProf	Indicates the number of in-profile packets or octets discarded, as determined by the SAP egress QoS policy
Dro. OutProf	Indicates the number of out-of-profile packets or octets discarded, as determined by the SAP egress QoS policy
For. InProf	Indicates the number of in-profile packets or octets (rate below CIR) forwarded, as determined by the SAP egress QoS policy
For. OutProf	Indicates the number of out-of-profile packets or octets (rate above CIR) forwarded, as determined by the SAP egress QoS policy

Table 32: SAP Fields (Continued)

Label	Description
Sap per Queue stats	
Ingress Queue n	Specifies the index of the ingress QoS queue of this SAP, where n is the index number
Off. HiPrio	Indicates the number of packets or octets of high-priority traffic for the SAP (offered)
Off. LoPrio	Indicates the number or packets or octets of low-priority traffic for the SAP (offered)
Dro. HiPrio	Indicates the number of high-priority traffic packets or octets dropped
Dro. LoPrio	Indicates the number of low-priority traffic packets or octets dropped
For. InProf	Indicates the number of in-profile packets or octets (rate below CIR) forwarded
For. OutProf	Indicates the number of out-of-profile packets or octets (rate above CIR) forwarded
Egress Queue n	Specifies the index of the egress QoS queue of the SAP, where n is the index number
For. InProf	Indicates the number of in-profile packets or octets (rate below CIR) forwarded
For. OutProf	Indicates the number of out-of-profile packets or octets (rate above CIR) forwarded
Dro. InProf	Indicates the number of in-profile packets or octets dropped for the SAP
Dro. OutProf	Indicates the number of out-of-profile packets or octets discarded
ATM SAP Configuration Information	
Ingress TD Profile	The profile ID of the traffic descriptor applied to the ingress SAP
Egress TD Profile	The profile ID of the traffic descriptor applied to the egress SAP
Alarm Cell Handling	Indicates that OAM cells are being processed
OAM Termination	Indicates whether this SAP is an OAM termination point

Table 32: SAP Fields (Continued)

Label	Description
CEM SAP Configuration Information	
Endpoint Type	Specifies the type of endpoint
Bit-rate	Specifies the number of DS0s or timeslots in the channel group
Payload Size	Specifies the number of octets contained in the payload of a TDM PW packet when the packet is transmitted
Jitter Buffer	Specifies the size of the receive jitter buffer, expressed in milliseconds
Use RTP Header	Specifies whether RTP headers are used in CES packets (Yes or No)
CAS Framing	Specifies the type of CAS framing
Effective PVDT	Displays the peak-to-peak packet delay variation (PDV) used by the circuit emulation service. Since the operating system may adjust the jitter buffer setting in order to ensure no packet loss, the configured jitter buffer value may not be the value used by the system. The effective PVDT provides an indication that the PVD has been adjusted by the operating system (see Jitter Buffer on page 110)
Cfg Alarm	Specifies the alarms that have alarm reporting enabled
Alarm Status	Indicates the current alarm state (for example, stray, malformed, packet loss, overrun, underrun, remote packet loss, remote fault, or remote RDI)
CEM SAP Statistics	
Packets	(Column heading) Displays the number of packets counted for the statistic since the last counter reset
Seconds	(Column heading) Displays the number of seconds elapsed for the statistic since the last counter reset
Events	(Column heading) Displays the number of events counted for the statistic since the last counter reset
Egress Stats	Indicates that the following statistics are egress statistics
Forwarded	Displays the number of forwarded packets
Missing	Displays the number of missing packets
Reordered and Forwarded	Displays the number of packets that have been reordered and forwarded

Table 32: SAP Fields (Continued)

Label	Description
Underrun	Displays the accumulated number of underrun packets for the number of underrun events
Overrun	Displays the accumulated number of overrun packets for the number of overrun events
Misordered Dropped	Displays the number of misordered packets that have been dropped
Malformed Dropped	Displays the number of malformed packets that have been dropped
Error	Displays the accumulated number of seconds that have passed while any error has occurred
Severely Error	Displays the accumulated number of seconds that have passed while severe errors has occurred
Unavailable	Displays the accumulated number of seconds that have passed while the Cpipe is unavailable
Failure Count	Displays the accumulated number of failed events
Ingress Stats	Indicates that the following statistics are ingress statistics
Forwarded	Displays the number of forwarded packets
Dropped	Displays the number of dropped packets

The following CLI sample outputs are shown:

- [Sample Output \(Apipe\)](#)
- [Sample Output \(Epipe\)](#)

Sample Output (Apipe)

```
*A:csasim2>show>service>id# sap 1/4/1.1:2 detail
```

```
=====
Service Access Points (SAP)
=====
Service Id      : 2
SAP             : 1/4/1.1:2          Encap           : atm
Description     : Apipe SAP
Admin State     : Up                 Oper State      : Down
Flags           : PortOperDown L2OperDown
Multi Svc Site  : None
Last Status Change : 04/30/2008 13:55:04
Last Mgmt Change  : 05/07/2008 15:51:51
Sub Type        : regular

Admin MTU       : 1572                Oper MTU        : 1572
Ingr IP Fltr-Id : n/a                 Egr IP Fltr-Id  : n/a
```

Show Commands

```

Ingr Mac Fltr-Id   : n/a
tod-suite          : None
Egr Agg Rate Limit : max
Endpoint           : N/A

Acct. Pol          : None
Collect Stats      : Disabled

-----
QOS
-----
Ingress qos-policy : 1
Shared Q plcy      : n/a
Egress qos-policy  : 1
Multipoint shared  : Disabled
-----
Sap Statistics
-----
Last Cleared Time   : N/A

Forwarding Engine Stats
Packets
Octets
Dropped             : 0
Off. HiPrio         : 21900
Off. LowPrio        : n/a
Queueing Stats(Ingress QoS Policy 1)
Dro. HiPrio         : 0
Dro. LowPrio        : n/a
For. InProf         : 10950
For. OutProf        : 10950
Queueing Stats(Egress QoS Policy 1)
Dro. InProf         : 0
Dro. OutProf        : n/a
For. InProf         : 21900
For. OutProf        : n/a
-----
Sap per Queue stats
-----
Packets
Octets
Ingress Queue 1 (Unicast) (Priority)
Off. HiPrio         : 21900
Off. LoPrio         : n/a
Dro. HiPrio         : 0
Dro. LoPrio        : n/a
For. InProf         : 10950
For. OutProf        : 10950
Egress Queue 1
For. InProf         : 21900
For. OutProf        : n/a
Dro. InProf         : 0
Dro. OutProf        : n/a
-----
ATM SAP Configuration Information
-----
Ingress TD Profile : 1
Alarm Cell Handling: Enabled
OAM Termination    : Disabled
Egress TD Profile  : 1
Periodic Loopback  : Disabled
=====

```



```
*A:csasim2>show>service>id#
```

Sample Output (Epipe)

```
*A:csasim2>show>service>id# sap 1/3/1:* detail
```

Service Access Points (SAP)

```
=====
Service Id      : 3
SAP             : 1/3/1:*
Admin State     : Up
Flags           : ServiceAdminDown
Multi Svc Site  : None
Last Status Change : 04/30/2008 13:55:04
Last Mgmt Change  : 05/07/2008 16:54:57
Sub Type        : regular
Dot1Q Ethertype : 0x8100
QinQ Ethertype  : 0x8100

Admin MTU       : 1518
Ingr IP Fltr-Id : n/a
Ingr Mac Fltr-Id : n/a
tod-suite       : None
Egr Agg Rate Limit : max
Endpoint        : N/A
Q Frame-Based Acct : Disabled
Vlan-translation : None

Acct. Pol       : None
Collect Stats   : Disabled
=====
```

QOS

```
-----
Ingress qos-policy : 1
Shared Q plcy      : n/a
Egress qos-policy  : 1
Multipoint shared  : Disabled
-----
```

Sap Statistics

```
-----
Last Cleared Time : 05/07/2008 21:32:32
-----
```

	Packets	Octets
Forwarding Engine Stats		
Dropped	: 0	0
Off. HiPrio	: 2655264	2655264
Off. LowPrio	: 2655264	2655264

Queueing Stats(Ingress QoS Policy 1)

Dro. HiPrio	: 0	0
Dro. LowPrio	: 0	0
For. InProf	: 3982896	3982896
For. OutProf	: 1327632	1327632

Queueing Stats(Egress QoS Policy 1)

Dro. InProf	: 0	0
Dro. OutProf	: 0	0
For. InProf	: 2655264	2655264
For. OutProf	: 2655264	2655264

```

-----
Sap per Queue stats
-----

```

	Packets	Octets
Ingress Queue 1 (Unicast) (Priority)		
Off. HiPrio	: 0	0
Off. LoPrio	: 0	0
Dro. HiPrio	: 0	0
Dro. LoPrio	: 0	0
For. InProf	: 0	0
For. OutProf	: 0	0
Egress Queue 1		
For. InProf	: 0	0
For. OutProf	: 0	0
Dro. InProf	: 0	0
Dro. OutProf	: 0	0

```

=====

*A:csasim2>show>service>id#

```

sap-using

Syntax	sap-using [sap <i>sap-id</i>] sap-using [ingress egress] atm-td-profile <i>td-profile-id</i> sap-using [ingress egress] qos-policy <i>qos-policy-id</i>
Context	show>service
Description	<p>This command displays SAP information.</p> <p>If no optional parameters are specified, the command displays a summary of all defined SAPs.</p> <p>The optional parameters restrict output to only SAPs matching the specified properties.</p>
Parameters	<p>ingress — specifies matching an ingress policy</p> <p>egress — specifies matching an egress policy</p> <p>qos-policy <i>qos-policy-id</i> — identifies the ingress or egress QoS Policy for which to display matching SAPs</p> <p>Values 1 to 65535</p> <p>atm-td-profile <i>td-profile-id</i> — displays SAPs using this traffic description</p>

sap sap-id — specifies the physical port identifier portion of the SAP definition

Values *sap-id*: null [port-id | bundle-id]
dot1q [port-id | bundle-id]:qtag1
atm [port-id | bundle-id][:vpi/vci | vpi | vpi1.vpi2]
port-id slot/mda/port[.channel]
bundle-type-slot/mda.bundle-num
bundle keyword
type ima, ppp
bundle-num 1 to 10
qtag1 0 to 4094
vpi NNI 0 to 4095
UNI 0 to 255
vci 1, 2, 5 to 65535

Output **Show Service SAP** — The following table describes show service SAP output fields.

Table 33: Show Service SAP Output Fields

Label	Description
PortID	Displays the ID of the access port where the SAP is defined
SvcID	Identifies the service
Ing.QoS	Displays the SAP ingress QoS policy number specified on the ingress SAP
Egr.QoS	Displays the SAP egress QoS policy number specified on the egress SAP
Adm	Specifies the desired state of the SAP
Opr	Indicates the actual state of the SAP

Sample Output

```
*A:ALU-48# show service sap-using
```

```
=====
```

```
Service Access Points
```

```
=====
```

PortId	SvcId	Ing. QoS	Ing. Fltr	Egr. QoS	Egr. Fltr	Adm	Opr
1/2/7:1	103	1	none	1	none	Up	Up
1/2/7:2	104	1	none	1	none	Up	Up
1/2/7:3	105	1	none	1	none	Up	Up
1/1/1.1	303	1	none	1	none	Up	Up
1/1/1.2	304	1	none	1	none	Up	Up
1/1/1.3	305	1	none	1	none	Up	Up
1/1/9.1:10/50	701	1	none	1	none	Up	Down
1/1/9.1:20	702	1	none	1	none	Up	Down
1/1/9.1:10/51	703	1	none	1	none	Up	Down
1/1/9.1:30	704	1	none	1	none	Up	Down
1/1/9.1:10/52	705	1	none	1	none	Up	Down

Show Commands

```
1/1/9.1:40      706      1      none    1      none    Up    Down
1/1/9.1:11/50   805      1      none    1      none    Up    Down
1/1/9.1:21      806      1      none    1      none    Up    Down
1/1/9.1:12/52   807      1      none    1      none    Up    Down
1/1/9.1:41      808      1      none    1      none    Up    Down
1/1/1.9         903      1      none    1      none    Up    Up
1/1/1.10        904      1      none    1      none    Up    Up
```

Number of SAPs : 18

=====

```
*A:ALU-48#
```

```
*A:ALU-48# show service sap-using sap 1/1/21:0
```

```
Service Access Points Using Port 1/1/21:0
```

PortId	SvcId	Ing. QoS	Ing. Fltr	Egr. QoS	Egr. Fltr	Adm	Opr
1/1/21:0	1	1	none	1	none	Up	Down

Number of SAPs : 1

=====

```
*A:ALU-48#
```

```
*A:ALU-48# show service sap-using egress atm-td-profile 1
```

```
Service Access Point Using ATM Traffic Profile 1
```

PortId	SvcId	Ing. QoS	Ing. Fltr	Egr. QoS	Egr. Fltr	Adm	Opr
1/1/9.1:10/50	701	1	none	1	none	Up	Down
1/1/9.1:20	702	1	none	1	none	Up	Down
1/1/9.1:10/51	703	1	none	1	none	Up	Down
1/1/9.1:30	704	1	none	1	none	Up	Down
1/1/9.1:10/52	705	1	none	1	none	Up	Down
1/1/9.1:40	706	1	none	1	none	Up	Down
1/1/9.1:11/50	805	1	none	1	none	Up	Down
1/1/9.1:21	806	1	none	1	none	Up	Down
1/1/9.1:12/52	807	1	none	1	none	Up	Down
1/1/9.1:41	808	1	none	1	none	Up	Down

Saps : 10

=====

```
*A:ALU-12#
```

sdp

Syntax	sdp [<i>sdp-id</i> far-end <i>ip-address</i>] [detail]
Context	show>service>id
Description	Displays information for the SDPs associated with the service. If no optional parameters are specified, a summary of all associated SDPs is displayed.
Parameters	<i>sdp-id</i> — Displays only information for the specified SDP ID. Values 1 — 17407 <i>far-end ip-address</i> — Displays only SDPs matching the specified far-end IP address. Default SDPs with any far-end IP address. detail — Displays detailed SDP information.
Output	Show Service-ID SDP — The following table describes show service-id SDP output fields.

Table 34: SDP Output Fields

Label	Description
Service Destination Points (SDPs)	
Description	Displays generic information about the SDP
SDP Id	Identifies the SDP
Type	Identifies the service SDP binding type (for example, spoke)
VC Type	Displays the VC type for the SDP (for example, CESoPSN)
VC Tag	The explicit dot1Q value used when encapsulating to the SDP far end
Admin Path MTU	Specifies the desired largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented
Oper Path MTU	Specifies the actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented
Far End	Displays the IP address of the far end of the MPLS or GRE tunnel defined by this SDP
Delivery	Specifies the type of delivery used by the SDP (MPLS or GRE)
Admin State	Specifies the administrative state of this SDP
Oper State	Specifies the operational state of this SDP
Acct. Pol	The accounting policy ID assigned to the SAP

Table 34: SDP Output Fields (Continued)

Label	Description
Collect Stats	Specifies whether collect stats is enabled
Ingress Label	Displays the label used by the far-end device to send packets to this device in this service by this SDP
Egress Label	Displays the label used by this device to send packets to the far-end device in this service by this SDP
Admin ControlWord	Specifies the administrative state of the control word: Preferred (control word enabled) or Not Preferred (control word disabled)
Oper ControlWord	Specifies the operational state of the control word: True (control word enabled) or False (control word disabled)
Last Status Change	Specifies the time of the most recent operating status change to this spoke SDP
Signaling	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP
Last Mgmt Change	Specifies the time of the most recent management-initiated change to this spoke SDP
Flags	Displays the conditions that affect the operating status of this spoke SDP. Display output includes PathMTUtooSmall, SdpOperDown, NoIngVCLLabel, NoEgrVCLLabel, and so on
Mac Move	Indicates the administrative state of the MAC movement feature associated with the service
Peer Pw Bits	Displays the setting of the pseudowire peer bits. Display output includes pwNotforwarding, psnIngressFault, psnEgressFault, lacIngressFault, lacEgressFault
Peer Fault Ip	N/A
Peer Vccv CV Bits	Displays the setting of the pseudowire peer VCCV control verification bits (lspPing)
Peer Vccv CC Bits	Displays the setting of the pseudowire peer VCCV control channel bits (pwe3ControlWord and/or mplsRouterAlertLabel)

Table 34: SDP Output Fields (Continued)

Label	Description
Keepalive Information	
Admin State	Specifies the administrative state of the keepalive protocol
Oper State	Specifies the operational state of the keepalive protocol
Hello Time	Specifies how often the SDP Echo Request messages are transmitted on this SDP
Hello Msg Len	Specifies the length of the SDP Echo Request messages transmitted on this SDP
Max Drop Count	Specifies the maximum number of consecutive SDP Echo Request messages that can be unacknowledged before the keepalive protocol reports a fault
Hold Down Time	Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state
Statistics	
I. Fwd. Pkts.	Specifies the number of forwarded ingress packets
I. Dro. Pkts.	Specifies the number of dropped ingress packets
I. Fwd. Octs.	Specifies the number of forwarded ingress octets
I. Dro. Octs.	Specifies the number of dropped ingress octets
E. Fwd. Pkts.	Specifies the number of forwarded egress packets
E. Fwd. Octets	Specifies the number of forwarded egress octets
Associated LSP LIST	
Lsp Name	Specifies the name of the static LSP
Admin State	Specifies the administrative state of the associated LSP
Oper State	Specifies the operational state of the associated LSP
Time Since Last Tr*	Specifies the time that the associated static LSP has been in service

Table 34: SDP Output Fields (Continued)

Label	Description
APIPE Service Destination Point specifics	
Admin Concat Limit	Specifies the administrative (configured) value for the maximum number of cells for cell concatenation, as defined via the <code>max-cells</code> command
Oper Concat Limit	Specifies the operational value for the maximum number of cells for cell concatenation
Peer Concat Limit	Specifies the far-end value for the maximum number of cells for cell concatenation
Max Concat Delay	Specifies the amount of time to wait while cell concatenation is occurring, as defined via the <code>max-delay</code> command
CPIPE Service Destination Point specifics	
Local Bit-rate	Specifies the number of DS0s used by the local SDP
Peer Bit-rate	Specifies the number of DS0s used by the far-end SDP
Local Payload Size	Specifies the local payload size, in bytes, used by the local SDP
Peer Payload Size	Specifies the peer payload size, in bytes, used by the far-end SDP
Local Sig Pkts	Specifies the type of signaling packets used by the local SDP
Peer Sig Pkts	Specifies the type of signaling packets used by the far-end SDP
Local CAS Framing	Specifies the type of CAS framing used by the local SDP
Peer CAS Framing	Specifies the type of CAS framing used by the far-end SDP
Local RTP Header	Specifies whether the local router inserts the RTP header
Peer RTP Header	Specifies whether the peer router inserts the RTP header
Number of SDPs	Specifies the number of SDPs bound to the service

Sample Output (Cpipe)

```
*A:csasim2>show>service>id# sdp 1 detail
```

```
=====
Service Destination Point (Sdp Id : 1) Details
=====
```

```
-----
Sdp Id 1:1  -(10.10.10.100)
-----
```

SDP Id	: 1:1	Type	: Spoke
VC Type	: CESoPSN	VC Tag	: 0
Admin Path MTU	: 0	Oper Path MTU	: 0
Far End	: 10.10.10.100	Delivery	: LDP
Admin State	: Up	Oper State	: Down
Acct. Pol	: None	Collect Stats	: Disabled
Ingress Label	: 0	Egress Label	: 0
Ing mac Fltr	: n/a	Egr mac Fltr	: n/a
Ing ip Fltr	: n/a	Egr ip Fltr	: n/a
Admin ControlWord	: Preferred	Oper ControlWord	: True
Admin BW(Kbps)	: 0	Oper BW(Kbps)	: 0
Last Status Change	: 04/30/2008 13:55:10	Signaling	: TLDP
Last Mgmt Change	: 05/02/2008 21:37:14		
Endpoint	: N/A	Precedence	: 4
Class Fwding State	: Down		
Flags	: SdpOperDown		
	NoIngVCLabel NoEgrVCLabel		
	PathMTUTooSmall		
Mac Move	: Ukwn	Blockable Level	: Unknown
Peer Pw Bits	: None		
Peer Fault Ip	: None		
Peer Vccv CV Bits	: None		
Peer Vccv CC Bits	: None		

```
KeepAlive Information :
```

Admin State	: Disabled	Oper State	: Disabled
Hello Time	: 10	Hello Msg Len	: 0
Max Drop Count	: 3	Hold Down Time	: 10

```
Statistics :
```

I. Fwd. Pkts.	: 0	I. Dro. Pkts.	: 0
I. Fwd. Octs.	: 0	I. Dro. Octets.	: 0
E. Fwd. Pkts.	: 0	E. Fwd. Octets	: 0

```
-----
CPIPE Service Destination Point specifics
-----
```

Local Bit-rate	: 1	Peer Bit-rate	: n/a
Local Payload Size	: 64	Peer Payload Size	: n/a
Local Sig Pkts	: No Sig.	Peer Sig Pkts	: No Sig.
Local CAS Framing	: No CAS	Peer CAS Framing	: No CAS
Local RTP Header	: No	Peer RTP Header	: No
Local Differential	: No	Peer Differential	: No
Local Timestamp	: 0	Peer Timestamp	: 0

```
=====
*A:csasim2>show>service>id#
```

Clear Commands

counters

Syntax	counters
Context	clear>service>statistics>id
Description	This command clears all traffic queue counters associated with the service ID.

id

Syntax	<code>id service-id</code>
Context	<code>clear>service</code> <code>clear>service>statistics</code>
Description	This command clears commands for a specific service.
Parameters	<i>service-id</i> — uniquely identifies a service

sap

Syntax	sap <i>sap-id</i> {all cem counters}		
Context	clear>service>statistics		
Description	This command clears SAP statistics for a SAP.		
Parameters	<i>sap-id</i> — specifies the physical port identifier portion of the SAP definition		
	Values	<i>sap-id</i> :	null [<i>port-id</i> <i>bundle-id</i>] dot1q [<i>port-id</i> <i>bundle-id</i>]: <i>qtag1</i> atm [<i>port-id</i> <i>bundle-id</i>][: <i>vpi/vci</i> <i>vpi</i> <i>vpi1.vpi2</i>] port-id <i>slot/mda/port</i> [. <i>channel</i>] bundle-type-slot/mda.bundle-num bundle keyword type ima, ppp bundle-num 1 to 10 qtag1 0 to 4094 vpi NNI 0 to 4095 UNI 0 to 255 vci 1, 2, 5 to 65535

all — clears all SAP queue statistics and STP statistics

cem — clears all queue statistics associated with a cem SAP

counters — clears all queue statistics associated with the SAP

sdp

Syntax **sdp** *sdp-id* **keep-alive**

Context clear>service>statistics

Description This command clears keepalive statistics associated with the SDP ID.

Parameters *sdp-id* — identifies the SDP for which to clear keepalive statistics

Values 1 to 17407

spoke-sdp

Syntax **spoke-sdp** *sdp-id:vc-id* **ingress-vc-label**
spoke-sdp *sdp-id:vc-id* {**all** | **counters**}

Context clear>service>id
clear>service>statistics>id

Description This command clears and resets the spoke SDP bindings for the service.

Parameters *sdp-id* — the spoke SDP ID to be reset

Values 1 to 17407

vc-id — the virtual circuit ID on the SDP ID to be reset

Values 1 to 4294967295

all — clears all queue statistics and STP statistics associated with the SDP

counters — clears all queue statistics associated with the SDP

ingress-vc-label — clears the VC ingress value associated with the specified connection

Clear Commands

Internet Enhanced Service

In This Chapter

This chapter provides information about Internet Enhanced Service (IES) used to facilitate the transport of in-band management datagrams of the 7705 SAR over ATM links.

Topics in this chapter include:

- [IES for In-band Management on page 238](#)
- [Setting Up Connections Between the 5620 SAM and the 7705 SAR on page 239](#)
- [Encapsulation on page 240](#)
- [Layer 2 and Layer 3 Traffic Management on page 241](#)
- [Troubleshooting and Fault Detection Services on page 242](#)
- [Configuring an IES Management Service with CLI on page 243](#)
- [IES Management Command Reference on page 253](#)

IES for In-band Management

In the HSDPA offload application (see [HSDPA Offload on page 44](#)), the main uplink out of a typical cell site is over the ATM network using leased lines. Mission-critical traffic such as voice, signaling, and synchronization traffic is carried over the ATM network.

Internet Enhanced Service (IES) provides a reliable means of diverting the node management IP packets from the DSL IP network to the more reliable Layer 2 ATM network. To do this, IES provides an IP address and interworking function between the Layer 3 IP network and the Layer 2 ATM network. Without this capability, the in-band IP management traffic for the 7705 SAR could only be connected to an IP network.

In Release 1.1, IES is used only for in-band management of the 7705 SAR over the ATM network. It is not used to offer routing services for customers, which is a typical use with other service router products, such as the 7710 SR. The 7705 SAR supports VLL services (Apipes, Cpipes, and Epipes) to transport customer traffic.

IES is supported on the 16-port T1/E1 ASAP Adapter card of the 7705 SAR-8 or on the T1/E1 ports of the 7705 SAR-F. The service can be created on an ATM port or on an IMA group.

In the 7705 SAR, all traffic received over IES is extracted directly to the control plane (CSM) in the same way as management traffic received over the CSM console port or Ethernet management port, or management traffic destined for the 7705 SAR over an Ethernet or MLPPP encapsulated network port. With IES management, the traffic transported is always IP packets. At the termination point of the ATM link, the IP packets are extracted to the CSM for further processing.

Setting Up Connections Between the 5620 SAM and the 7705 SAR

IP over ATM is used for in-band management of the 7705 SAR. This requires the use of IP addresses so that the packets can be routed through the network using a routing table to indicate the next hop. Because Apipe interfaces (SAPs) do not have IP addresses, Apipes cannot be used to carry the management traffic.

With IES, the ATM SAP can be used for the forwarding of management IP packets. To set up a connection, IES is enabled on an interface on the 7705 SAR and the IP address for the interface is defined. A PVCC connection is then set up between the 7705 SAR and the remote router (SR) attached to the network manager (5620 SAM).

The IP datagrams are encapsulated into AAL5 for transport over the ATM network.

At the remote SR end, the SAP is bound to a VPRN instance to ensure that LDP signaling to the system IP address of the 7705 SAR flows through the IP/GRE link and not over the ATM link. Within the VPRN, an IP address is assigned at the termination SAP. The IP datagram is extracted from the ATM cell at this termination point and is routed to the 5620 SAM.

Alternatively, manually configured connections can be used instead of signaled pseudowires.



Note: The remote IP address must be manually configured and a static route must be set up between the two connections. This configuration is beyond the scope of this document; refer to the 7705 SAR OS Router Configuration Guide for information.

For redundancy, it is recommended that two VCs be configured per ATM port or IMA group. This requires the configuration of two static routes. ECMP must be enabled to allow duplicate routes in the routing table, and BFD can be enabled to trigger a faster handover to the other route in case of route failure.

Encapsulation

To run IP traffic over ATM links, the system uses routed VC-mux encapsulation as specified in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*. Since the only supported Layer 3 protocol over the management VC is IP, the VC mux encapsulation method is implemented to reduce complexity and overhead; likewise, routing mode is preferred over bridged mode.

The maximum MTU size supported is 1524 bytes.

Layer 2 and Layer 3 Traffic Management

ATM traffic descriptors can be applied at the ingress (policing) and egress (shaping and service category scheduling and prioritization) of the IES SAP in order to provide traffic management functions at Layer 2.

Management IP traffic that is destined for the CSM is classified at Layer 3 and is forwarded into the fabric from one of three of the adapter card control queues:

- high priority
- low priority
- FTP priority

The high-priority and low-priority queues are limited to 1 Mb/s and the FTP queue is rate-limited to 3 Mb/s ingress to the fabric toward the control plane.



Note: Proper configuration of the traffic descriptor profiles is essential for proper operation of the IES SAP. If no profile is assigned, the default UBR service category is assumed. All IES 7705 SAR traffic is scheduled; no shaping is supported in this mode. To ensure that IP traffic transported over the IES SAP is prioritized fairly, ATM layer traffic descriptors should be assigned. See [IES SAP Commands on page 262](#) in the [IES Management Command Reference](#) section for information.

Troubleshooting and Fault Detection Services

The IES in-band management service supports ATM OAM F4 (VP level) and F5 (VC level) cell generation and termination. For more information on OAM, refer to the chapter on [OAM and SAA on page 277](#).

Bidirectional forwarding detection (BFD) can also be configured on the IES SAP. BFD is a simple protocol for detecting failures in a network. BFD uses a “hello” mechanism that sends control messages periodically to the far end and receives periodic control messages from the far end. In Release 1.1 of the 7705 SAR, BFD is implemented for static routes in asynchronous mode only, meaning that neither end responds to control messages; rather, the messages are sent in the time period configured at each end.

To support redundancy, ECMP must be enabled to allow duplicate routes in the routing table, and BFD must be enabled to trigger the handover to the other route in case of failure.

Due to the lightweight nature of BFD, it can detect failures faster than other detection protocols, making it ideal for use in applications such as mobile transport.

If the configured number of consecutive BFD messages is not received in the configured timeframe, the static route to the peer is declared not active.



Note: Layer 2 AIS/RDI cells that are received on the IES SAP will disable the IP interface. Link failures detected by BFD will also disable the IP interface.

Configuring an IES Management Service with CLI

This section provides the information required to configure IES for in-band management of the 7705 SAR over ATM links.

Topics in this section include:

- [List of Commands on page 244](#)
- [Common Configuration Tasks on page 246](#)
- [Configuring IES Components on page 247](#)
 - [Creating an IES Service on page 247](#)
 - [Configuring Interface Parameters on page 248](#)
 - [Configuring IES SAP Parameters on page 249](#)
- [Service Management Tasks on page 251](#)
 - [Modifying IES Service Parameters on page 251](#)
 - [Disabling an IES Service on page 251](#)
 - [Re-enabling an IES Service on page 252](#)
 - [Deleting an IES Service on page 252](#)

List of Commands

[Table 35](#) lists all the IES configuration commands, indicating the configuration level at which each command is implemented with a short command description. IES services are configured in the `config>service` context. The command list is organized in the following task-oriented manner:

- [Configure an IES service](#)
- [Configure IES interface parameters](#)
- [Configure IES SAP parameters](#)
- [Configure IES ingress filter policies](#)
- [Configure IES SAP ATM parameters](#)
- [Configure IES SAP ATM egress and ingress parameters](#)

Table 35: CLI Commands to Configure IES Management Service Parameters

Command	Description	Page
Configure an IES service		
<code>config>service>ies service-id [customer customer-id] [vpn vpn-id]</code>		258
<code>service-id</code>	Specifies a unique service identification number identifying the service in the service domain	258
<code>customer-id</code>	Specifies the existing customer ID number associated with the service	258
<code>vpn-id</code>	Specifies the VPN ID number, which allows you to identify VPNs	258
<code>description</code>	Specifies a text string describing the service	256
<code>shutdown</code>	Administratively enables or disables the IES service	256
Configure IES interface parameters		
<code>config>service>ies>interface</code>		259
<code>address</code>	Assigns an IP address to the IES interface	260
<code>bfd</code>	Configures the time interval in which BFD control messages are transmitted and received on the interface and the number of control messages to be transmitted and received within that interval	261
<code>description</code>	Specifies a text string describing the interface	256
<code>ip-mtu</code>	Configures the IP MTU for the interface	261

Table 35: CLI Commands to Configure IES Management Service Parameters (Continued)

Command	Description	Page
shutdown	Administratively enables or disables the IES interface	256
Configure IES SAP parameters		
config>service>ies>if>sap		262
atm	Enables access to the context to configure ATM-related attributes	265
description	Specifies a text string describing the IES SAP	256
ingress	Enables access to the context to associate ingress filter policies with the SAP	264
shutdown	Administratively enables or disables the SAP	256
Configure IES ingress filter policies		
config>service>ies>if>sap>ingress		
filter ip	Associates a filter policy with an ingress SAP	264
Configure IES SAP ATM parameters		
config>service>ies>if>sap>atm		
encapsulation	Configures an ATM VC SAP for encapsulation in accordance with RFC 2684	265
egress	Configures egress ATM attributes for the SAP	265
ingress	Configures ingress ATM attributes for the SAP	266
oam	Enables access to the context to configure OAM functionality for a PVCC delimiting a SAP	266
Configure IES SAP ATM egress and ingress parameters		
config>service>ies>if>sap>atm>egress		
config>service>ies>if>sap>atm>ingress		
traffic-desc	Assigns an ATM traffic descriptor profile to a SAP	266

Common Configuration Tasks

The following list provides a brief overview of the tasks that must be performed to configure IES for in-band management service.

- Associate the IES service with a customer ID.
- Create an IP interface on the 7705 SAR.
- Specify the IP address of the interface.
- Define interface parameters.
- Define SAP parameters for the ATM VC (**Note:** defining two SAPs per port or IMA group is recommended for redundancy).
- Manually configure the remote address of the far-end router to which the 5620 SAM network manager is connected (far-end router must be enabled for IES service).*
- Create a static route to the remote router and 5620 SAM.*
- Enable the service.



Note: *Remote address and static route configuration is beyond the scope of this document. For information, refer to the 7705 SAR OS Router Configuration Guide.

Configuring IES Components

This section provides configuration examples for components of the IES Management service. Each component includes some or all of the following: introductory information, CLI syntax, a specific CLI example, and a sample CLI display output. Included are the following components:

- [Creating an IES Service](#)
- [Configuring Interface Parameters](#)
- [Configuring IES SAP Parameters](#)

Creating an IES Service

Use the following CLI syntax to create an IES service.

CLI Syntax: `config>service# ies service-id [customer customer-id]
[create] [vpn vpn-id]
 description description-string
 interface ip-int-name [create]
 no shutdown`

Example: `A:ALU-41>config>service# ies 5 customer 1 create
A:ALU-41>config>service>ies# description "IES for in-band
management"
A:ALU-41>config>service>ies# interface "ATMoIP
Management" create
A:ALU-41>config>service>ies# no shutdown
A:ALU-41>config>service>ies#`

The following example displays the IES service creation output.

```
A:ALU-41>config>service# info
-----
...
    ies 5 customer 1 create
        description "IES for in-band management"
        interface "ATMoIP Management"
        no shutdown
    exit
...
-----
```

Configuring Interface Parameters

Use the following CLI syntax to configure interface parameters for the IES service.

CLI Syntax: `config>service# ies service-id [customer customer-id]
[create] [vpn vpn-id]
 interface ip-int-name
 address if-ip-address
 bfd transmit-interval [receive receive-interval]
 [multiplier multiplier]
 description description-string
 ip-mtu octets
 no shutdown`

Example: `A:ALU-41>config>service# ies 5
A:ALU-41>config>service>ies# interface "ATMoIP
Management"
A:ALU-41>config>service>ies>if# address 3.3.3.3/24
A:ALU-41>config>service>ies>if# ip-mtu 1524
A:ALU-41>config>service>ies>if# no shutdown
A:ALU-41>config>service>ies>if#`

The following example displays the IES interface creation output.

```
A:ALU-41>config>service>ies>if# info detail
-----
...
        no description
        address 3.3.3.3/24
        ip-mtu 1524
        no bfd
        exit
        no shutdown
...
-----
```


Configuring IES SAP Parameters

Use the following CLI syntax to configure IES SAP parameters.



Note: The encapsulation type is always aal5mux-ip.

CLI Syntax:

```
config>service# ies service-id [customer customer-id]
[create] [vpn vpn-id]
    interface ip-int-name
        sap sap-id [create]
            atm
                encapsulation encap-type
                egress
                    traffic-desc traffic-desc-profile-id
            ingress
                traffic-desc traffic-desc-profile-id
            oam
                alarm-cells
        description description-string
    ingress
        filter ip ip-filter-id
    no shutdown
```

Example:

```
A:ALU-41>config>service# ies 5
A:ALU-41>config>service>ies# interface "ATMoIP
Management"
A:ALU-41>config>service>ies>if# sap 1/1/1.1:0/32 create
A:ALU-41>config>service>ies>if>sap# ingress
A:ALU-41>config>service>ies>if>sap>ingress# filter ip 3
A:ALU-41>config>service>ies>if>sap>ingress# exit
A:ALU-41>config>service>ies>if>sap# atm
A:ALU-41>config>service>ies>if>sap>atm# encapsulation
aal5mux-ip
A:ALU-41>config>service>ies>if>sap>atm# egress
A:ALU-41>config>service>ies>if>sap>atm>egress# traffic-
desc 3
A:ALU-41>config>service>ies>if>sap>atm>egress# exit
A:ALU-41>config>service>ies>if>sap>atm# ingress
A:ALU-41>config>service>ies>if>sap>atm>ingress# traffic-
desc 2
A:ALU-41>config>service>ies>if>sap>atm>ingress# exit
A:ALU-41>config>service>ies>if>sap>atm# oam
A:ALU-41>config>service>ies>if>sap>atm>oam# alarm-cells
A:ALU-41>config>service>ies>if>sap>atm>oam# exit
A:ALU-41>config>service>ies>if>sap>atm# exit
A:ALU-41>config>service>ies>if>sap# exit
A:ALU-41>config>service>ies>if# exit
```

```
A:ALU-41>config>service>ies#
```

The following example displays the IES SAP creation output.

```
A:ALU-41>config>service>ies>if>sap# info detail
```

```
-----  
...  
    no description  
    ingress  
        filter ip 3  
    exit  
    atm  
        encapsulation aal5mux-ip  
    ingress  
        traffic-desc 2  
    exit  
    egress  
        traffic-desc 3  
    exit  
    oam  
        alarm-cells  
    exit  
    exit  
    no shutdown  
...  
-----
```

Service Management Tasks

This section discusses the following service management tasks:

- [Modifying IES Service Parameters](#)
- [Disabling an IES Service](#)
- [Re-enabling an IES Service](#)
- [Deleting an IES Service](#)

Modifying IES Service Parameters

Existing IES service parameters can be modified, added, removed, enabled, or disabled.

To display a list of customer IDs, use the `show>service>customer` command.

Enter the parameters (such as description, interface information, or SAP information), and then enter the new information.

The following is an example of changing the IP MTU size.

Example:

```
A:ALU-41>config>service# ies 5
A:ALU-41>config>service>ies# interface "testname"
A:ALU-41>config>service>ies>if# ip-mtu 1517
A:ALU-41>config>service>ies>if# exit
```

Disabling an IES Service

An IES service can be shut down without deleting the service parameters.

Use the `shutdown` command to shut down an IES service.

CLI Syntax:

```
config>service# ies service-id
shutdown
```

Example:

```
A:ALU-41>config>service# ies 5
A:ALU-41>config>service>ies# shutdown
A:ALU-41>config>service>ies# exit
```

Re-enabling an IES Service

Use the `no shutdown` command to re-enable a previously disabled IES service.

CLI Syntax: `config>service# ies service-id
no shutdown`

Example: `A:ALU-41>config>service# ies 5
A:ALU-41>config>service>ies# no shutdown
A:ALU-41>config>service>ies# exit`

Deleting an IES Service

An IES service cannot be deleted until SAPs and interfaces are shut down and deleted and the service is shut down on the service level.

Use the following CLI syntax to delete an IES service:

CLI Syntax: `config>service#
ies service-id
interface ip-int-name
sap sap-id
shutdown
exit
no sap sap-id
interface ip-int-name
shutdown
exit
no interface ip-int-name
shutdown
exit
no ies service-id`

IES Management Command Reference

Command Hierarchies

- [IES Management Configuration Commands](#)
- [Show Commands](#)

IES Management Configuration Commands

```

config
  — service
    — ies service-id [customer customer-id] [create] [vpn vpn-id]
    — no ies service-id
      — description description-string
      — no description
      — [no] interface ip-int-name [create]
        — address {ip-address/mask | ip-address netmask}
        — no address
        — bfd {transmit-interval} [receive receive-interval] [multiplier
          multiplier]
        — no bfd
        — description description-string
        — no description
        — ip-mtu octets
        — no ip-mtu
        — [no] sap sap-id [create]
          — atm
            — encapsulation atm-encap-type
            — egress
              — traffic-desc traffic-desc-profile-id
              — no traffic-desc
            — ingress
              — traffic-desc traffic-desc-profile-id
              — no traffic-desc
            — oam
              — [no] alarm-cells
          — description description-string
          — no description
          — ingress
            — filter ip ip-filter-id
            — no filter ip
            — no filter ip [ip ip-filter-id]
          — [no] shutdown
        — [no] shutdown
      — [no] shutdown

```

Show Commands

```

show
  — service
    — id service-id
      — all

```

IES Management Configuration Commands

- [Generic Commands on page 256](#)
- [IES Global Commands on page 258](#)
- [IES Interface Commands on page 259](#)
- [IES SAP Commands on page 262](#)

Generic Commands

description

Syntax	description <i>description-string</i> no description
Context	config>service>ies config>service>ies>interface config>service>ies>interface>sap
Description	This command creates a text description stored in the configuration file for a configuration context. The no form of this command removes the string from the context.
Default	No description is associated with the configuration context.
Parameters	<i>description-string</i> — 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>service>ies config>service>ies>interface config>service>ies>interface>sap
Description	<p>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. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many objects must be shut down before they may be deleted. Many entities must be explicitly enabled using the no shutdown command.</p> <p>The no form of this command places the entity into an administratively enabled state.</p> <p>Services are created in the administratively down (shutdown) state. When a no shutdown command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities are described in the following Special Cases.</p>

Special Cases

IES — the default administrative status of an IES service is down. While the service is down, its associated interface is operationally down.

For example, if 1) An IES service is operational and its associated interface is shut down

2) The IES service is administratively shut down and brought back up

3) The interface that is shut down remains in the administrative shutdown state

A service is regarded as operational provided that one IP interface is operational.

IES IP Interfaces — when the IP interface is shut down, it enters the administratively and operationally down states. For a SAP bound to the IP interface, no packets are transmitted out of the SAP and all packets received on the SAP are dropped and the packet discard counter is incremented.

IES Global Commands

ies

Syntax	ies <i>service-id</i> [customer <i>customer-id</i>] [create] [vpn <i>vpn-id</i>] no ies <i>service-id</i>
Context	config>service
Description	<p>This command enables Internet Enhanced Service (IES). IES in Release 1.1 of the 7705 SAR is used only for in-band management of the 7705 SAR over ATM links.</p> <p>The no form of this command deletes the IES service instance with the specified <i>service-id</i>.</p> <p>The service cannot be deleted until all the IP interfaces defined within the service ID have been shut down and deleted.</p>
Parameters	<p><i>service-id</i> — uniquely identifies a service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The <i>service-id</i> must be the same number used for every 7705 SAR on which this service is defined.</p> <p>Values 1 to 2147483647</p> <p>customer <i>customer-id</i> — specifies the customer ID number to be associated with the service. This parameter is required on service creation and is optional for service editing or deleting.</p> <p>Values 1 to 2147483647</p> <p>vpn <i>vpn-id</i> — specifies the VPN ID number, which allows you to identify virtual private networks (VPNs) by a VPN identification number. If this parameter is not specified, the VPN ID uses the service ID number.</p> <p>Values 1 to 2147483647</p> <p>Default null (0)</p>

IES Interface Commands

interface

Syntax	interface <i>ip-int-name</i> [create] no interface <i>ip-int-name</i>
Context	config>service>ies
Description	<p>This command creates a logical IP routing interface for an Internet Enhanced Service (IES). Once created, attributes like an IP address and service access point (SAP) can be associated with the IP interface.</p> <p>The interface command, under the context of services, is used to create and maintain IP routing interfaces within IES service IDs. The interface command can be executed in the context of an IES service ID. Two SAPs can be assigned to a single group interface.</p> <p>Interface names are case-sensitive and must be unique within the group of IP interfaces defined for config router interface and config service ies interface (that is, the network core router instance). Interface names cannot be in the dotted decimal notation of an IP address. For example, the name “1.1.1.1” is not allowed, but “int-1.1.1.1” is allowed. Show commands for router interfaces use either interface names or the IP addresses. Use unique IP address values and IP address names to maintain clarity. It could be unclear to the user if the same IP address and IP address name values are used. Although not recommended, duplicate interface names can exist in different router instances.</p> <p>When a new name is entered, a new logical router interface is created. When an existing interface name is entered, the user enters the router interface context for editing and configuration.</p> <p>There are no default IP interface names defined within the system. All IES IP interfaces must be explicitly defined. Interfaces are created in an enabled state.</p> <p>The no form of this command removes the IP interface and all the associated configurations. The interface must be administratively shut down before issuing the no interface command. The IP interface must be shut down before the SAP on that interface can be removed.</p>
Default	No interfaces or names are defined within the system.
Parameters	<p><i>ip-int-name</i> — the name of the IP interface. Interface names must be unique within the group of IP interfaces defined for the network core router instance. 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.</p> <p>Values 1 to 32 characters (must start with a letter)</p> <p>If the <i>ip-int-name</i> already exists, the context is changed to maintain that IP interface. If the <i>ip-int-name</i> already exists as an IP interface defined within the config router commands, an error will occur and the context will not be changed to that IP interface. If the <i>ip-int-name</i> does not exist, the interface is created and the context is changed to that interface for further command processing.</p>

address

Syntax	address <i>{ip-address/mask ip-address netmask}</i> no address
Context	config>service>ies>interface <i>ip-int-name</i>
Description	<p>This command assigns an IP address and IP subnet to an IES IP interface. Only one IP address can be associated with an IP interface.</p> <p>An IP address must be assigned to each IP interface. An IP address and a mask combine to create a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. The IP prefix cannot overlap with other existing IP prefixes defined as local subnets on other IP interfaces in the same routing context within the 7705 SAR.</p> <p>The IP address for the interface can be entered in either CIDR (classless inter-domain routing) notation or traditional dotted decimal notation. Show commands display CIDR notation and are stored in configuration files.</p> <p>By default, no IP address or subnet association exists on an IP interface until it is explicitly created.</p> <p>The no form of the command removes the IP address assignment from the IP interface. The no form of this command can only be performed when the IP interface is administratively shut down. Shutting down the IP interface brings the interface operationally down.</p>
Default	No IP address is assigned to the IP interface.
Parameters	<p><i>ip-address</i> — the IP address of the IP interface. The <i>ip-address</i> portion of the address command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.</p> <p>Values 1.0.0.0 to 223.255.255.255</p> <p><i>/</i> — the forward slash is a parameter delimiter that separates the <i>ip-address</i> portion of the IP address from the mask that defines the scope of the local subnet. No spaces are allowed between the <i>ip-address</i>, the “/”, and the <i>mask</i> parameter. If a forward slash does not immediately follow the <i>ip-address</i>, a dotted decimal mask must follow the prefix.</p> <p><i>mask</i> — the subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (/) separates the <i>ip-address</i> from the <i>mask</i> parameter. The <i>mask</i> parameter indicates the number of bits used for the network portion of the IP address; the remainder of the IP address is used to determine the host portion of the IP address.</p> <p>Values 1 to 32 (mask length of 32 is reserved for system IP addresses)</p> <p><i>netmask</i> — the subnet mask in dotted decimal notation</p> <p>Values 0.0.0.0 to 255.255.255.255 (network bits all 1 and host bits all 0)</p>

bfd

Syntax	bfd { <i>transmit-interval</i> } [receive <i>receive-interval</i>] [multiplier <i>multiplier</i>] no bfd
Context	config>service>ies>interface <i>ip-int-name</i>
Description	This command configures the time interval in which BFD control messages are transmitted and received on the interface and the number of control messages to be transmitted and received within that interval. This mechanism is used to detect failures in the network. If either end does not receive the specified number of messages in the specified time interval, the far end is declared to be down.
Default	no bfd
Parameters	<p><i>transmit-interval</i> — the number of milliseconds between transmitted control messages</p> <p>Values 100 to 100000</p> <p>Default 100</p> <p><i>receive-interval</i> — the number of milliseconds between received control messages</p> <p>Values 100 to 100000</p> <p>Default 100</p> <p><i>multiplier</i> — the number of control messages to be sent during the configured transmit and receive intervals</p> <p>Values 3 to 20</p> <p>Default 3</p>

ip-mtu

Syntax	ip-mtu <i>octets</i> no ip-mtu
Context	config>service>ies>interface> <i>ip-int-name</i>
Description	<p>This command configures the IP maximum transmit unit (packet size) for this interface.</p> <p>The no form of the command returns the default value.</p>
Parameters	<p><i>octets</i> — the MTU for the interface</p> <p>Values 512 to 1524</p>

IES SAP Commands

sap

Syntax	sap <i>sap-id</i> [create] no sap <i>sap-id</i>
Context	config>service>ies>interface <i>ip-int-name</i>
Description	<p>This command creates a SAP within an IES service. Each SAP must be unique.</p> <p>All SAPs must be explicitly created with the create keyword. If no SAPs are created within a service or on an IP interface, a SAP will not exist on that object.</p> <p>Enter an existing SAP without the create keyword to edit SAP parameters.</p> <p>A SAP can only be associated with a single service. The SAP is owned by the service in which it was created. An IES SAP can only be defined on an ATM port or IMA group that has been configured as an access port in the config>port <i>port-id</i> context using the mode access command. Fractional TDM ports are always access ports. Refer to the 7705 SAR OS Interface Configuration Guide for information on access ports.</p> <p>If a port is shut down, all SAPs on that port become operationally down. When a service is shut down, SAPs for the service are not displayed as operationally down although all traffic traversing the service will be discarded. The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.</p> <p>The no form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP will also be deleted.</p>
Default	No SAPs are defined.
Parameters	<i>sap-id</i> — specifies the physical port identifier portion of the SAP definition

The *sap-id* can be configured in one of the formats described in [Table 36](#).

Table 36: SAP ID Configurations

Type	Syntax	Example
port-id	<i>slot/mda/port[.channel]</i>	1/1/5
atm or ima group	<i>[port-id bundle-id][:vpi/vci vpi]</i>	<i>port-id:</i> 1/1/1.1 <i>bundle-id:</i> bundle-ima-1/1.1 <i>vpi/vci:</i> 16/32 <i>vpi:</i> 16
Values	<i>sap-id:</i> <div> atm <i>[port-id][:vpi/vci vpi]</i> IMA group <i>[bundle-id][:vpi/vci vpi]</i> port-id <i>slot/mda/port[.channel]</i> bundle-type-slot/mda.bundle-num bundle keyword type ima bundle-num 1 to 10 vpi NNI 0 to 4095 UNI 0 to 255 vci 1, 2, 5 to 65535 </div>	

port-id — specifies the physical port ID in the *slot/mda/port* format

If the card in the slot has a T1/E1 ASAP Adapter card installed, the *port-id* must be in the slot_number/MDA_number/port_number format. For example 1/2/3 specifies port 3 on MDA 2 in slot 1.

The *port-id* must reference a valid port type. When the *port-id* parameter represents TDM channels, the port ID must include the channel ID. A period “.” separates the physical port from the *channel-id*. The port must be configured as an access port.

bundle-id — specifies the multilink bundle to be associated with this IP interface. The **bundle** keyword must be entered at the beginning of the parameter. The command syntax must be configured as follows:

bundle-id: **bundle-type-slot-id/mda-slot.bundle-num**
bundle-id value range: 1 to 10

For example:

```
*A:ALU-12>config# port bundle-ppp-5/1.1
*A:ALU-12>config>port# multilink-bundle
```

create — keyword used to create a SAP instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

ingress

Syntax	ingress
Context	config>service>ies>interface <i>ip-int-name</i> >sap <i>sap-id</i>
Description	This command enables access to the context to associate ingress filter policies with the SAP. If an ingress filter is not defined, no filtering is performed.

filter ip

Syntax	filter ip <i>ip-filter-id</i> no filter no filter [<i>ip ip-filter-id</i>]
Context	config>service>ies>interface <i>ip-int-name</i> >sap <i>sap-id</i> >ingress
Description	<p>This command associates an IP filter policy with an ingress SAP. Filter policies control the forwarding and dropping of packets based on the IP match criteria. Only one filter ID can be specified.</p> <p>The filter policy must already be defined before the filter command is executed. If the filter policy does not exist, the operation fails and an error message is returned. Filters applied to the ingress SAP apply to all IP packets on the SAP.</p> <p>The no form of this command removes any configured filter ID association with the SAP.</p>
Default	No filter is specified.
Parameters	ip <i>ip-filter-id</i> — the filter name acts as the ID for the IP filter policy expressed as a decimal integer. The filter policy must already exist within the config>filter>ip-filter context.
Values	1 to 65535



Note: For information on configuring IP filter IDs, see the 7705 SAR OS Router Configuration Guide.

atm

Syntax	atm
Context	config>service>ies>interface <i>ip-int-name</i> >sap <i>sap-id</i>
Description	<p>This command enables access to the context to configure ATM-related attributes. This command can only be used when a given context (for example, a channel or SAP) supports ATM functionality such as:</p> <ul style="list-style-type: none"> • configuring ATM port or ATM port-related functionality on T1/E1 ASAP Adapter cards or T1/E1 ports • configuring ATM-related configuration for ATM-based SAPs that exist on T1/E1 ASAP Adapter cards or T1/E1 ports <p>If ATM functionality is not supported for a given context, the command returns an error.</p>

encapsulation

Syntax	encapsulation <i>atm-encap-type</i>
Context	config>service>ies>interface <i>ip-int-name</i> >sap <i>sap-id</i> >atm
Description	<p>This command configures an ATM VC SAP for encapsulation in accordance with RFC 2684, <i>Multiprotocol Encapsulation over ATM Adaptation Layer 5</i>.</p> <p>In Release 1.1, the only supported encapsulation type is aal5mux-ip.</p> <p>Ingress traffic that does not match the configured encapsulation is dropped.</p>
Default	aal5mux-ip
Parameters	<i>atm-encap-type</i> — aal5mux-ip (routed IP encapsulation for a VC multiplexed circuit as defined in RFC 2684)


egress

Syntax	egress
Context	config>service>ies>interface <i>ip-int-name</i> >sap <i>sap-id</i> >atm
	This command provides access to the context to configure egress ATM traffic policies for the SAP.

ingress

Syntax	ingress
Context	config>service>ies>interface <i>ip-int-name</i> >sap <i>sap-id</i> >atm
Description	This command provides access to the context to configure ingress ATM traffic policies for the SAP.

traffic-desc

Syntax	traffic-desc <i>traffic-desc-profile-id</i> no traffic-desc
Context	config>service>ies>interface <i>ip-int-name</i> >sap <i>sap-id</i> >atm>egress config>service>ies>interface <i>ip-int-name</i> >sap <i>sap-id</i> >atm>ingress
Description	<p>This command assigns an ATM traffic descriptor profile to an egress or ingress SAP.</p> <p>When configured under the ingress context, the specified traffic descriptor profile defines the traffic contract in the forward direction.</p> <p>When configured under the egress context, the specified traffic descriptor profile defines the traffic contract in the backward direction.</p> <p> Note: Proper configuration of the traffic descriptor profiles is essential for proper operation of the IES SAP. If no profile is assigned, the default UBR service category is assumed. All IES 7705 SAR traffic is scheduled; no shaping is supported in this mode. To ensure that IP traffic transported over the IES SAP is prioritized fairly, ATM layer traffic descriptors should be assigned.</p> <p>The no form of the command reverts the traffic descriptor to the default traffic descriptor profile.</p>
Default	The default traffic descriptor (trafficDescProfileId. = 1) is associated with newly created ATM VC SAPs.
Parameters	<i>traffic-desc-profile-id</i> — specifies a defined traffic descriptor profile (for information on defining traffic descriptor profiles, see the 7705 SAR OS Quality of Service Guide)
Values	1 to 1000

oam

Syntax	oam
Context	config>service>ies>interface <i>ip-int-name</i> >sap <i>sap-id</i> >atm
Description	This command enables the context to configure OAM functionality for an IES SAP.

The T1/E1 ASAP Adapter card supports F4 and F5 end-to-end OAM functionality (AIS, RDI, Loopback).

alarm-cells

Syntax	[no] alarm-cells
Context	config>service>ies>interface <i>ip-int-name</i> >sap <i>sap-id</i> >atm>oam
Description	<p>This command configures AIS/RDI fault management on a PVCC. Fault management allows PVCC terminations to monitor and report the status of their connection by propagating fault information through the network and by driving the PVCC's operational status.</p> <p>Layer 2 OAM AIS/RDI cells that are received on the IES SAP will cause the IP interface to be disabled.</p> <p>The no command disables alarm-cells functionality for the SAP. When alarm-cells functionality is disabled, OAM cells are not generated as result of the SAP going into the operationally down state.</p>
Default	enabled

Show Commands

all

Syntax	all
Context	show>service>id
Description	This command displays detailed information for all aspects of the service.
Output	Show service id <service-id> all Output — The following table describes the show service id <service-id> all command output fields.

Table 37: Show Service ID All Command Output Fields

Label	Description
Service Detailed Information	
Service Id	Identifies the service by its ID number
VPN Id	Identifies the VPN by its ID number
Service Type	Specifies the type of service (IES)
Description	Displays generic information about the service
Customer Id	Identifies the customer by its ID number
Last Status Change	Displays the date and time of the most recent status change to this service
Last Mgmt Change	Displays the date and time of the most recent management-initiated change to this service
Admin State	Specifies the desired state of the service
Oper State	Specifies the operating state of the service
MTU	Specifies the service MTU
SAP Count	Displays the number of SAPs specified for this service
Service Access Points	
Service Id	Identifies the service
SAP	Specifies the ID of the access port where this SAP is defined
Encap	Specifies the encapsulation type for this SAP on the access port
Admin State	Specifies the desired state of the SAP

Table 37: Show Service ID All Command Output Fields (Continued)

Label	Description
Oper State	Specifies the operating state of the SAP
Flags	Specifies the conditions that affect the operating status of this SAP. Display output includes ServiceAdminDown, PortOperDown, and so on.
Last Status Change	Specifies the date and time of the most recent status change to this SAP
Last Mgmt Change	Specifies the date and time of the most recent management-initiated change to this SAP
Admin MTU	Specifies the desired largest service frame size (in octets) that can be transmitted through this SAP to the far-end router, without requiring the packet to be fragmented
Oper MTU	Specifies the actual largest service frame size (in octets) that can be transmitted through this SAP to the far-end router, without requiring the packet to be fragmented
Ingr IP Fltr-Id	Specifies the ingress IP filter policy ID assigned to the SAP
Egr IP Fltr-Id	Specifies the egress IP filter policy ID assigned to the SAP (not applicable)
Ingr Mac Fltr-Id	Specifies the ingress MAC filter policy ID assigned to the SAP (not applicable)
Egr Mac Fltr-Id	Specifies the egress MAC filter policy ID assigned to the SAP (not applicable)
Acct. Pol	Specifies the accounting policy applied to the SAP (not applicable)
Collect Stats	Specifies whether accounting statistics are collected on the SAP (not applicable)
QoS	
Ingress qos-policy	Displays the SAP ingress QoS policy ID
Egress qos-policy	Displays the SAP egress QoS policy ID
SAP Statistics	
Last Cleared Time	Displays the date and time that a clear command was issued on statistics

Table 37: Show Service ID All Command Output Fields (Continued)

Label	Description
Forwarding Engine Stats	
Dropped	Indicates the number of packets or octets dropped by the forwarding engine
Off. HiPrio	Indicates the number of high-priority packets or octets offered to the forwarding engine
Off. LowPrio	Indicates the number of low-priority packets offered to the forwarding engine
Queueing Stats (Ingress QoS Policy)	
Dro. HiPrio	Indicates the number of high-priority packets or octets discarded, as determined by the SAP ingress QoS policy
Dro. LowPrio	Indicates the number of low-priority packets discarded, as determined by the SAP ingress QoS policy
For. InProf	Indicates the number of in-profile packets or octets (rate below CIR) forwarded, as determined by the SAP ingress QoS policy
For. OutProf	Indicates the number of out-of-profile packets or octets (rate above CIR) forwarded, as determined by the SAP ingress QoS policy
Queueing Stats (Egress QoS Policy)	
Dro. InProf	Indicates the number of in-profile packets or octets discarded, as determined by the SAP egress QoS policy
Dro. OutProf	Indicates the number of out-of-profile packets or octets discarded, as determined by the SAP egress QoS policy
For. InProf	Indicates the number of in-profile packets or octets (rate below CIR) forwarded, as determined by the SAP egress QoS policy
For. OutProf	Indicates the number of out-of-profile packets or octets (rate above CIR) forwarded, as determined by the SAP egress QoS policy
Sap per Queue stats	
Ingress Queue <i>n</i>	Specifies the index of the ingress QoS queue of this SAP, where <i>n</i> is the index number
Off. HiPrio	Indicates the number of packets or octets of high-priority traffic for the SAP (offered)

Table 37: Show Service ID All Command Output Fields (Continued)

Label	Description
Off. LoPrio	Indicates the number of packets or octets count of low-priority traffic for the SAP (offered)
Dro. HiPrio	Indicates the number of high-priority traffic packets or octets dropped
Dro. LoPrio	Indicates the number of low-priority traffic packets or octets dropped
For. InProf	Indicates the number of in-profile packets or octets (rate below CIR) forwarded
For. OutProf	Indicates the number of out-of-profile packets or octets (rate above CIR) forwarded
Egress Queue <i>n</i>	Specifies the index of the egress QoS queue of the SAP, where <i>n</i> is the index number
For. InProf	Indicates the number of in-profile packets or octets (rate below CIR) forwarded
For. OutProf	Indicates the number of out-of-profile packets or octets (rate above CIR) forwarded
Dro. InProf	Indicates the number of in-profile packets or octets dropped for the SAP
Dro. OutProf	Indicates the number of out-of-profile packets or octets discarded
ATM SAP Configuration Information	
Ingress TD Profile	The profile ID of the traffic descriptor applied to the ingress SAP
Egress TD Profile	The profile ID of the traffic descriptor applied to the egress SAP
Alarm Cell Handling	Indicates that OAM cells are being processed
AAL-5 Encap	Specifies the AAL-5 encapsulation type — for Release 1.1, this is always mux-ip
OAM Termination	Indicates whether this SAP is an OAM termination point
Services Interfaces	
If Name	The name used to refer to the IES interface
Admin State	The administrative state of the interface
Oper State	The operational state of the interface

Table 37: Show Service ID All Command Output Fields (Continued)

Label	Description
IP Addr/mask	The IP address and subnet mask length of the interface
Address Type	Specifies whether the IP address for the interface is the primary or secondary address on the interface (in Release 1.1, this is always primary)
Broadcast Address	The broadcast address of the interface
If Index	The interface index corresponding to the IES interface
Virt. If Index	The virtual interface index of the IES interface
Last Oper Chg	Specifies the date and time of the last operating state change on the interface
Global IF Index	The global interface index of the IES interface
SAP Id	The SAP identifier
TOS Marking	Specifies whether the ToS marking state is trusted or untrusted for the IP interface
If Type	The type of interface: IES
IES ID	The service identifier
MAC Address	The IEEE 802.3 MAC address
Arp Timeout	The timeout for an ARP entry learned on the interface
IP MTU	The IP maximum transmit unit for the interface
ICMP Mask Reply	Specifies whether the IP interface replies to a received ICMP mask request
ARP Populate	Specifies if ARP is enabled or disabled
ICMP Details	
Redirects	Specifies the maximum number of ICMP redirect messages that the IP interface will issue in a given period of time, in seconds Disabled — indicates that the IP interface will not generate ICMP redirect messages

Table 37: Show Service ID All Command Output Fields (Continued)

Label	Description
Unreachables	Specifies the maximum number of ICMP destination unreachable messages that the IP interface will issue in a given period of time, in seconds Disabled — indicates that the IP interface will not generate ICMP destination unreachable messages
TTL Expired	Specifies the maximum number of ICMP TTL expired messages that the IP interface will issue in a given period of time, in seconds Disabled — indicates that the IP interface will not generate ICMP TTL expired messages

Sample Output (IES Management Service)

A:ALU-2# show service id 751 all

```

=====
Service Detailed Information
=====
Service Id       : 751
Service Type     : IES
Description      : ATM_Backhaul_SAM_Mgmt
Customer Id      : 10
Last Status Change: 09/09/2008 16:26:25
Last Mgmt Change  : 09/09/2008 16:25:04
Admin State      : Up                Oper State      : Up
SAP Count        : 2
-----

Service Access Points
-----

-----
SAP bundle-ima-1/3.1:0/75
-----
Service Id       : 751
SAP              : bundle-ima-1/3.1:0/75   Encap          : atm
Admin State      : Up                Oper State      : Up
Flags           : None
Multi Svc Site   : None
Last Status Change: 09/09/2008 16:26:25
Last Mgmt Change  : 09/09/2008 16:25:04
Sub Type         : regular

Admin MTU        : 1572                Oper MTU        : 1572
Ingr IP Fltr-Id  : 1                  Egr IP Fltr-Id  : n/a
Ingr Mac Fltr-Id : n/a                Egr Mac Fltr-Id : n/a
tod-suite        : None                qinq-pbit-marking : both
Egr Agg Rate Limit : max

Acct. Pol        : None                Collect Stats    : Disabled
Anti Spoofing    : None                Nbr Static Hosts : 0

```

Show Commands

```

-----
QoS
-----
Ingress qos-policy : 1                      Egress qos-policy : 1
Shared Q plcy      : n/a                    Multipoint shared : Disabled
-----

Sap Statistics
-----
Last Cleared Time      : N/A

                                Packets          Octets
Forwarding Engine Stats
Dropped                : 0                      n/a
Off. HiPrio            : 802789                  n/a
Off. LowPrio           : n/a                     n/a

Queueing Stats(Ingress QoS Policy 1)
Dro. HiPrio            : 0                      n/a
Dro. LowPrio           : n/a                     n/a
For. InProf            : 802789                  69039854
For. OutProf           : 0                      0

Queueing Stats(Egress QoS Policy 1)
Dro. InProf            : 0                      n/a
Dro. OutProf           : n/a                     n/a
For. InProf            : 802829                  41753273
For. OutProf           : n/a                     n/a
-----

Sap per Queue stats
-----
                                Packets          Octets

Ingress Queue 1 (Unicast) (Priority)
Off. HiPrio            : 802789                  n/a
Off. LoPrio            : n/a                     n/a
Dro. HiPrio            : 0                      n/a
Dro. LoPrio            : n/a                     n/a
For. InProf            : 802789                  69039854
For. OutProf           : 0                      0

Egress Queue 1
For. InProf            : 802829                  41753273
For. OutProf           : n/a                     n/a
Dro. InProf            : 0                      n/a
Dro. OutProf           : n/a                     n/a
-----

ATM SAP Configuration Information
-----
Ingress TD Profile : 32                      Egress TD Profile : 32
Alarm Cell Handling: Enabled                  AAL-5 Encap       : mux-ip
OAM Termination    : Enabled                  Periodic Loopback  : Disabled

```

```
-----
Service Interfaces
-----
```

```
-----
Interface
-----
```

```
If Name       : IP_10.75.11.0/24
Admin State   : Up                      Oper State    : Up
Protocols     : None
IP Addr/mask  : 10.75.11.2/24          Address Type  : Primary
IGP Inhibit   : Disabled              Broadcast Address : Host-ones
-----
```

```
-----
Details
-----
```

```
If Index      : 3                      Virt. If Index : 3
Last Oper Chg : 09/09/2008 16:26:25  Global If Index : 32
SAP Id        : bundle-ima-1/3.1:0/75
TOS Marking   : Untrusted              If Type       : IES
SNTP B.Cast   : False                  IES ID        : 751
MAC Address   : 00:00:00:00:00:10      Arp Timeout   : 14400
IP MTU        : 1524                   ICMP Mask Reply : True
Arp Populate  : Disabled               Host Conn Verify : Disabled
LdpSyncTimer  : None
```

```
Proxy ARP Details
```

```
Rem Proxy ARP : Disabled              Local Proxy ARP : Disabled
Policies      : none
```

```
ICMP Details
```

```
Redirects      : Number - 100          Time (seconds) - 10
Unreachables   : Number - 100          Time (seconds) - 10
TTL Expired    : Number - 100          Time (seconds) - 10
```

```
IPCP Address Extension Details
```

```
Peer IP Addr   : Not configured
Peer Pri DNS Addr : Not configured
Peer Sec DNS Addr : Not configured
=====
```

```
*A:ALU-2#
```



Note: For more examples of Show commands for services, see [Show Commands on page 193](#).

Show Commands

In This Chapter

This chapter provides information about the Operations, Administration and Management (OAM) and Service Assurance Agent (SAA) commands available in the CLI for troubleshooting services.

Topics in this chapter include:

- [OAM Overview on page 278](#)
 - [LSP Diagnostics on page 278](#)
 - [SDP Diagnostics on page 279](#)
 - [Service Diagnostics on page 280](#)
 - [VLL Diagnostics on page 281](#)
 - [EFM OAM on page 283](#)
 - [OAM Propagation to Attachment Circuits on page 284](#)
 - [LDP Status Signaling on page 285](#)
- [Service Assurance Agent Overview on page 287](#)
 - [SAA Application on page 287](#)
- [OAM and SAA List of Commands on page 288](#)
- [OAM and SAA Command Reference on page 293](#)

OAM Overview

Delivery of services requires that a number of operations occur properly and at different levels in the service delivery model. For example, operations—such as the association of packets to a service, VC-labels to a service, and each service to a service tunnel—must be performed properly in the forwarding plane for the service to function properly. In order to verify that a service is operational, a set of in-band, packet-based OAM tools is required, with the ability to test each of the individual packet operations.

For in-band testing, the OAM packets closely resemble customer packets in order to effectively test the customer's forwarding path, but they are distinguishable from customer packets so they can be kept within the service provider's network and not forwarded to the customer.

The suite of OAM diagnostics supplements the basic IP ping and traceroute operations with diagnostics specialized for the different levels in the service delivery model. In addition, there are diagnostics for MPLS LSPs, SDPs, and Services within a service.

LSP Diagnostics

The 7705 SAR LSP diagnostics are implementations of LSP ping and LSP traceroute based on RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*. LSP ping and LSP traceroute are modeled after the ICMP echo request/reply used by ping and traceroute to detect and localize faults in IP networks.

LSP Ping

LSP ping, as described in RFC 4379, provides a mechanism to detect data plane failures in MPLS LSPs. For a given FEC, LSP ping verifies whether the packet reaches the egress label edge router (LER).

LSP Traceroute

In LSP traceroute mode, a packet is sent to each transit label switched router (LSR) along a communications path until the far-end router is reached. The path is traced one LSR at a time, where each LSR that receives a traceroute packet replies to the initiating 7705 SAR with a packet that identifies itself. Once the final LSR is identified, the initiating LSR has a list of all LSRs on the path. Like IP traceroute, LSP traceroute is a hop-by-hop operation (that is, LSR by LSR).

Use LSP traceroute to determine the exact location of LSP failures.

SDP Diagnostics

The 7705 SAR SDP diagnostics include SDP ping and SDP MTU path discovery.

SDP Ping

SDP ping performs in-band unidirectional or round-trip connectivity tests on SDPs. The SDP ping OAM packets are sent in-band, in the tunnel encapsulation, so it will follow the same path as traffic within the service. The SDP ping response can be received out-of-band in the control plane, or in-band using the data plane for a round-trip test.

For a unidirectional test, the SDP ping tests:

- the egress SDP ID encapsulation
- the ability to reach the far-end IP address of the SDP ID within the SDP encapsulation
- the path MTU to the far-end IP address over the SDP ID
- the forwarding class mapping between the near-end SDP ID encapsulation and the far-end tunnel termination

For a round-trip test, SDP ping uses a local egress SDP ID and an expected remote SDP ID. Since SDPs are unidirectional tunnels, the remote SDP ID must be specified and must exist as a configured SDP ID on the far-end 7705 SAR. SDP round-trip testing is an extension of SDP connectivity testing with the additional ability to test:

- the remote SDP ID encapsulation
- the potential service round-trip time
- the round-trip path MTU
- the round-trip forwarding class mapping

SDP MTU Path Discovery

In a large network, network devices can support a variety of packet sizes that are transmitted across its interfaces. This capability is referred to as the maximum transmission unit (MTU) of network interfaces. It is important to understand the MTU of the entire path end-to-end when provisioning services, especially for VLL services where the service must support the ability to transmit the largest customer packet.

The Path MTU Discovery tool provides a powerful tool that enables service providers to get the exact MTU supported between the service ingress and service termination points, accurate to 1 byte.

Service Diagnostics

The Alcatel-Lucent Service ping feature provides end-to-end connectivity testing for an individual service. Service ping operates at a higher level than the SDP diagnostics in that it verifies an individual service and not the collection of services carried within an SDP.

Service Ping

Service (SVC) ping is initiated from a 7705 SAR router to verify round-trip connectivity and delay to the far-end of the service. The Alcatel-Lucent implementation functions for GRE and MPLS tunnels and tests the following from edge-to-edge:

- tunnel connectivity
- VC label mapping verification
- service existence
- service provisioned parameter verification
- round-trip path verification
- service dynamic configuration verification



Note: Service ping uses GRE encapsulation.

VLL Diagnostics

This section describes VCCV ping, the VLL diagnostic capability for the 7705 SAR.

VCCV Ping

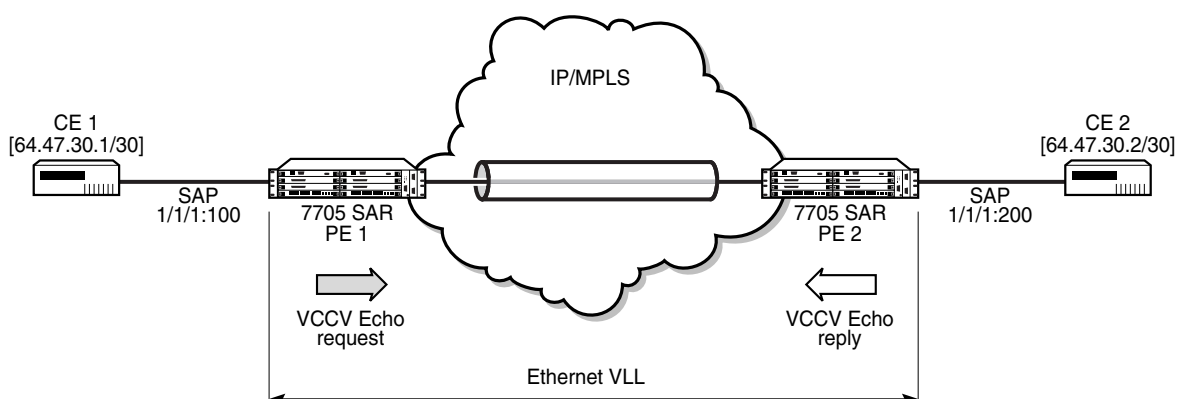
VCCV ping is used to check connectivity (in-band) of a VLL. It checks that the destination (target) PE is the egress point for the Layer 2 FEC. It provides a cross-check between the data plane and the control plane. It is in-band, meaning that the VCCV ping message is sent using the same encapsulation and along the same path as user packets in that VLL. This is equivalent to the LSP ping for a VLL service. VCCV ping reuses an LSP ping message format and can be used to test a VLL configured over an MPLS or GRE SDP.

VCCV Ping Application

VCCV creates an IP control channel within the pseudowire between PE1 and PE2 (see [Figure 24](#)). PE2 should be able to distinguish, on the receive side, VCCV control messages from user packets on that VLL. The 7705 SAR uses the router alert label immediately above the VC label to identify the VCCV ping message. This method has a drawback in that if ECMP is applied to the outer LSP label, such as the transport label, the VCCV message will not follow the same path as the user packets.

When sending the label mapping message for the VLL, PE1 and PE2 include an optional VCCV TLV in the PW FEC interface parameter field. The TLV indicates that the control channel uses the router alert label method.

Figure 24: VCCV Ping Application



19485

A VCCV-ping is an LSP echo request message as defined in the LSP ping specification. It contains a Layer 2 FEC stack TLV in which it must include the sub-TLV type 10 FEC 128 pseudowire. It also contains a field that indicates to the destination PE which reply mode to use.

The 7705 SAR supports the following reply modes:

- reply by an IPv4 UDP packet
This is the default mode for any service that does not have Control Word enabled.
- reply by application-level control channel
This mode sends the reply message in-band over the pseudowire from PE2 to PE1. PE2 will encapsulate the echo reply message using the CC type negotiated with PE1. This is the default mode of operation for Cpipe services.

The reply is an LSP echo reply message as defined in the LSP ping specification. The message is sent as per the reply mode requested by PE1. The return codes supported are the same as those currently supported in the 7705 SAR LSP ping capability.

The VCCV ping feature is in addition to the service ping OAM feature which can be used to test a service between 7705 SAR nodes. The VCCV ping feature can test connectivity of a VLL with any third party node that is compliant with *draft-ietf-pwe3-vcv-xx.txt*.

From the connection verification (CV) perspective, ICMP ping and LSP ping are both supported. From the control channel (CC) perspective, Router Alert is supported. In Release 1.1, VCCV based PW tests are only supported on dynamically signaled PWs (not on statically signaled PWs).

Table 38: Supported VCCV CC and CV Types

Type	Supported for	Details
Control Channel		
1	All supported VLLs	Use of CW, in-band, special bit stream “001b”
2	All supported VLLs	With insertion of Router Alert header, out-of-band
Connection Verification		
0	All supported VLLs	ICMP Ping
1	All supported VLLs	LSP Ping

EFM OAM

802.3ah clause 57 defines the EFM OAM sublayer. It is a link level Ethernet OAM. It provides network operators the ability to monitor the health of link operation and quickly determine the location of failing links or fault conditions.

EFM OAM defines a set of events that may impact link operation. The following events are supported:

- critical link events (defined in 802.3ah clause 57.2.10.1)
 - link fault: the PHY has determined a fault has occurred in the receive direction of the local DTE
 - dying gasp: an unrecoverable local failure condition has occurred
 - critical event: an unspecified critical event has occurred

These critical link events are signaled to the remote DTE by the flag field in OAMPDUs.

Unidirectional OAM Operation

Some physical layer devices support unidirectional OAM operation. When a link is operating in unidirectional OAM mode, the OAM sublayer ensures that only information OAMPDUs with the Link Fault critical link event indication set and no Information TLVs are sent across the link.

Remote Loopback

EFM OAM provides a link-layer frame loopback mode, which can be controlled remotely.

To initiate a remote loopback, the local EFM OAM client sends a loopback control OAMPDU with the “enable OAM remote loopback” command. After receiving the loopback control OAMPDU, the remote OAM client puts the port into frame loopback mode.

To exit a remote loopback, the local EFM OAM client sends a loopback control OAMPDU with the “disable OAM remote loopback” command. After receiving the loopback control OAMPDU, the remote OAM client put the port back into normal forwarding mode.

Note that during remote loopback test operation, all frames except EFM OAMPDUs are dropped at the local port for both receive and transmit directions, where remote loopback is enabled. This behavior can result in many protocols (e.g., STP) resetting their state machines.

When a port is in loopback mode, service mirroring is not operational if the port is a mirror-source or mirror-destination SAP.

802.3ah OAMPDU Tunneling for Epipe Services

Some customers subscribing to Epipe services treat the service as a wire. They can run 802.3ah between devices located at each end of the Epipe. This only applies to port-based Epipe SAPs as 802.3ah runs at the port level not at the VLAN level.

When OAMPDU tunneling is enabled, 802.3ah OAMPDUs received at one end of an Epipe are forwarded through the service. This feature must be enabled at both ends of the Epipe; when OAMPDU tunneling is disabled (by default), OAMPDUs are dropped or processed locally according to the EFM OAM configuration.

OAMPDU tunneling and 802.3ah cannot both be enabled on the same port. This is enforced by the CLI.

OAM Propagation to Attachment Circuits

Typically, T1/E1 equipment at a site relies on the physical availability of the T1/E1 ports to determine the uplink capacity. When a failure in the access link between the 7705 SAR and the T1/E1 equipment is detected, notification of the failure is propagated by the PW status signaling using one of two methods — label withdrawal or TLV (see [LDP Status Signaling on page 285](#)). In addition, the PW failure must also be propagated to the devices attached to the T1/E1 equipment. The propagation method depends on the type of port used by the access circuit (ATM, T1/E1 TDM, or Ethernet) and is described below.

ATM Ports

Propagation of ATM PW failures to the ATM port is achieved through the generation of AIS and RDI alarms.

In an HSDPA offload application, if a GRE SDP or the IP network it is riding over fails, the ATM SAPs must be rerouted to the ATM ports used for backhauling the traffic. When a fault is detected, the GRE tunnel is taken down and an SNMP trap is sent to the 5620 SAM. The 5620 SAM then reconfigures the ATM SAPs to use the network-facing ATM ports.

T1/E1 TDM Ports

If a port on a T1/E1 ASAP Adapter card is configured for CESoPSN VLL service, failure of the VLL forces a failure of the associated DS0s (timeslots). Since there can be $n \times$ DS0s bound to a CESoPSN VLL service as the attachment circuit, an alarm is propagated to the bound DS0s only. In order to emulate the failure, an 'all 1s' or an 'all 0s' signal is sent through the DS0s. The bit pattern can be configured to be either all 1s or all 0s.

Ethernet Ports

For an Ethernet port-based Ethernet VLL, failure of the VLL forces a failure of the local Ethernet port. That is, the local attachment port is taken out of service at the physical layer and the Tx is turned off on the associated Ethernet port.

LDP Status Signaling

The failure of a local circuit needs to be propagated to the far end PE, which then propagates the failure to its attached circuits. The 7705 SAR can propagate failures over the PW using one of the following methods:

- LDP status via label withdrawal
- LDP status via TLV

LDP Status via Label Withdrawal

Label withdrawal is negotiated during the PW status negotiation phase and needs to be supported by both the near-end and the far-end points. If the far-end does not support label withdrawal, the 7705 SAR still withdraws the label in case the local attachment circuit is removed or shut down.

Label withdrawal occurs only when the attachment circuit is administratively shut down or deleted. If there is a failure of the attached circuit, the label withdrawal message is not generated.

When the local circuit is re-enabled after shutdown, the VLL must be re-established, which causes some delays and signaling overhead.

LDP Status via TLV

Signaling PW status via TLV is supported as per RFC 4447. Signaling PW status via TLV is advertised during the PW capabilities negotiation phase. It is more efficient and is preferred over the label withdrawal method.

For cell mode ATM PWs, when an AIS message is received from the local attachment circuit, the AIS message is propagated to the far-end PE unaltered and PW status TLV is not initiated.

Service Assurance Agent Overview

In the last few years, service delivery to customers has drastically changed. The introduction of Broadband Service Termination Architecture (BSTA) applications such as Voice over IP (VoIP), TV delivery, video and high-speed Internet services force carriers to produce services where the health and quality of Service Level Agreement (SLA) commitments are verifiable to the customer and internally within the carrier.

SAA is a feature that monitors network operations using statistics such as latency, response time, and packet loss. The information can be used to troubleshoot network problems, and help in problem prevention, and network topology planning.

The results are saved in SNMP tables that are queried by either the CLI or a management system. Threshold monitors allow for both rising and falling threshold events to alert the provider if SLA performance statistics deviate from the required parameters.

SAA Application

SAA allows two-way timing for several applications. This provides the carrier and their customers with data to verify that the SLA agreements are being properly enforced.

Two-way time measures requests from this node to the specified DNS server. This is done by performing an address request followed by an immediate release of the acquired address once the time measurement has been performed.

Traceroute Implementation

Various applications, such as `lsp-trace`, pass through the network processor on the way to the control CPU. At this point, and when it egresses the control CPU, the network processor should insert a timestamp inside the packet. Only packets processed by the control CPU are processed.

When interpreting these timestamps, care must be taken that some nodes are not capable of providing timestamps, as such timestamps must be associated with the same IP address that is being returned to the originator to indicate what hop is being measured.

OAM and SAA List of Commands

[Table 39](#) lists the OAM and SAA commands and command uses, indicating the configuration level at which each command is implemented with a short command description.

The command list is organized in the following task-oriented manner:

- [ATM diagnostic commands](#)
- [LSP diagnostic commands](#)
- [SDP diagnostic commands](#)
- [Service diagnostic commands](#)
- [VLL diagnostic commands](#)
- [EFM diagnostic commands](#)
- [SAA configuration commands](#)
- [SAA test type configuration commands](#)

Table 39: OAM Command Summary

Command	Description	Page
ATM diagnostic commands		
oam		
atm-ping	Tests ATM path connectivity on an ATM VCC	302
LSP diagnostic commands		
oam		
lsp-ping	Verifies LSP connectivity	322
lsp-trace	Determines the hop-by-hop path for an LSP	323
SDP diagnostic commands		
oam		
sdp-mtu	Performs in-band MTU path tests on an SDP to determine the largest path-mtu supported on an SDP	304
sdp-ping	Tests an SDP for in-band unidirectional or round-trip connectivity with a round-trip time estimate	325

Table 39: OAM Command Summary (Continued)

Command	Description	Page
Service diagnostic commands		
oam		
svc-ping	Tests a service ID for correct and consistent provisioning between two service endpoints. The following information can be determined from svc-ping: <ul style="list-style-type: none"> • local and remote service existence • local and remote service state • local and remote service type correlation • local and remote customer association • local and remote service-to-SDP bindings and state • local and remote ingress and egress service label association 	306
VLL diagnostic commands		
oam		
vccv-ping	Configures a Virtual Circuit Connectivity Verification (VCCV) test	332
EFM diagnostic commands		
oam>efm		316
local-loopback	Enables local loopback tests on the specified port	316
remote-loopback	Enables remote EFM OAM loopback tests on the specified port	316
SAA configuration commands		
config>saa>test		
description	Description for this SAA test	317
latency-event	At the termination of an SAA test, evaluates the rising and falling thresholds against the configuration and generated events	320
loss-event	At the termination of an SAA test, evaluates the rising and falling thresholds against the configuration and generated events	321

Table 39: OAM Command Summary (Continued)

Command	Description	Page
shutdown	Administratively enables or disables the saa test functionality	300
type	Enables access to the context to provide the test type for the named test	332

SAA test type configuration commands

```
config>saa>test>type
```

icmp-ping	Specifies that icmp-ping packets be used for this test	318
lsp-ping	Specifies that lsp-ping packets be used for this test	322
lsp-trace	Specifies that lsp-trace packets be used for this test	323
sdp-ping	Performs an SAA test on a SDP for either one-way or two-way timing	325
vccv-ping	Configures a VCCV ping test	332

Configuring SAA Test Parameters

Use the following CLI syntax to create SAA test parameters.

Example:

```
config# saa
config>saa# test t1
config>saa>test$ type
config>saa>test>type$ lsp-ping to-104 interval 4 send-
count 5
config>saa>test>type$ exit
config>saa>test# no shutdown
config>saa>test# exit
config>saa# exit
```

The following example displays the saa test configuration output.

```
A:ALU-48>config>saa
-----
test "t1"
type
lsp-ping "to-104" interval 4 send-count 5
exit
no shutdown
exit
-----
```

The following example displays the result after running the test twice.

```
A:ALU-48>config>saa# show saa t1
Test Run: 1
Total number of attempts: 5
Number of requests that failed to be sent out: 1
Number of responses that were received: 4
Number of requests that did not receive any response: 0
Total number of failures: 1, Percentage: 20
Roundtrip Min: 0 ms, Max: 30 ms, Average: 15 ms
Per test packet:
  Sequence: 1, Result: The active lsp-id is not found., Roundtrip: 0 ms
  Sequence: 2, Result: Response Received, Roundtrip: 0 ms
  Sequence: 3, Result: Response Received, Roundtrip: 0 ms
  Sequence: 4, Result: Response Received, Roundtrip: 30 ms
  Sequence: 5, Result: Response Received, Roundtrip: 30 ms
Test Run: 2
Total number of attempts: 5
Number of requests that failed to be sent out: 0
Number of responses that were received: 5
Number of requests that did not receive any response: 0
Total number of failures: 0, Percentage: 0
Roundtrip Min: 0 ms, Max: 40 ms, Average: 14 ms
Per test packet:
  Sequence: 1, Result: Response Received, Roundtrip: 40 ms
  Sequence: 2, Result: Response Received, Roundtrip: 0 ms
  Sequence: 3, Result: Response Received, Roundtrip: 0 ms
  Sequence: 4, Result: Response Received, Roundtrip: 0 ms
  Sequence: 5, Result: Response Received, Roundtrip: 30 ms
```

OAM and SAA Command Reference

Command Hierarchies

- [Operational Commands](#)
 - [ATM Diagnostics](#)
 - [LSP Diagnostics](#)
 - [SDP Diagnostics](#)
 - [Service Diagnostics](#)
 - [VLL Diagnostics](#)
 - [Ethernet in the First Mile \(EFM\) Commands](#)
- [OAM Commands](#)
- [SAA Configuration Commands](#)
 - [SAA Diagnostics](#)
- [Show Commands](#)
- [Clear Commands](#)
- [Debug Commands](#)

Operational Commands

- global
- **ping** *[ip-address | dns-name] [rapid | detail] [ttl time-to-live] [tos type-of-service] [size bytes] [pattern pattern] [source ip-address] [interval seconds] [{next-hop ip-address | interface interface-name} | bypass-routing] [count requests] [do-not-fragment] [router router-instance] [timeout timeout]*
 - **traceroute** *[ip-address | dns-name] [ttl ttl] [wait milli-seconds] [no-dns] [source ip-address] [tos type-of-service] [router [router-instance]]*

OAM Commands

ATM Diagnostics

- global
- oam
 - **atm-ping** *port-id bundle-id[:vpi|vpi/vci] [end-to-end | segment] [dest destination-id] [send-count sendcount] [timeout timeout] [interval interval]*

LSP Diagnostics

- global
- oam
 - **lsp-ping** *prefix ip-prefix/mask [fc fc-name [profile {in | out}]] [size octets] [ttl label-ttl] [send-count send-count] [timeout timeout] [interval interval] [detail]*
 - **lsp-trace** *prefix ip-prefix/mask [max-fail no-response-count] [fc fc-name [profile {in | out}]] [probe-count probes-per-hop] [size octets] [min-ttl min-label-ttl] [max-ttl max-label-ttl] [timeout timeout] [interval interval] [detail]*

SDP Diagnostics

- global
- oam
 - **sdp-mtu** *orig-sdp-id size-inc start-octets end-octets [step step-size] [timeout timeout] [interval interval]*
 - **sdp-ping** *orig-sdp-id [resp-sdp resp-sdp-id] [fc fc-name [profile {in | out}]] [size octets] [count send-count] [timeout timeout] [interval interval]*

Service Diagnostics

- global
- oam
 - **svc-ping** *ip-address service service-id [local-sdp] [remote-sdp]*

VLL Diagnostics

```

global
  — oam
    — vccv-ping sdp-id:vc-id [src-ip-address ip-addr dst-ip-address ip-addr pw-id pw-id] [reply-mode {ip-routed | control-channel}] [fc fc-name [profile {in | out}]] [size octets] [count send-count] [timeout timeout] [interval interval] [ttl vc-label-ttl]

```

Ethernet in the First Mile (EFM) Commands

```

global
  — oam
    — efm port-id
      — local-loopback {start | stop}
      — remote-loopback {start | stop}

```

SAA Configuration Commands

```

config
  — saa
    — [no] test test-name [owner test-owner]
      — description description-string
      — no description
      — [no] latency-event rising-threshold threshold [falling-threshold threshold] [direction]
      — [no] loss-event rising-threshold threshold [falling-threshold threshold] [direction]
      — [no] shutdown
      — [no] type
        — icmp-ping ip-address|dns-name [rapid|detail] [ttl time-to-live] [tos type-of-service] [size bytes] [pattern pattern] [source ip-address] [interval seconds] [{next-hop ip-address} | {interface interface-name} | bypass-routing] [count requests] [do-not-fragment] [router router-instance] [timeout timeout]
        — lsp-ping [{lsp-name [path path-name]}] | {prefix ip-prefix/mask} [fc fc-name [profile {in | out}]] [size octets] [ttl label-ttl] [send-count send-count] [timeout timeout] [interval interval] [path-destination ip-address [interface if-name | next-hop ip-address]]
        — lsp-trace [{lsp-name [path path-name]}] | {prefix ip-prefix/mask} [fc fc-name [profile {in | out}]] [max-fail no-response-count] [probe-count probes-per-hop] [size octets] [min-ttl min-label-ttl] [max-ttl max-label-ttl] [timeout timeout] [interval interval] [path-destination ip-address [interface if-name | next-hop ip-address]]
        — sdp-ping orig-sdp-id [resp-sdp resp-sdp-id] [fc fc-name [profile {in | out}]] [size octets] [count send-count] [timeout timeout] [interval interval]
        — vccv-ping sdp-id:vc-id [src-ip-address ip-addr dst-ip-address ip-addr pw-id pw-id] [reply-mode {ip-routed | control-channel}] [fc fc-name [profile {in | out}]] [size octets] [count send-count] [timeout timeout] [interval interval] [ttl vc-label-ttl]

```

SAA Diagnostics

```
global
— oam
— saa test-name [owner test-owner] {start | stop}
```

Show Commands

```
show
— saa [test-name [owner test-owner]]
```

Clear Commands

```
clear
— saa [test-name [owner test-owner]]
```

Debug Commands

```
debug
— [no] oam
— lsp-ping-trace [tx | rx | both] [raw | detail]
— no lsp-ping-trace
```

OAM and SAA Commands

- [Operational Commands on page 298](#)
- [ATM Diagnostics on page 302](#)
- [Service Diagnostics on page 304](#)
- [EFM Commands on page 316](#)
- [Service Assurance Agent \(SAA\) Commands on page 317](#)
- [OAM SAA Commands on page 336](#)

Operational Commands

ping

Syntax	ping [<i>ip-address</i> <i>dns-name</i>] [rapid detail] [ttl <i>time-to-live</i>] [tos <i>type-of-service</i>] [size <i>bytes</i>] [pattern <i>pattern</i>] [source <i>ip-address</i>] [interval <i>interval</i>] [{ next-hop <i>ip-address</i> } { interface <i>interface-name</i> } bypass-routing] [count <i>requests</i>] [do-not-fragment] [router <i>router-instance</i>] [timeout <i>timeout</i>]
Context	<GLOBAL>
Description	This command verifies the reachability of a remote host.
Parameters	<p><i>ip-address</i> — identifies the far-end IP address to which to send the svc-ping request message in dotted decimal notation</p> <p>Values <i>ipv4-address:</i> a.b.c.d <i>dns-name</i></p> <p><i>dns-name</i> — identifies the DNS name of the far-end device to which to send the svc-ping request message, expressed as a character string</p> <p>rapid — specifies that packets will be generated as fast as possible instead of the default 1 per second</p> <p>detail — displays detailed information</p> <p>ttl <i>time-to-live</i> — specifies the TTL value for the MPLS label, expressed as a decimal integer</p> <p>Values 1 to 128</p> <p>tos <i>type-of-service</i> — specifies the service type</p> <p>Values 0 to 255</p> <p>size <i>bytes</i> — specifies the request packet size in bytes, expressed as a decimal integer</p> <p>Values 0 to 16384</p> <p>pattern <i>pattern</i> — specifies the pattern that will be used to fill the date portion in a ping packet. If no pattern is specified, position information will be filled instead</p> <p>Values 0 to 65535</p> <p>source <i>ip-address</i> — specifies the IP address to be used</p> <p>Values <i>ipv4-address:</i> a.b.c.d</p>

interval *interval* — defines the minimum amount of time, expressed as a decimal integer, that must expire before the next message request is sent.

This parameter is used to override the default request message send interval. If the **interval** is set to 1 second, and the **timeout** value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Default 1

Values 1 to 10

next-hop *ip-address* — displays only the static routes with the specified next-hop IP address

Values ipv4-address: a.b.c.d (host bits must be 0)

interface *interface-name* — specifies the name of an IP interface. The name must already exist in the **config>router>interface** context

bypass-routing — specifies whether to send the ping request to a host on a directly attached network bypassing the routing table

count *requests* — specifies the number of times to perform an OAM ping probe operation. Each OAM echo message request must either time out or receive a reply before the next message request is sent.

Values 1 to 100000

Default 5

do-not-fragment — sets the DF (Do Not Fragment) bit in the ICMP ping packet

router *router-instance* — specifies the router name or service ID

Values router-name: Base, management
service-id: 1 to 2147483647

Default Base

timeout *timeout* — specifies the amount of time that the router will wait for a message reply after sending the message request. Upon the expiration of message timeout, the requesting router assumes that the message response will not be received. Any response received after the request times out will be silently discarded.

This value is used to override the default timeout value.

Default 5

Values 1 to 10

shutdown

Syntax	[no] shutdown
Context	config>saa>test
Description	<p>The shutdown command administratively disables a test. A shutdown can only be performed if a test is not executing at the time the command is entered.</p> <p>When a test is created, it remains in shutdown mode until a no shutdown command is executed.</p> <p>In order to modify an existing test, it must first be shut down.</p> <p>The no form of this command sets the state of the test to operational.</p>

traceroute

Syntax	traceroute [<i>ip-address</i> <i>dns-name</i>] [ttl <i>ttl</i>] [wait <i>milli-seconds</i>] [no-dns] [source <i>ip-address</i>] [tos <i>type-of-service</i>] [router <i>router-instance</i>]
Context	<GLOBAL>
Description	This command determines the route to a destination address.
Parameters	<p><i>ip-address</i> — specifies the far-end IP address to which to send the traceroute request message in dotted decimal notation</p> <p>Values ipv4-address : a.b.c.d</p> <p><i>dns-name</i> — specifies the DNS name of the far-end device to which to send the traceroute request message, expressed as a character string</p> <p>ttl <i>ttl</i> — specifies the maximum Time-To-Live (TTL) value to include in the traceroute request, expressed as a decimal integer</p> <p>Values 1 to 255</p> <p>wait <i>milli-seconds</i> — specifies the time in milliseconds to wait for a response to a probe, expressed as a decimal integer</p> <p>Default 5000</p> <p>Values 10 to 60000</p> <p>no-dns — when the no-dns keyword is specified, DNS lookups of the responding hosts will not be performed; only the IP addresses will be printed</p> <p>Default DNS lookups of the responding hosts are performed</p> <p>source <i>ip-address</i> — specifies the source IP address to use as the source of the probe packets in dotted decimal notation. If the IP address is not one of the device's interfaces, an error is returned.</p>

tos *type-of-service* — specifies the type-of-service (TOS) bits in the IP header of the probe packets, expressed as a decimal integer

Values 0 to 255

router *router-instance* — specifies a router name or service ID

Default Base

Values router-name Base, management
service-id 1 to 2147483647

Output **Sample Destination Address Route**

```
*A:ALU-1# traceroute 192.168.xx.xx4
traceroute to 192.168.xx.xx4, 30 hops max, 40 byte packets
 1 192.168.xx.xx4 0.000 ms 0.000 ms 0.000 ms
*A:ALU-1#
```

ATM Diagnostics

atm-ping

Syntax `atm-ping port-id | bundle-id [:vpi | vpi/vci] [end-to-end | segment] [dest destination-id] [send-count send-count] [timeout timeout] [interval interval]`

Context oam

Description This command tests ATM path connectivity on an ATM VCC.

Parameters *port-id:vpi/vci* — specifies the ID of the access port of the target VC. This parameter is required.

Values	port-id	slot/mda/port
	bundle-id	bundle-type-slot/mda.bundle-num
	bundle	keyword
	type	ima
	bundle-num	1 to 10
	vpi	0 to 4095 (NNI)
		0 to 255 (UNI)
	vci	1, 2, 5 to 65535

end-to-end | segment — specifies whether the ATM OAM loopback cell is destined for the first segment point in the line direction or the PVCC's connection endpoint

dest destination-id — defines the LLID field in an OAM loopback cell. If set to all 1s, only the connection end (end-to-end ping) or segment end (segment ping) will respond to the ping. If the “segment” parameter is specified and 'dest' is set to a specific destination, only the destination will respond to the ping.

Values a 16-byte octet string, with each octet separated by a colon; if not specified, the value of 0x11 will be used

send-count send-count — the number of messages to send, expressed as a decimal integer. The send-count parameter is used to override the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent. The message interval value must be expired before the next message request is sent.

Default 1

Values 1 to 100

timeout timeout — specifies the amount of time that the router will wait for a message reply after sending the message request. Upon the expiration of message timeout, the requesting router assumes that the message response will not be received. Any response received after the request times out will be silently discarded.

This value is used to override the default timeout value.

Default 5

Values 1 to 10

interval *interval* — specifies the minimum amount of time that must expire before the next message request is sent.

If the **interval** is set to 1 second, and the **timeout** value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

This parameter is used to override the default request message send interval.

Default 1

Values 1 to 10

Service Diagnostics

sdp-mtu

Syntax	sdp-mtu <i>orig-sdp-id</i> size-inc <i>start-octets end-octets</i> [step <i>step-size</i>] [timeout <i>timeout</i>] [interval <i>interval</i>]
Context	oam
Description	This command performs MTU path tests on an SDP to determine the largest path-mtu supported on an SDP. The size-inc parameter can be used to easily determine the path-mtu of a given SDP-ID. The forwarding class is assumed to be Best-Effort Out-of-Profile. The message reply is returned with IP encapsulation from the far-end 7705 SAR. OAM request messages sent within an IP SDP must have the “DF” IP header bit set to 1 to prevent message fragmentation.

To terminate an **sdp-mtu** in progress, use the CLI break sequence <Ctrl-C>.

Special Cases

SDP Path MTU Tests — SDP Path MTU tests can be performed using the **sdp-mtu size-inc** keyword to easily determine the **path-mtu** of a given SDP-ID. The forwarding class is assumed to be Best-Effort Out-of-Profile. The message reply is returned with IP encapsulation from the far-end 7705 SAR.

With each OAM Echo Request sent using the **size-inc** parameter, a response line is displayed as message output. The path MTU test displays incrementing packet sizes, the number sent at each size until a reply is received and the response message.

As the request message is sent, its size value is displayed followed by a period for each request sent of that size. Up to three requests will be sent unless a valid response is received for one of the requests at that size. Once a response is received, the next size message is sent. The response message indicates the result of the message request.

After the last reply has been received or a response timeout occurs, the maximum size message replied to indicates the largest size OAM Request message that received a valid reply.

Parameters	<i>orig-sdp-id</i> — specifies the SDP-ID to be used by sdp-ping , expressed as a decimal integer. The far-end address of the specified SDP-ID is the expected <i>responder-id</i> within each reply received. The specified SDP-ID defines the SDP tunnel encapsulation used to reach the far end — GRE or MPLS. If <i>orig-sdp-id</i> is invalid or administratively down or unavailable for some reason, the SDP Echo Request message is not sent and an appropriate error message is displayed (once the interval timer expires, sdp-ping will attempt to send the next request if required).
-------------------	---

Values 1 to 17407

size-inc *start-octets end-octets* — indicates that an incremental Path MTU test will be performed by sending a series of message requests with increasing MTU sizes

start-octets — specifies the beginning size in octets of the first message sent for an incremental MTU test, expressed as a decimal integer

Values 40 to 9198

end-octets — specifies the ending size in octets of the last message sent for an incremental MTU test, expressed as a decimal integer. The specified value must be greater than *start-octets*.

Values 40 to 9198

step *step-size* — specifies the number of octets to increment the message size request for each message sent for an incremental MTU test, expressed as a decimal integer. The next size message will not be sent until a reply is received or three messages have timed out at the current size.

If the incremented size exceeds the *end-octets* value, no more messages will be sent.

Default 32

Values 1 to 512

timeout *timeout* — specifies the amount of time that the router will wait for a message reply after sending the message request. Upon the expiration of message timeout, the requesting router assumes that the message response will not be received. A “request timeout” message is displayed by the CLI for each message request sent that expires. Any response received after the request times out will be silently discarded.

This value is used to override the default **timeout** value.

Default 5

Values 1 to 10

interval *interval* — defines the minimum amount of time that must expire before the next message request is sent.

If the **interval** is set to 1 second, and the **timeout** value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

This parameter is used to override the default request message send interval.

Default 1

Values 1 to 10

Output **Sample SDP MTU Path Test Output**

```
*A:router 1> sdp-mtu 6 size-inc 512 3072 step 256
  Size      Sent      Response
  -----
    512      .      Success
    768      .      Success
   1024      .      Success
   1280      .      Success
   1536      .      Success
   1792      .      Success
   2048      .      Success
   2304      ...     Request Timeout
   2560      ...     Request Timeout
   2816      ...     Request Timeout
```

```
3072          ...      Request Timeout
Maximum Response Size: 2048
```

svc-ping

Syntax **svc-ping** *ip-address* **service** *service-id* [**local-sdp**] [**remote-sdp**]

Context oam

Description This command tests a service ID for correct and consistent provisioning between two service endpoints. The command accepts a far-end IP address and a Service-ID for local and remote service testing. The following information can be determined from **svc-ping**:

- Local and remote service existence
- Local and remote service state
- Local and remote service type correlation
- Local and remote customer association
- Local and remote service-to-SDP bindings and state
- Local and remote ingress and egress service label association

Unlike **sdp-ping**, only a single message will be sent per command; no count or interval parameter is supported and round-trip time is not calculated. A timeout value of 10 seconds is used before failing the request. The forwarding class is assumed to be Best-Effort Out-of-Profile.

If no request is sent or a reply is not received, all remote information will be shown as N/A.

To terminate an **svc-ping** in progress, use the CLI break sequence <Ctrl-C>.

Upon request timeout, message response, request termination, or request error, the following local and remote information will be displayed. Local and remote information is dependent upon service existence and reception of reply.

The following table describes the svc ping report fields.

Table 40: SVC Ping Report Fields

Field	Description	Values
Request Result	The result of the svc-ping request message	Sent - Request Timeout
		Sent - Request Terminated
		Sent - Reply Received
		Not Sent - Non-Existent Service-ID
		Not Sent - Non-Existent SDP for Service
		Not Sent - SDP For Service Down
		Not Sent - Non-existent Service Egress Label
Service-ID	The Service-ID being tested	service-id
Local Service Type	The type of service being tested. If <i>service-id</i> does not exist locally, N/A is displayed.	Epip, Apip
		TLS
		IES
		Mirror-Dest
		N/A
Local Service Admin State	The local administrative state of <i>service-id</i> . If the service does not exist locally, the administrative state will be Non-Existent.	Admin-Up
		Admin-Down
		Non-Existent
Local Service Oper State	The local operational state of <i>service-id</i> . If the service does not exist locally, the state will be N/A.	Oper-Up
		Oper-Down
		N/A
Remote Service Type	The remote type of service being tested. If <i>service-id</i> does not exist remotely, N/A is displayed.	Epip, Apip
		TLS
		IES
		Mirror-Dest
		N/A

Table 40: SVC Ping Report Fields (Continued)

Field	Description	Values
Remote Service Admin State	The remote administrative state of <i>service-id</i> . If the service does not exist remotely, the administrative state is Non-Existent.	Up Down Non-Existent
Local Service MTU	The local service-mtu for <i>service-id</i> . If the service does not exist, N/A is displayed.	service-mtu N/A
Remote Service MTU	The remote service-mtu for <i>service-id</i> . If the service does not exist remotely, N/A is displayed.	remote-service-mtu N/A
Local Customer ID	The local <i>customer-id</i> associated with <i>service-id</i> . If the service does not exist locally, N/A is displayed.	customer-id N/A
Remote Customer ID	The remote <i>customer-id</i> associated with <i>service-id</i> . If the service does not exist remotely, N/A is displayed.	customer-id N/A
Local Service IP Address	The local system IP address used to terminate a remotely configured SDP-ID (as the far-end address). If an IP interface has not been configured to be the system IP address, N/A is displayed.	system-ip-address N/A
Local Service IP Interface Name	The name of the local system IP interface. If the local system IP interface has not been created, N/A is displayed.	system-interface-name N/A
Local Service IP Interface State	The state of the local system IP interface. If the local system IP interface has not been created, Non-Existent is displayed.	Up Down Non-Existent
Expected Far-end Address	The expected IP address for the remote system IP interface. This must be the far-end address entered for the svc-ping command.	orig-sdp-far-end-addr dest-ip-addr N/A
Actual Far-end Address	The returned remote IP address. If a response is not received, the displayed value is N/A. If the far-end service IP interface is down or non-existent, a message reply is not expected. sdp-ping should also fail.	resp-ip-addr N/A

Table 40: SVC Ping Report Fields (Continued)

Field	Description	Values
Responders Expected Far-end Address	The expected source of the originator's SDP-ID from the perspective of the remote 7705 SAR terminating the SDP-ID. If the far end cannot detect the expected source of the ingress SDP-ID or the request is transmitted outside the SDP-ID, N/A is displayed.	resp-rec-tunnel-far-end-address N/A
Originating SDP-ID	The SDP-ID used to reach the far-end IP address if sdp-path is defined. The originating SDP-ID must be bound to the <i>service-id</i> and terminate on the far-end IP address. If an appropriate originating SDP-ID is not found, Non-Existent is displayed.	orig-sdp-id Non-Existent
Originating SDP-ID Path Used	Indicates whether the originating 7705 SAR used the originating SDP-ID to send the svc-ping request. If a valid originating SDP-ID is found, is operational and has a valid egress service label, the originating 7705 SAR should use the SDP-ID as the requesting path if sdp-path has been defined. If the originating 7705 SAR uses the originating SDP-ID as the request path, Yes is displayed. If the originating 7705 SAR does not use the originating SDP-ID as the request path, No is displayed. If the originating SDP-ID is non-existent, N/A is displayed.	Yes No N/A
Originating SDP-ID Administrative State	The local administrative state of the originating SDP-ID. If the SDP-ID has been shut down, Admin-Down is displayed. If the originating SDP-ID is in the no shutdown state, Admin-Up is displayed. If an originating SDP-ID is not found, N/A is displayed.	Admin-Up Admin-Down N/A
Originating SDP-ID Operating State	The local operational state of the originating SDP-ID. If an originating SDP-ID is not found, N/A is displayed.	Oper-Up Oper-Down N/A
Originating SDP-ID Binding Admin State	The local administrative state of the originating SDP-ID's binding to <i>service-id</i> . If an SDP-ID is not bound to the service, N/A is displayed.	Admin-Up Admin-Down N/A
Originating SDP-ID Binding Oper State	The local operational state of the originating SDP-ID's binding to <i>service-id</i> . If an SDP-ID is not bound to the service, N/A is displayed.	Oper-Up Oper-Down N/A

Table 40: SVC Ping Report Fields (Continued)

Field	Description	Values
Responding SDP-ID	The SDP-ID used by the far end to respond to the svc-ping request. If the request was received without the sdp-path parameter, the responding 7705 SAR will not use an SDP-ID as the return path, but the appropriate responding SDP-ID will be displayed. If a valid SDP-ID return path is not found to the originating 7705 SAR that is bound to the <i>service-id</i> , Non-Existent is displayed.	resp-sdp-id Non-Existent
Responding SDP-ID Path Used	Indicates whether the responding 7705 SAR used the responding SDP-ID to respond to the svc-ping request. If the request was received via the originating SDP-ID and a valid return SDP-ID is found, is operational and has a valid egress service label, the far-end 7705 SAR should use the SDP-ID as the return SDP-ID. If the far end uses the responding SDP-ID as the return path, Yes is displayed. If the far end does not use the responding SDP-ID as the return path, No is displayed. If the responding SDP-ID is non-existent, N/A is displayed.	Yes No N/A
Responding SDP-ID Administrative State	The administrative state of the far-end SDP-ID associated with the return path for <i>service-id</i> . When a return path is administratively down, Admin-Down is displayed. If the return SDP-ID is administratively up, Admin-Up is displayed. If the responding SDP-ID is non-existent, N/A is displayed.	Admin-Up Admin-Down N/A
Responding SDP-ID Operational State	The operational state of the far-end SDP-ID associated with the return path for <i>service-id</i> . When a return path is operationally down, Oper-Down is displayed. If the return SDP-ID is operationally up, Oper-Up is displayed. If the responding SDP-ID is non-existent, N/A is displayed.	Oper-Up Oper-Down N/A
Responding SDP-ID Binding Admin State	The local administrative state of the responder's SDP-ID binding to <i>service-id</i> . If an SDP-ID is not bound to the service, N/A is displayed.	Admin-Up Admin-Down N/A
Responding SDP-ID Binding Oper State	The local operational state of the responder's SDP-ID binding to <i>service-id</i> . If an SDP-ID is not bound to the service, N/A is displayed.	Oper-Up Oper-Down N/A
Originating VC-ID	The originator's VC-ID associated with the SDP-ID to the far-end address that is bound to <i>service-id</i> . If the SDP-ID signaling is off, <i>originator-vc-id</i> is 0. If the <i>originator-vc-id</i> does not exist, N/A is displayed.	originator-vc-id N/A

Table 40: SVC Ping Report Fields (Continued)

Field	Description	Values
Responding VC-ID	The responder's VC-ID associated with the SDP-ID to <i>originator-id</i> that is bound to <i>service-id</i> . If the SDP-ID signaling is off or the service binding to SDP-ID does not exist, <i>responder-vc-id</i> is 0. If a response is not received, N/A is displayed.	responder-vc-id N/A
Originating Egress Service Label	The originating service label (VC-Label) associated with the <i>service-id</i> for the originating SDP-ID. If <i>service-id</i> does not exist locally, N/A is displayed. If <i>service-id</i> exists, but the egress service label has not been assigned, Non-Existent is displayed.	egress-vc-label N/A Non-Existent
Originating Egress Service Label Source	The originating egress service label source. If the displayed egress service label is manually defined, Manual is displayed. If the egress service label is dynamically signaled, Signaled is displayed. If the <i>service-id</i> does not exist or the egress service label is non-existent, N/A is displayed.	Manual Signaled N/A
Originating Egress Service Label State	The originating egress service label state. If the originating 7705 SAR considers the displayed egress service label operational, Up is displayed. If the originating 7705 SAR considers the egress service label inoperative, Down is displayed. If the <i>service-id</i> does not exist or the egress service label is non-existent, N/A is displayed.	Up Down N/A
Responding Service Label	The actual responding service label in use by the far-end 7705 SAR for this <i>service-id</i> to the originating 7705 SAR. If <i>service-id</i> does not exist in the remote 7705 SAR, N/A is displayed. If <i>service-id</i> does exist remotely but the remote egress service label has not been assigned, Non-Existent is displayed.	rec-vc-label N/A Non-Existent
Responding Egress Service Label Source	The responder's egress service label source. If the responder's egress service label is manually defined, Manual is displayed. If the responder's egress service label is dynamically signaled, Signaled is displayed. If the <i>service-id</i> does not exist on the responder or the responder's egress service label is non-existent, N/A is displayed.	Manual Signaled N/A
Responding Service Label State	The responding egress service label state. If the responding considers its egress service label operational, Up is displayed. If the responding 7705 SAR considers its egress service label inoperative, Down is displayed. If the <i>service-id</i> does not exist or the responder's egress service label is non-existent, N/A is displayed.	Up Down N/A

Table 40: SVC Ping Report Fields (Continued)

Field	Description	Values
Expected Ingress Service Label	The locally assigned ingress service label. This is the service label that the far end is expected to use for <i>service-id</i> when sending to the originating 7705 SAR. If <i>service-id</i> does not exist locally, N/A is displayed. If <i>service-id</i> exists but an ingress service label has not been assigned, Non-Existent is displayed.	ingress-vc-label N/A Non-Existent
Expected Ingress Label Source	The originator's ingress service label source. If the originator's ingress service label is manually defined, Manual is displayed. If the originator's ingress service label is dynamically signaled, Signaled is displayed. If the <i>service-id</i> does not exist on the originator or the originator's ingress service label has not been assigned, N/A is displayed.	Manual Signaled N/A
Expected Ingress Service Label State	The originator's ingress service label state. If the originating 7705 SAR considers its ingress service label operational, Up is displayed. If the originating 7705 SAR considers its ingress service label inoperative, Down is displayed. If the <i>service-id</i> does not exist locally, N/A is displayed.	Up Down N/A
Responders Ingress Service Label	The assigned ingress service label on the remote 7705 SAR. This is the service label that the far end is expecting to receive for <i>service-id</i> when sending to the originating 7705 SAR. If <i>service-id</i> does not exist in the remote 7705 SAR, N/A is displayed. If <i>service-id</i> exists, but an ingress service label has not been assigned in the remote 7705 SAR, Non-Existent is displayed.	resp-ingress-vc-label N/A Non-Existent
Responders Ingress Label Source	The assigned ingress service label source on the remote 7705 SAR. If the ingress service label is manually defined on the remote 7705 SAR, Manual is displayed. If the ingress service label is dynamically signaled on the remote 7705 SAR, Signaled is displayed. If the <i>service-id</i> does not exist on the remote 7705 SAR, N/A is displayed.	Manual Signaled N/A
Responders Ingress Service Label State	The assigned ingress service label state on the remote 7705 SAR. If the remote 7705 SAR considers its ingress service label operational, Up is displayed. If the remote 7705 SAR considers its ingress service label inoperative, Down is displayed. If the <i>service-id</i> does not exist on the remote 7705 SAR or the ingress service label has not been assigned on the remote 7705 SAR, N/A is displayed.	Up Down N/A

Parameters *ip-address* — specifies the far-end IP address to which to send the **svc-ping** request message in dotted decimal notation

service *service-id* — identifies the service being tested. The Service ID need not exist on the local 7705 SAR to receive a reply message.

This is a mandatory parameter.

Values 1 to 2147483647

local-sdp — specifies that the **svc-ping** request message should be sent using the same service tunnel encapsulation labeling as service traffic.

If **local-sdp** is specified, the command attempts to use an egress SDP-ID bound to the service with the specified **far-end** IP address with the VC-Label for the service. The far-end address of the specified SDP-ID is the expected *responder-id* within the reply received. The SDP-ID defines the SDP tunnel encapsulation used to reach the far end — GRE or MPLS. On originator egress, the service-ID must have an associated VC-Label to reach the far-end address of the SDP-ID and the SDP-ID must be operational for the message to be sent.

If **local-sdp** is not specified, the **svc-ping** request message is sent with GRE encapsulation with the OAM label.

[Table 41](#) indicates whether a message is sent and how the message is encapsulated based on the state of the service ID.

Table 41: Local SDP Message Results

Local Service State	local-sdp Not Specified		local-sdp Specified	
	Message Sent	Message Encapsulation	Message Sent	Message Encapsulation
Invalid Local Service	Yes	Generic IP/GRE OAM (PLP)	No	None
No Valid SDP-ID Bound	Yes	Generic IP/GRE OAM (PLP)	No	None
SDP-ID Valid But Down	Yes	Generic IP/GRE OAM (PLP)	No	None
SDP-ID Valid and Up, But No Service Label	Yes	Generic IP/GRE OAM (PLP)	No	None
SDP-ID Valid, Up and Egress Service Label	Yes	Generic IP/GRE OAM (PLP)	Yes	SDP Encapsulation with Egress Service Label (SLP)

remote-sdp — specifies that the **svc-ping** reply message from the **far-end** should be sent using the same service tunnel encapsulation labeling as service traffic.

If **remote-sdp** is specified, the **far-end** responder attempts to use an egress SDP-ID bound to the service with the message originator as the destination IP address with the VC-Label for the service. The SDP-ID defines the SDP tunnel encapsulation used to reply to the originator — GRE or MPLS. On responder egress, the service-ID must have an associated VC-Label to reach the originator address of the SDP-ID and the SDP-ID must be operational for the message to be sent. If **remote-sdp** is not specified, the **svc-ping** request message is sent with GRE encapsulation with the OAM label.

Table 42 indicates how the message response is encapsulated based on the state of the remote Service ID.

Table 42: Remote SDP Message Results

Remote Service State	Message Encapsulation	
	remote-sdp Not Specified	remote-sdp Specified
Invalid Ingress Service Label	Generic IP/GRE OAM (PLP)	Generic IP/GRE OAM (PLP)
Invalid Service-ID	Generic IP/GRE OAM (PLP)	Generic IP/GRE OAM (PLP)
No Valid SDP-ID Bound on Service-ID	Generic IP/GRE OAM (PLP)	Generic IP/GRE OAM (PLP)
SDP-ID Valid But Down	Generic IP/GRE OAM (PLP)	Generic IP/GRE OAM (PLP)
SDP-ID Valid and Up, but No Service Label	Generic IP/GRE OAM (PLP)	Generic IP/GRE OAM (PLP)
SDP-ID Valid and Up, Egress Service Label, but VC-ID Mismatch	Generic IP/GRE OAM (PLP)	Generic IP/GRE OAM (PLP)
SDP-ID Valid and Up, Egress Service Label, but VC-ID Match	Generic IP/GRE OAM (PLP)	SDP Encapsulation with Egress Service Label (SLP)

Sample Output

```
*A:router1> svc-ping far-end 10.10.10.10 service 101 local-sdp remote-sdp
Service-ID: 101
```

```
Err Info          Local          Remote
-----
Type:             CPIPE          CPIPE
Admin State:      Up              Up
Oper State:       Up              Up
Service-MTU:      1000            1000
Customer ID:      1001            1001

==> IP Interface State: Down
Actual IP Addr:    10.10.10.11      10.10.10.10
Expected Peer IP:  10.10.10.10      10.10.10.11

==> SDP Path Used:  Yes             Yes
SDP-ID:            123             325
Admin State:       Up              Up
Operative State:   Up              Up
Binding Admin State: Up            Up
Binding Oper State: Up            Up
Binding VC ID:     101             101
Binding Type:      Spoke           Spoke
Binding Vc-type:   CesoPsn         CesoPsn
Binding Vlan-vc-tag: 0              0
```

```
==> Egress Label:      131066      131064
      Ingress Label:    131064      131066
      Egress Label Type: Signaled    Signaled
      Ingress Label Type: Signaled   Signaled
```

```
Request Result: Sent - Reply Received
```

EFM Commands

efm

Syntax	efm <i>port-id</i>
Context	oam
Description	This command enables Ethernet in the First Mile (EFM) OAM loopbacks on the specified port. The EFM OAM remote loopback OAMPDU will be sent to the peering device to trigger a remote loopback.
Parameters	<i>port-id</i> — specifies the port ID in the <i>slot/mda/port</i> format

local-loopback

Syntax	local-loopback { start stop }
Context	oam>efm
Description	This command enables local loopback tests on the specified port.

remote-loopback

Syntax	remote-loopback { start stop }
Context	oam>efm
Description	This command enables remote EFM OAM loopback tests on the specified port. The EFM OAM remote loopback OAMPDU will be sent to the peering device to trigger a remote loopback.

Service Assurance Agent (SAA) Commands

saa

Syntax	saa
Context	config
Description	This command creates the context to configure the SAA tests.

test

Syntax	test <i>test-name</i> [owner <i>test-owner</i>] [no] test <i>test-name</i> [owner <i>test-owner</i>]
Context	config>saa
Description	<p>This command identifies a test and creates or modifies the context to provide the test parameters for the named test. Subsequent to the creation of the test instance, the test can be started in the OAM context.</p> <p>A test must be shut down before it can be modified or removed from the configuration.</p> <p>The no form of this command removes the test from the configuration.</p>
Parameters	<p><i>test-name</i> — identifies the saa test name to be created or edited</p> <p>owner <i>test-owner</i> — specifies the owner of an SAA operation, up to 32 characters in length</p>
Values	if a <i>test-owner</i> value is not specified, tests created by the CLI have a default owner "TiMOS CLI"

description

Syntax	description <i>description-string</i> no description
Context	config>saa>test
Description	<p>This command creates a text description stored in the configuration file for a configuration context.</p> <p>The no form of this command removes the string from the configuration.</p>
Default	No description associated with the configuration context.

Parameters *description-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.

icmp-ping

Syntax **icmp-ping** [*ip-address* | *dns-name*] [**rapid** | **detail**] [**ttl** *time-to-live*] [**tos** *type-of-service*] [**size** *bytes*] [**pattern** *pattern*] [**source** *ip-address*] [**interval** *seconds*] [{**next-hop** *ip-address*} | {**interface** *interface-name/bypass-routing*}] [**count** *requests*] [**do-not-fragment**] [**router** *router-instance*] [**timeout** *timeout*]

Context **config>saa>test>type**

Description This command configures an ICMP traceroute test.

Parameters *ip-address* — identifies the far-end IP address to which to send the **icmp-ping** request message in dotted decimal notation

Values ipv4-address: a.b.c.d

dns-name — identifies the DNS name of the far-end device to which to send the **icmp-ping** request message, expressed as a character string to a maximum of 63 characters

Values 128 characters maximum

rapid — specifies that packets will be generated as fast as possible instead of the default 1 per second

detail — displays detailed information

ttl *time-to-live* — specifies the TTL value for the MPLS label, expressed as a decimal integer

Default 64

Values 1 to 128

tos *type-of-service* — specifies the service type

Default 0

Values 0 to 255

size *bytes* — specifies the request packet size in bytes, expressed as a decimal integer

Default 56

Values 0 to 16384

pattern *pattern* — specifies the pattern that will be used to fill the data portion in a ping packet. If no pattern is specified, position information will be filled instead.

Values 0 to 65535

source *ip-address* — specifies the IP address to be used

Values ipv4-address: a.b.c.d

interval *seconds* — defines the minimum amount of time, expressed as a decimal integer, that must expire before the next message request is sent.

This parameter is used to override the default request message send interval. If the **interval** is set to 1 second, and the **timeout** value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Default 1

Values 1 to 10000

next-hop *ip-address* — displays only the static routes with the specified next-hop IP address

Values ipv4-address: a.b.c.d (host bits must be 0)

interface *interface-name* — specifies the name of an IP interface. The name must already exist in the **config>router>interface** context.

bypass-routing — specifies whether to send the ping request to a host on a directly attached network bypassing the routing table

count *requests* — specifies the number of times to perform an OAM ping probe operation. Each OAM echo message request must either time out or receive a reply before the next message request is sent.

Values 1 to 100000

Default 5

do-not-fragment — sets the DF (Do Not Fragment) bit in the ICMP ping packet

router *router-instance* — specifies the router name or service ID

Values router-name: Base, management
service-id: 1 to 2147483647

Default Base

timeout *timeout* — specifies the amount of time that the router will wait for a message reply after sending the message request. Upon the expiration of message timeout, the requesting router assumes that the message response will not be received. A “request timeout” message is displayed by the CLI for each message request sent that expires. Any response received after the request times out will be silently discarded.

This value is used to override the default timeout value.

Default 5

Values 1 to 10

latency-event

Syntax	[no] latency-event rising-threshold <i>threshold</i> [falling-threshold <i>threshold</i>] [<i>direction</i>]
Context	config>saa>test
Description	<p>This command specifies that at the termination of an SAA test probe, the calculated latency event value is evaluated against the configured rising and falling latency event thresholds. SAA threshold events are generated as required.</p> <p>The configuration of latency event thresholds is optional.</p>
Parameters	<p>rising-threshold <i>threshold</i> — specifies a rising threshold latency value. When the test run is completed, the calculated latency value is compared to the configured latency rising threshold. If the test run latency value is greater than the configured rising threshold value, then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.</p> <p>Default 0</p> <p>Values 0 to 2147483647 ms</p> <p>falling-threshold <i>threshold</i> — specifies a falling threshold latency value. When the test run is completed, the calculated latency value is compared to the configured latency falling threshold. If the test run latency value is greater than the configured falling threshold value, then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.</p> <p>Default 0</p> <p>Values 0 to 2147483647 ms</p> <p><i>direction</i> — specifies the direction for OAM ping responses received for an OAM ping test run</p> <p>Values</p> <ul style="list-style-type: none"> inbound — monitors the value of jitter calculated for the inbound, one-way, OAM ping responses received for an OAM ping test run outbound — monitors the value of jitter calculated for the outbound, one-way, OAM ping requests sent for an OAM ping test run roundtrip — monitors the value of jitter calculated for the round-trip, two-way, OAM ping requests and replies for an OAM ping test run <p>Default roundtrip</p>

loss-event

Syntax	[no] loss-event rising-threshold <i>threshold</i> [falling-threshold <i>threshold</i>] [direction]
Context	config>saa>test
Description	<p>This command specifies that at the termination of an SAA test run, the calculated loss event value is evaluated against the configured rising and falling loss event thresholds. SAA threshold events are generated as required.</p> <p>The configuration of loss event thresholds is optional.</p>
Parameters	<p>rising-threshold <i>threshold</i> — specifies a rising threshold loss event value. When the test run is completed, the calculated loss event value is compared to the configured loss event rising threshold. If the test run loss event value is greater than the configured rising threshold value, then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.</p> <p>Default 0</p> <p>Values 0 to 2147483647 packets</p> <p>falling-threshold <i>threshold</i> — specifies a falling threshold loss event value. When the test run is completed, the calculated loss event value is compared to the configured loss event falling threshold. If the test run loss event value is greater than the configured falling threshold value, then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.</p> <p>Default 0</p> <p>Values 0 to 2147483647 packets</p> <p>direction — specifies the direction for OAM ping responses received for an OAM ping test run</p> <p>Values</p> <ul style="list-style-type: none"> inbound — monitors the value of jitter calculated for the inbound, one-way, OAM ping responses received for an OAM ping test run outbound — monitors the value of jitter calculated for the outbound, one-way, OAM ping requests sent for an OAM ping test run roundtrip — monitors the value of jitter calculated for the round-trip, two-way, OAM ping requests and replies for an OAM ping test run <p>Default roundtrip</p>

lsp-ping

Syntax	lsp-ping prefix <i>ip-prefix/mask</i> [fc <i>fc-name</i> [profile { in out }]] [size <i>octets</i>] [ttl <i>label-ttl</i>] [send-count <i>send-count</i>] [timeout <i>timeout</i>] [interval <i>interval</i>] [detail]												
Context	oam config>saa>test>type												
Description	<p>This command performs in-band LSP connectivity tests using the protocol and data structures defined in RFC 4379, <i>Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures</i>.</p> <p>The LSP ping operation is modeled after the IP ping utility, which uses ICMP echo request and reply packets to determine IP connectivity.</p> <p>In an LSP ping, the originating device creates an MPLS echo request packet for the LSP and path to be tested. The MPLS echo request packet is sent through the data plane and awaits an MPLS echo reply packet from the device terminating the LSP. The status of the LSP is displayed when the MPLS echo reply packet is received.</p> <p>The detail parameter is available only from the oam context.</p>												
Parameters	<p>prefix <i>ip-prefix/mask</i> — Specifies the address prefix and subnet mask of the destination node</p> <p>Values</p> <table> <tr> <td>ipv4-address:</td><td>a.b.c.d</td></tr> <tr> <td>mask:</td><td>value must be 32</td></tr> </table> <p>fc <i>fc-name</i> — Indicates the forwarding class of the MPLS echo request packets. The actual forwarding class encoding is controlled by the network egress LSP-EXP mappings.</p> <p>The LSP-EXP mappings on the receive network interface control the mapping back to the internal forwarding class used by the far-end 7705 SAR that receives the message request. The egress mappings of the egress network interface on the far-end 7705 SAR control the forwarding class markings on the return reply message.</p> <p>The LSP-EXP mappings on the receive network interface control the mapping of the message reply back at the originating 7705 SAR.</p> <p>Default be</p> <p>Values be, l2, af, l1, h2, ef, h1, nc</p> <p>profile {in out} — Specifies the profile state of the MPLS echo request encapsulation</p> <p>Default out</p> <p>size <i>octets</i> — Specifies the MPLS echo request packet size in octets, expressed as a decimal integer. The request payload is padded with zeroes to the specified size.</p> <p>Default</p> <table> <tr> <td>80</td><td>— Prefix-specified ping</td></tr> <tr> <td>92</td><td>— LSP name-specified ping</td></tr> </table> <p>The system sends the minimum packet size, depending on the type of LSP. No padding is added</p> <p>Values</p> <table> <tr> <td>80, and 85 to 1500</td><td>— Prefix-specified ping</td></tr> <tr> <td>92, and 97 to 1500</td><td>— LSP name-specified ping</td></tr> </table>	ipv4-address:	a.b.c.d	mask:	value must be 32	80	— Prefix-specified ping	92	— LSP name-specified ping	80, and 85 to 1500	— Prefix-specified ping	92, and 97 to 1500	— LSP name-specified ping
ipv4-address:	a.b.c.d												
mask:	value must be 32												
80	— Prefix-specified ping												
92	— LSP name-specified ping												
80, and 85 to 1500	— Prefix-specified ping												
92, and 97 to 1500	— LSP name-specified ping												

ttl *label-ttl* — Specifies the TTL value for the MPLS label, expressed as a decimal integer

Default 255

Values 1 to 255

send-count *send-count* — The number of messages to send, expressed as a decimal integer. The send-count parameter is used to override the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent. The message interval value must be expired before the next message request is sent.

Default 1

Values 1 to 100

timeout *timeout* — Specifies the amount of time that the router will wait for a message reply after sending the message request. Upon the expiration of message timeout, the requesting router assumes that the message response will not be received. A “request timeout” message is displayed by the CLI for each message request sent that expires. Any response received after the request times out will be silently discarded.

This value is used to override the default timeout value.

Default 5

Values 1 to 10

interval *interval* — Specifies the minimum amount of time that must expire before the next message request is sent.

If the **interval** is set to 1 second, and the **timeout** value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

This parameter is used to override the default request message send interval.

Default 1

Values 1 to 10

detail — Displays detailed information

lsp-trace

Syntax **lsp-trace prefix** *ip-prefix/mask* [**max-fail** *no-response-count*] [**fc** *fc-name* [**profile** {*in* | *out*}]] [**probe-count** *probes-per-hop*] [**size** *octets*] [**min-ttl** *min-label-ttl*] [**max-ttl** *max-label-ttl*] [**timeout** *timeout*] [**interval** *interval*] [**detail**]

Context oam
config>saa>test>type

Description This command displays the hop-by-hop path for an LSP traceroute using the protocol and data structures defined in RFC 4379 *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*.

The LSP traceroute operation is modeled after the IP traceroute utility, which uses ICMP echo request and reply packets with increasing TTL values to determine the hop-by-hop route to a destination IP.

In an LSP traceroute, the originating device creates an MPLS echo request packet for the LSP to be tested with increasing values of the TTL in the outermost label. The MPLS echo request packet is sent through the data plane and awaits a TTL exceeded response or the MPLS echo reply packet from the device terminating the LSP. The devices that reply to the MPLS echo request packets with the TTL exceeded and the MPLS echo reply are displayed.

The `detail` parameter is available only from the `oam` context.

Parameters **prefix** *ip-prefix/mask* — Specifies the address prefix and subnet mask of the destination node

Values **ipv4-address:** a.b.c.d (host bits must be 0)
 mask: 0 to 32

size *octets* — Specifies the MPLS echo request packet size in octets, expressed as a decimal integer. The request payload is padded with zeroes to the specified size.

Default 104 — The system sends the minimum packet size, depending on the type of LSP. No padding is added.

Values 104 to 1500

min-ttl *min-label-ttl* — Specifies the minimum TTL value in the MPLS label for the LSP trace test, expressed as a decimal integer

Default 1

Values 1 to 255

max-ttl *max-label-ttl* — Specifies the maximum TTL value in the MPLS label for the LDP trace test, expressed as a decimal integer

Default 30

Values 1 to 255

max-fail *no-response-count* — Specifies the maximum number of consecutive MPLS echo requests, expressed as a decimal integer, that do not receive a reply before the trace operation fails for a given TTL

Default 5

Values 1 to 255

probe-count *probes-per-hop* — Specifies the number of OAM requests sent for a particular TTL value, expressed as a decimal integer

Default 1

Values 1 to 10

timeout *timeout* — Specifies the amount of time that the router will wait for a message reply after sending the message request. Upon the expiration of message timeout, the requesting router assumes that the message response will not be received. A “request timeout” message is displayed by the CLI for each message request sent that expires. Any response received after the request times out will be silently discarded.

This value is used to override the default timeout value.

Default 3

Values 1 to 60

interval *interval* — Specifies the minimum amount of time that must expire before the next message request is sent.

If the **interval** is set to 1 second, and the **timeout** value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

This parameter is used to override the default request message send interval.

Default 1

Values 1 to 10

detail — Displays detailed information

fc *fc-name* — Indicates the forwarding class of the MPLS echo request packets. The actual forwarding class encoding is controlled by the network egress LSP-EXP mappings.

The LSP-EXP mappings on the receive network interface control the mapping back to the internal forwarding class used by the far-end 7705 SAR that receives the message request. The egress mappings of the egress network interface on the far-end 7705 SAR control the forwarding class markings on the return reply message.

The LSP-EXP mappings on the receive network interface control the mapping of the message reply back at the originating 7705 SAR.

Default be

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

profile {**in** | **out**} — Specifies the profile state of the MPLS echo request encapsulation

Default out

sdp-ping

Syntax **sdp-ping** *orig-sdp-id* [**resp-sdp** *resp-sdp-id*] [**fc** *fc-name* [**profile** {**in** | **out**}]] [**timeout** *timeout*] [**interval** *interval*] [**size** *octets*] [**count** *send-count*]

Context config>saa>test>type

Description This command tests SDPs for unidirectional or round-trip connectivity and performs SDP MTU path tests.

The **sdp-ping** command accepts an originating SDP-ID and an optional responding SDP-ID. The size, number of requests sent, message time out and message send interval can be specified. All sdp-ping requests and replies are sent with PLP OAM-Label encapsulation, as a service-id is not specified.

For round-trip connectivity testing, the **resp-sdp** keyword must be specified. If resp-sdp is not specified, a unidirectional SDP test is performed.

To terminate an sdp-ping in progress, use the CLI break sequence <Ctrl-C>.

An sdp-ping response message indicates the result of the sdp-ping message request. When multiple response messages apply to a single SDP Echo Request/Reply sequence, the response message with the highest precedence will be displayed. The following table displays the response messages sorted by precedence.

Table 43: SDP Ping Response Messages

Result of Request	Displayed Response Message	Precedence
Request timeout without reply	Request Timeout	1
Request not sent due to non-existent <i>orig-sdp-id</i>	Orig-SDP Non-Existent	2
Request not sent due to administratively down <i>orig-sdp-id</i>	Orig-SDP Admin-Down	3
Request not sent due to operationally down <i>orig-sdp-id</i>	Orig-SDP Oper-Down	4
Request terminated by user before reply or timeout	Request Terminated	5
Reply received, invalid <i>origination-id</i>	Far End: Originator-ID Invalid	6
Reply received, invalid <i>responder-id</i>	Far End: Responder-ID Error	7
Reply received, non-existent <i>resp-sdp-id</i>	Far End: Resp-SDP Non-Existent	8
Reply received, invalid <i>resp-sdp-id</i>	Far End: Resp-SDP Invalid	9
Reply received, <i>resp-sdp-id</i> down (admin or oper)	Far-end: Resp-SDP Down	10
Reply received, No Error	Success	11

Parameters *orig-sdp-id* — The SDP-ID to be used by sdp-ping, expressed as a decimal integer. The far-end address of the specified SDP-ID is the expected responder-id within each reply received. The specified SDP-ID defines the SDP tunnel encapsulation used to reach the far end — GRE or MPLS. If orig-sdp-id is invalid or administratively down or unavailable for some reason, the SDP Echo Request message is not sent and an appropriate error message is displayed (once the interval timer expires, sdp-ping will attempt to send the next request if required).

Values 1 to 17407

resp-sdp *resp-sdp-id* — Specifies the return SDP-ID to be used by the far-end 7705 SAR for the message reply for round-trip SDP connectivity testing. If resp-sdp-id does not exist on the far-end 7705 SAR, terminates on another 7705 SAR different from the originating 7705 SAR, or another issue prevents the far-end 7705 SAR from using resp-sdp-id, the SDP Echo Reply will be sent using generic OAM encapsulation. The received forwarding class (as mapped on the ingress network interface for the far end) defines the forwarding class encapsulation for the reply message.

This is an optional parameter.

Default null. Use the non-SDP return path for message reply.

Values 1 to 17407

fc *fc-name* — Indicates the forwarding class of the SDP encapsulation. The actual forwarding class encoding is controlled by the network egress DSCP or LSP-EXP mappings.

The DSCP or LSP-EXP mappings on the receive network interface control the mapping back to the internal forwarding class used by the far-end 7705 SAR that receives the message request. The egress mappings of the egress network interface on the far-end 7705 SAR control the forwarding class markings on the return reply message.

The DSCP or LSP-EXP mappings on the receive network interface control the mapping of the message reply back at the originating 7705 SAR. This is displayed in the response message output upon receipt of the message reply.

Default be

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

profile {*in* | *out*} — Specifies the profile state of the SDP encapsulation

Default out

timeout *timeout* — Specifies the amount of time that the router will wait for a message reply after sending the message request. Upon the expiration of message timeout, the requesting router assumes that the message response will not be received. A “request timeout” message is displayed by the CLI for each message request sent that expires. Any response received after the request times out will be silently discarded.

This value is used to override the default timeout value.

Default 5

Values 1 to 10

interval *interval* — Specifies the minimum amount of time that must expire before the next message request is sent.

If the **interval** is set to 1 second, and the **timeout** value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

This parameter is used to override the default request message send interval.

Default 1

Values 1 to 10

size *octets* — The size parameter in octets, expressed as a decimal integer. This parameter is used to override the default message size for the sdp-ping request. Changing the message size is a method of checking the ability of an SDP to support a path-mtu. The size of the message does not include the SDP encapsulation, VC-Label (if applied) or any DLC headers or trailers.

When the OAM message request is encapsulated in an SDP, the IP “DF” (Do Not Fragment) bit is set. If any segment of the path between the sender and receiver cannot handle the message size, the message is discarded. MPLS LSPs are not expected to fragment the message either, as the message contained in the LSP is not an IP packet.

Default 40

Values 72 to 1500

count *send-count* — The number of messages to send, expressed as a decimal integer. The count parameter is used to override the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent. The message interval value must be expired before the next message request is sent.

Default 1

Values 1 to 100

Special Cases

Single Response Connectivity Tests — A single response sdp-ping test provides detailed test results.

Upon request timeout, message response, request termination, or request error, the following local and remote information will be displayed. Local and remote information will be dependent upon SDP-ID existence and reception of reply.

Table 44: Single Response Connectivity

Field	Description	Values
Request Result	The result of the sdp-ping request message	Sent - Request Timeout Sent - Request Terminated Sent - Reply Received Not Sent - Non-Existent Local SDP-ID Not Sent - Local SDP-ID Down
Originating SDP-ID	The originating SDP-ID specified by orig-sdp	orig-sdp-id
Originating SDP-ID Administrative State	The local administrative state of the originating SDP-ID. If the SDP-ID has been shut down, Admin-Down is displayed. If the originating SDP-ID is in the no shutdown state, Admin-Up is displayed. If the <i>orig-sdp-id</i> does not exist, Non-Existent is displayed.	Admin-Up Admin-Down Non-Existent
Originating SDP-ID Operating State	The local operational state of the originating SDP-ID. If <i>orig-sdp-id</i> does not exist, N/A will be displayed.	Oper-Up Oper-Down N/A
Originating SDP-ID Path MTU	The local path-mtu for <i>orig-sdp-id</i> . If <i>orig-sdp-id</i> does not exist locally, N/A is displayed.	orig-path-mtu N/A
Responding SDP-ID	The SDP-ID requested as the far-end path to respond to the sdp-ping request. If resp-sdp is not specified, the responding 7705 SAR will not use an SDP-ID as the return path and N/A will be displayed.	resp-sdp-id N/A
Responding SDP-ID Path Used	Displays whether the responding 7705 SAR used the responding SDP-ID to respond to the sdp-ping request. If <i>resp-sdp-id</i> is a valid, operational SDP-ID, it must be used for the SDP Echo Reply message. If the far end uses the responding SDP-ID as the return path, Yes will be displayed. If the far end does not use the responding SDP-ID as the return path, No will be displayed. If resp-sdp is not specified, N/A will be displayed.	Yes No N/A

Table 44: Single Response Connectivity (Continued)

Field	Description	Values
Responding SDP-ID Administrative State	The administrative state of the responding SDP-ID. When <i>resp-sdp-id</i> is administratively down, Admin-Down will be displayed. When <i>resp-sdp-id</i> is administratively up, Admin-Up will be displayed. When <i>resp-sdp-id</i> exists on the far-end 7705 SAR but is not valid for the originating 7705 SAR, Invalid is displayed. When <i>resp-sdp-id</i> does not exist on the far-end 7705 SAR, Non-Existent is displayed. When resp-sdp is not specified, N/A is displayed.	Admin-Down Admin-Up Invalid Non-Existent N/A
Responding SDP-ID Operational State	The operational state of the far-end SDP-ID associated with the return path for <i>service-id</i> . When a return path is operationally down, Oper-Down is displayed. If the return SDP-ID is operationally up, Oper-Up is displayed. If the responding SDP-ID is non-existent, N/A is displayed.	Oper-Up Oper-Down N/A
Responding SDP-ID Path MTU	The remote path-mtu for <i>resp-sdp-id</i> . If <i>resp-sdp-id</i> does not exist remotely, N/A is displayed.	resp-path-mtu N/A
Local Service IP Address	The local system IP address used to terminate remotely configured SDP-IDs (as the SDP-ID far-end address). If an IP address has not been configured to be the system IP address, N/A is displayed.	system-ip-addr N/A
Local Service IP Interface Name	The name of the local system IP interface. If the local system IP interface has not been created, N/A is displayed.	system-interface-name N/A
Local Service IP Interface State	The state of the local system IP interface. If the local system IP interface has not been created, Non-Existent is displayed.	Up Down Non-Existent
Expected Far End Address	The expected IP address for the remote system IP interface. This must be the far-end address configured for the <i>orig-sdp-id</i> .	orig-sdp-far-end-addr dest-ip-addr N/A
Actual Far End Address	The returned remote IP address. If a response is not received, the displayed value is N/A. If the far-end service IP interface is down or non-existent, a message reply is not expected.	resp-ip-addr N/A
Responders Expected Far End Address	The expected source of the originator's SDP-ID from the perspective of the remote 7705 SAR terminating the SDP-ID. If the far end cannot detect the expected source of the ingress SDP-ID, N/A is displayed.	resp-rec-tunnel-far-end-addr N/A
Round Trip Time	The round-trip time between SDP Echo Request and the SDP Echo Reply. If the request is not sent, times out or is terminated, N/A is displayed.	delta-request-reply N/A

Single Response Round-trip Connectivity Test Sample Output

```
A:router1> oam sdp-ping 10 resp-sdp 22 fc ef
Err SDP-ID Info Local Remote
-----
SDP-ID: 10 22
Administrative State: Up Up
Operative State: Up Up
Path MTU: 4470 4470
Response SDP Used: Yes

==> IP Interface State: Up
Actual IP Address: 10.10.10.11 10.10.10.10
Expected Peer IP: 10.10.10.10 10.10.10.11

Forwarding Class ef ef
Profile Out Out

Request Result: Sent - Reply Received
RTT: 30ms
```

Multiple Response Connectivity Tests — When the connectivity test count is greater than one (1), a single line is displayed per SDP Echo Request send attempt.

The request number is a sequential number starting with 1 and ending with the last request sent, incrementing by one for each request. This should not be confused with the message-id contained in each request and reply message.

A response message indicates the result of the message request. Following the response message is the round-trip time value. If any reply is received, the round-trip time is displayed.

After the last reply has been received or response timed out, a total is displayed for all messages sent and all replies received. A maximum, minimum and average round-trip time is also displayed. Error response and timed-out requests do not apply toward the average round-trip time.

Multiple Response Round-trip Connectivity Test Sample Output

```
A:router1> oam sdp-ping 6 resp-sdp 101 size 1514 count 5
Request Response RTT
-----
1 Success 10ms
2 Success 15ms
3 Success 10ms
4 Success 20ms
5 Success 5ms
Sent: 5 Received: 5
Min: 5ms Max: 20ms Avg: 12ms
```

type

Syntax	type [no] type
Context	config>saa>test
Description	<p>This command creates the context to provide the test type for the named test. Only a single test type can be configured.</p> <p>A test can only be modified while the test is in shutdown mode.</p> <p>Once a test type has been configured, the command can be modified by re-entering the command. The test type must be the same as the previously entered test type.</p> <p>To change the test type, the old command must be removed using the config>saa>test>no type command.</p>

vccv-ping

Syntax	vccv-ping <i>sdp-id:vc-id</i> [src-ip-address <i>ip-addr</i> dst-ip-address <i>ip-addr</i> pw-id <i>pw-id</i>] [reply-mode { ip-routed control-channel }] [fc <i>fc-name</i> [profile { in out }]] [size <i>octets</i>] [count <i>send-count</i>] [timeout <i>timeout</i>] [interval <i>interval</i>] [ttl <i>vc-label-ttl</i>]
Context	oam config>saa>test>type
Description	<p>This command configures a virtual circuit connectivity verification (VCCV) ping test. A vccv-ping test checks connectivity of a VLL in-band. It checks to verify that the destination (target) PE is the egress for the Layer 2 FEC. It provides for a cross-check between the data plane and the control plane. It is in-band, which means that the vccv-ping message is sent using the same encapsulation and along the same path as user packets in that VLL. The vccv-ping test is the equivalent of the lsp-ping test for a VLL service. The vccv-ping reuses an lsp-ping message format and can be used to test a VLL configured over an MPLS or GRE SDP.</p>

Note that VCCV ping can be initiated on TPE or SPE. If initiated on the SPE, the **reply-mode** parameter must be used with the ip-routed value. The ping from the TPE can either have values or the values can be omitted.

If a VCCV ping is initiated from a TPE to a neighboring SPE (one segment only) it is sufficient to only use the *sdpid:vcid* parameter. However, if the ping is across two or more segments, at the least the *sdpId:vcId*, **src-ip-address** *ip-addr*, **dst-ip-address** *ip-addr*, **ttl** *vc-label-ttl* and **pw-id** *pw-id* parameters are used where:

- the *src-ip-address* is the system IP address of the router preceding the destination router
- the *pw-id* is actually the VC ID of the last pseudowire segment
- the *vc-label-ttl* must have a value equal to or greater than the number of pseudowire segments

Parameters *sdp-id:vc-id* — Identifies the virtual circuit of the pseudowire being tested. The VC ID needs to exist on the local router and the far-end peer needs to indicate that it supports VCCV to allow the user to send a vccv-ping message.

This is a mandatory parameter.

Values sdp-id: 1 to 17407
 vc-id: 1 to 2147483647

src-ip-address *ip-addr* — Specifies the source IP address

Values ipv4-address: a.b.c.d

dst-ip-address *ip-addr* — Specifies the destination IP address

Values ipv4-address: a.b.c.d

pw-id *pw-id* — Specifies the pseudowire ID to be used for performing a **vccv-ping** operation. The pseudowire ID is a non-zero, 32-bit connection ID required by the FEC 128, as defined in RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*.

Values 0 to 4294967295

reply-mode {**ip-routed** | **control-channel**} — Specifies the method for sending the reply message to the far-end 7705 SAR.

This is a mandatory parameter.

Values **ip-routed** — Indicates a reply mode out-of-band using UDP IPv4
 control-channel — Indicates a reply mode in-band using vccv control channel

Default control-channel

fc *fc-name* — Indicates the forwarding class of the MPLS echo request packets. The actual forwarding class encoding is controlled by the network egress LSP-EXP mappings.

The LSP-EXP mappings on the receive network interface control the mapping back to the internal forwarding class used by the far-end 7705 SAR that receives the message request. The egress mappings of the egress network interface on the far-end router control the forwarding class markings on the return reply message. The LSP-EXP mappings on the receive network interface control the mapping of the message reply back at the originating SR.

Default be

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

profile {**in** | **out**} — Specifies the profile state of the MPLS echo request encapsulation

Default out

timeout *timeout* — Specifies the amount of time that the router will wait for a message reply after sending the message request. Upon the expiration of message timeout, the requesting router assumes that the message response will not be received. A “request timeout” message is displayed by the CLI for each message request sent that expires. Any response received after the request times out will be silently discarded.

This value is used to override the default timeout value.

Default 5

Values 1 to 10

interval *interval* — Specifies the minimum amount of time that must expire before the next message request is sent.

If the **interval** is set to 1 second, and the **timeout** value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

This parameter is used to override the default request message send interval.

Default 1

Values 1 to 10

size *octets* — Specifies the VCCV ping echo request packet size in octets, expressed as a decimal integer. The request payload is padded with zeroes to the specified size.

Default 88

Values 88 to 9198

count *send-count* — The number of messages to send, expressed as a decimal integer. The count parameter is used to override the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent. The message interval value must be expired before the next message request is sent.

Default 1

Values 1 to 100

ttl *vc-label-ttl* — Specifies the time-to-live value for the vc-label of the echo request message. The outer label TTL is still set to the default of 255 regardless of this value.

Values 1 to 255

Sample Output

Ping from TPE to TPE:

```
*A:ALU-dut-b_a# oam vccv-ping 1:1 src-ip-address 5.5.5.5 dst-ip-address 3.3.3.3 pw-id
1 ttl 3
VCCV-PING 1:1 88 bytes MPLS payload
Seq=1, reply from 3.3.3.3 via Control Channel
      udp-data-len=32 rtt=10ms rc=3 (EgressRtr)

---- VCCV PING 1:1 Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min = 10.0ms, avg = 10.0ms, max = 10.0ms, stddev < 10ms
```

Ping from TPE to SPE:

```

*A:ALU-dut-b_a# oam vccv-ping 1:1
VCCV-PING 1:1 88 bytes MPLS payload
Seq=1, reply from 4.4.4.4 via Control Channel
      udp-data-len=32 rtt<10ms rc=8 (DSRtrMatchLabel)

---- VCCV PING 1:1 Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min < 10ms, avg < 10ms, max < 10ms, stddev < 10ms

*A:ALU-dut-b_a# oam vccv-ping 1:1 src-ip-address 4.4.4.4 dst-ip-address 5.5.5.5 ttl 2
pw-id 200
VCCV-PING 1:1 88 bytes MPLS payload
Seq=1, reply from 5.5.5.5 via Control Channel
      udp-data-len=32 rtt<10ms rc=8 (DSRtrMatchLabel)

---- VCCV PING 1:1 Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min < 10ms, avg < 10ms, max < 10ms, stddev < 10ms

```

Ping from SPE (on single or multi-segment):

```

*A:ALU-dut-b_a# oam vccv-ping 4:200 reply-mode ip-routed
VCCV-PING 4:200 88 bytes MPLS payload
Seq=1, reply from 5.5.5.5 via IP
      udp-data-len=32 rtt<10ms rc=8 (DSRtrMatchLabel)

---- VCCV PING 4:200 Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min < 10ms, avg < 10ms, max < 10ms, stddev < 10ms

*A:ALU-dut-b_a# oam vccv-ping 4:200 reply-mode ip-routed src-ip-address 5.5.5.5 dst-
ip-address 3.3.3.3 ttl 2 pw-id 1
VCCV-PING 4:200 88 bytes MPLS payload
Seq=1, reply from 3.3.3.3 via IP
      udp-data-len=32 rtt<10ms rc=3 (EgressRtr)

---- VCCV PING 4:200 Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min < 10ms, avg < 10ms, max < 10ms, stddev < 10ms

```

OAM SAA Commands

saa

Syntax	saa <i>test-name</i> [owner <i>test-owner</i>] { start stop }
Context	oam
Description	This command starts or stops an SAA test.
Parameters	<p><i>test-name</i> — Specifies the name of the SAA test to be run. The test name must already be configured in the config>saa>test context.</p> <p>owner <i>test-owner</i> — Specifies the owner of an SAA operation, up to 32 characters in length</p> <p>Values If a <i>test-owner</i> value is not specified, tests created by the CLI have a default owner “TiMOS CLI”</p> <p>start — Starts the test. A test cannot be started if the same test is still running.</p> <p>A test cannot be started if it is in a shutdown state. An error message and log event will be generated to indicate a failed attempt to start an SAA test run.</p> <p>stop — Stops a test in progress. A log message will be generated to indicate that an SAA test run has been aborted.</p>

Show Commands

saa

Syntax	saa [<i>test-name</i>] [<i>owner test-owner</i>]
Context	show>saa
Description	<p>This command displays information about the SAA test.</p> <p>If no specific test is specified, a summary of all configured tests is displayed.</p> <p>If a specific test is specified, then detailed test results for that test are displayed for the last three occurrences that this test has been executed, or since the last time the counters have been reset via a system reboot or clear command.</p>
Parameters	<p><i>test-name</i> — Specifies the SAA test to display. The test name must already be configured in the config>saa>test context.</p> <p>This is an optional parameter.</p> <p><i>owner test-owner</i> — Specifies the owner of an SAA operation up to 32 characters in length.</p> <p>Default If a <i>test-owner</i> value is not specified, tests created by the CLI have a default owner “TiMOS CLI”</p>
Output	SAA Output — The following table describes SAA fields.

Table 45: SAA Field Descriptions

Label	Description
Test name	Displays the name of the test
Owner name	Displays the test owner’s name
Administrative status	Indicates the administrative state of the test
Test type	Identifies the type of test configured
Test runs since last clear	Indicates the total number of tests performed since the last time the tests were cleared
Number of failed tests run	Specifies the total number of tests that failed
Last test result	Indicates the last time a test was run

Sample Output

The following displays an SAA test result:

```
*A:SR-3>config>saa>test$ show saa
```

```
=====
SAA Test Information
=====
Test name           : test5
Owner name          : reuben
Administrative status : Enabled
Test type           : sdp-ping 600 resp-sdp 700 fc "nc" count 50
Test runs since last clear : 1
Number of failed test runs : 0
Last test result     : Success
-----
Threshold
Type           Direction Threshold Value      Last Event           Run #
-----
Latency-in    Rising      None      None      Never              None
              Falling      None      None      Never              None
Latency-out   Rising      None      None      Never              None
              Falling      None      None      Never              None
Latency-rt    Rising      50        None      Never              None
              Falling      50        10        04/23/2008 22:29:40 1
Loss-in       Rising      None      None      Never              None
              Falling      None      None      Never              None
Loss-out      Rising      None      None      Never              None
              Falling      None      None      Never              None
Loss-rt       Rising      8         None      Never              None
              Falling      8         0         04/23/2008 22:30:30 1
=====
*A:SR-3>config>saa>test$
```

Clear Commands

saa

Syntax	saa-test [<i>test-name</i>] [owner <i>test-owner</i>]
Context	clear
Description	This command clears the SAA results for the specified test and the history for the test. If the test name is omitted, all the results for all tests are cleared.
Parameters	<i>test-name</i> — Specifies the SAA test to clear. The test name must already be configured in the config>saa>test context. owner <i>test-owner</i> — Specifies the owner of an SAA operation, up to 32 characters in length
Default	If a <i>test-owner</i> value is not specified, tests created by the CLI have a default owner “TiMOS CLI”

Debug Commands

lsp-ping-trace

Syntax	lsp-ping-trace [tx rx both] [raw detail] no lsp-ping-trace
Context	debug>oam
Description	This command enables debugging for lsp-ping.
Parameters	tx rx both — Specifies the direction for the LSP ping debugging: TX, RX, or both RX and TX raw detail — Displays output for the debug mode

Tools Command Reference

Command Hierarchies

- [Tools Dump Commands](#)
- [Tools Perform Commands](#)

Tools Dump Commands

```

tools
  — dump
    — ppp port-id
    — router router-instance
      — ldp
        — fec prefix ip-prefix/mask
        — fec vc-type {ethernet | vlan} vc-id vc-id
        — instance
        — interface [ip-int-name | ip-address]
        — memory-usage
        — peer ip-address
        — session [ip-addr[:label-space]] [connection | peer | adjacency]
        — sockets
        — timers
      — mpls
        — ftn [endpoint endpoint | sender sender | nexthop nexthop | lsp-id lsp-id
              | tunnel-id tunnel-id | label start-label end-label]
        — ilm [endpoint endpoint | sender sender | nexthop nexthop | lsp-id lsp-id
              | tunnel-id tunnel-id | label start-label end-label]
        — lspinfo [detail]
        — memory-usage
    — system-resources slot-number

```

Tools Perform Commands

```

tools
  — perform
    — cron
      — action
        — stop [action-name] [owner action-owner] [all]
    — ima
      — reset [bundle-id]
    — log
      — test-event
    — router [router-instance]
      — mpls
        — resignal lsp lsp-name path path-name
        — trap-suppress number-of-traps time-interval
    — security
      — authentication-server-check server-address ip-address [port port] user-name
        DHCP client user name password password secret key [source-address ip-
        address] [timeout seconds] [router router-instance]

```

Tools Configuration Commands

- [Generic Commands on page 345](#)
- [Dump Commands on page 346](#)
- [Router Commands on page 347](#)

Generic Commands

tools

Syntax	tools
Context	<root>
Description	This command creates the context to enable useful tools for debugging purposes.
Default	none

Dump Commands

dump

Syntax	dump
Context	tools
Description	This command creates the context to display information for debugging purposes.
Default	none

ppp

Syntax	ppp <i>port-id</i>
Context	tools>dump
Description	This command displays PPP information for a port.
Default	none
Parameters	<i>port-id</i> — specifies the port ID
	Syntax: <i>port-id</i> <i>slot/mda/port[.channel]</i> bundle <i>bundle-type-slot/mda.bundle-num</i> bundle keyword type ima, ppp bundle-num1 to 10

system-resources

Syntax	system-resources <i>slot-number</i>
Context	tools>dump
Description	This command displays system resource information.
Default	none
Parameters	<i>slot-number</i> — Specifies a specific slot to view system resources information.

Router Commands

router

Syntax	router <i>router-instance</i>									
Context	tools>dump tools>perform									
Description	This command enables tools for the router instance.									
Default	none									
Parameters	router <i>router-instance</i> — specifies the router name and service ID									
	<table><tr><td>Values</td><td><i>router-name:</i></td><td>Base, management</td></tr><tr><td></td><td><i>service-id:</i></td><td>1 to 2147483647</td></tr><tr><td>Default</td><td></td><td>Base</td></tr></table>	Values	<i>router-name:</i>	Base, management		<i>service-id:</i>	1 to 2147483647	Default		Base
Values	<i>router-name:</i>	Base, management								
	<i>service-id:</i>	1 to 2147483647								
Default		Base								

fec

Syntax	fec prefix <i>ip-prefix/mask</i> fec vc-type { ethernet vlan } vc-id <i>vc-id</i>								
Context	tools>dump>router>ldp								
Description	This command displays information for an LDP FEC.								
Default	none								
Parameters	<i>ip-prefix/mask</i> — specifies the IP prefix and host bits <table><tr><td>Values</td><td>host bits:</td><td>must be 0</td></tr><tr><td></td><td>mask:</td><td>0 to 32</td></tr></table> <p>vc-type — Specifies the VC type signaled for the spoke or mesh binding to the far end of an SDP. The VC type is a 15-bit quantity containing a value that represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the vc-type command can still be used to define the dot1q value expected by the far-end provider equipment. A change of the binding's VC type causes the binding to signal the new VC type to the far end when signaling is enabled.</p> <p>VC types are derived according to IETF <i>draft-martini-l2circuit-trans-mpls</i>.</p> <ul style="list-style-type: none">• Ethernet — The VC type value for Ethernet is 0x0005.• VLAN — The VC type value for an Ethernet VLAN is 0x0004. <p><i>vc-id</i> — Specifies the virtual circuit identifier</p> <table><tr><td>Values</td><td>1 to 4294967295</td></tr></table>	Values	host bits:	must be 0		mask:	0 to 32	Values	1 to 4294967295
Values	host bits:	must be 0							
	mask:	0 to 32							
Values	1 to 4294967295								

ftn

Syntax	ftn [endpoint <i>endpoint</i> sender <i>sender</i> nexthop <i>nexthop</i> lsp-id <i>lsp-id</i> tunnel-id <i>tunnel-id</i> label <i>start-label end-label</i>]
Context	tools>dump>router>mpls
Description	This command displays FEC-to-NHLFE (FTN) dump information for MPLS. (NHLFE is the acronym for Next Hop Label Forwarding Entry.)
Default	none
Parameters	<p>endpoint <i>endpoint</i> — specifies the IP address of the last hop</p> <p>Values a.b.c.d</p> <p>sender <i>sender</i> — specifies the IP address of the sender</p> <p>Values a.b.c.d</p> <p>nexthop <i>nexthop</i> — specifies the IP address of the next hop</p> <p>Values a.b.c.d</p> <p>lsp-id <i>lsp-id</i> — specifies the label switched path that is signaled for this entry</p> <p>Values 0 to 65535</p> <p>tunnel-id <i>tunnel-id</i> — specifies the SDP ID</p> <p>Values 0 to 65535</p> <p>label <i>start-label end-label</i> — specifies the label range for the information dump</p> <p>Values start-label — 32 to 131071 end-label — 32 to 131071</p>

ilm

Syntax	ilm [endpoint <i>endpoint</i> sender <i>sender</i> nexthop <i>nexthop</i> lsp-id <i>lsp-id</i> tunnel-id <i>tunnel-id</i> label <i>start-label end-label</i>]
Context	tools>dump>router>mpls
Description	This command displays incoming label map (ILM) information for MPLS.
Default	none
Parameters	<p>endpoint <i>endpoint</i> — specifies the IP address of the last hop</p> <p>Values a.b.c.d</p> <p>sender <i>sender</i> — specifies the IP address of the sender</p> <p>Values a.b.c.d</p>

nexthop *nexthop* — specifies the IP address of the next hop

Values a.b.c.d

lsp-id *lsp-id* — specifies the label switched path that is signaled for this entry

Values 0 to 65535

tunnel-id *tunnel-id* — specifies the SDP ID

Values 0 to 65535

label *start-label end-label* — specifies the label range for the information dump

Values start-label — 32 to 131071

end-label — 32 to 131071

instance

Syntax	instance
Context	tools>dump>router>ldp
Description	This command displays information for an LDP instance.

interface

Syntax	interface [<i>ip-int-name</i> <i>ip-address</i>]
Context	tools>dump>router>ldp
Description	This command displays information for an LDP interface.
Default	none
Parameters	<i>ip-int-name</i> — specifies the interface name <i>ip-address</i> — specifies the IP address

ldp

Syntax	ldp
Context	tools>dump>router
Description	This command enables dump tools for LDP.
Default	none

lspinfo

Syntax	lspinfo [detail]
Context	tools>dump>router>mpls
Description	This command displays LSP information for MPLS.
Default	none

memory-usage

Syntax	memory-usage
Context	tools>dump>router>ldp
Description	This command displays memory usage information for the specific context (LDP or MPLS).
Default	none

mpls

Syntax	mpls
Context	tools>dump>router
Description	This command enables the context to display MPLS information.
Default	none

peer

Syntax	peer <i>ip-address</i>
Context	tools>dump>router>ldp
Description	This command displays information for an LDP peer.
Default	none
Parameters	<i>ip-address</i> — specifies the IP address

session

Syntax	session [<i>ip-address</i> [:<i>label</i> <i>space</i>] [<i>connection</i> <i>peer</i> <i>adjacency</i>]
---------------	---

Context	tools>dump>router>ldp
Description	This command displays information for an LDP session.
Default	none
Parameters	<i>ip-address</i> — specifies the IP address of the LDP peer <i>label-space</i> — specifies the label space identifier that the router is advertising on the interface connection — displays connection information peer — displays peer information adjacency — displays hello adjacency information

sockets

Syntax	sockets
Context	tools>dump>router>ldp
Description	This command displays information for all sockets being used by the LDP protocol.
Default	none

timers

Syntax	timers
Context	tools>dump>router>ldp
Description	This command displays timer information for LDP.
Default	none

Tools Performance Commands

perform

Syntax	perform
Context	tools
Description	This command enables the context to enable tools to perform specific tasks.
Default	none

action

Syntax	action
Context	tools>perform>cron
Description	This command enables the context to stop the execution of a script started by CRON action. See the stop command.

authentication-server-check

Syntax	authentication-server-check server-address <i>ip-address</i> [port <i>port</i>] user-name <i>dhcp-client-user-name</i> password <i>password</i> secret <i>key</i> [source-address <i>ip-address</i>] [timeout <i>seconds</i>] [router <i>router-instance</i>]		
Context	tools>perform>security		
Description	This command checks connection to the RADIUS server.		
Parameters	router <i>router-instance</i> — specifies the router name or service ID		
	Values	<i>router-name:</i>	Base, management
		<i>service-id:</i>	1 to 2147483647
	Default	Base	
	server-address <i>ip-address</i> — specifies the server ID		
	Values	a.b.c.d	
	port <i>port</i> — specifies the port ID		
	Values	1 to 65535	
	user-name <i>DHCP client user name</i> — specifies the DHCP client		
	Values	256 characters maximum	

password *password* — specifies the CLI access password

Values 10 characters maximum

secret *key* — specifies the authentication key

Values 20 chars max

source-address *ip-address* — specifies the source IP address of the DHCP relay messages

Values a.b.c.d

timeout *seconds* — specifies the timeout in seconds

Values 1 to 90

cron

Syntax	cron
Context	tools>perform
Description	This command enables the context to perform CRON (scheduling) control operations.
Default	none

ima

Syntax	ima
Context	tools>perform
Description	This command enables the context to perform IMA operations.
Default	none

log

Syntax	log
Context	tools>perform
Description	This command enables event logging tools.

mpls

Syntax	mpls
Context	tools>perform>router

Description This command enables the context to perform specific MPLS tasks.

Default none

reset

Syntax **reset** *bundle-id*

Context tools>perform>ima

Description This command resets an IMA bundle to the start-up state.

Default none

Parameters *bundle-id* — specifies the IMA bundle ID

Syntax: *bundle-id* bundle-ima-slot/mda.bundle-num
 bundle-ima keyword
 bundle-num 1 to 10

resignal

Syntax **resignal** **lsp** *lsp-name* **path** *path-name*

Context tools>perform>router>mpls

Description This command resignals specified LSP paths.

Default none

Parameters **lsp** *lsp-name* — specifies the LSP name. The LSP name can be up to 32 characters long and must be unique.

path *path-name* — specifies the name for the LSP path, up to 32 characters in length

security

Syntax **security**

Context tools>perform

Description This command provides tools for testing security.

stop

Syntax **stop** [*action-name*] [**owner** *action-owner*] [**all**]

Context	tools>perform>cron>action
Description	This command stops execution of a script started by CRON action.
Parameters	<i>action-name</i> — specifies the action name
Values	maximum 32 characters
owner	<i>action-owner</i> — specifies the owner name
Default	TiMOS CLI
all	— specifies to stop all CRON scripts

test-event

Syntax	test-event
Context	tools>perform>log
Description	This command generates a test event.

trap-suppress

Syntax	trap-suppress [<i>number-of-traps</i>] [<i>time-interval</i>]
Context	tools>perform>router>mpls
Description	This command modifies thresholds for trap suppression.
Default	none
Parameters	<i>number-of-traps</i> — specifies the number of traps in multiples of 100. An error message is generated if an invalid value is entered.
Values	100 to 1000
	<i>time-interval</i> — specifies the timer interval in seconds
Values	1 to 300

Standards and Protocol Support

Standards Compliance

IEEE 802.1p/q VLAN Tagging
IEEE 802.3 10BaseT
IEEE 802.3u 100BaseTX
IEEE 802.3x Flow Control
IEEE 802.3z 1000BaseSX/LX

Protocol Support

LDP

RFC 5036 LDP Specification

MPLS

RFC 3031 MPLS Architecture
RFC 3032 MPLS Label Stack Encoding
RFC 4379 Detecting Multi-Protocol Label
Switched (MPLS) Data Plane Failures

DIFFERENTIATED SERVICES

RFC 2474 Definition of the DS Field in the IPv4
and IPv6 Headers
RFC 2597 Assured Forwarding PHB Group
RFC 2598 An Expedited Forwarding PHB
RFC 3140 Per-Hop Behavior Identification Codes

TCP/IP

RFC 768 UDP
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 Telnet
RFC 1350 The TFTP Protocol (Rev. 2)
RFC 1812 Requirements for IPv4 Routers

PPP

RFC 1332 PPP IPCP
RFC 1661 PPP
RFC 1662 PPP in HDLC-like Framing
RFC 1989 PPP Link Quality Monitoring
RFC 1990 The PPP Multilink Protocol (MP)

ATM

RFC 2514 Definitions of Textual Conventions and
OBJECT_IDENTITIES for ATM
Management, February 1999
RFC 2515 Definition of Managed Objects for ATM
Management, February 1999
RFC 2684 Multiprotocol Encapsulation over ATM
Adaptation Layer 5
af-tm-0121.000 Traffic Management Specification
Version 4.1, March 1999
ITU-T Recommendation I.610 - B-ISDN Operation
and Maintenance Principles and Functions version
11/95
ITU-T Recommendation I.432.1 - B-ISDN user-
network interface - Physical layer specification:
General characteristics
GR-1248-CORE - Generic Requirements for
Operations of ATM Network Elements (NEs). Issue
3 June 1996
GR-1113-CORE - Bellcore, Asynchronous Transfer
Mode (ATM) and ATM Adaptation Layer (AAL)
Protocols Generic Requirements, Issue 1, July 1994

PSEUDOWIRES

- RFC 4385 Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
- RFC 4446 IANA Allocation for PWE3
- RFC 4447 Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)
- RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks
- RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
- RFC 4717 Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks
- RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
- RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires

RADIUS

- RFC 2865 Remote Authentication Dial In User Service
- RFC 2866 RADIUS Accounting

SSH

- draft-ietf-secsh-architecture.txt SSH Protocol Architecture
- draft-ietf-secsh-userauth.txt SSH Authentication Protocol
- draft-ietf-secsh-transport.txt SSH Transport Layer Protocol
- draft-ietf-secsh-connection.txt SSH Connection Protocol
- draft-ietf-secsh-newmodes.txt SSH Transport Layer Encryption Modes

TACACS+

- draft-grant-tacacs-02.txt The TACACS+ Protocol

SYNCHRONIZATION

- G.813 Timing characteristics of SDH equipment slave clocks (SEC)
- G.8261 Timing and synchronization aspects in packet networks
- G.8262 Timing characteristics of synchronous Ethernet equipment slave clock
- GR 1244 CORE Clocks for the Synchronized Network: Common Generic Criteria

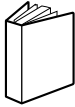
NETWORK MANAGEMENT

- ITU-T X.721: Information technology- OSI-Structure of Management Information
- ITU-T X.734: Information technology- OSI-Systems Management: Event Report Management Function
- M.3100/3120 Equipment and Connection Models
- TMF 509/613 Network Connectivity Model
- RFC 1157 SNMPv1
- RFC 1305 Network Time Protocol (Version 3) Specification, Implementation and Analysis
- RFC 1907 SNMPv2-MIB
- RFC 2011 IP-MIB
- RFC 2012 TCP-MIB
- RFC 2013 UDP-MIB
- RFC 2030 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
- RFC 2138 RADIUS
- RFC 2571 SNMP-FRAMEWORKMIB
- RFC 2572 SNMP-MPD-MIB
- RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
- RFC 2574 SNMP-USER-BASED-SMMIB
- RFC 2575 SNMP-VIEW-BASED ACM-MIB
- RFC 2576 SNMP-COMMUNITY-MIB
- RFC 2665 EtherLike-MIB
- RFC 2819 RMON-MIB
- RFC 2863 IF-MIB
- RFC 2864 INVERTED-STACK-MIB
- RFC 3014 NOTIFICATION-LOG MIB
- RFC 3164 The BSD Syslog Protocol
- RFC 3273 HCRMON-MIB
- RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413 Simple Network Management Protocol (SNMP) Applications
- RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3418 SNMP MIB
- draft-ietf-disman-alarm-mib-04.txt
- draft-ietf-mpls-ldp-mib-07.txt
- IANA-IFTtype-MIB

Proprietary MIBs

TIMETRA-ATM-MIB.mib
TIMETRA-CAPABILITY-7705-V1.mib
TIMETRA-CFLOWD-MIB.mib
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-LDP-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MPLS-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-PPP-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-ROUTE-POLICY-MIB.mib
TIMETRA-SAP-MIB.mib
TIMETRA-SDP-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib

Customer documentation and product support



Customer documentation

<http://www.alcatel-lucent.com/osds>

Product manuals and documentation updates are available through the Alcatel-Lucent Support Documentation and Software Download service at [alcatel-lucent.com](http://www.alcatel-lucent.com). If you are a new user and require access to this service, please contact your Alcatel-Lucent sales representative.



Technical support

<http://www.alcatel-lucent.com/support>



Customer documentation feedback

documentation.feedback@alcatel-lucent.com

